

# Quantum Authenticated Key Expansion with Key Recycling

Wen Yu Kon, Jefferson Chu, Kevin Han Yong Loh, Obada Alia, Omar Amer, Marco Pistoia, Kaushik Chakraborty, and Charles Lim

Global Technology Applied Research, JPMorganChase

Data privacy and authentication are two main security requirements for remote access and cloud services. While QKD has been explored to address data privacy concerns, often-times its use is separate from the client authentication protocol despite implicitly providing authentication. Here, we present a *quantum authentication key expansion* (QAKE) protocol that (1) integrates both authentication and key expansion within a single protocol, and (2) provides key recycling property – allowing all authentication keys to be reused. We analyse the security of the protocol in a QAKE framework adapted from a classical authentication key exchange (AKE) framework, providing separate security conditions for authentication and data privacy. We experimentally implemented the protocol with appropriate post-selection. Additional results on the security of pseudorandom basis generation in QAKE and decoy state BB84 are provided.

## 1 Introduction

In this distributed digital era, remote access and cloud services are becoming increasingly popular, where a client device can access another device or a server, at any time, and from anywhere. Such services typically has two main security requirements: authentication and data privacy. To restrict access to these devices/servers for security or compliance reasons, such as in banking, healthcare, or government, it is necessary for the identity of the client to be authenticated. Data privacy, on the other hand, ensures that the data transferred between the client and server, which may contain highly sensitive business or personal information (e.g. while looking at a remote desktop display of client details), is private from any eavesdroppers. Fig. 1 presents a scenario where such a central server can identify its end-users via authentication and aid in the key generation between distant end-users.

Many current remote access and cloud services establishes a *virtual private networks* (VPNs)

Wen Yu Kon: [wenyu.kon@jpmchase.com](mailto:wenyu.kon@jpmchase.com)

Kaushik Chakraborty: [kaushik.chakraborty@jpmchase.com](mailto:kaushik.chakraborty@jpmchase.com)

by means of internet protocols like IPsec. Such protocols rely on either *public key infrastructure* (PKI) or symmetric key cryptography to provide the necessary security requirements. PKI offers convenient key exchange without pre-shared secrets, but older schemes such as RSA [33] are vulnerable to quantum attacks [35]. While post-quantum PKI schemes such as lattice-based cryptography that have been standardized by NIST [27] are believed to be quantum-safe, PKI remains susceptible to *harvest-now-decrypt-later* attacks. On the other hand, symmetric key cryptography offers stronger long-term data privacy, but requires pre-shared secrets keys that have to be regularly refreshed after a fixed number of uses or duration [2], posing a practical challenge.

To address the need for key refresh in symmetric key cryptography, internet service providers explored the use of *quantum key distribution* (QKD) for key expansion. In this process, a separate authentication protocol is utilised to authenticate the client of the remote access service before utilising QKD to expand secret keys shared between the client and server. Therefore, we propose a *quantum authenticated key expansion* (QAKE) protocol that improves efficiency by combining all entity and message authentication steps into two authentication steps: one from Alice to Bob and one from Bob to Alice. This integrated approach provides both client-server authentication and key expansion within a single protocol session.

Another useful property for authentication to have in practice is key recycling [17], where all secret keys (e.g. authentication keys) remain secure if the protocol succeeds. In the context of cloud services, it eliminates the need for cloud service providers to update the clients' authentication key across all its cloud servers after every session, saving significant communication resources. Authentication schemes with key recycling have been proposed, but they either do not recycle the full authentication key (require recycling of an OTP key, which we call authentication masking key) [9, 28], or do not account for experimental imperfections such as loss and multi-photon events [17, 23, 29]. The QAKE proposed here is designed with key recycling in mind, using the corrected bitstring, which is expected to have high min-entropy when the protocol passes,

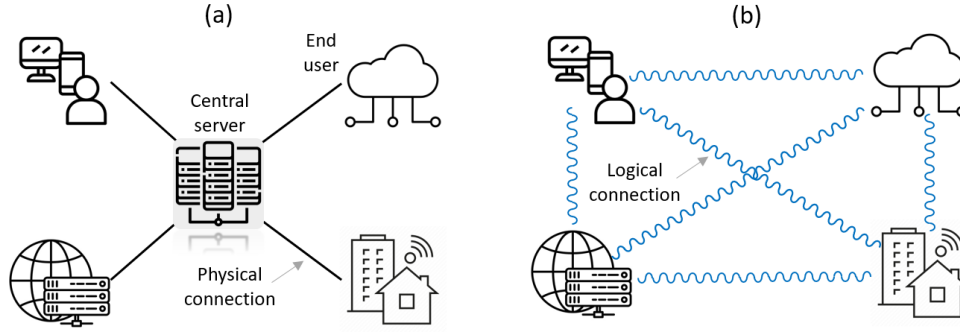


Figure 1: Schematic for end user key generation via a central server in a star network topology. (a) End users share a direct physical connection to the central server, and can establish keys with it via the authenticated key exchange protocol. (b) By performing operations on the keys, the central server is able aid the end users establish shared keys between them without the end users sharing a direct link.

to mask the authentication key and authentication masking keys and allow them to be reused.

To analyse both the authentication and key exchange tasks in QAKE, we adapt the classical authenticated key exchange (AKE) framework [13], where separate security conditions for authentication and key exchange are presented. This highlights the role of various protocol components in providing data privacy and authentication, and allows for comparison with the case of two separate protocols – one for key exchange and one for authentication.

We demonstrated the protocol using commercial QKD devices. The raw data collected from the QKD devices are post-processed offline through a software stack. This includes error correction by adapting the LDPC IP cores from Xilinx [1], and privacy amplification using Toeplitz hashing. With a detection rate of about  $10^{-4}$  and a quantum bit error rate (QBER) of about 2 %, the QAKE protocol is able to provide a key rate of about  $10^{-5}$ .

## 2 Quantum Authenticated Key Exchange

### 2.1 Message Authentication in QKD

In QKD, message authentication, which can double as entity authentication, typically relies on information-theoretic message authentication protocols (such as Wegman-Carter [9]) to authenticate every message sent between the parties. These message authentication protocols have composable security and can thus be used in QKD securely. Oftentimes, the QKD keys generated are then utilized for the next session’s authentication.

However, a direct utilization of the typical protocol design above may not be desirable in the practical setting. While authenticating every message may

simplify the security analysis, it might lead to significant authentication costs due to the shared randomness required, thereby reducing key rates. This issue may be exacerbated by for instance the use of Cascade [5] as a means for error correction since it requires multiple rounds of communication, each of which may need to be authenticated if we naively apply message authentication to every communication steps. This is addressed in Ref. [21], where authentication is performed only in the last two communication steps, thereby reducing the authentication costs.

Using QKD keys for future authentication sessions requires updating the authentication keys after each use. If the authentication keys can remain static, this would enable a wider range of applications. For instance, in applications where a clients access services at multiple locations (e.g. ATM), authentication keys may be stored in multiple regional databases. Updating the authentication keys in all databases after every authentication session would be operationally inefficient.

### 2.2 QAKE Protocol

As such, the QAKE protocol focuses on incorporating the entity authentication check into the QKD process in an efficient manner, namely: (1) reducing authentication costs, (2) removing the need for key updating, (3) combining error verification with authentication, (4) secure reusing of privacy amplification seed.

To reduce communication costs, the QAKE protocol follows the proposal in Ref. [21] and performs authentication only twice, once to authenticate Alice (and communication transcript) and once to authenticate Bob. Since the order of certain steps in QKD is crucial for security, most notably that Bob’s measurement should occur before the basis is announced, careful design is necessary. For instance, we require that Bob announces his basis choice before

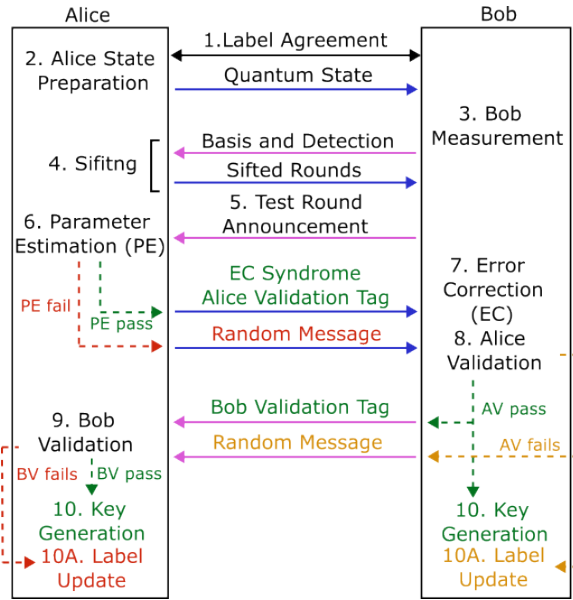


Figure 2: Summary of the QAKE protocol proposed. The protocol begins with both parties establishing the label to use, followed by Alice sending quantum states to Bob. Bob announces his basis choice and detected rounds and Alice responds with the sifted rounds. Bob announces the test round results, for which Alice can use for parameters estimation. If this passes, error correction and validation of Alice's identity would occur followed by validation of Bob's identity. Finally, the two parties independently decide whether to generate secret keys or update their label.

Alice announces hers for sifting. This prevents Eve from storing the quantum states and measuring them when the basis is announced since that requires Eve to commit to a response of Bob's measurement basis choice to Alice before Bob has actually selected the basis.

To remove the need for key updating, the idea of key recycling or reusing of authentication keys has been proposed. Early proposals of key recycling [9, 28] requires pre-sharing of authentication masking keys (one for each authentication) to act as a one-time pad for the authentication tag, which may be impractical in practice for lightweight devices (e.g. ATM cards). Later proposals [17, 23, 29] that only require updating of authentication masking keys when authentication fails require additional quantum communication separate from the QKD process for

message authentication, but the protocols proposed do not fully account for experimental imperfections (loss, errors, multi-photon events etc). Here, we propose the utilization of the corrected bitstring in QKD, where min-entropy can be guaranteed by the parameter estimation in QKD, as a means to protect the authentication key and authentication masking key when the protocol succeeds. Besides straightforwardly accounting for experimental imperfections via the QKD protocol, combining the quantum process for both protocols can reduce finite-size effects, since there need not be separate parameter estimation for both the process in QKD and authentication of Ref. [17, 23].

We also provide further improvements by having the message authentication scheme double as error verification, since the corrected bitstring is hashed there. This reduces the number of shared randomness between Alice and Bob that is utilized in the post-processing of the QKD protocol.

The final modification made is to allow the privacy amplification seed  $R$  to be pre-shared between Alice and Bob and reused for future privacy amplification. Unlike typical QKD protocols where Alice (or Bob) selects a random seed and publicly announces it, in this case, Alice and Bob do not announce  $R$ . As such, reusing  $R$  does not impact security since for quantum-proof strong extractors, the keys generated are close to independent on  $R$ . This use of a pre-shared random  $R$  could simplify practical implementation since the *field programmable gate array* (FPGA) used for privacy amplification can be pre-programmed with the seed and also reduce communication and authentication costs since  $R$  does not need to be sent from Alice to Bob.

To illustrate the effects of key recycling and reusing of privacy amplification seed  $R$ , we need to consider that the protocol can be repeated multiple times. We call each complete run of the protocol as a session, and assume that we can have up to  $n_{sess}$  sessions of the protocol. In each session, Alice and Bob exchange  $n_{rnd}$  quantum states and we call each quantum state exchange as a single round (like QKD).

---

**Protocol 1** Quantum Authenticated Key Exchange
 

---

*Goal.* Alice and Bob authenticates one another, and performs key exchange.

1. **Label Agreement:** Alice and Bob exchange  $\alpha$  and  $\alpha'$ . Alice (resp. Bob) sends  $\alpha$  (resp.  $\alpha'$ ) and receives  $\alpha'_r$  (resp.  $\alpha_r$ ), which results in a label choice  $\beta = \max\{\alpha, \alpha'_r\}$  (resp.  $\beta' = \max\{\alpha_r, \alpha'\}$ ).
2. **Alice State Preparation:** Alice randomly chooses a  $n_{rnd}$ -bit basis string  $\theta$ , a  $n_{rnd}$ -bit string  $X$  and a  $n_{rnd}$ -trit string  $v \in \{0, 1, 2\}^{n_{rnd}}$  according to probability distribution  $p_v$ . She then prepares  $n_{rnd}$  quantum systems  $Q_i$  in phase-randomised coherent BB84 states  $\left\{ \rho_{Q_i}^{\theta_i, X_i, \mu_{v_i}} \right\}_{i \in [1, n_{rnd}]}$ , with basis  $\theta_i$ , bit value  $X_i$ , and intensity  $\mu_{v_i}$ .
3. **Bob Measurement:** Alice sends  $Q^{n_{rnd}}$  to Bob, who measures subsystems  $Q_i$  using a randomly chosen basis  $\theta' \in \{0, 1\}^{n_{rnd}}$ , and records outcome  $X'_i$ . If Bob detects no clicks, he declares  $X'_i = \perp$ . If Bob detects multiple clicks, he randomly selects  $x'_i \in \{0, 1\}$ .
4. **Sifting:** Bob records the detection rounds,  $P = \{i : X'_i \neq \perp\}$ , and announces  $P$  and  $\theta'_P = \{\theta'_i : i \in P\}$  to Alice. Alice computes the sifted rounds  $P^{\text{sift}} = \{i : i \in P, \theta'_{i,r} = \theta_i\}$ , and forwards it to Bob.
5. **Test Round Announcement:** Bob randomly splits the sifted rounds into  $P_1^{\text{sift}}$  and  $P_2^{\text{sift}}$ , with  $|P_1^{\text{sift}}| = \lceil f_{P_1} |P^{\text{sift}}| \rceil$ , where  $f_{P_1}$  is some pre-determined fraction of rounds. Bob announces  $P_1^{\text{sift}}$ ,  $P_2^{\text{sift}}$  and  $X'_{P_1^{\text{sift}}}$ .
6. **Parameter Estimation:** Alice checks if: (1) the number of test rounds matches the expected number  $|P_{1,r}^{\text{sift}}| = \lceil f_{P_1} |P^{\text{sift}}| \rceil$ , (2) the number of sifted rounds exceeds a threshold,  $|P_r^{\text{sift}}| \geq P_{\text{tol}}^{\text{sift}}$ , (3) the lower bound on single-photon events in sets  $P_{2,r}^{\text{sift}}$  and  $P_{1,r}^{\text{sift}}$  (estimated via decoy state analysis) exceeds a threshold,  $\hat{N}_{P_{2,r}^{\text{sift}},1}^{\text{LB}} \geq N_{P_{2,r}^{\text{sift}},1}^{\text{tol}}$ ,  $\hat{N}_{P_{1,r}^{\text{sift}},1}^{\text{LB}} \geq N_{P_{1,r}^{\text{sift}},1}^{\text{tol}}$ , (4) the upper bound on single-photon bit-error rate in set  $P_{1,r}^{\text{sift}}$  (estimated via decoy-state analysis) falls below a threshold,  $\hat{e}_{\text{bit}, P_{1,r}^{\text{sift}},1}^{\text{UB}} \leq e_{\text{bit},1,\text{tol}}$ , and (5) the upper bound on bit error rate in set  $P_{1,r}^{\text{sift}}$  (estimated via Serfling bound) falls below a threshold,  $\hat{e}_{\text{bit}, P_{2,r}^{\text{sift}}}^{\text{UB}} \leq e_{\text{bit},\text{tol}}$ . If all checks pass, Alice sets  $D_{\text{PE}} = 1$ , otherwise she sets  $D_{\text{PE}} = 0$ .
7. **Error Correction:** If  $D_{\text{PE}} = 1$ , Alice generates a syndrome  $\text{syn} = f_{\text{syn}}(X_{P_{2,r}^{\text{sift}}})$  of length  $l_{\text{syn}}$  and forwards it to Bob, otherwise, Alice sends a random string of length  $l_{\text{syn}}$  to Bob. Bob receives the syndrome  $\text{syn}_r$  and computes the corrected bit string  $\hat{X}_{P_{2,r}^{\text{sift}},r} = f_{\text{ec}}(X'_{P_{2,r}^{\text{sift}}}, \text{syn}_r)$ .
8. **Alice Validation:** If  $D_{\text{PE}} = 1$ , Alice generates a tag  $T_{\text{AV}} = h_1(K_1^h, X_{P_{2,r}^{\text{sift}}} \| P_r \| \theta'_{P,r} \| P^{\text{sift}} \| X'_{P_1^{\text{sift}},r} \| P_{1,r}^{\text{sift}} \| P_{2,r}^{\text{sift}} \| \text{syn}) \oplus K_{1,\beta}^{\text{mask}}$  and forwards it to Bob, otherwise, Alice sends a random string of the same length as the tag. Bob receives tag  $T_{\text{AV},r}$  and generates verification tag  $\tilde{T}_{\text{AV}} = h_1(K_1^h, \hat{X}_{P_{2,r}^{\text{sift}}} \| P \| \theta'_P \| P_r^{\text{sift}} \| X'_{P_1^{\text{sift}},r} \| P_1^{\text{sift}} \| P_2^{\text{sift}} \| \text{syn}_r) \oplus K_{1,\beta'}^{\text{mask}}$  and checks if  $T_{\text{AV},r} = \tilde{T}_{\text{AV}}$ . If the tags matches, Bob validates Alice and output  $F_B = 1$ , otherwise, he sets  $F_B = 0$ .
9. **Bob Validation:** If  $F_B = 1$ , Bob generates a tag,  $T_{\text{BV}} = h_2(K_2, \hat{X}_{P_{2,r}^{\text{sift}}})$ , and sends  $T_{\text{BV}}$  to Alice. If  $F_B = 0$ , Bob sends a random string of the same length instead. Alice receives the tag  $T_{\text{BV},r}$ , and computes the verification tag,  $\tilde{T}_{\text{BV}} = h_2(K_2, X_{P_{2,r}^{\text{sift}}})$ . If  $T_{\text{BV},r} = \tilde{T}_{\text{BV}}$ , Alice validates Bob,  $D_{\text{BV}} = 1$ , otherwise, she sets  $D_{\text{BV}} = 0$ .
10. **Secret Key Generation and Label Update:** Alice decides whether to accept the session based on her parameter estimation and validation of Bob, i.e.  $F_A = D_{\text{PE}} \wedge D_{\text{BV}}$ . If Alice (resp. Bob) accepts the session and decides to perform key generation,  $F_A = 1$  (resp.  $F_B = 1$ ), she (resp. he) performs privacy amplification  $K_A = h_{\text{PA}}(R, X_{P_{2,r}^{\text{sift}}})$  (resp.  $K_B = h_{\text{PA}}(R, \hat{X}_{P_{2,r}^{\text{sift}}})$ ) and sets  $\alpha = \beta$  (resp.  $\alpha' = \beta'$ ), where  $K_A K_B$  are the cryptographically secure keys that can be used for other purposes. If key generation is not performed, the labels are updated, i.e. if  $F_A = 0$ , Alice updates her label  $\alpha = \beta + 1$  and if  $F_B = 0$ , Bob updates his label  $\alpha' = \beta' + 1$ .

---

The full  $n_{\text{sess}}$ -session protocol begins with two parties, Alice and Bob, sharing secrets  $S$  containing: (1) authentication keys  $K_1^h$  and  $K_2$ , (2) privacy amplification seed  $R$ , and (3) authentication masking key with  $m$  separate keys  $K_1^{\text{mask}} = \{K_{1,j}^{\text{mask}}\}_{j=1,\dots,m}$ .

Alice and Bob each has a label,  $\alpha$  and  $\alpha'$  respectively, that notes the secrets to utilise for the round, thereby allowing secrets to be replaced (by never using them again) when authentication fails. They also publicly share a  $\varepsilon_{\text{MAC},1}$ -almost XOR 2-universal hash

function  $h_1$  (uses authentication key  $K_1^h$ ), a  $\varepsilon_{\text{MAC},2}$ -almost strongly 2-universal hash function  $h_2$  (uses authentication key  $K_2$ ) to generate the authentication tags  $T_{AV}$  and  $T_{BV}$  respectively [28, 34, 36], and a 2-universal hash function  $h_{\text{PA}}$  (uses privacy amplification seed  $R$ ) for privacy amplification to generate secret keys [28, 36]. Alice and Bob also agrees on a fraction of rounds  $f_{P_1}$  to use as test rounds for parameter estimation and an error correction protocol which includes syndrome generation function  $f_{\text{syn}}$  (to generate a syndrome of length  $l_{\text{syn}}$ ) and error correction function  $f_{\text{ec}}$  (to correct the message using the syndrome). The protocol steps are summarised in Fig. 2, with additional details provided in protocol 1 below. We note here that the subscript  $r$  on any random variables represent the received variable, e.g.  $\alpha_r$  is received by Bob when  $\alpha$  is sent by Alice, and  $\wedge$  refers to the AND gate. Each protocol session is able to be triggered by either Alice and Bob at any time (e.g. when an ATM card is plugged into an ATM) by for instance using a handshake protocol without authentication. During the session, Alice and Bob update the parameters  $F_A$  and  $F_B$  respectively to bit 0 or 1, which indicates whether they wish to accept the session and generate a key. The values of  $F_A$  and  $F_B$  are initialised as  $\phi$  and is always reset independently by Alice and Bob to  $F_A = F_B = \phi$  at the end of each session if they participated in the session, but we analyse the security of the protocol at the point before this reset occurs. Note that if Alice and Bob did not participate in a session, their value of  $F_A$  and  $F_B$  respectively would remain as  $\phi$ .

### 3 Protocol Security

QKD, while achieving the task of authenticated key exchange (AKE) [26], separates the message authentication and key exchange tasks completely, and combines their security using composability arguments. This makes it difficult to analyse the QAKE protocol directly in the QKD security framework since (1) message authentication is only used in the final two communication steps, which may allow the adversary to alter the ordering of prior steps, and (2) the message authentication steps are also used to check for matching bit strings between Alice and Bob (correctness condition in QKD). Therefore, we introduce a QAKE security definition which includes both authentication and key exchange, similar to those discussed in Ref. [30].

#### 3.1 Multi-Session Security and Reduction to Single-session Security

Let  $\rho_0$  be the initial quantum state, where the shared secrets  $S$  are generated, and  $\mathcal{P}_i$  be the  $i$ -th session of the protocol. For simplicity, we assume that the sessions are sequential, i.e. one session must end

before a new session can begin, and we can express  $i$  sessions of the protocol as  $\mathcal{P}^i = \mathcal{P}_i \circ \dots \circ \mathcal{P}_1$ . For each session, we can consider an overall input state  $\rho^{\text{in}}$  shared across all parties that acts as an input to the channel  $\mathcal{P}_i$  and an output state  $\rho^{\text{out}} = \mathcal{P}_i(\rho^{\text{in}})$  shared by all parties at the end of each session. Note that the output state also acts as the input state to the next session. We define the security of the multi-session protocol by requiring the output state to be close to an ideal output state for every session, i.e. trace distance between output state and ideal output state is  $\Delta(\mathcal{P}^i(\rho_0), \rho^{\text{out}}) \leq \varepsilon$  for all  $i = 1, \dots, n_{\text{sess}}$ , where  $\rho^{\text{out}} \in \mathcal{S}'_{\text{out}}$  is an ideal output state satisfying QAKE security conditions (to be defined later). Since each session accepts the secrets (such as authentication key and privacy amplification seeds) as inputs, there could be input states where the secrets are correlated to the adversary. Therefore, the protocol cannot be composable in the usual sense – that  $\mathcal{P}_i$  is  $\varepsilon$ -close to an ideal functionality. However, assuming that these secrets are not additionally leaked between sessions via side-channels, we can restrict the input states to an ideal set of input states  $\mathcal{S}_{\text{in}}$  (to be defined later) that results in the output state being  $\varepsilon$ -close to an ideal output state<sup>1</sup>.

We can reduce the multi-session analysis to a single-session security with appropriate definitions of  $\mathcal{S}_{\text{in}}$  and  $\mathcal{S}'_{\text{out}}$ , where  $\mathcal{S}'_{\text{out}}$  contains an additional condition that the privacy for the secrets that are utilised in the next session be maintained. If the protocol maps  $\mathcal{S}_{\text{in}}$  to  $\mathcal{S}'_{\text{out}}$ , and  $\mathcal{S}'_{\text{out}} \subseteq \mathcal{S}_{\text{in}}$ , an inductive argument can be made that the protocol is secure – similar to composability arguments, except with restricted input states. This is presented formally as

**Theorem 1.** *Suppose we have the conditions:*

1. *The initial state is an ideal input state  $\rho_0 \in \mathcal{S}_{\text{in}}$ .*
2. *There exists an ideal output state which preserves any necessary secrets that is  $\varepsilon_{\text{sec,int}}$ -close to the output state of a single session  $\mathcal{P}_i$ , i.e. for any  $\sigma \in \mathcal{S}_{\text{in}}$ , there exists a state  $\rho \in \mathcal{S}'_{\text{out}}$  such that*

$$\Delta(\mathcal{P}_i(\sigma), \rho) \leq \varepsilon_{\text{sec,int}}.$$

3. *The set of ideal output states is a subset of the set of ideal input states  $\mathcal{S}'_{\text{out}} \subseteq \mathcal{S}_{\text{in}}$ .*

*Then, for all  $i \in [1, n_{\text{sess}}]$ , there exists  $\rho_i \in \mathcal{S}'_{\text{out}}$  such that*

$$\Delta(\mathcal{P}^i(\rho_0), \rho_i) \leq i\varepsilon_{\text{sec,int}}.$$

<sup>1</sup>Note that QKD implicitly requires such an assumption when authentication keys are carried between sessions, since any leakage of authentication keys outside of the QKD protocol can compromise QKD security. Additionally, if one can guarantee the input states are ideal (like QKD), it may be possible to define an equivalent protocol  $\mathcal{P}'_i$  that is composable, where the secrets are generated within each protocol session.

*Proof.* See Appendix C.1.  $\square$

The theorem reduces the security analysis to the analysis of single-session protocol.

### 3.2 Security Conditions

To analyse the single-session security, we define the set of ideal input states  $\mathcal{S}_{in}$  and output states  $\mathcal{S}'_{out}$ . We make two assumptions here, that the generated secret keys can be leaked to the adversary between sessions (e.g. if the keys are used for encryption), and that the bitstring  $X$  is no longer accessible to any party at the end of a session except what is announced or leaked during the session. We note that the latter assumption is also implicit in device-dependent QKD, where the bit values are

$$\rho_{LSE}^{in,jj'} = |jj'\rangle\langle jj'|_{\alpha\alpha'} \otimes \tau_{K_2 RK_{1,j}^{mask} \dots K_{1,m}^{mask}} \otimes \mathcal{E}_{K_1^h K_{1,j-1}^{mask} E_{j-1} \rightarrow E} \circ \dots \circ \mathcal{E}_{K_1^h K_{1,j'}^{mask} E_{j'} \rightarrow E_{j'+1}} (\tau_{K_1^h K_{1,j'}^{mask} \dots K_{1,j-1}^{mask}} \otimes \rho_{E_{j'}}), \quad (1)$$

where  $\tau_A = \sum_{a \in \mathcal{A}} \frac{1}{|\mathcal{A}|} |a\rangle\langle a|$  is a uniformly distributed state of variable  $A$ ,  $\mathcal{E}_{K_1^h K_{1,i}^{mask} E_i \rightarrow E_{i+1}}$  are quantum channels that allow the adversary to generate  $T_{AV}$  for any chosen message,  $L = \alpha\alpha'$  are the labels and  $S = K_1^h K_2 RK_{1,j}^{mask} \dots K_{1,m}^{mask}$  refer to the secrets.

The set of ideal output states is defined based on the ideal functionality given the ideal input states, which are required to satisfy a mix of QKD and authentication conditions as well as the requirement for  $\mathcal{S}'_{out} \subseteq \mathcal{S}_{in}$ . As such, we adapt a recently proposed classical authenticated key exchange (AKE) framework [13], where the tasks of authentication and key secrecy are defined and their relation made explicit. Let  $\rho_B^a$  be the conditional state of system  $B$  conditioned on event  $A = a$ , and  $\rho_{B \wedge A=a} = p_a \rho_B^a$  be the sub-normalised conditional state. This gives us a set of five security conditions (including one from  $\mathcal{S}'_{out} \subseteq \mathcal{S}_{in}$ ), given by

1. **Robustness:** In the absence of any adversary, the authentication should pass with high probability, i.e.  $\Pr[F_A = F_B = 1] \geq 1 - \varepsilon_{rob}$ .
2. **Explicit Entity Authentication:** When Alice accepts the QAKE session,  $F_A = 1$ , Bob must have accepted as well,  $F_B = 1$ . This condition on Alice, termed full (f) explicit entity authentication, requires that  $\Pr[F_A = 1, F_B \neq 1] \leq \varepsilon_{EA,f}$ . A similar condition, termed almost-full (af) explicit entity authentication, requires that when Bob accepts the session,  $F_B = 1$ , Alice must be involved in the session, i.e.  $F_A \neq \phi$ . As such, the con-

dition requires that  $\Pr[F_A = \phi, F_B = 1] \leq \varepsilon_{EA,af}$ , with  $\varepsilon_{EA} = \varepsilon_{EA,af} + \varepsilon_{EA,f}$  (Recall  $F_A = \phi$  if Alice did not participate in the session).

3. **Match Security:** When Alice and Bob accepts the authentication, they will generate the same key, i.e.  $\Pr[K_A \neq K_B, F_A = 1, F_B = 1] \leq \varepsilon_{MS}$ .
4. **Key Secrecy:** When keys are generated by Bob, they should remain uniform and secret from the adversary, i.e.  $\rho_{K_B LSE \wedge (F_A, F_B) \in \{01, 11\}}$  is  $\varepsilon_{KS}$ -close in trace distance to  $\tau_{K_B} \otimes \rho_{LSE \wedge (F_A, F_B) \in \{01, 11\}}$ .
5. **Shared Secrets Privacy:** The privacy of the shared secrets  $S$  should be maintained as necessary, which is achieved by the output state being  $\varepsilon_{SP}$ -close to an ideal input state in  $\mathcal{S}_{in}$ . More formally,  $\sum_{(f_A, f_B) \notin \mathcal{S}_{SP}} p_{f_A f_B} \rho_{LSE}^{f_A, f_B}$  is  $\varepsilon_{SP}$ -close in trace distance to  $\sum_{(f_A, f_B) \notin \mathcal{S}_{SP}} p_{f_A f_B} \sigma_{LSE}^{f_A, f_B}$ , where  $\sigma_{LSE}^{f_A, f_B} \in \mathcal{S}_{in}$ ,  $p_{f_A f_B}$  is the probability of  $(F_A, F_B) = (f_A, f_B)$  and  $\mathcal{S}_{SP} = \{0\phi, \phi 0, 10\}$ .

The property of explicit entity authentication highlights an observation, also discussed in the context of QKD [21, 28, 30], where the abort decision may not be shared by both Alice and Bob, and one party could choose to generate keys while the other does not. This condition is imposed on Alice and Bob differently. Since Alice is the receiver of the final authentication tag, when Bob accepts and sends this final tag, he is unable to guarantee that Alice will accept since this final tag can be modified by the adversary, as noted also in Ref. [21]. We note that the match security condition matches the correctness condition in QKD and the key secrecy matches the secrecy condition in QKD. For shared secrets privacy,

<sup>2</sup>For any correlations between bit values of different sessions, i.e. source correlation, it can be accounted in the same way as QKD, such as introducing a leakage channel.

the events  $(F_A, F_B) = (0\phi), (\phi 0), (10)$  are excluded since these events are accounted for in explicit entity authentication.

The steps to generalize the AKE framework to the quantum regime could be of independent interest, since similar the classical AKE framework could be generalized to other quantum variants. Examples include quantum anonymous key exchange where authentication is made one-way, or QAKE with computationally secure message authentication. The generalization of the AKE framework to QAKE can

$$\begin{aligned} \rho^{\text{ideal,int}} = & |\perp\perp\rangle\langle\perp\perp|_{K_A K_B} \otimes \left[ p_{0\phi} |0\phi\rangle\langle 0\phi|_{F_A F_B} \otimes \sigma_{LSE}^{0\phi} + p_{\phi 0} |\phi 0\rangle\langle \phi 0|_{F_A F_B} \otimes \sigma_{LSE}^{\phi 0} + p_{00} |00\rangle\langle 00|_{F_A F_B} \otimes \sigma_{LSE}^{00} \right] \\ & + p_{01} |01\rangle\langle 01|_{F_A F_B K_A} \otimes \tau_{K_B} \otimes \sigma_{LSE}^{01} + p_{11} |11\rangle\langle 11|_{F_A F_B} \otimes \tilde{\tau}_{K_A K_B} \otimes \sigma_{LSE}^{11}, \end{aligned} \quad (2)$$

where  $\tilde{\tau}_{K_A K_B} = \frac{1}{|\mathcal{K}|} \sum_{k \in \mathcal{K}} |kk\rangle\langle kk|_{K_A K_B}$  is a uniformly distributed state of variable  $K_A$  and  $K_B$ , with  $K_A = K_B$ . The single-session security is thus given by the statement: for any  $\sigma_{LSE} \in \mathcal{S}_{in}$ , there exists  $\rho_{F_A F_B K_A K_B LSE} \in \mathcal{S}'_{out}$  such that  $\Delta(\mathcal{P}(\sigma_{LSE}), \rho_{F_A F_B K_A K_B LSE}) \leq \varepsilon_{sec,int}$ .

To simplify the security analysis, we can reduce the trace distance to the security conditions, similarly to how QKD security can be reduced to correctness and secrecy,

**Theorem 2.** *Consider a protocol  $\mathcal{P}$  with an ideal input state  $\sigma_{LSE} \in \mathcal{S}_{in}$ . Then, overall protocol security is satisfied when the security parameter is*

$$\varepsilon_{sec,int} = \varepsilon_{EA} + \varepsilon_{MS} + \varepsilon_{KS} + \varepsilon_{SP}.$$

*Proof.* See Appendix C.2.  $\square$

### 3.3 Single-session Security

The defined set of input and output states satisfy conditions 1 and 3 in Thm. 1 trivially, while the remaining condition is demonstrated in the theorem below, where we assume an ideal state preparation and fair sampling (transmission  $\eta$  is basis-independent). A sketch of the security proof is provided below, with the full security proof presented in Appendix C.3.

**Theorem 3.** *The QAKE protocol  $\mathcal{P}$  is secure with security parameters*

$$\begin{aligned} \varepsilon_{EA} = & \varepsilon_{MAC,1} + 2^{-P_{tol}^{\text{sift}} [1+h_{\text{bin}}(f_{P_1})]+\log_2(P_{tol}^{\text{sift}}+1)} + \frac{1}{|\mathcal{T}_{BV}|} \\ \varepsilon_{MS} = & \varepsilon_{MAC,2} \\ \varepsilon_{KS} = & 2\sqrt{2\varepsilon_{\text{serf},1}} + \frac{1}{2} \times 2^{-\frac{1}{2}[H' - l_{K_B}]} + \varepsilon_{\mathcal{P}'}, \\ \varepsilon_{SP} = & \varepsilon'_{SP,01,11} + \varepsilon_{\mathcal{P}'}, \end{aligned}$$

be found in Appendix B.

The set of ideal output states would thus be those satisfying conditions 2 to 5 perfectly. The explicit entity authentication condition will define the combinations of  $F_A F_B$  present in the ideal output state, with the match security requiring  $K_A = K_B$  and key secrecy enforcing independence of the keys from  $E$ . The shared secrets privacy requirement enforces that the output state forms a mixture of  $\sigma_{LSE}^{f_A f_B} \in \mathcal{S}_{in}$ . Therefore, the set of ideal output state  $\mathcal{S}'_{out} = \{\rho^{\text{ideal,int}}\}$  contains states of the form

where  $l_{K_B}$  is the length of  $K_B$ ,  $\varepsilon_{\text{serf},1}$  is a penalty term associated with the use of modified Serfling bound [12, 42] to estimate the single-photon bit error rate in  $P_2^{\text{sift}}$  from that of  $P_1^{\text{sift}}$ . The penalty associated with shifting to an idealised protocol  $\mathcal{P}'$  is

$$\varepsilon_{\mathcal{P}'} = 2(\varepsilon_{MAC,1} + \varepsilon_{MAC,2} + \varepsilon_{ds} + \varepsilon_{SO})$$

$$\varepsilon_{SO} = 2^{-P_{tol}^{\text{sift}}} + 2^{-N_{P_{2,1}^{\text{sift}}}^{\text{tol}}} + 2^{-P_{tol}^{\text{sift}} h_{\text{bin}}(f_{P_1}) + \log_2(P_{tol}^{\text{sift}} + 1)},$$

the shared secrets privacy parameter for the idealised protocol when  $F_B = 1$  is

$$\varepsilon'_{SP,01,11} = 4\sqrt{2\varepsilon_{\text{serf},1}} + 2(\varepsilon_2 + \varepsilon_3)$$

$$+ \varepsilon_{SP,MAC,1} + \varepsilon_{SP,MAC,2}$$

$$\varepsilon_{SP,MAC,1} = \sqrt{(|\mathcal{T}_{AV}| \varepsilon_{MAC,1} - 1) + 2^{\log_2\left(\frac{2+\varepsilon_3}{\varepsilon_3 |\mathcal{T}_{BV}|}\right) - H'}}$$

$$\varepsilon_{SP,MAC,2} = \sqrt{(|\mathcal{T}_{BV}| \varepsilon_{MAC,2} - 1) + 2^{\log_2\left(\frac{2}{\varepsilon_2} + 1\right) - H'}},$$

the smooth min-entropy term is

$$H' = N_{P_2^{\text{sift}},1}^{\text{tol}} [1 - h_{\text{bin}}(e'_{\text{ph,tol}})] - 2 - \log_2 |\mathcal{T}_{AV}| |\mathcal{T}_{BV}| - \text{leak}_{EC},$$

$\varepsilon_2$  and  $\varepsilon_3$  are parameters to optimise over,  $|\mathcal{T}_{AV}|$  and  $|\mathcal{T}_{BV}|$  are the size (dimension) of the respective tag,  $P_{tol}^{\text{sift}}$  is the minimum tolerated number of sifted rounds,  $\varepsilon_{ds}$  accounts for errors associated with decoy state analysis,  $N_{P_{2,1}^{\text{sift}}}^{\text{tol}}$  is the minimum tolerated number of single-photon rounds in set  $P_2^{\text{sift}}$ , and  $e'_{\text{ph,tol}}$  is the maximum tolerated single-photon phase error rate in set  $P_2^{\text{sift}}$ , and  $\text{leak}_{EC}$  is the information leakage due to error correction.

*Proof Sketch.* The explicit entity authentication security condition relies on the fact that when  $F_A = \phi$  (resp.  $F_B \neq 1$ ), the tag  $T_{AV}$  (resp.  $T_{BV}$ ) is not generated. As such, the adversary has to guess a correct message-tag pair to trigger  $F_B = 1$  (resp.

$F_A = 1$ ). By the nature of the strong 2-universal hash function, the probability guessing a correct message-tag pair is small.

For match security, like the correctness condition of QKD, the security is based on error verification. Bob's tag  $T_{BV}$  involves the corrected bitstring  $\hat{X}_{P_{2,r}^{\text{sift}}}$ , which has to be checked against tag  $\tilde{T}_{BV}$  involving  $X_{P_{2,r}^{\text{sift}}}$ . If the bitstrings do not match (and thus the keys are mismatched as well), the probability of matching tags are small.

For key secrecy, message authentication provided by the authentication steps allows the security condition to be reduced to that of QKD with "idealised" message authentication and where protocol step ordering is obeyed. The proof then follows from that of QKD, where we seek to lower bound the smooth min-entropy  $H_{\min}^{\varepsilon_{\text{sm},1}}(\hat{X}_{P_{2,r}^{\text{sift}}} | \beta K_1^h K_2 K_{1,\beta}^{\text{mask}} E)$ .

Shared secrets privacy requires that necessary secrets remain private. The main protection on  $K_2$  and  $(K_1^h, K_{1,\beta}^{\text{mask}})$  when the protocol succeeds and they are reused is based on the value of  $\hat{X}_{P_2^{\text{sift}}}$  included as part of the message while generating tags  $T_{BV}$  and  $T_{AV}$ . Based on the ideal key privacy property [17] along with quantum leftover hash lemma [41], the overall hash function  $h_1$  with mask and  $h_2$  are  $\varepsilon_{\text{MAC},1}$  and  $\varepsilon_{\text{MAC},2}$  strong extractors respectively, thereby preserving the secrecy of the authentication and mask keys  $K_2$  and  $(K_1^h, K_{1,\beta}^{\text{mask}})$ .  $\square$

The final condition to consider is the robustness of the protocol. The main sources of non-acceptance of a session would be either failure of the parameter estimation checks or error correction failure. We can use concentration bounds [48] to compute the probability of failure of the parameter estimation checks, which we label as  $\varepsilon_{\text{ds},\text{rob}}$  for terms associated with the decoy state checks,  $\varepsilon_{\mathcal{E},P_1,\text{rob}}$  for the bit error check in set  $P_1$ , and  $\varepsilon_{\text{rob},P}$  for terms associated with bounding  $|P|$  (bounds  $P^{\text{tol}} \leq |P| \leq P^{\text{UB}}$ ). The error correction failures can either be due to the bit error rate in set  $P_2$  exceeding some tolerance bound, or failure to correct for errors even within the tolerance bound. In the former case, knowing the bit error rate in set  $P_1$  falls below  $e_{\text{bit},1,\text{tol}}$ , the probability that the error rate in set  $P_2$  exceeding some tolerance value  $e'_{\text{bit},\text{tol}}$  can be computed based on the modified Serfling bound [12, 42], with failure probability  $\varepsilon_{\text{serf},2}$ . The failure probability of the latter case depends on the error correction protocol utilised, and we define the error probability as  $\varepsilon_{\text{EC}}$  for total communication  $l_{\text{syn}}$ -bits during the error correction phase. As such, the overall robustness can be quantified by  $\varepsilon_{\text{rob}}$ ,

$$\varepsilon_{\text{rob}} = \varepsilon_{\text{rob},P} + \varepsilon_{\text{serf},2} + \varepsilon_{\text{ds},\text{rob}} + \varepsilon_{\mathcal{E},P_1,\text{rob}} + \varepsilon_{\text{EC}}. \quad (3)$$

## 4 Numerical Analysis

We analyse the performance of the QAKE protocol by simulating the length of keys generated based on Thm. 3. We assume a simple experimental model with Alice preparing decoy BB84 states, sending it through a channel with loss  $\eta$ , and Bob performing measurement in a random basis, i.e. with detection probability  $p_{\text{det},\mu_j} = p_{\mu_j}(1 - e^{-\eta\mu_j})$ . Additionally, Bob's detector is assumed to have zero dark counts. We fix  $\mu_0 = 0.45$ ,  $\mu_1 = 0.225$ ,  $\mu_2 = 0$  as the decoy intensities,  $p_{\mu_0} = 0.2$ ,  $p_{\mu_1} = 0.6$  and  $p_{\mu_2} = 0.2$  as their respective probabilities. We also fix the length of the authentication tags to be 80 bits each, with  $\varepsilon_{\text{MAC},1} = \varepsilon_{\text{MAC},2} = 2^{-80}$ , i.e. the authentication is 2-universal, allowing us to use the tighter bound for  $\varepsilon_{\text{SP}}$  shown in Thm. 19. The error correction is assumed to utilise 30 % of the sifted bits.

The simulation is then performed by rearranging the result in Thm. 3, and optimising  $l_{K_B}$  over the splitting ratio (also size of test set)  $f_{P_1}$ , robustness and secrecy parameters (components of  $\varepsilon_{\text{rob}}$  and  $\varepsilon_{\text{sec,int}}$ ) in Matlab, with other parameters fixed as described in the results. We choose the security parameter of each session of the protocol as  $\varepsilon_{\text{sec}} = 10^{-15}$ , which yields an overall protocol security of  $10^{-6}$  when we allow it to run up to  $10^9$  sessions. The robustness parameter is chosen at  $\varepsilon_{\text{rob}} = 10^{-10}$ , and each session involves  $n_{\text{rnd}} = 10^{10}$  signals being sent by Alice to Bob. The concentration bound used for robustness parameters is the tight bound on binomial distribution [48] due to i.i.d. state preparation noting independence of the detection probability on basis selection by fair sampling assumption. The concentration bound used for estimation of the expectation values,  $\mathbb{E}[N_{\mu_v,P_i}]$ , from the observed values,  $N_{\mu_v,P_i}$ , associated with decoy state estimation (errors form part of decoy state related parameters  $\varepsilon_{\text{ds}}$ ) is Kato's bound [11, 19, 46]. The simulation results are shown in Fig. 3 for various QBER values  $Q$ .

In terms of key generation rate, QAKE has a slightly higher key rate than standard QKD, though the extent of improvement depends on the length of the authentication tags used and the number of communication rounds. If we use the QAKE protocol and revert it to a standard QKD protocol, i.e. using authenticated communication channel and having error verification step, one would need to generate seven authentication tags (2 for label agreement, 2 for sifting, 1 for test round announcement, 1 for error correction, 1 for error verification) instead of two, leading to an additional 400 bits of key utilized. Therefore, QAKE may provide a significant advantage when key generation rates are low, such as when block sizes are small (e.g. satellite QKD) or loss is high, or when there is a large number of communication rounds (e.g. for

Cascade) – since more bits have to be sacrificed for message authentication.

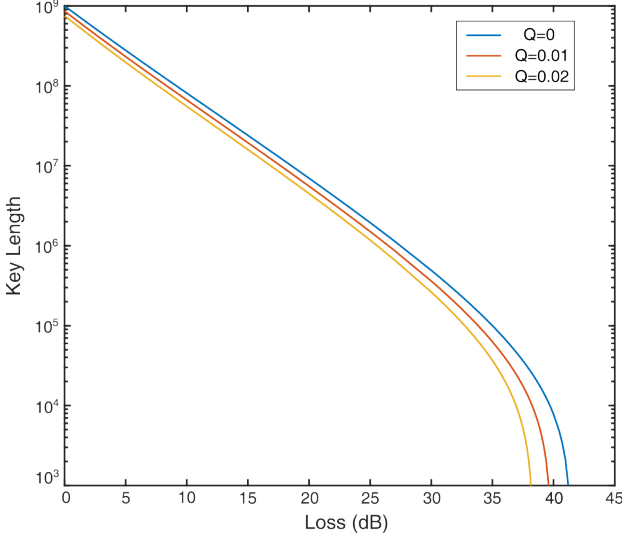


Figure 3: Simulated key length for QAKE protocol at various signal loss values (including detector loss), various QBER values  $Q$ , with  $n_{rnd} = 2 \times 10^{10}$  signals sent,  $\varepsilon_{rob} = 10^{-10}$ , and  $\varepsilon_{sec} = 10^{-15}$ . The authentication tag used is 80-bits, i.e.  $|T_{AV}| = |T_{BV}| = 80$ , and we assume the error correction to utilise 30 % of the sifted bits. The system parameters are chosen to be  $\mu_0 = 0.45$ ,  $\mu_1 = 0.225$ ,  $\mu_2 = 0$  as the decoy intensities,  $p_{\mu_0} = 0.2$ ,  $p_{\mu_1} = 0.6$  and  $p_{\mu_2} = 0.2$  as their respective probabilities, and we assume the system to have zero dark counts.

## 5 Experimental Validation

### 5.1 Experimental Setup

We validated our results by implementing the QAKE protocol on the ID Quantique Clavis XGR QKD systems, with the setup shown in Fig. 4. We connected Alice and Bob in a back-to-back configuration with an optical attenuator of 10 dB emulating a fiber distance of 45 km ( $0.22 \text{ dB km}^{-1}$ ). We also configured the intensity  $\mu_0 = 0.45$  and the probability of Alice selecting each basis to about 50 %. The QKD systems provide QKD raw data, which includes the encoded qubit values from the transmitter (Alice) and the measured qubit values from the receiver (Bob) during the key exchange process. We collected the raw data using an Application Programming Interface (API) command in a text format, which was utilised to estimate the QBER and detection rate.

Due to the lack of a direct interface between the QKD system’s raw data output and our FPGA, the post-processing of the raw data was performed offline (not in real-time). Firstly, to balance the basis detection rates, we performed post-selection of the data such that the detection probability in each basis is about 50 %. Secondly, sifting is performed to

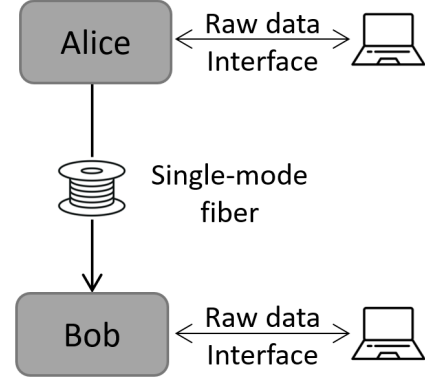


Figure 4: Experimental setup implementing the protocol, with 10 dB of channel loss from a 45 km fiber (emulated with an optical attenuator). The quantum state preparation and measurement are performed by the ID Quantique Clavis XGR QKD systems, which outputs the relevant raw data (including state prepared and measurement outcomes). Post-selection is performed on the raw data to match the protocol requirements of having balanced (50 %) detector basis choice. The remaining steps of the protocols are then simulated (including error correction, authentication tag generation and privacy amplification) using the post-selected data.

ensure that Alice and Bob has matching basis. The data is then utilised to run the protocol in a software stack. This includes the use of Toeplitz hashing as the XOR two-universal hash function and as the two-universal hash function respectively for the authentication step and privacy amplification steps, and the use of a two-way *low-density parity-check* (LDPC) code for error correction. Details of the LDPC and Toeplitz hashing implementation are presented in the subsequent subsections.

We utilise similar parameters for authentication tag size as the numerical simulation, while the number of bits communicated for error correction is set to a maximum of 30 % of the size of set  $P_2$  (containing bits used for key generation) based on LDPC performance.

### 5.2 Toeplitz Hashing

Toeplitz hashing is implemented on a Virtex Ultra-scale+ XCVU9p FPGA, running at a clock frequency of 332 MHz. Due to the limitation of resources in FPGA, we decomposed the large Toeplitz matrix evenly into small submatrix multiplication steps [47]. We designed pipelined modules for Toeplitz submatrix construction, matrix multiplication and intermediate accumulation for processing 32 input bits from the FPGA interface on every clock cycle. The matrix construction module consists of a 32-bit wide FIFO that stores the large Toeplitz matrix, and a shift register that stores the submatrix. On every clock cycle, the submatrix is constructed by reading 32-bits from the FIFO and using it to shifting the regis-

ter. Matrix multiplication is realized by bitwise-AND and XOR-reduction. An accumulation register performs bitwise-XOR for matrix multiplication outputs on each clock cycle, to generate the final output bits.

### 5.3 Error Correction

For error correction, we implemented a two-way *low-density parity-check* (LDPC) code on the same FPGA by adapting LDPC IP cores from Xilinx [1]. We used the following settings on the LDPC IP: base matrix choice  $bg = 0$ , syndrome length control  $mb = 5$ , code-word length controls  $z_{set} = 5$  and  $z_j = 5$ , normalisation factor  $sc_{idx} = 14$ , and scaling  $llr_{scale} = 14$ . This results in a codeword size of 1188 bytes and syndrome size of 220 bytes. The LDPC IP core is designed for standard error correction usage (e.g. in 5G), where the syndrome is also sent through the channel and experiences the same error rate as the data, unlike in QAKE where the syndrome is assumed to be error-free. Let  $X$  be a 1188-byte data string ( $X'$  being Bob's data string),  $X_1$  and  $X_2$  be the first 968 bytes and last 220 bytes of data, and  $syn$  be the syndrome. The adapted protocol we use is as follows:

1. For every 1188 bytes of data, Alice generates a 220-byte syndrome from the first 968 bytes of data,  $X_1$ , and XOR the syndrome with  $X_2$ , i.e.  $syn' = syn \oplus X_2$ .
2. Alice computes a 16-byte (128-bit) hash of the data string using SHA-256 (second half of the hash is discarded),  $T = SHA256(X)$ .
3. Alice sends  $syn'$  and  $T$  to Bob.
4. Bob performs XOR of his last 220 bytes of data with the syndrome, i.e.  $syn'' = syn' \oplus X_2'$ . Note this is equivalent to introducing the error bits  $X_2' \oplus X_2$  onto the syndrome,  $syn''$ .
5. Bob performs error correction with  $X_1'$  and  $syn''$  using the LDPC IP core, and obtains a corrected data string  $\hat{X}_1$  and corrected syndrome  $\hat{syn}$ .
6. Bob computes the correction on the second part of his data string, with  $\hat{X}_2 = X_2' \oplus \hat{syn} \oplus syn'$ .
7. Bob computes the hash of the corrected data string using SHA-256,  $T' = SHA256(\hat{X})$ , and compares it with the hash sent by Alice.
8. If the hash does not match, Bob will inform Alice to increase the syndrome length by 44 bytes, and send that additional 44 bytes to Bob.
9. Alice and Bob repeat steps 4 to 8 until the hash matches. If the syndrome length longer than the maximum transmission unit (MTU) size the FPGA can support ( $mb = 10$ , syndrome = 440 bytes, maximum of 6 rounds), Alice will simply reveal all 1188 bytes of data to Bob instead.

