A consolidated and accessible security proof for finite-size decoy-state quantum key distribution

Jerome Wiesemann [1], Jan Krause [1], Devashish Tupkary [2], Norbert Lütkenhaus [2], Davide Rusca [3,4,5], and Nino Walenta [1]

[1]Fraunhofer Institute for Telecommunications, Heinrich-Hertz-Institut, HHI, 10587 Berlin, Germany

[2]Institute for Quantum Computing and Department of Physics and Astronomy, University of Waterloo, N2L 3G1, Canada

[3]Vigo Quantum Communication Center, University of Vigo, Vigo E-36310, Spain

[4]Escuela de Ingeniería de Telecomunicación, Department of Signal Theory and Communications, University of Vigo, Vigo E-36310, Spain

[5]AtlanTTic Research Center, University of Vigo, Vigo E-36310, Spain

arXiv:2405.16578v3 [quant-ph] 16 Mar 2026

In recent years, quantum key distribution (QKD) has evolved from a scientific research field to a commercially available security solution, supported by mathematically formulated security proofs. However, since the knowledge required for a full understanding of a security proof is scattered across numerous publications, it has proven difficult to gain a comprehensive understanding of all steps involved in the process and their limitations without considerable effort and attention to detail. Our paper aims to address this issue by providing a rigorous and comprehensive security proof for the finite-size 1-decoy and 2-decoy BB84 protocols against coherent attacks within Renner's entropic uncertainty relation framework. We resolve important technical flaws found in previous works regarding the fixed-length treatment of protocols and the careful handling of acceptance testing. To this end, we provide various technical arguments, including an analysis accounting for the important distinction of the 1-decoy protocol where statistics are computed after error correction, along with a slight improvement of the secure-key length. We also explicitly clarify the aspect of conditioning on events, addressing a technical detail often overlooked and essential for rigorous proofs. We extensively consolidate and unify concepts from many works, thoroughly discussing the underlying assumptions and resolving technical inconsistencies. Therefore, our contribution represents a significant advancement towards a broader and deeper understanding of QKD security proofs.

Contents

1 Introduction **3**

2 Preliminaries **6**

2.1 The 1-decoy state BB84 protocol 6

2.1.1 Fixed-length protocols 6

2.1.2 Protocol description 7

2.2 Theoretical background 11

2.2.1 Representing quantum systems 12

2.2.2 Distance between quantum states 12

2.2.3 Bipartite quantum systems 13

2.3 Definition of security 14

Jerome Wiesemann: jwiesemann@uwaterloo.ca

2.3.1 Information-theoretic security . . . 14
2.3.2 Assumptions of quantum key distribution . . . 15
2.3.3 Security parameters . . . 15
2.3.4 Conditional bounds expansion . . . 20
2.3.5 Composable security . . . 20
2.3.6 The one-time pad . . . 20

3 Universal$_2$ hashing **21**
3.1 Error correction and verification . . . 21
3.2 Privacy amplification . . . 23

4 The quantum leftover hash lemma **23**
4.1 Eve's guessing probability and the min-entropy . . . 24
4.2 The smooth min-entropy . . . 26
4.3 The quantum leftover hash lemma . . . 27
4.4 Expanding the smooth min-entropy . . . 29
4.4.1 Chain rule for smooth min-entropies . . . 29
4.4.2 Source-replacement scheme . . . 31
4.4.3 Entropic uncertainty relation . . . 31

5 Decoy bounds **35**
5.1 Finite-size photon event statistics . . . 35
5.1.1 Lower bound on the number of vacuum events . . . 37
5.1.2 Upper bound on the number of vacuum events . . . 38
5.1.3 Lower bound on the number of single-photon events . . . 39
5.1.4 Upper bound on the number of single-photon errors . . . 39
5.2 Upper bound on the phase error rate . . . 40

6 Extractable secure-key length **40**
6.1 Operational expression for the secure-key length . . . 40
6.2 Simplified expression for the secure-key length . . . 42

7 Discussion **43**

8 Conclusion **45**

List of symbols **46**

A Appendix **46**
A.1 Model assumptions . . . 46
A.2 Bounds for the 2-decoy state protocol . . . 47
A.2.1 Lower bound for the vacuum events . . . 47
A.2.2 Lower bound for the vacuum events . . . 47
A.2.3 Upper bound on the number of single-photon events . . . 48
A.2.4 Security analysis . . . 48
A.3 Intuition on the trace distance . . . 48
A.4 Comparison between the von Neumann entropy and min-entropy . . . 49
A.5 Derivation of the expression for the Hoeffding-delta . . . 49
A.6 Scenario where Alice chooses the intensity after detection . . . 50
A.7 Asymptotic secure-key rate . . . 51

1 Introduction

Quantum key distribution (QKD) is a method for remotely establishing a secure key between two parties. While classical cryptographic methods rely on unproven computational hardness assumptions of certain mathematical problems [1–4], the protocol security of QKD is based on the laws of quantum mechanics and does not make any assumptions about the computational power of a potential eavesdropper. In fact, no proven secure method currently exists for remotely establishing a secure key by means of classical communication alone [5]. At its core, QKD relies on carriers of quantum information [6], which cannot be eavesdropped without causing noticeable disturbances. With its security proofs formulated in the universal composability framework, QKD can be combined with other composable cryptographic primitives, such as encryption algorithms, to yield *information-theoretically secure* protocols [7–12]. Nevertheless, it is important to distinguish between *protocol security* and *implementation security*. The former refers to the theoretical security guarantees of the QKD protocol, whereas the latter deals with security implications of the physical implementations, including device imperfections and the resulting side-channels. In this work, we aim to present a baseline security proof and thus focus on protocol security.

The concept of QKD was proposed in 1984 by Bennett and Brassard, inspired by earlier works from Wiesner [13], leading to the formulation of what is today recognized as the *BB84 protocol* [14]. While the protocol itself remains largely unchanged to this day, its security analysis has undergone significant improvements and refinements. The original protocol assumed single photons as information carriers. Today, however, owing to their greater practicality, weak coherent states, for example generated by lasers in gain-switched operation, are used in practical implementations [15]. Due to the intrinsic non-zero probability for multi-photon emissions by coherent sources, the protocol was adjusted to mitigate so-called photon-number splitting attacks [16–18]. This was achieved by the *decoy-state method*, first introduced in 2003 [19–21]. Its core idea involves monitoring the photon-number-dependent channel transmission by preparing the weak coherent states with randomly chosen intensities unknown to an adversary. A rigorous security proof was in turn presented in 2005 by Lo et al. [21] for asymptotic key rates and by Wang for a finite amount of decoy states [20]. While the security of QKD with coherent sources can also be maintained by other means [22, 23], the decoy-state method remains the only one with a linear relation between the channel transmission and secure-key rate. In 2005, security proofs were reformulated within the universal composability framework [8] by Renner [24], taking into account the effects caused by finite post-processing block sizes, thereby laying the foundation for the formulation of modern QKD security proofs.

There have been a variety of papers on a finite-size security proof for decoy-state BB84 against coherent attacks [25–27]. In 2014, a notable advancement towards practical applications was made by Lim et al. [26], who presented a proof using entropic uncertainty relations [28], requiring just two additional decoy-state intensities, also called the *2-decoy state BB84 protocol* [29]. This approach was applied to the *1-decoy state BB84 protocol* by Rusca et al. [27] in 2018 (see also Ref. [30]). Even though many other protocols have been proposed [23,31–34], the family of decoy-state BB84 protocols remains the most widespread protocol family, both in academia and industry, and will thus be the focus of this work. In particular, we will focus on Refs. [26, 27].

The knowledge necessary for a complete understanding of modern QKD security proofs is scattered across numerous publications, often exhibiting technical inconsistencies. Therefore, it has proven difficult to gain a comprehensive understanding of each step involved in the security proof process and their limitations without considerable effort and attention to detail. This problem has been addressed in 2017 by Tomamichel and Leverrier, who presented a self-contained security proof for entanglement-based and prepare-and-measure protocols [35]. However, they explicitly do not cover the case of signals generated by weak coherent pulses and therefore exclude the treatment of decoy states. Furthermore, their work requires a solid understanding of the mathematical foundations of quantum information theory, which restricts its accessibility.

Contributions. We aim to present a rigorous security proof for the 1-decoy and 2-decoy BB84 protocols, resolving various technical flaws found in previous works. We provide a rigorous treatment for fixed-length protocols with acceptance testing, focusing on the subtle but important fact that, following the fixed-length definition of security, the length of the secure-key must be fixed prior to running the protocol. We also account for the distinction in the 1-decoy approach where acceptance testing occurs after error correction, rather than based on public announcements directly after sifting, as is common in traditional protocols. These arguments, overlooked in earlier analyses, are explicitly addressed in this work. To this end, we make it a point to explicitly clarify the aspect of conditioning on states throughout the analysis. Security proofs for variable-length protocols require additional arguments and do not trivially follow from fixed-length statements. This issue extends to works such as Refs. [26, 27] which do not rigorously handle fixed-length protocols (via acceptance testing) or variable-length protocols. In this work, we aim to address the issues stated above and present a rigorous fixed-length security proof in the entropic uncertainty relation framework using smooth min-entropies. Moreover, we slightly improve the secure-key length by using a suitable combination of min-entropy chain rules and update the protocol description to address the issue of iterative sifting observed in earlier works [26, 36]. We also address several technical gaps pointed out in Ref. [37].

We also aim at largely increasing the accessibility of the security proof by employing a constructive approach: starting from the general definition of security, we systematically expand and bound each term, providing a clear, step-by-step framework for the proof. We discuss underlying concepts in detail, providing a proof outlined in a coherent manner. Underlying and often hidden assumptions are named and listed, cf. App. A.1. These assumptions should be kept in mind when designing practical QKD systems as the discrepancies between the security proof and the practical implementation can lead to side-channel attacks compromising the security of QKD systems [38–41]. With the inclusion of decoy states, we derive equations expressed in terms of experimentally accessible parameters, thus allowing for direct applications in practical systems. The proof builds upon the works by Rusca et al. [27] and Lim et al. [26], focusing on the derivation of an expression for the secure-key length in the 1-decoy protocol, but also deriving the necessary bounds for the 2-decoy variant. We take finite-size effects into account and prove security against coherent attacks, the most general form of attacks.

The proof is performed in Renner's framework, i.e. by applying the quantum leftover hash lemma and bounding the relevant entropies using the entropic uncertainty relation (EUR) [42]. We note that other approaches to security proofs exist, such as using the post-selection technique reduction [43, 44] to IID attacks followed by an IID security proof, the generalized entropy accumulation theorem [45], and the phase error correction framework [46], each with their advantages and drawbacks. With numerous examples and remarks, we hope to largely improve the comprehensibility of the security proof. While assuming general knowledge of QKD and quantum mechanics, no prior exposure to security proofs is required. For an overview of quantum key distribution, we refer to the extensive reviews [10, 11, 47] and recent theoretical books [48, 49], and for an introduction to quantum mechanics and quantum information theory, we refer to the standard textbooks [50, 51]. We strive to present a rigorous yet accessible security proof for the 1-decoy and 2-decoy state BB84 protocols that can serve as a foundation for the discussion of their security and for the identification of potential vulnerabilities. Additionally, this work aims at providing a robust reference for practical implementations of the protocol.

Outline. The structure of the security proof is illustrated in Fig. 1. Section 2 first discusses fixed-length protocols and formally describes the 1-decoy state protocol, which we slightly adjust to rigorously treat acceptance testing. Then, the theoretical background is laid out and core concepts such as density operators, the trace distance and bipartite quantum systems are introduced. Information theoretic security is then defined and the security parameters are constructively introduced as a metric to evaluate the distance to a perfectly secure system. The assumptions of quantum key distribution and its composition with other cryptographic primitives such as the one-time pad are also described.

The terms appearing in the definition of security are then separately addressed to prove protocol security. We first bound the correctness parameter in Sec. 3 using universal$_2$ hashing, which is introduced

as part of the error verification and privacy amplification steps of the post-processing. The quantum leftover hash lemma, first introduced by Renner in Ref. [24], is then presented in Sec. 4. It provides a bound on the secrecy parameter and is expanded in terms of the number of photon events and errors using the entropic uncertainty relation by bounding the relevant entropies. For this, the min-entropy as well as its smoothed version are introduced. The result of this section is an expression linking the secure-key length to the min-entropy, which represents the information a potential eavesdropper could have gathered about the key.

Since the number of m-photon events and errors is not directly accessible, the aim of Sec. 5 is to estimate and bound these quantities in terms of experimentally accessible parameters using the Poissonian statistics of weak coherent sources. Putting everything together, an operational expression for the secure-key length is derived in Sec. 6. This expression solely depends on experimental parameters (the acceptance bounds on the number of photon events and errors), the predefined security parameters, and the information leaked during error correction and verification.

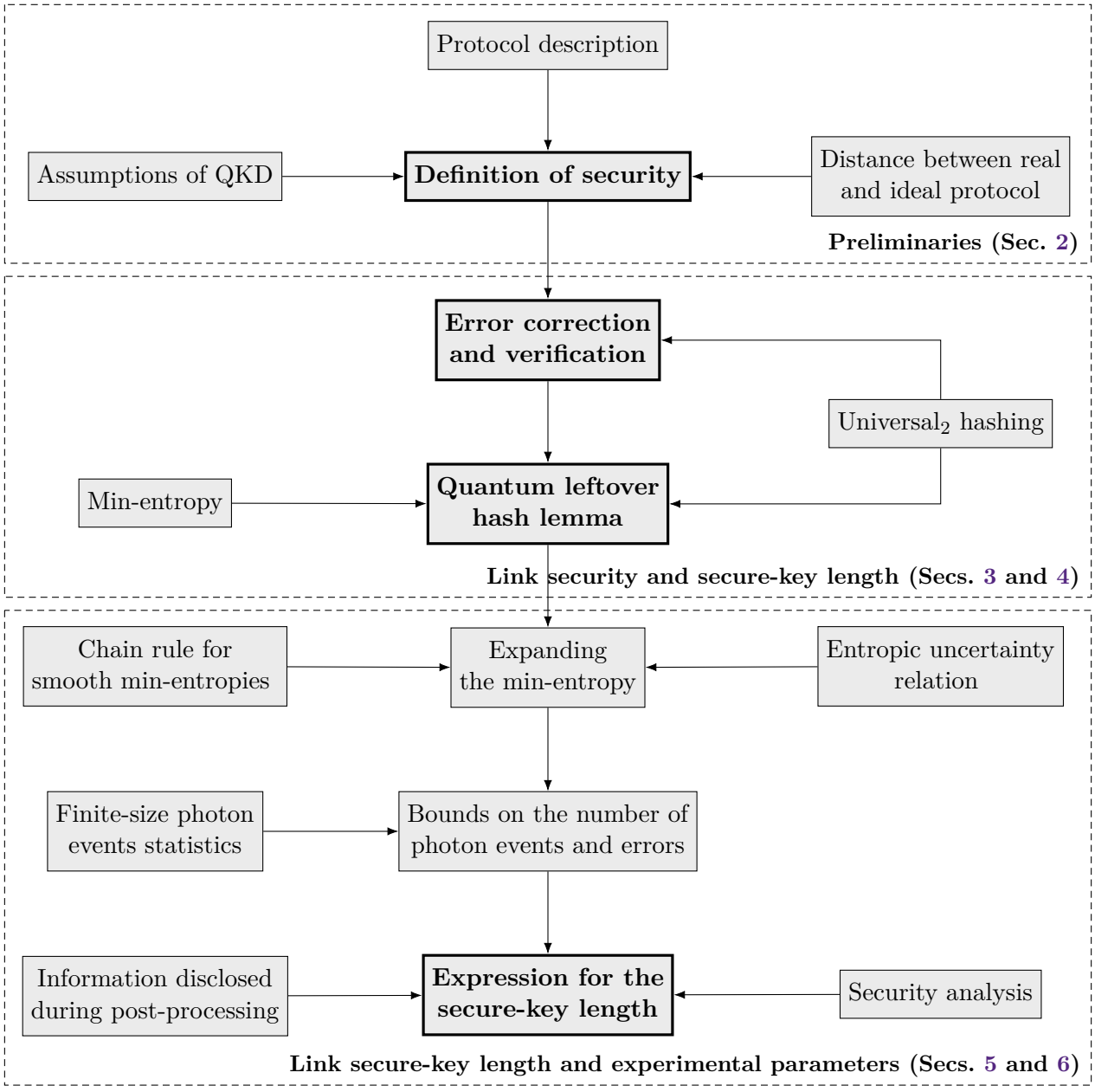


Figure 1: Structure of the 1-decoy and 2-decoy state security proofs.