Based on our tests for a bit error rate of 2%, the LDPC code can almost always succeed with a sacrifice of at most 30% of the sifted bitstring.

### 5.4 Experimental Results

We run the protocol a total of three separate times, and fix a testing probability of 25%, which is close to the optimal testing probability at the same transmission range in the numerical simulation. Table 1 show the results obtained for the various runs. All three runs recorded around  $2 \times 10^{10}$  signals sent after post-selection, with an average bit error rate of 2% and key length of  $2 \times 10^5$ . This is roughly in line with the simulated results for an ideal setting presented in Fig. 3.

## 6 Discussion

We presented a QAKE protocol that incorporates entity authentication with key expansion. It compresses the authentication steps to the last two communication steps to reduce authentication cost. The protocol is also designed to allow for key recycling, where the authentication keys and masking keys need not be refreshed after each protocol session. Key recycling can be useful for applications since communication overhead from the sharing of the refreshed secrets by the server (e.g. between all remote access servers) can be removed when the protocol passes.

**Open Problems:** There are some limitations to the presented protocol and security analysis, which can open up areas that can be explored in the future.

An interesting area to explore is the expansion of QAKE or QKD to achieve other tasks within the classical AKE framework. For instance, classical AKE can allow for anonymous key exchange by not requiring mutual authentication for all parties (perhaps necessary only to authenticate the client but not for the client to authenticate the server), or allow for client-server authentication (without key generation). Such expansion of tasks may require protocol changes that can be informed by the modifications within the classical AKE framework, which is well-studied by the classical cryptography community.

It is also worthwhile to have a more comprehensive AKE framework that incorporates both classical and quantum AKE. This brings the analysis closer to a practical setting, where both classical authentication and key exchange methods may live with QAKE and other quantum protocols. Analysing the interplay between these protocols and their respective guarantees can provide insight into how these diverse systems can be incorporated in practice, and allow us to understand the types of attacks and risks we

Table 1: Experimental results for three runs of the protocol with  $n_{rnd}$  number of signals sent (after post-selection) for each run. The detection probability per signal,  $p_{det}$ , and average bit error rate is computed from the measurement results. The key length is optimised over the various epsilon terms, including errors associated with decoy state method,  $\epsilon_{ds}$ , and the modified Serfling bound error for single-photon bit error rate  $\epsilon_{serf,1}$ , with the optimal values presented here, for secrecy parameter  $\epsilon_{sec} = 10^{-15}$ .

| Run | $n_{rnd}$             | $p_{det}$             | QBER   | Key Length         | $\epsilon_{ds}$        | $\epsilon_{serf,1}$    |
|-----|-----------------------|-----------------------|--------|--------------------|------------------------|------------------------|
| 1   | $2.04 \times 10^{10}$ | $1.03 \times 10^{-4}$ | 0.0196 | $1.77 \times 10^5$ | $1.30 \times 10^{-16}$ | $3.17 \times 10^{-33}$ |
| 2   | $2.36 \times 10^{10}$ | $1.03 \times 10^{-4}$ | 0.0202 | $2.13 \times 10^5$ | $1.29 \times 10^{-16}$ | $3.24 \times 10^{-33}$ |
| 3   | $2.13 \times 10^{10}$ | $1.03 \times 10^{-4}$ | 0.0203 | $2.13 \times 10^5$ | $1.30 \times 10^{-16}$ | $3.20 \times 10^{-34}$ |

should consider in QKD or QAKE design. Moreover, such an endeavour can build a common language with classical cryptography that would make QKD or similar quantum cryptographic protocol security more accessible.

**Additional Results:** Pre-sharing of basis information between Alice and Bob can avoid penalties to key rate from sifting, but renders the protocol inefficient due to the large size of  $\theta$  required. The most practical solution to this problem is to use a shorter pre-shared basis seed and generate a longer string as the shared basis from a quantum-safe *pseudorandom number generator* (PRNG) like AES [16]. In Appendix D, we present a QAKE protocol that is adapted from the authentication protocol by Fehr et. al. [17], which utilises pre-shared pseudorandom basis, and we present a formal analysis of the use of pseudorandom basis in decoy state BB84 in Appendix E. We note that the secret keys generated remains information-theoretic secure, provided that the adversary is computationally bounded during the protocol itself. Inspired by the authentication achieved by Fehr et. al. [17] with a single communication step, we also developed a two-step (one challenge and one response) client authentication protocol that is secure in the practical setting (with channel loss, noise and multi-photon events). This result is presented in Appendix F.

## Acknowledgments

This paper was prepared for informational purposes by the Global Technology Applied Research center of JPMorgan Chase & Co. This paper is not a product of the Research Department of JPMorgan Chase & Co. or its affiliates. Neither JPMorgan Chase & Co. nor any of its affiliates makes any explicit or implied representation or warranty and none of them accept any liability in connection with this paper, including, without limitation, with respect to the completeness, accuracy, or reliability of the information contained herein and the potential legal, compliance, tax, or accounting effects thereof. This document is not intended as investment research or investment advice, or as a recommendation, offer, or solicitation for the purchase or sale of any security, financial instrument,

financial product or service, or to be used in any way for evaluating the merits of participating in any transaction. All contributions by J.C., K.H.Y.L., O. Alia, M.P. and C.L. were made while working at JPMorgan Chase.

## Author Contributions

W.Y.K. and K.C. conceptualized the work; W.Y.K. and K.C. performed the formal analysis; J.C. and K.H.Y.L. designed and implemented the software; O. Alia and J.C. performed the experiment and data collection; C.L. and M.P. provided overall supervision of the project; all authors contributed to the drafting and reviewing of the manuscript.

## References

- [1] Advanced Micro Devices. ldpc encoder/decoder. URL <https://www.xilinx.com/products/intellectual-property/ef-di-ldpc-enc-dec.html>.
- [2] E. Barker. Recommendation for Key Management: Part 1 – General. May 2020. DOI: [10.6028/nist.sp.800-57pt1r5](https://doi.org/10.6028/nist.sp.800-57pt1r5).
- [3] E. Barker and J. Kelsey. Recommendation for Random Number Generation Using Deterministic Random Bit Generators. June 2015. DOI: [10.6028/nist.sp.800-90ar1](https://doi.org/10.6028/nist.sp.800-90ar1).
- [4] M. Bellare, A. Desai, E. Jokipii, and P. Rogaway. A concrete security treatment of symmetric encryption. In *Proceedings 38th Annual Symposium on Foundations of Computer Science*, pages 394–403, 1997. DOI: [10.1109/SFCS.1997.646128](https://doi.org/10.1109/SFCS.1997.646128).
- [5] G. Brassard and L. Salvail. Secret-key reconciliation by public discussion. In Tor Hellese, editor, *Advances in Cryptology — EUROCRYPT '93*, pages 410–423, Berlin, Heidelberg, 1994. Springer Berlin Heidelberg. ISBN 978-3-540-48285-7. DOI: [10.1007/3-540-48285-7\\_35](https://doi.org/10.1007/3-540-48285-7_35).
- [6] C. Brzuska, M. Fischlin, B. Warinschi, and S. C. Williams. Composability of bellare-rogoway key exchange protocols. In *Proceedings of the 18th ACM Conference on Computer and Communications Security, CCS '11*, page 51–62, New

- York, NY, USA, 2011. Association for Computing Machinery. ISBN 9781450309486. DOI: [10.1145/2046707.2046716](https://doi.org/10.1145/2046707.2046716).
- [7] R. Canetti. Security and composition of multi-party cryptographic protocols. *J. Cryptology*, 13: 143–202, 2000. DOI: [10.1007/s001459910006](https://doi.org/10.1007/s001459910006).
  - [8] R. Canetti. Universally composable security: A new paradigm for cryptographic protocols. In *Proceedings of the 42nd IEEE Symposium on Foundations of Computer Science*, FOCS '01, page 136, USA, 2001. IEEE Computer Society. ISBN 0769513905. DOI: [10.1109/sfcs.2001.959888](https://doi.org/10.1109/sfcs.2001.959888).
  - [9] J. L. Carter and M. N. Wegman. Universal classes of hash functions. *Journal of Computer and System Sciences*, 18:143–154, 1979. DOI: [10.1016/0022-0000\(79\)90044-8](https://doi.org/10.1016/0022-0000(79)90044-8).
  - [10] T. M. Cover and J. A. Thomas. *Information Theory and Statistics*, chapter 11, pages 347–408. John Wiley & Sons, Ltd, 2005. ISBN 9780471748823. DOI: [10.1002/047174882X.ch11](https://doi.org/10.1002/047174882X.ch11).
  - [11] G. Currás-Lorenzo, Á. Navarrete, K. Azuma, G. Kato, M. Curty, and M. Razavi. Tight finite-key security for twin-field quantum key distribution. *npj Quantum Information*, 7:22, 2021. DOI: [10.1038/s41534-020-00345-3](https://doi.org/10.1038/s41534-020-00345-3).
  - [12] M. Curty, F. Xu, W. Cui, C. C. W. Lim, K. Tamaki, and H.-K. Lo. Finite-key analysis for measurement-device-independent quantum key distribution. *Nature Communications*, 5:3732, 2014. DOI: [10.1038/ncomms4732](https://doi.org/10.1038/ncomms4732).
  - [13] C. D. de Saint Guilhem, M. Fischlin, and B. Warinski. Authentication in key-exchange: Definitions, relations and composition. In *2020 IEEE 33rd Computer Security Foundations Symposium (CSF)*, pages 288–303, 2020. DOI: [10.1109/CSF49147.2020.00028](https://doi.org/10.1109/CSF49147.2020.00028).
  - [14] Y. Dodis, D. Pointcheval, S. Ruhault, D. Vergniaud, and D. Wichs. Security analysis of pseudo-random number generators with input: /dev/random is not robust. In *Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security, CCS '13*, page 647–658, New York, NY, USA, 2013. Association for Computing Machinery. ISBN 9781450324779. DOI: [10.1145/2508859.2516653](https://doi.org/10.1145/2508859.2516653).
  - [15] M. Doosti, M. Delavar, E. Kashefi, and M. Arapinis. A unified framework for quantum unforgeability, 2021. arXiv:2103.13994.
  - [16] M. Dworkin, E. Barker, J. Nechvatal, J. Fote, L. Bassham, E. Roback, and J. Dray. Advanced encryption standard (aes). 2001-11-26 2001. DOI: [10.6028/NIST.FIPS.197](https://doi.org/10.6028/NIST.FIPS.197).
  - [17] S. Fehr and L. Salvail. Quantum authentication and encryption with key recycling. In Jean-Sébastien Coron and Jesper Buus Nielsen, editors, *Advances in Cryptology – EUROCRYPT 2017*, pages 311–338, Cham, 2017. Springer International Publishing. ISBN 978-3-319-56617-7. DOI: [10.1007/978-3-319-56617-7\\_11](https://doi.org/10.1007/978-3-319-56617-7_11).
  - [18] V. T. Hoang and Y. Shen. Security analysis of nist ctr-drbg. In *Advances in Cryptology – CRYPTO 2020*, volume 12170. Springer, Cham, 2020. ISBN 978-3-030-56784-2. DOI: [10.1007/978-3-030-56784-2\\_8](https://doi.org/10.1007/978-3-030-56784-2_8).
  - [19] G. Kato. Concentration inequality using unconfirmed knowledge, 2020. arXiv:2002.04357.
  - [20] J. Katz and Y. Lindell. *Introduction to Modern Cryptography*. Chapman & Hall/CRC, 2014. ISBN 1466570261. DOI: [doi.org/10.1201/9781351133036](https://doi.org/10.1201/9781351133036).
  - [21] E. O. Kiktenko, A. O. Malyshev, M. A. Gavreev, A. A. Bozhedarov, N. O. Pozhar, M. N. Anufriev, and A. K. Fedorov. Lightweight authentication for quantum key distribution. *IEEE Transactions on Information Theory*, 66(10):6354–6368, 2020. DOI: [10.1109/TIT.2020.2989459](https://doi.org/10.1109/TIT.2020.2989459).
  - [22] R. König, R. Renner, and C. Schaffner. The operational meaning of min- and max-entropy. *IEEE Transactions on Information Theory*, 55(9):4337–4347, 2009. DOI: [10.1109/TIT.2009.2025545](https://doi.org/10.1109/TIT.2009.2025545).
  - [23] D. Leermakers and B. Skoric. Security proof for quantum key recycling with noise. *Quantum Information & Computation*, 19:0913–0934, 2019. DOI: [10.26421/QIC19.11-12-2](https://doi.org/10.26421/QIC19.11-12-2).
  - [24] C. C. W. Lim, M. Curty, N. Walenta, F. Xu, and H. Zbinden. Concise security bounds for practical decoy-state quantum key distribution. *Physical Review A*, 89:022307, Feb 2014. DOI: [10.1103/PhysRevA.89.022307](https://doi.org/10.1103/PhysRevA.89.022307).
  - [25] M. Mitzenmacher and E. Upfal. *Probability and Computing: Randomization and Probabilistic Techniques in Algorithms and Data Analysis*. Cambridge University Press, USA, 2nd edition, 2017. ISBN 110715488X. DOI: [10.1017/CBO9780511813603](https://doi.org/10.1017/CBO9780511813603).
  - [26] M. Mosca, D. Stebila, and B. Ustaoglu. Quantum key distribution in the classical authenticated key exchange framework. In P. Gaborit, editor, *Post-Quantum Cryptography*, pages 136–154, Berlin, Heidelberg, 2013. Springer Berlin Heidelberg. ISBN 978-3-642-38616-9. URL [https://link.springer.com/chapter/10.1007/978-3-642-38616-9\\_9](https://link.springer.com/chapter/10.1007/978-3-642-38616-9_9).
  - [27] National Institute of Standards and Technology. Module-lattice-based key-encapsulation mechanism standard. (FIPS 203), 2024. DOI: [10.6028/nist.fips.203](https://doi.org/10.6028/nist.fips.203).
  - [28] C. Portmann. Key recycling in authentication. *IEEE Transactions on Information Theory*, 60(7):4383–4396, 2014. DOI: [10.1109/TIT.2014.2317312](https://doi.org/10.1109/TIT.2014.2317312).
  - [29] C. Portmann. Quantum authentication with key recycling. In *Advances in Cryptology – EU-*

- ROCRYPT 2017*, pages 339–368, Cham, 2017. Springer International Publishing. ISBN 978-3-319-56617-7. DOI: [10.1007/978-3-319-56617-7\\_12](https://doi.org/10.1007/978-3-319-56617-7_12).
- [30] C. Portmann and R. Renner. Security in quantum cryptography. *Reviews of Modern Physics*, 94:025008, Jun 2022. DOI: [10.1103/RevModPhys.94.025008](https://doi.org/10.1103/RevModPhys.94.025008).
  - [31] A. B. Price, John G. Rarity, and C. Erven. A quantum key distribution protocol for rapid denial of service detection. *EPJ Quantum Technology*, 7:8, 2021. DOI: [10.1140/epjqt/s40507-020-00084-6](https://doi.org/10.1140/epjqt/s40507-020-00084-6).
  - [32] J. M. Renes and R. Renner. One-shot classical data compression with quantum side information and the distillation of common randomness or secret keys. *IEEE Transactions on Information Theory*, 58(3):1985–1991, 2012. DOI: [10.1109/TIT.2011.2177589](https://doi.org/10.1109/TIT.2011.2177589).
  - [33] R. L. Rivest, A. Shamir, and L. Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21(2):120–126, feb 1978. ISSN 0001-0782. DOI: [10.1145/359340.359342](https://doi.org/10.1145/359340.359342).
  - [34] P. Rogaway. Bucket hashing and its application to fast message authentication. *Journal of Cryptology*, 12:91–115, 1999. DOI: [10.1007/PL00003822](https://doi.org/10.1007/PL00003822).
  - [35] P.W. Shor. Algorithms for quantum computation: discrete logarithms and factoring. In *Proceedings 35th Annual Symposium on Foundations of Computer Science*, pages 124–134, 1994. DOI: [10.1109/SFCS.1994.365700](https://doi.org/10.1109/SFCS.1994.365700).
  - [36] D.R. Stinson. Universal hashing and authentication codes. *Designs, Codes and Cryptography*, 4: 369–380, 1994. DOI: [10.1007/BF01388651](https://doi.org/10.1007/BF01388651).
  - [37] M. Tomamichel. *Quantum Information Processing with Finite Resources*. Springer Briefs in Mathematical Physics. Springer Cham, 2015. DOI: [10.1007/978-3-319-21891-5](https://doi.org/10.1007/978-3-319-21891-5).
  - [38] M. Tomamichel and A. Leverrier. A largely self-contained and complete security proof for quantum key distribution. *Quantum*, 1:14, 2017. DOI: [10.22331/q-2017-07-14-14](https://doi.org/10.22331/q-2017-07-14-14).
  - [39] M. Tomamichel and R. Renner. Uncertainty relation for smooth entropies. *Physical Review Letters*, 106:110506, Mar 2011. DOI: [10.1103/PhysRevLett.106.110506](https://doi.org/10.1103/PhysRevLett.106.110506).
  - [40] M. Tomamichel, R. Colbeck, and R. Renner. Duality between smooth min- and max-entropies. *IEEE Transactions on Information Theory*, 56(9):4674–4681, 2010. DOI: [10.1109/TIT.2010.2054130](https://doi.org/10.1109/TIT.2010.2054130).
  - [41] M. Tomamichel, C. Schaffner, A. Smith, and R. Renner. Leftover hashing against quantum side information. *IEEE Transactions on Information Theory*, 57(8):5524–5535, 2011. DOI: [10.1109/TIT.2011.2158473](https://doi.org/10.1109/TIT.2011.2158473).
  - [42] M. Tomamichel, C. C. W. Lim, N. Gisin, and R. Renner. Tight finite-key analysis for quantum cryptography. *Nature Communications*, 3(1):634, 2012. DOI: [10.1038/ncomms1631](https://doi.org/10.1038/ncomms1631).
  - [43] A. S. Trushechkin, P. A. Tregubov, E. O. Kiktenko, Y. V. Kurochkin, and A. K. Fedorov. Quantum-key-distribution protocol with pseudo-random bases. *Physical Review A*, 97:012311, Jan 2018. DOI: [10.1103/PhysRevA.97.012311](https://doi.org/10.1103/PhysRevA.97.012311).
  - [44] X. Xue and Ni. Calabretta. Nanosecond optical switching and control system for data center networks. *Nature Communications*, 13(1):2257, 2022. DOI: [10.1038/s41467-022-29913-1](https://doi.org/10.1038/s41467-022-29913-1).
  - [45] Y.-K. Yeo, Z. Xu, C.-Y. Liaw, D. Wang, Y. Wang, and T.-H. Cheng. A 448× 448 optical cross-connect for high-performance computers and multi-terabit/s routers. In *Optical Fiber Communication Conference*, page OMP6. Optica Publishing Group, 2010. DOI: [10.1364/ofc.2010.omp6](https://doi.org/10.1364/ofc.2010.omp6).
  - [46] X. Zhang, P. Zeng, T. Ye, H.-K. Lo, and X. Ma. Quantum complementarity approach to device-independent security. *Physical Review Letters*, 131:140801, Oct 2023. DOI: [10.1103/PhysRevLett.131.140801](https://doi.org/10.1103/PhysRevLett.131.140801).
  - [47] Xiaoguang Zhang, You-Qi Nie, Hao Liang, and Jun Zhang. Fpga implementation of toeplitz hashing extractor for real time post-processing of raw random numbers. In *2016 IEEE-NPSS Real Time Conference (RT)*, pages 1–5, 2016. DOI: [10.1109/RTC.2016.7543094](https://doi.org/10.1109/RTC.2016.7543094).
  - [48] A. M. Zubkov and A. A. Serov. A complete proof of universal inequalities for the distribution function of the binomial law. *Theory of Probability & Its Applications*, 57(3):539–544, 2013. DOI: [10.1137/S0040585X97986138](https://doi.org/10.1137/S0040585X97986138).

## A Preliminaries

### A.1 Quantum Systems

The state of a generic quantum system  $A$  can be represented by a density matrix  $\rho_A$ . For a classical random variable  $Y$  that takes on values  $y \in \mathcal{Y}$  according to probability distribution  $p_y$ , it can be expressed as a quantum state  $\rho_Y = \sum_{y \in \mathcal{Y}} p_y \tilde{\Pi}_Y^y$ , where  $\tilde{\Pi}_Y^y = |y\rangle\langle y|_Y$  for simplicity. Two special classical states are the uniformly distributed system, with  $p_y = \frac{1}{|\mathcal{Y}|}$  represented by  $\tau_Y$ , and the uniformly distributed systems with matching values,  $\tilde{\tau}_{YY'}$ , where  $p_y = \frac{1}{|\mathcal{Y}|}$  and  $y = y'$  for all  $y, y' \in \mathcal{Y}$ . A classical-quantum state with classical random variable  $A$  and quantum subsystem  $B$  can be expressed as

$$\rho_{AB} = \sum_a p_a \tilde{\Pi}_A^a \otimes \rho_B^a,$$

where  $\rho_B^a$  (or sometimes  $\rho_{B|A=a}$ ) is the quantum state of subsystem  $B$  conditioned on event  $A = a$ . We further define the sub-normalized conditional state  $\rho_{B \wedge A=a}$  as  $p_a \rho_B^a$ . We label a quantum channel that maps inputs  $I$  to output  $O$ , with fixed inputs  $a$  by  $\mathcal{E}_{I \rightarrow O}^a$ . The symbol  $\mathcal{E}$  is used to label quantum channels controlled by an adversary while letters  $\mathcal{A}, \mathcal{B}, \mathcal{C}$  are used to label quantum channels corresponding to actions by honest or hypothetical parties. We label a quantum measurement on system  $A$  with outcome  $X = x$  by the general measurement operator  $F_A^x$ , with corresponding positive operator-value measure (POVM)  $\Pi_A^x = (O_A^x)^\dagger O_A^x$ . For projections onto an orthonormal basis, the POVMs (also general measurement operators) are expressed as projectors,  $\{\tilde{\Pi}_Y^y\}_{y \in \mathcal{Y}}$ .

### A.2 Quantum Information Theory

We use the generalised trace distance measure to measure the distinguishability of two (possibly sub-normalized) quantum states  $\rho$  and  $\sigma$  [37],

$$\Delta(\rho, \sigma) := \frac{1}{2} \|\rho - \sigma\|_1 + \frac{1}{2} |\text{Tr}(\rho - \sigma)|, \quad (4)$$

where  $\|\cdot\|_1$  is the trace norm. Another useful distance measure is the purified distance,

$$P(\rho, \sigma) = \sqrt{1 - \left[ \text{Tr} |\sqrt{\rho} \sqrt{\sigma}| + \sqrt{(1 - \text{Tr} \rho)(1 - \text{Tr} \sigma)} \right]^2}, \quad (5)$$

which can be bounded by the trace distance,  $P(\rho, \sigma) \leq \sqrt{2\Delta(\rho, \sigma)}$ . The min-entropy is defined as [37]

$$H_{\min}(A|E)_{\rho_{AE}} := \sup\{\lambda \in \mathbb{R}, \sigma_B : \rho_{AE} \leq 2^{-\lambda} \mathbb{I}_A \otimes \sigma_B\}, \quad (6)$$

with max-entropy defined as a min-entropy through the duality relation,  $H_{\max}(A|B)_\rho := -H_{\min}(A|E)_\rho$  for pure  $\rho_{ABE}$ . The smooth min- and max-entropy are defined as

$$\begin{aligned} H_{\min}^\varepsilon(A|E)_{\rho_{AE}} &:= \max_{\substack{\rho'_{AE} : \text{Tr}[\rho'_{AE}] \leq 1, \\ P(\rho_{AE}, \rho'_{AE}) \leq \varepsilon}} H_{\min}(A|E)_{\rho'_{AE}} \\ H_{\max}^\varepsilon(A|E)_{\rho_{AE}} &:= \min_{\substack{\rho'_{AE} : \text{Tr}[\rho'_{AE}] \leq 1, \\ P(\rho_{AE}, \rho'_{AE}) \leq \varepsilon}} H_{\max}(A|E)_{\rho'_{AE}} \end{aligned} \quad (7)$$

### A.3 Two-Universal Hash Functions

For information-theoretic authentication schemes constructed from universal hash functions, a client generates a valid tag from the hash function with an authentication key and the message, which is then verified by a server with the same hash function and authentication key. We note that there are alternative frameworks of authentication with quantum access to the hash function based on unforgeability [15], but we assume here that only classical access to the hash function is allowed, given that the adversary in our proposed protocols has no direct access to the hash function. Utilising a  $\varepsilon$ -almost strong 2-universal hash function prevents message tampering,

**Definition 1** ( $\varepsilon$ -almost strong 2-universal hash function [28, 36]). *A family of hash functions  $\{h(k, \cdot) : \mathcal{M} \rightarrow \mathcal{T}\}_{k \in \mathcal{K}}$  is  $\varepsilon$ -almost strongly 2-universal if for all messages  $m_1, m_2 \in \mathcal{M}$  and  $m_1 \neq m_2$ , and all  $t_1, t_2 \in \mathcal{T}$ ,*

$$\frac{1}{|\mathcal{K}|} \sum_{k \in \mathcal{K}} \Pr[h(k, m_1) = t_1 \wedge h(k, m_2) = t_2] \leq \frac{\varepsilon}{|\mathcal{T}|},$$

and

$$\frac{1}{|\mathcal{K}|} \sum_{k \in \mathcal{K}} \Pr[h(k, m) = t] = \frac{1}{|\mathcal{T}|}.$$

An  $\varepsilon$ -almost strong 2-universal hash function  $h$  can be formed from an  $\varepsilon$ -almost XOR 2-universal hash function  $h'$  where the average probability of  $h'(k, m_1) \oplus h'(k, m_2) = t$  for any  $t$  is bounded by  $\varepsilon$  [34], and a authentication masking key (used as a one-time pad),  $h(k, m) = h'(k^h, m) \oplus k^{\text{mask}}$  [9, 28]. A weaker notion of universality can be defined, where an  $\varepsilon$ -almost 2-universal hash function refers to one where the average probability of  $h(m_1) = h(m_2)$  is bounded by  $\varepsilon$  [41].

It is clear that if the authentication masking key is never used again after the hash is performed,  $K^h$  remains secure and tag  $T$  appears as a random string to the adversary,

**Theorem 4.** *Let  $h'$  be a  $\varepsilon$ -almost XOR 2-universal hash function with authentication key  $K^h$ , and  $h(k, m) = h'(k^h, m) \oplus k^{\text{mask}}$ , with a fully random masking string  $K^{\text{mask}}$ . Consider an adversary which was provided with a valid message-tag pair  $(m, t)$ , and the honest party which discards (trace away)  $K^{\text{mask}}$  (i.e.  $K^{\text{mask}}$  acts as a one-time pad). The seed  $K^h$  remains private, in the sense that*

$$\rho_{K^h M T E} = \tau_{K^h} \otimes \tau_T \otimes \rho_{M E}.$$

A property of  $\varepsilon$ -almost 2-universal hash functions that is useful is that they are strong extractors. This is demonstrated from the quantum leftover hash lemma (QLHL) [38, 41],

**Theorem 5** (Quantum leftover hash lemma). *Let  $h$  be a  $\varepsilon$ -almost 2-universal hash function with key  $K$ . Consider a protocol which begins with state  $\tau_K \otimes \rho_{M E}$ , and the hash is computed as  $Y = h(K, M)$ . Then, for any  $\varepsilon_{\text{sm}} \geq 0$  and  $\varepsilon' > 0$ ,*

$$\Delta(\rho_{Y K E}, \tau_Y \otimes \tau_K \otimes \rho_E) \leq 2\varepsilon_{\text{sm}} + 2\varepsilon' + \sqrt{2^l \varepsilon - 1 + 2^{l - H_{\min}^{\varepsilon_{\text{sm}}}(M|E) + \log_2(\frac{2}{\varepsilon^2} + 1)}},$$

where  $l = |Y|$  is the length of tag  $Y$ . We call the hash function a  $\delta$ -strong extractor, where  $\delta$  matches the RHS of the inequality. If  $h$  is instead 2-universal, then

$$\Delta(\rho_{Y K E}, \tau_Y \otimes \tau_K \otimes \rho_E) \leq 2\varepsilon_{\text{sm}} + \frac{1}{2} \times 2^{-\frac{1}{2}[H_{\min}^{\varepsilon_{\text{sm}}}(M|E) - l]}.$$

## A.4 Pseudorandom Number Generation

The security of cryptographically-secure PRNGs are defined by the probability that any distinguishing protocol with limited resources can distinguish between the PRNG output and an ideal random number generator (IRNG) output [20]. We note that this security is in general composable when considering computational security. [7, 8]. We can consider quantum adversaries in general since the QAKE protocol involves quantum steps. Since we are interested in computing key generation rates, we adopt a more concrete security definition with resources  $t$  [4, 14] (e.g. time) instead of presenting security against quantum polynomial-time (QPT) adversaries<sup>3</sup>.

**Definition 2** (Quantum-secure PRNG). *A pseudorandom number generator (PRNG) is a function  $G^{\text{PRNG}} : \mathcal{K} \rightarrow \mathcal{Y}$  that takes as input a seed  $k \in \mathcal{K}$  with length  $l$  and outputs a bit string  $y \in \mathcal{Y}$  with length  $n$ , where  $l < n$ . A  $(l, n)$ -standard PRNG is  $(t, \varepsilon)$  quantum-secure if for any quantum algorithm  $\mathcal{A}_D^t$  constrained by some resources  $t$  with output  $D$ , the PRNG equipped with a random seed  $G_{\mathcal{K}}^{\text{PRNG}}$  is indistinguishable from an ideal random number generator  $G^{\text{IRNG}}$  that samples random numbers  $r$  uniformly at random from  $\mathcal{Y}$ ,*

$$\left| \Pr[\mathcal{A}_D^{G_{\mathcal{K}}^{\text{PRNG}}, t} = 1] - \Pr[\mathcal{A}_D^{G^{\text{IRNG}}, t} = 1] \right| \leq \varepsilon.$$

One important property of the PRNG is the difficulty in guessing the seed of the PRNG when given partial information of the output, which can only succeed with a small probability  $\varepsilon_{\text{guess}}$ , as summarised below.

**Theorem 6.** *Consider a scenario where a random number  $y \in \{0, 1\}^n$  is prepared from a  $(t', \varepsilon_{\text{PRNG}})$ -quantum-secure PRNG with a random seed  $k$  of length  $l$  with security parameter  $\varepsilon_{\text{PRNG}}$ , i.e.  $y = G^{\text{PRNG}}(k)$ , and a  $n$ -bit bit string  $z$ , with  $\Pr[z_i = 1] = p_1$ , for  $i = 1, \dots, n$ , with  $n > 2l$ . Suppose an adversary is provided with*

<sup>3</sup>QPT adversaries are adversaries with polynomial access to both classical and quantum resources (e.g. polynomial storage and computational power)

$y_{z=1} := \{y_i : z_i = 1\}$ ,  $G^{\text{PRNG}}$  and  $z$ , and is tasked to guess the seed  $k$ . When  $t' \geq t + t_{SG,PR}$ , the probability that any quantum adversary with resource upper bounded by  $t$  can correctly guess  $k$  is bounded by

$$\Pr[\hat{k} = k] \leq \varepsilon_{\text{guess}}$$

where  $\varepsilon_{\text{guess}} \leq \varepsilon_{\text{PRNG}} + 2^{-n+l}$ , and  $t_{SG,PR}$  is the total resources required for generating string  $z$  and generating  $y$  from a master key using the PRNG.

*Proof.* We start with noting that correctly guessing the seed allows one to guess all the outcomes  $y$  from the PRNG. If there is an algorithm which can guess the seed from the set  $y_{z=1}$ , it can be used to distinguish whether a string  $y \in \{0, 1\}^n$  is being generated from a PRNG or from an IRNG. Therefore, it will violate the security of the  $(t', \varepsilon_{\text{PRNG}})$ -PRNG.

Suppose for contradiction that an algorithm  $\mathcal{A}$  with resources  $t$  is able to guess the seed  $k$  correctly with probability at least  $\varepsilon_{\text{guess}} > 2^{-l}$  (note  $\varepsilon_{\text{guess}} \leq 2^{-l}$  is trivially achievable with random guess), i.e.,

$$\Pr[\mathcal{A}(y_{z=1}) = k] > \varepsilon_{\text{guess}}. \quad (8)$$

We construct an algorithm  $\hat{\mathcal{A}}$  that distinguishes  $G^{\text{PRNG}}(k)$  from  $G^{\text{IRNG}}$  as follows:

1. Upon receiving a string  $y \in \{0, 1\}^n$ , it generates a string  $z = z_1 \dots z_n$ , where  $z_i \in \{0, 1\}$ , and  $\Pr[z_i = 1] = p_1$ , for all  $i \in \{1, \dots, n\}$ .
2. From  $z$ , and  $y$ , it constructs the set  $y_{z=1}$ , and feed it to the algorithm  $\mathcal{A}$  to guess the seed. Suppose  $\mathcal{A}(y_{z=1}) = \hat{k}$ .
3. If  $G^{\text{PRNG}}(\hat{k}) = y$ , the algorithm returns 1, indicating  $y$  is being generated via a PRNG.
4. Otherwise, the algorithm returns 0, indicating  $y$  is sampled via an IRNG.

The additional resources required for the generation of string  $z$  and generation of  $y$  from the master key guess  $\hat{k}$  is defined as  $t_{SG,PR}$ . As such,  $\hat{\mathcal{A}}$  requires  $t + t_{SG,PR}$  resources.

When the protocol is implemented on the PRNG, it is clear that if the guess of  $\hat{k}$  is correct, i.e.  $\hat{k} = k$ , the algorithm returns 1. Therefore,

$$\Pr[\hat{\mathcal{A}}^{G^{\text{PRNG}}, t+t_{SG,PR}} = 1] > \varepsilon_{\text{guess}}.$$

When the protocol is implemented on an IRNG, the range of  $G^{\text{PRNG}}$  is limited by the size of the seed,  $2^l$ . For any  $y$  outside the range of  $G^{\text{PRNG}}$ , it is clear that  $G^{\text{PRNG}}(k) \neq y$  for any  $k$ , and  $\hat{\mathcal{A}}^{G^{\text{IRNG}}, t+t_{SG,PR}}$  returns 0. Therefore, for uniformly generated  $y \in \{0, 1\}^n$ ,

$$\Pr[\hat{\mathcal{A}}^{G^{\text{IRNG}}, t+t_{SG,PR}} = 1] \leq 2^{-n+l}.$$

Given the condition that  $n > 2l$  and  $\varepsilon_{\text{guess}} > 2^{-l}$ , the IRNG term is smaller and the ability of  $\hat{\mathcal{A}}$  to distinguish between the PRNG and IRNG is then

$$\left| \Pr[\hat{\mathcal{A}}^{G^{\text{PRNG}}, t+t_{SG,PR}} = 1] - \Pr[\hat{\mathcal{A}}^{G^{\text{IRNG}}, t+t_{SG,PR}} = 1] \right| > \varepsilon_{\text{guess}} - 2^{-n+l}.$$

According to the definition of the PRNG,  $\left| \Pr[\hat{\mathcal{A}}_D^{G^{\text{PRNG}}, t'} = 1] - \Pr[\hat{\mathcal{A}}_D^{G^{\text{IRNG}}, t'} = 1] \right| \leq \varepsilon_{\text{PRNG}}$ . Since  $t' \geq t + t_{SG,PR}$ , the bound holds in particular for algorithm  $\hat{\mathcal{A}}^{G^{\text{PRNG}}, t+t_{SG,PR}}$ . Therefore, when  $\varepsilon_{\text{guess}} - 2^{-n+l} = \varepsilon_{\text{PRNG}}$ , we encounter a contradiction and  $\Pr[\hat{k} = k] \leq \varepsilon_{\text{guess}} = \varepsilon_{\text{PRNG}} + 2^{-n+l}$ .  $\square$

## B Adapting AKE Framework to QAKE Security

We seek to incorporate standard QKD with authentication security in a QAKE security framework, which utilises the same terminology and tools as a classical AKE framework. Here, we present only the main points of the classical AKE framework relevant in the context of QKD, and we refer the reader to Ref. [13] for more details on the classical AKE framework.

## B.1 Security Model

We begin by first examining the security model of QAKE, based off the QKD security model and authentication requirements before linking the model to the classical AKE framework. QAKE adopts a security model where the target key generation partner is between honest Alice and Bob, with an adversary (or eavesdropper) present in their communication channel that could seek to impersonate either party or steal the shared keys between Alice and Bob. The protocol can be generalised to multiple parties, with any pre-shared secrets used for authentication being shared pairwise. In general, the protocol involve input registers  $S$  representing the pre-shared secrets (e.g. authentication keys),  $L$  for any labels (e.g. to indicate the secret to use), with  $E$  labelling any side-information of the adversary. After the protocol, the output would include  $F_A F_B$ , which represent the respective parties' choice: (1)  $F = \phi$  representing that it is not involved in the session, (2)  $F = 0$  representing that it chose not to authenticate the other party, and (3)  $F = 1$  representing that it chose to authenticate the other party. It would also output keys  $K_A$  and  $K_B$  respectively if  $F_A = 1$  and  $F_B = 1$  (Note that this can in principle be decoupled – i.e. parties can choose to authenticate, but not generate keys, but we couple them for simplicity). Otherwise, it would output  $\perp$  signalling that no secure keys are generated.

The classical AKE framework [13] is broader in its model, examining multiple parties, each with its own unique identity. While classical AKE do not require all parties to provide information for other parties to authenticate its identity (to provide for instances where anonymous key generation is acceptable), we require mutual authentication for the QAKE protocol, i.e. setting the set of parties that need to provide authentication information to be the set of all parties. During each session of the protocol, each party can set up local sessions (an instance that is present locally which runs the protocol steps and stores the outputs, e.g. in QKD, this could be Alice's QKD box running Alice's steps in a single protocol session and storing the outputs), labelled by  $l = (i, j, k)$ , with its identity  $i$  (e.g. Alice), intended peer  $j$  (e.g. Bob), and session number  $k$ . The parties are assumed to hold public-private key pairs  $(pk_i, sk_i)$  for authentication purposes. For QAKE, we generalize to allow for the use of symmetric keys by having parties hold “matching keys”  $mk_i$  instead, which can either contain  $sk_i$  for symmetric keys or  $pk_i$  for public keys<sup>4</sup>. We note also that the corresponding peers should hold the corresponding matching key  $mk_i$  that allows them to authenticate party  $i$ .

During the protocol, the adversary is present in the network between all parties, and is able to interfere with the communication, e.g. delay, redirect or alter messages. In addition, the adversary is in general allowed to call on the session to reveal the session key and corrupt any party, which forces the reveal of the party's secret keys  $sk_i$ . We note that the security conditions (e.g. key secrecy) will impose conditions (e.g. party not corrupted) on the use of such attacks. For QAKE, since Alice and Bob are assumed to be honest, the reveal of the session key, along with corrupting of Alice and Bob is disallowed.

During the protocol or at the end of the protocol, various outputs or information would be present with each party's local sessions. These are:

1. Session acceptance: Indicates if a party has accepted or rejected the session. If a party is not involved, the session acceptance is maintained as  $\phi$  as initialized. This matches exactly the choice  $F_A F_B$  of the QAKE protocol.
2. Keys: The session outputs keys, which is set to  $\perp$  unless the session is accepted – matching  $K_A K_B$  in QAKE.
3. Session identifier: Initialized as  $\perp$ , and changed to other values when the session is accepted. This value is meant to identify local sessions that are partners – local sessions with same session identifier are partners (note that they have to both accept the session). This value is implicitly part of QAKE protocols, where Alice's and Bob's generated local sessions are partners. To explicitly include the identifier, one can simply modify the local session label  $L$  to an identifier, e.g. setting identifier as  $(i, j, k)$  if  $i < j$  and  $(j, i, k)$  otherwise, or include a random string that is sent and authenticated during the protocol. We take the first case for simplicity, and also note that for the QAKE protocol, these partnering local sessions are always between two different parties (Alice and Bob).
4. Entity confirmation identifier: Indicates the local sessions that eventually would partner, i.e. similar to session identifier, but can be set earlier than protocol acceptance stage. For the QAKE protocol, we can set these values as  $(i, j, k)$  (or  $(j, i, k)$ ) after the first message is sent or arrives at the party.<sup>5</sup>

---

<sup>4</sup>We note that this generalization has an impact on certain attacks. For instance, the classical AKE model captures the key-compromise impersonation attack, where an adversary that knows the secret key of Alice attempts to impersonate Bob and get Alice to accept the authentication. The leakage of  $sk_A$  alone would not cause this compromise, but with the use of symmetric keys, the protocol would no longer provide resistance to key-compromise impersonation. However, since this attack is not relevant to the QAKE of interest, where both Alice and Bob are assumed to be honest, we leave the account of such changes to future work.

5. Key confirmation identifier: Indicates the local sessions that eventually would generate the same key, and this can be chosen similarly to the entity confirmation identifier for QAKE.

## B.2 Security Conditions

With the input and output registers defined, let us formally introduce the security definitions. We note that the classical AKE framework has multiple security conditions that are related and corresponds to desirable properties. However, we choose only the most suitable, with many of the other properties being derivable from these conditions.

The first condition, robustness, is not part of the classical AKE framework, but is important nonetheless. It necessitates that the protocol can succeed when the adversary is absent, and the protocol is not trivially rejecting all authentication to always guarantee security.

**Definition 3** ( $\varepsilon_{\text{rob}}$ -robustness). *A QAKE protocol is  $\varepsilon_{\text{rob}}$ -robust if it passes with high probability in the absence of any adversary, i.e.*

$$\Pr[F_A = F_B = 1] \geq 1 - \varepsilon_{\text{rob}}.$$

The second condition, explicit entity authentication, addresses the security associated with mutual authentication between Alice and Bob. It comes in two variants: full explicit entity authentication and almost-full explicit entity authentication.

We impose full explicit entity authentication on Alice, requiring that Bob will generate a partnering local session when Alice accepts. More formally, the definition in Ref. [13] presents a predicate that states that for all local sessions  $l$ , when the local session accepts, there exists a partner local session  $l'$ , and this local session belongs to the intended peer of the local session<sup>6</sup>. This includes a simplification noting that for QAKE, mutual authentication is expected, and both Alice and Bob are assumed to be honest. As such, we have the implication that  $F_A = 1 \implies F_B = 1$ , which the security condition requires to be true with high probability.

The condition on almost-full explicit entity authentication is imposed on Bob, who sends the final authentication message to Alice. As such, he is unable to guarantee that at the end of the protocol, Alice would generate an accepting local session (necessary for session identifier generation and partnering) since the adversary can interfere with the final authentication message transmission. More formally, the definition in Ref. [13] presents a predicate that states that for all local sessions  $l$ , when the local session accepts, there exists a local session  $l'$  with the same entity confirmation identifier, which is a partner to  $l$  if  $l'$  generates a session identifier, and this partner must be the peer of  $l$ . This includes the same simplification that mutual authentication is expected, and both Alice and Bob are assumed to be honest. As such, we have the implication that  $F_B = 1 \implies F_A = 0, 1$ , where Alice's local session either rejects the session (same entity confirmation identifier, but not partners) or accepts the session (partners)<sup>7</sup>.

The security of both conditions requires that the probability of the predicates being false is small, i.e. the probability of “bad events” is small. We note that the security is defined relative to a computationally bounded adversary, with the small probability given as negligible relative to a security parameter. We can generalise here (and in the following security definitions) to a general unbounded adversary, and define some small parameter  $\varepsilon$  to quantify the “negligible” probability. As such, we define the explicit entity authentication as

**Definition 4** ( $(\varepsilon_{\text{EA},f}, \varepsilon_{\text{EA},af})$ -explicit entity authentication). *A QAKE protocol has  $\varepsilon_{\text{EA},f}$ -full explicit entity authentication for Alice if the authentication fails with high probability when Bob is not accepting, i.e.*

$$\Pr[F_A = 1, F_B = 0] + \Pr[F_A = 1, F_B = \phi] \leq \varepsilon_{\text{EA},f},$$

*and it has  $\varepsilon_{\text{EA},af}$ -almost full explicit entity authentication for Bob if the authentication fails with high probability when Alice is not involved in the session, i.e.*

$$\Pr[F_A = \phi, F_B = 1] \leq \varepsilon_{\text{EA},af}.$$

<sup>5</sup>The choice of the confirmation identifier should coincide with when the identity of the peer (e.g. Bob) is made known to the the party (e.g. Alice). In classical AKE and QAKE, a pre-specified peer model is assumed, where each local session knows its intended partner's identity. As such, these information should be exchange at the start of the protocol in practice.

<sup>6</sup>We note there is a separate subtle implication that any partner to  $l$  must belong to the intended peer defined in explicit entity authentication. This means that the predicate does not preclude the possibility that two local sessions can be established on Bob that partners the same Alice. Since Alice and Bob are considered honest in QAKE, this can be simply prevented by having them to individually check that they do not have local sessions with the same session identifiers.

<sup>7</sup>There is similar subtle implication as per full explicit entity authentication where the definition does not prevent multiple accepting local sessions to be established on Alice, though that can be addressed similarly since Alice is honest.

Note that we label  $\varepsilon_{EA} = \varepsilon_{EA,f} + \varepsilon_{EA,af}$  for brevity.

The third security condition is termed Match-security, though in the context of the QAKE protocol, it reduces to the correctness condition. This security condition mainly elevates the entity authentication security condition to provide key authentication as well – where Alice and Bob can guarantee that the other party will generate the same key confirmation identifier and keys if both local sessions are accepting<sup>8</sup>. Formally, Ref. [13] defines the Match-predicate as four conditions: (1) partner local sessions generate the same key, (2) partner local sessions generate same key confirmation identifier, (3) at most two local sessions can generate the same session identifier, and (4) local sessions with the same key confirmation identifier would generate the same key if both local sessions are accepting. The four conditions, in the context of QAKE, can be simplified:

1. This condition can be summarised as when partnering local sessions are accepting (in QAKE this means that they are key generating as well), they will generate the same keys, i.e.  $F_A = F_B = 1 \implies K_A = K_B$ .
2. Since we set key confirmation identifier and session identifier in the same way for QAKE, this condition is always true.
3. This condition is always guaranteed in QAKE since the choice of session identifier as  $(i, j, k)$  (or  $(j, i, k)$ ), along with honest Alice and Bob, and the fact that only one pair of local sessions have same set of parties  $(i, j)$  and same index  $k$ , means that only two local sessions can generate the same session identifier.
4. Equivalent to condition 1 since key confirmation identifier and session identifier are set in the same way.

Condition 1 in the context of QAKE therefore matches the correctness condition of QKD, while the remaining are either always true or reduce to condition 1. Therefore, we can define the Match-security as

**Definition 5** ( $\varepsilon_{MS}$ -Match security). *A QAKE protocol has  $\varepsilon_{MS}$ -Match security if*

$$\Pr[K_A \neq K_B, F_A = 1, F_B = 1] \leq \varepsilon_{MS}.$$

The final condition is key secrecy (also termed BR-secrecy), which requires that any keys generated be secret from the adversary. Ref. [13] defines the secrecy as a secrecy game, being the ability for an adversary to distinguish between an ideal key sampled from the key distribution and the actual key. Certain secrecy freshness conditions are necessary for the game, such as the owner and peer being honest, the session key not directly revealed to the adversary (e.g. announced), and that there is expected mutual authentication, which are all part of the assumptions of QAKE, i.e. the freshness condition is satisfied. More formally, the secrecy condition is defined by [13]

$$|\Pr[\mathcal{A}_D^{\text{real}} = 1] - \Pr[\mathcal{A}_D^{\text{ideal}} = 1]| = \text{negl}, \quad (9)$$

where a distinguisher  $\mathcal{A}$  makes the guess  $D$  on whether the keys are the actual key ( $D = 1$ ) or an ideal key ( $D = 0$ ), guess  $D$  is set as  $\perp$  if the local session is not accepting [6], and  $\text{negl}$  representing negligible in some security parameter. Noting that when  $D = \perp$ , the ideal and real cases are identical, and with the upgrade from a computationally bounded adversary to an unbounded adversary with quantum capabilities, the secrecy condition can be redefined in terms of trace distance, representing the ability to distinguish between the ideal and real keys. Note that we explicitly take only the cases of  $(F_A, F_B)$  being  $(0, 1)$  and  $(1, 1)$ , since the probability of  $F_B = 1$  when  $F_A = \phi$  is small, and accounted for in entity authentication. As such, we define key secrecy as

**Definition 6** ( $\varepsilon_{KS}$ -key secrecy). *A QAKE protocol has  $\varepsilon_{KS}$ -key secrecy if*

$$\Delta(\rho_{F_A F_B K_B LSE \wedge (F_A, F_B) \in \{0,1,11\}}, \tau_{K_B} \otimes \rho_{F_A F_B LSE \wedge (F_A, F_B) \in \{0,1,11\}}) \leq \varepsilon_{KS}.$$

## C Security Analysis of QAKE Protocol

### C.1 Multi-Session to Single-Session Security Reduction

Here, we prove a tighter version of Thm. 1 using an inductive proof, noting that the final session need not keep the secrets private, where we define the set of ideal states for this final session as  $\mathcal{S}_{\text{out}}$ .

**Theorem 7.** *Suppose we have the conditions:*

1. *The initial state is an ideal input state  $\rho_0 \in \mathcal{S}_{\text{in}}$ .*

<sup>8</sup>There is a separate condition termed key-match soundness that is required to elevate explicit entity authentication to explicit key authentication. This condition is proven in classical AKE framework based on match secrecy and key secrecy conditions.

2. There exists an ideal output state which preserves any necessary secrets that is  $\varepsilon_{\text{sec,int}}$ -close to the output state of a single session  $\mathcal{P}_i$ , i.e. for any  $\sigma \in \mathcal{S}_{\text{in}}$ , there exists a state  $\rho \in \mathcal{S}'_{\text{out}}$  such that

$$\Delta(\mathcal{P}_i(\sigma), \rho) \leq \varepsilon_{\text{sec,int}}.$$

3. The set of ideal output states is a subset of the set of ideal input states  $\mathcal{S}'_{\text{out}} \subseteq \mathcal{S}_{\text{in}}$ .

4. There exists an ideal output state that is  $\varepsilon_{\text{sec}}$ -close to the output state of a single session  $\mathcal{P}_i$ , i.e. for any  $\sigma \in \mathcal{S}_{\text{in}}$ , there exists a state  $\rho \in \mathcal{S}_{\text{out}}$  such that

$$\Delta(\mathcal{P}_i(\sigma), \rho) \leq \varepsilon_{\text{sec}}.$$

Then, for all  $i \in [1, n_{\text{sess}}]$ , there exists  $\rho_i \in \mathcal{S}_{\text{out}}$  such that

$$\Delta(\mathcal{P}^i(\rho_0), \rho_i) \leq (i-1)\varepsilon_{\text{sec,int}} + \varepsilon_{\text{sec}}.$$

*Proof.* The proof is by induction. Let us consider a statement that for any  $i \in [1, n_{\text{sess}}-1]$ , there exists  $\rho_i \in \mathcal{S}'_{\text{out}}$  such that

$$\Delta(\mathcal{P}^i(\rho_0), \rho_i) \leq i\varepsilon_{\text{sec,int}}. \quad (10)$$

For  $i = 1$ , the statement is trivially true from conditions 1 and 2. Suppose the statement is true for index  $j$ , i.e. there exists  $\rho_j \in \mathcal{S}'_{\text{out}}$  such that  $\Delta(\mathcal{P}^j(\rho_0), \rho_j) \leq j\varepsilon_{\text{sec,int}}$ . From condition 3, we know that  $\rho_j \in \mathcal{S}'_{\text{out}} \subseteq \mathcal{S}_{\text{in}}$  is a valid input state as well. As such, by condition 2, there exists a state  $\rho_{j+1} \in \mathcal{S}'_{\text{out}}$  such that

$$\Delta(\mathcal{P}(\rho_j), \rho_{j+1}) \leq \varepsilon_{\text{sec,int}}. \quad (11)$$

We can expand the LHS term for the  $(j+1)$ -th index, where there exists  $\rho_{j+1} \in \mathcal{S}'_{\text{out}}$  such that

$$\begin{aligned} & \Delta(\mathcal{P}^{j+1}(\rho_0), \rho_{j+1}) \\ & \leq \Delta(\mathcal{P}^{j+1}(\rho_0), \mathcal{P}(\rho_j)) + \Delta(\mathcal{P}(\rho_j), \rho_{j+1}) \\ & \leq \Delta(\mathcal{P}^j(\rho_0), \rho_j) + \varepsilon_{\text{sec,int}} \\ & \leq (j+1)\varepsilon_{\text{sec,int}}, \end{aligned} \quad (12)$$

where the first line applies the triangle inequality, and the second line notes that the CPTP map  $\mathcal{P}$  cannot increase trace distance. Since the statement is true for  $i = 1$ , and the statement being true for  $j$  implies that it is true for  $j+1$ , by mathematical induction, the statement is true for any  $i \in [1, n_{\text{sess}}-1]$ .

To prove the statement of Thm. 1, we first note that since  $\rho_i \in \mathcal{S}'_{\text{out}} \subseteq \mathcal{S}_{\text{in}}$ , condition 4 states that there exists a state  $\rho_{i+1} \in \mathcal{S}_{\text{out}}$  such that

$$\Delta(\mathcal{P}(\rho_i), \rho_{i+1}) \leq \varepsilon_{\text{sec}}. \quad (13)$$

As such, we can use the triangle inequality to arrive at

$$\begin{aligned} \Delta(\mathcal{P}^{i+1}(\rho_0), \rho_{i+1}) & \leq \Delta(\mathcal{P}^{i+1}(\rho_0), \mathcal{P}(\rho_m)) + \Delta(\mathcal{P}(\rho_m), \rho_{i+1}) \\ & \leq \Delta(\mathcal{P}^i(\rho_0), \rho_i) + \varepsilon_{\text{sec}} \\ & \leq i\varepsilon_{\text{sec,int}} + \varepsilon_{\text{sec}} \end{aligned} \quad (14)$$

for any  $i \in [1, n_{\text{sess}}]$ . The same statement is true for  $i = 0$  by condition 4, and thus we can arrive at the theorem.  $\square$

Condition 2 requires an additional condition for the set of ideal states, which we express as  $\rho^{\text{ideal,int}} \in \mathcal{S}'_{\text{out}}$ , to match  $\mathcal{S}_{\text{in}}$ , where the necessary secrets  $S$  are kept private. Crucially, the main difference between  $\rho^{\text{ideal,int}} \in \mathcal{S}'_{\text{out}}$  and  $\rho^{\text{ideal}} \in \mathcal{S}_{\text{out}}$  is the form of the *LSE* subsystem. In general,  $\rho^{\text{ideal}}$  has *LSE* subsystems that can take any form, including one matching the actual output state while the form of  $\rho^{\text{ideal,int}}$  has *LSE* subsystems that are of a specific form (depending on the protocol requirement). This forms the rationale behind the definition of the shared secrets privacy condition<sup>9</sup>:

**Definition 7** ( $\varepsilon_{\text{SP}}$ -Shared Secrets Privacy). A QAKE protocol has  $\varepsilon_{\text{SP}}$ -shared secrets privacy if

$$\Delta \left( \sum_{(f_A, f_B) \notin \mathcal{S}_{\text{SP}}} p_{f_A f_B} \rho_{LSE}^{f_A f_B}, \sum_{(f_A, f_B) \notin \mathcal{S}_{\text{SP}}} p_{f_A f_B} \sigma_{LSE}^{f_A f_B} \right) \leq \varepsilon_{\text{SP}},$$

where  $p_{f_A f_B}$  is the probability of the output state recording  $(F_A, F_B) = (f_A, f_B)$ ,  $\mathcal{S}_{\text{SP}} = \{\phi 1, 1\phi, 10\}$  and  $\sigma_{LSE}^{f_A f_B} \in \mathcal{S}_{\text{in}}$ .

<sup>9</sup>In classical AKE [13], this requirement of maintaining secret values from one session to the next is part of the parameter crypt. Here, we make the requirement explicit with  $\varepsilon_{\text{SP}}$  distance from full secrecy.

## C.2 Single-Session Security Conditions

Recall that the set of ideal input state is defined by  $\mathcal{S}_{in} = \{\rho^{in} = \sum_{jj'} p_{jj'} \rho_{LSE}^{in,jj'}\}$ , where

$$\rho_{LSE}^{in,jj'} = |jj'\rangle\langle jj'|_{\alpha\alpha'} \otimes \tau_{K_2 R K_{1,j}^{mask} \dots K_{1,m}^{mask}} \otimes \mathcal{E}_{K_1^h K_{1,j-1}^{mask} E_{j-1} \rightarrow E} \circ \dots \circ \mathcal{E}_{K_1^h K_{1,j'}^{mask} E_{j'} \rightarrow E_{j'+1}} (\tau_{K_1^h K_{1,j'}^{mask} \dots K_{1,j-1}^{mask}} \otimes \rho_{E_{j'}}),$$

where  $L = \alpha\alpha'$  are the labels and  $S$  refer to the secrets. We note here an observation that when a partial trace of  $K_{1,j'}^{mask}$  is applied to the state, it effectively removes the corresponding channel  $\mathcal{E}_{K_1^h K_{1,j'}^{mask} E_{j'} \rightarrow E_{j'+1}}$ , with appropriate relabelling of  $E_{j'}$  as  $E_{j'+1}$ .<sup>10</sup> Similarly, recall that the set of ideal output state is given by  $\mathcal{S}'_{out} = \{\rho^{ideal,int}\}$ , where

$$\begin{aligned} \rho^{ideal,int} = & |\perp\perp\rangle\langle\perp\perp|_{K_A K_B} \otimes \left[ p_{0\phi} |0\phi\rangle\langle 0\phi|_{F_A F_B} \otimes \sigma_{LSE}^{0\phi} + p_{\phi 0} |\phi 0\rangle\langle \phi 0|_{F_A F_B} \otimes \sigma_{LSE}^{\phi 0} + p_{00} |00\rangle\langle 00|_{F_A F_B} \otimes \sigma_{LSE}^{00} \right] \\ & + p_{01} |01, \perp\rangle\langle 01, \perp|_{F_A F_B K_A} \otimes \tau_{K_B} \otimes \sigma_{LSE}^{01} + p_{11} |11\rangle\langle 11|_{F_A F_B} \otimes \tilde{\tau}_{K_A K_B} \otimes \sigma_{LSE}^{11}, \end{aligned}$$

for  $\sigma_{LSE}^{f_A f_B} \in \mathcal{S}_{in}$ . We note that for  $\mathcal{S}_{out}$ , the ideal output state would be of a similar form,

$$\begin{aligned} \rho^{ideal} = & |\perp\perp\rangle\langle\perp\perp|_{K_A K_B} \otimes \left[ p_{0\phi} |0\phi\rangle\langle 0\phi|_{F_A F_B} \otimes \rho_{LSE}^{0\phi} + p_{\phi 0} |\phi 0\rangle\langle \phi 0|_{F_A F_B} \otimes \rho_{LSE}^{\phi 0} + p_{00} |00\rangle\langle 00|_{F_A F_B} \otimes \rho_{LSE}^{00} \right] \\ & + p_{01} |01, \perp\rangle\langle 01, \perp|_{F_A F_B K_A} \otimes \tau_{K_B} \otimes \rho_{LSE}^{01} + p_{11} |11\rangle\langle 11|_{F_A F_B} \otimes \tilde{\tau}_{K_A K_B} \otimes \rho_{LSE}^{11}. \end{aligned} \quad (15)$$

With the output state descriptions, and noting that  $K_A K_B F_A F_B$  can be incorporated into  $E$  for the next session, we can observe that the output state in  $\mathcal{S}'_{out}$  is a linear combination of  $\sigma_{LSE}^{\alpha\alpha'}$ , matching the general input state and thus satisfying condition 3 in Thm. 1. Condition 1 in the same theorem is trivially satisfied since all secrets begin as private with index  $\alpha = \alpha' = 1$ . Therefore, we can focus on analysing security conditions 2 and 4. The security definition is given by the statement: for any  $\sigma_{LSE} \in \mathcal{S}_{in}$ , there exists  $\rho^{ideal,int} \in \mathcal{S}'_{out}$  and  $\rho^{ideal} \in \mathcal{S}_{out}$  such that

$$\begin{aligned} \Delta(\mathcal{P}(\sigma_{LSE}), \rho_{F_A F_B K_A K_B LSE}^{ideal,int}) &\leq \varepsilon_{sec,int} \\ \Delta(\mathcal{P}(\sigma_{LSE}), \rho_{F_A F_B K_A K_B LSE}^{ideal}) &\leq \varepsilon_{sec} \end{aligned} \quad (16)$$

Here, we prove the generalized version of Thm. 2, which allows the security analysis to be reduced to various security conditions.

**Theorem 8.** *Consider a protocol  $\mathcal{P}$  with an ideal input state  $\sigma_{LSE} \in \mathcal{S}_{in}$ . Then, overall protocol security is satisfied when the intermediate session security parameter is*

$$\varepsilon_{sec,int} = \varepsilon_{EA} + \varepsilon_{MS} + \varepsilon_{KS} + \varepsilon_{SP},$$

and the final session security parameter is

$$\varepsilon_{sec} = \varepsilon_{EA} + \varepsilon_{MS} + \varepsilon_{KS}.$$

*Proof.* For any input state  $\sigma_{LSE} \in \mathcal{S}_{in}$ , let  $\rho_{F_A F_B K_A K_B LSE} = \mathcal{P}(\sigma_{LSE})$  be the output state. We seek find an ideal output state  $\rho_{F_A F_B K_A K_B LSE}^{ideal}$  that is close to the actual output state with probabilities  $p_{F_A F_B}^{ideal}$ , where we note the additional superscript ideal to distinguish it from the actual output distribution  $p_{F_A F_B}^{real}$  of  $\rho_{F_A F_B K_A K_B LSE}$ . We define

$$p_{F_A F_B}^{ideal} = \begin{cases} p_{\phi 0}^{real} + p_{\phi 1}^{real} & F_A = \phi, F_B = 0 \\ p_{0\phi}^{real} + p_{1\phi}^{real} & F_A = 0, F_B = \phi \\ p_{00}^{real} + p_{10}^{real} & F_A = 0, F_B = 0 \\ p_{F_A F_B}^{real} & \text{Otherwise} \end{cases}, \quad (17)$$

while the  $\rho_{LSE}^{ideal, f_A f_B} = \rho_{LSE}^{f_A f_B}$  of  $\rho_{F_A F_B K_A K_B LSE}$  for  $(F_A, F_B) \notin \{\phi 1, 1\phi, 10\}$ . With this definition, we can split the trace distance for  $\varepsilon_{sec}$ -security into components, first extracting the components where  $F_A$  or  $F_B$  is  $\phi$ ,

$$\begin{aligned} \Delta(\rho, \rho^{ideal}) \leq & \Delta(\rho_{\wedge(F_A, F_B) \in \{01, 11\}}, \rho_{\wedge(F_A, F_B) \in \{01, 11\}}^{ideal}) + \Delta(\rho_{\wedge F_A = \phi}, \rho_{\wedge F_A = \phi}^{ideal}) + \Delta(\rho_{\wedge F_B = \phi}, \rho_{\wedge F_B = \phi}^{ideal}) \\ & + \Delta(\rho_{\wedge(F_A, F_B) \in \{00, 10\}}, \rho_{\wedge(F_A, F_B) \in \{00, 10\}}^{ideal}), \end{aligned} \quad (18)$$

<sup>10</sup>More formally, the partial trace can be shifted to before the corresponding channel  $\mathcal{E}_{K_1^h K_{1,j'}^{mask} E_{j'} \rightarrow E_{j'+1}}$ , which describes the adversary querying the oracle, followed by  $K_{1,j'}^{mask}$  being discarded. Since  $K_{1,j'}^{mask}$  acts as an one-time pad on the tag  $T_{AV}$ , Thm. 4 implies that  $T_{AV}$  would appear random to the adversary. As such, this is equivalent to the adversary randomly sampling  $T_{AV}$  and using that value instead. As such, the process can be described by simply  $\mathcal{E}_{E_{j'} \rightarrow E_{j'+1}}$ , an internal update of the adversary's internal state.

where the subsystem labels  $K_A K_B F_A F_B LSE$  are dropped for brevity.

We now show that the latter three trace distances are bounded by the explicit entity authentication security condition. Expanding the first term explicitly, we have

$$\begin{aligned}
& \Delta(\rho_{\wedge F_A=\phi}, \rho_{\wedge F_A=\phi}^{\text{ideal}}) \\
& \leq p_{\phi 0}^{\text{real}} \Delta(\rho_{|F_A=\phi, F_B=0}, \rho_{|F_A=\phi, F_B=0}^{\text{ideal}}) + p_{\phi 1}^{\text{real}} \Delta(\rho_{|F_A=\phi, F_B=1}, \rho_{|F_A=\phi, F_B=1}^{\text{ideal}}) \\
& \leq \Delta(|\perp\perp\rangle\langle\perp\perp|_{\phi 0} |_{K_A K_B F_A F_B} \otimes \rho_{LSE}^{\phi 0}, |\perp\perp\rangle\langle\perp\perp|_{\phi 0} |_{K_A K_B F_A F_B} \otimes \rho_{LSE}^{\phi 0}) + p_{\phi 1}^{\text{real}} \\
& = p_{\phi 1}^{\text{real}},
\end{aligned} \tag{19}$$

where we note that the trace distance in the third line is 0. A similar argument can be made for the second term for  $F_B = \phi$ , resulting in an upper bound of  $p_{1\phi}^{\text{real}}$ . The final term gives

$$\begin{aligned}
& \Delta(\rho_{\wedge (F_A, F_B) \in \{00, 10\}}, \rho_{\wedge (F_A, F_B) \in \{00, 10\}}^{\text{ideal}}) \\
& \leq \Delta(|\perp\perp\rangle\langle\perp\perp|_{00} |_{K_A K_B F_A F_B} \otimes \rho_{LSE}^{00}, |\perp\perp\rangle\langle\perp\perp|_{00} |_{K_A K_B F_A F_B} \otimes \rho_{LSE}^{00}) + p_{10}^{\text{real}} \\
& = p_{10}^{\text{real}}.
\end{aligned} \tag{20}$$

As such, the three trace distances are upper bounded by

$$\Pr[F_A = 1, F_B = 0] + \Pr[F_A = 1, F_B = \phi] + \Pr[F_A = \phi, F_B = 1] \leq \varepsilon_{\text{EA}}. \tag{21}$$

This accounts for the explicit entity authentication security condition contribution to the security.

The second security condition to extract is match security. To isolate its contribution, we need to first introduce an intermediate state  $\tilde{\rho}$ , for which the value of  $K_A$  when  $F_A = 1, F_B = 1$  is replaced by  $K_B$ , i.e.  $\tilde{\rho} = \mathcal{M}_{K_B \rightarrow K_A}(\rho)$ , where  $\mathcal{M}_{K_B \rightarrow K_A} = |11\rangle\langle 11|_{F_A F_B} \otimes (\sum_k |kk\rangle\langle kk|_{K_A K_B} \circ \text{Tr}_{K_A})$ . As such, we can apply the triangle inequality to expand

$$\begin{aligned}
& \Delta(\rho_{\wedge (F_A, F_B) \in \{01, 11\}}, \rho_{\wedge (F_A, F_B) \in \{01, 11\}}^{\text{ideal}}) \\
& \leq \Delta(\tilde{\rho}_{\wedge (F_A, F_B) \in \{01, 11\}}, \rho_{\wedge (F_A, F_B) \in \{01, 11\}}^{\text{ideal}}) + \Delta(\rho_{\wedge F_A=F_B=1}, \tilde{\rho}_{\wedge F_A=F_B=1}),
\end{aligned} \tag{22}$$

noting that  $\rho_{\wedge F_A=0, F_B=1}$  is identical to  $\tilde{\rho}_{\wedge F_A=0, F_B=1}$  since  $\mathcal{M}_{K_B \rightarrow K_A}$  does not alter the input state. We now focus on the latter term, where we can expand the trace distance

$$\begin{aligned}
& \Delta(\rho_{\wedge F_A=F_B=1}, \tilde{\rho}_{\wedge F_A=F_B=1}) \\
& = p_{11}^{\text{real}} \Delta\left(\sum_{k_A k_B} p_{k_A k_B | 11} |k_A k_B\rangle\langle k_A k_B|_{K_A K_B} \otimes \rho_{LSE}^{11, k_A k_B}, \sum_{k_A k_B} p_{k_A k_B | 11} |k_A k_A\rangle\langle k_A k_A|_{K_A K_B} \otimes \rho_{LSE}^{11, k_A k_B}\right) \\
& = \frac{p_{11}^{\text{real}}}{2} \left\| \sum_{k_A \neq k_B} p_{k_A k_B | 11} (|k_A k_B\rangle\langle k_A k_B|_{K_A K_B} - |k_B k_B\rangle\langle k_B k_B|_{K_A K_B}) \otimes \rho_{LSE}^{11, k_A k_B} \right\|_1 \\
& \leq \frac{p_{11}^{\text{real}}}{2} \sum_{k_A \neq k_B} p_{k_A k_B | 11} \left\| |k_A k_B\rangle\langle k_A k_B|_{K_A K_B} - |k_B k_B\rangle\langle k_B k_B|_{K_A K_B} \right\|_1 \left\| \rho_{LSE}^{11, k_A k_B} \right\|_1 \\
& = \Pr[K_A \neq K_B, F_A = 1, F_B = 1] \\
& \leq \varepsilon_{\text{MS}}.
\end{aligned} \tag{23}$$

This accounts for the contribution of match security.

The final term can be reduced to the key secrecy condition. We first note that when  $F_A = F_B = 1$ , whenever the key  $K_A$  is generated, it will be identical to  $K_B$  in both  $\tilde{\rho}$  and  $\rho^{\text{ideal}}$ . When  $F_A = 0, F_B = 1$  instead,  $K_A$  is simply  $\perp$ . As such, we can define a CPTP map to get a value of  $K_A$  based on  $F_A$  and  $K_B$ . Since CPTP maps cannot increase trace distance, we can remove the  $K_A$  subsystem from the trace distance. Expanding the final

term, we get

$$\begin{aligned}
& \Delta \left( \tilde{\rho}_{\wedge(F_A, F_B) \in \{01, 11\}}, \rho_{\wedge(F_A, F_B) \in \{01, 11\}}^{\text{ideal}} \right) \\
& \leq \Delta \left( \sum_{(f_A, f_B) \in \mathcal{S}'} p_{f_A f_B}^{\text{real}} |f_A f_B\rangle\langle f_A f_B| \otimes \rho_{K_B LSE}^{f_A f_B}, \sum_{(f_A, f_B) \in \mathcal{S}'} p_{f_A f_B}^{\text{real}} |f_A f_B\rangle\langle f_A f_B| \otimes \tau_{K_B} \otimes \rho_{LSE}^{f_A f_B} \right) \\
& = \Delta \left( \rho_{K_B F_A F_B LSE \wedge (F_A, F_B) \in \{01, 11\}}, \tau_{K_B} \otimes \rho_{K_B F_A F_B LSE \wedge (F_A, F_B) \in \{01, 11\}} \right) \\
& \leq \varepsilon_{KS}
\end{aligned} \tag{24}$$

where  $\mathcal{S}'$  refers to the set  $\{01, 11\}$ . Combining the results, we have that

$$\Delta(\rho, \rho^{\text{ideal}}) \leq \varepsilon_{EA} + \varepsilon_{MS} + \varepsilon_{KS}, \tag{25}$$

which we can use to define  $\varepsilon_{\text{sec}}$ .

In the case of the intermediate sessions, we can find an  $\rho_{K_A K_B F_A F_B LSE}^{\text{ideal, int}} \in \mathcal{S}'_{out}$  with the same probability distribution  $p_{F_A F_B}^{\text{ideal}}$ , but with  $\sigma_{LSE}^{f_A f_B} \in \mathcal{S}_{in}$ . We first note that if we choose an ideal state  $\rho^{\text{ideal, 1}}$  that is the same as  $\rho^{\text{ideal}}$  except that  $\rho_{LSE}^{\text{ideal, } f_A, f_B} = \frac{p_{f_A f_B}^{\text{real}}}{p_{f_A f_B}^{\text{real}} + p_{f'_A f'_B}^{\text{real}}} \rho_{LSE}^{f_A f_B} + \frac{p_{f'_A f'_B}^{\text{real}}}{p_{f_A f_B}^{\text{real}} + p_{f'_A f'_B}^{\text{real}}} \sigma_{LSE}^{f'_A f'_B}$  for  $(f_A, f_B, f'_A, f'_B) \in \{(\phi, 0, \phi, 1), (0, \phi, 1, \phi), (0, 0, 1, 0)\}$  and any  $\sigma_{LSE}^{f'_A f'_B} \in \mathcal{S}_{in}$ , the analysis above remains unchanged and by the triangle inequality,

$$\Delta(\rho, \rho^{\text{ideal, int}}) \leq \varepsilon_{EA} + \varepsilon_{MS} + \varepsilon_{KS} + \Delta(\rho^{\text{ideal, 1}}, \rho^{\text{ideal, int}}). \tag{26}$$

The trace distance can be expanded as

$$\begin{aligned}
& \Delta(\rho^{\text{ideal, 1}}, \rho^{\text{ideal, int}}) \\
& \leq \Delta \left( \sum_{(f_A, f_B) \notin \mathcal{S}_{SP}} p_{f_A f_B}^{\text{real}} \sigma_{K_A K_B}^{f_A f_B} \otimes \rho_{LSE}^{f_A f_B}, \sum_{(f_A, f_B) \notin \mathcal{S}_{SP}} p_{f_A f_B}^{\text{real}} \sigma_{K_A K_B}^{f_A f_B} \otimes \sigma_{LSE}^{f_A f_B} \right) \\
& \leq \Delta \left( \sum_{(f_A, f_B) \notin \mathcal{S}_{SP}} p_{f_A f_B}^{\text{real}} \rho_{LSE}^{f_A f_B}, \sum_{(f_A, f_B) \notin \mathcal{S}_{SP}} p_{f_A f_B}^{\text{real}} \sigma_{LSE}^{f_A f_B} \right) \\
& \leq \varepsilon_{SP},
\end{aligned} \tag{27}$$

where  $\sigma_{K_A K_B}^{f_A f_B}$  is the ideal form of the keys (either  $\perp$  or uniform) depending on  $f_A, f_B$ , and  $\sigma_{K_A K_B}^{f_A f_B}$  is identical in both  $\rho^{\text{ideal}}$  and  $\rho^{\text{ideal, int}}$ . The second inequality stems from reversing the CPTP map of selecting  $K_A K_B$  from  $F_A F_B$ , which is implicitly part of  $E$  since these values can be public in general. Combining the results, we get that

$$\Delta(\rho, \rho^{\text{ideal, int}}) \leq \varepsilon_{EA} + \varepsilon_{MS} + \varepsilon_{KS} + \varepsilon_{SP}, \tag{28}$$

which we can use to define  $\varepsilon_{\text{sec, int}}$ .  $\square$

### C.3 Single-Session Security Analysis

Since the protocol  $\mathcal{P}$  is a linear map, we can break the output state into components based on the input state, i.e.  $\rho^{\text{out, } jj'} = \mathcal{P}(\rho_{LSE}^{\text{in, } jj'})$ , and the examine their trace distances separately,

$$\Delta(\rho^{\text{out}}, \rho^{\text{ideal, int}}) \leq \sum_{jj'} p_{jj'} \Delta(\mathcal{P}(\rho^{\text{out, } jj'}), \rho^{\text{ideal, int, } jj'}). \tag{29}$$

As such, it is sufficient to analyse the single-session security for a single component,

$$\begin{aligned}
\Delta(\rho^{\text{out, } jj'}, \rho^{\text{ideal, int, } jj'}) & \leq \varepsilon_{\text{sec, int, } jj'} \\
\Delta(\rho^{\text{out, } jj'}, \rho^{\text{ideal, } jj'}) & \leq \varepsilon_{\text{sec, } jj'},
\end{aligned} \tag{30}$$

with overall security  $\varepsilon_{\text{sec}} = \max_{jj'} \varepsilon_{\text{sec, } jj'}$  and  $\varepsilon_{\text{sec, int}} = \max_{jj'} \varepsilon_{\text{sec, int, } jj'}$ . Furthermore, noting that there are restrictions of labels  $\beta$  and  $\beta'$  when the ideal input state has label  $\alpha$  and  $\alpha'$ , the ideal state for a single component

can be further restricted to states of the form

$$\begin{aligned}
\rho^{\text{ideal,int},jj'} = & |\perp\perp\rangle\langle\perp\perp|_{K_A K_B} \otimes \left[ |0\phi\rangle\langle 0\phi|_{F_A F_B} \otimes \sum_{\tilde{j} \geq j} p_{0\phi,\tilde{j}} \sigma_{LSE}^{0\phi,\tilde{j}+1,j'} + |\phi 0\rangle\langle \phi 0|_{F_A F_B} \otimes \sum_{\tilde{j}' \geq j'} p_{\phi 0,\tilde{j}'} \sigma_{LSE}^{\phi 0,\tilde{j}'+1} \right. \\
& + |00\rangle\langle 00|_{F_A F_B} \otimes \sum_{\tilde{j} \geq j, \tilde{j}' \geq j'} p_{00,\tilde{j}\tilde{j}'} \sigma_{LSE}^{00,\tilde{j}+1,\tilde{j}'+1} \left. + |01, \perp\rangle\langle 01, \perp|_{F_A F_B K_A} \otimes \tau_{K_B} \otimes \sum_{\tilde{j} \geq \max\{j, j'\}} p_{01,\tilde{j}} \sigma_{LSE}^{01,\tilde{j}+1,\tilde{j}} \right. \\
& \left. + |11\rangle\langle 11|_{F_A F_B} \otimes \tilde{\tau}_{K_A K_B} \otimes \sum_{\tilde{j} \geq \max\{j, j'\}} p_{11,\tilde{j}} \sigma_{LSE}^{11,\tilde{j}\tilde{j}}, \right.
\end{aligned} \tag{31}$$

where  $\sigma_{LSE}^{f_A f_B, jj'} \in \mathcal{S}_{in}$ ,  $\tilde{j}$  and  $\tilde{j}'$  indicates  $\beta = \tilde{j}$  and  $\beta' = \tilde{j}'$ , with the summation of  $\tilde{j}$  or  $\tilde{j}'$  stemming from the ability for an adversary to force Alice and Bob to adopt a larger index  $\beta$  and  $\beta'$  during the session by attacking the label agreement step. As such, when we perform the security analysis, we focus on a single component ideal input state and ideal output states with the form above.

The single-session security can be summarised as Thm. 3, which is restated below.

**Theorem 3.** *The QAKE protocol  $\mathcal{P}$  is secure with security parameters*

$$\begin{aligned}
\varepsilon_{EA} &= \varepsilon_{MAC,1} + 2^{-P_{\text{tol}}^{\text{sift}} [1+h_{\text{bin}}(f_{P_1})]+\log_2(P_{\text{tol}}^{\text{sift}}+1)} + \frac{1}{|\mathcal{T}_{BV}|} \\
\varepsilon_{MS} &= \varepsilon_{MAC,2} \\
\varepsilon_{KS} &= 2\sqrt{2\varepsilon_{\text{serf},1}} + \frac{1}{2} \times 2^{-\frac{1}{2}[H'-l_{K_B}]} + \varepsilon_{\mathcal{P}'}, \\
\varepsilon_{SP} &= \varepsilon'_{SP,01,11} + \varepsilon_{\mathcal{P}'},
\end{aligned}$$

where  $l_{K_B}$  is the length of  $K_B$ ,  $\varepsilon_{\text{serf},1}$  is a penalty term associated with the use of modified Serfling bound [12, 42] to estimate the single-photon bit error rate in  $P_2^{\text{sift}}$  from that of  $P_1^{\text{sift}}$ . The penalty associated with shifting to an idealised protocol  $\mathcal{P}'$  is

$$\begin{aligned}
\varepsilon_{\mathcal{P}'} &= 2(\varepsilon_{MAC,1} + \varepsilon_{MAC,2} + \varepsilon_{ds} + \varepsilon_{SO}) \\
\varepsilon_{SO} &= 2^{-P_{\text{tol}}^{\text{sift}}} + 2^{-N_{P_{2,1}}^{\text{sift}}} + 2^{-P_{\text{tol}}^{\text{sift}} h_{\text{bin}}(f_{P_1})+\log_2(P_{\text{tol}}^{\text{sift}}+1)},
\end{aligned}$$

the shared secrets privacy parameter for the idealised protocol when  $F_B = 1$  is

$$\begin{aligned}
\varepsilon'_{SP,01,11} &= 4\sqrt{2\varepsilon_{\text{serf},1}} + 2(\varepsilon_2 + \varepsilon_3) \\
&\quad + \varepsilon_{SP,MAC,1} + \varepsilon_{SP,MAC,2} \\
\varepsilon_{SP,MAC,1} &= \sqrt{(|\mathcal{T}_{AV}|\varepsilon_{MAC,1} - 1) + 2^{\log_2\left(\frac{2+\varepsilon_3}{\varepsilon_3|\mathcal{T}_{BV}|}\right)-H'}} \\
\varepsilon_{SP,MAC,2} &= \sqrt{(|\mathcal{T}_{BV}|\varepsilon_{MAC,2} - 1) + 2^{\log_2\left(\frac{2}{\varepsilon_2}+1\right)-H'}},
\end{aligned}$$

the smooth min-entropy term is

$$H' = N_{P_{2,1}}^{\text{tol}} [1 - h_{\text{bin}}(e'_{\text{ph,tol}})] - 2 - \log_2 |\mathcal{T}_{AV}| |\mathcal{T}_{BV}| - \text{leak}_{EC},$$

$\varepsilon_2$  and  $\varepsilon_3$  are parameters to optimise over,  $|\mathcal{T}_{AV}|$  and  $|\mathcal{T}_{BV}|$  are the size (dimension) of the respective tag,  $P_{\text{tol}}^{\text{sift}}$  is the minimum tolerated number of sifted rounds,  $\varepsilon_{ds}$  accounts for errors associated with decoy state analysis,  $N_{P_{2,1}}^{\text{tol}}$  is the minimum tolerated number of single-photon rounds in set  $P_2^{\text{sift}}$ , and  $e'_{\text{ph,tol}}$  is the maximum tolerated single-photon phase error rate in set  $P_2^{\text{sift}}$ , and  $\text{leak}_{EC}$  is the information leakage due to error correction.

*Sketch Proof.* To aid in the proof, we present a figure summarising the protocol in Fig. 5. Thm. 9 presents the proof of explicit entity authentication. When Alice is not involved,  $F_A = \phi$ , even with access to an oracle giving one message-tag pair for  $T_{AV}$ , the  $\varepsilon_{MAC,1}$ -almost 2-universal hash function ensures that  $F_B = 0$  since it is difficult for the adversary to find a second message-tag pair. On the other hand, when  $F_B = \phi$  or  $F_B = 0$ , no

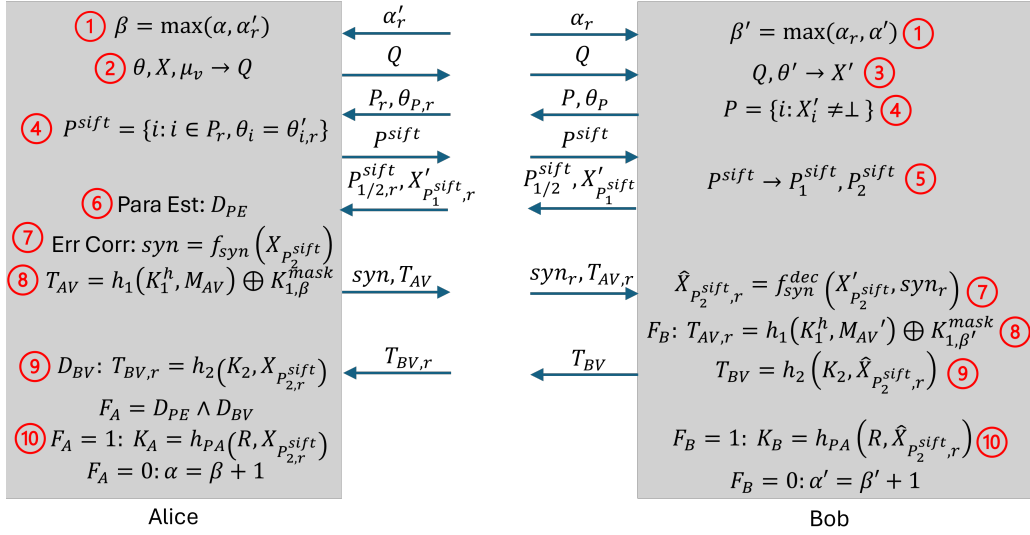


Figure 5: Summary of Protocol 1.  $M_{AV}$  labels the messages to be authenticated for which Alice hashes and  $M'_{AV}$  labels the corresponding messages hashed by Bob to authenticated these messages.

$T_{BV}$  is generated by Bob and thus by  $\epsilon_{MAC,2}$ -almost 2-universal property of  $h_2$ , Alice would not authenticate Bob,  $F_A = 0$ .

Thm. 10 bounds the match security parameter, which is identical to the correctness property of QKD. This is guaranteed by the error verification using hash function  $h_2$ .

The authentication steps guarantee not only entity authentication, but also message authentication. This ensures ideal features, such as: (1) labels match,  $\beta = \beta'$ , (2) step ordering is obeyed, (3) messages match, (4) tags unaltered. In Thm. 12, we show that we can convert the authentication checks into ideal checks for these features without much penalty. Furthermore, in Thm. 11, we also reduce the parameter estimation to an ideal parameter check. These modification reduces the analysis for key secrecy to a QKD analysis – where these ideal features occur, and we prove key secrecy in Thm. 13.

Finally, shared secrets privacy accounts for the fact that in the worst case when keys are not generated  $F_B \neq 1$ , either no secrets is leaked when authentication fails or at most  $T_{AV}$  is announced. Thm. 17 and Thm. 18 shows that this leads to an ideal output state in  $\mathcal{S}'_{out}$ . When keys are generated, i.e. parameter estimation passes, Thm. 19 shows that the min-entropy of  $X_{P_2^{sift}}$  ensures that authentication tags  $T_{AV}$  and  $T_{BV}$  leak minimal information on the authentication and masking key, while the strong extractor property for key generation ensures the privacy amplification key  $R$  is kept secret.  $\square$

We note that while the overall security parameters  $\epsilon_{sec}$  and  $\epsilon_{sec,int}$  can be determined by a sum of the respective security parameters, the bound may be tightened due to overlapping considerations for different security conditions.

### C.3.1 Explicit Entity Authentication

Here, we consider the first security condition of explicit entity authentication, which consists of Alice's full explicit entity authentication and Bob's almost-full explicit entity authentication. We note that the events of  $F_A = \phi$ ,  $F_B = \phi$  and  $F_A, F_B \neq \phi$  are mutually exclusive and the adversary is assumed to select one attack at the start of the protocol.

**Theorem 9.** Consider the QAKE protocol  $\mathcal{P}$ , the full explicit entity authentication security parameter is

$$\epsilon_{EA,f} = \frac{\Pr[F_B \neq 1]}{|\mathcal{T}_{BV}|}.$$

and the almost-full explicit entity authentication security parameter is

$$\epsilon_{EA,af} = \Pr[F_A = \phi](\epsilon_{MAC,1} + 2^{-P_{tol}^{sift}[1+h_{bin}(f_{P_1})]+\log_2(P_{tol}^{sift}+1)}).$$

*Proof.* We begin with the case of full explicit entity authentication, which we recall bounds the probability of events  $(F_A, F_B) \in \{10, 1\phi\}$ . To obtain  $F_A = 1$ , Alice needs to at least successfully validate Bob by checking if  $\tilde{T}_{BV} = T_{BV,r}$ , i.e.  $\Pr[F_A = 1|F_B = \phi] \leq \Pr[\tilde{T}_{BV} = T_{BV,r}|F_B = \phi]$ . Since  $K_2$  remains private from the adversary without Bob sending  $T_{BV}$ , we can use the uniformity of the strong 2-universal hash function to have

$$\Pr[F_A = 1|F_B = \phi] \leq \Pr[h_2(K_2, M) = T_{BV,r}] = \frac{1}{|\mathcal{T}_{BV}|} \quad (32)$$

for any  $T_{BV,r}$ . A similar argument holds when conditioned on  $F_B = 0$  since a random string is sent in place of a valid tag. As such, full explicit entity authentication security parameter is  $\varepsilon_{EA,f} = \frac{\Pr[F_B \neq 1]}{|\mathcal{T}_{BV}|}$ .

For the case of almost-full explicit entity authentication, Alice does not participate in the protocol,  $F_A = \phi$ . When  $\alpha > \beta'$ , the adversary may have partial information on  $(K_1^h, K_{1,\beta'}^{\text{mask}})$  from a previous session via a tag generated with a chosen message input  $M$ . As such, the two events that can lead to  $F_B = 1$ , or successful validation  $\tilde{T}_{AV} = T_{AV,r}$ , are either: (1) message  $M$  generating the tag matches the message  $M'_{AV}$  in the current session, or (2) guessing the correct  $T_{AV,r}$  to send to Bob for a mismatch message,  $M \neq M'_{AV}$ . As such, we can bound

$$\begin{aligned} \Pr[F_B = 1|F_A = \phi] &\leq \Pr[h_1(K_1^h, M'_{AV}) \oplus K_{1,\beta'}^{\text{mask}} = T_{AV,r} | h_1(K_1^h, M) \oplus K_{1,\beta'}^{\text{mask}} = T_{AV}, M \neq M'_{AV}] + p_{\text{guess}}(M'_{AV}) \\ &\leq \varepsilon_{\text{MAC},1} + 2^{-P_{\text{tol}}^{\text{sift}}[1+h_{\text{bin}}(f_{P_1})]+\log_2(P_{\text{tol}}^{\text{sift}}+1)}, \end{aligned} \quad (33)$$

where the  $\varepsilon_{\text{MAC},1}$ -almost strong 2-universal hash function guarantees that the adversary cannot successfully guess a second message-tag pair with probability higher than  $\varepsilon_{\text{MAC},1}$  and the guessing of  $M'_{AV}$  for  $F_A = \phi$  reduces to the ability to guess  $\theta'_P$  and  $P_1^{\text{sift}}$ . As such, the almost-full explicit entity authentication security parameter is  $\varepsilon_{EA,af} = \Pr[F_A = \phi](\varepsilon_{\text{MAC},1} + 2^{-P_{\text{tol}}^{\text{sift}}[1+h_{\text{bin}}(f_{P_1})]+\log_2(P_{\text{tol}}^{\text{sift}}+1)})$ .  $\square$

### C.3.2 Match Security

The match security condition is similar to the correctness condition of QKD, and the security guarantee can be provided during Bob validation, where the string  $X_{P_{2,r}^{\text{sift}}}$  and  $\hat{X}_{P_{2,r}^{\text{sift}}}$  are matched via a hash.

**Theorem 10.** *Consider the QAKE protocol  $\mathcal{P}$ , the match security parameter is*

$$\varepsilon_{\text{MS}} = \varepsilon_{\text{MAC},2}.$$

*Proof.* Since the keys generated  $K_A = h_{\text{PA}}(R, X_{P_{2,r}^{\text{sift}}})$  and  $K_B = h_{\text{PA}}(R, \hat{X}_{P_{2,r}^{\text{sift}}})$  with the same privacy amplification seed  $R$  would match when  $X_{P_{2,r}^{\text{sift}}} = \hat{X}_{P_{2,r}^{\text{sift}}}$ , i.e.  $\{X_{P_{2,r}^{\text{sift}}} = \hat{X}_{P_{2,r}^{\text{sift}}}\} \implies \{K_A = K_B\}$ , the converse gives

$$\Pr[K_A \neq K_B, F_A = F_B = 1] \leq \Pr[X_{P_{2,r}^{\text{sift}}} \neq \hat{X}_{P_{2,r}^{\text{sift}}}, F_A = F_B = 1]. \quad (34)$$

The event  $F_A = 1$  contains the event  $\tilde{T}_{BV} = T_{BV,r}$  (part of  $D_{BV} = 1$ ), allowing us to upper bound by

$$\Pr[h_2(K_2, X_{P_{2,r}^{\text{sift}}}) = T_{BV,r} | X_{P_{2,r}^{\text{sift}}} \neq \hat{X}_{P_{2,r}^{\text{sift}}}, h_2(K_2, \hat{X}_{P_{2,r}^{\text{sift}}}) = T_{BV}], \quad (35)$$

which describes the probability that an adversary can provide a valid tag to a message when given the tag to a different message. Since  $K_2$  is private from the adversary, by the  $\varepsilon_{\text{MAC},2}$ -almost strong 2-universal property of the hash,  $\Pr[K_A \neq K_B, F_A = F_B = 1] \leq \varepsilon_{\text{MAC},2}$ .  $\square$

### C.3.3 Idealised Parameter Estimation

To simplify analysis, we introduced an “idealised” version of parameter estimation related to the decoy state analysis. We define an idealised version of the the check  $D_{\text{PE}}$  as

$$\tilde{D}_{\text{PE}} = \begin{cases} 1 & \begin{aligned} &N_{P_{2,r}^{\text{sift}},1} \geq N_{P_{2,r}^{\text{sift}},1}^{\text{tol}}, N_{P_{1,r}^{\text{sift}},1} \geq N_{P_{1,r}^{\text{sift}},1}^{\text{tol}}, D_{\text{PE}}=1 \\ &\frac{wt(X_{P_{1,r}^{\text{sift}},1} \oplus X'_{P_{1,r}^{\text{sift}},1} | \{P_{1,r}^{\text{sift}},1\})}{N_{P_{1,r}^{\text{sift}},1}} \leq e_{\text{bit},1,\text{tol}} \end{aligned} \\ 0 & \text{otherwise} \end{cases}, \quad (36)$$

where  $X'_{P_{1,r}^{\text{sift}}}$  refers to the bit values of the bitstring  $X'_{P_{1,r}^{\text{sift}}}$  at indices where  $i \in P_{1,r}^{\text{sift}}$ , and a single photon is sent, and  $wt(S)$  gives the Hamming weight of a string  $S$ , i.e. the final condition means the actual single photon events in  $P_{1,r}^{\text{sift}}$  gives a bit error value upper bounded by  $e_{\text{bit},1,\text{tol}}$ . Here, we added the three desired conditions (actual single-photon detection/error fall within the bounds).

**Theorem 11.** *Let  $\mathcal{P}''$  be the protocol when  $D_{\text{PE}}$  is replaced with  $\tilde{D}_{\text{PE}}$ . Then, for any  $\sigma_{\text{LSE}} \in \mathcal{S}_{\text{in}}$ ,*

$$\Delta(\mathcal{P}(\sigma_{\text{LSE}}), \mathcal{P}''(\sigma_{\text{LSE}})) \leq 2\varepsilon_{\text{ds}},$$

where  $\varepsilon_{\text{ds}}$  accounts for errors associated with decoy state analysis.

*Proof.* The replacement of  $D_{\text{PE}}$  with  $\tilde{D}_{\text{PE}}$  would result in a difference only when  $D_{\text{PE}} = 1$  but  $\tilde{D}_{\text{PE}} = 0$ . The probability of this event is tied to decoy state analysis. From decoy state analysis [24], the single-photon quantities of interest can always be bounded by

$$\begin{aligned} N_{P_i^{\text{sift}},1} &\geq \frac{p_1\mu_0}{(\mu_1 - \mu_2)(\mu_0 - \mu_1 - \mu_2)} \times \left[ \frac{e^{\mu_1}}{p_{\mu_1}} \left( 1 - \frac{\mu_2(\mu_1 + \mu_2)}{\mu_0^2} \right) \mathbb{E}[N_{P_i^{\text{sift}},\mu_1}] - \frac{(\mu_1^2 - \mu_2^2)e^{\mu_0}}{\mu_0^2 p_{\mu_0}} \mathbb{E}[N_{P_i^{\text{sift}},\mu_0}] \right. \\ &\quad \left. - \frac{e^{\mu_2}}{p_{\mu_2}} \left( 1 - \frac{\mu_1(\mu_1 + \mu_2)}{\mu_0^2} \right) \mathbb{E}[N_{P_i^{\text{sift}},\mu_2}] \right] \\ \mathcal{E}_{P_1^{\text{sift}},1} &\leq \frac{p_1}{\mu_1 - \mu_2} \left( \frac{e^{\mu_1}}{p_{\mu_1}} \mathbb{E}[N_{\mathcal{E},P_1^{\text{sift}},\mu_1}] - \frac{e^{\mu_2}}{p_{\mu_2}} \mathbb{E}[N_{\mathcal{E},P_1^{\text{sift}},\mu_2}] \right), \end{aligned}$$

where  $\mathcal{E}_{P_1^{\text{sift}},1}$  is the number of error bits in the single photon events in set  $P_1^{\text{sift}}$ , and  $p_1$  is the probability of single-photon signals sent by the source. The estimated quantities  $\hat{N}_{P_i^{\text{sift}},1}^{\text{LB}}$  and  $\hat{e}_{\text{bit},P_i^{\text{sift}},1}^{\text{UB}}$  can be computed similarly from the above bounds, but utilises appropriate bounds on the expectation values  $\mathbb{E}[N_{P_i^{\text{sift}},\mu_j}]$  and  $\mathbb{E}[N_{\mathcal{E},P_i^{\text{sift}},\mu_j}]$  derived from the values observed during the protocol. For instance,  $\hat{N}_{P_i^{\text{sift}},1}^{\text{LB}}$  utilises the estimated lower bound  $\mathbb{E}[N_{P_i^{\text{sift}},\mu_1}^{\text{LB}}]$  instead of  $\mathbb{E}[N_{P_i^{\text{sift}},\mu_1}]$  (which it does not have access to), estimated using concentration bounds (we use Kato's inequality [11, 19] as the concentration bound) from the observed  $N_{P_i^{\text{sift}},\mu_1}$  value. The probability of the estimated lower bound  $\mathbb{E}[N_{P_i^{\text{sift}},\mu_1}^{\text{LB}}]$  exceeding the true expectation value  $\mathbb{E}[N_{P_i^{\text{sift}},\mu_1}]$  is quantified by  $\varepsilon_{N_{P_i^{\text{sift}},\mu_1}}$ . As such, when these concentration bounds are respected, we have that  $N_{P_i^{\text{sift}},1} \geq \hat{N}_{P_i^{\text{sift}},1}^{\text{LB}}$ , which implies that the probability that  $N_{P_i^{\text{sift}},1} < N_{P_i^{\text{sift}},1}^{\text{tol}}$  while  $\hat{N}_{P_i^{\text{sift}},1}^{\text{LB}} \geq N_{P_i^{\text{sift}},1}^{\text{tol}}$  is bounded by the events where the concentration bounds are violated. As such, the probability of  $D_{\text{PE}} = 1$  but  $\tilde{D}_{\text{PE}} = 0$  is the sum of all such concentration bound violation events and is labelled  $\varepsilon_{\text{ds}}$ . Therefore, the trace distance on the output states gains a  $2\varepsilon_{\text{ds}}$  penalty when we replace the decision  $D_{\text{PE}}$  with its idealised version  $\tilde{D}_{\text{PE}}$ .  $\square$

Applying Thm. 11 replaces the parameter check with an ideal check of the single qubit parameters. As such, the later analysis also applies to a QAKE protocol where single-qubit BB84 states are prepared and single qubit bit error and number of rounds can be observed directly.

### C.3.4 Idealised Authentication

The validation steps in the protocol also serve as message authentication steps. To further simplify the analysis, we introduce an “idealised” version of message authentication checks, replacing the authentication decisions  $F_{\text{B}}$  and  $D_{\text{BV}}$  with idealised versions. The purposes of authentication checks are twofold; They serve to ensure that the message transmitted between Alice and Bob match, and that the order of the communication steps are obeyed. As such, when we define the idealised authentication checks, these are the conditions that we impose. Crucially, there are several events that we desire in an ideal check which are provided with high probability:

1. Matching label agreement,  $\beta = \beta'$ , is desirable to ensure the label agreement step is obeyed. Its security is provided by the fact that the masking key  $K_{1,\beta}^{\text{mask}}$  choice is label-dependent, and mismatching masking key would lead to failed authentication.
2. Parameter estimation passing,  $D_{\text{PE}} = 1$ , is meant to indicate to Bob that parameter estimation has passed. Its security is guaranteed by Alice's decision to not send a valid  $T_{\text{AV}}$  when  $D_{\text{PE}} = 0$ .

3. Alice's tag generation occurs before Alice's tag is validated, which indicates the ordering of Alice's Validation step is obeyed, i.e. the event  $\Omega_{5 \rightarrow 6}$ , where  $\Omega_{i \rightarrow j}$  labels that the  $i$ -th step occur before the  $j$ -th step. Note here that the steps refers a set of action by either Alice or Bob, receiving an input and providing and output from the communication channel. For QAKE, there are a total of seven steps.
4. Matching message,  $M_{AV} = M'_{AV}$ , where  $M_{AV} = (X_{P_{2,r}^{\text{sift}}}, P_r, \theta'_{P_r}, P^{\text{sift}}, X'_{P_1^{\text{sift},r}}, P_{1,r}^{\text{sift}}, P_{2,r}^{\text{sift}}, \text{syn})$  and  $M'_{AV} = (\hat{X}_{P_{2,r}^{\text{sift}}}, P, \theta'_P, P_r^{\text{sift}}, X'_{P_1^{\text{sift}}}, P_1^{\text{sift}}, P_2^{\text{sift}}, \text{syn}_r)$ , which also contains the error verification check ( $X_{P_{2,r}^{\text{sift}}} = \hat{X}_{P_{2,r}^{\text{sift}}}$ ).
5. Tags unaltered,  $T_{AV} = T_{AV,r}$ .
6. Protocol steps before Alice's validation are obeyed, namely the event  $\{\Omega_{i \rightarrow i+1}\}_{i \in [2,4]}$ . We note that the first step, Alice's state preparation, would WLOG occur before step 2 (Bob responding with  $P$  and basis  $\theta_P$ )<sup>11</sup>.

As such, we label a replacement decision  $\tilde{F}_B$ , which is made at the same time as  $F_B$ , but with separate checks<sup>12</sup>. For validation of Alice, this replacement made is

$$\tilde{F}_B = \begin{cases} 1 & \beta = \beta', D_{PE}=1, T_{AV}=T_{AV,r}, \\ & M_{AV}=M'_{AV}, \Omega_{2 \rightarrow 3 \rightarrow 4 \rightarrow 5 \rightarrow 6}, \\ 0 & \text{otherwise} \end{cases}, \quad (37)$$

where  $\Omega_{2 \rightarrow 3 \rightarrow 4 \rightarrow 5 \rightarrow 6}$  is the event where the step ordering is  $2 \rightarrow 3 \rightarrow 4 \rightarrow 5 \rightarrow 6$ . The list of steps are:

1. Alice's state preparation and sending of quantum state.
2. Bob's measurement and reply of  $P$  and  $\theta'_P$ .
3. Alice's sifting and response  $P^{\text{sift}}$ .
4. Bob's choice of test round and announcement of  $P_1^{\text{sift}}$ ,  $P_2^{\text{sift}}$  and  $X'_{P_1^{\text{sift}}}$ .
5. Alice's parameter estimation and validation tag generation, sending syndrome  $\text{syn}$  and tag  $T_{AV}$  to Bob.
6. Bob performs Alice's validation, and responds with his own validation tag  $T_{BV}$ .
7. Alice validates Bob's tag.

The replacement of  $D_{BV}$  is simpler, with

$$\tilde{D}_{BV} = \begin{cases} 1 & \tilde{F}_B = 1, T_{BV} = T_{BV,r}, \Omega_{6 \rightarrow 7}, \\ 0 & \text{otherwise} \end{cases}, \quad (38)$$

where  $\Omega_{6 \rightarrow 7}$  indicates that Bob sends  $T_{BV}$  before Alice is requested to verify, and  $\tilde{F}_A := \tilde{D}_{BV} \wedge D_{PE}$ .

**Theorem 12.** *Let  $\mathcal{P}$  be the protocol and  $\mathcal{P}'$  be the idealised protocol (with  $D_{PE}$ ,  $F_B$ ,  $D_{BV}$  replaced with  $\tilde{D}_{PE}$ ,  $\tilde{F}_B$  and  $\tilde{D}_{BV}$ ). Then, for any  $\sigma_{LSE} \in \mathcal{S}_{in}$ ,*

$$\Delta(\mathcal{P}(\sigma_{LSE}), \mathcal{P}'(\sigma_{LSE})) \leq 2(\varepsilon_{\text{MAC},1} + \varepsilon_{\text{SO}}) + 2\varepsilon_{\text{MAC},2} + 2\varepsilon_{\text{ds}},$$

where  $\varepsilon_{\text{SO}} = 2^{-P_{\text{tol}}^{\text{sift}}} + 2^{-N_{P_{2,1}^{\text{sift}}}^{\text{tol}}} + 2^{-P_{\text{tol}}^{\text{sift}} h_{\text{bin}}(f_{P_1}) + \log_2(P_{\text{tol}}^{\text{sift}} + 1)}$ .