2 Preliminaries

The aim of this section is twofold. First, the 1-decoy state BB84 protocol is formally described in Sec. 2.1. Then, mathematical concepts and the notation used throughout this work are introduced in Secs. 2.2 and 2.3.

2.1 The 1-decoy state BB84 protocol

The *1-decoy state protocol* [27] described in Fig. 2 is based on the original *BB84 protocol* proposed by Bennett and Brassard [14] and constitutes a slight variation of the *2-decoy state protocol* [26] in the sense that it only requires two intensity[1] levels μ_1, μ_2 for the state preparation instead of three. In this scenario, Alice and Bob are linked by a quantum channel as well as an authenticated classical channel (see Ref. [12, Sec. VII.A] for how to construct an authenticated channel). Their goal is to create a symmetric binary key that is unknown to a potential eavesdropper, Eve, who has access to both the quantum and classical channels. In order to generate a key, Alice sends signals encoded in weak coherent optical pulses that are in turn measured by Bob. In the so-called post-processing, the resulting bit strings are distilled into a secure key.

The authenticity of the classical channel ensures that Eve cannot perform man-in-the-middle attacks by tampering with the channel (swapping, modifying, adding or removing messages). Although authenticated, information transmitted over the classical channel is considered insecure as it can be read by Eve without Alice and Bob noticing. As such, in the following, it will be assumed that Eve has knowledge about all classical communications and that all messages exchanged during the post-processing are authenticated, e.g. using [52–54].

Following the no-cloning theorem of quantum mechanics (see Refs. [6] and [51, Box 12.1] for a proof), the same principle does not apply to the quantum channel, where, even though Eve has access to the channel, her interference causes measurable disturbances. This is in turn taken into account during the privacy amplification step and allows Alice and Bob to estimate bounds for the correlation of their key with Eve's quantum system. These estimates are used in the privacy amplification, which shortens the key so as to arbitrarily reduce Eve's correlation with the final key.

2.1.1 Fixed-length protocols

For the entirety of this work, we consider a fixed-length protocol, as opposed to a variable-length protocol [55, 56] [57, Ch. 3] [58, Supplementary note A]. This informs the definition of security, which we introduce in Sec. 2.3.3 and only holds for keys of length known prior to running the protocol, a subtle fact easily overlooked. The more general definition of security, i.e. when keys of different lengths can be generated, exhibits an additional sum over all possible key lengths, which is formalized in the references above. For fixed-length protocols, the length of the secure-key is fixed prior to running the protocol and does not depend on the statistics observed during the protocol run. The protocol then outputs a secure-key pair, S_A and S_B, shared by Alice and Bob where the keys are either finite bit strings of fixed size l if the protocol run was successful, or $\perp$ if the protocol aborts. This means that any *acceptance parameter* determining the secure-key length must be fixed by Alice and Bob before the protocol run[2]. These parameters define a set of conditions that must be fulfilled by the observed statistics during the so-called *acceptance test* in order for the protocol to not abort, i.e. produce a non-trivial key. This step is often also called *parameter estimation* in the literature.

More formally, prior to running the protocol, Alice and Bob agree on an *acceptance set* Q such that the protocol aborts if the observed statistics F_{obs} are not in the acceptance set, i.e. $F_{\text{obs}} \notin Q$[3].

[1] More precisely, this denotes the mean photon number. Nevertheless, in the following we adhere to the name conventionally used in the literature.

[2] The parameters may however be adjusted between protocol runs.

[3] Unlike other works, where F_{obs} is a frequency vector, here F_{obs} is a set of statistics observed during the protocol.

This means that if any of the conditions fails, the protocol aborts. See Example 1 for an illustrative example and Refs. [24, 55, 59] for a more detailed discussion.

Example 1. *To illustrate the acceptance test, consider, as an example, a protocol for which two conditions need to be satisfied, e.g. $x < X$ and $y \geq Y$ with $x, y \in \mathbb{N}$. The acceptance set can then be parameterized as*

$$Q = \left\{(x, y) \in \mathbb{N}^2 \,|\, x < X \wedge y \geq Y\right\}. \tag{1}$$

A protocol run produces statistics $F_{\text{obs}} = (x_0, y_0)$. During the acceptance test, the protocol aborts if $F_{\text{obs}} \notin Q$, i.e. if at least one of the conditions in Q is not fulfilled. If $F_{\text{obs}} \in Q$, then the length of the key generated is given by

$$l = \min_{(x,y)\in Q} l(x, y)\,, \tag{2}$$

i.e. by minimizing the secure-key length $l(x, y)$ over all possible statistics (x, y) in the acceptance set Q. Note that this optimization is done analytically in this work.

If the protocol does not abort, the secure-key length is given by minimizing the expression for the secure-key length over all possible sets of observations contained in Q. One advantage of this approach is that instead of computing and optimizing the secure-key length during each run, it must only be minimized once for a given Q. Then, only a set of conditions must be verified during the protocol to produce a key of said length. In general, relaxing the conditions imposed by Q lowers the probability for the protocol to abort but also decreases the secure-key length as it is minimized over a larger set. A good choice for Q should thus depend on the practical implementation. For systems with stable channels, e.g. fiber-based systems, a tight set of conditions based on statistics observed in previous protocol runs might be chosen. In this case, if the observed statistics do not fluctuate much, the probability that the protocol aborts is low for appropriately chosen acceptance tests.

For unstable systems, e.g. satellite-based systems, more relaxed bounds may be necessary for the protocol to not abort, which decreases the secure-key length. In this case, a variable-length protocol may be more suitable. For methods to prove variable-length security in the EUR framework, see Refs. [37, Apps. B and F] and [58, Supplementary Note A]. Finally, as discussed in Sec. 6, the approach taken in this work using smooth min-entropies enables an analytical lower bound on the secure-key length which does not require a numerical optimization since the expression on the secure key is monotonously dependent on the set of observed statistics.

2.1.2 Protocol description

The 1-decoy state BB84 protocol is formally described in Fig. 2. Here, we aim at describing the protocol more intuitively. As discussed in the previous section, we consider a fixed-length protocol.

Before the protocol run, Alice and Bob agree on the set of parameters that define the protocol and which can be chosen to optimize the performance. They choose two intensities, μ_1 and μ_2, with $\mu_1 > \mu_2 > 0$, the probability p_k for Alice to choose the intensity k and the probability[4] p_{Z}^A (p_{Z}^B) for Alice (Bob) to choose the Z-basis for state preparation (measurement) with $0 < p_{\mathsf{Z}}^A, p_{\mathsf{Z}}^B < 1$. They also agree on a value for the security parameters ϵ'_{sec} and ϵ_{cor}, the number of bits leak_{EC} to leak for error correction and the number of signals N for Alice to send.

They then agree on an acceptance set Q which defines a set of conditions that need to be fulfilled for the protocol to output a non-trivial key, as discussed in Sec. 2.1.1. For this purpose, they choose values for the acceptance conditions in Q, namely the number of bits used for key generation and parameter estimation, N_{Z} and N_{X} respectively, and choose values for $s^{\text{l}}_{\mathsf{Z},0}$, $s^{\text{l}}_{\mathsf{Z},1}$, $s^{\text{l}}_{\mathsf{X},1}$ and $\Lambda^{\text{u}}_{\mathsf{X}}$, which set the acceptance threshold bounds on the computed decoy statistics, as summarized in Table 1 [60, App. B]. The conditions are verified during the protocol, namely the sifting step and acceptance test, as described in Fig. 2. The acceptance parameters and acceptance test are more thoroughly discussed in

[4] Other publications often only introduce one basis choice probability $p_{\mathsf{Z}} = p_{\mathsf{Z}}^A = p_{\mathsf{Z}}^B$, but this is not necessary.

Remark 1, and in later sections. Finally, they agree on a secure-key length l, cf. Eq. (121), which only depends on parameters fixed prior to running the protocol, including the acceptance parameters. The parameter agreement step (where Alice and Bob determine the protocol parameters and acceptance parameters) is usually not understood as part of the protocol and the acceptance set Q can be adjusted each protocol run. In this work, the parties fix the security parameters (as well as the remaining protocol parameters), which yields an upper bound on the achievable secure-key length l via Eq. (121). Alternatively, one may instead fix the key length l and the length of the hash used for error verification (as well as the remaining protocol parameters), in which case the resulting security parameters are determined accordingly.

The protocol starts with the *state preparation*. For each signal transmitted from Alice to Bob, Alice randomly chooses a bit value, the encoding basis according to p_{Z}^A and an intensity level according to p_k. The signal is then transmitted to Bob who randomly chooses a *measurement* basis according to p_{Z}^B. In practical scenarios, for most signals, Bob does not detect any photons due to losses in the quantum channel. If more than one of Bob's detectors click, he randomly assigns a measurement outcome (see Footnote 9). The first two steps are repeated N times.

Those instances for which Bob had no clicks or Alice and Bob chose different bases do not contain usable information and are discarded during *sifting*. Hence, Alice announces the signal indices and measurement bases. Bob then discards his information about detected signals where Alice chose a different basis or he did not detect a signal, and informs Alice about the remaining measurement results to keep, i.e. those that Bob did not discard. Alice also informs Bob about her intensity choices, which will be required during the acceptance test. For the analysis in this work, it is important to not publish the basis choices before all N signals have been received, cf. Remark 2. In fact, various errors and subtleties in the analysis of protocols with so-called iterative sifting were pointed out in Ref. [61]. For methods to address these issues, we refer to Ref. [62]. During the sifting step, Alice and Bob verify a set of conditions described in Fig. 2. The basis and detect/no-detect announcements are stored in a classical register $\tilde{C}^N$.

After the sifting step, Alice and Bob possess sifted keys $\tilde{Z}_A, \tilde{Z}_B \in \mathcal{Z}$ of length N_{Z}, which are partially correlated with Eve and where $\mathcal{Z} = \{0,1\}^{N_{\mathsf{Z}}}$ is the set containing all possible keys of length N_{Z}. Due to experimental limitations (imperfect state preparation, channel noise, imperfect photon detection) or the presence of an eavesdropper, the sifted keys are usually not identical, hence why during the *error correction* step, Bob corrects his key in order to obtain a key Z_B ideally identical to Z_A. To achieve this, Alice transmits $\mathrm{leak}_{\mathrm{EC}}$ bits of information about her key to Bob. Error correction algorithms usually require an estimate of the error rate, which can for example be obtained from previously processed blocks[5]. We denote Ω_{EC} as the event in which error correction succeeded and store the communications in a classical register C_{EC}. It follows that $|C_{\mathrm{EC}}| = \mathrm{leak}_{\mathrm{EC}}$. The measurement outcomes obtained in the X-basis are publicly revealed and no error correction is applied. The X-basis measurements do not contribute to the final key.

Error correction algorithms are not guaranteed to succeed. Hence, errors might remain unnoticed. To ensure that the keys are equal up to a small probability without disclosing them, a hash of Alice's key is transmitted to Bob, who compares it with a hash of his key. We define Ω_{EV} as the event in which error verification was successful and set $S_A = S_B = \perp$ if it fails. The choice of hash function and the hash of Alice's key are stored in a classical register C_{EV}, which is communicated to Bob. After error verification, Alice's and Bob's keys are identical up to a probability ϵ_{cor}[6], which we show in Sec. 3.1.

Additionally, Bob now has full knowledge over all errors in the Z-basis by comparing the corrected key to his sifted key, allowing him to count the number of errors for a certain basis and intensity, $c_{\mathsf{X},k}$, $c_{\mathsf{Z},k}$, where $k \in \{\mu_1, \mu_2\}$[7]. Bob then verifies an additional set of conditions (cf. Fig. 2 and Remark 1).

[5] We note that a wrong estimate for the error rate does not affect the security in any way but merely increases the probability of the error verification test failing.

[6] This statement should be interpreted with care, see Sec. 2.3.3 and Remark 8.

[7] Notice that Bob only obtained the correct number of errors if error correction succeeded.

Observed statistics	Decoy bound	Acceptance parameter	Acceptance condition
$\lvert X^{\mathrm{S}}\rvert$ (Fig. 2)	-	N_{X}	$\lvert X^{\mathrm{S}}\rvert \geq N_{\mathsf{X}}$
$\lvert Z^{\mathrm{S}}\rvert$ (Fig. 2)	-	N_{Z}	$\lvert Z^{\mathrm{S}}\rvert \geq N_{\mathsf{Z}}$
$s_{\mathsf{Z},0}$	$s^{-}_{\mathsf{Z},0}$ (Eq. (103))	$s^{\mathrm{l}}_{\mathsf{Z},0}$	$s^{-}_{\mathsf{Z},0} \geq s^{\mathrm{l}}_{\mathsf{Z},0}$
$s_{\mathsf{Z},1}$	$s^{-}_{\mathsf{Z},1}$ (Eq. (114))	$s^{\mathrm{l}}_{\mathsf{Z},1}$	$s^{-}_{\mathsf{Z},1} \geq s^{\mathrm{l}}_{\mathsf{Z},1}$
$s_{\mathsf{X},1}$	$s^{-}_{\mathsf{X},1}$ (Eq. (114))	$s^{\mathrm{l}}_{\mathsf{X},1}$	$s^{-}_{\mathsf{X},1} \geq s^{\mathrm{l}}_{\mathsf{X},1}$
Λ_{X}	Λ^{+}_{X} (Eq. (117))	$\Lambda^{\mathrm{u}}_{\mathsf{X}}$	$\Lambda^{+}_{\mathsf{X}} \leq \Lambda^{\mathrm{u}}_{\mathsf{X}}$

Table 1: Acceptance tests performed on the observed statistics and decoy bounds. If any of the conditions fails, the protocol aborts. The acceptance bounds have a pre-defined value that can be freely chosen e.g. to maximize the secure-key length or lower the probability of an abort. See Remark 1 for more details.

We call this step *acceptance test*. We denote Ω_{AT} as the event in which $F_{\mathrm{obs}} \in Q$, i.e. all conditions verified in the sifting step and acceptance test are satisfied. Acceptance testing is summarized in Table 1 and Remark 1. To simplify the notation, we define $\Omega_{\top} := \Omega_{\mathrm{AT}} \wedge \Omega_{\mathrm{EV}}$ such that $\Pr[\Omega_{\top}]$ denotes the probability that the protocol does not abort. The acceptance decision (pass/fail) following the acceptance test and error verification is stored in a classical register C_{AT}.

In contrast to the 2-decoy state protocol, the 1-decoy state protocol requires the number of errors in the Z-basis to compute a bound on the number of single-photon events. Consequently, Bob requires the number of Z-basis errors for the acceptance test, hence why it is performed after error correction. This introduces subtleties in the analysis [37, Remark 14] which are often overlooked in existing works but are explicitly addressed in this work. Bob may in theory also estimate these errors using traditional acceptance testing, which is done right after sifting, by disclosing and discarding a fraction of the key. However, the approach taken in this work allows for tighter bounds and does not disclose Z-basis measurement outcomes, leading to overall higher secure-key rates[8].

Finally, to reduce Eve's knowledge about the key, it is shortened during *privacy amplification* using a randomly chosen hash function. The choice of hash function is stored in a classical register C_{PA} and communicated from Alice to Bob. The secure-key length is calculated using the quantum leftover hash lemma, the entropic uncertainty relation and the decoy-state method which provides bounds on the number of photon events and errors using concentration inequalities, resulting in Eq. (121). We denote Ω_{B} the event where all bounds given by the decoy concentration inequalities hold. For clarity, we list all events used for the fixed-length protocol and their relation to one another in Table 2. We also list all classical communication registers in Table 3. To simplify the notation, we define $C := \tilde{C}^{N} C_{\mathrm{EC}} C_{\mathrm{EV}} C_{\mathrm{AT}} C_{\mathrm{PA}}$ as the classical register storing all classical communications occurring between Alice and Bob during the protocol run.