*Proof.* From Thm. 11, the switch to  $\tilde{D}_{PE}$  introduces a  $2\varepsilon_{\text{ds}}$  penalty. As such, we can consider only the changes in  $F_B$  and  $D_{BV}$ , and combine the results using triangle inequality at the end.

<sup>11</sup>If the state preparation occurs after step 2, the state is always equivalent to one where the state preparation occurs before step 2 but with the adversary not interacting with the quantum state sent by Alice prior to step 2. This is because the state preparation does not require any input from the channel.

<sup>12</sup>The checks can be considered to be performed by a hypothetical third-party, though such a party need not be physically present in the protocol.

For the switch from  $F_B$  to  $\tilde{F}_B$  for scenarios where  $(K_1^h, K_{1,\beta'}^{\text{mask}})$  is private (where  $\beta' \geq \alpha$ ), the replacement results in a penalty of  $2\Pr[F_B = 1, \tilde{F}_B = 0]$ . This probability can be computed,

$$\begin{aligned}
& \Pr[F_B = 1, \tilde{F}_B = 0] \\
& \leq \Pr[F_B = 1, (\Omega_{5 \rightarrow 6}^c \vee D_{\text{PE}} = 0)] + \Pr[F_B, D_{\text{PE}} = 1, \Omega_{5 \rightarrow 6}, \beta \neq \beta'] \\
& \quad + \Pr[F_B, D_{\text{PE}} = 1, \Omega_{5 \rightarrow 6}, \beta = \beta', M_{\text{AV}} \neq M'_{\text{AV}}] \\
& \quad + \Pr[F_B, D_{\text{PE}} = 1, \Omega_{5 \rightarrow 6}, \beta = \beta', M_{\text{AV}} = M'_{\text{AV}}, T_{\text{AV}} \neq T_{\text{AV},r}] \\
& \quad + \Pr[F_B, D_{\text{PE}} = 1, \Omega_{5 \rightarrow 6}, \beta = \beta', M_{\text{AV}} = M'_{\text{AV}}, T_{\text{AV}} = T_{\text{AV},r}, \Omega_{1 \rightarrow 2 \rightarrow 3 \rightarrow 4}^c] \\
& \leq \frac{\Pr[\Omega_{5 \rightarrow 6}^c \vee D_{\text{PE}} = 0]}{|\mathcal{T}_{\text{AV}}|} + \frac{\Pr[D_{\text{PE}} = 1, \Omega_{5 \rightarrow 6}, \beta \neq \beta']}{|\mathcal{T}_{\text{AV}}|} + \Pr[D_{\text{PE}} = 1, \Omega_{5 \rightarrow 6}, \beta = \beta', M_{\text{AV}} \neq M'_{\text{AV}}] \varepsilon_{\text{MAC},1} \\
& \quad + \Pr[M_{\text{AV}} = M'_{\text{AV}}, \Omega_{2 \rightarrow 3}^c] + \Pr[M_{\text{AV}} = M'_{\text{AV}}, \Omega_{2 \rightarrow 3}, \Omega_{3 \rightarrow 4}^c] + \Pr[M_{\text{AV}} = M'_{\text{AV}}, \Omega_{2 \rightarrow 3 \rightarrow 4}, \Omega_{4 \rightarrow 5}^c] \\
& \leq \varepsilon_{\text{MAC},1} + p_{\text{guess}}(\theta'_P) + p_{\text{guess}}(\theta_P) + p_{\text{guess}}(P_1^{\text{sift}}),
\end{aligned} \tag{39}$$

where  $p_{\text{guess}}(Z)$  is the probability of the adversary guessing the parameter  $Z$  successfully before  $Z$  is announced. The first inequality splits the “bad events” into different cases. The second inequality uses the fact that when  $\Omega_{5 \rightarrow 6}^c$  or  $D_{\text{PE}} = 0$ , no valid tag is generated before Bob checks Alice’s authentication tag. Therefore, by the property of the strong 2-universal hash function, the probability of  $F_B = 1$  is no better than a random guess of the tag. When  $\beta \neq \beta'$ , since authentication key  $K_{1,\beta}$  is random and uncorrelated to  $K_{1,\beta'}$ , the adversary can do no better than make a random guess of the tag, which results in a  $\frac{1}{|\mathcal{T}_{\text{AV}}|}$  penalty. As for message mismatch, the property of strong 2-universal hash function ensures that the probability of generating a correct tag for  $M'_{\text{AV}}$  is bounded by  $\varepsilon_{\text{MAC},1}$ . The final inequality combines the first three terms to upper bound it by  $\varepsilon_{\text{MAC},1}$ , while events  $\Omega_{i \rightarrow j}^c$  with matching messages indicate that the adversary made a correct guess of the message sent in step  $i$ , which we label  $p_{\text{guess}}(Z)$  for message  $Z$ . For step 2 (Bob response after quantum state measurement), the adversary has to guess  $\theta'_P$ , while for step 3, this quantity is  $\theta_P$  (equivalent to guessing  $P^{\text{sift}}$  with knowledge of  $\theta'_P$  from step 2), and in step 4, the quantity is the choice of test round  $P_1^{\text{sift}}$  from  $P^{\text{sift}}$ .

We can bound the guessing probability explicitly. The guessing probability of  $\theta'_P$  is  $2^{-|P|} \leq 2^{-P_{\text{tol}}^{\text{sift}}}$  since the basis are randomly chosen, and  $|P| \leq P_{\text{tol}}^{\text{sift}}$ . The probability of guessing  $\theta_P$  can be bounded by the probability of guessing Alice’s basis choice for the  $N_{P_1^{\text{sift}}}^{\text{tol}}$  single-photon rounds, where the quantum state cannot provide any information on the basis. Finally, the probability of guessing the test round choice is [10]

$$\left( \frac{|P^{\text{sift}}|}{f_{P_1^{\text{sift}}} |P^{\text{sift}}|} \right)^{-1} \leq 2^{-|P^{\text{sift}}| h_{\text{bin}}(f_{P_1^{\text{sift}}}) + \log_2(|P^{\text{sift}}| + 1)} \leq 2^{-P_{\text{tol}}^{\text{sift}} h_{\text{bin}}(f_{P_1}) + \log_2(P_{\text{tol}}^{\text{sift}} + 1)}, \tag{40}$$

where we drop the ceiling function ( $\lceil \cdot \rceil$ ) for simplicity and note that the second term is decreasing in  $|P|$  for any chosen number of test rounds (at least 1 test and key round). The overall penalty to satisfy step order can be summarised as  $\varepsilon_{\text{SO}} = 2^{-P_{\text{tol}}^{\text{sift}}} + 2^{-N_{P_1^{\text{sift}}}^{\text{tol}}} + 2^{-P_{\text{tol}}^{\text{sift}} h_{\text{bin}}(f_{P_1}) + \log_2(P_{\text{tol}}^{\text{sift}} + 1)}$ .

To make the same switch for cases when  $(K_1^h, K_{1,\beta'}^{\text{mask}})$  is accessible via a single oracle access  $(\mathcal{E}_{K_1^h, K_{1,\beta'}^{\text{mask}} E_i \rightarrow E_{i+1}})$ , we first note that such cases require  $\beta' < \alpha$  and by extension  $\beta' < \beta$ , i.e.  $\tilde{F}_B$  should always return 0 since  $\beta$  and  $\beta'$  are mismatched. We first note that  $T_{\text{AV}}$  generated with private  $K_{1,\beta}^{\text{mask}}$  provides no advantage to the adversary in passing  $F_B$ . As such, we can follow the argument in Thm. 9 to show that the probability of  $F_B = 1$  is upper bounded by the probability of  $F_B = 1$  when  $F_A = \phi$ . Combining both results, we can thus replace  $F_B$  by  $\tilde{F}_B$  in general in this protocol with a penalty of  $2(\varepsilon_{\text{MAC},1} + \varepsilon_{\text{SO}})$ .

By similar arguments, the replacement of  $D_{\text{BV}}$  to  $\tilde{D}_{\text{BV}}$ , which involves mainly Bob’s validation step, yields an error of up to  $\varepsilon_{\text{MAC},2}$ . As such, these changes result in a penalty to the trace distance of  $2\varepsilon_{\text{MAC},2}$ .  $\square$

### C.3.5 Key Secrecy

Key secrecy analyses the two specific cases where Bob generates a key,  $(F_A, F_B) \in \{01, 11\}$ . Intuitively, since the protocol is similar to decoy-state BB84 with modifications only in its authentication steps, the key secrecy security condition relies heavily on the secrecy condition of BB84. We can summarise the result as a theorem,

**Theorem 13.** *Consider the QAKE protocol  $\mathcal{P}$ . Then, the key secrecy security parameter is*

$$\varepsilon_{\text{KS}} = \varepsilon'_{\text{KS}} + 2(\varepsilon_{\text{ds}} + \varepsilon_{\text{MAC},1} + \varepsilon_{\text{SO}} + \varepsilon_{\text{MAC},2})$$

where

$$\varepsilon'_{\text{KS}} = 2\sqrt{2\varepsilon_{\text{serf},1}} + \frac{1}{2} \times 2^{-\frac{1}{2}[N_{P_2,1}^{\text{tol}} - N_{P_2,1}^{\text{tol}} h_{\text{bin}}(e'_{\text{ph,tol}}) - 2 - \log_2 |\mathcal{T}_{\text{AV}}| |\mathcal{T}_{\text{BV}}| - \text{leak}_{\text{EC}} - l_{K_B}]}$$

is the key secrecy of the idealised protocol  $\mathcal{P}'$ .

*Proof.* We begin by performing a swap to an “idealised” version of the protocol  $\mathcal{P}'$  by replacing  $F_B$ ,  $D_{\text{BV}}$  and  $D_{\text{PE}}$ . By Thm. 12, this gives

$$\begin{aligned} \Delta(\rho_{F_A F_B K_B LSE \wedge (F_A, F_B) \in \{01, 11\}}^{\text{out}, jj'}, \tau_{K_B} \otimes \rho_{F_A F_B LSE \wedge (F_A, F_B) \in \{01, 11\}}^{\text{out}, jj'}) \\ \leq \Delta(\rho_{\tilde{F}_A \tilde{F}_B K_B LSE \wedge (\tilde{F}_A, \tilde{F}_B) \in \{01, 11\}}^{\text{out}, jj'}, \tau_{K_B} \otimes \rho_{\tilde{F}_A \tilde{F}_B LSE \wedge (\tilde{F}_A, \tilde{F}_B) \in \{01, 11\}}^{\text{out}, jj'}) \\ + 2(\varepsilon_{\text{ds}} + \varepsilon_{\text{MAC},1} + \varepsilon_{\text{SO}} + \varepsilon_{\text{MAC},2}), \quad (41) \end{aligned}$$

where  $\rho'$  label the output state when an idealised version of the protocol is utilised. We first combine 01 and 11 cases into a single one by arguing that the trace distance is independent of the final communication step using Thm. 14. This is followed by analysing the trace distance shown in Thm. 15. Combining the results, we obtain the security parameter stated in the theorem.  $\square$

To simplify the analysis, we combine the cases of  $(\tilde{F}_A, \tilde{F}_B)$  being 01 and 11 into a single condition on  $\tilde{F}_B = 1$  since only the key  $K_B$  is of interest.

**Theorem 14.** *Consider the QAKE protocol  $\mathcal{P}'$ . Then, we have*

$$\Delta(\rho_{\tilde{F}_A \tilde{F}_B K_B LSE \wedge (\tilde{F}_A, \tilde{F}_B) \in \{01, 11\}}^{\text{out}, jj'}, \tau_{K_B} \otimes \rho_{\tilde{F}_A \tilde{F}_B LSE \wedge (\tilde{F}_A, \tilde{F}_B) \in \{01, 11\}}^{\text{out}, jj'}) \leq \Delta(\rho_{K_B L'S'E \wedge \tilde{F}_B=1}^{\text{out}, jj'}, \tau_{K_B} \otimes \rho_{L'S'E \wedge \tilde{F}_B=1}^{\text{out}, jj'}),$$

where the states on RHS has subsystems  $L'S'$ , indicating the labels and secrets correspond to that when the final step of Alice has been removed.

*Proof.* We first note that since  $\tilde{F}_B = 1$ , we have  $\tilde{D}_{\text{PE}} = 1$  and the decision of  $\tilde{F}_A$  depends solely on  $\tilde{D}_{\text{BV}}$  generated in the final step. Moreover, since  $T_{\text{BV}} \neq \perp$ , the  $\tilde{F}_A$  condition depends solely on  $T_{\text{BV}} = T_{\text{BV},r}$ , i.e. whether the adversary altered  $T_{\text{BV}}$  transmission from Bob to Alice. As such, the final step can be re-expressed as a CPTP map that maps  $T_{\text{BV}}$  and  $T_{\text{BV},r}$  (part of  $E$ ) to  $\tilde{F}_A$  followed by generating secret  $S$  from  $S'$ . Since CPTP maps cannot increase trace distance, we can reverse the map (i.e. reversing Alice’s decision step and subsequent index update, which WLOG is the final step of the protocol), yielding

$$\Delta(\rho_{F_A F_B K_B LSE \wedge (\tilde{F}_A, \tilde{F}_B) \in \{01, 11\}}^{\text{out}, jj'}, \tau_{K_B} \otimes \rho_{\tilde{F}_A \tilde{F}_B LSE \wedge (\tilde{F}_A, \tilde{F}_B) \in \{01, 11\}}^{\text{out}, jj'}) \leq \Delta(\rho_{K_B L'S'E \wedge \tilde{F}_B=1}^{\text{out}, jj'}, \tau_{K_B} \otimes \rho_{L'S'E \wedge \tilde{F}_B=1}^{\text{out}, jj'}), \quad (42)$$

where the  $L'S'E$  indicates that the state of the subsystem before Alice’s final protocol step. This aligns with our understanding that  $\tilde{F}_A$  outcome has no impact on the privacy of  $K_B$  since it does not reveal additional information.  $\square$

With the simplification, we proceed to prove the key secrecy security parameter for the QAKE protocol with idealised parameter estimation and authentication checks,

**Theorem 15.** *Consider the QAKE protocol  $\mathcal{P}'$ . Then, we have that*

$$\Delta(\rho_{K_B L'S'E \wedge \tilde{F}_B=1}^{\text{out}, jj'}, \tau_{K_B} \otimes \rho_{L'S'E \wedge \tilde{F}_B=1}^{\text{out}, jj'}) \leq 2\sqrt{2\varepsilon_{\text{serf},1}} + \frac{1}{2} \times 2^{-\frac{1}{2}[N_{P_2,1}^{\text{tol}} - N_{P_2,1}^{\text{tol}} h_{\text{bin}}(e'_{\text{ph,tol}}) - 2 - \log_2 |\mathcal{T}_{\text{AV}}| |\mathcal{T}_{\text{BV}}| - \text{leak}_{\text{EC}} - l_{K_B}]},$$

where  $e'_{\text{ph,tol}}$  is the error tolerance inclusive of the correction due to Serfling bound.

*Proof.* Let  $\tilde{\Omega}_{\text{PE}}$  be the event where parameter estimation checks  $N_{P_1^{\text{sift}},1} \geq N_{P_1^{\text{sift}},1}^{\text{tol}}$ ,  $N_{P_2^{\text{sift}},1} \geq N_{P_2^{\text{sift}},1}^{\text{tol}}$ ,  $\frac{wt(X_{P_1^{\text{sift}},1} \oplus X'_{P_1^{\text{sift}},1})}{N_{P_1^{\text{sift}},1}} \leq e_{\text{bit},1,\text{tol}}$  are successful, for which the actual  $P_1^{\text{sift}}$  and  $P_2^{\text{sift}}$  sets are utilised instead of the received  $P_{1,r}^{\text{sift}}$  and  $P_{2,r}^{\text{sift}}$  in the  $\tilde{D}_{\text{PE}} = 1$  condition. Due to the matching message condition in idealised authentication check, when  $\tilde{F}_B = 1$ ,  $\rho_{\tilde{F}_B=1 \wedge \tilde{\Omega}_{\text{PE}}} = \rho_{\tilde{F}_B=1 \wedge \tilde{\Omega}_{\text{PE}}}$ . Noting that  $h_{\text{PA}}$  is 2-universal, we bound the

trace distance using the quantum leftover hash lemma [38, 41],

$$\Delta(\rho_{K_B L' S' E'' \wedge \tilde{F}_B=1}^{'out, jj'}, \tau_{K_B} \otimes \rho_{L' S' E \wedge \tilde{F}_B=1}^{'out, jj'}) \leq \Delta(\rho_{K_B L' S' E \wedge \tilde{F}_B=1 \wedge \tilde{\Omega}_{PE}}^{'out, jj'}, \tau_{K_B} \otimes \rho_{L' S' E \wedge \tilde{F}_B=1 \wedge \tilde{\Omega}_{PE}}^{'out, jj'})$$

$$\leq \frac{1}{2} \left\{ 4\varepsilon_{sm,1} + 2 \left[ H_{\min}^{\varepsilon_{sm,1}}(\hat{X}_{P_{2,r}^{\text{sift}}} | L' S'' E)_{\rho_{\hat{X}_{P_{2,r}^{\text{sift}}} L' S' E \wedge \tilde{F}_B=1 \wedge \tilde{\Omega}_{PE}}^{'out, jj'}}} - l_{K_B} \right] \right\}, \quad (43)$$

where  $S'' = S' \setminus R$ . Focusing only on the terms relevant to the current session, we can express the smooth min-entropy as

$$H_{\min}^{\varepsilon_{sm,1}}(\hat{X}_{P_{2,r}^{\text{sift}}} | L' S' E)_{\rho_{\hat{X}_{P_{2,r}^{\text{sift}}} L' S' E \wedge \tilde{F}_B=1 \wedge \tilde{\Omega}_{PE}}^{'out, jj'}}} = H_{\min}^{\varepsilon_{sm,1}}(\hat{X}_{P_{2,r}^{\text{sift}}} | K_1^h K_2 K_{1,\beta}^{\text{mask}} E)_{\rho_{\hat{X}_{P_{2,r}^{\text{sift}}} K_1^h K_2 K_{1,\beta}^{\text{mask}} E \wedge \tilde{F}_B=1 \wedge \tilde{\Omega}_{PE}}^{'out, jj'}}}, \quad (44)$$

where we note the labels are implicitly contained in  $E$ . Before simplifying the min-entropy, we first list the important conditions required for  $\tilde{F}_B = 1$  (inclusive of  $\tilde{D}_{PE} = 1$ ). These are

1.  $\beta = \beta'$ : The index chosen for the protocol session matches.
2.  $M_{AV} = M'_{AV}$ : Classical messages exchanged between Alice and Bob before Alice Validation step matches.
3.  $\Omega_{2 \rightarrow 3 \rightarrow 4 \rightarrow 5 \rightarrow 6}$ : Protocol step order is respected from steps 2 to 6.
4.  $\tilde{\Omega}_{PE}$ : Standard parameter estimation checks.

With the conditions, we can simplify the smooth min-entropy term similarly to QKD, using Thm. 10 of Ref. [38] to remove  $\wedge \Omega$  conditions when necessary,

$$\begin{aligned} & H_{\min}^{\varepsilon_{sm,1}}(\hat{X}_{P_{2,r}^{\text{sift}}} | K_1^h K_2 K_{1,\beta}^{\text{mask}} E)_{\rho_{\hat{X}_{P_{2,r}^{\text{sift}}} K_1^h K_2 K_{1,\beta}^{\text{mask}} E \wedge \tilde{F}_B=1 \wedge \tilde{\Omega}_{PE}}^{'out, jj'}}} \\ &= H_{\min}^{\varepsilon_{sm,1}}(X_{P_2^{\text{sift}}} | K_1^h K_2 K_{1,\beta}^{\text{mask}} T_{BV} \tilde{F}_B E_6)_{\rho_{X_{P_2^{\text{sift}}} K_1^h K_2 K_{1,\beta}^{\text{mask}} T_{BV} \tilde{F}_B E_6 \wedge \beta=\beta' \wedge M_{AV}=M'_{AV} \wedge \Omega_{2 \rightarrow 3 \rightarrow 4 \rightarrow 5 \rightarrow 6} \wedge \tilde{\Omega}_{PE}}^{'out, jj'}}} \\ &\geq H_{\min}^{\varepsilon_{sm,1}}(X_{P_2^{\text{sift}}} | K_1^h K_{1,\beta}^{\text{mask}} T_{AV} \tilde{D}_{PE} \text{syn} E_5)_{\rho_{X_{P_2^{\text{sift}}} K_1^h K_{1,\beta}^{\text{mask}} T_{AV} \tilde{D}_{PE} \text{syn} E_5 \wedge \beta=\beta' \wedge M_{AV}=M'_{AV} \wedge \Omega_{2 \rightarrow 3 \rightarrow 4 \rightarrow 5} \wedge \tilde{\Omega}_{PE}}^{'out, jj'}}} - 1 - \log_2 |\mathcal{T}_{BV}| \\ &\geq H_{\min}^{\varepsilon_{sm,1}}(X_{P_2^{\text{sift}}} | P_1^{\text{sift}} P_2^{\text{sift}} X'_{P_1^{\text{sift}}} E_4)_{\rho_{X_{P_2^{\text{sift}}} P_1^{\text{sift}} P_2^{\text{sift}} X'_{P_1^{\text{sift}}} E_4 \wedge M_{AV}=M'_{AV} \wedge \Omega_{2 \rightarrow 3 \rightarrow 4} \wedge \tilde{\Omega}_{PE}}^{'out, jj'}}} - 2 - \log_2 |\mathcal{T}_{BV}| |\mathcal{T}_{AV}| - \text{leak}_{EC} \\ &\geq H_{\min}^{\varepsilon_{sm,1}}(X_{P_2^{\text{sift}}} | P_1^{\text{sift}} P_2^{\text{sift}} X'_{P_1^{\text{sift}}} \theta_P \theta'_P P E_1)_{\rho_{X_{P_2^{\text{sift}}} P_1^{\text{sift}} P_2^{\text{sift}} X'_{P_1^{\text{sift}}} \theta_P \theta'_P P E_1 \wedge \tilde{\Omega}_{PE}}^{'out, jj'}}} - 2 - \log_2 |\mathcal{T}_{BV}| |\mathcal{T}_{AV}| - \text{leak}_{EC} \end{aligned} \quad (45)$$

The first equality uses the fact that Bob's corrected bit string matches Alice's and that  $P_2^{\text{sift}} = P_{2,r}^{\text{sift}}$ , and expands  $E = E_5 T_{BV} \tilde{F}_B$ , corresponding to output of the sixth step. The second inequality notes the removal of the classical  $T_{BV}$  and  $\tilde{F}_B$  using the chain rule of smooth min-entropy for classical systems [37], followed by removing  $K_2$ , noting that it is independent of the rest of the state without  $T_{BV}$ . Furthermore, the CPTP map describing Eve taking the outputs of step 5 and preparing inputs of step 6 is reversed. The third inequality removes the classical  $T_{AV}$ ,  $\tilde{D}_{PE}$  and  $\text{syn}$  using the chain rule of smooth min-entropy, followed by removal of  $K_1^h$  and  $K_{1,\beta}^{\text{mask}}$  since they are independent of the state after removal of  $T_{AV}$ . Furthermore, the CPTP map describing Eve taking the outputs of step 4 and preparing the inputs of step 5 is reversed. The final inequality reverses the remaining CPTP map to arrive at the state after step 1.

The quantum state  $\rho_{X_{P_2^{\text{sift}}} P_1^{\text{sift}} P_2^{\text{sift}} X'_{P_1^{\text{sift}}} \theta_P \theta'_P P E_1 \wedge \tilde{\Omega}_{PE}}^{'out, jj'}}$  can be viewed as being generated from a standard decoy-state BB84. As such, assuming ideal state preparation and fair sampling, we can bound the min-entropy by [24, 38],

$$H_{\min}^{\varepsilon_{sm,1}}(X_{P_2^{\text{sift}}} | P_1^{\text{sift}} P_2^{\text{sift}} X'_{P_1^{\text{sift}}} \theta_P \theta'_P P E_1)_{\rho_{X_{P_2^{\text{sift}}} P_1^{\text{sift}} P_2^{\text{sift}} X'_{P_1^{\text{sift}}} \theta_P \theta'_P P E_1 \wedge \tilde{\Omega}_{PE}}^{'out, jj'}}} \geq N_{P_2^{\text{sift}},1}^{\text{tol}} [1 - h_{\text{bin}}(e'_{\text{ph,tol}})], \quad (46)$$

where  $\varepsilon_{\text{sm},1} \geq \sqrt{2\varepsilon_{\text{serf},1}}$ ,  $N_{P_2^{\text{sift}},1}^{\text{tol}}$  is a lower bound on the number of single-photon events in set  $P_2^{\text{sift}}$ , with phase error tolerance

$$e'_{\text{ph,tol}} = e_{\text{bit},1,\text{tol}} + g(N_{P_1^{\text{sift}},1}^{\text{tol}}, N_{P_2^{\text{sift}},1}^{\text{tol}}, \varepsilon_{\text{serf},1}), \quad (47)$$

and  $g(k, n, \varepsilon) = \sqrt{\frac{(n+k)(k+1)}{2nk^2} \ln \frac{1}{\varepsilon}}$  stemming from the modified Serfling bound estimating the single-photon bit error rate in the key generation rounds of  $P_2^{\text{sift}}$  from that of  $P_1^{\text{sift}}$  [12, 42].  $\square$

### C.3.6 Shared Secrets Privacy

The final security parameter to examine is the shared secrets privacy condition, which can be summarised as

**Theorem 16.** *Consider the QAKE protocol  $\mathcal{P}$ . Then, the shared secrets privacy security condition satisfies*

$$\varepsilon_{\text{SP}} = \varepsilon'_{\text{SP},01,11} + 2(\varepsilon_{\text{ds}} + \varepsilon_{\text{MAC},1} + \varepsilon_{\text{SO}} + \varepsilon_{\text{MAC},2})$$

where

$$\begin{aligned} \varepsilon'_{\text{SP},01,11} &= 4\sqrt{2\varepsilon_{\text{serf},1}} + 2(\varepsilon_2 + \varepsilon_3) + \varepsilon_{\text{SP},\text{MAC},1} + \varepsilon_{\text{SP},\text{MAC},2}, \\ \varepsilon_{\text{SP},\text{MAC},1} &= \sqrt{(|\mathcal{T}_{\text{AV}}|\varepsilon_{\text{MAC},1} - 1) + 2^{\log_2\left(\frac{2}{\varepsilon_3} + 1\right) + \text{leak}_{\text{EC}} + 2 + \log_2|\mathcal{T}_{\text{AV}}| - N_{P_2^{\text{sift}},1}^{\text{tol}}[1 - h_{\text{bin}}(e'_{\text{ph,tol}})]}} \\ \varepsilon_{\text{SP},\text{MAC},2} &= \sqrt{(|\mathcal{T}_{\text{BV}}|\varepsilon_{\text{MAC},2} - 1) + 2^{\log_2\left(\frac{2}{\varepsilon_2} + 1\right) + \text{leak}_{\text{EC}} + 2 + \log_2|\mathcal{T}_{\text{AV}}||\mathcal{T}_{\text{BV}}| - N_{P_2^{\text{sift}},1}^{\text{tol}}[1 - h_{\text{bin}}(e'_{\text{ph,tol}})]}} \end{aligned}$$

is the shared secrets privacy parameter for idealised protocol  $\mathcal{P}'$  for cases where  $F_{\text{B}} = 1$ .

*Proof.* We begin by performing the swap to an “idealised” version of the protocol  $\mathcal{P}'$  following Thm. 12, with replacement of  $F_{\text{B}}$ ,  $D_{\text{BV}}$  and  $D_{\text{PE}}$ , which incurs a penalty of  $2(\varepsilon_{\text{ds}} + \varepsilon_{\text{MAC},1} + \varepsilon_{\text{MAC},2} + \varepsilon_{\text{SO}})$ . We then analyse the components of the shared secrets privacy trace distance separately, based on the  $(\tilde{F}_{\text{A}}, \tilde{F}_{\text{B}})$  values. For the  $(\tilde{F}_{\text{A}}, \tilde{F}_{\text{B}}) = (\phi, 0)$  case, the switch to “idealised” checks means none of the secrets are utilised and thus are not leaked, as presented in Thm. 17. For the case of  $(\tilde{F}_{\text{A}}, \tilde{F}_{\text{B}}) \in \{0\phi, 00\}$ , which is analysed together in Thm. 18, the main leakage concern is that from sending  $T_{\text{AV}}$ . There, we provide a clear reason for the necessity of the channels  $\mathcal{E}_{K_1^h K_{1,i}^{\text{mask}} E_i \rightarrow E_{i+1}}$  to quantify the leakage of information when  $T_{\text{AV}}$  is sent, but where  $K_{1,i}^{\text{mask}}$  is still required for future sessions. Finally, the case of  $(\tilde{F}_{\text{A}}, \tilde{F}_{\text{B}}) \in \{01, 11\}$  can be analysed in a similar way to the key secrecy condition. The privacy of secrets  $K_1^h K_{1,i}^{\text{mask}} K_2$  is maintained via the strong extractor property and QLHL [17, 41], where the adversary’s uncertainty of  $\tilde{X}_{P_2^{\text{sift}},r}$  provides masking for the keys of the 2-universal hash function, as shown in Thm. 19. Combining all the results, we get the statement presented in the theorem.  $\square$

We analyse the condition with the ideal output state from Eqn. 31, and we recall that an ideal state in  $\mathcal{S}_{in}$  has the form

$$\rho_{LSE}^{\text{in},jj'} = |jj'\rangle\langle jj'|_{\alpha\alpha'} \otimes \tau_{K_2 R K_{1,j}^{\text{mask}} \dots K_{1,m}^{\text{mask}}} \otimes \mathcal{E}_{K_1^h K_{1,j-1}^{\text{mask}} E_{j-1} \rightarrow E} \circ \dots \circ \mathcal{E}_{K_1^h K_{1,j'}^{\text{mask}} E_{j'} \rightarrow E_{j'+1}} (\tau_{K_1^h K_{1,j'}^{\text{mask}} \dots K_{1,j-1}^{\text{mask}}} \otimes \rho_{E_{j'}}). \quad (48)$$

We begin with the case of  $(\tilde{F}_{\text{A}}, \tilde{F}_{\text{B}}) = (\phi, 0)$ ,

**Theorem 17.** *Consider the QAKE protocol  $\mathcal{P}'$ . Then, there exists  $\sigma_{LSE}^{\phi 0, jj'} \in \mathcal{S}_{in}$  such that*

$$\Delta \left( p_{\phi 0}^{\text{real}} \rho_{LSE|(\tilde{F}_{\text{A}}, \tilde{F}_{\text{B}})=\phi 0}^{\text{'out}, jj'}, \sum_{\tilde{j}' \geq j'} p_{\phi 0, \tilde{j}'} \sigma_{LSE}^{\phi 0, j, \tilde{j}'+1} \right) = 0.$$

*Proof.* The goal here and in subsequent theorems is to prove that secrets that should not be leaked remains private. The trace distance can be expressed as

$$\Delta \left( p_{\phi 0}^{\text{real}} \rho_{LSE|(\tilde{F}_{\text{A}}, \tilde{F}_{\text{B}})=\phi 0}^{\text{'out}, jj'}, \sum_{\tilde{j}' \geq j'} p_{\phi 0, \tilde{j}'} \sigma_{LSE}^{\phi 0, j, \tilde{j}'+1} \right) \leq \sum_{\tilde{j}' \geq j'} p_{\phi 0, \tilde{j}'} \Delta \left( \rho_{LSE|(\tilde{F}_{\text{A}}, \tilde{F}_{\text{B}})=\phi 0, \beta'=\tilde{j}'}^{\text{'out}, jj'}, \sigma_{LSE}^{\phi 0, j, \tilde{j}'+1} \right), \quad (49)$$

for  $\tilde{j}' \geq j'$ , noting that the choice of  $\beta' < j'$  is not possible (by definition of  $\beta'$ ). We can thus analyse the trace distance separately for each  $\tilde{j}'$  selection.

Here, we focus on an arbitrary  $\tilde{j}'$  for analysis. We first note that with the change to idealised checks, the protocol does not utilise any of the shared secrets when  $\tilde{F}_A = \phi$  and thus would not leak them. As such, the only operation on the secrets is the tracing away of  $K_{1,i}^{\text{mask}}$  for  $i \leq \min\{j, \tilde{j}' + 1\}$ , which will no longer be used. For input state with  $\rho_{LSE}^{\text{in},jj'} \in \mathcal{S}_{in}$ , tracing away  $K_{1,i}^{\text{mask}}$  would lead to removal of its corresponding channel  $\mathcal{E}_{K_1^h K_{1,i}^{\text{mask}} E_i \rightarrow E_{i+1}}$  for  $i \in [\min\{j, \tilde{j}'\}, \in \{j, \tilde{j}' + 1\}]$ , resulting in a state of the form  $\rho_{LSE}^{\text{in},j,\tilde{j}'+1}$  above. Therefore, the output state is ideal.  $\square$

We can consider the cases of  $(\tilde{F}_A, \tilde{F}_B) = (0, \phi)$  and  $\tilde{F}_A = \tilde{F}_B = 0$  cases together, since they share a common event  $\tilde{F}_A = 0$ .

**Theorem 18.** *Consider the QAKE protocol  $\mathcal{P}'$ . Then, there exists  $\sigma_{LSE}^{0\phi,jj'}, \sigma_{LSE}^{00,jj'} \in \mathcal{S}_{in}$  such that*

$$\Delta \left( p_{0\phi}^{\text{real}} \rho_{LSE|(\tilde{F}_A, \tilde{F}_B)=0\phi}^{\text{'out},jj'} + p_{00}^{\text{real}} \rho_{LSE|(\tilde{F}_A, \tilde{F}_B)=00}^{\text{'out},jj'}, \sum_{\tilde{j} \geq j} p_{0\phi,\tilde{j}} \sigma_{LSE}^{0\phi,\tilde{j}+1,j'} + \sum_{\tilde{j} \geq j, \tilde{j}' \geq j'} p_{00,\tilde{j}\tilde{j}'} \sigma_{LSE}^{00,\tilde{j}+1,\tilde{j}'+1} \right) = 0.$$

*Proof.* We can split the trace distance according to the  $\tilde{j}$  and  $\tilde{j}'$  values,

$$\sum_{\tilde{j} \geq j} p_{0\phi,\tilde{j}} \Delta \left( \rho_{LSE|(\tilde{F}_A, \tilde{F}_B)=0\phi, \beta=\tilde{j}}^{\text{'out},jj'}, \sigma_{LSE}^{0\phi,\tilde{j}+1,j'} \right) + \sum_{\tilde{j} \geq j, \tilde{j}' \geq j'} p_{00,\tilde{j}\tilde{j}'} \Delta \left( \rho_{LSE|(\tilde{F}_A, \tilde{F}_B)=00, (\beta, \beta')=\tilde{j}\tilde{j}'}^{\text{'out},jj'}, \sigma_{LSE}^{00,\tilde{j}+1,\tilde{j}'+1} \right), \quad (50)$$

and evaluate the individual terms. We note that when  $\tilde{F}_B \neq 1$ ,  $K_2$  and  $R$  remain private since they are not used.

We begin with studying the terms of the  $(\tilde{F}_A, \tilde{F}_B) = (0, \phi)$  case, which we have to split further into two sub-cases: (1)  $\tilde{j} + 1 \leq j'$  and (2)  $\tilde{j} + 1 > j'$ . Since Alice sends tag  $T_{AV}$  irrespective of  $\tilde{F}_A$ , some information of  $(K_1^h, K_{1,\tilde{j}}^{\text{mask}})$  can be leaked, though how it manifests in the ideal state depends on the sub-case. In sub-case (1), we note that  $K_{1,i}^{\text{mask}}$  for any  $i \leq \tilde{j}$  will not be utilised in the future and can be traced out. This includes tracing away  $K_{1,\tilde{j}}^{\text{mask}}$ , which by Thm. 4, guarantees that  $K_1^h$  remains private, which leads to an output state of the form  $\rho_{LSE}^{\text{in},\tilde{j}+1,j'}$ . In sub-case (2),  $K_{1,\tilde{j}}^{\text{mask}}$  may be utilised in future sessions. Since the only information of the secrets learnt in the protocol session is via  $T_{AV}$ , we can consider a worse case where the adversary has a single access to an oracle where it can select any message  $M$  and obtain a corresponding tag, i.e.  $\mathcal{E}_{K_1^h K_{1,\tilde{j}} E_{\tilde{j}} \rightarrow E}$ . This leads to an additional channel in the state, thereby matching the form of  $\rho_{LSE}^{\text{in},\tilde{j}+1,j'}$  when  $\tilde{j} + 1 > j'$ . Combining both arguments and selecting the appropriate  $\sigma_{LSE}^{0\phi,\tilde{j}+1,j}$  states, the trace distance contribution when  $(\tilde{F}_A, \tilde{F}_B) = (0, \phi)$  is 0.

In the  $(\tilde{F}_A, \tilde{F}_B) = (0, 0)$  case,  $T_{AV}$  announcement remains the main concern. Similar to the previous case, when  $\tilde{j} + 1 > \tilde{j}' + 1$ , the leakage of  $(K_1^h, K_{1,\tilde{j}}^{\text{mask}})$  results in an additional channel  $\mathcal{E}_{K_1^h K_{1,\tilde{j}} E_{\tilde{j}} \rightarrow E}$  in the output state, while for  $\tilde{j} + 1 \leq \tilde{j}' + 1$ , the tracing out of  $K_{1,\tilde{j}}^{\text{mask}}$  ensures that  $K_1^h$  remains private. In addition,  $K_{1,i}^{\text{mask}}$  for  $i \leq \min\{\tilde{j}, \tilde{j}'\}$  are traced out. The resulting output state would therefore match  $\rho_{LSE}^{\text{in},\tilde{j}+1,\tilde{j}'+1}$ , yielding a trace distance of 0.  $\square$

Here, we analyse the final two cases of  $(\tilde{F}_A, \tilde{F}_B) \in \{01, 11\}$  jointly since they are similar.

**Theorem 19.** *Consider the QAKE protocol  $\mathcal{P}'$ . Then, there exists  $\sigma_{LSE}^{01,jj'}, \sigma_{LSE}^{11,jj'} \in \mathcal{S}_{in}$  such that*

$$\Delta \left( p_{01}^{\text{real}} \rho_{LSE|(\tilde{F}_A, \tilde{F}_B)=01}^{\text{'out},jj'} + p_{11}^{\text{real}} \rho_{LSE|(\tilde{F}_A, \tilde{F}_B)=11}^{\text{'out},jj'}, \sum_{\tilde{j} \geq \max\{j,j'\}} p_{01,\tilde{j}} \sigma_{LSE}^{01,\tilde{j}+1,\tilde{j}} + \sum_{\tilde{j} \geq \max\{j,j'\}} p_{11,\tilde{j}} \sigma_{LSE}^{11,\tilde{j},\tilde{j}} \right) \leq \epsilon'_{\text{SP},01,11}$$

where

$$\epsilon'_{\text{SP},01,11} = 4\sqrt{2\epsilon_{\text{serf},1}} + 2(\epsilon_2 + \epsilon_3) + \sqrt{(|\mathcal{T}_{BV}|\epsilon_{\text{MAC},2} - 1) + 2^{\log_2\left(\frac{2}{\epsilon_2} + 1\right) + \text{leak}_{\text{EC}} + 2 + \log_2 |\mathcal{T}_{AV}| |\mathcal{T}_{BV}| - N_{P_2^{\text{sift}},1}^{\text{tol}} [1 - h_{\text{bin}}(e'_{\text{ph,tol}})]}} \\ + \sqrt{(|\mathcal{T}_{AV}|\epsilon_{\text{MAC},1} - 1) + 2^{\log_2\left(\frac{2}{\epsilon_3} + 1\right) + \text{leak}_{\text{EC}} + 2 + \log_2 |\mathcal{T}_{AV}| - N_{P_2^{\text{sift}},1}^{\text{tol}} [1 - h_{\text{bin}}(e'_{\text{ph,tol}})]}},$$

where  $\epsilon_1$  and  $\epsilon_2$  are parameters to optimise over. If the hash functions are 2-universal, then

$$\epsilon'_{\text{SP},01,11} = 4\sqrt{2\epsilon_{\text{serf},1}} + \frac{1}{2} \times 2^{-\frac{1}{2}[N_{P_2^{\text{tol}},1} - N_{P_2^{\text{tol}},1} h_{\text{bin}}(e'_{\text{ph,tol}}) - \text{leak}_{\text{EC}} - 2 - \log_2 |\mathcal{T}_{AV}| |\mathcal{T}_{BV}|]} \left( 1 + 2^{-\frac{1}{2} \log_2 |\mathcal{T}_{AV}|} \right).$$

*Proof.* We can explicitly express the form of the output state and selected  $\sigma_{LSE}^{01,jj'}, \sigma_{LSE}^{11,jj'}$  states,

$$\begin{aligned}
p_{01}^{\text{real}} \rho_{LSE|(\tilde{F}_A, \tilde{F}_B)=01}^{\text{'out}, jj'} &= \sum_{\tilde{j} \geq j_{\max}} |\tilde{j}+1, \tilde{j}\rangle\langle \tilde{j}+1, \tilde{j}|_{\alpha\alpha'} \otimes \rho_{K_1^h K_2 R K_{1,[\tilde{j}, m]}^{\text{mask}} E \wedge \tilde{F}_B=1 \wedge \tilde{F}_A=0 \wedge \beta=\tilde{j}}^{\text{'out}, jj'} \\
p_{11}^{\text{real}} \rho_{LSE|(\tilde{F}_A, \tilde{F}_B)=11}^{\text{'out}, jj'} &= \sum_{\tilde{j} \geq j_{\max}} |\tilde{j}, \tilde{j}\rangle\langle \tilde{j}, \tilde{j}|_{\alpha\alpha'} \otimes \rho_{K_1^h K_2 R K_{1,[\tilde{j}, m]}^{\text{mask}} E \wedge \tilde{F}_B=1 \wedge \tilde{F}_A=1 \wedge \beta=\tilde{j}}^{\text{'out}, jj'} \\
\sum_{\tilde{j} \geq \max\{j, j'\}} p_{01, \tilde{j}} \sigma_{LSE}^{01, \tilde{j}+1, \tilde{j}} &= \sum_{\tilde{j} \geq j_{\max}} |\tilde{j}+1, \tilde{j}\rangle\langle \tilde{j}+1, \tilde{j}|_{\alpha\alpha'} \otimes \tau_{K_1^h K_2 R K_{1,[\tilde{j}, m]}^{\text{mask}}} \otimes \rho_{E \wedge \tilde{F}_B=1 \wedge \tilde{F}_A=0 \wedge \beta=\tilde{j}}^{\text{'out}, jj'} \\
\sum_{\tilde{j} \geq \max\{j, j'\}} p_{11, \tilde{j}} \sigma_{LSE}^{11, \tilde{j}, \tilde{j}} &= \sum_{\tilde{j} \geq j_{\max}} |\tilde{j}, \tilde{j}\rangle\langle \tilde{j}, \tilde{j}|_{\alpha\alpha'} \otimes \tau_{K_1^h K_2 R K_{1,[\tilde{j}, m]}^{\text{mask}}} \otimes \rho_{E \wedge \tilde{F}_B=1 \wedge \tilde{F}_A=1 \wedge \beta=\tilde{j}}^{\text{'out}, jj'}.
\end{aligned} \tag{51}$$

We note that  $\tilde{F}_A$  and  $\tilde{F}_B$  is implicitly stored in  $E$ , and can be utilised to compute  $\alpha\alpha'$ . As such, we can express the overall trace distance as  $\Delta(\rho_{K_1^h K_2 R K_{1,[\tilde{j}, m]}^{\text{mask}} E \wedge \tilde{F}_B=1}, \tau_{K_1^h K_2 R K_{1,[\tilde{j}, m]}^{\text{mask}}} \otimes \rho_{E \wedge \tilde{F}_B=1}^{\text{'out}, jj'})$ , where  $R$  and  $K_{1,[\tilde{j}+1, m]}^{\text{mask}}$  are removed since they are unused in this protocol session, and thus remain private.

We simplify the trace distance by first introducing an intermediate state with only  $K_2$  being private,

$$\begin{aligned}
&\Delta(\rho_{K_1^h K_2 R K_{1,[\tilde{j}, m]}^{\text{mask}} E \wedge \tilde{F}_B=1}, \tau_{K_1^h K_2 R K_{1,[\tilde{j}, m]}^{\text{mask}}} \otimes \rho_{E \wedge \tilde{F}_B=1}^{\text{'out}, jj'}) \\
&\leq \Delta(\rho_{K_1^h K_2 R K_{1,[\tilde{j}, m]}^{\text{mask}} E \wedge \tilde{F}_B=1}, \tau_{K_2} \otimes \rho_{K_1^h K_2 R K_{1,[\tilde{j}, m]}^{\text{mask}} E \wedge \tilde{F}_B=1}^{\text{'out}, jj'}) + \Delta(\rho_{K_1^h K_2 R K_{1,[\tilde{j}, m]}^{\text{mask}} E \wedge \tilde{F}_B=1}, \tau_{K_1^h K_2 R K_{1,[\tilde{j}, m]}^{\text{mask}}} \otimes \rho_{E \wedge \tilde{F}_B=1}^{\text{'out}, jj'}).
\end{aligned} \tag{52}$$

To simplify the trace distance, we first note that  $h_1(K_1^h, X) \oplus K_1^{\text{mask}}$  is an  $\varepsilon_{\text{MAC},1}$ -almost strong 2-universal hash function with keys  $(K_1^h, K_1^{\text{mask}})$ . Therefore, we can apply Thm. 5,

$$\begin{aligned}
&\Delta(\rho_{K_1^h K_2 R K_{1,[\tilde{j}, m]}^{\text{mask}} E \wedge \tilde{F}_B=1}, \tau_{K_1^h K_2 R K_{1,[\tilde{j}, m]}^{\text{mask}}} \otimes \rho_{E \wedge \tilde{F}_B=1}^{\text{'out}, jj'}) \leq 2(\varepsilon_{\text{sm},2} + \varepsilon_{\text{sm},3} + \varepsilon_2 + \varepsilon_3) \\
&+ \sqrt{(|\mathcal{T}_{\text{BV}}| \varepsilon_{\text{MAC},2} - 1) + 2^{\log_2 |\mathcal{T}_{\text{BV}}| + \log_2 (\frac{2}{\varepsilon_2} + 1) - H_{\min}^{\varepsilon_{\text{sm},2}}(\hat{X}_{P_2^{\text{sift}},r} | K_1^h K_{1,\beta}^{\text{mask}} E) \wedge \tilde{\Omega}_{\text{PE}} \wedge \tilde{F}_B=1}} \\
&+ \sqrt{(|\mathcal{T}_{\text{AV}}| \varepsilon_{\text{MAC},1} - 1) + 2^{\log_2 |\mathcal{T}_{\text{AV}}| + \log_2 (\frac{2}{\varepsilon_3} + 1) - H_{\min}^{\varepsilon_{\text{sm},3}}(\hat{X}_{P_2^{\text{sift}},r} | E) \wedge \tilde{\Omega}_{\text{PE}} \wedge \tilde{F}_B=1}}
\end{aligned} \tag{53}$$

where we label  $\wedge \tilde{\Omega}_{\text{PE}}$  on smooth min-entropy as evaluation on the corresponding state when event  $\tilde{\Omega}_{\text{PE}}$  occurs. We can now follow a similar analysis as in the proof of Thm. 13, with the main difference being the lack of conditioning on some secrets. For the first smooth min-entropy with smoothing parameter  $\varepsilon_{\text{sm},2}$ , the conditioning on  $K_2$  is not present. Therefore,  $T_{\text{BV}}$ , as the output of a  $\varepsilon_{\text{MAC},2}$ -almost strongly 2-universal hash function, is uniform and independent of the input, importantly  $X_{P_2^{\text{sift}}}$ . As such, it can be removed without using the min-entropy chain rule, i.e. without incurring a  $\log_2 |\mathcal{T}_{\text{BV}}|$  penalty, resulting in

$$H_{\min}^{\varepsilon_{\text{sm},2}}(\hat{X}_{P_2^{\text{sift}},r} | K_1^h K_{1,\beta}^{\text{mask}} E) \rho_{\hat{X}_{P_2^{\text{sift}},r} K_1^h K_{1,\beta}^{\text{mask}} E \wedge \tilde{\Omega}_{\text{PE}} \wedge \tilde{F}_B=1}^{\text{'out}, jj'} \geq N_{P_2^{\text{sift}},1}^{\text{tol}} - N_{P_2^{\text{sift}},1}^{\text{tol}} h_{\text{bin}}(e'_{\text{ph,tol}}) - \text{leak}_{\text{EC}} - \log_2 |\mathcal{T}_{\text{AV}}| - 2. \tag{54}$$

In the second term, both the conditioning on  $K_2$  and  $K_1^h K_{1,\beta}^{\text{mask}}$  are absent. Similarly, we can argue that  $T_{\text{AV}}$  and  $T_{\text{BV}}$  are uniform and independent of  $X_{P_2}$  since the respective keys of the almost 2-universal hash functions are not part of the conditioning. As such, we have

$$H_{\min}^{\varepsilon_{\text{sm},3}}(\hat{X}_{P_2^{\text{sift}},r} | E) \rho_{\hat{X}_{P_2^{\text{sift}},r} E \wedge \tilde{\Omega}_{\text{PE}} \wedge \tilde{F}_B=1}^{\text{'out}, jj'} \geq N_{P_2^{\text{sift}},1}^{\text{tol}} - N_{P_2^{\text{sift}},1}^{\text{tol}} h_{\text{bin}}(e'_{\text{ph,tol}}) - \text{leak}_{\text{EC}} - 2. \tag{55}$$

Combining the results, the trace distance is bounded by

$$\begin{aligned}
&\Delta(\rho_{K_1^h K_2 R K_{1,[\tilde{j}, m]}^{\text{mask}} E \wedge \tilde{F}_B=1}, \tau_{K_1^h K_2 R K_{1,[\tilde{j}, m]}^{\text{mask}}} \otimes \rho_{E \wedge \tilde{F}_B=1}^{\text{'out}, jj'}) \leq 4\sqrt{2\varepsilon_{\text{serf},1}} + 2(\varepsilon_2 + \varepsilon_3) \\
&+ \sqrt{(|\mathcal{T}_{\text{BV}}| \varepsilon_{\text{MAC},2} - 1) + 2^{\log_2 (\frac{2}{\varepsilon_2} + 1) + \text{leak}_{\text{EC}} + 2 + \log_2 |\mathcal{T}_{\text{AV}}| - N_{P_2^{\text{sift}},1}^{\text{tol}} [1 - h_{\text{bin}}(e'_{\text{ph,tol}})]}} \\
&+ \sqrt{(|\mathcal{T}_{\text{AV}}| \varepsilon_{\text{MAC},1} - 1) + 2^{\log_2 (\frac{2}{\varepsilon_3} + 1) + \text{leak}_{\text{EC}} + 2 + \log_2 |\mathcal{T}_{\text{AV}}| - N_{P_2^{\text{sift}},1}^{\text{tol}} [1 - h_{\text{bin}}(e'_{\text{ph,tol}})]}}.
\end{aligned} \tag{56}$$

We can repeat the analysis with two-universal hash function using QLHL to obtain the second set of bounds in the theorem.  $\square$

## D QAKE with Pseudorandom Basis Choice

The QAKE protocol, similar to many QKD protocols, suffers from key rate loss due to sifting. One method to avoid sifting is to pre-share basis information and having Bob measure in the same basis as Alice. However, this introduces two issues which renders the protocol inefficient: (1) Alice and Bob needs to pre-share a basis  $\theta$  that is large to account for signal loss and finite-size effects (we require on the order of  $10^{10}$  signals in our experiment), (2) the pre-shared basis has to be refreshed every session via key updating due to leakage from multi-photon events. The most practical solution to the problem is to use a shorter pre-shared master key and generate a larger key from a quantum-safe *pseudorandom number generator* (PRNG) like AES [16]. We note that even without pre-sharing the basis, using PRNG still confers the advantage of reducing the length of the random string required to generate the basis. We note that there are similar proposals in QKD where the basis information is generated or encrypted using a PRNG [31, 43].