Remark 1. *The steps involved in the acceptance test for the protocol described in Fig. 2 can be summarized as follows (as depicted in Table 1 and described in Sec. 2.1.1)*

1. *Alice and Bob agree on acceptance parameters before the protocol run (third column in Table 1).*
2. *During the protocol, they have access to certain statistics, e.g. the number of* X*-basis and* Z*-basis detections after sifting, $\lvert X^{\mathrm{S}}\rvert$ and $\lvert Z^{\mathrm{S}}\rvert$. However, they cannot determine the exact number of vacuum or single-photon events, denoted $s_{\mathsf{Z},0}, s_{\mathsf{Z},1}$ and $s_{\mathsf{X},1}$, nor the exact error rate Λ_{X}. Therefore, they compute bounds for the inaccessible statistics using the decoy-state method (second column in Table 1). We denote these bounds with subscripts + and - throughout this work to differentiate them from acceptance bounds which are denoted with subscripts* u *and* l*. As such, the bounds denoted with subscripts + and - are random variables observed during the protocol while the acceptance bounds have fixed values.*

[8] We note that for the 2-decoy state protocol, the number of errors in the Z-basis are not required, cf. App. A.2. In this case, the acceptance test can be performed before error correction. The proof can however be performed analogously.

3. *They verify the corresponding acceptance conditions for the observed and the computed statistics by comparing them to the acceptance parameters (fourth column in Table 1), and abort the protocol if any of the conditions is not met. The acceptance set Q is defined by the set of acceptance conditions, see Example 1.*

Remark 2. *Usually, Alice and Bob disclose the basis choices and whether or not Bob detected a signal only after all signals have been received. For practical reasons, e.g. to lower memory usage, it may be convenient to perform on-the-fly announcements during the signal transmission and measurement stage of the protocol. This complicates the analysis [61,62]. In this work, we perform traditional sifting, as described in Fig. 2, where all announcements take place after all signals have been measured.*

Remark 3. *In Fig. 2, part of the acceptance conditions are verified during the sifting step and not in the acceptance test. The advantage of this approach is that the protocol may already abort before error correction and verification if insufficient signals are detected. For the analysis, we assume the scenario where all conditions are verified during the acceptance test, but note that both scenarios are equivalent for the purposes of proving security.*

Figure 2: **Protocol description**

Inputs:

Security parameters:	$\epsilon_{\text{sec}'} \in (0,1),\ \epsilon_{\text{cor}} \in (0,1),\ \epsilon_{\text{sec}'} + \epsilon_{\text{cor}} \leq \epsilon$
Setup parameters:	$\mu_1 > \mu_2 > 0,\ p_k \in (0,1),\ p^A_{\mathsf{Z}} \in (0,1),\ p^B_{\mathsf{Z}} \in (0,1),\ N \geq 0$
Acceptance parameters:	$N_{\mathsf{X}},\ N_{\mathsf{Z}},\ s^{\text{l}}_{\mathsf{Z},0},\ s^{\text{l}}_{\mathsf{Z},1},\ s^{\text{l}}_{\mathsf{X},1},\ \Lambda^{\text{u}}_{\mathsf{X}} \geq 0$
Post-processing parameters:	$\text{leak}_{\text{EC}} \geq 0,\ l > 0$ computed from Eq. (121)

1. **State preparation:** For the i-th signal, Alice chooses a basis $b^A_i \in \{\mathsf{X}, \mathsf{Z}\}$ with probability p^A_{Z} of choosing the Z-basis, which is used to generate the key, and probability p^A_{X} of choosing the X-basis, which is used for monitoring the phase error rate. She then chooses an intensity $k_i \in \{\mu_1, \mu_2\}$ according to p_k and encodes a randomly chosen bit value $y^A_i \in \{0,1\}$ in a weak coherent and phase-randomized optical pulse she sends to Bob through the quantum channel.

2. **Measurement:** For each signal, Bob measures in the basis $b^B_i \in \{\mathsf{X}, \mathsf{Z}\}$, randomly chosen with probabilities p^B_{X} and p^B_{Z}, yielding $y^B_i \in \{0, 1, \varnothing\}$, with $\varnothing$ denoting the case where he does not detect a signal. In the case of multiple detections, Bob randomly assigns one of the measurement outcomes to the signal[9].

3. **Sifting:** The two first steps are repeated N times. Alice and Bob then communicate their choice of basis and intensity in the classical channel and only keep the signals for which $b^A_i = b^B_i$. As such, we define the sets $X^{\text{S}} \coloneqq \{i : b^A_i = b^B_i = \mathsf{X} \wedge y^B_i \neq \varnothing\}$ and $Z^{\text{S}} \coloneqq \{i : b^A_i = b^B_i = \mathsf{Z} \wedge y^B_i \neq \varnothing\}$. Here, they also sift out all signals that were not detected, i.e. resulting in $y^{\text{B}}_i \neq \varnothing$. They verify the following conditions:

$$|X^{\text{S}}| \geq N_{\mathsf{X}} \qquad \text{and} \qquad |Z^{\text{S}}| \geq N_{\mathsf{Z}}\,. \tag{3}$$

   If any condition does not hold, they set $S_A = S_B = \perp$ and abort the protocol. Otherwise, they choose random subsets $\Gamma_{\mathsf{X}} \subset X^{\text{S}}$ and $\Gamma_{\mathsf{Z}} \subset Z^{\text{S}}$ of sizes N_{X} and N_{Z}, respectively[10]. Alice's and

[9] For the canonical model of ideal threshold detectors, this is mandatory to satisfy the basis-efficiency mismatch condition from the phase error rate estimation discussed in Sec. 4.4. Discarding these detections also makes the systems vulnerable to an attack exploiting this [38, Table 4.3].

[10] This step involves classical communications between Alice and Bob as they agree on the same subsets Γ_{X} and Γ_{Z}. Nevertheless, since the subsets are chosen at random, they are not correlated with the raw key and it can be shown that they do not provide any information to Eve, analogously to the argument used for the error verification hash function, cf. Eq. (60).

Bob's sifted keys in the Z-basis are defined as the bit sequences $\tilde{Z}_A \coloneqq (y_i^A)_{i\in\Gamma_\mathsf{Z}}$ and $\tilde{Z}_B \coloneqq (y_i^B)_{i\in\Gamma_\mathsf{Z}}$. For the X-basis, we define $\tilde{X}_A \coloneqq (y_i^A)_{i\in\Gamma_\mathsf{X}}$ and $\tilde{X}_B \coloneqq (y_i^B)_{i\in\Gamma_\mathsf{X}}$. Additionally, we define $\Gamma_{\mathsf{Z},k} \coloneqq \{i \in \Gamma_\mathsf{Z} : k_i = k\}$ and $\tilde{Z}_{B,k} \coloneqq (y_i^B)_{i\in\Gamma_{\mathsf{Z},k}}$, which corresponds to the part of Bob's sifted key that originated from detections with intensity choice k. We analogously define $\tilde{X}_{A,k}$ and $\tilde{X}_{B,k}$.

4. **Error correction:** An error correction scheme that publishes $\mathrm{leak}_{\mathrm{EC}}$ bits of information is applied in order for Bob to compute an estimate Z_B of $\tilde{Z}_A$, also called corrected key. Let f be a helper function that maps an index $j \in \{1, ..., N_\mathsf{Z}\}$ to the corresponding index in terms of the signal rounds $\{1, ..., N\}$. Then, we define $\Gamma^{\mathrm{cor}}_{\mathsf{Z},k} \coloneqq \{j : k_{f(j)} = k\}$ and therefore $Z_{B,k} \coloneqq (Z_B^j)_{j\in\Gamma^{\mathrm{cor}}_{\mathsf{Z},k}}$ is the error-corrected bit string corresponding to detections with intensity choice k, in analogy to $\tilde{Z}_{B,k}$, where Z_B^j is the j-th element of Z_B. Alice's key remains unchanged and we define $Z_A = \tilde{Z}_A$ as Alice's key after error correction. The X-basis detections $\tilde{X}_A$ and $\tilde{X}_B$ also remain unchanged.

5. **Error verification:** Alice then computes the hash of length $\lceil \log_2 1/\epsilon_{\mathrm{cor}} \rceil$ corresponding to Z_A given a randomly chosen universal$_2$ hash function. She sends the hash as well as her choice of hash function to Bob who in turn computes the hash of Z_B using the same hash function as Alice. If both hashes disagree, the protocol aborts and they set $S_A = S_B = \perp$. Otherwise, the protocol continues and the corrected keys are called verified keys.

6. **Acceptance test:** Alice discloses her X-basis bits. For each intensity k, Bob compares $\tilde{Z}_{B,k}$ with $Z_{B,k}$ to determine the number of errors, $c_{\mathsf{Z},k} = |\tilde{Z}_{B,k} \oplus Z_{B,k}|$, and $\tilde{X}_{A,k}$ with $\tilde{X}_{B,k}$ to determine $c_{\mathsf{X},k} = |\tilde{X}_{A,k} \oplus \tilde{X}_{B,k}|$. The Hamming distance $|\cdot \oplus \cdot|$ corresponds to the number of bits that do not coincide in both strings. Bob computes $c_\mathsf{X} = \sum_k c_{\mathsf{X},k}$ and $c_\mathsf{Z} = \sum_k c_{\mathsf{Z},k}$. He then computes the bounds $s^-_{\mathsf{Z},0}, s^-_{\mathsf{Z},1}$, $s^-_{\mathsf{X},1}$ and Λ^+_X from the observations using the decoy-state method, cf. Sec. 5. They perform the acceptance test by verifying the following conditions:

$$s^-_{\mathsf{Z},0} \geq s^{\mathrm{l}}_{\mathsf{Z},0} \quad \text{and} \quad s^-_{\mathsf{Z},1} \geq s^{\mathrm{l}}_{\mathsf{Z},1} \quad \text{and} \quad s^-_{\mathsf{X},1} \geq s^{\mathrm{l}}_{\mathsf{X},1} \quad \text{and} \quad \Lambda^+_\mathsf{X} \leq \Lambda^{\mathrm{u}}_\mathsf{X}\,. \tag{4}$$

If any condition does not hold, they set $S_A = S_B = \perp$ and abort the protocol.

7. **Privacy amplification:** Alice extracts a secure key S_A of fixed length l, cf. Eq. (121), from Z_A using a randomly chosen universal$_2$ hash function. The choice of function is communicated to Bob who uses it to compute a secure key S_B from Z_B.

Event	Description	Relation
Ω_{EC}	Error correction succeeded	-
Ω_{EV}	Error verification passed	-
Ω_{AT}	Acceptance test passed	-
$\Omega_\top$	Protocol did not abort	$\Omega_\top = \Omega_{\mathrm{EV}} \wedge \Omega_{\mathrm{AT}}$
$\tilde{\Omega}$	Protocol did not abort and error correction succeeded	$\tilde{\Omega} = \Omega_\top \wedge \Omega_{\mathrm{EC}}$
Ω_{B}	Decoy bounds hold	-
$\Omega_\circ$	True values of the statistics are in the acceptance set	$\Omega_{\mathrm{AT}} \wedge \Omega_{\mathrm{EC}} \wedge \Omega_{\mathrm{B}} \Rightarrow \Omega_\circ$

Table 2: Overview of the various events used in the protocol described in Fig. 2.

2.2 Theoretical background

The aim of this section is to provide a theoretical background and thus form a foothold for the concepts discussed in this work but does not aim at deriving each concept introduced. We refer to the textbooks [50, 51] or more recently [48, 49] for a more detailed discussion. These textbooks also serve as a good

Register	Description
$\tilde{C}^N$	Basis and detect/no-detect announcements
C_{EC}	Bits leaked for error correction, $\lvert C_{\mathrm{EC}}\rvert = \mathrm{leak}_{\mathrm{EC}}$
C'_{EV}	Hash of Alice's corrected key, $\lvert C'_{\mathrm{EV}}\rvert = \log_2 2/\epsilon_{\mathrm{cor}}$
C''_{EV}	Choice of hash function for error verification
C_{EV}	$C_{\mathrm{EV}} = C'_{\mathrm{EV}} C''_{\mathrm{EV}}$
C_{AT}	Acceptance decision (pass/fail)
C_{PA}	Choice of hash function for privacy amplification
C	$C = \tilde{C}^N C_{\mathrm{EC}} C_{\mathrm{EV}} C_{\mathrm{AT}} C_{\mathrm{PA}}$
C'	Generic classical register

Table 3: Overview of the classical communication registers used in the protocol described in Fig. 2.

introduction to the basics of the quantum mechanical formalism and quantum information theory. For a more mathematical description, Tomamichel's book [63] as well as his thesis [64] serve as good references and discuss many of the concepts used in this work.

2.2.1 Representing quantum systems

We assume that the reader is familiar with the Dirac notation of quantum mechanics and the density operator formalism. In the following, the density operator

$$\rho_A = \sum_a P_A(a) \lvert a\rangle\langle a\rvert \in S(\mathcal{H}_A)\,, \tag{5}$$

acting on a Hilbert space $\mathcal{H}_{\mathcal{A}}$ describes the quantum state of a quantum system A, where $P_A(a)$ can be interpreted as the probability of preparing the system in the state $\lvert a\rangle$ and $S(\mathcal{H}_A)$ is the set of positive semi-definite matrices of trace one acting on $\mathcal{H}_A$.

Consider a *classical random variable* Z following a distribution P_Z on some set $\mathcal{Z}$ where the probability of each outcome $z \in \mathcal{Z}$ is given by $P_Z(z)$. The classical values z can be represented as orthogonal states $\lvert z\rangle \in \mathcal{H}_Z$ reflecting their distinguishability, which is a property common to classical variables [24, Sec. 2.1]. Indeed, distinguishability describes the ability to differentiate two states given the outcome of a measurement. In the quantum realm, states are reliably distinguishable if the outcome of a measurement can be uniquely assigned to a quantum state. In theory, this can always be done for orthogonal states $\{\lvert z\rangle\}_z$, as we can define a measurement operator $M = \sum_z M_z$ with $M_z = z\lvert z\rangle\langle z\rvert$ for which the measurement results are unique for each $\lvert z\rangle$ and given by the eigenvalue problem $M\lvert z\rangle = z\lvert z\rangle$. A proof that non-orthogonal states cannot be reliably distinguished can be found in Ref. [51, Sec. 2.2.4]. Given these properties, the density operator representation of a classical distribution P_Z can be written as

$$\rho_Z = \sum_z P_Z(z) \lvert z\rangle\langle z\rvert\,, \tag{6}$$

in analogy to Eq. (5).

2.2.2 Distance between quantum states

In order to quantify the distinguishability of two density operators, one introduces a distance measure which is directly related to the probability of distinguishing them. For two density operators ρ and σ, the *trace distance* is defined as

$$D(\rho,\sigma) \coloneqq \frac{1}{2}\lVert\rho-\sigma\rVert_1\,, \tag{7}$$

where $\|\tau\|_1 = \mathrm{Tr}\left\{\sqrt{\tau^\dagger \tau}\right\}$ denotes the *trace norm* (also called Schatten 1-norm) of a density operator τ. The trace distance generalizes the *total variation distance* from the field of statistics, i.e. classical probability distributions to density operators.

Now, the density operators are said to be ζ-*close* if $D(\rho, \sigma) \leq \zeta$. An intuitive operational interpretation of the trace distance is given by the following scenario. We assume a source capable of preparing two known quantum states ρ and σ with equal probability, for which $D(\rho, \sigma) \leq \zeta$. The task is to determine which state was prepared, only by measuring the resulting quantum state. The probability with which the measurement result can be assigned to the correct quantum state is directly related to the trace distance and upper-bounded by

$$P_{\text{distinguish}}(\rho, \sigma) \leq \frac{1}{2} + \frac{\zeta}{2}, \tag{8}$$

regardless of the measurement strategy adopted, cf. Ref. [65, Sec. 9.1.4] for a proof, and Refs. [51, Sec. 9.1] [64, Sec. 3.2.1] [66, Sec. 2.4.2] for discussions. In other words, two ζ-close operators cannot be distinguished with a probability more than ζ [24, Sec. 2.1.4], meaning that the trace distance can be interpreted as a *distinguishing advantage*. This statement will have profound implications for the intuition behind the security of a protocol, as will be discussed in Sec. 2.3.

Intuitively, in the case of pure orthonormal states, $D(\rho, \sigma) = 1$ as they can be reliably distinguished. Identical quantum states, on the other hand, cannot be distinguished and $D(\rho, \sigma) = 0$. For a more detailed discussion about the intuition behind the trace distance, we refer to App. A.3.

As any density operator ρ is Hermitian, $\rho^\dagger = \rho$ by definition and ρ is diagonalizable, so that $\|\rho\|_1 = \sum_i |p_i|$ where $\{p_i\}_i$ is the set of eigenvalues of ρ. This representation of $\|\rho\|_1$ as a function of the probability mass functions $\{p_i\}_i$ directly connects the density operator to the classical distributions discussed in App. A.3 and will be used when discussing the entropy of a quantum system in Sec. 4. As such, classical distributions and their quantum analogues exhibit the same properties regarding the interpretation of the trace distance as distinguishing advantage. For a more detailed discussion, we refer to Refs. [12, App. A] [63, Sec. 3.2] [51, Sec. 9.2] [64, Sec. 3.2].

2.2.3 Bipartite quantum systems

In the scenario where Alice and Bob exchange information through a quantum channel, the density operators ρ_A and ρ_B describe their respective quantum information. The bipartite system of two quantum systems A and B describing the joint quantum state of the systems is represented by $\rho_{AB} \in S(\mathcal{H}_{AB})$, where $\mathcal{H}_{AB} = \mathcal{H}_A \otimes \mathcal{H}_B$, $S(\mathcal{H}_{AB})$ is the set of positive semi-definite Hermitian matrices of trace one acting on $\mathcal{H}_{AB}$ and $\otimes$ denotes the tensor product.

If $\rho_{A|Z}$ represents a quantum system A that depends on a classical variable Z, we can write the *classical-quantum bipartite system* as

$$\rho_{ZA} = \sum_z P_Z(z) \, |z\rangle\langle z| \otimes \rho_{A|Z=z}, \tag{9}$$

where $\rho_{A|Z=z}$ describes quantum system A conditioned on $Z = z$ [24, Sec. 2.1.3]. Intuitively, the bipartite system describes two correlated quantum systems, where A depends on the outcome of Z. In turn, this means that any measurement on Z also influenced the outcome of A. For an event Ω on the classical register Z, (where an event is defined to be any set of classical outcomes), the state $\rho_{ZA|\Omega}$ *conditioned on the event* Ω, is written as

$$\rho_{ZA|\Omega} = \frac{\rho_{ZA\wedge\Omega}}{\mathrm{Tr}\{\rho_{ZA\wedge\Omega}\}}, \qquad \text{with} \qquad \rho_{ZA\wedge\Omega} = \sum_{z\in\Omega} P_Z(z) \, |z\rangle\langle z| \otimes \rho_{A|Z=z}. \tag{10}$$

Note that $\rho_{ZA|\Omega}$ is a normalized density matrix, while $\rho_{ZA\wedge\Omega}$ (sometimes referred to as *partial* state) is sub-normalized. In the following, the operator $\wedge$ has higher precedence than the operator $|$, i.e. it acts before the operator $|$. An expression such as $\rho_{ZA|\Omega_1\wedge\Omega_2}$ is to be interpreted as $\rho_{ZA|(\Omega_1\wedge\Omega_2)}$.

Remark 4. *The steps involved in a QKD protocol run depend on the specific events that occur during that run, following the protocol description in Fig. 2. Therefore, for rigorous security proofs, it is essential to compute relevant entropies and statistics on states that are properly conditioned on these events. This is crucial because conditioning can affect entropies in significant ways. In this work, we almost exclusively use the normalized variant of conditioning on events, i.e.* $\rho_{ZA|\Omega}$*. Furthermore, we make it a point to explicitly clarify this aspect of conditioning in all our calculations, addressing a detail that is often overlooked.*

Remark 5. *When conditioning on events, it is also important to ensure that the event is well-defined. In particular, there must exist (in theory) a classical register that determines whether or not the event occurred. Note that we are free to trace out this classical register after conditioning on it. For example,* $\rho_{A\wedge\Omega} = \mathrm{Tr}_Z\{\rho_{ZA\wedge\Omega}\}$ *is a well-defined state conditioned on* Ω*, which does not include the register* Z *determining the event.*

2.3 Definition of security

The goal of a quantum key distribution protocol is to establish a shared random key known only to Alice and Bob. This is achieved by making use of the laws of quantum mechanics combined with classical information theory and cryptography.

This section aims at defining the security of the protocol and is structured as follows. First, we introduce the concept of information-theoretic security in Sec. 2.3.1 and state the assumptions of quantum key distribution, underlying all further analyses, in Sec. 2.3.2. Using the trace distance defined in Sec. 2.2.1, we are then able to define the secrecy, correctness and security of the protocol in Sec. 2.3.3 in terms of so-called ϵ-parameters. We will introduce these parameter constructively starting out with the general definition of security. The secrecy parameter is then expanded in terms of the decoy concentration inequalities holding and failing in Sec. 2.3.4. Finally, the concept of composable security is introduced in Sec. 2.3.5 and the one-time pad discussed in Sec 2.3.6 as an information-theoretically secure cryptographic primitive for message encryption.

2.3.1 Information-theoretic security

A key generation protocol is said to be *perfectly secure* if an adversary with infinite computing power cannot gather any information about the key [67]. This condition is guaranteed if the key output meets following criteria [5, 68]:

1. The key is secret.
2. It has been randomly generated, following a uniform distribution.

The second condition can be fulfilled by using an ideal quantum random number generator [69]. In contrast, the first condition is more difficult to fulfill when the generated key is shared by multiple parties. In fact, the only known method to classically share a perfectly secure key is by transporting it physically, e.g. from Alice to Bob[11]. There is no known and proven way to accomplish this task using only a classical channel.

However, QKD provides a solution based on the laws of quantum mechanics. Even though perfect security can also not be guaranteed by QKD, it allows for an arbitrarily close approximation of the ideal case. The remaining deviation from perfect security is described in terms of ϵ-parameters, which are introduced in Sec. 2.3.3, therefore enabling *information-theoretic security*. In classical cryptography, there is no proven method to share an information-theoretically secure key remotely. Remotely shared symmetric keys can only be generated algorithmically, when replacing the requirements for information-theoretical security by the stronger assumption of a computational bound on Eve.

[11] This is also known as the *courier problem*.

We note that, in the case assumed in the following, where the key is shared between multiple parties, i.e. Alice and Bob, an additional condition stating that Alice's and Bob's keys must be identical is appended to the list above.

2.3.2 Assumptions of quantum key distribution

As mentioned in the previous section, information-theoretical security is made possible by quantum key distribution, which does not make any assumptions about Eve's computing power. This relaxation enables the sharing of keys that fulfill the conditions for information-theoretic security as stated in Sec. 2.3.1. However, QKD is not deprived of assumptions, but rather based on a set of three assumptions, namely [12, Sec. IV.A]

1. Quantum physics is a correct and complete theory [70].
2. The classical channel used by Alice and Bob is authenticated.
3. The devices used during the protocol perform exactly as instructed[12].

The first condition is rather fundamental and widely accepted. In the QKD security-proof literature, the term *authenticated channel* is typically used to refer to an idealized classical communication channel in which all messages sent by one party are eventually received correctly by the other party. This is the model assumed throughout this work. We emphasize that such a guarantee cannot be achieved in practice. Instead, practical authentication schemes ensure that *either* a transmitted message is received correctly, *or* the receiving party obtains a special symbol indicating authentication failure (see, e.g., Refs. [54, 71]). Importantly, the security of QKD protocols using such authentication mechanisms can be reduced to the security analysis in the idealized authenticated channel model assumed here, using Ref. [72]. For subsequent rounds, a part of the secure key from previous rounds can be used for authentication [12, 54][13].

The last condition is perhaps the most difficult to ensure as devices, such as single-photon detectors and photon sources, are necessarily imperfect, making room for a wide variety of *side-channel attacks* that specifically aim to exploit these loopholes in order to obtain more information about the key than initially modeled in the security proof. In recent years, *quantum hacking* has become a prominent field of research as QKD systems become more viable and are commercialized, strengthening the importance of characterizing them and ensuring no loophole can be exploited by potential eavesdroppers [40, 41, 74, 75]. In general, these loopholes can be addressed by adjusting the device modeling in the security proof or by redesigning practical implementations[14]. Our work aims to establish a baseline security proof and therefore does not consider these complications. For a more thorough discussion, we refer to Refs. [38, 39].

2.3.3 Security parameters

Due to the probabilistic nature of quantum key distribution, information theory and the cryptographic post-processing, perfect security of a QKD protocol cannot be guaranteed. Therefore, we define so-called *security parameters*, or ϵ-*parameters*, that dictate how close the protocol should be from a perfectly secure protocol which generates keys that fulfill the criteria stated in the previous section. Choosing sufficiently small ϵ-parameters, the protocol can be chosen to be arbitrarily close to a perfectly secure protocol. The goal of this section is to introduce these parameters and discuss their direct

[12] In our case, this implies that we assume no device imperfections are present.

[13] Quantum key distribution can thus be described as a key expansion method since it requires a seed key for authentication, cf. Refs. [12, 73] for a more thorough discussion.

[14] *Device-independent* protocols [32, 76] reduce the assumptions on the devices by partly removing the need to trust them, which can also be used to address the issue of device imperfections and loopholes.

operational meaning. We start with the general definition of security and constructively introduce the correctness and secrecy parameters by conditioning the trace distance on various events.

Let S_A and S_B be Alice's and Bob's secure keys, output by the protocol after having performed all the steps described in Fig. 2.1. Recall that we use the convention that the key registers store $\perp$ whenever the protocol aborts. In the following, A, B and E represent Alice's, Bob's and Eve's quantum systems, respectively, with C denoting the classical register storing all classical communications, cf. Table 3.

Definition 1 (Security)**.** *A protocol is called ϵ-secure if*

$$D(\rho_{S_A S_B EC}, \rho^{\text{ideal}}_{S_A S_B EC}) \leq \epsilon\,, \tag{11}$$

where $\rho_{S_A S_B EC}$ describes the quantum system of Alice's key, Bob's key, Eve and the classical communications at the output of the protocol. The state $\rho^{\text{ideal}}_{S_A S_B EC}$ denotes the output state obtained for the actual protocol, but where the key registers are replaced with perfect keys $U_{S_A S_B}$ if the protocol accepts, and $\perp$ if the protocol aborts, and where

$$U_{S_A S_B} = \frac{1}{|\mathcal{S}|} \sum_{s \in \mathcal{S}} |s\rangle\langle s|_A \otimes |s\rangle\langle s|_B \tag{12}$$

is the uniform distribution of all possible keys s represented by $|s\rangle$ [24, Sec. 2.2.2].

The definition of security stated above holds for fixed-length protocols where the size of the key registers is fixed and known prior to running the protocol, a subtle fact often overlooked. A more general definition of security, i.e. for variable-length protocols, requires an additional sum over all possible key lengths in Eq. (11), as mentioned in Sec. 2.1.1. We discuss the operational interpretation of this definition later in this section. The main goal of the security proof is precisely to determine ϵ and relate it to the length of the key produced by the protocol whenever it does not abort.

Throughout the protocol, Alice and Bob perform the steps described in Fig. 2 on their system. As such, in the following, the description of the system $\rho_{S_A S_B EC}$ involves careful conditioning on various events, cf. Sec. 2.2.3, describing the different outcomes of their actions and decisions. This structure can be visualized in a probability tree depicted in Fig. 3, which serves as a reference point that we will refer to throughout this work. To avoid cluttering the notation, we define the distance to an ideal protocol, conditioned on an event Ω, as

$$d_{\text{sec}}(S_A S_B EC)_{\rho|\Omega} \coloneqq D(\rho_{S_A S_B EC|\Omega}, \rho^{\text{ideal}}_{S_A S_B EC|\Omega})\,, \tag{13}$$

where we use the normalized conditioning introduced in Sec. 2.2.3. For simplicity, it is common to reformulate Eq. (11) in terms of the *correctness* and *secrecy* parameters [12]. Therefore, we expand the definition of security to constructively introduce these parameters in the following. We use the triangle inequality of the trace distance to write

$$d_{\text{sec}}(S_A S_B EC)_\rho \leq \Pr[\Omega_{\text{EC}}] d_{\text{sec}}(S_A S_B EC)_{\rho|\Omega_{\text{EC}}} + \Pr[\neg\Omega_{\text{EC}}] d_{\text{sec}}(S_A S_B EC)_{\rho|\neg\Omega_{\text{EC}}}\,, \tag{14}$$

where we have split the trace distance in components conditioned on error correction succeeding and failing. The probabilities $\Pr[\Omega_{\text{EC}}]$ and $\Pr[\neg\Omega_{\text{EC}}]$ are not known in practice as they depend on the sifted key (which depends on Eve's attack) and the error correction algorithm used. The above inequality directly corresponds to the first node in Fig. 3. Expanding the second term in Eq. (14) using the triangle inequality again yields

$$\Pr[\neg\Omega_{\text{EC}}] d_{\text{sec}}(S_A S_B EC)_{\rho|\neg\Omega_{\text{EC}}} \leq \Pr[\neg\Omega_{\text{EC}} \wedge \Omega_{\text{EV}}] \cdot 1 + \Pr[\neg\Omega_{\text{EC}} \wedge \neg\Omega_{\text{EV}}] \cdot 0\,, \tag{15}$$

where we used the fact that when the protocol aborts, i.e. $\neg\Omega_{\text{EV}}$ occurs, the distance to an ideal protocol is zero as Alice's and Bob's key are trivially $S_A = S_B = \perp$ [12, Sec. III.B]. We also substituted $d_{\text{sec}}(S_A S_B EC)_{\rho|\neg\Omega_{\text{EC}}\wedge\Omega_{\text{EV}}} \leq 1$ as no better bound is known when error correction fails. The term

$\Pr[\neg\Omega_{\mathrm{EC}} \wedge \Omega_{\mathrm{EV}}]$ corresponds to branch (a) in Fig. 3 and will explicitly be addressed in Sec. 3.1 when introducing universal$_2$ hashing for error verification. We may now rewrite the first term in Eq. (14). Since it is conditioned on error correction succeeding, we can write

$$D(\rho_{S_A S_B EC|\Omega_{\mathrm{EC}}}, \rho^{\mathrm{ideal}}_{S_A S_B EC|\Omega_{\mathrm{EC}}}) = D(\rho_{S_A EC|\Omega_{\mathrm{EC}}}, \rho^{\mathrm{ideal}}_{S_A EC|\Omega_{\mathrm{EC}}}) \tag{16}$$

and omit Bob's system for this term in the following. Analogously to above, applying the triangle inequality yields

$$\Pr[\Omega_{\mathrm{EC}}] d_{\mathrm{sec}}(S_A EC)_{\rho|\Omega_{\mathrm{EC}}} \leq \Pr[\Omega_{\mathrm{EC}} \wedge \Omega_{\mathrm{EV}}] d_{\mathrm{sec}}(S_A EC)_{\rho|\Omega_{\mathrm{EC}}\wedge\Omega_{\mathrm{EV}}}\,, \tag{17}$$

where we used $d_{\mathrm{sec}}(S_A EC)_{\rho|\Omega_{\mathrm{EC}}\wedge\neg\Omega_{\mathrm{EV}}} = 0$ as the protocol aborts[15]. This inequality can be rewritten by applying the triangle inequality one last time, yielding

$$\Pr[\Omega_{\mathrm{EC}} \wedge \Omega_{\mathrm{EV}}] d_{\mathrm{sec}}(S_A EC)_{\rho|\Omega_{\mathrm{EC}}\wedge\Omega_{\mathrm{EV}}} \leq \Pr[\Omega_{\top} \wedge \Omega_{\mathrm{EC}}] d_{\mathrm{sec}}(S_A EC)_{\rho|\Omega_{\top}\wedge\Omega_{\mathrm{EC}}} \tag{18}$$

where we substituted $d_{\mathrm{sec}}(S_A EC)_{\rho|\Omega_{\mathrm{EC}}\wedge\Omega_{\mathrm{EV}}\neg\Omega_{\mathrm{AT}}} = 0$ when $\neg\Omega_{\mathrm{AT}}$ occurs, i.e. the protocol aborts during the acceptance test. We recall that $\Omega_{\top} = \Omega_{\mathrm{EV}} \wedge \Omega_{\mathrm{AT}}$ describes the event that the protocol does not abort, cf. Table 1. We can explicitly write the ideal state conditioned on the protocol not aborting and error correction succeeding as

$$\rho^{\mathrm{ideal}}_{S_A EC|\Omega_{\top}\wedge\Omega_{\mathrm{EC}}} = U_{S_A} \otimes \rho_{EC|\Omega_{\top}\wedge\Omega_{\mathrm{EC}}}\,, \tag{19}$$

following Def. 1. Finally, combining the above expressions, we can rewrite the definition of security as

$$\boxed{d_{\mathrm{sec}}(S_A S_B EC)_{\rho} \leq \underbrace{\Pr[\neg\Omega_{\mathrm{EC}} \wedge \Omega_{\mathrm{EV}}]}_{\leq \epsilon_{\mathrm{cor}}} + \underbrace{\Pr[\Omega_{\top} \wedge \Omega_{\mathrm{EC}}] d_{\mathrm{sec}}(S_A EC)_{\rho|\Omega_{\top}\wedge\Omega_{\mathrm{EC}}}}_{\leq \epsilon'_{\mathrm{sec}}} \leq \epsilon\,,} \tag{20}$$

which is a more convenient expression to prove security in the rest of this work. We now define the correctness and secrecy parameters using the convention commonly used, which slightly differs from the expression derived above, cf. Remark 6.