### D.1 Protocol

We begin with two parties, Alice and Bob, sharing secrets  $S$ : (1) shared basis seed  $\tilde{\theta} = \{\tilde{\theta}_j\}_{j=1,\dots,m}$ , where  $\tilde{\theta}_i \in \{0,1\}^{l_{\tilde{\theta}}}$ , (2) authentication keys  $K_1^h$  and  $K_2$ , (3) privacy amplification seed  $R$ , and (4) authentication masking key  $K_1^{\text{mask}} = \{K_{1,j}^{\text{mask}}\}_{j=1,\dots,m}$ . We note that the authentication keys and privacy amplification seed always remain secret and unchanged. Alice and Bob each has a label,  $\alpha$  and  $\alpha'$  respectively, that notes the secrets to utilise for the session (i.e. which  $\tilde{\theta}_i$  and  $K_{1,i}^{OTP}$  to utilise), thereby allowing secrets to be replaced (by never using them again) when authentication fails. They also publicly share a  $\varepsilon_{\text{MAC},1}$ -almost XOR 2-universal hash function  $h_1$  (authentication key  $K_1^h$ ), a  $\varepsilon_{\text{MAC},2}$ -almost strongly 2-universal hash function  $h_2$  (authentication key  $K_2$ ) to generate the authentication tags, and a 2-universal hash function  $h_{\text{PA}}$  for privacy amplification to generate secret keys. Alice and Bob also agrees on an error correction protocol, with syndrome generation function  $f_{\text{syn}}$ , error correction function  $f_{\text{ec}}$  and an error correction efficiency of  $\gamma_{\text{EC}}$ . They also agree on the use of a  $(t', \varepsilon_{\text{PRNG}})$ -quantum secure PRNG,  $G^{\text{PRNG}}$ . We note here that the subscript  $r$  on any random variables represent the received variable, e.g.  $\alpha_r$  is received by Bob when  $\alpha$  is sent by Alice, since the adversary could alter the messages sent through the classical communication channel. The protocol schematic is shown in Fig. 6, and is detailed below.

We note here that we choose the PRNG with  $t' \geq 2(t + t_{MG}) + t_{ex} + t_{SG,PR}$ , for an adversary assumed to be limited by resource  $t$  during the protocol (e.g. limited run time). The resource  $t_{MG}$  and  $t_{ex}$  relate to the security analysis of the protocol with PRNG, used to prove that the gap between bit and phase error is small in Appendix E.2. The resource  $t_{SG,PR}$  relates to the limited ability of the adversary to guess the basis seed during before it is announced, as shown in Appendix A. We note additionally that the PRNG master key is much smaller than the basis string length, importantly  $2|\tilde{\theta}_\beta| < n_{\text{rnd}}$ .

---

**Protocol 2** Quantum Authenticated Key Exchange with Pseudorandom Basis Selection

---

*Goal.* Alice and Bob authenticates one another, and performs key exchange.

1. **Label Agreement:** Alice and Bob exchange  $\alpha$  and  $\alpha'$ . Alice (resp. Bob) sends  $\alpha$  (resp.  $\alpha'$ ) and receives  $\alpha'_r$  (resp.  $\alpha_r$ ), which results in a label choice  $\beta = \max\{\alpha, \alpha'_r\}$  (resp.  $\beta' = \max\{\alpha_r, \alpha'\}$ ).
  2. **Alice State Preparation:** Alice generates a  $n_{rnd}$ -bit basis string with a PRNG using the basis seed,  $\theta_\beta = G^{\text{PRNG}}(\tilde{\theta}_\beta)$ , randomly chooses a  $n_{rnd}$ -bit string  $X$  and a  $n_{rnd}$ -trit string  $v \in \{0, 1, 2\}^{n_{rnd}}$  according to probability distribution  $p_v$ . She then prepares  $n_{rnd}$  quantum systems  $Q_i$  in phase-randomised coherent BB84 states  $\left\{ \rho_{Q_i}^{\theta_i, X_i, \mu_{v_i}} \right\}_{i \in [1, n_{rnd}]}$ , with basis  $\theta_i$ , bit value  $X_i$ , and intensity  $\mu_{v_i}$ .
  3. **Bob Measurement:** Alice sends  $Q^{n_{rnd}}$  to Bob, who measures subsystems  $Q_i$  using basis  $\theta'_{\beta'} = G^{\text{PRNG}}(\tilde{\theta}'_{\beta'})$ , and records outcome  $X'_i$ . If Bob detects no clicks, he declares  $X'_i = \perp$ . If Bob detects multiple clicks, he randomly selects  $X'_i \in \{0, 1\}$ .
  4. **Test Round Announcement:** Bob records the detection rounds,  $P = \{i : X'_i \neq \perp\}$ , and randomly splits it into  $P_1$  and  $P_2$ , with  $|P_1| = \lceil f_{P_1} |P| \rceil$ , where  $f_{P_1}$  is some pre-determined fraction of rounds for parameter estimation. Bob announces  $P_1, P_2, \theta'_{\beta'}$  and  $X'_{P_1}$ .
  5. **Parameter Estimation:** Alice checks if: (1) the number of test rounds matches the expected number  $|P_{1,r}| = \lceil f_{P_1} |P| \rceil$ , (2) the basis seed matches,  $\tilde{\theta}'_{\beta',r} = \tilde{\theta}_\beta$ , (3) the lower bound on single-photon events in sets  $P_{2,r}$  and  $P_{1,r}$  (estimated via decoy state analysis) exceeds a threshold,  $\hat{N}_{P_{2,r},1}^{\text{LB}} \geq N_{P_{2,r},1}^{\text{tol}}, \hat{N}_{P_{1,r},1}^{\text{LB}} \geq N_{P_{1,r},1}^{\text{tol}}$ , (4) the upper bound on single-photon bit-error rate in set  $P_{1,r}$  (estimated via decoy-state analysis) falls below a threshold,  $\hat{e}_{\text{bit}, P_{1,r}, 1}^{\text{UB}} \leq e_{\text{bit}, 1, \text{tol}}$ , and (5) the upper bound on bit error rate in set  $P_{2,r}$  (estimated via Serfling bound) falls below a threshold,  $\hat{e}_{\text{bit}, P_{2,r}}^{\text{UB}} \leq e_{\text{bit}, \text{tol}}$ . If all checks pass, Alice sets  $D_{\text{PE}} = 1$ , otherwise she sets  $D_{\text{PE}} = 0$ .
  6. **Error Correction:** If  $D_{\text{PE}} = 1$ , Alice generates a syndrome  $\text{syn} = f_{\text{syn}}(X_{P_{2,r}})$  of length  $l_{\text{syn}}$  and forwards it to Bob, otherwise, Alice sends a random string of length  $l_{\text{syn}}$  to Bob. Bob receives the syndrome  $\text{syn}_r$  and computes the corrected bit string  $\hat{X}_{P_{2,r}} = f_{\text{ec}}(X'_{P_2}, \text{syn}_r)$ .
  7. **Alice Validation:** If  $D_{\text{PE}} = 1$ , Alice generates a tag  $T_{\text{AV}} = h_1(K_1^h, X'_{P_{1,r}} || P_{1,r} || P_{2,r} || X_{P_{2,r}} || \text{syn}) \oplus K_{1,\beta}^{\text{mask}}$  and forwards it to Bob, otherwise, Alice sends a random string of the same length as the tag. Bob receives tag  $T_{\text{AV},r}$  and generates verification tag  $\tilde{T}_{\text{AV}} = h_1(K_1^h, X'_{P_1} || P_1 || P_2 || \hat{X}_{P_{2,r}} || \text{syn}_r) \oplus K_{1,\beta'}^{\text{mask}}$  and checks if  $T_{\text{AV},r} = \tilde{T}_{\text{AV}}$ . If the tags matches, Bob validates Alice and output  $F_B = 1$ , otherwise, he sets  $F_B = 0$ .
  8. **Bob Validation:** If  $F_B = 1$ , Bob generates a tag,  $T_{\text{BV}} = h_2(K_2, \hat{X}_{P_{2,r}})$ , and sends  $T_{\text{BV}}$  to Alice. If  $F_B = 0$ , Bob sends a random string of the same length as the tag instead. Alice receives the tag  $T_{\text{BV},r}$ , and computes the verification tag,  $\tilde{T}_{\text{BV}} = h_2(K_2, X_{P_{2,r}})$ . If  $T_{\text{BV},r} = \tilde{T}_{\text{BV}}$ , Alice validates Bob,  $D_{\text{BV}} = 1$ , otherwise, she sets  $D_{\text{BV}} = 0$ .
  9. **Secret Key Generation and Label Update:** Alice decides whether to accept the session based on her parameter estimation and validation of Bob, i.e.  $F_A = D_{\text{PE}} \wedge D_{\text{BV}}$ . If Alice (resp. Bob) decides to perform key generation,  $F_A = 1$  (resp.  $F_B = 1$ ), she (resp. he) performs privacy amplification  $K_A || \tilde{\theta}_\beta = h_{\text{PA}}(R, X_{P_{2,r}})$  (resp.  $K_B || \tilde{\theta}'_{\beta'} = h_{\text{PA}}(R, \hat{X}_{P_{2,r}})$ ) and sets  $\alpha = \beta$  (resp.  $\alpha' = \beta'$ ), where the basis seed  $\tilde{\theta}$  is updated and  $K_A K_B$  are the cryptographically secure keys that can be used for other purposes. If key generation is not performed, the labels are updated, i.e. if  $F_A = 0$ , Alice updates her label  $\alpha = \beta + 1$  and if  $F_B = 0$ , Bob updates his label  $\alpha' = \beta' + 1$ .
- 

## D.2 Overall Protocol Security

As per the security analysis of the original QAKE protocol, the focus of the security analysis here would be for a single-session, for which we have to first define the set of ideal input and output states. The labels remain  $\alpha$  and  $\alpha'$ , with the shared secrets  $S$  having additionally basis seed  $\tilde{\theta}_i$ . The basis seed  $\tilde{\theta}_i$  used to generate the shared basis can potentially be leaked after utilisation in a protocol session, so we let basis seeds for indices  $i \leq \alpha_{\text{max}} - 1$  ( $\alpha_{\text{max}} = \max\{\alpha, \alpha'\}$ ) be leaked. Authentication masking keys behave similarly, with keys corresponding to indices  $i < \alpha_{\text{min}} - 1$  ( $\alpha_{\text{min}} = \min\{\alpha, \alpha'\}$ ) no longer being used. Unlike the original QAKE protocol, authentication key  $K_1^h$  will always remain secure, alongside authentication key  $K_2$  and privacy amplification seed  $R$ . This difference stems from Bob's reply of the basis seed  $\tilde{\theta}'_{\beta'}$ , which serves as a method for

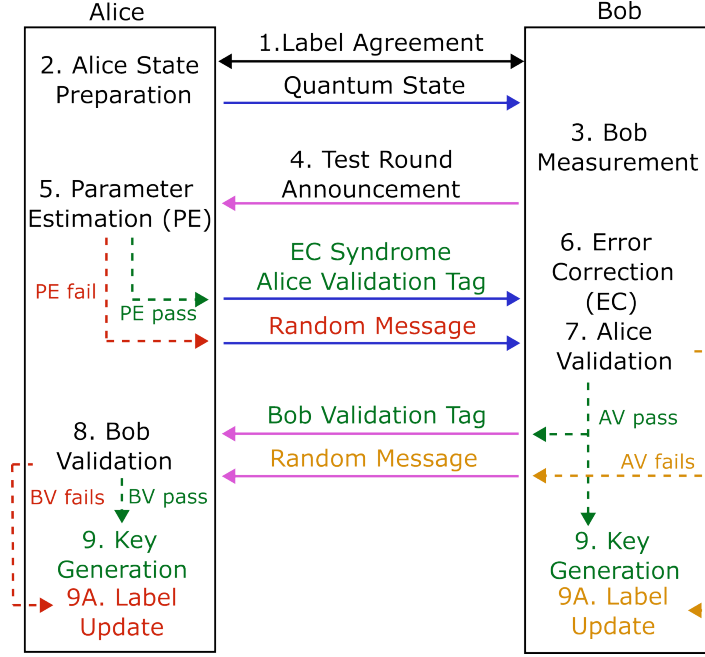


Figure 6: Summary of the QAKE with pseudorandom basis protocol proposed. The protocol begins with both parties establishing the label to use, followed by Alice sending quantum states to Bob. Bob announces the test round results, which Alice can then use for parameter estimation. If this passes, error correction and validation of Alice's identity would occur followed by validation of Bob's identity. Finally, the two parties independently decide whether to generate secret keys or update their label (signalling a protocol failure).

Alice to authenticate Bob, preventing  $T_{AV}$  from being announced when this check fails. As such, we define the ideal input state  $\rho^{\text{in}} = \sum_{jj'} p_{jj'} \rho_{LSE}^{\text{in}, jj'}$ , where

$$\rho_{LSE}^{\text{in}, jj'} = |jj'\rangle\langle jj'|_{\alpha\alpha'} \otimes \tau_{K_1^h K_2 R K_{1, j\min}^{\text{mask}} \dots K_{1, m}^{\text{mask}}} \otimes \tilde{\tau}_{\tilde{\theta}_{j\max} \dots \tilde{\theta}_m \tilde{\theta}'_{j\max} \dots \tilde{\theta}'_m} \otimes \rho_E, \quad (57)$$

where  $L = \alpha\alpha'$  and  $S$  refer to the secrets.

The ideal output state in the intermediate sessions contains the secret key variables  $K_A K_B$ , the decision labels  $F_A F_B$  which also doubles as authentication success/failure indicators, and  $LSE$ . Following the argument in Sec. C.3, we can analyse the trace distance corresponding to each input state separately. The QAKE security conditions then dictate that the ideal intermediate output state is of the form

$$\begin{aligned} \rho^{\text{ideal}, \text{int}, jj'} = & |\perp\perp\rangle\langle\perp\perp|_{K_A K_B} \otimes \left[ |0\phi\rangle\langle 0\phi|_{F_A F_B} \otimes \sum_{\tilde{j} \geq j} p_{0\phi, \tilde{j}} \sigma_{LSE}^{0\phi, \tilde{j}+1, j'} + |\phi 0\rangle\langle \phi 0|_{F_A F_B} \otimes \sum_{\tilde{j}' \geq j'} p_{\phi 0, \tilde{j}'} \sigma_{LSE}^{\phi 0, \tilde{j}', j'+1} \right. \\ & \left. + |00\rangle\langle 00|_{F_A F_B} \otimes \sum_{\tilde{j} \geq j, \tilde{j}' \geq j'} p_{00, \tilde{j}\tilde{j}'} \sigma_{LSE}^{00, \tilde{j}+1, \tilde{j}'+1} \right] + |01, \perp\rangle\langle 01, \perp|_{F_A F_B K_A} \otimes \tau_{K_B} \otimes \sum_{\tilde{j} \geq \max\{j, j'\}} p_{01, \tilde{j}} \sigma_{LSE}^{01, \tilde{j}+1, \tilde{j}} \\ & + |11\rangle\langle 11|_{F_A F_B} \otimes \tilde{\tau}_{K_A K_B} \otimes \sum_{\tilde{j} \geq \max\{j, j'\}} p_{11, \tilde{j}} \sigma_{LSE}^{11, \tilde{j}\tilde{j}}, \end{aligned} \quad (58)$$

where  $\sigma_{LSE}^{f_A f_B, jj'} \in \mathcal{S}_{in}$ , matching Eqn. (31). Conditions 1 and 3 in Thm. 1 are trivially satisfied by observation, allowing us to focus on the single-session security for a single component, with overall security  $\varepsilon_{\text{sec}}$ .

We can summarise the security of the protocol as

**Theorem 20.** Consider a QAKE protocol with PRNG basis choice  $\mathcal{P}$ , where the adversary is limited by resource  $t$  and the PRNG selected is  $(t', \varepsilon_{\text{PRNG}})$ -quantum-secure with  $t' \geq 2(t + t_{MG}) + t_{ex}$  and  $t' \geq t + t_{SG, PR}$ . The protocol is  $\left( \frac{1}{|\mathcal{T}_{AV}|} + \frac{1}{|\mathcal{T}_{BV}|}, \varepsilon_{\text{MAC}, 2}, \varepsilon'_{\text{KS}} + \varepsilon_{\mathcal{P}'}, \varepsilon'_{SP, 10, 11} + \varepsilon_{\hat{\theta}, \text{PRNG}} + \varepsilon_{\mathcal{P}'} \right)$ -secure. The penalty associated with

shifting to an idealised protocol  $\mathcal{P}'$  is

$$\varepsilon_{\mathcal{P}'} = 2(\varepsilon_{\text{MAC},1} + \varepsilon_{\hat{\theta},\text{PRNG}} + \varepsilon_{\text{MAC},2} + \varepsilon_{\text{ds}}),$$

where  $\varepsilon_{\text{ds}}$  accounts for errors associated with decoy state analysis and  $\varepsilon_{\hat{\theta},\text{PRNG}}$  is the error associated with guessing the basis generation seed  $\hat{\theta}$ . The key secrecy parameter for the idealised protocol is

$$\varepsilon'_{\text{KS}} = 4\varepsilon_{\text{sm}} + 2^{-\frac{1}{2}[N_{P_2,1}^{\text{tol}} - N_{P_2,1}^{\text{tol}} h_{\text{bin}}(e'_{\text{ph,tol}}) - 2 - \log_2 |\mathcal{T}_{\text{AV}}| |\mathcal{T}_{\text{BV}}| - \text{leak}_{\text{EC}} - l_{K_B} - l_{\hat{\theta}}]},$$

where  $e'_{\text{ph,tol}}$  is the phase error tolerance inclusive of the correction due to Serfling bound (with error  $\varepsilon_{\text{serf},1}$ ),  $|\mathcal{T}_{\text{AV}}|$  and  $|\mathcal{T}_{\text{BV}}|$  are the size of the respective tags and  $\text{leak}_{\text{EC}}$  is the information leakage from error correction. The shared secrets privacy parameter for the idealised protocol when  $F_B = 1$  is

$$\begin{aligned} \varepsilon'_{\text{SP},10,11} &= 10\varepsilon_{\text{sm}} + 4(\varepsilon_2 + \varepsilon_3) + \varepsilon_{\text{SP,PA}} + \varepsilon_{\text{SP,MAC},1} + \varepsilon_{\text{SP,MAC},2}, \\ \varepsilon_{\text{SP,PA}} &= 2^{-\frac{1}{2}[N_{P_2,1}^{\text{tol}} - N_{P_2,1}^{\text{tol}} h_{\text{bin}}(e'_{\text{ph,tol}}) - \text{leak}_{\text{EC}} - \log_2 |\mathcal{T}_{\text{AV}}| |\mathcal{T}_{\text{BV}}| - l_{K_B} - l_{\hat{\theta}}]} \\ \varepsilon_{\text{SP,MAC},1} &= \sqrt{(|\mathcal{T}_{\text{AV}}| \varepsilon_{\text{MAC},1} - 1) + 2^{\log_2 \left( \frac{2}{\varepsilon_3} + 1 \right) + \text{leak}_{\text{EC}} + 2 + \log_2 |\mathcal{T}_{\text{AV}}| - N_{P_2,1}^{\text{tol}} [1 - h_{\text{bin}}(e'_{\text{ph,tol}})]}} \\ \varepsilon_{\text{SP,MAC},2} &= \sqrt{(|\mathcal{T}_{\text{BV}}| \varepsilon_{\text{MAC},2} - 1) + 2^{\log_2 \left( \frac{2}{\varepsilon_2} + 1 \right) + \text{leak}_{\text{EC}} + 2 + \log_2 |\mathcal{T}_{\text{AV}}| |\mathcal{T}_{\text{BV}}| - N_{P_2,1}^{\text{tol}} [1 - h_{\text{bin}}(e'_{\text{ph,tol}})]}} \end{aligned}$$

the associated smoothing parameter is

$$\varepsilon_{\text{sm}} = \sqrt{2(2\varepsilon_{\text{IRNG}} + \varepsilon_{\text{PRNG}} + \varepsilon_{\text{serf},1})},$$

and where  $\varepsilon_{\text{IRNG}}$  is the statistical error associated with estimating the bit-phase error gap with an ideal RNG,  $N_{P_2,1}^{\text{tol}}$  is the minimum tolerated number of single-photon rounds in set  $P_2$ , and  $\varepsilon_2$  and  $\varepsilon_3$  are parameters to optimise over.

*Sketch Proof.* Thm. 21 and Thm. 22 bounds the explicit entity authentication and match security respectively. They follow closely the proofs of Thm. 9 and Thm. 10, with the main difference being that no oracle access to generate  $T_{\text{AV}}$ .

Similar to QAKE security, the authentication steps can be used to guarantee ideal features. In Thm. 23, we show that  $D_{\text{PE}}$ ,  $F_B$  and  $D_{\text{BV}}$  can be changed to their idealised versions, with some small penalty. This reduces the analysis for key secrecy to a QKD analysis in Thm. 24, and the corresponding QKD scheme with pseudorandom basis choice is analysed in Appendix E.

Similar to the original QAKE, shared secrets privacy when keys are not generated result in no secrets being leaked or the secret leaked, namely the basis generation seed  $\tilde{\theta}_\beta$ , is no longer utilised due to labels being updated. Notably, the use of basis generation seed  $\tilde{\theta}_{\beta'}$  as a response provide additional security since Alice do not reveal  $T_{\text{AV}}$  when the basis generation seed it receives does not match her own. This results in an output state in  $\mathcal{S}'_{\text{out}}$ , as presented in Thm. 26 and Thm. 27. When keys are generated, the parameter estimation passing ensures  $X_{P_2}$  has sufficient min-entropy such that  $T_{\text{AV}}$  and  $T_{\text{BV}}$  leak minimal information on the authentication and masking key while also refreshing the basis generation seed  $\tilde{\theta}_\beta$ . This is presented in Thm. 28.  $\square$

We note that while the overall security parameters  $\varepsilon_{\text{sec}}$  and  $\varepsilon_{\text{sec,int}}$  can be determined by a sum of the respective security parameters, the bound can be tightened due to overlapping considerations for different security conditions. For instance, the secret key generation and label update hashes  $X_{P_2,r}$  and outputs both the key  $K_A$  and the updated basis string  $\tilde{\theta}_\beta$ . As such, in the analysis of both key secrecy and shared secrets privacy, the same security consideration with penalty term relating to smooth min-entropy of  $X_{P_2,r}$  is included.

#### D.2.1 Explicit Entity Authentication

The explicit entity authentication security condition looks at the probability of  $(F_A, F_B) \in \{(1, \phi), (\phi, 1), (1, 0)\}$ .

**Theorem 21.** Consider the QAKE protocol  $\mathcal{P}$  with adversary resource limit  $t$  and a  $(t', \varepsilon_{\text{PRNG}})$ -quantum-secure PRNG. The full explicit entity authentication security parameter is

$$\varepsilon_{\text{EA,f}} = \frac{\Pr[F_B \neq 1]}{|\mathcal{T}_{\text{BV}}|}.$$

and the almost-full explicit entity authentication security parameter is

$$\varepsilon_{\text{EA,af}} = \frac{\Pr[F_A = \phi]}{|\mathcal{T}_{\text{AV}}|}.$$

*Proof.* We begin with the case of full explicit authentication, which is defined with  $\Pr[F_A = 1, F_B = \phi] + \Pr[F_A = 1, F_B = 0]$ . Using the same analysis as in Thm. 9, we can use the fact that  $K_2$  remains private to show that  $\varepsilon_{\text{EA,f}} = \frac{\Pr[F_B \neq 1]}{|\mathcal{T}_{\text{BV}}|}$ .

For almost-full explicit authentication, Alice does not participate in the protocol,  $F_A = \phi$ . We can follow the analysis of Thm. 9, but with some simplification. To obtain a result of  $F_B = 1$ , Bob needs to successfully validate Alice by checking if  $\tilde{T}_{\text{AV}} = T_{\text{AV},r}$ , where  $T_{\text{AV},r}$  has to be chosen by the adversary. Suppose a worse case where a message  $M$  can be known to the adversary. Since  $(K_1^h, K_{1,\beta'}^{\text{mask}})$  remains private from the adversary, by the uniformity property of a strong 2-universal hash function, we have that

$$\Pr[F_B = 1 | F_A = \phi] \leq \Pr[h_1(K_1^h, M) \oplus K_{1,\beta'}^{\text{mask}} = T_{\text{AV},r}] = \frac{1}{|\mathcal{T}_{\text{AV}}|}. \quad (59)$$

As such,  $\Pr[F_A = \phi, F_B = 1] = \frac{\Pr[F_A = \phi]}{|\mathcal{T}_{\text{AV}}|}$ .  $\square$

### D.2.2 Match Security

**Theorem 22.** Consider the QAKE protocol  $\mathcal{P}$  with adversary resource limit  $t$  and a  $(t', \varepsilon_{\text{PRNG}})$ -quantum-secure PRNG. The match security parameter is

$$\varepsilon_{\text{MS}} = \varepsilon_{\text{MAC},2}.$$

*Proof.* Same as Thm. 10.  $\square$

### D.2.3 Idealised Parameter Estimation and Authentication

To simplify the analysis for some security conditions, we similarly introduce “idealised” versions of the parameter estimation and authentication checks. We first note that the steps are given by:

1. Alice’s state preparation and sending of quantum state.
2. Bob’s measurement and test round announcement, with reply  $P_1, P_2, \tilde{\theta}'_{\beta'}$  and  $X'_{P_1}$ .
3. Alice’s parameter estimation and validation tag generation, sending syndrome  $\text{syn}$  and tag  $T_{\text{AV}}$  to Bob.
4. Bob performs Alice’s validation, and responds with his own validation tag  $T_{\text{BV}}$ .
5. Alice validates Bob’s tag.

The replacement of the decoy state parameter estimation  $D_{\text{PE}}$  to  $\tilde{D}_{\text{PE}}$  and Bob’s validation  $D_{\text{BV}}$  to  $\tilde{D}_{\text{BV}}$  can be performed as described in Sec. C.3.3 and Sec. C.3.4 (note  $\tilde{D}_{\text{BV}}$  has  $\Omega_{4 \rightarrow 5}$  instead). The replacement for Alice’s validation  $F_B$  to  $\tilde{F}_B$  is modified since the steps of the protocol are different, and the announcement of  $\tilde{\theta}_\beta$  can provide additional authentication ability. We define instead

$$\tilde{F}_B = \begin{cases} 1 & \beta = \beta', D_{\text{PE}} = 1, T_{\text{AV}} = T_{\text{AV},r}, \\ & M_{\text{AV}} = M'_{\text{AV}}, \Omega_{2 \rightarrow 3 \rightarrow 4} \\ 0 & \text{otherwise} \end{cases}. \quad (60)$$

**Theorem 23.** Let  $\mathcal{P}$  be the protocol and  $\mathcal{P}'$  be the idealised protocol (with  $D_{\text{PE}}, F_B, D_{\text{BV}}$  replaced with  $\tilde{D}_{\text{PE}}, \tilde{F}_B$  and  $\tilde{D}_{\text{BV}}$ ). Then, for any  $\sigma_{\text{LSE}} \in \mathcal{S}_{\text{in}}$ ,

$$\Delta(\mathcal{P}(\sigma_{\text{LSE}}), \mathcal{P}'(\sigma_{\text{LSE}})) \leq 2(\varepsilon_{\text{MAC},1} + \varepsilon_{\tilde{\theta}, \text{PRNG}}) + 2\varepsilon_{\text{MAC},2} + 2\varepsilon_{\text{ds}},$$

where  $\varepsilon_{\tilde{\theta}, \text{PRNG}}$  is the probability of guessing the basis generation seed.

*Proof.* Since  $(K_1^h, K_{1,\beta'}^{\text{mask}})$  is always private, we can follow the same argument in Thm. 12 to show

$$\begin{aligned} \Pr[F_B = 1, \tilde{F}_B = 0] &\leq \varepsilon_{\text{MAC},1} + \Pr[F_B = 1, D_{\text{PE}} = 1, \Omega_{3 \rightarrow 4}, \beta = \beta', M_{\text{AV}} = M'_{\text{AV}}, T_{\text{AV}} = T_{\text{AV},r}, \Omega_{2 \rightarrow 3}^c] \\ &\leq \varepsilon_{\text{MAC},1} + \Pr[D_{\text{PE}} = 1, \beta = \beta', \Omega_{2 \rightarrow 3}^c] \\ &\leq \varepsilon_{\text{MAC},1} + p_{\text{guess}}(\tilde{\theta}_\beta), \end{aligned} \quad (61)$$

where the first inequality uses the expansion in Eqn. (39) with the first three terms bounded by  $\varepsilon_{\text{MAC},1}$ , while the remaining term relates to step ordering. The third inequality simplifies the probability to a guessing probability since  $\tilde{\theta}_\beta$  has to be matched for  $D_{\text{PE}} = 1$ , and this has to take place for  $\beta = \beta'$  ( $\tilde{\theta}_{\beta'}$  not leaked to adversary prior to the session) and before Bob announces  $\tilde{\theta}_\beta$  in step 2. The guessing probability of  $\tilde{\theta}_\beta$  can be computed, since it is only utilised to generate the quantum state in the first session. For a given choice of parameter with  $p_{\geq 2}$  probability of multi-photon events which we assume in the worst case would provide  $\theta_i$  to the adversary, then given a  $(t', \varepsilon_{\text{PRNG}})$ -quantum secure PRNG with  $t' \geq t + t_{\text{SG},PR}$  and  $2l_{\tilde{\theta}} < n_{\text{rnd}}$ , by Thm. 6, the probability of guessing  $\tilde{\theta}_\beta$  is bounded by  $\varepsilon_{\tilde{\theta},\text{PRNG}} = \varepsilon_{\text{PRNG}} + 2^{-n_{\text{rnd}} + l_{\tilde{\theta}}}$ , where  $n_{\text{rnd}}$  is the number of signals sent. As such, these changes result in a similar penalty to the trace distance, with a penalty of  $2(\varepsilon_{\text{MAC},1} + \varepsilon_{\tilde{\theta},\text{PRNG}}) + 2\varepsilon_{\text{MAC},2} + 2\varepsilon_{\text{ds}}$ .  $\square$

#### D.2.4 Key Secrecy

Key secrecy analyses the two specific cases where  $K_B$  generates a key,  $(F_A, F_B) \in \{01, 11\}$ . Instead of having the security relying on the secrecy condition of decoy-state BB84 like in the original QAKE protocol, it relies on the secrecy condition of decoy-state BB84 with shared pseudorandom basis in Appendix E.3.

**Theorem 24.** *Consider the QAKE protocol  $\mathcal{P}$  with adversary resource limit  $t$  and a  $(t', \varepsilon_{\text{PRNG}})$ -quantum-secure PRNG. Then, the key secrecy security parameter is*

$$\varepsilon_{\text{KS}} = \varepsilon'_{\text{KS}} + 2(\varepsilon_{\text{MAC},1} + \varepsilon_{\tilde{\theta},\text{PRNG}}) + 2\varepsilon_{\text{MAC},2} + 2\varepsilon_{\text{ds}} \quad (62)$$

where

$$\begin{aligned} \varepsilon'_{\text{KS}} &= 4\varepsilon_{\text{sm}} + 2^{-\frac{1}{2}[N_{P_2,1}^{\text{tol}} - N_{P_2,1}^{\text{tol}} h_{\text{bin}}(e'_{\text{ph,tol}}) - 2 - \log_2 |\tilde{T}_{\text{AV}}| |\tilde{T}_{\text{BV}}| - \text{leak}_{\text{EC}} - l_{K_B} - l_{\tilde{\theta}}]} \\ \varepsilon_{\text{sm}} &= \sqrt{2(2\varepsilon_{\text{IRNG}} + \varepsilon_{\text{PRNG}} + \varepsilon_{\text{serf},1})} \end{aligned}$$

is the key secrecy of the idealised protocol  $\mathcal{P}'$ ,  $\varepsilon_{\tilde{\theta},\text{PRNG}}$  is the error associated with guessing the basis generation seed  $\tilde{\theta}$ ,  $e'_{\text{ph,tol}}$  is the error tolerance inclusive of the correction due to Serfling bound.

*Proof.* From Thm. 23, we can swap to an idealised version of the protocol  $\mathcal{P}'$  with penalty  $2(\varepsilon_{\text{ds}} + \varepsilon_{\text{MAC},1} + \varepsilon_{\tilde{\theta},\text{PRNG}} + \varepsilon_{\text{MAC},2})$ . Following the argument of Thm. 14, by reversing the final step of Alice, we can combine the cases of  $(\tilde{F}_A, \tilde{F}_B) = (0, 1), (1, 1)$  into a single case, giving

$$\Delta(\rho'_{\tilde{F}_A \tilde{F}_B K_B LSE \wedge (\tilde{F}_A, \tilde{F}_B) \in \{01, 11\}}, \tau_{K_B} \otimes \rho'_{\tilde{F}_A \tilde{F}_B LSE \wedge (\tilde{F}_A, \tilde{F}_B) \in \{01, 11\}}) \leq \Delta(\rho'_{K_B L' S' E \wedge \tilde{F}_B = 1}, \tau_{K_B} \otimes \rho'_{L' S' E \wedge \tilde{F}_B = 1}). \quad (63)$$

With the removal of  $\tilde{F}_A$ , we can provide a key secrecy security parameter for  $\mathcal{P}'$ .

Let us first note that  $\tilde{\theta}_\beta$  is refreshed during key generation, and we label the original value before refresh as  $\tilde{\theta}_\beta^{\text{in}}$  for clarity. We follow a similar analysis as Thm. 15 and we first define  $\tilde{\Omega}_{\text{PE}}$  to be the event where parameter estimation checks  $N_{P_1,1} \geq N_{P_1,1}^{\text{tol}}$ ,  $N_{P_2,1} \geq N_{P_2,1}^{\text{tol}}$ ,  $\frac{wt(X_{P_1,1} \oplus X'_{P_1,1})}{N_{P_1,1}} \leq e_{\text{bit},1,\text{tol}}$  are successful, for which the actual  $P_1$  and  $P_2$  sets are utilised. Due to the condition of  $(P_1, P_2, X'_{P_1}) = (P_{1,r}, P_{2,r}, X'_{P_{1,r}})$ , when  $F_B = 1$ ,  $\rho_{\wedge F_B=1 \wedge \Omega_{\text{PE}}} = \rho_{\wedge F_B=1 \wedge \tilde{\Omega}_{\text{PE}}}$ . Let us define  $\tilde{L}' = L' \setminus \tilde{\theta}_\beta$ , where the refreshed  $\tilde{\theta}_\beta$  has to be uniformly independent as well (part of shared secret privacy). Noting that  $h_{\text{PA}}$  is 2-universal, we bound the trace distance using the quantum leftover hash lemma [38, 41],

$$\begin{aligned} &\Delta(\rho'_{K_B L' S' E' \wedge \tilde{F}_B = 1}, \tau_{K_B} \otimes \rho'_{L' S' E' \wedge \tilde{F}_B = 1}) \\ &\leq 2p_{\tilde{\Omega}_{\text{PE}}} \Delta(\rho'_{K_B \tilde{\theta}_\beta \tilde{L}' S' E' \wedge \tilde{F}_B = 1 | \tilde{\Omega}_{\text{PE}}}, \tau_{K_B \tilde{\theta}_\beta} \otimes \rho'_{\tilde{L}' S' E' \wedge \tilde{F}_B = 1 | \tilde{\Omega}_{\text{PE}}}) \\ &\leq p_{\tilde{\Omega}_{\text{PE}}} \left\{ 4\varepsilon_{\text{sm},1} + 2^{-\frac{1}{2}[H_{\min}^{\varepsilon_{\text{sm},1}}(\tilde{X}_{P_2,r} | L' S'' E) - \rho'_{\tilde{X}_{P_2,r} L' S'' E \wedge \tilde{F}_B = 1 | \tilde{\Omega}_{\text{PE}}} - l_{K_B} - l_{\tilde{\theta}}]} \right\}, \end{aligned} \quad (64)$$

where  $S'' = S' \setminus R$ , and the first inequality uses the property  $\Delta(\rho_{ABC}, \tau_A \otimes \rho_{BC}) \leq 2\Delta(\rho_{ABC}, \tau_{AB} \otimes \rho_C)$ .  $L'$  is simply equal values of  $\beta$  and  $\beta'$  since  $\tilde{F}_B = 1$  leaves it unchanged and the step updating  $\beta$  (Alice's final step) has been removed.  $S''$  includes  $K_1^h$ ,  $K_2$ ,  $\{\tilde{\theta}_i\}_i$ , and  $\{K_{1,i}^{\text{mask}}\}_i$ . We note that any  $\tilde{\theta}_i$  and  $K_{1,i}^{\text{mask}}$  secrets for  $i < \beta$  along with  $\tilde{\theta}_\beta^{\text{in}}$  would be part of  $E'$  (either announced or not required to remain secret) and those for  $i > \beta$

would be independent of  $\hat{X}_{P_2,r}$  since they are not utilised in the protocol yet. As such, following the arguments in the proof of Thm. 15, we can simplify

$$\begin{aligned}
& H_{\min}^{\varepsilon_{\text{sm},1}}(\hat{X}_{P_2,r} | L' S'' E)_{\rho_{\hat{X}_{P_2,r} L' S'' E \wedge \tilde{F}_B=1 | \tilde{\Omega}_{\text{PE}}}}^{\prime \text{out}, jj'} \\
&= H_{\min}^{\varepsilon_{\text{sm},1}}(\hat{X}_{P_2,r} | \beta K_1^h K_2 K_{1,\beta}^{\text{mask}} E)_{\rho_{\hat{X}_{P_2,r} K_1^h K_2 K_{1,\beta}^{\text{mask}} E \wedge \tilde{F}_B=1 | \tilde{\Omega}_{\text{PE}}}}^{\prime \text{out}, jj'} \\
&\geq H_{\min}^{\varepsilon_{\text{sm},1}}(X_{P_2} | \beta P_1 P_2 X'_{P_1} \tilde{\theta}_\beta^{\text{in}} E_2)_{\rho_{\beta X_{P_2} P_1 P_2 X'_{P_1} \tilde{\theta}_\beta^{\text{in}} E_2 | \tilde{\Omega}_{\text{PE}}}}^{\prime \text{out}, jj'} - 2 - \log_2 |\mathcal{T}_{\text{BV}}| |\mathcal{T}_{\text{AV}}| - \text{leak}_{\text{EC}}.
\end{aligned} \tag{65}$$

The quantum state  $\rho_{\beta X_{P_2} E_2 P_1 P_2 X'_{P_1} \tilde{\theta}_\beta^{\text{in}} | \tilde{\Omega}_{\text{PE}}}^{\prime \text{out}, jj'}$  can be viewed as being generated from a protocol matching that in Thm. 32. Since the chosen PRNG has  $t' \geq 2(t + t_{MG}) + t_{ex}$ , we can apply Thm. 32 and bound the min-entropy of interest,

$$H_{\min}^{\varepsilon_{\text{sm},1}}(X_{P_2} | \beta P_1 P_2 \tilde{\theta}_\beta X'_{P_1} E_2)_{\rho_{\beta P_1 P_2 \tilde{\theta}_\beta X'_{P_1} E_2 | \tilde{\Omega}_{\text{PE}}}}^{\prime \text{out}, jj'} \geq N_{P_2,1}^{\text{tol}} - N_{P_2,1}^{\text{tol}} h_{\text{bin}}(e'_{\text{ph,tol}}), \tag{66}$$

where  $\varepsilon_{\text{sm},1} \geq \sqrt{2\varepsilon_{\text{ph}}}$ ,

$$\varepsilon_{\text{ph}} = 2\varepsilon_{\text{IRNG}} + \frac{\varepsilon_{\text{PRNG}}}{p_{\tilde{\Omega}_{\text{PE}}}^2} + \varepsilon_{\text{serf},1} \tag{67}$$

and phase error tolerance

$$e'_{\text{ph,tol}} = e_{\text{bit},1,\text{tol}} + g(N_{P_1,1}^{\text{tol}}, N_{P_2,1}^{\text{tol}}, \varepsilon_{\text{serf},1}) + 2\sqrt{\frac{2}{N_{P_2,1}^{\text{tol}}} \ln \frac{1}{\varepsilon_{\text{IRNG}}}}, \tag{68}$$

from the EUR analysis. Combining the results, we have that  $\varepsilon_{\text{sm},1} = \sqrt{2\left(2\varepsilon_{\text{IRNG}} + \frac{\varepsilon_{\text{PRNG}}}{p_{\tilde{\Omega}_{\text{PE}}}^2} + \varepsilon_{\text{serf},1}\right)}$  and

$$H_{\min}^{\varepsilon_{\text{sm},1}}(\hat{X}_{P_2,r} | \beta K_1^h K_2 K_{1,\beta}^{\text{mask}} E)_{\rho_{\hat{X}_{P_2,r} \wedge \tilde{F}_B=1 | \tilde{\Omega}_{\text{PE}}}}^{\prime \text{out}, jj'} \geq N_{P_2,1}^{\text{tol}} - N_{P_2,1}^{\text{tol}} h_{\text{bin}}(e'_{\text{ph,tol}}) - \text{leak}_{\text{EC}} - \log_2 |\mathcal{T}_{\text{AV}}| |\mathcal{T}_{\text{BV}}| - 2. \tag{69}$$

□

#### D.2.5 Shared Secrets Privacy

The final security parameter is the shared secrets privacy condition, which can be summarised as

**Theorem 25.** *Consider the QAKE protocol  $\mathcal{P}$  with adversary resource limit  $t$  and a  $(t', \varepsilon_{\text{PRNG}})$ -quantum-secure PRNG. Then, the shared secrets privacy security condition satisfies*

$$\varepsilon_{\text{SP}} = \varepsilon'_{\text{SP},10,11} + \varepsilon_{\hat{\theta},\text{PRNG}} + 2(\varepsilon_{\text{MAC},1} + \varepsilon_{\hat{\theta},\text{PRNG}} + \varepsilon_{\text{MAC},2} + \varepsilon_{\text{ds}}),$$

where

$$\begin{aligned}
\varepsilon'_{\text{SP},10,11} &= 10\varepsilon_{\text{sm}} + 4(\varepsilon_2 + \varepsilon_3) + \varepsilon_{\text{SP,PA}} + \varepsilon_{\text{SP,MAC},1} + \varepsilon_{\text{SP,MAC},2}, \\
\varepsilon_{\text{sm}} &= \sqrt{2(2\varepsilon_{\text{IRNG}} + \varepsilon_{\text{PRNG}} + \varepsilon_{\text{serf},1})} \\
\varepsilon_{\text{SP,PA}} &= 2^{-\frac{1}{2}} [N_{P_2,1}^{\text{tol}} - N_{P_2,1}^{\text{tol}} h_{\text{bin}}(e'_{\text{ph,tol}}) - \text{leak}_{\text{EC}} - \log_2 |\mathcal{T}_{\text{AV}}| |\mathcal{T}_{\text{BV}}| - l_{K_B} - l_{\hat{\theta}}] \\
\varepsilon_{\text{SP,MAC},1} &= \sqrt{(|\mathcal{T}_{\text{AV}}| \varepsilon_{\text{MAC},1} - 1) + 2^{\log_2 \left(\frac{2}{\varepsilon_3} + 1\right) + \text{leak}_{\text{EC}} + 2 + \log_2 |\mathcal{T}_{\text{AV}}| - N_{P_2,1}^{\text{tol}} [1 - h_{\text{bin}}(e'_{\text{ph,tol}})]}} \\
\varepsilon_{\text{SP,MAC},2} &= \sqrt{(|\mathcal{T}_{\text{BV}}| \varepsilon_{\text{MAC},2} - 1) + 2^{\log_2 \left(\frac{2}{\varepsilon_2} + 1\right) + \text{leak}_{\text{EC}} + 2 + \log_2 |\mathcal{T}_{\text{AV}}| |\mathcal{T}_{\text{BV}}| - N_{P_2,1}^{\text{tol}} [1 - h_{\text{bin}}(e'_{\text{ph,tol}})]}}
\end{aligned}$$

is the shared secrets privacy parameter for idealised protocol  $\mathcal{P}'$  for cases where  $F_B = 1$ .

*Proof.* For simplicity, we perform a swap to an “idealised” version of the protocol  $\mathcal{P}'$  by replacing  $F_B$ ,  $D_{\text{BV}}$  and  $D_{\text{PE}}$ , resulting in a trace distance penalty of  $2(\varepsilon_{\text{ds}} + \varepsilon_{\text{MAC},1} + \varepsilon_{\hat{\theta},\text{PRNG}} + \varepsilon_{\text{MAC},2})$ . To simplify, we shall examine the components of the sum over  $(\tilde{F}_A, \tilde{F}_B)$  separately, noting the exclusion of  $(\phi, 1)$ ,  $(1, \phi)$  and  $(1, 0)$  events. Thm. 26 shows that the trace distance is 0 in the  $(\phi, 0)$  case. In cases where  $F_A = 0$ , Thm. 27 shows that the trace distance is bounded by  $\varepsilon_{\hat{\theta},\text{PRNG}}$ . The final theorem, Thm. 28, shows the trace distance bound for the remaining cases where  $F_B = 1$ . When combined, the trace distance bound is as presented in the theorem. □

We recall that the input state in  $\mathcal{S}_{in}$  is of the form

$$\rho_{LSE}^{in,jj'} = |jj'\rangle\langle jj'|_{\alpha\alpha'} \otimes \tau_{K_1^h K_2 R K_{1,j_{\min}}^{\text{mask}} \dots K_{1,m}^{\text{mask}}} \otimes \tilde{\tau}_{\tilde{\theta}_{j_{\max}} \dots \tilde{\theta}_m \tilde{\theta}'_{j_{\max}} \dots \tilde{\theta}'_m} \otimes \rho_E, \quad (70)$$

with  $j_{\min} = \min\{j, j'\}$  and  $j_{\max} = \max\{j, j'\}$ . For the case of  $(\tilde{F}_A, \tilde{F}_B) = (\phi, 0)$ , the trace distance is simply 0,

**Theorem 26.** *Consider the QAKE protocol  $\mathcal{P}'$ . Then, there exists  $\sigma_{LSE}^{\phi, jj'} \in \mathcal{S}_{in}$  such that*

$$\Delta \left( p_{\phi 0}^{\text{real}} \rho_{LSE|(\tilde{F}_A, \tilde{F}_B)=\phi 0}^{\text{'out}, jj'}, \sum_{\tilde{j}' \geq j'} p_{\phi 0, \tilde{j}} \sigma_{LSE}^{\phi 0, j, \tilde{j}'+1} \right) = 0.$$

*Proof.* We start by splitting the trace distance based on  $\tilde{j}'$ ,

$$\Delta \left( p_{\phi 0}^{\text{real}} \rho_{LSE|(\tilde{F}_A, \tilde{F}_B)=\phi 0}^{\text{'out}, jj'}, \sum_{\tilde{j}' \geq j'} p_{\phi 0, \tilde{j}} \sigma_{LSE}^{\phi 0, j, \tilde{j}'+1} \right) \leq \sum_{\tilde{j}' \geq j'} p_{\phi 0, \tilde{j}} \Delta \left( \rho_{LSE|(\tilde{F}_A, \tilde{F}_B)=\phi 0, \beta'=\tilde{j}'}^{\text{'out}, jj'}, \sigma_{LSE}^{\phi 0, j, \tilde{j}'+1} \right), \quad (71)$$

noting that  $\beta' < j'$  is not possible (by definition of  $\beta'$ ), allowing us to analyse the trace distance separately for each  $\tilde{j}'$  selection.

When  $\tilde{F}_A = \phi$ ,  $\tilde{F}_B = 0$ , the only steps that are relevant are Bob's measurement, test round announcement and Alice validation. Since Alice validation failure stems from simply  $T_{AV} = \perp$ , these steps do not utilise shared secrets  $K_2$ ,  $K_1^h$ ,  $K_{1,j'}^{\text{mask}}$ , and  $R$ , which remain private from the adversary. We note that the protocol would implicitly trace out  $K_{[\min\{j-1, j'-1\}, \min\{j-1, \tilde{j}'\}]}^{\text{mask}}$  since these would no longer be available for use at later steps, and what remains to show is that  $\tilde{\theta}_{[\tilde{j}_{\max}, m]} \tilde{\theta}'_{[\tilde{j}_{\max}, m]}$  remains private. It is clear that the basis generation seed  $\tilde{\theta}'_{\tilde{j}'}$  is utilised during Bob's measurement step. However, since Bob's index is updated to  $\tilde{j}' + 1$ , leakage (even fully) of  $\tilde{\theta}'_{\tilde{j}'}$ , would still allow it to match the form of the ideal state since these are allowed to be part of  $E$  when  $\tilde{j}_{\max} > \tilde{j}'$ . Therefore, the output state can match the ideal output state (i.e. there exists  $\sigma_{LSE}^{\phi 0, j, \tilde{j}'+1} \in \mathcal{S}_{in}$  which matches the output state), and the resulting trace distance is zero.  $\square$

The cases of  $(\tilde{F}_A, \tilde{F}_B) = (0, \phi)$  and  $\tilde{F}_A = \tilde{F}_B = 0$  cases are considered together. In both cases, the risk of leakage is due to the possibility of announcement of the tag  $T_{AV}$  by Alice, though this occurs with low probability.

**Theorem 27.** *Consider the QAKE protocol  $\mathcal{P}'$  with adversary resource limit  $t$  and a  $(t', \varepsilon_{\text{PRNG}})$ -quantum-secure PRNG. Then, there exists  $\sigma_{LSE}^{\phi 0, jj'}, \sigma_{LSE}^{00, jj'} \in \mathcal{S}_{in}$  such that*

$$\Delta \left( p_{0\phi}^{\text{real}} \rho_{LSE|(\tilde{F}_A, \tilde{F}_B)=0\phi}^{\text{'out}, jj'} + p_{00}^{\text{real}} \rho_{LSE|(\tilde{F}_A, \tilde{F}_B)=00}^{\text{'out}, jj'}, \sum_{\tilde{j} \geq j} p_{0\phi, \tilde{j}} \sigma_{LSE}^{0\phi, \tilde{j}+1, j'} + \sum_{\tilde{j} \geq j, \tilde{j}' \geq j'} p_{00, \tilde{j}\tilde{j}'} \sigma_{LSE}^{00, \tilde{j}+1, \tilde{j}'+1} \right) \leq \varepsilon_{\hat{\theta}, \text{PRNG}}.$$

*Proof.* We can split the trace distance according to the  $\tilde{j}$  and  $\tilde{j}'$  values,

$$\sum_{\tilde{j} \geq j} p_{0\phi, \tilde{j}} \Delta \left( \rho_{LSE|(\tilde{F}_A, \tilde{F}_B)=0\phi, \beta=\tilde{j}}^{\text{'out}, jj'}, \sigma_{LSE}^{0\phi, \tilde{j}+1, j'} \right) + \sum_{\tilde{j} \geq j, \tilde{j}' \geq j'} p_{00, \tilde{j}\tilde{j}'} \Delta \left( \rho_{LSE|(\tilde{F}_A, \tilde{F}_B)=00, (\beta, \beta')=\tilde{j}\tilde{j}'}^{\text{'out}, jj'}, \sigma_{LSE}^{00, \tilde{j}+1, \tilde{j}'+1} \right),$$

and evaluate the individual terms instead. For any  $\tilde{j}$  and  $\tilde{j}'$ , the secrets  $R$  and  $K_2$  remain secure since they are not utilised when  $\tilde{F}_A = 0$  and  $\tilde{F}_B \neq 1$ , which leaves the secrecy of  $K_1^h$ ,  $K_{1,j}^{\text{mask}}$  and  $\tilde{\theta}$  to examine.

Due to possible differences in the adversary's information (based on input state) when  $\tilde{j}$  and  $\tilde{j}'$  are mismatched, we further split the analysis into three scenarios: (1)  $\tilde{j}' > \tilde{j}$ , (2)  $\tilde{j}' < \tilde{j}$  and (3)  $\tilde{j}' = \tilde{j}$ . We note that  $\tilde{j}' = j'$  in the case where  $\tilde{F}_B = \phi$ .

In case (1), it is clear that any attempt to learn  $\tilde{\theta}_{\tilde{j}'}$ , would not impact shared secrets privacy since it is either not utilised (when  $\tilde{F}_B = \phi$ ) or no longer have to be private (when  $\tilde{F}_B = 0$ , since updated index is  $\tilde{j}' + 1$ ). As such, what remains is  $K_1^h$  and  $K_{1,\tilde{j}}^{\text{mask}}$ , which if  $\tilde{D}_{\text{PE}} = 0$ , would not be leaked since  $T_{AV}$  is not announced. However, a worse case one can consider when  $\tilde{j}' > \tilde{j}$  is that  $\tilde{\theta}_{\tilde{j}}$  can be known to the adversary (input state

does not guarantee privacy of  $\tilde{\theta}_{\tilde{j}}$  when  $\tilde{j} < j'$ ). Having the basis information allows the adversary to easily pass parameter estimation,  $\tilde{D}_{\text{PE}} = 1$ , by simulating an honest Bob that measures with basis generated from basis seed  $\tilde{\theta}_{\tilde{j}}$ . In such a scenario, the syndrome  $\text{syn}$  and tag  $T_{\text{AV}}$  would be announced by Alice, which may compromise shared secrets  $K_1^h$  and  $K_{1,\tilde{j}}^{\text{mask}}$ . Since  $\tilde{F}_A = 0$ , and  $\tilde{j} < \tilde{j}'$ , the updated index at the end of the protocol gives  $j_{\min} = \tilde{j} + 1$ , which implies that  $K_{1,\tilde{j}}^{\text{mask}}$  is traced away. From Thm. 4, and noting that  $\tilde{D}_{\text{BV}}$  has no relation to  $K_1^h$ , the shared secret  $K_1^h$  remains secure from the adversary. As such, the trace distance in this case is simply 0 since the output state is ideal.