Definition 2 (Correctness)**.** *A protocol is called ϵ_{cor}-correct if $\Pr[\neg\Omega_{\mathrm{EC}} \wedge \Omega_{\top}] = \Pr[S_A \neq S_B \wedge \Omega_{\top}] \leq \epsilon_{\mathrm{cor}}$, i.e. the probability that the protocol does not abort and the keys are not identical is upper-bounded*[16]*.*

Definition 3 (Secrecy)**.** *A protocol is called ϵ_{sec}-secret if*

$$\Pr[\Omega_{\top}] D(\rho_{S_A EC|\Omega_{\top}}, U_{S_A} \otimes \rho_{EC|\Omega_{\top}}) \leq \epsilon_{\mathrm{sec}}\,, \tag{21}$$

where $\Pr[\Omega_{\top}] = 1 - \Pr[S_A = \perp]$ is the probability that the protocol does not abort, $\rho_{S_A EC|\Omega_{\top}}$ describes the bipartite quantum system of Alice's key and Eve as well as the classical communications, conditioned on the protocol not aborting, and

$$U_{S_A} = \frac{1}{|\mathcal{S}|} \sum_{s \in \mathcal{S}} |s\rangle\langle s| \tag{22}$$

is the uniform distribution of all possible secure keys s represented by $|s\rangle$ [24, Sec. 2.2.2].

[15] We also note that $\Pr[\Omega_{\mathrm{EC}} \wedge \neg\Omega_{\mathrm{EV}}] = 0$ as error verification always succeeds if the keys are identical, which follows from the definition of universal$_2$ hashing discussed in Sec. 3.1.

[16] Setting $S_A = S_B = \perp$ if the protocol aborts ensures that the more general definition $\Pr[S_A \neq S_B] \leq \epsilon_{\mathrm{cor}}$ follows from the one stated above, cf. Remark 8.

Remark 6. *When considering traditional acceptance testing, which is performed directly after sifting, Eq. (20) further simplifies to* $\epsilon_{\text{cor}} + \epsilon_{\text{sec}} \leq \epsilon$*. Typically, a security proof for QKD protocols is then obtained by showing that the protocol satisfies the* ϵ_{cor}*-correctness and* ϵ_{sec}*-secrecy criteria separately, and argue that this implies the* $(\epsilon_{\text{cor}} + \epsilon_{\text{sec}})$*-security of the QKD protocol. In this work, we do not prove secrecy and correctness as defined above separately, but still include a discussion of these concepts in this section for pedagogical reasons. This is because the 1-decoy state protocol requires error correction to succeed for Bob to obtain the correct number of errors in the* Z*-basis and therefore make the correct acceptance decision. Thus, the second term in Eq. (20) is additionally conditioned on* Ω_{EC} *compared to Def. 3, hence why we define it as* ϵ'_{sec}*. This is different from typical QKD protocols, where the accept decision is only based on public announcements. Nevertheless, the first term in Eq. (20) directly corresponds to the correctness parameter as* $\Pr[\neg\Omega_{\text{EC}} \wedge \Omega_{\text{EV}}] \geq \Pr[\neg\Omega_{\text{EC}} \wedge \Omega_{\top}]$*. We emphasize that the discrepancy in the definition of the secrecy parameter does not alter the security of the protocol in any way, as the resulting bounds satisfy the definition of security, cf. Def. 1. Defining correctness and secrecy is merely a common intermediate step performed for convenience.*

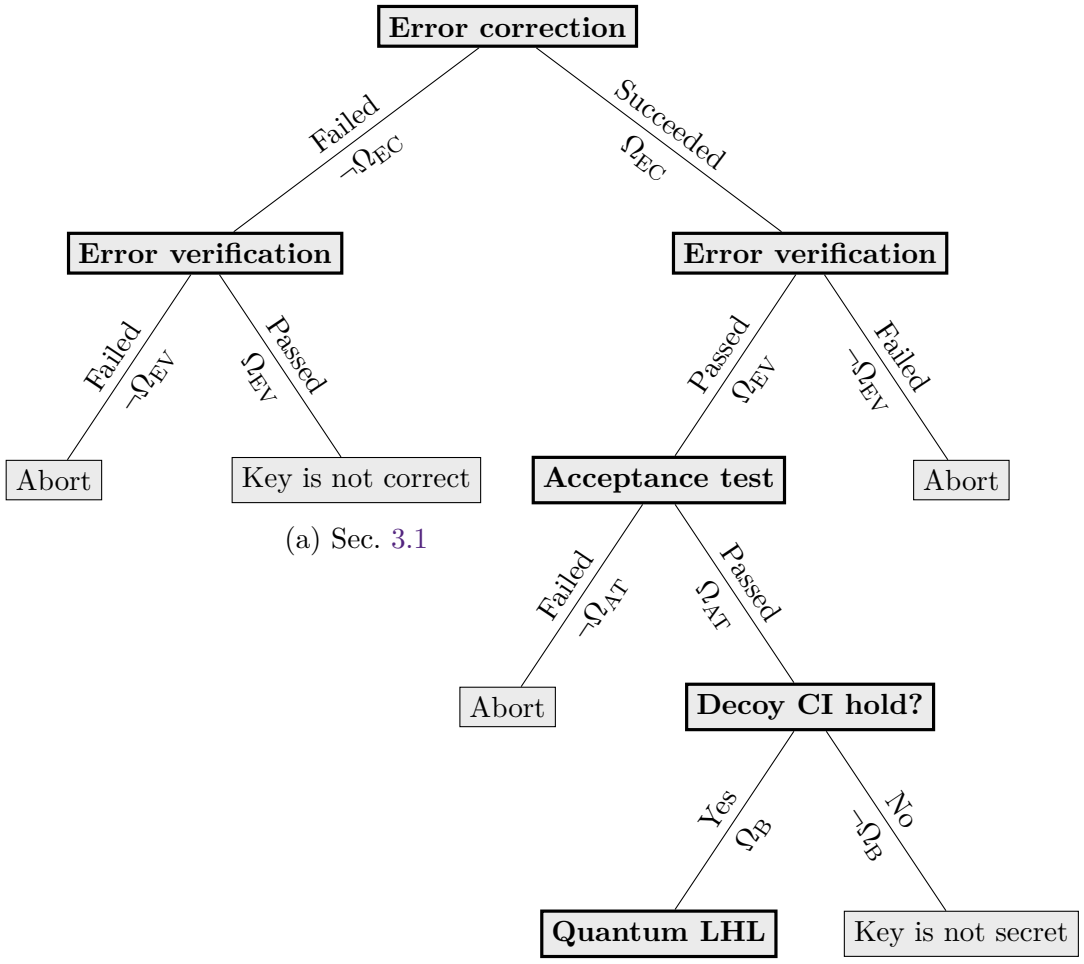


Figure 3: Probability tree diagram representing the different steps of the protocol and conditional bounds on the various events. The branches denoted by (a), (b) and (c) are addressed in separate sections. LHL: leftover hash lemma, CI: concentration inequalities.

Note that, following Eq. (16), we don't need to define a secrecy criterion for Bob. Indeed, if the correctness and secrecy criteria are met, then Bob's key is also necessarily secret. As such, to avoid cluttering the notation, in the following, we use S to describe the secure key when S_A and S_B can be used interchangeably. In the following, we assume an authenticated channel and focus on the

correctness and secrecy parameters as they are usually at the heart of QKD security proofs.

The secrecy criterion states that the product of the probability of not aborting the protocol and the distance to an ideal key is smaller than ϵ_{sec}, where ϵ_{sec} is usually chosen to be small. As an example (inspired by the manner in which security is proven), the secrecy criterion can be interpreted as either the key $\rho_{SEC|\Omega_\top}$ being close to an ideal system $U_S \otimes \rho_{EC|\Omega_\top}$ or the protocol aborting with high probability. For this ideal system, the key is uniformly distributed, $\rho_S = U_S$, and independent of Eve, as we can write the combined quantum system as a tensor product $U_S \otimes \rho_{EC|\Omega_\top}$, meaning that Eve's quantum system does not depend on the secure key. It describes an information-theoretically secure key, where S is uniformly distributed and independent of E, as discussed in Sec. 2.3.1. Stating that a key is close to ideal is not to confuse with an ϵ_{sec}-secret protocol, as it is conditioned on the probability $\Pr[\Omega_\top]$ of the protocol not aborting. The secrecy of a QKD system must be given according to ϵ_{sec} as defined in Def. 3, meaning that the probability for the protocol to pass and for Eve to have significant information about the key is small [77]. This definition takes into accounts attacks where the protocol aborts most of the time but when it passes, Eve is certain to have information about the key. One example is the so-called *swap attack* where Eve intercepts all of Alice's signals, sends random ones to Bob and measures her signals only when the basis choices are published. Most of the time, Bob's error rate will be too high and the protocol will abort, but when Eve gets lucky and the protocol does not abort, she has full information about the key.

Similarly, we note that the correctness parameter describes the correctness of the protocol but not the key itself. As a simple example, consider an error correction algorithm that always outputs two different keys. In this case, the protocol will abort most of the time during error verification, meaning the protocol is ϵ_{cor}-correct, but whenever it does not abort, which inherently occurs with non-zero probability, the keys are not identical. Following this discussion, it is important to emphasize that no claims about the secrecy or correctness of the key can be made when the protocol does not abort. Instead, the security parameters describe the security of *the protocol as a whole*, not the specific instances where it succeeds in producing a non-trivial key. Indeed, intuitively, the security parameters also include the cases where the protocol aborts and the keys are trivially correct and secret, cf. Def. 1. Given that the probability of aborting is unknown, we cannot extend the security claims about the protocol to the non-trivial keys.

The value of ϵ'_{sec} can be freely chosen depending on the practical use case. To give this parameter a more tangible interpretation, assume there exists the following bound on the second term in Eq. (20),

$$d_{\text{sec}}(S_A EC)_{\rho|\Omega_\top \wedge \Omega_{\text{EC}}} \leq \Delta\,. \tag{23}$$

Then the probability for Eve to guess the entirety of the key when the protocol does not abort is upper-bounded by [12, Lemma 11]

$$P_{\text{guess}}(S|EC)_\rho \leq \frac{1}{|\mathcal{S}|} + \epsilon'_{\text{sec}}\,, \tag{24}$$

where $\Delta \leq \epsilon'_{\text{sec}}$. However, any non-trivial bound Δ depends on the probability to abort the protocol, which is under Eve's control. Therefore, we cannot obtain a practical bound on Eq. (23) directly. What we can bound is the second term in Eq. (20), which includes the abort probability. Nevertheless, we can see that the parameter ϵ'_{sec} loosely has an operational meaning in the sense that it describes the deviation from an ideal key for which $P_{\text{guess}}(S|EC)_{U_S \otimes \rho_{EC}} = \frac{1}{|\mathcal{S}|}$ and $|\mathcal{S}| = 2^l$ is the number of possible keys of length l. This intuitive expression can serve as a general guideline to estimate the value of the security parameter ϵ in practical scenarios.

All in all, based on the triangle inequality type arguments discussed above, the security parameter ϵ upper-bounds the probability for at least one of the following events occurring: the protocol did not abort and the key is distinguishable from an ideal key $U_S \otimes \rho_{EC}$, or the protocol did not abort and the keys S_A and S_B are not identical. The main goal of the security proof is to bound all the terms appearing in Fig. 3, i.e. Eq. (20), and derive an expression for the secure-key length l such that the protocol is ϵ-secure by either aborting or generating a key of length l. Deriving an operational

expression for the first term in Eq. (20) is the goal of Sec. 3.1. The second term requires more work, involving the quantum leftover hash lemma and bounding min-entropies, as discussed in Secs. 3.2, 4, 5 and 6.

Remark 7. *An additional parameter, called robustness parameter, is sometimes introduced to quantify the resilience of the protocol or the expected key rate. Indeed, a protocol that consistently aborts is inherently secure but fails to produce a useful output. In fact, a protocol is called* ϵ_{rob}*-robust if, in the absence of an adversary, the probability that the protocol aborts is* $1 - \Pr[\Omega_\top] \leq \epsilon_{\text{rob}}$*, meaning that the protocol outputs a non-trivial key with a probability of at least* $1 - \epsilon_{\text{rob}}$ *[78].*

2.3.4 Conditional bounds expansion

The main goal of the security proof is to ensure that the security criterion, i.e. Def. 1, is fulfilled by the protocol described in Sec. 2.1. To achieve this, concentration inequalities are used to derive bounds on the detection statistics which are used to perform the acceptance test and determine the secure-key length, as will be discussed in Sec. 5. These bounds come with an associated probability of failure, which is not explicitly reflected in the second term in Eq. (20). Recall that we denote Ω_{B} the event where all bounds given by the decoy concentration inequalities hold. To simplify the notation, we define $\tilde{\Omega} \coloneqq \Omega_\top \wedge \Omega_{\text{EC}}$ in the following. We thus reformulate this term in preparation for Sec. 4, by applying the triangle inequality of the trace distance

$$\Pr[\tilde{\Omega}] d_{\text{sec}}(S_A E C)_{\rho|\tilde{\Omega}} \leq \Pr[\tilde{\Omega} \wedge \Omega_{\text{B}}] d_{\text{sec}}(S_A E C)_{\rho|\tilde{\Omega}\wedge\Omega_{\text{B}}} + \Pr[\tilde{\Omega} \wedge \neg\Omega_{\text{B}}]\,, \tag{25}$$

where we have split the terms conditioned on the decoy concentration inequalities holding and failing, represented by the branches (b) and (c), respectively, in Fig. 3. We have used $d_{\text{sec}}(S_A E C)_{\rho|\tilde{\Omega}\wedge\neg\Omega_{\text{B}}} \leq 1$ as no better bound is known when the concentration inequalities do not hold. This reformulation is better suited for the analysis as we can separately bound each term appearing in the above inequality. A bound on the first term in Eq. (25) is provided by the quantum leftover hash lemma and will be tackled in Secs. 4.3 and 4.4. An expression for the probability $\Pr[\tilde{\Omega} \wedge \neg\Omega_{\text{B}}]$ will be derived in Sec. 6.1 in terms of the probability that the concentration inequalities do not hold.

2.3.5 Composable security

QKD protocols are almost always combined with other cryptographic schemes as the mere generation of a secure key is of little interest. Hence, in this scenario, we are interested in describing how the security of the combined system behaves. The security definition in terms of the trace distance inherits an intuitive property from the *universal composability framework* that enables the description of combined systems [8, 12].

Assume, as an example, that the key produced by the QKD protocol is ϵ-secure and used to encrypt a message with an ϵ_{enc}-secure encryption scheme (in the universal composability framework)[17]. This means that the QKD protocol is indistinguishable from an ideal QKD protocol up to a probability ϵ, as discussed in Sec. 2.3.3, and the message encrypted is indistinguishable from a perfect encryption procedure up to a probability ϵ_{enc}. Now, following the properties of universal composability, the combined system is $(\epsilon + \epsilon_{\text{enc}})$-secure and $\epsilon + \epsilon_{\text{enc}}$ upper-bounds the probability of either the key generation or encryption failing. The same applies when concatenating n different ϵ-secure keys, where the resulting key is $n\epsilon$-secure [78].

2.3.6 The one-time pad

As discussed in the previous section, the key produced by a QKD protocol is almost always used as part of other cryptographic schemes. In fact, the key is often used to establish secure communication between two parties. In this case, the message, also known as *plaintext*, is encrypted and transformed

[17] For one-time pad encryption, as described in Sec. 2.3.6, $\epsilon_{\text{enc}} = 0$.

into a *ciphertext*, which can in turn be publicly communicated to a receiver who is also in possession of the key. Making use of its key, the receiver can decrypt the ciphertext and retrieve the plaintext. A straightforward method to achieve this is the so-called *one-time pad*, where the encryption and decryption processes involve performing an XOR-operation $\oplus$ between the key S, the plaintext M and the ciphertext M'. As such, the ciphertext is computed using

$$M' = S \oplus M \tag{26}$$

and can be decrypted by the receiver using the key to retrieve the plaintext,

$$M = S \oplus M' \,. \tag{27}$$

This encryption procedure is perfectly secure, i.e. $\epsilon_{\text{enc}} = 0$, if the key used is secure (cf. Sec 2.3.1) and the following conditions are met [5, 68]:

1. The key has the same length as the plaintext to be encrypted.
2. It is only used once (hence the name one-time pad).

If these conditions are met and the key is generated by an ϵ-secure QKD protocol, as described in Sec. 2.1, then the resulting communications are ϵ-secure. Although mathematically sound, we note that, in practice, the one-time pad is not the preferred encryption scheme as it is expensive in terms of key rates [79].

3 Universal$_2$ hashing

This section serves to introduce *universal$_2$ hashing*, also called *two-universal hashing*, originally presented in Ref. [80], and describe its use during the error verification and privacy amplification steps, cf. Sec. 2.1. In fact, using universal$_2$ hashing, we can compare Alice's and Bob's corrected keys Z_A and Z_B and ensure that they are identical up to a small probability without revealing them. The properties of universal$_2$ hashing directly provide a bound on branch (a) from Fig. 3 and enable the derivation of an operational expression for ϵ_{cor} in Sec. 3.1. Additionally, using a universal$_2$ family of hash functions, the keys are mapped to shorter hashes and, as formalized by the quantum leftover hash lemma, their secrecy regarding an eavesdropper is increased, which is specifically the goal of the privacy amplification step, as discussed in Sec. 3.2 and further developed in Sec. 4.

3.1 Error correction and verification

During the error correction step, leak_{EC} bits are disclosed to Eve over the classical communication channel and stored in C_{EC} in order for Alice to correct her sifted key $\tilde{Z}_A$, cf. Fig. 2. For numerical analyses, this quantity can be approximated by [81]

$$\text{leak}_{\text{EC}} \approx N_{\mathsf{Z}} f_{\text{EC}} h\left(\frac{1}{N_{\mathsf{Z}}}|\tilde{Z}_A \oplus Z_A|\right) , \tag{28}$$

where $f_{\text{EC}} > 1$ is the error correction inefficiency, which depends on the error rate and the correction scheme used[18]. Alice and Bob then possess a corrected key pair Z_A and Z_B.

The aim of the error verification step is to ensure that Alice's and Bob's corrected keys are identical up to a small probability without disclosing them. In fact, if Z_A and Z_B are not identical, the protocol aborts with high probability and $S_A = S_B = \perp$. This corresponds to the first two branches in Fig. 3.

[18] Usually, $f_{\text{EC}} \in [1.05, 1.2]$ [81].

The idea is that instead of comparing Z_A and Z_B directly, we compare $f_y(Z_A)$ and $f_y(Z_B)$ where f_y is a randomly chosen hash function[19], resulting in two possibilities:

$$Z_A = Z_B \Rightarrow f_y(Z_A) = f_y(Z_B)\,, \tag{29}$$
$$Z_A \neq Z_B \Rightarrow \Pr[f_y(Z_A) = f_y(Z_B)] \leq \delta\,, \tag{30}$$

where δ is formally defined in Def. 4. In other words, if $Z_A = Z_B$ we get with certainty $f_y(Z_A) = f_y(Z_B)$ and if $Z_A \neq Z_B$, we observe $f_y(Z_A) \neq f_y(Z_B)$ up to a small probability δ, which correspond to the correctness parameter introduced in Sec. 2.3.3. Additionally, Z_A and Z_B cannot reliably be reconstructed from $f_y(Z_A)$ and $f_y(Z_B)$ as hash functions are chosen to be deterministically random and non-invertible, and leak at maximum the length of the hash in bits. For universal$_2$ hashing, the index 2 denotes the fact that the comparison occurs between two elements and the properties need only to hold for pairs of elements. This is more formally described in the following definition.

Definition 4 (Universal$_2$)**.** *Let $\mathcal{F} = \{f_y\}_y$ be a family of hash functions mapping a set $\mathcal{Z}$ onto a set $\mathcal{S}$, where $|\mathcal{Z}| > |\mathcal{S}|$. $\mathcal{F}$ is called universal$_2$ if for all $z, \tilde{z} \in \mathcal{Z}$ with $z \neq \tilde{z}$, we have $f_y(z) = f_y(\tilde{z})$ for at most a fraction $\delta := 1/|\mathcal{S}|$ of the functions f_y (see Refs. [80] and [83, Sec. 2.1]). In this context, $\mathcal{Z}$ is called the set of possible keys and $\mathcal{S}$ the set of hashes (also called indices in the original work).*

In the following, the term hash of z will be used to describe $f_y(z)$. Using the definition above, we can bound the first term in Eq.(20), i.e. branch (a) in Fig. 3. We recall that Ω_{EC} denotes the event where error correction succeeds, i.e. $Z_A = Z_B$, and Ω_{EV} the error verification passing, i.e. $f_y(Z_A) = f_y(Z_B)$. Following Def. 4, we can state that $\Pr[\Omega_{\mathrm{EV}}|\neg\Omega_{\mathrm{EC}}] \leq \delta$ is bounded. Using Bayes' theorem, this directly bounds branch (a) as $\Pr[\neg\Omega_{\mathrm{EC}} \wedge \Omega_{\mathrm{EV}}] \leq \Pr[\Omega_{\mathrm{EV}}|\neg\Omega_{\mathrm{EC}}]$, cf. Eq. (15). We can thus choose $\delta \leq \epsilon_{\mathrm{cor}}$, cf. Def. 2, as $\Pr[\neg\Omega_{\mathrm{EC}} \wedge \Omega_{\top}] \leq \Pr[\neg\Omega_{\mathrm{EC}} \wedge \Omega_{\mathrm{EV}}] \leq \delta$.

Recalling that $\delta = 1/|\mathcal{S}|$ is defined in terms of the number of possible hash function f_y, we can determine the length c of the hash required for the correctness criterion to hold. Indeed, we note that for a bit string of length c, $|\mathcal{S}| = 2^c$. Thus, in order to fulfill the correctness criterion, we can see that $c \geq \lceil \log_2 1/\epsilon_{\mathrm{cor}} \rceil$ as

$$\boxed{\Pr[\Omega_{\mathrm{EV}} \wedge \neg\Omega_{\mathrm{EC}}] \leq \Pr[\Omega_{\mathrm{EV}} \,|\, \neg\Omega_{\mathrm{EC}}] \leq \delta \leq 2^{-\lceil \log_2 1/\epsilon_{\mathrm{cor}} \rceil} \leq \epsilon_{\mathrm{cor}}\,,} \tag{31}$$

which bounds branch (a) in Fig. 3, i.e. the first term in Eq. (20), and thus fulfills the correctness criterion, cf. Def. 2. Or, by adding one bit to the hash function length to avoid rounding up, $c = \log_2 2/\epsilon_{\mathrm{cor}}$,

$$\Pr[\Omega_{\mathrm{EV}} \,|\, \neg\Omega_{\mathrm{EC}}] \leq 2^{-\log_2 2/\epsilon_{\mathrm{cor}}} = 2^{-1}\epsilon_{\mathrm{cor}} \leq \epsilon_{\mathrm{cor}}\,. \tag{32}$$

It follows that $\log_2 2/\epsilon_{\mathrm{cor}}$ bits are used for the hash function and disclosed to Eve through the classical channel for error verification. We store the choice of hash function as well as the hash of Alice's corrected key in a classical register C_{EV}. Error verification using universal$_2$ hashing thus directly provides a bound on branch (a), i.e. the protocol is ϵ_{cor}-correct, as summarized by Theorem 1. We may now focus on branches (c) and (d), i.e. Eq. (25), which require more work and will be the aim of the following sections.

Theorem 1. *Consider the protocol described in Fig. 2, where a universal$_2$ family of hash functions $\mathcal{F} = \{f_y\}_y$ is used during the error verification step, with $f_y : \mathcal{Z} \to \mathcal{S}$. Then, the protocol is ϵ_{cor}-correct if the length $\log_2 |\mathcal{S}|$ of the hashes is at least $\lceil \log_2 1/\epsilon_{\mathrm{cor}} \rceil$.*

Proof. The proof is given above. □

Remark 8. *Setting $S_A = S_B = \perp$ when the protocol aborts leads to a more general definition for the correctness parameter, namely $\Pr[S_A \neq S_B] \leq \epsilon_{\mathrm{cor}}$ as [48]*

$$\Pr[S_A \neq S_B] = \Pr[S_A \neq S_B \wedge \Omega_{\top}] + \Pr[S_A \neq S_B \wedge \neg\Omega_{\top}] \leq \epsilon_{\mathrm{cor}} \tag{33}$$

[19] An example of widely used hash functions is Toeplitz matrices [82].

where $\Pr[S_A \neq S_B \wedge \Omega_\top] \leq \epsilon_{\text{cor}}$ *and* $\Pr[S_A \neq S_B \wedge \neg\Omega_\top] = 0$ *as upon aborting the protocol, we trivially have* $\Pr[S_A = S_B] = 1$ *since* $S_A = S_B = \perp$*. As discussed in Sec. 2.3.3, we may however not make any claims about the correctness of the key when conditioning on the protocol not aborting.*

3.2 Privacy amplification

Another application of universal$_2$ hashing is privacy amplification. As perfect security can never be ensured, we introduced the definition of security in Sec. 2.3, which allows us to quantified how close the key output is from a perfectly secure key. By performing privacy amplification, a key arbitrarily close to a perfectly secure key can be produced. In fact, the privacy amplification step is performed by taking the verified key Z and a hash function f_y chosen at random following a uniform distribution U_Y from a universal$_2$ family of hash functions[20], in order to produce a secure key S of length l which is shorter than Z and (ideally) independent of E. The systems Z and S represent classical distributions and can hence be represented using Eq. (6).

Let $\mathcal{F} = \{f_y\}_y$ be a universal$_2$ family of hash functions from $\mathcal{Z}$ to $\mathcal{S}$, as defined in Def. 4, describing the privacy amplification step. The output string is given by [24]

$$S = f_Y(Z) = \sum_{f_y \in \mathcal{F}} U_Y(f_y) f_y(Z)\,, \tag{34}$$

where $l = |S| < |Z| = N_{\mathsf{Z}}$ and the hash function f_y is chosen uniformly at random from $\mathcal{F}$. Alice (or Bob) publicly communicates her choice of hash function to Bob (Alice) and both compute the hash of their verified key using the same hash function. The choice of hash function should not be disclosed before Bob has received all signals from Alice. It can be shown that for the resulting key S, ϵ'_{sec} exponentially decreases with the length difference $N_{\mathsf{Z}} - l$, meaning that virtually any ϵ'_{sec} can be chosen if the length N_{Z} of the verified key is long enough and the length l of the secure key is short enough[21] [83, Sec. 4.1]. This relation is given by the *quantum leftover hash lemma*, linking the extractable secure-key length to ϵ'_{sec}, which we introduce and discuss in the next section in order to bound branch (b) in Fig. 3.

4 The quantum leftover hash lemma

In Sec. 2.3, we have defined the security of the protocol and expanded it by conditioning on various events and applying the triangle inequality to obtain Eq. (20), which we recall to be

$$d_{\text{sec}}(S_A S_B EC)_\rho \leq \Pr[\neg\Omega_{\text{EC}} \wedge \Omega_{\text{EV}}] + \Pr[\Omega_\top \wedge \Omega_{\text{EC}}] d_{\text{sec}}(S_A EC)_{\rho|\Omega_\top \wedge \Omega_{\text{EC}}} \leq \epsilon\,, \tag{35}$$

where we have bound the first term with ϵ_{cor} in Sec. 3.1. We now focus on the second term. Therefore, in the following sections, we assume that the keys have already passed all steps in the protocol, as described in Fig. 2, up to but not including privacy amplification.

We consider the event $\Omega_\top \wedge \Omega_{\text{EC}}$. Alice and Bob thus possess a verified key pair Z_A and Z_B of length N_Z which is correct but still potentially strongly correlated with Eve. This means that Eve potentially holds substantial information about their keys. The goal of the privacy amplification step is to produce a key that is ideally independent of Eve, i.e. fulfilling the secrecy criterion, as discussed in Sec. 3.2. In this section, we use Z to describe Z_A and Z_B interchangeably as we condition on the error correction succeeding, i.e. Z_A and Z_B are identical. We have further expanded the above expression in Sec. 2.3.4 in terms of the decoy concentration inequalities holding and failing (Eq. (25)) to obtain

$$\Pr[\tilde{\Omega}] d_{\text{sec}}(SEC)_{\rho|\tilde{\Omega}} \leq \Pr[\tilde{\Omega} \wedge \Omega_{\text{B}}] d_{\text{sec}}(SEC)_{\rho|\tilde{\Omega} \wedge \Omega_{\text{B}}} + \Pr[\tilde{\Omega} \wedge \neg\Omega_{\text{B}}]\,, \tag{36}$$

[20] A more general definition of universal$_2$ hashing exists that does not require keys to be chosen uniformly at random. However, in this work we assume uniformity, as it is the most common approach in practical implementations.

[21] Note, however, that l needs to be finite and positive for key generation. Thus, one cannot increase $N_{\mathsf{Z}} - l$ arbitrarily.

where we recall that $\tilde{\Omega} = \Omega_\top \wedge \Omega_{\mathrm{EC}} = \Omega_{\mathrm{AT}} \wedge \Omega_{\mathrm{EV}} \wedge \Omega_{\mathrm{EC}}$, cf. Table 2. The quantum leftover hash lemma in fact provides a bound on $d_{\mathrm{sec}}(SEC)_{\rho|\tilde{\Omega}\wedge\Omega_{\mathrm{B}}}$, conditioned on the decoy concentration inequalities holding, in terms of the secure-key length and will thus be the focus of this section. This term corresponds to branch (b) in Fig. 3. The term corresponding to the concentration inequalities not holding, i.e. the second term in Eq. (36) (branch (c)), will be tackled in Sec. 6.1.

First, the min-entropy will be introduced in Secs. 4.1 and 4.2 as a conservative way to describe Eve's uncertainty about the sifted key. The quantum leftover hash lemma will then formally be introduced in Sec. 4.3, relating ϵ'_{sec} to the min-entropy and the secure-key length. A bound on the min-entropy is finally derived in terms of the numbers of photon events and errors in Sec. 4.4 by applying the chain rule for smooth min-entropies and using the entropic uncertainty relation.

4.1 Eve's guessing probability and the min-entropy

The *von Neumann entropy* $S(\rho)$ of a quantum system ρ is a measure for the average uncertainty of an observer about the system [50]. It constitutes a generalization of the Shannon entropy from classical information theory and is defined as

$$S(\rho) = -\operatorname{Tr}\{\rho \log_2 \rho\}\,. \tag{37}$$

Using the spectral decomposition of ρ, the von Neumann entropy can be rewritten equivalently to the Shannon entropy as

$$S(\rho) = -\sum_z p_z \log_2 p_z\,, \tag{38}$$

where p_z are the eigenvalues of ρ. The von Neumann entropy is bounded by (for a proof, see Ref. [50, Sec. 5.1])

$$0 \leq S(\rho) \leq \log_2 \dim \mathcal{H} \tag{39}$$

and is maximal when considering a uniform distribution $\{p_x\}_x$ as it constitutes the case of maximum uncertainty. In fact, in this case, $\rho = \frac{1}{\dim \mathcal{H}} I$ and $S(\rho) = \log_2 \dim \mathcal{H}$, where I is the identity matrix acting on $\mathcal{H}$. For example, in the case of l uniformly distributed qubits, $\dim \mathcal{H} = 2^l$ and $S(\rho) = l$.