In case (2), similarly, any attempt to learn  $\tilde{\theta}_{\tilde{j}}$  is fruitless since it no longer has to be private at the end of the protocol when  $\tilde{F}_A = 0$ . As such, the focus is on  $K_1^h$  and  $K_{1,\tilde{j}}^{\text{mask}}$ . Here, we notice that unlike the first case,  $\tilde{\theta}_{\tilde{j}}$  is inaccessible to the adversary at the start of the protocol, as guaranteed by the input state since  $\tilde{j} \geq j \geq j_{\max}$ . Without prior knowledge of the basis generation seed, the adversary would have little ability to pass the parameter estimation step. More concretely, it is upper bounded by the probability of providing a matching  $\tilde{\theta}_{\tilde{j}}$  from the generated quantum state alone

$$\Pr[\tilde{D}_{\text{PE}} = 1] \leq \Pr[\hat{\theta} = \tilde{\theta}], \quad (72)$$

which in turn is small. Given that the adversary has access to at most  $t$  resources, by the  $(t', \varepsilon_{\text{PRNG}})$ -quantum secure PRNG property, with  $t' \geq t + t_{\text{SG,PR}}$ , and that  $2l_{\tilde{\theta}} < n_{\text{rnd}}$ , Thm. 6 gives

$$\Pr[\hat{\theta} = \tilde{\theta}] \leq \varepsilon_{\hat{\theta}, \text{PRNG}}, \quad (73)$$

where  $\varepsilon_{\hat{\theta}, \text{PRNG}}$  matches  $\varepsilon_{\text{guess}}$  in the theorem, and noting that only multi-photon events in the quantum states generated by Alice,  $Q$ , can provide information about the pseudorandom basis choice. Additionally, since  $\tilde{D}_{\text{PE}} = 0$  leads to an ideal state, the trace distance term when case (2) occurs is upper bounded by  $\varepsilon_{\hat{\theta}, \text{PRNG}}$ .

In the final case, the  $\tilde{F}_B = 0$  and  $\tilde{F}_B = \phi$  events have to be considered separately. When  $\tilde{F}_B = \phi$ , Bob is not involved in the protocol and thus  $\tilde{\theta}_{\tilde{j}}$  is not accessible to the adversary during the protocol, except from the quantum state  $Q$  sent by Alice. As such, we can follow the argument of case (2), to obtain a bound of  $\varepsilon_{\hat{\theta}, \text{PRNG}}$ . When  $\tilde{F}_B = 0$ , Bob's involvement in the protocol and subsequent announcement of  $\tilde{\theta}_{\tilde{j}}$ , can allow the adversary to pass the parameter estimation checks. Here, since both Alice and Bob's indices are updated and  $j_{\min} = \tilde{j} + 1$ , we can follow the argument of case (1) to get zero trace distance.

Combining the contribution for all  $\tilde{j}$  and  $\tilde{j}'$ , the overall trace distance can be bounded by  $\varepsilon_{\hat{\theta}, \text{PRNG}}$ .  $\square$

Here, we analyse the final two cases of  $(\tilde{F}_A, \tilde{F}_B) \in \{01, 11\}$  jointly since they are similar.

**Theorem 28.** Consider the QAKE protocol  $\mathcal{P}'$  with adversary resource limit  $t$  and a  $(t', \varepsilon_{\text{PRNG}})$ -quantum-secure PRNG. Then, there exists  $\sigma_{LSE}^{01, jj'}, \sigma_{LSE}^{11, jj'} \in \mathcal{S}_{\text{in}}$  such that

$$\Delta \left( p_{01}^{\text{real}} \rho_{LSE|(\tilde{F}_A, \tilde{F}_B)=01}^{\text{'out}, jj'}, \sum_{\tilde{j} \geq \max\{j, j'\}} p_{01, \tilde{j}} \sigma_{LSE}^{01, \tilde{j}+1, \tilde{j}} \right) + \Delta \left( p_{11}^{\text{real}} \rho_{LSE|(\tilde{F}_A, \tilde{F}_B)=11}^{\text{'out}, jj'}, \sum_{\tilde{j} \geq \max\{j, j'\}} p_{11, \tilde{j}} \sigma_{LSE}^{11, \tilde{j}, \tilde{j}} \right) \leq \varepsilon'_{\text{SP}, 01, 11},$$

where

$$\begin{aligned} \varepsilon'_{\text{SP}, 01, 11} = & 10\sqrt{2(\varepsilon_{\text{IRNG}} + \varepsilon_{\text{PRNG}} + \varepsilon_{\text{serf}, 1})} + 4(\varepsilon_2 + \varepsilon_3) + 2^{-\frac{1}{2}[N_{P_2, 1}^{\text{tol}} - N_{P_2, 1}^{\text{tol}} h_{\text{bin}}(e'_{\text{ph}, \text{tol}}) - \text{leak}_{\text{EC}} - \log_2 |\mathcal{T}_{\text{AV}}| |\mathcal{T}_{\text{BV}}| - l_{K_B} - l_{\tilde{\theta}}]} \\ & + \sqrt{(|\mathcal{T}_{\text{AV}}| \varepsilon_{\text{MAC}, 1} - 1) + 2^{\log_2 \left( \frac{2}{\varepsilon_3} + 1 \right) + \text{leak}_{\text{EC}} + 2 + \log_2 |\mathcal{T}_{\text{AV}}| - N_{P_2, 1}^{\text{tol}} [1 - h_{\text{bin}}(e'_{\text{ph}, \text{tol}})]}} \\ & + \sqrt{(|\mathcal{T}_{\text{BV}}| \varepsilon_{\text{MAC}, 2} - 1) + 2^{\log_2 \left( \frac{2}{\varepsilon_2} + 1 \right) + \text{leak}_{\text{EC}} + 2 + \log_2 |\mathcal{T}_{\text{AV}}| |\mathcal{T}_{\text{BV}}| - N_{P_2, 1}^{\text{tol}} [1 - h_{\text{bin}}(e'_{\text{ph}, \text{tol}})]}}, \end{aligned}$$

$\varepsilon_{\hat{\theta}, \text{PRNG}}$  is the error associated with guessing the basis generation seed  $\tilde{\theta}$ ,  $e'_{\text{ph}, \text{tol}}$  is the error tolerance inclusive of the correction due to Serfling bound. If 2-universal hash functions are used, then

$$\begin{aligned} \varepsilon'_{\text{SP}, 01, 11} = & 10\sqrt{2(\varepsilon_{\text{IRNG}} + \varepsilon_{\text{PRNG}} + \varepsilon_{\text{serf}, 1})} + 2^{-\frac{1}{2}[N_{P_2, 1}^{\text{tol}} - N_{P_2, 1}^{\text{tol}} h_{\text{bin}}(e'_{\text{ph}, \text{tol}}) - \text{leak}_{\text{EC}} - \log_2 |\mathcal{T}_{\text{AV}}| |\mathcal{T}_{\text{BV}}| - l_{K_B} - l_{\tilde{\theta}}]} \\ & + 2^{-\frac{1}{2}[N_{P_2, 1}^{\text{tol}} - N_{P_2, 1}^{\text{tol}} h_{\text{bin}}(e'_{\text{ph}, \text{tol}}) - \text{leak}_{\text{EC}} - 2 - \log_2 |\mathcal{T}_{\text{AV}}| |\mathcal{T}_{\text{BV}}|]} \left( 1 + 2^{-\frac{1}{2} \log_2 |\mathcal{T}_{\text{BV}}|} \right). \end{aligned}$$

*Proof.* We begin by explicitly expressing the form of the output state and selected  $\sigma_{LSE}^{01,jj'}$  and  $\sigma_{LSE}^{11,jj'}$  states,

$$\begin{aligned}
p_{01}^{\text{real}} \rho_{LSE|(\tilde{F}_A, \tilde{F}_B)=01}^{\text{'out}, jj'} &= \sum_{\tilde{j} \geq j_{\max}} |\tilde{j}+1, \tilde{j}\rangle\langle\tilde{j}+1, \tilde{j}|_{\alpha\alpha'} \otimes \rho_{K_1^h K_2 R K_{1, [\tilde{j}, m]}^{\text{mask}}}^{\text{'out}, jj'} \tilde{\theta}_{[\tilde{j}+1, m]}' \tilde{\theta}_{[\tilde{j}+1, m]}' E \wedge \tilde{F}_B=1 \wedge \tilde{F}_A=0 \wedge \beta=\tilde{j} \\
p_{11}^{\text{real}} \rho_{LSE|(\tilde{F}_A, \tilde{F}_B)=11}^{\text{'out}, jj'} &= \sum_{\tilde{j} \geq j_{\max}} |\tilde{j}, \tilde{j}\rangle\langle\tilde{j}, \tilde{j}|_{\alpha\alpha'} \otimes \rho_{K_1^h K_2 R K_{1, [\tilde{j}, m]}^{\text{mask}}}^{\text{'out}, jj'} \tilde{\theta}_{[\tilde{j}, m]}' \tilde{\theta}_{[\tilde{j}, m]}' \wedge \tilde{F}_B=1 \wedge \tilde{F}_A=1 \wedge \beta=\tilde{j} \\
\sum_{\tilde{j} \geq \max\{j, j'\}} p_{01, \tilde{j}} \sigma_{LSE}^{01, \tilde{j}+1, \tilde{j}} &= \sum_{\tilde{j} \geq j_{\max}} |\tilde{j}+1, \tilde{j}\rangle\langle\tilde{j}+1, \tilde{j}|_{\alpha\alpha'} \otimes \tau_{K_1^h K_2 R K_{1, [\tilde{j}, m]}^{\text{mask}}} \otimes \tilde{\tau}_{\tilde{\theta}_{[\tilde{j}+1, m]}'} \tilde{\theta}_{[\tilde{j}+1, m]}' \otimes \rho_{E \wedge \tilde{F}_B=1 \wedge \tilde{F}_A=0 \wedge \beta=\tilde{j}}^{\text{'out}, jj'} \\
\sum_{\tilde{j} \geq \max\{j, j'\}} p_{11, \tilde{j}} \sigma_{LSE}^{11, \tilde{j}\tilde{j}} &= \sum_{\tilde{j} \geq j_{\max}} |\tilde{j}, \tilde{j}\rangle\langle\tilde{j}, \tilde{j}|_{\alpha\alpha'} \otimes \tau_{K_1^h K_2 R K_{1, [\tilde{j}, m]}^{\text{mask}}} \otimes \tilde{\tau}_{\tilde{\theta}_{[\tilde{j}, m]}'} \tilde{\theta}_{[\tilde{j}, m]}' \otimes \rho_{E \wedge \tilde{F}_B=1 \wedge \tilde{F}_A=1 \wedge \beta=\tilde{j}}^{\text{'out}, jj'}
\end{aligned} \tag{74}$$

where the variables are explicitly listed, with suitable tracing out of  $K_{1, [\tilde{j}-1]}^{\text{mask}}$ , noting that  $\beta = \beta'$  by  $\tilde{F}_B = 1$  condition.

When  $\tilde{F}_B = 1$ , we are guaranteed that the corrected bit string  $\hat{X}_{P_{2,r}}$  matches exactly Alice's bit string  $X_{P_{2,r}}$ . Since the privacy amplification seed  $R$  matches as well, when  $\tilde{F}_A = 1$ , the updated basis seed matches as well,  $\tilde{\theta}_{\tilde{j}} = \tilde{\theta}_{\tilde{j}}'$ . As such, we can write a CPTP map that copies  $\tilde{\theta}_{\tilde{j}}'$  to  $\tilde{\theta}_{\tilde{j}}$ . Furthermore, we note that  $\alpha\alpha'$  can be computed from  $\beta$  alone (implicitly part of  $E$ ) since  $\tilde{F}_A$  and  $\tilde{F}_B$  are individually fixed in both trace distance. As such, we can simplify the trace distance using the strong convexity property, the fact that CPTP maps cannot increase trace distance, and removing common terms in the protocol (namely  $K_{1, [\tilde{j}+1, m]}^{\text{mask}}$  and  $\tilde{\theta}_{[\tilde{j}+1, m]}'$  and  $R$  when  $\tilde{F}_A = 0$ ),

$$\begin{aligned}
\Delta \left( p_{01}^{\text{real}} \rho_{LSE|(\tilde{F}_A, \tilde{F}_B)=01}^{\text{'out}, jj'}, \sum_{\tilde{j} \geq \max\{j, j'\}} p_{01, \tilde{j}} \sigma_{LSE}^{01, \tilde{j}+1, \tilde{j}} \right) &\leq \Delta \left( \rho_{K_1^h K_2 K_{1, \beta}^{\text{mask}}}^{\text{'out}, jj'} E \wedge \tilde{F}_B=1 \wedge \tilde{F}_A=0, \tau_{K_1^h K_2 K_{1, \beta}^{\text{mask}}} \otimes \rho_{E \wedge \tilde{F}_B=1 \wedge \tilde{F}_A=0}^{\text{'out}, jj'} \right) \\
&\leq \Delta \left( \rho_{K_1^h K_2 K_{1, \beta}^{\text{mask}}}^{\text{'out}, jj'} E \wedge \tilde{F}_B=1, \tau_{K_1^h K_2 K_{1, \beta}^{\text{mask}}} \otimes \rho_{E \wedge \tilde{F}_B=1}^{\text{'out}, jj'} \right) \\
\Delta \left( p_{11}^{\text{real}} \rho_{LSE|(\tilde{F}_A, \tilde{F}_B)=11}^{\text{'out}, jj'}, \sum_{\tilde{j} \geq \max\{j, j'\}} p_{11, \tilde{j}} \sigma_{LSE}^{11, \tilde{j}\tilde{j}} \right) &\leq \Delta \left( \rho_{K_1^h K_2 R K_{1, \beta}^{\text{mask}}}^{\text{'out}, jj'} \tilde{\theta}_{\beta}' E \wedge \tilde{F}_B=1 \wedge \tilde{F}_A=1, \tau_{K_1^h K_2 R K_{1, \beta}^{\text{mask}}} \tilde{\theta}_{\beta}' \otimes \rho_{E \wedge \tilde{F}_B=1 \wedge \tilde{F}_A=1}^{\text{'out}, jj'} \right) \\
&\leq \Delta \left( \rho_{K_1^h K_2 R K_{1, \beta}^{\text{mask}}}^{\text{'out}, jj'} \tilde{\theta}_{\beta}' E \wedge \tilde{F}_B=1, \tau_{K_1^h K_2 R K_{1, \beta}^{\text{mask}}} \tilde{\theta}_{\beta}' \otimes \rho_{E \wedge \tilde{F}_B=1}^{\text{'out}, jj'} \right),
\end{aligned} \tag{75}$$

where we further remove the  $\tilde{F}_A$  conditions respectively.

From these trace distances, we can follow a similar analysis as in the proof of Thm. 15. We follow the same label of the original basis seed before refresh as  $\tilde{\theta}_{\beta}^{\text{in}}$ , with the same condition  $\tilde{\Omega}_{\text{PE}}$ . We can split the trace distance for the  $\tilde{F}_A = 0$  case, and simplify each trace distance based on the quantum leftover hash lemma [38, 41] and almost two-universal property of the hash function [28] (similar to proof of Thm. 19),

$$\begin{aligned}
&\Delta \left( \rho_{\beta K_1^h K_2 K_{1, \beta}^{\text{mask}}}^{\text{'out}, jj'} E \wedge \tilde{F}_B=1, \tau_{K_1^h K_2 K_{1, \beta}^{\text{mask}}} \otimes \rho_{\beta E \wedge \tilde{F}_B=1}^{\text{'out}, jj'} \right) \\
&\leq p_{\tilde{\Omega}_{\text{PE}}} \left[ \Delta \left( \rho_{\beta K_1^h K_2 K_{1, \beta}^{\text{mask}}}^{\text{'out}, jj'} E \wedge \tilde{F}_B=1 | \tilde{\Omega}_{\text{PE}}, \tau_{K_2} \otimes \rho_{\beta K_1^h K_{1, \beta}^{\text{mask}}}^{\text{'out}, jj'} E \wedge \tilde{F}_B=1 | \tilde{\Omega}_{\text{PE}} \right) \right. \\
&\quad \left. + \Delta \left( \rho_{\beta K_1^h K_{1, \beta}^{\text{mask}}}^{\text{'out}, jj'} E \wedge \tilde{F}_B=1, \tau_{K_1^h K_{1, \beta}^{\text{mask}}} \otimes \rho_{\beta E \wedge \tilde{F}_B=1 | \tilde{\Omega}_{\text{PE}}}^{\text{'out}, jj'} \right) \right] \\
&\leq p_{\tilde{\Omega}_{\text{PE}}} \left[ 2(\varepsilon_{\text{sm}, 2} + \varepsilon_{\text{sm}, 3} + \varepsilon_2 + \varepsilon_3) + \sqrt{(|\mathcal{T}_{\text{AV}}| \varepsilon_{\text{MAC}, 1} - 1) + 2^{\log_2 |\mathcal{T}_{\text{AV}}| + \log_2 \left( \frac{2}{\varepsilon_3} + 1 \right) - H_{\min}^{\varepsilon_{\text{sm}, 3}}(\hat{X}_{P_{2,r}} | \beta E) \wedge \tilde{F}_B=1 | \tilde{\Omega}_{\text{PE}}}} \right. \\
&\quad \left. + \sqrt{(|\mathcal{T}_{\text{BV}}| \varepsilon_{\text{MAC}, 2} - 1) + 2^{\log_2 |\mathcal{T}_{\text{BV}}| + \log_2 \left( \frac{2}{\varepsilon_2} + 1 \right) - H_{\min}^{\varepsilon_{\text{sm}, 2}}(\hat{X}_{P_{2,r}} | \beta K_1^h K_{1, \beta}^{\text{mask}} E) \wedge \tilde{F}_B=1 | \tilde{\Omega}_{\text{PE}}}} \right]
\end{aligned} \tag{76}$$

and for the  $\tilde{F}_A = 1$  case,

$$\begin{aligned}
& \Delta \left( \rho_{\beta K_1^h K_2 R K_{1,\beta}^{\text{mask}} \tilde{\theta}'_{\beta} E \wedge \tilde{F}_B=1}, \tau_{\beta K_1^h K_2 R K_{1,\beta}^{\text{mask}} \tilde{\theta}'_{\beta}} \otimes \rho_{E \wedge \tilde{F}_B=1}'^{\text{out},jj'} \right) \\
& \leq p_{\tilde{\Omega}_{\text{PE}}} \left[ \Delta \left( \rho_{\beta K_1^h K_2 R K_{1,\beta}^{\text{mask}} \tilde{\theta}'_{\beta} K_B E \wedge \tilde{F}_B=1 | \tilde{\Omega}_{\text{PE}}}, \tau_{R \tilde{\theta}'_{\beta} K_B} \otimes \rho_{\beta K_1^h K_2 K_{1,\beta}^{\text{mask}} E \wedge \tilde{F}_B=1 | \tilde{\Omega}_{\text{PE}}}^{\text{out},jj'} \right) \right. \\
& \quad + \Delta \left( \rho_{\beta K_1^h K_2 K_{1,\beta}^{\text{mask}} E \wedge \tilde{F}_B=1 | \tilde{\Omega}_{\text{PE}}}, \tau_{K_2} \otimes \rho_{\beta K_1^h K_{1,\beta}^{\text{mask}} E \wedge \tilde{F}_B=1 | \tilde{\Omega}_{\text{PE}}}^{\text{out},jj'} \right) \\
& \quad \left. + \Delta \left( \rho_{\beta K_1^h K_{1,\beta}^{\text{mask}} E \wedge \tilde{F}_B=1}, \tau_{K_1^h K_{1,\beta}^{\text{mask}}} \otimes \rho_{\beta E \wedge \tilde{F}_B=1 | \tilde{\Omega}_{\text{PE}}}^{\text{out},jj'} \right) \right] \\
& \leq p_{\tilde{\Omega}_{\text{PE}}} \left\{ 2(\varepsilon_{\text{sm},1} + \varepsilon_{\text{sm},2} + \varepsilon_{\text{sm},3} + \varepsilon_2 + \varepsilon_3) + \frac{1}{2} \times 2^{-\frac{1}{2}} [H_{\min}^{\varepsilon_{\text{sm},1}}(\hat{X}_{P_{2,r}} | \beta K_1^h K_2 K_{1,\beta}^{\text{mask}} E) \wedge \tilde{F}_B=1 | \tilde{\Omega}_{\text{PE}} - l_{K_B} - l_{\tilde{\theta}}] \right. \\
& \quad + \sqrt{(|\mathcal{T}_{\text{AV}}| \varepsilon_{\text{MAC},1} - 1) + 2^{\log_2 |\mathcal{T}_{\text{AV}}| + \log_2 (\frac{2}{\varepsilon_3} + 1) - H_{\min}^{\varepsilon_{\text{sm},3}}(\hat{X}_{P_{2,r}} | \beta E) \wedge \tilde{F}_B=1 | \tilde{\Omega}_{\text{PE}}}} \\
& \quad \left. + \sqrt{(|\mathcal{T}_{\text{BV}}| \varepsilon_{\text{MAC},2} - 1) + 2^{\log_2 |\mathcal{T}_{\text{BV}}| + \log_2 (\frac{2}{\varepsilon_2} + 1) - H_{\min}^{\varepsilon_{\text{sm},2}}(\hat{X}_{P_{2,r}} | \beta K_1^h K_{1,\beta}^{\text{mask}} E) \wedge \tilde{F}_B=1 | \tilde{\Omega}_{\text{PE}}}} \right\},
\end{aligned} \tag{77}$$

where we label  $\wedge \tilde{F}_B = 1 | \tilde{\Omega}_{\text{PE}}$  as the evaluation of the min-entropy on the corresponding state conditioned on event  $\tilde{\Omega}_{\text{PE}}$  and when  $\tilde{F}_B = 1$ , and we reintroduced  $K_B$  since it is part of the output of the final hash function. Following the proof of Thm. 15, the smooth min-entropy term can be bounded by

$$H_{\min}^{\varepsilon_{\text{sm},1}}(\hat{X}_{P_{2,r}} | \beta K_1^h K_2 K_{1,\beta}^{\text{mask}} E)_{\rho_{\beta K_1^h K_2 K_{1,\beta}^{\text{mask}} E \wedge \tilde{F}_B=1 | \tilde{\Omega}_{\text{PE}}}'^{\text{out},jj'}} \geq N_{P_{2,1}}^{\text{tol}} - N_{P_{2,1}}^{\text{tol}} h_{\text{bin}}(e'_{\text{ph,tol}}) - \text{leak}_{\text{EC}} - \log_2 |\mathcal{T}_{\text{AV}}| |\mathcal{T}_{\text{BV}}| - 2. \tag{78}$$

The second term and third terms can follow a similar analysis, with the main difference being the lack of conditioning of some secrets. In the second term, the conditioning on  $K_2$  is not present. Therefore,  $T_{\text{BV}}$ , as the output of a  $\varepsilon_{\text{MAC},2}$ -almost strongly 2-universal hash function, is uniform and independent of the input, importantly  $X_{P_2}$ . As such, it can be removed without using the min-entropy chain rule, i.e. without incurring a  $\log_2 |\mathcal{T}_{\text{BV}}|$  penalty, resulting in

$$H_{\min}^{\varepsilon_{\text{sm},2}}(\hat{X}_{P_{2,r}} | \beta K_1^h K_{1,\beta}^{\text{mask}} E)_{\rho_{\beta \hat{X}_{P_{2,r}} K_1^h K_{1,\beta}^{\text{mask}} E \wedge \tilde{F}_B=1 | \tilde{\Omega}_{\text{PE}}}'}^{\text{out},jj'} \geq N_{P_{2,1}}^{\text{tol}} - N_{P_{2,1}}^{\text{tol}} h_{\text{bin}}(e'_{\text{ph,tol}}) - \text{leak}_{\text{EC}} - \log_2 |\mathcal{T}_{\text{AV}}| - 2. \tag{79}$$

In the third term, both the conditioning on  $K_2$  and  $K_1^h K_{1,\beta}^{\text{mask}}$  are absent. Similarly, we can argue that  $T_{\text{AV}}$  and  $T_{\text{BV}}$  are uniform and independent of  $X_{P_2}$  since the respective seeds of the almost 2-universal hash functions are not part of the conditioning. As such, we have

$$H_{\min}^{\varepsilon_{\text{sm},3}}(\hat{X}_{P_{2,r}} | \beta E)_{\rho_{\beta \hat{X}_{P_{2,r}} E \wedge \tilde{F}_B=1 | \tilde{\Omega}_{\text{PE}}}'}^{\text{out},jj'} \geq N_{P_{2,1}}^{\text{tol}} - N_{P_{2,1}}^{\text{tol}} h_{\text{bin}}(e'_{\text{ph,tol}}) - \text{leak}_{\text{EC}} - 2. \tag{80}$$

Combining the results, we recover the theorem. We can repeat the analysis with two-universal hash function to obtain the second set of bounds in the theorem.  $\square$

### D.3 Numerical Analysis

Before we proceed with the numerical simulation, we briefly introduce the robustness. The main sources of failure are the parameter estimation checks during the protocol or error correction failure, with overall robustness similarly quantified as original QAKE protocol,

$$\varepsilon_{\text{rob}} = \varepsilon_{\text{rob},P} + \varepsilon_{\text{serf},2} + \varepsilon_{\text{ds,rob}} + \varepsilon_{\mathcal{E},P_1,\text{rob}} + \varepsilon_{\text{EC}}, \tag{81}$$

where  $\varepsilon_{\text{rob},P}$  is associated with  $P^{\text{tol}} \leq |P| \leq P^{\text{UB}}$  bounds,  $\varepsilon_{\text{serf},2}$  is the error associated with modified Serfling bound [12, 42] for estimating bit error rate in  $P_2$ ,  $\varepsilon_{\text{ds,rob}}$  is associated with the decoy state,  $\varepsilon_{\mathcal{E},P_1,\text{rob}}$  is associated with the bit error tolerance in set  $P_1$ , and  $\varepsilon_{\text{EC}}$  is simply the failure rate of error correction. The concentration bound used for robustness parameters is the tight bound on binomial distribution [48] due to i.i.d. state preparation. The concentration bound used for estimation of the expectation values,  $\mathbb{E}[N_{\mu_v, P_i}]$ , from the observed values,  $N_{\mu_v, P_i}$ , associated with decoy state estimation (errors form part of decoy state  $\varepsilon_{\text{ds}}$  in  $\varepsilon_{\text{sec,int}}$ ) is Kato's bound [11, 19, 46].

We analyse the performance of the QAKE protocol by simulating the length of keys  $l_{KB}$  generated based on Thm. 20. We assume a simple experimental model with Alice preparing decoy BB84 states, sending it through a channel with loss  $\eta$ , and Bob performing measurement in the same basis as Alice. Bob's detector is assumed to have zero dark counts, and the overall experiment is assumed to have 2% QBER, with the following detection probability,  $\Pr[\text{det}, \mu_j] = p_{\mu_j}(1 - e^{-\eta\mu_j})$ , where we also fix  $\mu_0 = 0.45$ ,  $\mu_1 = 0.225$ ,  $\mu_2 = 0$  as the decoy intensity,  $p_{\mu_0} = 0.2$ ,  $p_{\mu_1} = 0.6$  and  $p_{\mu_2} = 0.2$  as their respective probabilities. The PRNG is assumed to use a 256-bit basis generation seed  $\tilde{\theta}_\beta$ . Given the adversary's resource  $t$  is limited by the duration of each protocol session (less than a minute), and additional resources  $t_{ex}$ ,  $t_{MG}$  and  $t_{SG,PR}$  are simple steps that can be performed within the protocol duration, it is safe to argue that the PRNG is secure. In this case, we assume a 128-bit security,  $\varepsilon_{\text{PRNG}} = 2^{-128}$ , which should be a conservative estimate of the security of the PRNG for the run time of the full protocol. We note that such quantum-secure PRNG can be constructed from well-known protocols, such as AES [16, 18]. In the simulation, we also fix the length of the authentication tags as 80 bits each, and that  $\varepsilon_{\text{MAC},1} = \varepsilon_{\text{MAC},2} = 2^{-80}$ , allowing us to use the tighter bound presented in Thm. 20 with 2-universal hash function. We set the error correction efficiency to be  $\gamma_{\text{EC}} = 1.2$ .

The security parameter of the each session of the protocol is fixed at  $\varepsilon_{\text{sec,int}} = 10^{-15}$ , which yields an overall protocol security of  $10^{-6}$  when we allow it to run up to  $10^9$  sessions. The robustness parameter is fixed at  $\varepsilon_{\text{rob}} = 10^{-10}$ , and each sessions involves  $n_{\text{rnd}} = 10^{10}$  signals being sent by Alice to Bob. The simulation is then performed by rearranging the result in Thm. 3, and optimising  $l_{KB}$  over the splitting ratio (also size of test set)  $f_{P_1}$ , robustness and secrecy parameters (components of  $\varepsilon_{\text{rob}}$  and  $\varepsilon_{\text{sec}}$ ) on Matlab, with other parameters fixed as described in the results in Fig. 7.

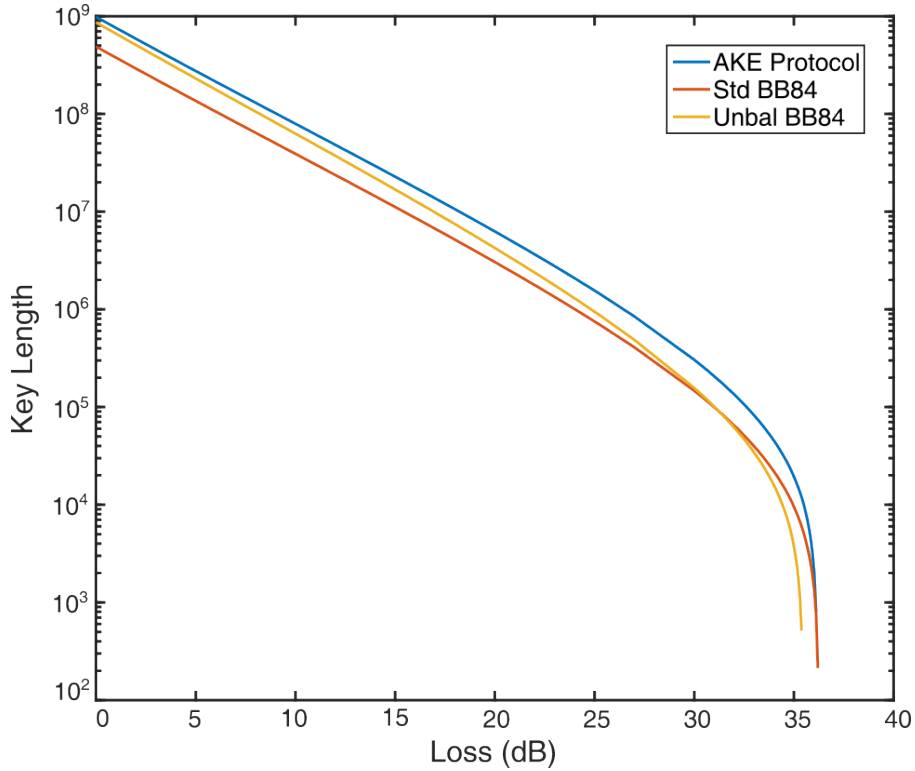


Figure 7: Simulated key length for QAKE with pseudorandom basis protocol at various signal loss values (including detector loss etc), standard BB84 protocol and unbalanced BB84 protocol, with  $n_{\text{rnd}} = 10^{10}$  signals sent,  $\varepsilon_{\text{rob}} = 10^{-10}$ , and  $\varepsilon_{\text{sec}} = 10^{-15}$ . The PRNG parameter is assumed to be  $\varepsilon_{\text{PRNG}} = 2^{-128}$ , with  $l_{\tilde{\theta}} = 256$ . The authentication tag used is 80-bits, i.e.  $|\mathcal{T}_{AV}| = |\mathcal{T}_{BV}| = 80$ , and we assume the error correction efficiency to be  $\gamma_{\text{EC}} = 1.2$ . The system parameters are chosen to be  $\mu_0 = 0.45$ ,  $\mu_1 = 0.225$ ,  $\mu_2 = 0$  as the decoy intensity,  $p_{\mu_0} = 0.2$ ,  $p_{\mu_1} = 0.6$  and  $p_{\mu_2} = 0.2$  as the respective probabilities, and we assume the system to have zero dark counts and a QBER of 2%.

To study the effect of the use of PRNG, we compare the results with the keys generated in a standard BB84 scheme [38] and a BB84 scheme with unbalanced basis choices [24]. To make the comparison fair, we utilise the same analysis results, but remove the penalties associated with PRNG, and make corresponding changes to the sifting and testing probability. The standard BB84 scheme [38] we compare to uses the same experimental

model, but due to sifting, has an additional sifting factor resulting in

$$\Pr[\text{det, sift}, \mu_j] = \frac{p_{\mu_j}}{2}(1 - e^{-\eta\mu_j}).$$

For the BB84 scheme with unbalanced basis choice [24], the probability of selecting  $X$  basis,  $p_X$ , is varied, and all rounds in the  $X$  basis is used as the test round. As such, the resulting model statistics has

$$\begin{aligned}\Pr[\text{det, test}, \mu_j] &= p_X^2 p_{\mu_j} (1 - e^{-\eta\mu_j}) \\ \Pr[\text{det, key}, \mu_j] &= (1 - p_X)^2 p_{\mu_j} (1 - e^{-\eta\mu_j}),\end{aligned}$$

while the test rounds in the earlier schemes have only an  $f_{P_1}$  factor to the detected rate. For both BB84 cases, due to lack of PRNG use, we simply set  $\varepsilon_{\text{PRNG}} = \varepsilon_{\hat{\theta}, \text{PRNG}} = \varepsilon_{\text{IRNG}} = 0$ , with no basis seed to refresh,  $l_{\hat{\theta}} = 0$ , phase error

$$e'_{\text{ph, tol}} = e_{\text{bit}, 1, \text{tol}} + g(N_{P_1, 1}^{\text{tol}}, N_{P_2, 1}^{\text{tol}}, \varepsilon_{\text{serf}, 1}).$$

They are simulated similarly by optimising  $l_{K_B}$  with the respective changes on Matlab. The results are shown in Fig. 7, where the protocol with PRNG generated basis has an advantage, mostly stemming from the lack of sifting. This shows up as a doubling of key rate of BB84, and an increasingly better key rate relative to BB84 with unbalanced basis as channel loss increases. There is a crossover at low key lengths, likely due to the impact of the 256-bit basis seed that has to be refreshed.

## D.4 Discussion

We note that compared to the original QAKE protocol, when PRNG is utilised, it loses the key recycling property. It only has a weaker key refreshing property, where most shared secrets can be recycled when the protocol passes, except for the basis seed  $\hat{\theta}$ , which needs to be refreshed every session. If one extends the assumption on the PRNG to remain secure for time  $t_{\text{sec}} \gg t'$  and  $m_{\text{sec}}$  sessions of protocol execution, one can recover the key recycling property by removing Bob's announcement of  $\hat{\theta}'_{\beta'}$  and using the random selection of test round to ensure that the adversary cannot successfully report a test round choice to Alice before it has received that information from Bob (i.e. Bob measured the quantum systems). The same basis generation seed could be used with a different public input (e.g. counter) to the PRNG for basis generation, thereby removing the need to refresh basis seed  $\hat{\theta}$  when the protocol passes, allowing for full key recycling. We note that  $\hat{\theta}$  would still have to be updated once  $t_{\text{sec}}$  has passed or when  $n_{\text{sess}}$  sessions has reached, and one could refer to NIST recommendations for the refresh rate for such symmetric keys [3].

One technical challenge to implement PRNG basis choice is the requirement of an active basis choice at the receiver to guarantee measurement in the same basis and the key rate advantage. This requires an extremely fast optical switch at the receiver to switch between the  $X$  and  $Z$  basis. A pulsed laser with a 500 MHz repetition rate would require a nanosecond optical switch. Nanosecond optical switches are commercially available with a low insertion loss of 0.7 dB, across the whole optical communication band. They have been demonstrated in data center networks [44] and dynamic optical switches with nanoseconds switching speed and large inputs/outputs ( $448 \times 448$ ) have also been previously demonstrated [45]. With the availability of nanosecond optical switches with low insertion loss, it may be feasible for high-speed implementation of the QAKE protocol with active basis selection.

## E Decoy-State BB84 with Pseudorandom Basis

### E.1 Motivation

The QAKE protocol with pseudorandom basis has key secrecy parameter dependent on the secrecy condition of decoy-state BB84 with shared pseudorandom basis. Here, we study such a protocol, where the main changes made relative to decoy-state BB84 are:

1. Alice and Bob pre-share a basis generation seed  $\tilde{\theta}_{\beta}$ .
2. During the protocol, Alice and Bob would use a PRNG  $G^{\text{PRNG}}$  to generate the basis to prepare and measure the quantum state respectively.
3. The sifting step is removed since Alice and Bob will always prepare and measure in the same basis.

Due to the removal of the sifting step, decoy state BB84 with shared pseudorandom basis is expected to gain a factor of 2 advantage in key generation rate. Similar protocols have been of interest in the literature, where basis information is generated or encrypted using a PRNG [31, 43]. However, a complete proof of security of the use of PRNG for basis selection remains elusive in the literature, with a security proof provided in Ref. [43] against only intercept-resend attacks. Here, we provide a complete security analysis through the *entropic uncertainty relation* (EUR).

Since the main goal in this section is to prove the security from the use of PRNG for basis generation, we focus on the main quantity of interest in the secrecy condition of QKD [38, 41]: the smooth min-entropy  $H_{\min}^\epsilon(X_{P_2} | \beta P_1 P_2 \tilde{\theta}_\beta X'_{P_1} E)_{\rho_{\beta X_{P_2} P_1 P_2 \tilde{\theta}_\beta X'_{P_1} E | \tilde{\Omega}_{PE}}}$ . The smooth min-entropy quantifies the maximum length of key that can be extracted from  $X_{P_2}$  that is private from the adversary. The smooth min-entropy is evaluated on the output state of the following process:

1. Alice prepares decoy state BB84 states, using the basis generated from the basis generation seed  $\tilde{\theta}_\beta$ , bit value  $X$  and intensity choice.
2. The adversary performs its attack on the state, mapping systems  $QE$  to  $PBE'$ .
3. Bob randomly selects  $P_1$  rounds and measure them in the basis generated from  $\tilde{\theta}_\beta$ , and outputs  $X'_{P_1}$ .
4. Based on  $X$ ,  $P_1$ ,  $P_2$  and  $X'_{P_1}$ , the decision of whether the parameter estimation step passes is made ( $\tilde{\Omega}_{PE}$  being the event where the parameter estimation passes).

In decoy-state BB84, entropic uncertainty relation (EUR) is one method to tightly bound the smooth min-entropy of the bit values of single photon events. Importantly, EUR lower bounds the smooth min-entropy by a function of the phase error rate, i.e. the mismatch of measurement outcomes in the complementary basis. Without PRNG and assuming uniform basis choice, the phase error rate matches the bit error rate (mismatch of measurement outcomes in the original basis) which can be estimated from the experiment. We argue that this gap between bit and phase error is small when PRNG is used, resulting in a slightly lower smooth min-entropy bound (and thus key rate). We present these arguments in later sub-sections, starting with analysing EUR with the use of PRNG in Appendix E.2, followed by the proof of the min-entropy lower bound in Appendix E.3. Detailed proof of the theorems on EUR with PRNG is presented in the final two sub-sections.

## E.2 Entropic Uncertainty Relation with PRNG

Entropic uncertainty relation describes the uncertainty a party has of performing incompatible measurements on a quantum state. Let us define a measurement on a subsystem  $C$  with initial basis choice  $\theta$ , a bijective function  $f_b$  to map  $\theta$  to a different basis choice, and measurement outcome  $Y$  by

$$\mathcal{M}_{f_b(\theta)C \rightarrow Y}(\rho) := \text{Tr}_C \left[ \sum_{\gamma, y} |y\rangle_Y (|\gamma\rangle\langle\gamma|_\theta \otimes O_C^{f_b(\gamma), y}) \rho (|\gamma\rangle\langle\gamma|_\theta \otimes O_C^{f_b(\gamma), y}) \langle y|_Y \right], \quad (82)$$

where  $O_C^{f_b(\theta), y}$  is the measurement operator on subsystem  $C$  with basis  $f_b(\theta)$ . The form of EUR of particular interest in our proof examines the following scenario:

1. The basis  $\theta$  is selected, and a quantum state with subsystems held by three parties, Alice ( $A$ ), Bob ( $B$ ), and ( $E$ ), is generated, i.e. state  $\rho_{\theta ABE}$ .
2. If Alice measures  $A$  in basis  $\theta$  and obtains outcome  $Y$ , i.e. perform  $\mathcal{M}_{\theta A \rightarrow Y}$ , Bob attempts to guess the value of  $Y$  from his subsystem  $B$  and  $\theta$ .
3. If Alice measures  $A$  in basis  $f_b(\theta)$  for some bijective map  $f_b$ , and obtains outcome  $\tilde{Y}$ , i.e. perform  $\mathcal{M}_{f_b(\theta) A \rightarrow \tilde{Y}}$ , Eve attempts to guess the value of  $\tilde{Y}$  from her subsystem  $E$  and  $\theta$ .

The EUR then quantifies the uncertainty on the outcomes  $Y$  and  $\tilde{Y}$  that subsystem  $E$  and  $B$  has respectively, which is related to the measurement operator incompatibility [39]. The more certain Eve can be on his guess of  $Y$  (smaller conditional entropy), the more uncertain Bob must be on her guess of  $\tilde{Y}$  (larger conditional entropy). Here, we present a modified variant of EUR, adapted from Ref. [38]. We note also that the EUR does not make any assumptions on how  $\theta$  is generated.

**Theorem 29.** Let  $\rho_{\theta ABE}$  be a tripartite quantum state and  $f_b$  be a bijective function on  $\theta$ . Then,

$$H_{\min}^{\varepsilon}(Y|\theta E)_{\mathcal{M}_{\theta A \rightarrow Y}(\rho_{\theta ABE})} \geq q - H_{\max}^{\varepsilon}(\tilde{Y}|\theta B)_{\mathcal{M}_{f_b(\theta)A \rightarrow \tilde{Y}}(\rho_{\theta ABE})},$$

where  $c_q = \max_{\theta} \max_{y, \tilde{y}} \left\| O_A^{\theta, y} (O_A^{f_b(\theta), \tilde{y}})^{\dagger} \right\|_{\infty}^2$  and  $q = \log_2 \frac{1}{c_q}$ .

*Proof.* We follow closely the proof of EUR in Ref. [38], where a similar form of EUR is proven, and taking inspiration from Ref. [39]. We begin by introducing the Stinespring dilation isometry of both measurement maps  $\mathcal{M}_{\theta A \rightarrow Y}$  and  $\mathcal{M}_{f_b(\theta)A \rightarrow \tilde{Y}}$  respectively,

$$\begin{aligned} V &= \sum_{\gamma, y} |yy\rangle_{YY'} \otimes |\gamma\rangle\langle\gamma|_{\theta} \otimes O_A^{\theta, y} \\ W &= \sum_{\gamma, \tilde{y}} |\tilde{y}\tilde{y}\rangle_{\tilde{Y}\tilde{Y}'} \otimes |\gamma\rangle\langle\gamma|_{\theta} \otimes O_A^{f_b(\theta), \tilde{y}}. \end{aligned} \quad (83)$$

We can purify the state  $\rho_{\theta ABE}$  to

$$|\psi\rangle_{\theta\theta'ABED} = \sum_{\gamma} \sqrt{p_{\alpha}} |\gamma\rangle_{\theta\theta'} \otimes |\phi_{\alpha}\rangle_{ABED}, \quad (84)$$

where  $|\phi_{\alpha}\rangle_{ABED}$  is a purification of  $\rho_{ABE|\theta=\gamma}$ , which can be performed by selecting  $D$  to be a sufficiently large auxiliary system. The post-measurement state after performing the latter measurement map  $\mathcal{M}_{f_b(\theta)A \rightarrow \tilde{Y}}$  can thus be written as

$$\rho_{\theta\theta'ABE\tilde{Y}\tilde{Y}'D} = W |\psi\rangle\langle\psi|_{\theta\theta'ABED} W^{\dagger} \quad (85)$$

Since the state is pure, we can apply the duality relation of smooth min- and max-entropy [22, 40],

$$H_{\max}^{\varepsilon}(\tilde{Y}|\theta B) + H_{\min}^{\varepsilon}(\tilde{Y}|\theta' AE\tilde{Y}'D) = 0, \quad (86)$$

and what remains is to bound the smooth min-entropy term, which is upper bounded by  $H_{\min}^{\varepsilon}(\tilde{Y}|\theta AE\tilde{Y}')$  since  $\theta = \theta'$ , and  $D$  can be removed by the data-processing inequality for CPTP map  $\text{Tr}_D$  [37].

The smooth min-entropy term is evaluated on the state  $[W\rho_{\theta AE}W^{\dagger}]$ , where we note that it is possible to reverse the measurement of system  $A$  using basis  $f_b(\theta)$  and measure it using basis  $\theta$ . This is expressed as a CPTP map, using the Stinespring dilation isometry of the measurement maps,

$$\mathcal{E} = \sum_{\gamma} \text{Tr}_{AY'} [VW^{\dagger} |\gamma\rangle\langle\gamma|_{\theta} \cdot |\gamma\rangle\langle\gamma|_{\theta} WV^{\dagger}], \quad (87)$$

where we have

$$\begin{aligned} &\mathcal{E}(\rho_{\theta AE\tilde{Y}\tilde{Y}'}) \\ &= \sum_{\gamma} \text{Tr}_{AY'} \{ VW^{\dagger} [|\gamma\rangle\langle\gamma|_{\theta} \otimes \sum_{yy'} |yy\rangle_{YY'} O_A^{f_b(\gamma), y} \rho_{AE|\theta=\gamma} (O_A^{f_b(\gamma), y'})^{\dagger} \langle y'y' |_{YY'}] WV^{\dagger} \} \\ &= \sum_{\gamma} \text{Tr}_{AY'} \{ V [|\gamma\rangle\langle\gamma|_{\theta} \otimes \sum_y (O_A^{f_b(\gamma), y})^{\dagger} O_A^{f_b(\gamma), y} \rho_{AE|\theta=\gamma} \sum_{y'} (O_A^{f_b(\gamma), y'})^{\dagger} O_A^{f_b(\gamma), y'}] V^{\dagger} \} \\ &= \text{Tr}_{AY'} [V \rho_{\theta AE} V^{\dagger}] \\ &= \rho_{\theta YE}, \end{aligned} \quad (88)$$

where  $\rho_{\theta YE}$  is the post-measurement state on  $\rho_{\theta ABE}$  with measurement map  $\mathcal{M}_{\theta A \rightarrow Y}$  and the appropriate trace, and we note that  $\sum_y (O_A^{f_b(\gamma), y})^{\dagger} O_A^{f_b(\gamma), y} = \mathbb{I}_A$ .

By definition of the smooth min-entropy, there exists a state  $\sigma_{\theta AE\tilde{Y}\tilde{Y}'}$ , and  $\omega_{\theta AE\tilde{Y}'}$ , such that purified distance  $P(\rho_{\theta AE\tilde{Y}\tilde{Y}'}, \sigma_{\theta AE\tilde{Y}\tilde{Y}'}) \leq \varepsilon$ , and

$$\sigma_{\theta AE\tilde{Y}\tilde{Y}'} \leq 2^{-\lambda} \mathbb{I}_{\tilde{Y}} \otimes \omega_{\theta AE\tilde{Y}'}, \quad (89)$$

where  $\lambda = H_{\min}^{\varepsilon}(\tilde{Y}|\theta AE\tilde{Y}')$ . We note here that any CPTP map should not increase the purified distance, which allows us to define a state  $\sigma_{\theta YE} := \mathcal{E}(\sigma_{\theta AE\tilde{Y}\tilde{Y}'}),$  such that it is  $\varepsilon$ -close in purified distance to  $\rho_{\theta YE}$ ,

$$P(\sigma_{\theta YE}, \rho_{\theta YE}) \leq P(\sigma_{\theta AE\tilde{Y}\tilde{Y}'}, \rho_{\theta AE\tilde{Y}\tilde{Y}'} ) \leq \varepsilon. \quad (90)$$

We can apply the channel  $\mathcal{E}$  on both sides of Eq. (89), giving

$$\sigma_{\theta YE} \leq 2^{-\lambda} \mathcal{E}(\mathbb{I}_{\tilde{Y}} \otimes \omega_{\theta AE\tilde{Y}'}). \quad (91)$$

The RHS term can be expanded as

$$\begin{aligned} \mathcal{E}(\mathbb{I}_{\tilde{Y}} \otimes \omega_{\theta AE\tilde{Y}'}) &= \sum_{\gamma y \tilde{y}} |\gamma y\rangle\langle \gamma y|_{\theta Y} \otimes \langle \tilde{y} | \text{Tr}_A [O_A^{\gamma, y} (O_A^{f_b(\gamma), \tilde{y}})^\dagger \hat{\omega}_{AE\tilde{Y}'}^\gamma O_A^{f_b(\gamma), \tilde{y}} (O_A^{\gamma, y})^\dagger] | \tilde{y}\rangle_{\tilde{Y}'} \\ &\leq \sum_{\gamma y \tilde{y}} |\gamma y\rangle\langle \gamma y|_{\theta Y} \otimes \left\| O_A^{\gamma, y} (O_{\tilde{y}}^{f_b(\gamma)})^\dagger \right\|_\infty^2 \langle \tilde{y} | \text{Tr}_A (\hat{\omega}_{AE\tilde{Y}'}^\gamma) | \tilde{y}\rangle_{\tilde{Y}'} \\ &\leq \left[ \max_{\gamma} \max_{y, \tilde{y}} \left\| O_A^{\gamma, y} (O_{\tilde{y}}^{f_b(\gamma)})^\dagger \right\|_\infty^2 \right] \sum_{\gamma y} |\gamma y\rangle\langle \gamma y|_{\theta Y} \otimes \text{Tr}_{A\tilde{Y}'} [\hat{\omega}_{AE\tilde{Y}'}^\gamma] \\ &= c_q \mathbb{I}_Y \otimes \hat{\omega}_{\theta E}, \end{aligned} \quad (92)$$

where  $\hat{\omega}_{\theta E} := \sum_{\gamma} |\gamma\rangle\langle \gamma|_{\theta} \otimes \text{Tr}_{A\tilde{Y}'} [\hat{\omega}_{AE\tilde{Y}'}^\gamma]$  and  $\hat{\omega}_{AE\tilde{Y}'}^\gamma := \langle \gamma | \omega_{\theta AE\tilde{Y}'} | \gamma \rangle$ . Therefore, by definition, the min-entropy is lower bounded,

$$H_{\min}(Y|\theta E)_{\sigma_{\theta YE}} \geq H_{\min}^\varepsilon(\tilde{Y}|\theta AE\tilde{Y}') + q, \quad (93)$$

where  $q = \log_2 \frac{1}{c_q}$ . Since  $\sigma_{\theta YE}$  is  $\varepsilon$ -close in purified distance to  $\rho_{\theta YE}$ , the smooth min-entropy can be bounded,

$$H_{\min}^\varepsilon(Y|\theta E)_{\rho_{\theta YE}} \geq H_{\min}^\varepsilon(\tilde{Y}|\theta AE\tilde{Y}') + q. \quad (94)$$

Combining the results, we end up with

$$H_{\min}^\varepsilon(Y|\theta E)_{\rho_{\theta YE}} + H_{\max}^\varepsilon(\tilde{Y}|\theta B)_{\rho_{\theta \tilde{Y} B}} \geq q. \quad (95)$$

Noting that  $\rho_{\theta YE} = \text{Tr}_B[\mathcal{M}_{\theta A \rightarrow Y}(\rho_{\theta ABE})]$  and  $\rho_{\theta \tilde{Y} B} = \text{Tr}_E[\mathcal{M}_{f_b(\theta) A \rightarrow \tilde{Y}}(\rho_{\theta ABE})]$ , we arrive at the form of the theorem.  $\square$

To bound the smooth min-entropy, we thus have to compute the smooth max-entropy  $H_{\max}^\varepsilon(\tilde{Y}|\theta B)_{\mathcal{M}_{f_b(\theta) A \rightarrow \tilde{Y}}(\rho_{\theta ABE})}$ . A typical reduction [32, 42] of the smooth max-entropy is to simplify it via data-processing inequality and bound it with  $h_{\text{bin}}(e_{\text{ph}})$ , where  $e_{\text{ph}} = \frac{wt(\tilde{Y}_A \oplus \tilde{Y}_B)}{n}$  is termed the phase error rate and  $n$  is the number of entries in  $\tilde{Y}_A$  (also number of qubit of subsystem  $A$ ), obtained from the state  $\mathcal{M}_{f_b(\theta) A \rightarrow \tilde{Y}_A} \circ \mathcal{M}_{f_b(\theta) B \rightarrow \tilde{Y}_B}(\rho_{\theta ABE}^{\text{PRNG}})$ . Since we never measure in the  $f_b(\theta)$  basis in the protocol, the phase error is typically computed from the bit error rate,  $e_{\text{bit}} := \frac{wt(Y_A \oplus Y_B)}{n}$ , from the state  $\mathcal{M}_{\theta A \rightarrow Y_A} \circ \mathcal{M}_{\theta B \rightarrow Y_B}(\rho_{\theta ABE}^{\text{PRNG}})$ . Typically, it is argued that the expectation values of the phase and bit error matches,  $\mathbb{E}[e_{\text{bit}}] = \mathbb{E}[e_{\text{ph}}]$  if the basis  $\theta \in \{0, 1\}^n$  is chosen uniformly at random and independent from subsystems  $ABE$  [38, 39].