When working in the realm of cryptography, the worst case scenario is typically considered and thus a more conservative entropy measure is introduced. In contrast to the von Neumann entropy, the *min-entropy* does not consider the average uncertainty of an adversary Eve, but her best possible attack strategy and quantifies the entropy in the case where her uncertainty is minimal and she is the most likely to guess the secure key [28, Sec. I.B]. Formally, the min-entropy of A conditioned on B of the state σ_{AB} is defined as [63, Def. 6.2]

$$H_{\min}(A|B)_\sigma = \sup_{\tau_B \in S_\leq(\mathcal{H}_B)} \sup\{\lambda \in \mathbb{R} : \sigma_{AB} \leq \exp(-\lambda) I_A \otimes \tau_B\}\,, \tag{40}$$

where I_A is the identity matrix acting on A ($\mathcal{H}_A$) and $S_\leq(\mathcal{H}_B)$ is the set of positive semi-definite matrices of trace less or equal to one acting on $\mathcal{H}_B$. When A is a classical register, the min-entropy has an operational interpretation in terms of the maximum guessing probability as follows.

Let C' denote a generic classical register storing classical communications. In the case where $\rho_{ZEC'}$ describes potentially correlated systems Z (describing the verified key) and EC', the min-entropy given side information E and C' is defined as

$$H_{\min}(Z|EC')_\rho = -\log_2 p_{\mathrm{guess}}(Z|EC')_\rho\,, \tag{41}$$

where $p_{\mathrm{guess}}(Z|EC')_\rho$ denotes Eve's maximum probability of guessing the key Z given her side information EC' (p_{guess} is formally defined in Ref. [84, Theorem 1]). A concrete comparison between the von Neumann and min-entropy can be found in App. A.4. In the following, we use the notation $H_{\min}(Z|EC')_\rho = H_{\min}(\rho_{Z|EC'})$. The notation $f(A|B)$ describes $f(A)$ given side information B. In the case of $H_{\min}(Z|EC')_\rho$, it is assumed that Eve has all information about the classical communications C' and she possesses the information E she gathered during the key distribution. As such, $H_{\min}(Z|EC')_\rho$ describes her uncertainty about Z with access to side information EC'.

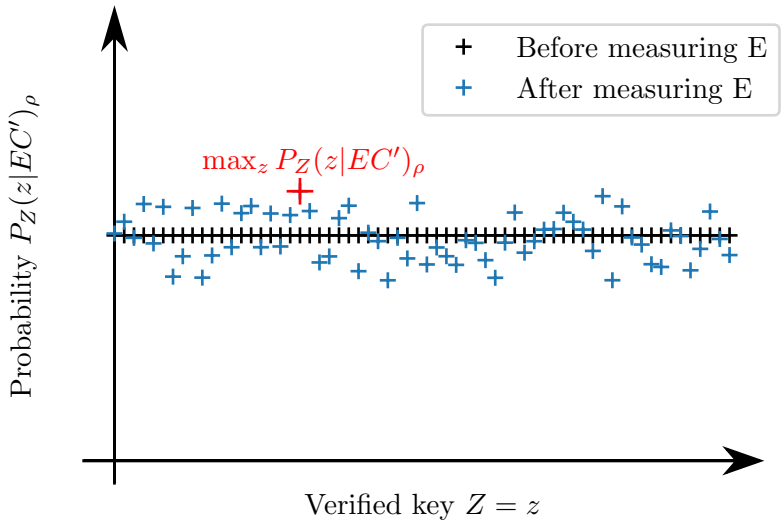


Figure 4: Illustration of the probability distribution of the verified key Z before and after Eve measures her quantum system, where the keys are originally uniformly distributed but correlated with Eve. The correlation translates into the probability distribution being affected by the measurement outcome, leading to some keys being more or less likely given Eve's perspective. Here, the abscissa represents all possible 6-bit verified keys in an arbitrary order.

Remark 9. *An illustrative example for Eve's guessing probability is given in the following. Assume that the verified keys Z are uniformly distributed but correlated with Eve. Then, for each measurement on her system E, the outcome influences her perspective of the distribution of the verified keys as she acquires information about Z. As such, from her point of view, some keys become more or less likely given that she measured a particular outcome. For a visual representation of how the verified key distribution changes from her perspective after performing a measurement on her system, see Fig. 4. Assuming perfect state preparation, before measuring E, Z is a uniform distribution of all possible keys. After measuring E, the probability distribution of the keys is altered as she is able to make certain predictions about the verified key given the measurement outcome. If Eve's quantum system is not correlated with Z, then any measurement on her system yields an outcome that does not give her any information about Z and the verified key distribution remains uniform from her perspective. The min-entropy assumes the worst case scenario where Eve picks the key that, in her perspective, has the highest probability of being generated, as marked by a red cross in Fig. 4. The maximum probability of guessing the key, cf. Eq. (41), is then given by the probability of generating the most probable key (from Eve's perspective).*

Hence, the min-entropy is a conservative measure of entropy as it considers the worst case scenario where Eve performs the best possible attack and has the highest probability of guessing Z while the von Neumann entropy describes the average uncertainty about the system. Using the bounds from Eq. (39) we find

$$0 \leq H_{\min}(\rho) \leq S(\rho) \leq \log_2 \dim \mathcal{H}\,, \tag{42}$$

where the maximum is attained for both entropy measures if ρ is a uniform distribution and is not correlated with another system.

Example 2. *If Z and EC' are uncorrelated, then $P_{\text{guess}}(Z|EC')_\rho = \max_z P_Z(z)$ does not depend on Eve's measurement outcome or strategy. Hence, $H_{\min}(Z|EC')_\rho = -\log_2 \max_z P_Z(z)$, following Eq. (41). In the case of l uniformly distributed qubits, $H_{\min}(Z|EC')_\rho = -\log_2 2^{-l} = l$, which is the length of the verified key and corresponds to the maximum uncertainty. In this situation, the entirety of the verified key is already secret. Note, that this is never the case when considering finite-size effects, cf. Sec. 5.*

4.2 The smooth min-entropy

The *smooth min-entropy* is a more optimal measure of entropy than the min-entropy, leading to greater secure-key lengths as it maximizes the min-entropy $H_{\min}(\rho)$ over all states $\bar{\rho}$ that are ζ-close to ρ in terms of a distance measure called the purified distance [64, Secs. 3.1 and 5.2][22]. More formally, it is evaluated at ρ by maximizing $H_{\min}(\bar{\rho})$ over all $\bar{\rho} \in \mathcal{B}^{\zeta}(\rho)$ where $\mathcal{B}^{\zeta}(\rho)$ is a set of density operators ζ-close to ρ, also called ζ-ball, such that

$$\mathcal{B}^{\zeta}(\rho) \coloneqq \{\sigma \in S_{\leq}(\mathcal{H}) : P(\sigma, \rho) \leq \zeta\}\,, \tag{43}$$

where [63, Def. 3.15]

$$P(\sigma, \rho) \coloneqq \sqrt{1 - \left(\mathrm{Tr}\{|\sqrt{\sigma}\sqrt{\rho}|\} + \sqrt{(1 - \mathrm{Tr}\{\rho\})(1 - \mathrm{Tr}\{\sigma\})}\right)_1^2} \tag{44}$$

is the purified distance. Here, a new distance measure, the *purified distance*, is introduced as a more optimal metric to define ζ-balls. In fact, $P(\sigma, \rho)$ represents the minimum trace distance between purifications of σ and ρ (see Refs. [63, Sec. 3.4] and [85, Def. 4]). The definition of the smooth entropies in terms of the purified distance is applied to derive the duality relation between smooth min- and max-entropies [85], which is in turn used for the uncertainty relation for smooth entropies [42], cf. Sec. 4.4.3. For a more detailed discussion about the purified distance, we refer to Ref. [64]. The purified distance inherits the same interpretation as the trace distance as distinguishing advantage [64, Sec. 3.2.3].

As such, for some $0 \leq \zeta < 1$, also called *smoothing parameter*[23], the smooth min-entropy of Z, given Eve's side information E and C', is defined as

$$H_{\min}^{\zeta}(Z|EC')_{\rho} \coloneqq \max_{\bar{\rho}_{ZEC'} \in \mathcal{B}^{\zeta}(\rho_{ZEC'})} H_{\min}(Z|EC')_{\bar{\rho}}\,. \tag{45}$$

Intuitively, a small error probability ζ that $\bar{\rho}_{SEC'}$ can be distinguished from $\rho_{SEC'}$ is tolerated in return for optimizing the min-entropy over an ζ-ball around $\rho_{SEC'}$. Intuitively, this can be done as two ζ-close states cannot be distinguished with a probability greater than ζ, meaning that for small ζ, both states are effectively indistinguishable (see Sec. 2.2). This optimization can lead to a much greater secure-key length than the non-smoothed min-entropy would allow. It should be noted that this does not weaken the protocol security in any way because the smoothing parameter is taken into account in ϵ'_{sec}. In a sense, a part of ϵ'_{sec} is used to optimize the smooth min-entropy over an ζ-ball around $\rho_{ZEC'}$. Indeed, in Sec. 4.3 it will be seen that the term 2ζ will appear in ϵ'_{sec} due to this optimization. Note that if no error is tolerated, then $\zeta = 0$ and the smooth and non-smoothed versions of the min-entropy coincide:

$$H_{\min}^{\zeta=0}(Z|EC')_{\rho} = H_{\min}(Z|EC')_{\rho}\,. \tag{46}$$

Now that we have formally introduced the smooth min-entropy, we can state and use the quantum leftover hash lemma in the next section to bound branch (b), i.e. the first term in Eq. (25).

Remark 10. *Often, a subindex ρ is introduced, such that $H_{\min}(Z|EC')_{\rho}$ describes Eve's uncertainty given access to side information E and C'. In this context, the subindex represents the state the entropy is evaluated at.*

[22] Indeed, the min-entropy, as defined in Eq. (41), can significantly change from small modifications of the system's state. The smoothed version of the min-entropy resolves this issue.

[23] Technically, the smoothing parameter of the smooth min-entropy evaluated for a state ρ lies in $[0, \sqrt{\mathrm{Tr}\{\rho\}})$. Throughout this work we typically have $\mathrm{Tr}\{\rho\} = 1$, but this becomes relevant when considering sub-normalized conditional states, such as in Eq. (53).

4.3 The quantum leftover hash lemma

We recall that in order to fulfill the security criterion, we require a bound on Eq. (11), which we expanded in terms of various events, as illustrated in Fig. 3. We have bounded branch (a) in Sec. 3.1 using the properties of universal$_2$ hash functions. In Sec. 2.3.4, we have further expanded in terms of the decoy concentration inequalities holding and failing, which corresponds to branches (b) and (c), respectively. Branch (c) will be tackled in Sec. 6.1. The quantum leftover hash lemma provides a bound on branch (b), i.e. the first term in Eq. (25), in terms of the secure-key length and the smooth min-entropy introduced in the last section.

We recall that the quantum state in branch (b) is conditioned on $\tilde{\Omega} \wedge \Omega_{\mathrm{B}}$. However, in Sec. 4.4.3, we will see that we cannot directly bound the min-entropy of such state when applying the entropic uncertainty relation[24]. To avoid this issue, we define $\Omega_\circ$ as the event where the true values of the observed statistics fulfill the acceptance condition, i.e. they are in the acceptance set, cf. Table 1. This event is not something we observe in the protocol, but is nevertheless required in the theoretical security proof. By definition, if the event $\Omega_{\mathrm{AT}} \wedge \Omega_{\mathrm{EC}} \wedge \Omega_{\mathrm{B}}$ is true, then $\Omega_\circ$ is also true, i.e. we can write

$$\Omega_{\mathrm{AT}} \wedge \Omega_{\mathrm{EC}} \wedge \Omega_{\mathrm{B}} \Rightarrow \Omega_\circ \,, \tag{47}$$

cf. Table 2. Using this, we show below that the bounds derived for states conditioned on $\Omega_\circ$ also hold for states conditioned on $\tilde{\Omega} \wedge \Omega_{\mathrm{B}}$ and we can thus bound branch (b). For now, however, we assume a conditioning on $\Omega_\circ$.

Assuming that a universal$_2$ family of hash functions is used in the privacy amplification step to extract a key S from Z, cf. Sec. 3.2, the quantum leftover hash lemma [35, App. B] [24, Corollary 5.6.1] provides an upper bound on the distance of the real key to an ideal key in terms of the secure-key length l and Eve's uncertainty about the key,

$$\boxed{d_{\mathrm{sec}}(SEC)_{\rho|\Omega_\circ} \leq 2\zeta + \frac{1}{2}\sqrt{2^{l - H_{\min}^{\zeta}\left(Z \,|\, E\tilde{C}^N C_{\mathrm{EC}} C_{\mathrm{EV}} C_{\mathrm{AT}}\right)_{\rho|\Omega_\circ}}} \,,} \tag{48}$$

where $d_{\mathrm{sec}}(SEC)_{\rho|\Omega_\circ}$ is defined in Eq. (13), with $0 \leq \zeta < 1$ and we recall that $C = \tilde{C}^N C_{\mathrm{EC}} C_{\mathrm{EV}} C_{\mathrm{AT}} C_{\mathrm{PA}}$, cf. Table 3. Notice that the choice of hash function for privacy amplification, stored in C_{PA}, does not appear on the right-hand side of the equation above. This can be written as

$$d_{\mathrm{sec}}(SEC)_{\rho|\Omega_\circ} \leq 2\zeta + \Delta_{\mathrm{pa}}^{\zeta} =: \Delta_{\mathrm{pa}} \,, \tag{49}$$

where we define

$$\Delta_{\mathrm{pa}}^{\zeta} := \frac{1}{2}\sqrt{2^{l - H_{\min}^{\zeta}\left(Z \,|\, E\tilde{C}^N C_{\mathrm{EC}} C_{\mathrm{EV}} C_{\mathrm{AT}}\right)_{\rho|\Omega_\circ}}} \,. \tag{50}$$

The term 2ζ results from the fact that the smooth min-entropy is optimized on a ζ-ball around $\rho_{ZE\tilde{C}^N C_{\mathrm{EC}} C_{\mathrm{EV}} C_{\mathrm{AT}}|\Omega_\circ}$ where an error 2ζ is tolerated. Indeed, in addition to $\Delta_{\mathrm{pa}}^{\zeta}$ which directly results from the privacy amplification, we have a contribution 2ζ due to the fact that $\rho_{ZE\tilde{C}^N C_{\mathrm{EC}} C_{\mathrm{EV}} C_{\mathrm{AT}}|\Omega_\circ}$ and $\bar{\rho}_{ZE\tilde{C}^N C_{\mathrm{EC}} C_{\mathrm{EV}} C_{\mathrm{AT}}|\Omega_\circ} \in \mathcal{B}^{\zeta}(\rho_{ZE\tilde{C}^N C_{\mathrm{EC}} C_{\mathrm{EV}} C_{\mathrm{AT}}|\Omega_\circ})$ are not perfectly indistinguishable, as discussed in Sec. 4.2. If we set $\zeta = 0$, the min-entropy without smoothing is used.

We consider two cases in the following. First, assume that $\zeta < \mathrm{Tr}\left\{(\rho_{ZEC|\Omega_\circ})_{\wedge\tilde{\Omega}\wedge\Omega_{\mathrm{B}}}\right\}$, where the normalized ($\Omega_\circ$) and sub-normalized ($\tilde{\Omega} \wedge \Omega_{\mathrm{B}}$) conditioning are used, as introduced in Sec. 2.2.3. We now show that applying the quantum leftover hash lemma for states conditioned on $\Omega_\circ$ also provides a bound for states conditioned on $\tilde{\Omega} \wedge \Omega_{\mathrm{B}}$, which is required to bound branch (b), i.e. the first term in

[24] As discussed in Sec. 4.4.3, this has to do with the subtle point that we cannot condition on $\Omega_{\mathrm{AT}}, \Omega_{\mathrm{EC}}$ nor Ω_{EV} while using the EUR because those events are not well-defined for certain states that show up in the EUR statement.