This argument breaks down when a PRNG is utilised since the basis is no longer uniformly distributed. Instead, we argue that the difference between the phase and bit error rates in the case where a quantum-secure PRNG is used (bit-phase error gap) is small. Consider two separate instances of an adversary that is bounded by resource  $t$ , and prepares the state  $\rho_{\theta ABE}$ , which would be measured in  $\theta$  and  $\bar{\theta}$  respectively ( $f_b$  refers to bit flip in this case) to obtain the bit and phase errors (see Fig. 8). The pseudorandomness property of the PRNG ensures that a similarly small bit-phase error gap must be present when a PRNG is utilised. Otherwise, the bit-phase error gap can be utilised by a distinguisher with  $t' \geq t_D$  resources (see Fig. 9) to distinguish a PRNG from an ideal RNG with probability greater than  $\varepsilon_{\text{PRNG}}$ , where  $t_D = 2(t + t_{MG}) + t_{ex}$ . We recall that the PRNG is chosen with  $t' = 2(t + t_{MG}) + t_{ex} + t_{SG, PR}$ .

We first show that the phase error rate can be lower bounded by the bit error rate with some penalty, stemming from the low bit-phase error gap for PRNG.

**Theorem 30.** *Suppose that the basis  $\theta$  is generated from a  $(t', \varepsilon_{\text{PRNG}})$ -quantum secure PRNG with  $t' \geq t_D$  and let  $\rho_{\theta ABE}^{\text{PRNG}}$  be the state prepared by the adversary (via protocol  $\mathcal{P}_{\text{Adv}}$ ), where  $A$  and  $B$  are  $n$ -qubit states, and  $\theta$  remain independent when generated by an IRNG,  $\rho_{\theta ABE}^{\text{IRNG}} = \tau_\theta \otimes \rho_{ABE}$ . Let  $\Omega := \{D_{\text{PE}} = 1\}$  be an event that can be decided from  $E$ , and  $e_{\text{bit}, \text{tol}}$  be the tolerance value for an upper bound on the bit error value, i.e.  $\Pr[e_{\text{bit}} \geq e_{\text{bit}, \text{tol}} | \Omega]_{\mathcal{M}_{\theta A \rightarrow Y_A} \circ \mathcal{M}_{\theta B \rightarrow Y_B}(\rho_{\theta ABE}^{\text{PRNG}})} \leq \varepsilon_{\text{bit}}$ . Then, an upper bound on the phase error for state  $\rho_{\theta ABE}^{\text{PRNG}}|_{\Omega}$*

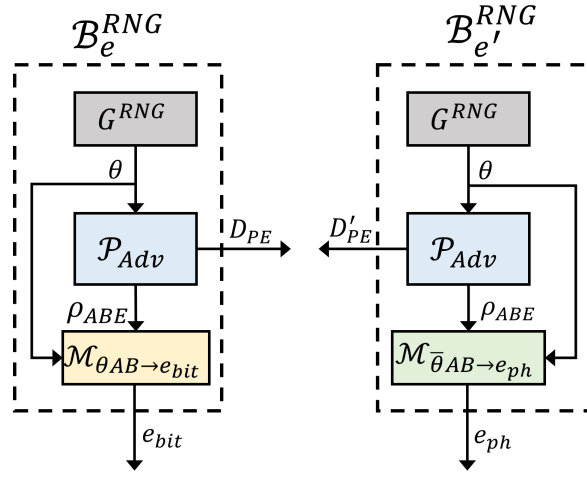


Figure 8: Description of quantum algorithms  $\mathcal{B}_e^{RNG}$  and  $\mathcal{B}_{e'}^{RNG}$ . Each algorithm begins with a run of the random number generator  $G^{RNG}$  which outputs  $\theta$ , followed by the generation of quantum state  $\rho_{\theta ABE}$  via a protocol  $\mathcal{P}_{Adv}$  (e.g. QAKE protocol with adversarial attack), and ends with a measurement on subsystems  $AB$  to compute the bit error  $e_{bit}$  and phase error  $e_{ph}$  respectively. The output  $D_{PE}$  forms a decision which defines the event set  $\Omega = \{D_{PE} = 1\}$ . We label the resources required for state preparation and measurement as  $t$ , with the other steps (e.g. flipping of  $\theta$  when computing phase error, and computing of bit/phase error) contributing resource  $t_{MG}$ , and overall resource requirement  $t_B = t + t_{MG}$ .

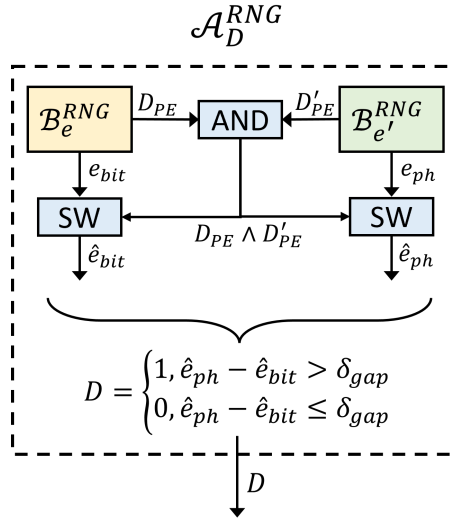


Figure 9: Description of distinguishing adversary with output decision  $D$ . The adversary computes  $D_{PE} \wedge D'_{PE}$ , where  $D_{PE}$  and  $D'_{PE}$  are obtained from the quantum process  $\mathcal{P}_{Adv}$ . The SW function is a switch which sets  $\hat{e}_{bit} = 0$  and  $\hat{e}_{ph} = 0$  respectively when  $D_{PE} \wedge D'_{PE} = 0$ , and leave  $\hat{e}_{bit} = e_{bit}$  and  $\hat{e}_{ph} = e_{ph}$  when  $D_{PE} \wedge D'_{PE} = 1$ . The decision  $D$  is made by comparing the bit-phase error gap with a target  $\delta_{gap}$ . The resource required for the adversary is defined as  $t_D$ , which comprises of  $2t_B$  and extra steps  $t_{ex}$ .

after measurement is

$$\begin{aligned} \Pr[e_{\text{ph}} \geq e_{\text{ph,tol}}]_{\mathcal{M}_{\bar{\theta}A \rightarrow \bar{Y}} \circ \mathcal{M}_{\bar{\theta}B \rightarrow \bar{Y}', (\rho_{\bar{\theta}ABE|\Omega}^{\text{PRNG}})} &\leq \varepsilon_{\text{ph}} \\ e_{\text{ph,tol}} = e_{\text{bit,tol}} + 2\sqrt{\frac{2}{n} \ln \frac{1}{\varepsilon_{\text{IRNG}}}} \\ \varepsilon_{\text{ph}} = 2\varepsilon_{\text{IRNG}} + \frac{\varepsilon_{\text{PRNG}}}{p_{\Omega}^2} + \varepsilon_{\text{bit}}. \end{aligned}$$

*Proof.* We first show that the bit-phase error gap is small. Since the algorithm in Fig. 9,  $\mathcal{A}_D^{G_{\kappa}^{\text{PRNG}}, t'}$  has resource restriction  $t_D$ , the quantum-secure PRNG cannot be distinguished via this algorithm,

$$\left| \Pr[\mathcal{A}_D^{G_{\kappa}^{\text{PRNG}}, t_D} = 1] - \Pr[\mathcal{A}_D^{G^{\text{IRNG}}, t_D} = 1] \right| \leq \varepsilon_{\text{PRNG}}. \quad (96)$$

By definition of the outcome  $D$ , the bit-phase error gap obtained from PRNG is no much different from that of an IRNG,

$$\Pr[\hat{e}_{\text{ph}} - \hat{e}_{\text{bit}} > \delta_{\text{gap}}]_{\mathcal{A}_D^{G_{\kappa}^{\text{PRNG}}, t_D}} - \Pr[\hat{e}_{\text{ph}} - \hat{e}_{\text{bit}} > \delta_{\text{gap}}]_{\mathcal{A}_D^{G^{\text{IRNG}}, t_D}} \leq \varepsilon_{\text{PRNG}}, \quad (97)$$

What remains to evaluate the IRNG bit-phase error rate gap.

We first show that the expected value of the bit and phase error matches for the IRNG case. When we have  $D_{\text{PE}} = 0$  or  $D'_{\text{PE}} = 0$ , both bit and phase error would be set to 0,  $\hat{e}_{\text{ph}} = \hat{e}_{\text{bit}}$ , and we can expand the probability

$$\Pr[\hat{e}_{\text{ph}} - \hat{e}_{\text{bit}} > \delta_{\text{gap}}]_{\mathcal{A}_D^{G^{\text{IRNG}}, t_D}} = p_{\Omega}^2 \Pr[e_{\text{ph}} - e_{\text{bit}} > \delta_{\text{gap}} | \Omega, \Omega']_{\mathcal{A}_D^{G^{\text{IRNG}}, t_D}}. \quad (98)$$

This conditional probability matches the probability of the phase-bit error gap exceeding  $\delta_{\text{gap}}$ , when the phase error and bit error are drawn from the conditional state  $\rho_{\theta ABE|\Omega}^{\text{IRNG}}$  in both instances instead. By assumption, when IRNG is utilised,  $\theta$  is independent of the prepared quantum state. Furthermore, since  $\Omega$  is decided from  $E$ ,  $\rho_{\theta ABE|\Omega}^{\text{IRNG}} = \tau_{\theta} \otimes \rho_{ABE|\Omega}^{\text{IRNG}}$ . Let  $e_i = Y_{A,i} \oplus Y_{B,i}$  and  $e'_i = \bar{Y}_{A,i} \oplus \bar{Y}_{B,i}$  be the bit error and phase error of round  $i$  of the two instances. Since  $\theta$  is uniformly random, the post-measurement state  $\rho_{Y_A Y_B|\Omega}$  and  $\rho_{\bar{Y}_A \bar{Y}_B|\Omega'}$  are identical (after tracing out  $\theta E$ ). As such, noting that errors between rounds can be correlated, we have that the expected bit and phase error matches, conditioned on earlier rounds,  $\mathbb{E}[e_i | e_1^{i-1}] = \mathbb{E}[e'_i | e_1'^{i-1}]$ , where the indexing  $e_i^j = e_i \cdots e_j$ .

Here, we demonstrate that both the bit and phase error are close to some combination of the conditional expectation value  $\mathbb{E}[e_i | e_1^{i-1}]$  to find the bit-phase error gap. We define

$$Z_j = \sum_{i=1}^j e_i - \mathbb{E}[e_i | e_1^{i-1}], \quad (99)$$

where  $e_1^{i-1}$  labels the first  $i-1$  outcomes for error measurement. The observed bit error can be expressed as

$$e_{\text{bit}} = \frac{1}{n} \sum_{i=1}^n e_i = \frac{Z_n}{n} - \frac{1}{n} \sum_{i=1}^n \mathbb{E}[e_i | e_1^{i-1}]. \quad (100)$$

The variable  $Z_j$  is bounded, the set  $n$  is finite and

$$\begin{aligned} &\mathbb{E}[Z_j | Z_1, \dots, Z_{j-1}] \\ &= Z_{j-1} + \mathbb{E}[e_j | Z_1, \dots, Z_{j-1}] - \mathbb{E}[e_j | e_1^{j-1}] \\ &= Z_{j-1}, \end{aligned} \quad (101)$$

since  $Z_1, \dots, Z_{j-1}$  values can be computed from  $e_1^{j-1}$  and vice versa, using the values of  $\mathbb{E}[e_i | e_1^{i-1}]$  recursively. These properties implies that  $Z_j$  is a martingale, and since  $|Z_j - Z_{j-1}| \leq 1$ , we can apply the Azuma-Hoeffding inequality [25],

$$\begin{aligned} \Pr[Z_n - Z_0 \leq -n\delta] &\leq e^{-\frac{n\delta^2}{2}} \\ \Pr[Z_n - Z_0 \geq n\delta] &\leq e^{-\frac{n\delta^2}{2}}. \end{aligned} \quad (102)$$

Performing the same analysis for  $e_{ph}$ , we arrive at

$$\begin{aligned} \Pr\left[\sum_{i=1}^n \frac{\mathbb{E}[e_i|e_1^{i-1}]}{n} \geq e_{\text{bit}} + \delta\right] &\leq e^{-\frac{n\delta^2}{2}} \\ \Pr\left[e_{\text{ph}} \geq \sum_{i=1}^n \frac{\mathbb{E}[e'_i|e_1'^{i-1}]}{n} + \delta\right] &\leq e^{-\frac{n\delta^2}{2}}, \end{aligned} \quad (103)$$

where a different (upper or lower) bound is utilised for the two instances.

Since the states are identical, the sum of conditional expectations of  $e_i$  matches. As such, the bit-phase error gap is

$$\Pr[e_{\text{ph}} - e_{\text{bit}} \geq 2\delta|\Omega, \Omega']_{\mathcal{A}_D^{\text{IRNG}, t_D}} \leq 2e^{-\frac{n\delta^2}{2}}. \quad (104)$$

Defining  $\delta_{\text{gap}} = 2\delta$ , the bit-phase error of the algorithm is

$$\Pr[e_{\text{ph}} - e_{\text{bit}} \geq 2\delta|\Omega, \Omega']_{\mathcal{A}_{e_{\text{bit}}, e_{\text{ph}}}^{\text{PRNG}, t_D}} \leq 2e^{-\frac{n\delta^2}{2}} + \frac{\varepsilon_{\text{PRNG}}}{p_{\Omega}^2}. \quad (105)$$

by combining the results. We note that the bit and phase error are obtained from two separate instances of bit value measurement and phase value measurement on identical  $\rho_{\theta ABE}^{\text{PRNG}}|_{\Omega}$  state. Given that the bit error value measured is, with probability larger than  $1 - \varepsilon_{\text{bit}}$ , larger than  $e_{\text{bit}, \text{tol}}$ , we are guaranteed that the phase error value measured on the same state satisfies

$$\Pr[e_{\text{ph}} \geq e_{\text{bit}, \text{tol}} + 2\delta|\Omega, \Omega']_{\mathcal{A}_{e_{\text{bit}}, e_{\text{ph}}}^{\text{PRNG}, t_D}} \leq \varepsilon_{\text{ph}}, \quad (106)$$

where  $\varepsilon_{\text{ph}} = 2e^{-\frac{n\delta^2}{2}} + \frac{\varepsilon_{\text{PRNG}}}{p_{\Omega}^2} + \varepsilon_{\text{bit}}$ . Since the probability no longer depends on the bit error rate  $e_{\text{bit}}$ , we can replace  $\mathcal{A}_{e_{\text{bit}}, e_{\text{ph}}}^{\text{PRNG}}$  with simply a phase error measurement on the common input state,

$$\Pr[e_{\text{ph}} \geq e_{\text{bit}, \text{tol}} + 2\delta|\Omega]_{\mathcal{M}_{\theta A \rightarrow Y} \circ \mathcal{M}_{\theta B \rightarrow Y'}(\rho_{\theta ABE}^{\text{PRNG}}|_{\Omega})} \leq \varepsilon_{\text{ph}}. \quad (107)$$

Further letting  $\varepsilon_{\text{IRNG}} := e^{-\frac{n\delta^2}{2}}$ , a simple rearrangement would yield the theorem.  $\square$

Combining the modified EUR and PRNG results, we can obtain a lower bound on the smooth min-entropy of interest.

**Theorem 31.** Suppose that the basis  $\theta$  is generated from a  $(t', \varepsilon_{\text{PRNG}})$ -quantum secure PRNG, with  $t' \geq t_D$ , and let  $\rho_{\theta ABE}^{\text{PRNG}}$  be the state prepared by the adversary (via protocol  $\mathcal{P}_{\text{Adv}}$ ), where  $A$  and  $B$  are  $n$ -qubit states, and  $\theta$  remain independent when generated by an IRNG,  $\rho_{\theta ABE}^{\text{IRNG}} = \tau_{\theta} \otimes \rho_{ABE}$ . Furthermore, assume the measurement operators of Alice act independently and identically on the subsystems,  $O_A^{\theta, y} = \bigotimes_i O_{A_i}^{\theta_i, y_i}$  and have overlap  $c_{q_1} := \max_{\theta_i} \max_{y_i, \tilde{y}_i} \left\| O_{A_i}^{\theta_i, y_i} (O_{A_i}^{\tilde{\theta}_i, \tilde{y}_i})^\dagger \right\|_{\infty}^2$ , with  $q_1 = \log_2 \frac{1}{c_{q_1}}$ . Let  $\Omega := \{D_{\text{PE}} = 1\}$  be an event that can be decided by  $E$ , then the conditional smooth min-entropy for a protocol with resource utilisation  $t$  (including adversary's resources) be

$$H_{\min}^{\sqrt{2\varepsilon_{\text{ph}}}}(Y|\theta E)_{\mathcal{M}_{\theta A \rightarrow Y}(\rho_{\theta ABE}^{\text{PRNG}}|_{\Omega})} \geq n[q_1 - h_{\text{bin}}(e_{\text{ph}, \text{tol}})],$$

where

$$\begin{aligned} e_{\text{ph}, \text{tol}} &= e_{\text{bit}, \text{tol}} + 2\sqrt{\frac{2}{n} \ln \frac{1}{\varepsilon_{\text{IRNG}}}} \\ \varepsilon_{\text{ph}} &= 2\varepsilon_{\text{IRNG}} + \frac{\varepsilon_{\text{PRNG}}}{p_{\Omega}^2} + \varepsilon_{\text{bit}}, \end{aligned}$$

$e_{\text{bit}, \text{tol}}$  is the tolerance value for an upper bound on the bit error value, and  $\Pr[e_{\text{bit}} \geq e_{\text{bit}, \text{tol}}|\Omega]_{\mathcal{M}_{\theta A \rightarrow Y_A} \circ \mathcal{M}_{\theta B \rightarrow Y_B}(\rho_{\theta ABE}^{\text{PRNG}}|_{\Omega})} \leq \varepsilon_{\text{bit}}$ .

*Proof.* For the state  $\rho_{\theta ABE}^{\text{PRNG}}$ , we are interested in finding the conditional smooth-min entropy, of  $Y$  conditioned on  $E$ , for the PRNG state conditioned on event  $\Omega$ ,  $H_{\min}^{\varepsilon_{\text{sm}}}(Y|\theta E)_{\mathcal{M}_{\theta A \rightarrow Y}(\rho_{\theta ABE}^{\text{PRNG}}|_{\Omega})}$ . Applying the entropic uncertainty relation presented in Thm. 29 with the bijective function  $f_b(\theta) = \bar{\theta}$ , we get

$$\begin{aligned} & H_{\min}^{\varepsilon_{\text{sm}}}(Y|\theta E)_{\mathcal{M}_{\theta A \rightarrow Y}(\rho_{\theta ABE}^{\text{PRNG}}|_{\Omega})} \\ & \geq q - H_{\max}^{\varepsilon_{\text{sm}}}(\tilde{Y}|\theta B)_{\mathcal{M}_{\bar{\theta} A \rightarrow Y}(\rho_{\bar{\theta} ABE}^{\text{PRNG}}|_{\Omega})} \\ & \geq q - H_{\max}^{\varepsilon_{\text{sm}}}(\tilde{Y}_A|\tilde{Y}_B)_{\mathcal{M}_{\bar{\theta} A \rightarrow \tilde{Y}_A} \circ \mathcal{M}_{\bar{\theta} B \rightarrow \tilde{Y}_B}(\rho_{\bar{\theta} ABE}^{\text{PRNG}}|_{\Omega})}, \end{aligned} \quad (108)$$

where the second inequality is obtained by the data processing inequality [37]. We can expand  $q = \log_2 \frac{1}{c_q}$  with

$$c_q = \max_{\theta} \max_{y, \tilde{y}} \left\| O_A^{\theta, y} (O_A^{\bar{\theta}, \tilde{y}})^{\dagger} \right\|_{\infty}^2, \quad (109)$$

where the bijective function is a flip from  $\theta$  to  $\bar{\theta}$ . Since the measurement operators are assumed to be independent and identical operators with overlap and applied independently on each subsystem  $A_i$ , the norm can be simplified as

$$\begin{aligned} \left\| O_A^{\theta, y} (O_A^{\bar{\theta}, \tilde{y}})^{\dagger} \right\|_{\infty}^2 &= \left\| \otimes_{i=1}^n (O_{A_i}^{\theta_i, y_i}) (\otimes_{i=1}^n (O_{A_i}^{\bar{\theta}_i, \tilde{y}_i}))^{\dagger} \right\|_{\infty}^2 \\ &= \prod_{i=1}^n \left\| F_{A_i}^{\theta_i, y_i} (O_{A_i}^{\bar{\theta}_i, \tilde{y}_i})^{\dagger} \right\|_{\infty}^2 \end{aligned} \quad (110)$$

Taking the maximum  $\theta$  would mean taking the maximum  $\theta_i$  for each index  $i$ . As such, we have  $q = nq_1$ .

From Thm. 30, we know that the state  $\mathcal{M}_{\bar{\theta} A \rightarrow \tilde{Y}_A} \circ \mathcal{M}_{\bar{\theta} B \rightarrow \tilde{Y}_B}(\rho_{\bar{\theta} ABE}^{\text{PRNG}}|_{\Omega})$  has a phase error upper bounded by  $e_{\text{ph, tol}}$  with probability larger than  $1 - \varepsilon_{\text{ph}}$ . As such, there exist a state  $\sigma_{\tilde{Y}_A \tilde{Y}_B}$  that is  $\varepsilon_{\text{ph}}$ -close in trace distance with a maximum phase error of  $e_{\text{ph, tol}}$ . The purified distance of these states can be bounded by  $\sqrt{2\varepsilon_{\text{ph}}}$  [37]. Therefore, if we set  $\varepsilon_{\text{sm}} \geq \sqrt{2\varepsilon_{\text{ph}}}$ , we can upper bound the smooth max-entropy by the max-entropy evaluated on  $\sigma$ ,

$$H_{\max}^{\varepsilon_{\text{sm}}}(\tilde{Y}_A|\tilde{Y}_B)_{\mathcal{M}_{\bar{\theta} A \rightarrow \tilde{Y}_A} \circ \mathcal{M}_{\bar{\theta} B \rightarrow \tilde{Y}_B}(\rho_{\bar{\theta} ABE}^{\text{PRNG}}|_{\Omega})} \leq H_{\max}(\tilde{Y}_A|\tilde{Y}_B)_{\sigma_{\tilde{Y}_A \tilde{Y}_B}}. \quad (111)$$

From Ref. [32], the max-entropy can be computed from the minimum number of bits required to correct for the error. Since the two values can only differ in at most  $\lfloor ne_{\text{ph, tol}} \rfloor$  locations, we have [42]

$$\begin{aligned} H_{\max}(\tilde{Y}_A|\tilde{Y}_B)_{\sigma_{\tilde{Y}_A \tilde{Y}_B}} &\leq \log_2 \sum_{i=0}^{\lfloor ne_{\text{ph, tol}} \rfloor} \binom{n}{i} \\ &\leq nh_{\text{bin}}(e_{\text{ph, tol}}). \end{aligned} \quad (112)$$

which completes the proof.  $\square$

### E.3 Security of decoy-state BB84 with PRNG basis

We can now adapt the min-entropy result to the actual decoy-state BB84 protocol.

**Theorem 32.** *Considering an adversary with resource limitation  $t$  and the use of  $(t', \varepsilon_{\text{PRNG}})$ -secure PRNG with  $t' \geq 2(t + t_{\text{MG}}) + t_{\text{ex}}$ , the min-entropy of interest, which can be described by the steps above, is lower bounded by*

$$H_{\min}^{\varepsilon}(X_{P_2}|\beta P_1 P_2 \tilde{\theta}_{\beta} X'_{P_1} E)_{\rho_{\beta X_{P_2} P_1 P_2 \tilde{\theta}_{\beta} X'_{P_1} E}|\hat{\Omega}_{\text{PE}}} \geq N_{P_2, 1}^{\text{tol}} - N_{P_2, 1}^{\text{tol}} h_{\text{bin}}(e'_{\text{ph, tol}}),$$

where  $\varepsilon \geq \sqrt{2\varepsilon_{\text{ph}}}$ , with

$$\begin{aligned} \varepsilon_{\text{ph}} &= 2\varepsilon_{\text{IRNG}} + \frac{\varepsilon_{\text{PRNG}}}{p_{\Omega_{\text{PE}}}^2} + \varepsilon_{\text{serf}, 1} \\ e'_{\text{ph, tol}} &= e_{\text{bit}, 1, \text{tol}} + g(N_{P_1, 1}^{\text{tol}}, N_{P_2, 1}^{\text{tol}}, \varepsilon_{\text{serf}, 1}) + 2\sqrt{\frac{2}{N_{P_2, 1}^{\text{tol}}} \ln \frac{1}{\varepsilon_{\text{IRNG}}}} \end{aligned}$$

and  $g(a, b, c) = \sqrt{\frac{(b+a)(a+1)}{2a^2b}} \ln \frac{1}{c}$ .

*Proof.* We first reduce the protocol to a worse case protocol to simplify analysis. The choice of decoy state intensity can be delayed, by allowing Alice to first sample a random photon number count for  $n_{rnd}$  rounds,  $N_{\text{PNR}}$ , and select decoy choice by sampling  $v$  based on  $N_{\text{PNR}}$ . In general, the photon numbers  $N_{\text{PNR}}$  can be accessible to the adversary, and any rounds  $Q_i$  where there are multi-photon events could leak the basis and bit value. As such, we let Alice announce the basis and bit value for all rounds with multi-photon events. For single-photon events, preparing BB84 states on system  $Q_i$  is identical to preparing  $|\Phi^+\rangle_{A_i Q_i}$ , and performing measurement on  $A_i$  with the X and Z-basis operators. This modification allows us to delay the measurement on  $A_i$  to a later step. We note that the corresponding measurement operators  $O_{A_i}^{\theta_i, X_i}$  acts independently and identically on the subsystems and has overlap  $q_1 = 1$ , assuming ideal preparation of the BB84 states. As such, we have a worse case of Alice preparing and sending out  $N_{\text{PNR}}$ ,  $\theta_{\geq 2}$ ,  $X_{\geq 2}$ , and  $Q_i$  of single-photon events instead of that in step 1 of the protocol. In fact, WLOG, we can let the adversary prepare the single-photon states, and select  $P$  at the same time, preparing  $\rho_{A_{P_{*,1}} B_{P_{*,1}} E'}$ . For steps 3 and 4, Alice and Bob can operate with simply these single-photon events since  $\tilde{\Omega}_{\text{PE}}$  is decided only on such events. This worse case protocol can thus be summarised as

1. The adversary announces  $\beta$  to Alice and Bob.
2. Alice draws a random photon number count for  $n_{rnd}$  rounds,  $N_{\text{PNR}}$ , based on a probability distribution computed from the intensity and probability settings.
3. From the basis generation seed  $\tilde{\theta}_\beta$  and  $N_{\text{PNR}}$ , Alice announces the basis  $\theta_{\geq 2}$  and random bit string  $X_{\geq 2}$ .
4. The adversary announces  $P$  and prepares accordingly the state  $\rho_{A_{P_{*,1}} B_{P_{*,1}} E'}$ , where  $A_{P_{*,1}}$  is handed to Alice and  $B_{P_{*,1}}$  is handed to Bob, where  $P_{*,1}$  is the set of single-photon events in  $P$ .
5. Bob selects randomly a subset  $P_1$  from set  $P$ . Define  $P_2 = P \setminus P_1$ .
6. Bob measures  $B_{P_1,1}$  to obtain  $X'_{P_1,1}$  and Alice measures  $A_{P_1,1}$  to obtain  $X_{P_1,1}$ .
7. Alice and Bob computes and checks the condition  $\tilde{\Omega}_{\text{PE}}$ , and they announce  $\tilde{\theta}_\beta$ .
8. Alice measures  $A_{P_2,1}$  to obtain  $X_{P_2,1}$ .

Note that  $X_{P_1,0}$  would be announced in the original protocol, but this is simply a random string uncorrelated with the rest of the variables and can be removed from the min-entropy.

We begin by first considering another worse case where Alice truncates the number of single-photon rounds in set  $P_2$  to  $N_{P_2,1}^{\text{tol}}$ , which can occur when  $\tilde{\Omega}_{\text{PE}}$  occurs. For  $\tilde{\Omega}_{\text{PE}}$ , Alice and Bob can replace the subsystem with  $N_{P_2,1}^{\text{tol}}$  Bell states, which does not affect min-entropy since it is evaluated conditioned on  $\tilde{\Omega}_{\text{PE}}$ . As such,

$$H_{\min}^\varepsilon(X_{P_2} | \beta P_1 P_2 \tilde{\theta}_\beta X'_{P_1} E')_{\rho_{\beta X_{P_2} P_1 P_2 \tilde{\theta}_\beta X'_{P_1} E'} | \tilde{\Omega}_{\text{PE}}}} \geq H_{\min}^\varepsilon(X_{P_2^{\text{trunc}}} | \beta P_1 P_2 \tilde{\theta}_\beta X'_{P_1,1} X_{P_1,1} N_{\text{PNR}} X_{\geq 2} E')_{\rho | \tilde{\Omega}_{\text{PE}}}},$$

where trunc superscript indicate truncation.

The state generated,  $\rho_{\beta X_{P_2^{\text{trunc}},1} P_1 P_2 \tilde{\theta}_\beta X'_{P_1,1} N_{\text{PNR}} X_{\geq 2} E' | \tilde{\Omega}_{\text{PE}}}$ , matches that described in EUR, Thm. 31. We note that the state can be expressed as

$$\rho_{X_{P_2^{\text{trunc}},1} \beta \tilde{\theta}_\beta E | \tilde{\Omega}_{\text{PE}}} = \mathcal{M}_{\theta_{P_2,1} A_{P_2,1}^{\text{trunc}} \rightarrow X_{P_2,1}^{\text{trunc}}}(\rho_{\beta \tilde{\theta}_\beta A_{P_2,1}^{\text{trunc}} B_{P_2,1}^{\text{trunc}} E | \tilde{\Omega}_{\text{PE}}}), \quad (113)$$

where  $E = P_1 P_2 X'_{P_1,1} X_{P_1,1} N_{\text{PNR}} X_{\geq 2} E'$ . We note that  $\tilde{\Omega}_{\text{PE}}$  can be determined from  $X'_{P_1,1} X_{P_1,1} N_{\text{PNR}} P_1 P_2$ , which are part of  $E$ . By the fair sampling assumption,  $P_1$  and  $P_2$  are independent of any basis selection. Moreover, if the basis choice  $\theta_{\beta, P_2^{\text{trunc}},1}$  is selected from an IRNG, it would be uniformly random and independent from the adversary (also from  $\beta$ ), since  $\theta_{P_1}$  and  $\theta_{P_2}$  are uncorrelated, i.e. we have  $\tau_{\theta_{P_2,1}}$  and uncorrelated from the rest of the state.

The final quantity to define is  $e_{\text{bit,tol}}$ , which in this case is the phase tolerance bound for the set  $P_{2,1}^{\text{trunc}}$ . This can be obtained by the modified Serfling bound [12, 42], since the choice of sets  $P_1$  and  $P_2$  is random. Since  $\tilde{\Omega}_{\text{PE}}$  gives  $N_{P_1,1}^{\text{tol}}$  as a lower bound on the number of single photon events, and that the bit error rate is upper bounded by  $e_{b,1,\text{tol}}$ , we have that

$$\Pr[e_{\text{bit}} \geq e_{\text{bit},1,\text{tol}} + g(N_{P_1,1}^{\text{tol}}, N_{P_2,1}^{\text{tol}}, \varepsilon_{\text{serf},1})] \leq \varepsilon_{\text{serf},1}. \quad (114)$$

Therefore, we can apply Thm. 31 to arrive at the result.  $\square$

## F Step-Efficient Client Authentication

### F.1 Protocol Description

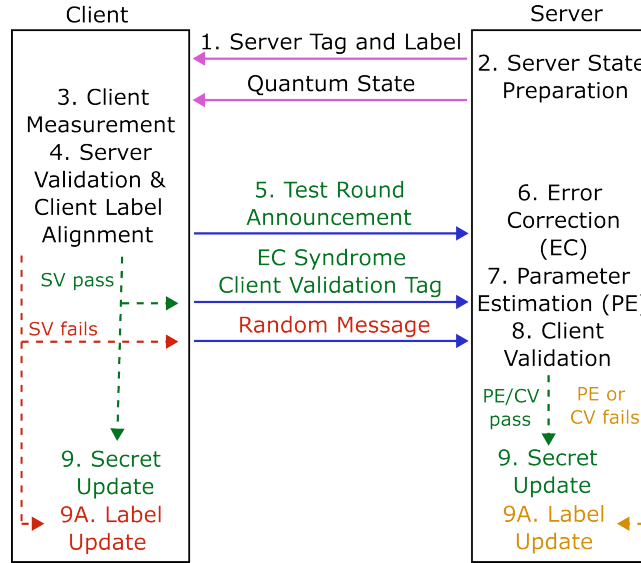


Figure 10: Summary of step-efficient CA protocol with two communication steps. In the first communication step, the server sends quantum states to the client, alongside its tag for validation by the client. After validation and client's measurement, the response would consist of the test round results, client validation tag for server to validate the client's identity, and information for error correction. At the end of the protocol, both parties would separately decide whether to update secrets or the label (indicating a protocol failure).

Inspired by the client authentication protocol in Ref. [17], we developed a step-efficient client authentication (CA) protocol requiring only two communication steps. The key modifications made to the proposed QAKE protocol with pseudorandom basis selection are:

1. Removing server validation since they are not required for client authentication. The validation is instead performed at the start of the next session, where it is required to ensure updated secrets are secure.
2. Replacing label agreement with the server utilising his own index  $\alpha'$  for the session. Any index mismatch would be picked up during client or server validation, and would be corrected with an additional session.

Incorporating these changes, alongside compression of communication rounds, leads to a protocol with two communication steps summarised in Fig. 10.

The client and server pre-share secrets and functions similar to the AKE protocol, except authentication key  $K_2$  and hash function  $h_2$ , which are not necessary in this protocol. The protocol is described in Protocol 3.

### F.2 Security Definition

The security definition for the protocol follows from standard client authentication security requirements. We begin with the first condition of robustness, which guarantees that the protocol should always succeed when a valid client approaches the server. We note that since the protocol has no label agreement step, any mismatch in indices requires 2 sessions to resolve. However, since index mismatch is unlikely in the honest case, we relax the robustness requirement to ensure that authentication passes in 2 sessions (similar to how clients has to try a second time to login when the first login fails). As such, we formally define this two session robustness as

---

**Protocol 3** Step-Efficient Client Authentication

---

*Goal.* Server authenticates client.

1. **Server's Tag and Label:** Server sends its authentication tag  $T_{SV,\alpha'}$  and index  $\alpha'$  to the client.
2. **Server State Preparation:** The server generates a  $n_{rnd}$ -bit basis string using the basis seed,  $\theta'_{\alpha'} = g(\tilde{\theta}'_{\alpha'})$ , randomly chooses a  $n_{rnd}$ -bit string  $X$  and a  $n_{rnd}$ -trit string  $v \in \{0, 1, 2\}^{n_{rnd}}$  according to probability distribution  $p_v$ . The server then sends  $n_{rnd}$  quantum systems  $Q_i$  in phase-randomised coherent BB84 states  $\left\{ \rho_{Q_i}^{\theta'_i, X_i, \mu_{v_i}} \right\}_{i \in [1, n_{rnd}]}$ , with basis  $\theta'_i$ , bit value  $X_i$ , and intensity  $\mu_{v_i}$ , to the client, acting as the "challenge".
3. **Server Validation and Client Label Alignment:** Based on the received label  $\alpha'_r$ , the client aligns its label. If  $\alpha'_r > \alpha$ , the client updates  $\beta = \alpha'_r$  and sets  $D_C = 1$ . If  $\alpha'_r = \alpha$ , the server sets  $\beta = \alpha$  and checks if  $\tilde{T}_{SV,\alpha} = T_{SV,\alpha',r}$ . If it matches, the client sets  $D_C = 1$ . Otherwise, the client sets  $D_C = 0$  and replaces any further responses with a random string. After the alignment is complete, the client sends  $D_C$  and  $\alpha$  to the server.
4. **Client Measurement:** The client measures subsystems  $Q_i$  using basis  $\theta_\beta = g(\tilde{\theta}_\beta)$ , and records outcome  $X'_i$ . If the client detects no clicks, it declares  $X'_i = \perp$ . If multiple clicks are detected, the bit value  $X'_i \in \{0, 1\}$  is randomly selected.
5. **Test Round Announcement:** The client records the detection rounds,  $P = \{i : X'_i \neq \perp\}$ , and randomly splits it into two sets,  $|P_1| = \lceil f_{P_1}|P| \rceil$ . The client announces  $P_1$ ,  $P_2$  and  $X'_{P_1}$ , and the server receives the announcement  $P_{1,r}$ ,  $P_{2,r}$  and  $X'_{P_{1,r}}$ .
6. **Error Correction:** The client generates a syndrome  $syn = f_{syn}(X'_{P_2})$  and forwards it to the server. The server receives the syndrome  $syn_r$  and computes the corrected bit string  $\hat{X}'_{P_2} = f_{ec}(X_{P_{2,r}}, syn_r)$ .
7. **Client Validation:** The client generates a tag  $T_{CV} = h_1(K_1^h, X'_{P_1} || P_1 || P_2 || X'_{P_2} || syn) \oplus K_{1,\beta}^{mask}$  and forwards it to the server. The server receives tag  $T_{CV,r}$  and generates verification tag  $\tilde{T}_{CV} = h_1(K_1^h, X_{P_{1,r}} || P_{1,r} || P_{2,r} || \hat{X}'_{P_2} || syn_r) \oplus K_{1,\alpha'}^{mask}$  and checks if  $T_{CV,r} = \tilde{T}_{CV}$ . If the tags matches, the server validates the client and output  $D_{CV} = 1$ , otherwise, he sets  $D_{CV} = 0$ .
8. **Parameter Estimation:** The server checks if: (1) the number of test rounds matches the expected number  $|P_{1,r}| = \lceil f_{P_1}|P| \rceil$ , (2) number of rounds in set  $P_1$  exceeds a threshold,  $|P_1| \geq P_{1,tol}$ , (3) the lower bound on single-photon events in sets  $P_{2,r}$  and  $P_{1,r}$  (estimated via decoy state analysis) exceeds a threshold,  $\hat{N}_{P_{2,r},1}^{LB} \geq N_{P_{2,r},1}^{tol}$ ,  $\hat{N}_{P_{1,r},1}^{LB} \geq N_{P_{1,r},1}^{tol}$ , (4) the upper bound on single-photon bit-error rate in set  $P_{1,r}$  (estimated via decoy-state analysis) falls below a threshold,  $\hat{e}_{bit,P_{1,r},1}^{UB} \leq e_{bit,1,tol}$ , and (5) the upper bound on bit error rate in set  $P_{2,r}$  (estimated via Serfling bound) falls below a threshold,  $\hat{e}_{bit,P_{2,r}}^{UB} \leq e_{bit,tol}$ . If all checks pass, the server sets  $D_{PE} = 1$ , otherwise it sets  $D_{PE} = 0$ .
9. **Secret Update and Label Update:** The server compares the index received  $\alpha_r$ ,  $D_C$  and its own index  $\alpha'$ . The server first updates  $\alpha_r = \alpha_r + 1$  if  $D_C = 0$ . If updated  $\alpha_r > \alpha'$ , the server sets  $\alpha' = \alpha_r - 1$  and sets  $D_{SA} = 0$ , otherwise he sets  $D_{SA} = 1$  (aligned indices). The client decides whether to generate the server's tag and update the basis seed based on  $D_C$ , while the server decides on the success of the authentication via  $F_S = D_{PE} \wedge D_{CV} \wedge D_{SA}$ . When the client (resp. the server) decides to generate the tag and update the basis seed, i.e.  $D_C = 1$  (resp.  $F_S = 1$ ), it performs privacy amplification  $\tilde{T}_{SV,\beta} || \tilde{\theta}_\beta = h_{PA}(R, X'_{P_2})$  (resp.  $T_{SV,\alpha'} || \tilde{\theta}'_{\alpha'} = h_{PA}(R, \hat{X}'_{P_2})$ ) and sets  $\alpha = \beta$ . If basis seed update and server tag generation is not performed, then the client (resp. the server) would update its label,  $\alpha = \beta + 1$  (resp.  $\alpha' = \alpha' + 1$ ).

---

**Definition 8** ( $\varepsilon_{2,rob}$ -2-session-robustness). A CA protocol is  $\varepsilon_{2,rob}$ -2-session-robustness if it passes with high probability in the absence of any adversary in either of the next two rounds, i.e. it fails to pass both rounds with low probability

$$\Pr[F_{S,j} = 0, F_{S,j+1} = 0] \leq \varepsilon_{rob},$$

where  $F_{S,i}$  refers to the server's label in the  $i$ -th round, and  $j \in [1, n_{sess} - 1]$ , where  $n_{sess}$  is the maximum number of sessions.

We note here that there can be other ways of defining the robustness condition. One such method is to assume that all prior sessions of the protocol are performed in the absence of an adversary. This is unlikely

to result in any index mismatch at the current session, and thus robustness can be guaranteed with high probability with a single session.

The second security condition in client authentication requires that a server interacting with an invalid client (or adversary) return an authentication failure with high probability. As such, when the authentication passes, the server can be highly confident that the client is valid. Therefore, we formally define the client authentication condition as

**Definition 9** ( $\varepsilon_{CV}$ -client validation). *An CA protocol has  $\varepsilon_{CV}$ -client validation if the authentication fails with high probability when the adversary attempts to impersonate the client, i.e.*

$$\Pr[F_S = 1 | D_C = \phi] \leq \varepsilon_{CV}.$$

While there is no imposition on the secrets of the protocol, they would obey additional conditions for future sessions to remain secure. This separate security condition has the same definition as shared secrets privacy in QAKE, albeit with different ideal input and output states.

### F.3 Overall Protocol Security

We can similarly define a  $n_{sess}$ -session protocol of CA, where all sessions has to satisfy the security condition, with each session satisfying some  $\varepsilon_{sec,i}$ -security condition defined by the trace distance from the ideal output state with  $\Pr[F_S = 1, D_C = \phi] = 0$ . We follow the same idea from Appendix. C.1 to reduce the multi-session analysis to single session, where additional shared secret preservation is necessary in the intermediate steps. However, since there is only a single security condition, client authentication, we shall examine both conditions together, defining the overall security as

$$\Delta(\rho_{D_C F_S LSE}, \rho_{D_C F_S LSE}^{\text{ideal, int}}) \leq \varepsilon_{sec, int}, \quad (115)$$

and it remains to identify the set of ideal input and output states.

The main difference in the identification of ideal input/output states for this protocol is the ability of the adversary to gain partial information of secrets and partial control of the client's action. Firstly, the client's tag can almost always be generated since there is no server check during the session itself. This leads to the authentication key  $K_1^h$  and authentication masking key  $K_{1,\beta}^{\text{mask}}$  being correlated with the adversary, although this correlation is via the tag  $T_{CV}$ . This is without a corresponding trace of the authentication masking key in the session since the client's index is not updated, though one expects the corresponding trace to occur when the client performs the server check in later sessions. Secondly, the generation of the server's tag verification value by the client,  $\tilde{T}_{SV,\alpha}$ , can be sometimes influenced by the adversary when it has prior knowledge of the basis generation seed. However, the adversary would not have direct access to this value since it is not announced. To account for these two leakages/controls available to the adversary, we define two oracles, the first  $\mathcal{E}_{K_1^h K_{1,\beta}^{\text{mask}} M_{CV} \rightarrow T_{CV}}$ , allows the adversary to choose any message  $M_{CV}$  and have the corresponding client tag generated for him. The second  $\mathcal{E}_{RM_{SV} \rightarrow \tilde{T}_{SV,\alpha}}$  allows the adversary to select any message  $M_{SV}$ , and generate the server authentication check tag for the client, who would utilise it to perform checks in later sessions when necessary. Note that for simplicity, we will label the oracles as  $\mathcal{E}_{K_1^h K_{1,\beta}^{\text{mask}} E \rightarrow E'}$  and  $\mathcal{E}_{RE \rightarrow \tilde{T}_{SV,\alpha} E'}$  since the adversary would decide the messages according to its system  $E$ , and  $T_{CV}$  is implicitly included in  $E'$  since it is directly accessible to the adversary.

To monitor the secrets and oracles accessible, we introduce a new label  $\alpha^U$ , which indicates the client's index if the server authentication is performed in the same session.  $\alpha^U$  is updated as follows: (1) if  $D_C = \phi$  within a session, leave  $\alpha^U$  unchanged, (2) if  $\alpha'_r \geq \alpha^U$ , set  $\alpha^U = \alpha'_r$ , and (3) if  $D_C = 1$  and  $F_S \neq 1$ , set  $\alpha^U = \alpha^U + 1$ . The second scenario occurs when the client's index is updated to an index that may not fail in the next session, while the third scenario requires that the server not pass server validation since server did not participate/did not select a server authentication tag that matches the client's. A general input state can be defined as a mixture of two variants of states  $\rho^{in} = \sum_{jj'} p_{jj'} \rho_{LSE}^{\text{in}, jjj'} + p_{j,j+1,j'} \rho_{LSE}^{\text{in}, j,j+1,j'}$ , where

$$\begin{aligned} \rho_{LSE}^{\text{in}, jjj'} &= |jjj'\rangle\langle jjj'|_{\alpha\alpha^U\alpha'} \otimes \rho_{SE}^{\text{in}, jjj'} \\ \rho_{SE}^{\text{in}, jjj'} &= \tau_{RK_{1,[j,m]}^{\text{mask}}} \otimes \tilde{\tau}_{\tilde{\theta}_{[j_{\max}, m]} \tilde{\theta}'_{[j_{\max}, m]}} \otimes \mathcal{E}_{K_1^h K_{1,[j',j-1]}^{\text{mask}} E' \rightarrow E}(\tau_{K_1^h K_{1,[j',j-1]}^{\text{mask}}} \otimes \rho_{E'}), \end{aligned} \quad (116)$$

$j_{\max} = \max\{j, j'\}$ , and  $E'$  contains the lost secrets  $\tilde{\theta}_{[1, j_{\max}-1]} \tilde{\theta}'_{[1, j_{\max}-1]}$ , and the state

$$\begin{aligned} \rho_{LSE}^{\text{in}, j, j+1, j'} &= |j, j+1, j'\rangle \langle j, j+1, j'|_{\alpha \alpha^U \alpha'} \otimes \rho_{SE}^{\text{in}, j, j+1, j'} \\ \rho_{SE}^{\text{in}, j, j+1, j'} &= \tau_{K_{1, [j+1, m]}^{\text{mask}}} \otimes \tilde{\tau}_{\tilde{\theta}_{[j_{\max}, m]}^U} \tilde{\theta}'_{[j_{\max}, m]} \otimes \mathcal{E}_{RK_1^h K_{1, [j', j]}^{\text{mask}}} E' \rightarrow \tilde{T}_{SV, j} E (\tau_{RK_1^h K_{1, [j', j]}^{\text{mask}}} \otimes \rho_{E'}), \end{aligned} \quad (117)$$

and  $j_{\max}^U = \max\{j+1, j'\}$ , and the oracle access for  $\mathcal{E}_{K_1^h K_{1, [j', j-1]}^{\text{mask}}} E' \rightarrow E$  and  $\mathcal{E}_{RK_1^h K_{1, j}^{\text{mask}}} E' \rightarrow \tilde{T}_{SV, j} E$  can have any order of  $\mathcal{E}_{K_1^h K_{1, \beta}^{\text{mask}}} E \rightarrow T_{CV} E'$  and  $\mathcal{E}_{RE \rightarrow \tilde{T}_{SV, \alpha} E'}$  in general. As such, we can link the two input state

$$\rho_{SE}^{\text{in}, j, j+1, j'} = \mathcal{E}_{RE' \rightarrow \tilde{T}_{SV, j} E} \circ \mathcal{E}_{K_1^h K_{1, j}^{\text{mask}}} E'' \rightarrow E' (\rho_{SE''}^{\text{in}, j+1, j+1, j'}), \quad (118)$$

which would be useful to simplify the analysis.

The set of ideal output state  $\mathcal{S}'_{out}$  has form  $\rho^{\text{out}} = \sum_{j, j^U \in \{j, j+1\}, j'} p_{jj^U j'} \rho^{\text{out}, jj^U j'}$  with the form

$$\begin{aligned} \rho^{\text{out}, jj^U j'} &= |\phi 0\rangle \langle \phi 0|_{D_C F_S} \otimes \sum_{\tilde{j} \geq j'+1} p_{\phi 0, \tilde{j}} \otimes \sigma_{LSE}^{\phi 0, jj^U, \tilde{j}'} + p_{0\phi} |0\phi\rangle \langle 0\phi|_{D_C F_S} \otimes \sigma_{LSE}^{0\phi, j+1, j+1, j'} \\ &+ |1\phi\rangle \langle 1\phi|_{D_C F_S} \otimes \sum_{\tilde{j} \geq j} p_{1\phi, \tilde{j}} \sigma_{LSE}^{1\phi, \tilde{j}, \tilde{j}+1, j'} + |00\rangle \langle 00|_{D_C F_S} \otimes \sum_{\tilde{j}' \geq j'+1} p_{00, \tilde{j}'} \sigma_{LSE}^{00, j+1, j+1, \tilde{j}'} \\ &+ |10\rangle \langle 10|_{D_C F_S} \otimes \sum_{\tilde{j} \geq j, \tilde{j}' \geq j'+1} p_{10, \tilde{j}\tilde{j}'} \sigma_{LSE}^{10, \tilde{j}, \tilde{j}+1, \tilde{j}'} + p_{11} |11\rangle \langle 11|_{D_C F_S} \otimes \sigma_{LSE}^{11, j' j' j'}, \end{aligned} \quad (119)$$

where  $\sigma_{LSE}^{f_A f_B, jj^U j'} \in \mathcal{S}_{in}$ . Note that unlike the QAKE protocol where  $D_C = 1$  is disallowed when  $F_S = \phi$ , the lack of a check for server validation in the same session allows an adversary to request  $T_{SV, \alpha'}$  from the server in a separate session and pass the server validation, i.e.  $D_C = 1$ . However, the mismatch of  $\alpha$  and  $\alpha^U$  guarantees that the next session with client involvement would result in  $D_C = 0$ , and an update of  $\alpha$  to indicate no confidence in the updated secrets.

By definition, the output state belongs to  $\mathcal{S}_{in}$ , thereby satisfying condition 3 in Thm. 1 when reducing to single round security. Condition 1 is trivially satisfied since all secrets remain private and indices begin with 1. As such, the security analysis reduces to the single-session security analysis for a single input component. The security can be summarised as

**Theorem 33.** *The CA protocol is secure with security parameter*

$$\begin{aligned} \varepsilon_{\text{sec, int}} &= 4\sqrt{2\varepsilon_{\text{ph}}} + 2\varepsilon_2 + 6\varepsilon_{\text{match}} + 5\varepsilon_{\text{MAC}, 1} + 2\varepsilon_{\text{ds}} + \frac{1}{2} \times 2^{-\frac{1}{2}[N_{P_2, 1}^{\text{tol}}[1-h_{\text{bin}}(e'_{\text{ph, tol}})]-l_{\tilde{\theta}}-\log_2 |\mathcal{T}_{SV}| |\mathcal{T}_{CV}| - \text{leak}_{\text{EC}}]} \\ &+ \sqrt{|\mathcal{T}_{CV}| \varepsilon_{\text{MAC}, 1} - 1 + 2^{\log_2 |\mathcal{T}_{CV}| + \log_2 \left(\frac{2}{\varepsilon_2} + 1\right) - N_{P_2, 1}^{\text{tol}}[1-h_{\text{bin}}(e'_{\text{ph, tol}})] + \text{leak}_{\text{EC}}}} + \frac{1}{|\mathcal{T}_{CV}|} + \frac{1}{|\mathcal{T}_{SV}|}, \end{aligned}$$

where  $\varepsilon_{\text{match}} = 2^{-P_{1, \text{tol}}[1-h_{\text{bin}}(e_{\text{bit, tol}})]}$ ,  $\varepsilon_{\text{ph}}$  is related to the smoothing parameter for decoy state with PRNG basis (Thm. 32),  $\varepsilon_{\text{ds}}$  accounts for errors associated with decoy state analysis,  $|\mathcal{T}_{CV}|$  and  $|\mathcal{T}_{SV}|$  are the size of the respective tags,  $\text{leak}_{\text{EC}}$  is the information leakage from error correction,  $N_{P_2, 1}^{\text{tol}}$  is the minimum tolerated number of single photon rounds in set  $P_2$ ,  $e'_{\text{ph, tol}}$  is the phase error tolerance inclusive of the correction due to Serfling bound and  $\varepsilon_2$  is a variable to optimise over.

*Sketch Proof.* We need to analyse the security for the two different input states  $\rho_{LSE}^{\text{in}, jjj'}$  and  $\rho_{LSE}^{\text{in}, j, j+1, j'}$ . In Thm. 35, we show that the security of  $\rho_{LSE}^{\text{in}, j, j+1, j'}$  can be related to the security of  $\rho_{LSE}^{\text{in}, jjj'}$ . The key observation for this proof is that only in one specific scenario where  $\alpha'_i \geq j+1$  and  $j \neq j'$ , i.e. the adversary forces the client's index to update to one  $\geq j+1$ , the client would proceed in the protocol using the updated index – and that matches with the case where the client begins with an index  $j+1$  and a restricted adversary. In all other cases, we have that the authentication fails with high probability,  $F_S = 0$ , (argued in Thm. 34) and the output state matches the ideal case closely.

With the reduction, focus is placed on the input state  $\rho_{LSE}^{\text{in}, jjj'}$ . The analysis can be broken in different scenarios based on the  $(D_C, F_S)$  values. Thm. 36 presents the case when the adversary tries to cheat the server without the client,  $D_C = \phi$ , for which the security is a consequence of Thm. 34 ensuring  $F_S = 0$  with

high probability. The case where the adversary tries to gain information from the client,  $F_S = \phi$ , is shown in Thm. 37. Since the adversary can in general trigger the client to proceed with the protocol, leakage of the basis seed, the announcement of  $T_{CV}$  and providing control to  $\tilde{T}_{SV,j}$  follow. However, this is exactly the situation accounted for as part of the input state definition for  $\alpha^U = \alpha + 1$ .

For cases where neither  $D_C$  nor  $F_S$  are  $\phi$ , both client and server are involved in the protocol. Similar to earlier analysis in Sec. D.2.3, we can simplify the analysis by defining idealised version of  $D_{PE}$  and  $D_C$ , with small penalty shown in Eqn. (126). With this change, when  $D_C = 0$ , Thm. 38 shows that similar to the  $D_C = \phi$  case,  $\tilde{F}_S = 0$  with high probability, and the leakage of  $T_{SV,j'}$  and  $\tilde{\theta}_{j'}$  can be accounted for by the updated index ( $j'$  index no longer utilised). When  $D_C = 1$  and  $\tilde{F}_S = 0$  ( $F_S$  but with ideal checks), the adversary can easily exploit the protocol to gain access to the oracle generating  $T_{AV}$  and have control over the generation of  $\tilde{T}_{SV,\alpha}$ . However, as shown in Thm. 39, this is exactly accounted for when  $\alpha^U$  is updated such that  $\alpha^U = \alpha + 1$ . Finally, Thm. 40 shows that in the case of  $D_C = \tilde{F}_S = 1$ , the ideal checks guarantee that  $X'_{P_2}$  has high min-entropy based on Thm. 32, thereby allowing the authentication key, authentication masking keys and  $R$  to remain secret.  $\square$

### F.3.1 Security for $\alpha^U \neq \alpha$ input state

Before beginning our analysis, let us define a useful theorem regarding the value of  $F_S$  when  $D_C \neq 1$ .

**Theorem 34.** *For any ideal input state  $\sigma_{LSE} \in \mathcal{S}_{in}$  where the adversary has no access to the basis seed  $\tilde{\theta}_{j'}$  and oracle  $\mathcal{E}_{K_1^h K_{1,j'}^{mask} M_{CV} \rightarrow T_{CV}}$ ,*

$$\Pr[F_S = 1 | D_C \neq 1] \leq \frac{1}{|\mathcal{T}_{CV}|}$$

On the other hand, if the oracle and basis seed is accessible

$$\Pr[F_S = 1 | D_C \neq 1] \leq \varepsilon_{MAC,1} + \varepsilon_{match},$$

where the matching probability is

$$\varepsilon_{match} = 2^{-|P_{1,tol}|[1-h_{bin}(e_{bit,tol})]},$$

noting that  $|\tilde{P}_1| \geq P_{1,tol}$ , where  $\tilde{P}_1$  is the set  $P_1$  as decided in the message  $M_{CV}$ .

*Proof.* Let us first consider the case where the oracle and basis seed are inaccessible. While the adversary may have some control of the message  $M_r$  sent to the client, since the adversary has no knowledge of  $K_1^h$  and  $K_{1,j'}^{mask}$ , the uniformity property of the strongly 2-universal hash function ensures that

$$\Pr[F_S = 1 | D_C \neq 1] \leq \Pr[T_{CV,r} = h_1(K_1^h, M_r || f(M_r, X)) \oplus K_1^{mask}] \leq \frac{1}{|\mathcal{T}_{CV}|}, \quad (120)$$

where  $f(M_r, X)$  labels the other terms required in the hash described in step 7 of the main protocol, for any  $T_{CV,r}$  selected by the adversary.

When access to the basis seed and oracle are available, the adversary is able to perform a call to the oracle for any message  $M_{CV}$ , receive the outcome  $T_{CV}$ , before given access to  $X$ , and deciding on the message  $M_r$  and tag  $T_{CV,r}$  to send to the server. Crucially, this forces the adversary to commit to a  $\tilde{P}_1$  set and  $\tilde{X}_{\tilde{P}_1}$  bit values when performing the oracle call. We can simplify the probability

$$\begin{aligned} & \Pr[D_{CV} \wedge D_{PE} = 1] \\ & \leq \Pr[D_{PE} = 1, (M_r || f(M_r, X)) \neq M, T_{CV,1,r} = \tilde{T}_{CV,1}] + \Pr[D_{PE} = 1, (M_r || f(M_r, X)) = M, T_{CV,1,r} = \tilde{T}_{CV,1}] \\ & \leq \Pr[T_{CV,1,r} = \tilde{T}_{CV,1} | (M_r || f(M_r, X)) \neq M] + \Pr[D_{PE} = 1, (M_r || f(M_r, X)) = M] \\ & \leq \varepsilon_{MAC,1} + \Pr[wt(X'_{P_{1,r}} \oplus X_{P_{1,r}}) \leq |P_{1,r}|e_{bit,tol}, \tilde{P}_1 = P_{1,r}, X'_{P_{1,r}} = \tilde{X}_{\tilde{P}_1}, |P_{1,r}| \geq P_{1,tol}] \\ & \leq \varepsilon_{MAC,1} + \Pr[wt(\tilde{X}_{\tilde{P}_1} \oplus X_{\tilde{P}_1}) \leq |\tilde{P}_1|e_{bit,tol}, |\tilde{P}_1| \geq P_{1,tol}] \\ & \leq \varepsilon_{MAC,1} + \max_{|\tilde{P}_1| \geq P_{1,tol}} \sum_{i=0}^{|\tilde{P}_1|e_{bit,tol}} \binom{|\tilde{P}_1|}{i} 2^{-|\tilde{P}_1|} \\ & \leq \varepsilon_{MAC,1} + 2^{-P_{1,tol}[1-h_{bin}(e_{bit,tol})]}. \end{aligned} \quad (121)$$

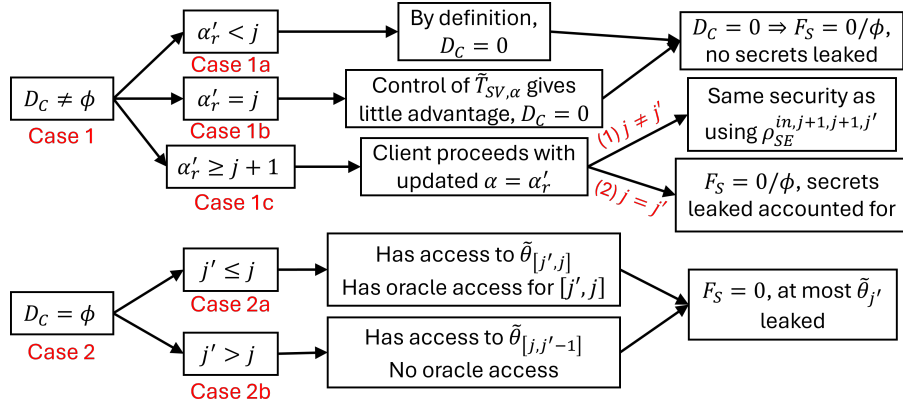


Figure 11: Schematic of the proof of Thm. 35.

The first inequality splits the probability based on the equality of the messages, and the second line simplifies them by removing some conditions. The third line notes that by the strongly 2-universal property of the hash function, with the keys not known to the adversary except via  $T_{CV}$ , the probability that the adversary can guess the correct tag for input  $(M_r || f(M_r, X))$  is bounded by  $\varepsilon_{MAC,1}$ . The third and fourth lines further removes conditions on  $D_{PE} = 1$  and the messages being equal, and focuses mainly on terms we can use to bound the probability, where  $\tilde{P}_1$  and  $\tilde{X}_{\tilde{P}_1}$  are the corresponding terms from the message  $M$ . The fifth line expands the probability of the bound on the Hamming weight, noting that the  $X$  is randomly generated and uncorrelated to  $\tilde{X}_{\tilde{P}_1}$ , which has to be decided before  $X$  is accessible to the adversary. The final line uses the property of the binomial coefficient to simplify, and noting that the maximum value corresponds to  $|\tilde{P}_1| = P_{1,tot}$ . It is clear that the result upper bounds  $\Pr[F_S = 1 | D_C \neq 1]$ .  $\square$

Here, we provide a reduction of the security for input state variants with  $\alpha^U = \alpha + 1$  to the security for input state variants with  $\alpha^U = \alpha$ , the latter of which we analyse in the later sections.

**Theorem 35.** Consider the CA protocol  $\mathcal{P}$ . Suppose that for any valid input state  $\rho_{LSE}^{in,j+1,j+1,j'}$  and adversarial strategy, there exists an ideal output state  $\rho^{out} \in \mathcal{S}'_{out}$  such that

$$\Delta(\mathcal{P}(\rho_{LSE}^{in,j+1,j+1,j'}), \rho^{out}) \leq \varepsilon_{sec}.$$

Then, for any valid input state  $\rho_{LSE}^{in,j,j+1,j'}$ , there exists an output state  $\rho^{out} \in \mathcal{S}'_{out}$  such that

$$\Delta(\mathcal{P}(\rho_{LSE}^{in,j,j+1,j'}), \rho^{out}) \leq \varepsilon_{sec} + \frac{1}{|\mathcal{T}_{CV}|} + \frac{1}{|\mathcal{T}_{SV}|} + 2\varepsilon_{MAC,1} + 2\varepsilon_{match}.$$

*Proof.* The protocol consists of three general steps:

1. Server's state generation and message.
2. Client's message receipt and response.
3. Server and Client post-processing.

where WLOG, the third step will always occur at the end of the protocol since it does not contain additional outputs to the adversary. Moreover, since the server's state generation and message requires no external inputs, the adversary will find no advantage in delaying it. As such, we can always take the protocol as one which follows the three step process. Fig. 11 provides a schematic of the proof for the different cases discussed below.

Let us consider first the case where the client is involved in the protocol,  $D_C \neq \phi$  (case 1). Furthermore, let us consider the case where  $\alpha'_r < j$  (case 1a), the client sets  $D_C = 0$  by the protocol. If instead  $\alpha'_r = j$  (case 1b), the decision would depend on  $\tilde{T}_{SV,j}$  and  $T_{SV,\alpha',r}$ . Since the adversary has oracle access for  $R$ , it is able to choose a message  $M_{SV}$  and have the client generate  $\tilde{T}_{SV,j} = h_{PA}(R, M_{SV})$ . Since  $R$  itself is inaccessible to the adversary, the uniformity property of the hash function means that

$$\Pr[D_C = 1 | \alpha'_r = j] = \Pr[\tilde{T}_{SV,j} = T_{SV,\alpha',r}] \leq \frac{1}{|\mathcal{T}_{SV}|}, \quad (122)$$

and the client sets  $D_C = 0$  with high probability. In both cases, if  $F_S = \phi$ , then no secrets are leaked and shared secrets privacy is maintained. Otherwise, when  $D_C = 0$ , then from Thm. 34, whether an oracle is accessible or not,  $\Pr[F_S = 1 | D_C = 0] \leq \varepsilon_{\text{MAC},1} + \varepsilon_{\text{match}}$ , i.e.  $F_S = 0$  with high probability. When  $D_C = 0$  and  $F_S = 0$ , only  $\tilde{\theta}_{j'}$  may in general be leaked to the adversary from the server state prepared. If  $j + 1 > j'$ , this information has already been assumed to be accessible to the adversary by the form of the input state. If instead  $j + 1 \leq j'$ , since  $\alpha'$  is increased by 1 when the authentication fails,  $F_S = 0$ , and this leakage is allowed (i.e. the ideal input state includes this leakage). Therefore, one is able to find an ideal output state with trace distance

$$\Delta(\mathcal{P}(\rho^{\text{in},j,j+1,j'})_{\wedge D_C \neq \phi}, \rho^{\text{out}}_{\wedge D_C \neq \phi}) \leq \frac{1}{|\mathcal{T}_{\text{SV}}|} + \varepsilon_{\text{MAC},1} + \varepsilon_{\text{match}} \quad (123)$$

from the actual output state.

In the case where  $\alpha'_r \geq j + 1$  (case 1c), the client updates  $\alpha$  to  $\alpha'_r$  and set  $D_C = 1$ .

Note that this implicitly means that the adversary does not utilise the  $\mathcal{E}_{\text{RM}_{\text{SV}},j \rightarrow \tilde{T}_{\text{SV}},j}$  oracle during this session and future sessions. After updating  $\alpha$ , the client proceeds with the protocol using the updated  $\alpha$ , and its action would be similar with one where the protocol begins with  $\rho^{\text{in},j+1,j+1,j'}$  instead, and for adversarial strategies which ensures  $D_C = 1$ . The main difference between starting with  $\rho^{\text{in},j,j+1,j'}$  and  $\rho^{\text{in},j+1,j+1,j'}$  then would be the access to the oracle  $\mathcal{E}_{K_{1,j}^{\text{h}} K_{1,j}^{\text{mask}} M_{\text{CV}} \rightarrow T_{\text{CV},j}}$  if  $j \geq j'$ . If we consider (1)  $j \neq j'$ , starting with either state makes no difference since  $K_{1,j}^{\text{mask}}$  is not utilised in the client validation step. This implies that the state  $\rho^{\text{out}} \in \mathcal{S}'_{\text{out}}$  for which  $\Delta(\mathcal{P}(\rho^{\text{in},j+1,j+1,j'}), \rho^{\text{out}}) \leq \varepsilon_{\text{sec}}$  is also close to the case when  $\rho^{\text{in},j,j+1,j'}$  is utilised, i.e.

$$\Delta(\mathcal{P}(\rho^{\text{in},j+1,j+1,j'})_{\wedge D_C \neq \phi, \alpha'_r \geq j+1}, \rho^{\text{out}}_{\wedge D_C \neq \phi, \alpha'_r \geq j+1}) \leq \varepsilon_{\text{sec}}. \quad (124)$$

In the case where (2)  $j = j'$ , since the client does not generate  $T_{\text{CV},j}$  during the protocol (recall  $\alpha \geq j + 1$ ), the adversary has to rely on the oracle to pass,  $F_S = 1$ . From Thm. 34, the probability of such an event is maximally  $\varepsilon_{\text{MAC},1} + \varepsilon_{\text{match}}$ . In this case, we therefore have  $F_S = 0$  or  $F_S = \phi$ . Since the client accepts the round,  $D_C = 1$ , additional oracles  $\mathcal{E}_{K_{1,j}^{\text{h}} K_{1,j}^{\text{mask}} M_{\text{CV}} \rightarrow T_{\text{CV},j}}$  and  $\mathcal{E}_{\text{RM}_{\text{SV}} \rightarrow \tilde{T}_{\text{SV}},j}$  for  $\tilde{j}$  representing the updated  $\alpha$  value are provided to the adversary, and the basis seeds  $\tilde{\theta}_{\tilde{j}}$  and  $\tilde{\theta}_{j'}$  are leaked. Since  $F_S \neq 1$  and  $D_C = 1$ , we have that the final index is  $\alpha = \tilde{j}$  and  $\alpha^U = \tilde{j} + 1$ , for which this leakage and additional oracle accesses are accounted for in the ideal output state (see form of  $\rho^{\text{in},j,j+1,j'}$ ).

Let us now consider the case where  $D_C = \phi$  (case 2), where the client is not involved in the protocol.

When  $j' \leq j$  (case 2a), the adversary would have access to  $\tilde{\theta}_{[j',j]}$  and oracle access to generate  $T_{\text{CV},i}$  for  $i \in [j',j]$ . From Thm. 34, this would result in the server rejecting the session with high probability,  $\Pr[F_S = 1 | D_C = \phi] \leq \varepsilon_{\text{MAC},1} + \varepsilon_{\text{match}}$ . Therefore, since  $F_S = 0$  would result in no further leakage except  $\tilde{\theta}_{j'}$ , which is already accessible to the adversary, we can find an ideal output state close to it. In the other case where  $j' > j$  (case 2b), the adversary has no oracle access. By Thm. 34, the probability of  $F_S = 1$  is bounded by  $\frac{1}{|\mathcal{T}_{\text{CV}}|}$ . From the server state generation,  $\tilde{\theta}_{j'}$  can be leaked. However, since  $\alpha'$  is updated when  $F_S = 0$  and  $j' > j$ ,  $j_{\text{max}} > j'$  and thus the leakage of  $\tilde{\theta}_{j'}$  is accounted for in the ideal state.

Combining the results, the trace distance can be reduced to  $\varepsilon_{\text{sec}} + \frac{1}{|\mathcal{T}_{\text{CV}}|} + \frac{1}{|\mathcal{T}_{\text{SV}}|} + 2\varepsilon_{\text{MAC},1} + 2\varepsilon_{\text{match}}$ .  $\square$

### F.3.2 One-Sided Attack

With accounting for all input state variant  $\rho^{\text{in},j,j+1,j'}$  complete, we present the security for input state variant  $\rho^{\text{in},jjj'}$  where only one party is involved in the protocol. We begin with the case of  $D_C = \phi$ ,

**Theorem 36.** *Consider the CA protocol  $\mathcal{P}$ . Then, for any valid input state  $\rho^{\text{in},jjj'}$ , there exists  $\rho^{\text{out}} \in \mathcal{S}'_{\text{out}}$  such that*

$$\Delta(\mathcal{P}(\rho^{\text{in},jjj'})_{\wedge D_C = \phi}, \rho^{\text{out}}_{\wedge D_C = \phi}) \leq \varepsilon_{\text{MAC},1} + \varepsilon_{\text{match}}.$$

*Proof.* This proof follows closely that of case 2 in Thm. 35. Let us consider two scenarios separately:  $j \leq j'$  and  $j > j'$ . For the case of  $j \leq j'$ , the adversary has no access to any oracles but has access to  $\tilde{\theta}_{[j,j'-1]}$ . From Thm. 34,  $\Pr[F_S = 1] \leq \frac{1}{|\mathcal{T}_{\text{CV}}|}$  and the authentication fails with high probability. In terms of secrets leaked,  $\tilde{\theta}_{j'}$  is leaked from the server state generation. However, since  $F_S = 0$  prompts the server to update index  $\alpha'$  and  $j' \geq j$ , the leakage of  $\tilde{\theta}_{j'}$  would have been accounted for in the ideal state since  $j_{\text{max}}$  is increased.

For the second case of  $j \geq j' + 1$ , the adversary has knowledge of  $\tilde{\theta}_{[j',j-1]}\tilde{\theta}'_{[j',j-1]}$ , and with oracle access from  $K_{1,j'}^{\text{mask}}$  to  $K_{1,j-1}^{\text{mask}}$ , where the relevant values  $\tilde{\theta}'_{j'}$  and oracle access for  $K_{1,j'}^{\text{mask}}$  are present. From Thm. 34, the authentication will fail with high probability,  $\Pr[F_S = 1|D_C = \phi] \leq \varepsilon_{\text{MAC},1} + \varepsilon_{\text{match}}$ . As such, no additional secret is leaked since  $\tilde{\theta}_{j'}$  is already assumed to be accessible to the adversary prior to the session.  $\square$

Another one-sided attack involves  $F_S = \phi$ , where the adversary can potentially gain access to the two oracle variants for  $(K_1^h, K_{1,i}^{\text{mask}})$  and  $R$ , since server authentication checks do not occur within the same session.

**Theorem 37.** *Consider the CA protocol  $\mathcal{P}$ . Then, for any valid input state  $\rho_{LSE}^{\text{in},jjj'}$ , there exists  $\rho^{\text{out}} \in \mathcal{S}'_{\text{out}}$  such that*

$$\Delta(\mathcal{P}(\rho_{LSE}^{\text{in},jjj'})_{\wedge F_S=\phi}, \rho_{\wedge F_S=\phi}^{\text{out}}) = 0.$$

*Proof.* When the adversary attacks only the client, it is in general possible for the adversary to trigger  $D_C = 1$  using a tag  $T_{SV,j}$  generated from an earlier session or select a suitable  $\alpha'_r > \alpha$ . Since the client proceeds with the protocol when  $D_C = 1$ , this would result in (1) the client leaking  $\tilde{\theta}_{\tilde{j}}$  due to the client measurement step and announcement of  $X$  values, where  $\tilde{j}$  represents the updated  $\alpha$  value, (2) the client announcing a client tag  $T_{CV}$  for which the adversary has some control of the input message, and (3) the adversary being able to influence the server validation tag  $\tilde{T}_{SV,\tilde{j}}$  generated by the client. Since  $D_C = 1$  and  $F_S \neq 1$ , the index  $\alpha^U$  is updated, i.e.  $\alpha^U = \tilde{j} + 1$ , for which the ideal state accounts for all three control/leakage available to the adversary in the form of leaked basis seed and oracle access to  $\mathcal{E}_{K_1^h K_{1,j}^{\text{mask}} \rightarrow T_{CV}}$  and  $\mathcal{E}_{RMSV \rightarrow \tilde{T}_{SV,\tilde{j}}}$ . In other words, the output state matches an ideal output state with the secrets of the form  $\rho_{SE}^{\text{in},\tilde{j},\tilde{j}+1,j'}$ .

On the other hand, if  $D_C = 0$ , none of the three events occur since the client responds with random strings. As such, the output state would match an ideal output state in  $\mathcal{S}'_{\text{out}}$ .  $\square$

### F.3.3 Man-in-the-Middle Attack

The final attack variant to consider is one where both parties are involved. We begin the analysis for a man-in-the-middle attack by replacing the decoy state parameter estimation with actual parameter checks and the authentication check with a matching check, similar to that in Appendix D.2.3. The  $\tilde{D}_{PE}$  decision modification would be the the same (note  $D_{PE}$  can have slight differences), and this would result in the same  $2\varepsilon_{\text{ds}}$  penalty. The authentication check to be replaced is the client validation step, where we replace  $D_{CV}$  with  $\tilde{D}_{CV}$ , defined as

$$\tilde{D}_{CV} = \begin{cases} 1 & \{\alpha > \alpha', M = (\tilde{X}_{P_2}, P_{2,r}, P_{1,r}, X'_{P_{1,r}}, S_r), T_{CV,\alpha'} = T_{CV,r}\} \\ & \vee \{\beta = \alpha', D_C = 1, T_{CV} = T_{CV,r}, (X'_{P_2}, P_{1,r}, P_{2,r}, X'_{P_{1,r}}, \text{syn}) = (\tilde{X}_{P_2}, P_{2,r}, P_{1,r}, X'_{P_{1,r}}, \text{syn}_r)\} \\ 0 & \text{otherwise} \end{cases}, \quad (125)$$

where  $\tilde{D}_{CV} = 1$  includes two scenarios: (1) the client validation tag with the index  $\alpha'$  comes from the client's response or (2) the client validation tag is generated from the adversary's oracle. In either case, the same condition of matching message and an untouched transmission ( $D_C = 1$  ensures a tag is generated for  $\beta = \alpha'$ ) gives  $D_{CV} = 1$ . The probability that  $D_{CV} = 1$  when  $\tilde{D}_{CV} = 0$  would be bounded by  $\varepsilon_{\text{MAC},1}$ , since a mismatched message would not allow the adversary to guess the correct tag, by the  $\varepsilon_{\text{MAC},1}$ -strong 2-universal property of the hash function. As such, the overall penalty can be summarised as

$$\Delta(\mathcal{P}(\rho_{LSE}^{\text{in},jjj'}), \rho^{\text{out},jjj'}) \leq \Delta(\mathcal{P}'(\rho_{LSE}^{\text{in},jjj'}), \rho'^{\text{out},jjj'}) + 2\varepsilon_{\text{MAC},1} + 2\varepsilon_{\text{ds}}, \quad (126)$$

and we can simplify the analysis, noting that the output state alters to  $\tilde{D}_{PE}$  and  $\tilde{D}_{CV}$  as well.

When both client and server are involved in the protocol, WLOG, the server's state generation is the first step of the protocol, since it does not take in any input from the adversary and thus can always be shifted to before the client's response. It can also be argued that the client's and server's index and secrets update would be the final steps, since they do not result in any output accessible to the adversary at the end of the session. The most general description of the protocol thus has fixed protocol steps, namely

$$\begin{aligned} \mathcal{P}' = & \mathcal{A}_{RX'P_2 \rightarrow \tilde{\alpha}\tilde{T}_{SV,\tilde{\alpha}}\tilde{\theta}_{\tilde{\alpha}}} \circ \mathcal{B}_{\alpha'\alpha_r \tilde{F}_S X \text{syn}_r R \rightarrow \tilde{\alpha}'T_{SV,\tilde{\alpha}'}\tilde{\theta}'_{\alpha'}} \circ \mathcal{C}_{\alpha'\alpha_r X X'_{P_{1,r}} P_{1,r} P_{2,r} \text{syn}_r T_{CV,r} E'' \rightarrow \tilde{D}_{PE} \tilde{F}_S} \\ & \circ \mathcal{E}_{D_C X'_{P_1} P_1 P_2 \text{syn} T_{CV} E' \rightarrow X'_{P_{1,r}} P_{1,r} P_{2,r} \text{syn}_r T_{CV,r} \alpha_r E''} \circ \mathcal{A}_{\alpha'\alpha'_r T_{SV,\alpha,r} \tilde{T}_{SV,\alpha} B \tilde{\theta}_{\beta} K_1^h K_{1,\beta}^{\text{mask}} \rightarrow D_C X' X'_{P_1} P_1 P_2 \text{syn} T_{CV}} \\ & \circ \mathcal{E}_{T_{SV,\alpha'} Q E \rightarrow \alpha'_r T_{SV,\alpha'}, BE'} \circ \mathcal{B}_{X \tilde{\theta}'_{\alpha'} \rightarrow Q}, \end{aligned} \quad (127)$$

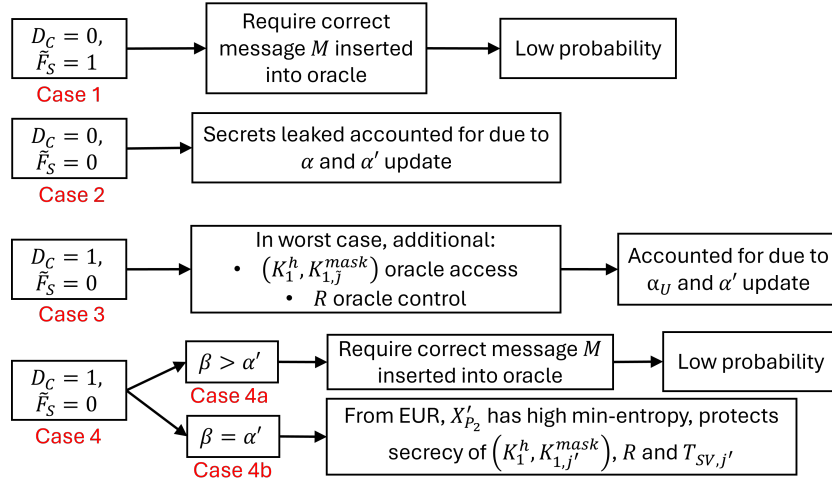


Figure 12: Schematic of proofs of Thm. 38 (case 1 and 2), Thm. 39 (case 3) and Thm. 40 (case 4).

where  $\mathcal{A}$  and  $\mathcal{B}$  refer to quantum channels performed at the server and client respectively and  $\mathcal{E}$  are quantum channels associated with adversary strategy. Note that we collate all decision for  $\tilde{F}_S$  and  $\tilde{D}_{PE}$  into a single channel  $\mathcal{C}$  separate from the rest of the steps and information for  $\tilde{D}_{PE}$  and  $\tilde{F}_S$  (same as  $F_S$  except that checks  $\tilde{D}_{PE}$  and  $\tilde{D}_{CV}$  are “ideal”) checks are captured within  $E''$ , such as the original values of the message sent by the client or the message utilised in the oracles.

The security analysis for man-in-the-middle attack can then be split into multiple cases. Fig. 12 provides a summary of the arguments of the various cases. The first case we consider for the analysis is the  $D_C = 0$  case.

**Theorem 38.** Consider the CA protocol  $\mathcal{P}$ , then there exists  $\sigma_{LSE}^{00,j+1,j+1,\tilde{j}'} \in \mathcal{S}_{in}$  such that

$$\Delta \left( \mathcal{P}'(\rho_{LSE}^{in,j,j,j'}) \wedge_{D_C=0}, \sum_{\tilde{j}' \geq j'+1} p_{00,\tilde{j}'} \sigma_{LSE}^{00,j+1,j+1,\tilde{j}'} \right) \leq \varepsilon_{\text{match}}.$$

*Proof.* The trace distance can be split into two components based on the  $\tilde{F}_S$  value by triangle inequality, where the  $\tilde{F}_S = 1$  case (case 1) can be further upper bounded by  $\Pr[\tilde{F}_S = 1, D_C = 0]$ .

By definition of  $\tilde{F}_S$ , we can further upper bound the probability by  $\Pr[\tilde{D}_{CV} = 1, \tilde{D}_{PE} = 1, D_C = 0]$ . With these conditions, the only case where it can occur is when  $\alpha > \alpha'$ , and the adversary correctly matches the messages. Following the proof of Thm. 34, since  $X$  is uncorrelated to the value  $\tilde{X}_{\tilde{P}_1}$  committed during the oracle call, the probability that the two values matched would be bounded by  $\varepsilon_{\text{match}}$ .

For the case of  $\tilde{F}_S = 1$  (case 2), the definition of  $\tilde{D}_{CV}$  necessarily requires  $\alpha'_r \leq j$ , leading the index update to be  $\tilde{\alpha} = j + 1$ . The server on the other hand updates based on  $\alpha_r = \tilde{j}' > j'$  announced to it, otherwise, it updates to  $j' + 1$ . As such, in general, the output indices are a mixture of  $(j + 1, j + 1, \tilde{j}')$  where  $\tilde{j}' \geq j' + 1$ , matching the index of the  $\sigma_{LSE}^{j+1,j+1,\tilde{j}'}$  as required. Furthermore, since  $D_C = 0$  implies the client responds with random strings, the only value that are leaked are  $T_{SV,j'}$  and  $\tilde{\theta}_{j'}$ . The updating of the indices to  $\alpha = j + 1$  and  $\alpha' > j'$  means that these values are no longer utilised (i.e. these leaks are already accounted for). Note that any oracle access to  $(K_1^h, K_{1,i}^{mask})$  for indices  $i < \tilde{j}'$  can be discarded according to Thm. 4 since the corresponding masking key are no longer utilised, and the basis seeds for the same indices are traced out. As such, the output state for the secret matches the ideal states  $\sigma_{SE}^{j+1,j+1,\tilde{j}'}$ , resulting in 0 trace distance.

Combining both cases 1 and 2, the resulting trace distance is bounded by  $\varepsilon_{\text{match}}$ .  $\square$

The next case to consider is  $D_C = 1, \tilde{F}_S = 0$  (case 3), which can occur without requiring complex attacks from the adversary since the client does not perform an authentication check of the server within the same session. It would, however, trigger an update of  $\alpha^U$ , indicating that server authentication check would fail in the next session involving a client.

**Theorem 39.** Consider the CA protocol  $\mathcal{P}$ . Then, there exists  $\sigma_{LSE}^{10, \tilde{j}, \tilde{j}+1, \tilde{j}' \in \mathcal{S}_{in}}$  such that

$$\Delta \left( \mathcal{P}'(\rho_{LSE}^{\text{in}, jjj'})_{\wedge D_C=1, \tilde{F}_S=0}, \sum_{\tilde{j} \geq j, \tilde{j}' \geq j'+1} p_{10, \tilde{j}, \tilde{j}'} \sigma_{LSE}^{10, \tilde{j}, \tilde{j}+1, \tilde{j}'} \right) = 0.$$

*Proof.* To achieve  $D_C = 1$ , the adversary is free to select  $\alpha'_r = \tilde{j} \geq j$  and since  $\tilde{F}_S = 0$ , the adversary is also free to select  $\alpha_r = \tilde{j}' - 1 \geq j'$ . As such, the updated indices would be  $\alpha = \tilde{j}$ ,  $\alpha' = \tilde{j}'$  with  $\alpha^U = \tilde{j} + 1$  due to the condition  $D_C = 1$  and  $\tilde{F}_S \neq 1$ . This matches with the indices of the ideal state as required.

What remains is to prove that the output state matches the ideal state in subsystems  $SE$  as well. For any combination of  $j$  and  $j'$ , we can always consider a more powerful adversary that has access to the client's basis seed  $\tilde{\theta}_{\tilde{j}}$ , which allows the adversary to prepare quantum states that results in a chosen  $X'$  to be received by the client. This has two results: (1) the adversary is able to partially select the message used to generate  $T_{CV}$  from authentication masking key  $K_{1, \tilde{j}}^{\text{mask}}$  and (2) the adversary is able to partially select the message used by the client to generate  $\tilde{T}_{SV, \tilde{j}}$  (and updated  $\tilde{\theta}_{\tilde{j}}$ ). We can proceed with providing the adversary more power – to be able to fully select the messages for both (1) and (2), without requiring that the messages be correlated. This corresponds with the adversary being provided with an oracle access to  $\mathcal{E}_{K_1^h K_{1, \tilde{j}}^{\text{mask}} \rightarrow T_{CV}}$  and one access to  $\mathcal{E}_{RM_{SV} \rightarrow \tilde{T}_{SV, \tilde{j}}}$ , and where  $\tilde{\theta}_{\tilde{j}}$  can be correlated to the adversary (but for which the adversary has no direct access to). The additional access to these two oracles and correlation of  $\tilde{\theta}_{\tilde{j}}$  (part of  $E$ ) are accounted for in the states  $\sigma_{LSE}^{\tilde{j}, \tilde{j}+1, \tilde{j}'}$  when  $\alpha^U = \alpha + 1$ . Therefore, the output state (in the worst case) corresponds to a state in  $\mathcal{S}_{in}$  and thus the trace distance is 0.  $\square$

The final case to consider is the case when  $D_C = \tilde{F}_S = 1$  (case 4). A critical component of security is provided by  $\tilde{D}_{CV}$ , where the requirement for the message selection limits the success to the case of  $\beta = \alpha'$ , along with an unmodified message. This allows us to reduce the analysis to a protocol that is similar to that of Thm. 32, where the entropic uncertainty relation is applied.

**Theorem 40.** Consider the CA protocol  $\mathcal{P}$ . Then, there exists  $\sigma_{LSE}^{j'j'j'} \in \mathcal{S}_{in}$  such that

$$\Delta(\mathcal{P}'(\rho_{LSE}^{\text{in}, jjj'})_{\wedge D_C=\tilde{F}_S=1}, p_{11} \sigma_{LSE}^{j'j'j'}) \leq 4\sqrt{2\varepsilon_{\text{ph}}} + 2\varepsilon_2 + \frac{1}{2} \times 2^{-\frac{1}{2}[N_{P_2,1}^{\text{tol}}[1-h_{\text{bin}}(e'_{\text{ph}, \text{tol}})]-l_{\tilde{\theta}}-\log_2 |\mathcal{T}_{SV}| |\mathcal{T}_{CV}| - \text{leak}_{\text{EC}}]} + \sqrt{|\mathcal{T}_{CV}| \varepsilon_{\text{MAC}, 1} - 1 + 2^{\log_2 |\mathcal{T}_{CV}| + \log_2 \left(\frac{2}{\varepsilon_2} + 1\right) - N_{P_2,1}^{\text{tol}}[1-h_{\text{bin}}(e'_{\text{ph}, \text{tol}})] + \text{leak}_{\text{EC}}}} + \varepsilon_{\text{match}},$$

where  $\varepsilon_2 > 0$  is a parameter to be optimised.

*Proof.* By definition, when  $\tilde{F}_S = 1$ , the announced index value  $\alpha_r \leq \alpha'$ , which leaves  $\alpha'$  unchanged throughout the protocol. The definition of  $\tilde{D}_{CV} = 1$  requires additionally that the client's updated index be  $\beta \geq \alpha'$ . Let us consider the case of  $\beta > \alpha'$  (case 4a), which necessarily requires  $\alpha > \alpha'$  for  $\tilde{D}_{CV} = 1$ . In this case, the adversary has oracle access to  $(K_1^h, K_{1, \alpha'}^{\text{mask}})$ , where the message inserted to the oracle has to match the server's received message. We can thus follow the proof of Thm. 34 to show that the probability of the message matching and thus this event occurring ( $\tilde{F}_S = 1$ ) is upper bounded by  $\varepsilon_{\text{match}}$ . Therefore, we can split off case 4a of  $\beta \geq \alpha > \alpha'$ , where the trace distance between the output state and ideal output would be bounded by  $\varepsilon_{\text{match}}$ .

What remains is the case where  $\beta = \alpha'$  (case 4b), which has  $\alpha \leq \alpha'$ , where  $\tilde{D}_{CV} = 1$  ensures that the messages from the client are not tampered with. Since  $\tilde{F}_S = D_C = 1$ , the final indices are  $\alpha = \alpha^U = \alpha' = j'$ , which corresponds to the index of the ideal state  $\sigma_{LSE}^{j'j'j'}$ . Let us consider one such state  $\sigma_{LSE}^{j'j'j'} \in \mathcal{S}_{in}$ , defined by

$$\sigma_{LSE}^{j'j'j'} = \tilde{\Pi}_{\alpha \alpha^U \alpha'}^{j'j'j'} \otimes \tau_{RK_{1, [j', m]}^{\text{mask}}} \otimes \tilde{\tau}_{\tilde{\theta}_{[j', m]} \tilde{\theta}'_{[j', m]}} \otimes \rho_{E \wedge D_C=\tilde{F}_S=1 \wedge \beta=j'} \quad (128)$$

The output state can be written as

$$\mathcal{P}'(\rho_{LSE}^{\text{in}, jjj'})_{\wedge D_C=\tilde{F}_S=1 \wedge \beta=j'} = \tilde{\Pi}_{\alpha \alpha^U \alpha'}^{j'j'j'} \otimes \tau_{K_{1, [j'+1, m]}^{\text{mask}}} \otimes \tilde{\tau}_{\tilde{\theta}_{[j'+1, m]} \tilde{\theta}'_{[j'+1, m]}} \otimes \rho_{RK_1^h K_{1, j'}^{\text{mask}} \tilde{\theta}_{j'} \tilde{\theta}'_{j'} T_{SV, j'} \tilde{T}_{SV, j'} E'' \wedge \Omega}, \quad (129)$$

where  $\Omega := \{\alpha_r \leq j', \alpha'_r = j', \tilde{D}_{PE} = \tilde{D}_{CV} = D_C = 1\}$  (which matches  $\{D_C = \tilde{F}_S = 1, \beta = j'\}$ ) and the  $\tilde{D}_S$  and  $D_C$  values has been absorbed into  $E''$ . We can simplify the trace distance as

$$\begin{aligned}
& \Delta(\mathcal{P}'(\rho_{LSE|j \leq j'}^{\text{in}, jjj'} \wedge \Omega, \rho_{\wedge \Omega}^{\text{out}, jjj'})) \\
& \leq \Delta(\rho_{RK_1^h K_{1,j'}^{\text{mask}} \tilde{\theta}_{j'} \tilde{\theta}'_{j'} T_{SV,j'} \tilde{T}_{SV,j'} E'' \wedge \Omega, \tau_R \otimes \tilde{\tau}_{\tilde{\theta}_{j'} \tilde{\theta}'_{j'}} \otimes \tilde{\tau}_{T_{SV,j'} \tilde{T}_{SV,j'}} \otimes \rho_{E'' \wedge \Omega}) \\
& \leq \Delta(\rho_{RK_1^h K_{1,j'}^{\text{mask}} \tilde{\theta}_{j'} \tilde{\theta}'_{j'} T_{SV,j'} \tilde{T}_{SV,j'} E'' \wedge \Omega, \tau_R \otimes \tilde{\tau}_{\tilde{\theta}_{j'} \tilde{\theta}'_{j'}} \otimes \tilde{\tau}_{T_{SV,j'} \tilde{T}_{SV,j'}} \otimes \rho_{K_1^h K_{1,j'}^{\text{mask}} E'' \wedge \Omega}) \\
& \quad + \Delta(\rho_{K_1^h K_{1,j'}^{\text{mask}} E'' \wedge \Omega, \tau_{K_1^h K_{1,j'}^{\text{mask}}} \otimes \rho_{E'' \wedge \Omega}) \\
& \leq \Delta(\rho_{RK_1^h K_{1,j'}^{\text{mask}} \tilde{\theta}_{j'} T_{SV,j'} E'' \wedge \Omega, \tau_{R \tilde{\theta}'_{j'} T_{SV,j'}} \otimes \rho_{K_1^h K_{1,j'}^{\text{mask}} E \wedge \Omega}) + \Delta(\rho_{K_1^h K_{1,j'}^{\text{mask}} E'' \wedge \Omega, \tau_{K_1^h K_{1,j'}^{\text{mask}}} \otimes \rho_{E \wedge \Omega}) \\
& \leq p_{\tilde{\Omega}_{PE}} \{2\varepsilon_{sm,1} + \frac{1}{2} \times 2^{-\frac{1}{2}[H_{\min}^{\varepsilon_{sm},1}(\hat{X}'_{P_2} | K_1^h K_{1,j'}^{\text{mask}} E'')_{\rho_{\wedge \Omega'} | \tilde{\Omega}_{PE}} - l_{\tilde{\theta}} - \log_2 |\mathcal{T}_{SV}|]} \\
& \quad + 2(\varepsilon_{sm,2} + \varepsilon_2) + \sqrt{|\mathcal{T}_{CV}| \varepsilon_{MAC,1} - 1 + 2^{\log_2 |\mathcal{T}_{CV}| + \log_2 (\frac{2}{\varepsilon_2} + 1) - H_{\min}^{\varepsilon_{sm},2}(\hat{X}'_{P_2} | E'')_{\rho_{\wedge \Omega'} | \tilde{\Omega}_{PE}}}} \},
\end{aligned} \tag{130}$$

where the first inequality considers a specific state in the class of ideal output states where  $T_{SV,j}$  and  $\tilde{T}_{SV,j}$  are equal and independent from the adversary. The second inequality applies the triangle inequality, while the third inequality invokes  $\tilde{D}_{CV} = 1$ , which indicates that the variables  $\hat{X}'_{P_2} = X'_{P_2}$  and thus the hashed outcomes  $(\tilde{\theta}_{j'}, \tilde{T}_{SV,j'}) = (\tilde{\theta}'_{j'}, T_{SV,j'})$ , allowing the trace distance to reduce to one set of variables (more formally, this is simulated by introducing a “copy” channel from one set to another and removing the CPTP “copy” channel). The fourth inequality applies the quantum leftover hash lemma (Thm. 5), noting again that  $\Omega$  implies  $\hat{X}'_{P_2} = X'_{P_2}$ , and that  $\Omega = \Omega' \wedge \tilde{\Omega}_{PE}$ , which is defined later.

Here, we analyse the first min-entropy term, which would also acts as a lower bound the second term. Let us list explicitly the conditions of  $\Omega$ ,

1.  $\alpha_r \leq j', \alpha'_r = j', D_C = 1$ : Conditions associated with index selection, and passing the initial client check.
2.  $(P_{2,r}, P_{1,r}, X'_{P_{1,r}}, \text{syn}_r) = (P_1, P_2, X'_{P_1}, \text{syn})$ : Message sent from client to server is unchanged.
3.  $T_{CV} = T_{CV,r}$ : The tag sent from the client to server is unchanged.
4.  $X'_{P_2} = \hat{X}_{P_2}$ : The server’s corrected bitstring matches with the client’s bitstring.
5.  $\frac{wt(X_{P_{1,r}} \oplus X'_{P_{1,r}}[\{P_{1,r}\}])}{N_{P_{1,r}}} \leq e_{b,tol}, |P_{1,r}| \geq P_{1,tol}$ : Remaining parameter estimation checks.
6.  $\tilde{\Omega}_{PE}$ : Standard parameter estimation checks.

where we list the events for the first five events from  $\Omega_1$  to  $\Omega_5$  as being part of  $\Omega'$ . We note here that  $\tilde{\Omega}_{PE}$  estimates directly on the  $(P_1, P_2, X'_{P_1})$  values instead of the received values, since  $\Omega_{PE} \wedge \Omega_2 = \tilde{\Omega}_{PE} \wedge \Omega_2$ . We first simplify by noting that  $\hat{X}'_{P_2}$  is computed from  $X_{P_{2,r}}$  and the syndrome  $\text{syn}_r$  received. Therefore, by data processing inequality[37], we have that

$$H_{\min}^{\varepsilon_{sm}}(\hat{X}'_{P_2} | K_1^h K_{1,j'}^{\text{mask}} E'')_{\rho_{\wedge \Omega'} | \tilde{\Omega}_{PE}}} \geq H_{\min}^{\varepsilon_{sm}}(X_{P_{2,r}} | K_1^h K_{1,j'}^{\text{mask}} \text{syn}_r E'')_{\rho_{\wedge \Omega'} | \tilde{\Omega}_{PE}}}, \tag{131}$$

noting that  $\text{syn}_r$  is in general able to be determined from  $E''$  (adversary stores a copy of the  $\text{syn}_r$  it sends to the server). Further imposing that  $P_{2,r} = P_2$  from the  $\Omega_2$  condition, we can simplify the min-entropy before removing the conditions of  $\Omega_2$  to  $\Omega_5$  [38], i.e.

$$H_{\min}^{\varepsilon_{sm}}(X_{P_{2,r}} | K_1^h K_{1,j'}^{\text{mask}} \text{syn}_r E'')_{\rho_{\wedge \Omega'} | \tilde{\Omega}_{PE}}} \geq H_{\min}^{\varepsilon_{sm}}(X_{P_2} | K_1^h K_{1,j'}^{\text{mask}} \text{syn}_r E'')_{\rho_{\wedge \Omega_1} | \tilde{\Omega}_{PE}}}. \tag{132}$$

Here, we can reverse the CPTP map used to generate  $\text{syn}_r E''$ , leaving us with

$$H_{\min}^{\varepsilon_{sm}}(X_{P_2} | K_1^h K_{1,j'}^{\text{mask}} \text{syn}_r E'')_{\rho_{\wedge \Omega_1} | \tilde{\Omega}_{PE}}} \geq H_{\min}^{\varepsilon_{sm}}(X_{P_2} | K_1^h K_{1,j'}^{\text{mask}} X'_{P_1} P_1 P_2 \text{syn} T_{CV} E')_{\rho_{\wedge \Omega_1} | \tilde{\Omega}_{PE}}}. \tag{133}$$

We can remove the syndrome  $\text{syn}$  and the tag  $T_{CV}$  utilising the min-entropy chain rule [37]. Furthermore, with the removal of  $T_{CV}$ ,  $K_1^h$  and  $K_{1,j'}^{\text{mask}}$  is uncorrelated with any other variables in the state and can be removed, leaving us with

$$H_{\min}^{\varepsilon_{sm}}(X_{P_2} | K_1^h K_{1,j'}^{\text{mask}} X'_{P_1} P_1 P_2 \text{syn} T_{CV} E')_{\rho_{\wedge \Omega_1} | \tilde{\Omega}_{PE}}} \geq H_{\min}^{\varepsilon_{sm}}(X_{P_2} | \tilde{\theta} X'_{P_1} P_1 P_2 E')_{\rho_{|\tilde{\Omega}_{PE}}}} - \text{leak}_{EC} - \log_2 |\mathcal{T}_{CV}|, \tag{134}$$

where we also remove the  $\Omega_1$  condition, and included additional  $\tilde{\theta}$  conditioning. Here, the protocol steps are simply:

1. The server prepares decoy state BB84, using the basis generated from  $\tilde{\theta}$  and bit value  $X$ .
2. The adversary performs its attack on the state, mapping  $QE$  to  $PBE'$ .
3. The client randomly select  $P_1$  rounds and measure them in the basis generated from  $\tilde{\theta}$  and outputs  $X'_{P_1}$ .
4. Based on  $X$ ,  $P_1$ ,  $P_2$  and  $X'_{P_1}$ , the parameter estimation decision is made (event  $\tilde{\Omega}_{PE}$ ),

This is exactly the same protocol steps as that in Thm. 32, and we can utilise the same analysis to demonstrate that

$$H_{\min}^{\varepsilon_{\text{sm}}}(\hat{X}'_{P_2} | K_1^h K_{1,j'}^{\text{mask}} E'')_{\rho_{\wedge \Omega' | \tilde{\Omega}_{PE}}} \geq N_{P_2,1}^{\text{tol}} [1 - h_{\text{bin}}(e'_{\text{ph,tol}})] - \text{leak}_{\text{EC}} - \log_2 |\mathcal{T}_{\text{CV}}|, \quad (135)$$

with  $\varepsilon_{\text{sm}} = \sqrt{2\varepsilon_{\text{ph}}}$ . The second min-entropy term can follow a similar analysis, but since  $K_1^h$  and  $K_{1,j'}^{\text{mask}}$  is traced out,  $T_{\text{CV}}$  would be a random string, and can be simply removed without incurring the  $\log_2 |\mathcal{T}_{\text{CV}}|$  penalty. As such, the overall trace distance is

$$\begin{aligned} \Delta(\Pi_{D_C \tilde{F}_S}^{11} \mathcal{P}'(\rho_{LSE}^{\text{in}, jjj'}) \Pi_{D_C \tilde{F}_S}^{11} \rho_{\wedge \Omega}^{\text{out}, jjj'}) &\leq 4\sqrt{2\varepsilon_{\text{ph}}} + 2\varepsilon_2 + \frac{1}{2} \times 2^{-\frac{1}{2}[N_{P_2,1}^{\text{tol}}[1 - h_{\text{bin}}(e'_{\text{ph,tol}})] - l_{\tilde{\theta}} - \log_2 |\mathcal{T}_{\text{SV}}| |\mathcal{T}_{\text{CV}}| - \text{leak}_{\text{EC}}]} \\ &\quad + \sqrt{|\mathcal{T}_{\text{CV}}| \varepsilon_{\text{MAC},1} - 1 + 2^{\log_2 |\mathcal{T}_{\text{CV}}| + \log_2 \left(\frac{2}{\varepsilon_2} + 1\right) - N_{P_2,1}^{\text{tol}}[1 - h_{\text{bin}}(e'_{\text{ph,tol}})] + \text{leak}_{\text{EC}}}}. \end{aligned} \quad (136)$$

□