Eq. (25). To see this, we can write

$$\Pr[\tilde{\Omega}\wedge\Omega_{\mathrm{B}}]d_{\mathrm{sec}}(SEC)_{\rho|\tilde{\Omega}\wedge\Omega_{\mathrm{B}}} = \Pr[\tilde{\Omega}\wedge\Omega_{\mathrm{B}}\wedge\Omega_{\circ}]d_{\mathrm{sec}}(SEC)_{\rho|\tilde{\Omega}\wedge\Omega_{\mathrm{B}}\wedge\Omega_{\circ}} \tag{51}$$

$$= \Pr[\Omega_{\circ}]d_{\mathrm{sec}}(SEC)_{(\rho|\Omega_{\circ})\wedge\tilde{\Omega}\wedge\Omega_{\mathrm{B}}} \tag{52}$$

$$\leq \Pr[\Omega_{\circ}]\left(2\zeta+\frac{1}{2}\sqrt{2^{l-H_{\min}^{\zeta}\left(Z\,|\,E\tilde{C}^{N}C_{\mathrm{EC}}C_{\mathrm{EV}}\right)_{(\rho|\Omega_{\circ})\wedge\tilde{\Omega}\wedge\Omega_{\mathrm{B}}}}}\right), \tag{53}$$

where we used $\Pr[\tilde{\Omega}\wedge\Omega_{\mathrm{B}}\wedge\neg\Omega_{\circ}]=0$ for the first equality, as, by definition, $\Omega_{\circ}$ follows from $\tilde{\Omega}\wedge\Omega_{\mathrm{B}}$, and we substituted the quantum leftover hash lemma, i.e. Eq. (48), in the last inequality. We also removed the register C_{AT} in the last step as we condition on the protocol not aborting, i.e. $\Omega_{\top}$, such that C_{AT} takes a fixed value. We may now use $H_{\min}^{\zeta}(A)_{\rho\wedge\Omega}\geq H_{\min}^{\zeta}(A)_{\rho}$ [35, Lemma 10] to find an upper bound on the above inequality without the event $\tilde{\Omega}\wedge\Omega_{\mathrm{B}}$, yielding Eq. (57) in Lemma 1.

On the other hand, if $\zeta\geq\mathrm{Tr}\left\{(\rho_{ZEC|\Omega_{\circ}})_{\wedge\tilde{\Omega}\wedge\Omega_{\mathrm{B}}}\right\}$, then ζ cannot be used as smoothing parameter, cf. Footnote 23. Fortunately, in this case we can bound Eq. (52) without the use of the quantum leftover hash lemma. First, we note that the ideal state can be written as the result of applying a CPTP map $\mathcal{E}$ on the real output such that

$$\mathcal{E}\left((\rho_{SEC|\Omega_{\circ}})_{\wedge\tilde{\Omega}\wedge\Omega_{\mathrm{B}}}\right)=U_S\otimes(\rho_{EC|\Omega_{\circ}})_{\wedge\tilde{\Omega}\wedge\Omega_{\mathrm{B}}}\,, \tag{54}$$

by replacing the key register with a perfect key. Additionally, the trace distance between two states ρ and σ is bounded by $(\mathrm{Tr}\{\rho\}+\mathrm{Tr}\{\sigma\})/2$ via the triangle inequality [51, Sec. 9.2]. Finally, we can write

$$\mathrm{Tr}\left\{(\rho_{ZEC|\Omega_{\circ}})_{\wedge\tilde{\Omega}\wedge\Omega_{\mathrm{B}}}\right\}=\mathrm{Tr}\left\{(\rho_{SEC|\Omega_{\circ}})_{\wedge\tilde{\Omega}\wedge\Omega_{\mathrm{B}}}\right\}=\mathrm{Tr}\left\{\mathcal{E}\left((\rho_{SEC|\Omega_{\circ}})_{\wedge\tilde{\Omega}\wedge\Omega_{\mathrm{B}}}\right)\right\}\leq\zeta\,, \tag{55}$$

for any map from Z to S. Putting the arguments together yields an upper bound on Eq. (52) without using the quantum leftover hash lemma,

$$d_{\mathrm{sec}}(SEC)_{(\rho|\Omega_{\circ})\wedge\tilde{\Omega}\wedge\Omega_{\mathrm{B}}}=\frac{1}{2}\left\|(\rho_{SEC|\Omega_{\circ}})_{\wedge\tilde{\Omega}\wedge\Omega_{\mathrm{B}}}-\mathcal{E}\left((\rho_{SEC|\Omega_{\circ}})_{\wedge\tilde{\Omega}\wedge\Omega_{\mathrm{B}}}\right)\right\|_1\leq\zeta\,. \tag{56}$$

We emphasize that this bound holds for any map from Z and S. In particular, if a privacy amplification step is performed to map Z to a key S of length l using a universal$_2$ family of hash functions, as done in the protocol described in Fig. 2, the bound still holds. We also observe that $\Pr[\Omega_{\circ}]\zeta$ is a lower bound on Eq. (53), which results from using the quantum leftover hash lemma in the first case considered. Therefore, we may restrict our attention to the first case as the bounds on the security parameters subsequently derived apply to both cases.

In the following sections, we derive an operational expression for the min-entropy appearing in Eq. (57) by using the chain rule for smooth min-entropies and the entropic uncertainty relation.

Lemma 1. *Let ρ_{SEC} be the state describing Eve and Alice's key S after privacy amplification, i.e. resulting from applying a randomly chosen hash function on her verified key Z, for the protocol described in Fig. 2. Let $\tilde{\Omega}$ denote the event that the protocol does not abort and error correction succeeds, and Ω_B denote the event that the decoy bounds hold, cf. Table 2. Finally, let $0\leq\zeta<1$. If $\zeta<\mathrm{Tr}\left\{(\rho_{ZEC|\Omega_{\circ}})_{\wedge\tilde{\Omega}\wedge\Omega_{\mathrm{B}}}\right\}$, then*

$$\boxed{\Pr[\tilde{\Omega}\wedge\Omega_{\mathrm{B}}]d_{\mathrm{sec}}(SEC)_{\rho|\tilde{\Omega}\wedge\Omega_{\mathrm{B}}}\leq\Pr[\Omega_{\circ}]\left(2\zeta+\frac{1}{2}\sqrt{2^{l-H_{\min}^{\zeta}\left(Z\,|\,E\tilde{C}^{N}C_{\mathrm{EC}}C_{\mathrm{EV}}\right)_{\rho|\Omega_{\circ}}}}\right),}\tag{57}$$

where $\Omega_{\circ}$ is defined as the event where the true values of the observed statistics fulfill the acceptance condition, cf. Eq. (47), and the classical registers are listed in Table 3. On the other hand, if $\zeta\geq\mathrm{Tr}\left\{(\rho_{ZEC|\Omega_{\circ}})_{\wedge\tilde{\Omega}\wedge\Omega_{\mathrm{B}}}\right\}$, then

$$\Pr[\tilde{\Omega}\wedge\Omega_{\mathrm{B}}]d_{\mathrm{sec}}(SEC)_{\rho|\tilde{\Omega}\wedge\Omega_{\mathrm{B}}}\leq\Pr[\Omega_{\circ}]\zeta\,. \tag{58}$$

Proof. The proof is given above. □

Remark 11. *It is also possible to minimize* Δ_{pa} *for a given secure-key length* l *by optimizing* ζ*, resulting in [36, Eq. (S2)]*

$$\Delta_{\mathrm{pa}} = \min_{\zeta} \left\{ 2\zeta + \Delta_{\mathrm{pa}}^{\zeta} \right\}. \tag{59}$$

However, in the following, we consider the case where Δ_{pa} *has a predefined upper bound and we are interested in determining the extractable secure-key length* l *as it is usually the case considered.*

4.4 Expanding the smooth min-entropy

The quantum leftover hash lemma, cf. Eq. (57), relates the secure-key length and the smooth min-entropy to ϵ'_{sec} through Eq. (25). The aim of this section is to expand the smooth min-entropy in terms of operational parameters, namely the acceptance bounds on the number of photon events and errors, cf. Sec. 2.1.2 and Table 1.

In fact, in the decoy-state protocol, a weak coherent photon source, which either emits multiple photons, one photon or no photon, following the Poisson distribution, is usually used (as will be discussed in Sec. 5.1). The number of m-photon events detected by Bob in the Z-basis is represented by $s_{\mathsf{Z},m}$ and the number of errors, due to experimental limitations or the presence of an eavesdropper, represented by $c_{\mathsf{Z},m}$. These quantities are formally defined in Sec. 5.1. Note that Bob obviously cannot determine these quantities experimentally as, following a detector click, the photon number remains unknown. However, using the decoy-state method, i.e. suitable concentration inequalities, we can estimate the amount of occurrences and derive bounds on the number of photon events and errors, namely $s^{-}_{\mathsf{Z},0}$, $s^{-}_{\mathsf{Z},1}$, $s^{-}_{\mathsf{X},1}$ and Λ^{+}_{X}. This will be the aim of Sec. 5. In this section, we assume that $\Omega_{\circ}$ is true, which, by definition, implies that $s_{\mathsf{Z},0} \geq s^{\mathrm{l}}_{\mathsf{Z},0}$, $s_{\mathsf{Z},1} \geq s^{\mathrm{l}}_{\mathsf{Z},1}$, $s_{\mathsf{X},1} \geq s^{\mathrm{l}}_{\mathsf{X},1}$ and $\Lambda_{\mathsf{X}} \leq \Lambda^{\mathrm{u}}_{\mathsf{X}}$ hold. Throughout this work, we use superscripts $+$ and $-$ to denote decoy bounds and superscripts u and l to denote the acceptance bounds defining the conditions in the acceptance set Q, cf. Table 1 and Remark 1.

4.4.1 Chain rule for smooth min-entropies

First, we recall that C_{EV} stores the hash of Alice's corrected key as well as her choice of hash function for error verification, which we denote C'_{EV} and C''_{EV} respectively, such that $C_{\mathrm{EV}} = C'_{\mathrm{EV}}C''_{\mathrm{EV}}$. We can now use the fact that the choice of hash function is not correlated to the corrected key Z, as it is chosen randomly and independently of Z, in order to remove the register C''_{EV} from the min-entropy appearing in Eq. (57), yielding [63, Theorem 6.2]

$$H^{\zeta}_{\min}(Z|E\tilde{C}^{N}C_{\mathrm{EC}}C'_{\mathrm{EV}}C''_{\mathrm{EV}})_{\rho|\Omega_{\circ}} = H^{\zeta}_{\min}(Z|E\tilde{C}^{N}C_{\mathrm{EC}}C'_{\mathrm{EV}})_{\rho|\Omega_{\circ}}. \tag{60}$$

Then, we can rewrite the min-entropy from the equation above in terms of the bits leaked during error correction and error verification, stored in C_{EC} and C'_{EV} respectively, by using the chain rule for smooth min-entropies (see Refs. [24, Theorem 3.2.12] and [36])

$$H^{\zeta}_{\min}(Z|E\tilde{C}^{N}C_{\mathrm{EC}}C'_{\mathrm{EV}})_{\rho|\Omega_{\circ}} \geq H^{\zeta}_{\min}(Z|E\tilde{C}^{N})_{\rho|\Omega_{\circ}} - \log_2 |C_{\mathrm{EC}}C'_{\mathrm{EV}}|, \tag{61}$$

where $\log_2 |C_{\mathrm{EC}}C'_{\mathrm{EV}}| = \mathrm{leak}_{\mathrm{EC}} + \log_2 \frac{2}{\epsilon_{\mathrm{cor}}}$ describes the classical communications and corresponds to the number of bits disclosed during error correction and error verification, cf. Sec. 3.1.

Remark 12. *Intuitively, Eve's uncertainty about the sifted key* Z *decreases during the protocol as she intercepts the bits disclosed through the classical channel during the error correction and error verification steps. Inequality (61) states that her uncertainty cannot decrease by more than the number of bits disclosed during these steps, i.e.* $\log_2 |C_{\mathrm{EC}}C'_{\mathrm{EV}}|$.

Now, $Z = Z_\mathrm{v} Z_\mathrm{s} Z_\mathrm{m}$ can be split into three subsystems, i.e. the vacuum, single-photon and multi-photon events Z_v, Z_s and Z_m respectively. Here, an m-photon event is defined as Alice sending m photons and Bob registering at least one click. Therefore, for example, a vacuum event may occur if Alice prepared a vacuum state but Bob nevertheless registered a click due to dark counts. Note that the number of rounds in Z_v and Z_s is given by $s_{\mathsf{Z},0} = |Z_\mathrm{v}|$ and $s_{\mathsf{Z},1} = |Z_\mathrm{s}|$ respectively, and is a random variable. However, since we condition on the event $\Omega_\circ$, we are guaranteed that $s_{\mathsf{Z},0} \geq s^\mathrm{l}_{\mathsf{Z},0}$ and $s_{\mathsf{Z},1} \geq s^\mathrm{l}_{\mathsf{Z},1}$ where $s^\mathrm{l}_{\mathsf{Z},0}$ and $s^\mathrm{l}_{\mathsf{Z},1}$ have fixed values that determine the accept conditions. We use this below.

Multi-photon events are entirely unsafe due to being prone to photon number splitting attacks, i.e. Eve has no uncertainty about multi-photon events. As such, we can remove the classical register Z_m using [63, Lemma 6.17], yielding

$$H^\zeta_\mathrm{min}(Z_\mathrm{v} Z_\mathrm{s} Z_\mathrm{m}|E\tilde{C}^N)_{\rho|\Omega_\circ} \geq H^\zeta_\mathrm{min}(Z_\mathrm{v} Z_\mathrm{s}|E\tilde{C}^N)_{\rho|\Omega_\circ} \geq H^\zeta_\mathrm{min}(Z^{s^\mathrm{l}_{\mathsf{Z},0}} Z^{s^\mathrm{l}_{\mathsf{Z},1}}|E\tilde{C}^N)_{\rho|\Omega_\circ}\,, \tag{62}$$

where, in the second inequality, we apply the Lemma again on the registers Z_v and Z_s, which we shrink according to the acceptance bounds on the number of vacuum and single-photon numbers. This step is necessary to remove any random variable and have registers of well-defined size $|Z^{s^\mathrm{l}_{\mathsf{Z},0}}| = s^\mathrm{l}_{\mathsf{Z},0}$ and $|Z^{s^\mathrm{l}_{\mathsf{Z},1}}| = s^\mathrm{l}_{\mathsf{Z},1}$, i.e. given by the acceptance set, as we consider a fixed-length protocol, cf. Sec. 2.1.1. To simplify the notation, we define $Z^\mathrm{l}_\mathrm{v} \coloneqq Z^{s^\mathrm{l}_{\mathsf{Z},0}}$ and $Z^\mathrm{l}_s \coloneqq Z^{s^\mathrm{l}_{\mathsf{Z},1}}$. Additionally, the chain rule for smooth min-entropies can be used to decompose the min-entropy[25]

$$H^{2\alpha_1+\alpha_2+\alpha_3}_\mathrm{min}(A'B'|C')_\rho \geq H^{\alpha_1}_\mathrm{min}(A'|B'C')_\rho + H^{\alpha_3}_\mathrm{min}(B'|C')_\rho - \log_2 \frac{2}{\alpha_2^2}\,, \tag{63}$$

where A', B', C' are generic classical and quantum systems, $\alpha_1, \alpha_3 \geq 0$ and $\alpha_2 > 0$, cf. Ref. [86, Theorem 13], and we used the fact that $\log_2 \frac{2}{\alpha^2} \geq \log_2 \frac{1}{1-\sqrt{1-\alpha^2}}$ for all $\alpha \in [0,1]$. Applying the chain rule to Eq. (62) with conveniently defined $\zeta = 2\alpha_1 + \alpha_2 + \alpha_3$ yields[26]

$$H^\zeta_\mathrm{min}(Z^\mathrm{l}_\mathrm{v} Z^\mathrm{l}_\mathrm{s}|E\tilde{C}^N)_{\rho|\Omega_\circ} \geq H^{\alpha_1}_\mathrm{min}(Z^\mathrm{l}_\mathrm{v}|Z^\mathrm{l}_\mathrm{s} E\tilde{C}^N)_{\rho|\Omega_\circ} + H^{\alpha_3}_\mathrm{min}(Z^\mathrm{l}_\mathrm{s}|E\tilde{C}^N)_{\rho|\Omega_\circ} - \log_2 \frac{2}{\alpha_2^2}\,. \tag{64}$$

Written in this form, we can determine an operational bound for the expression above in terms of the acceptance bounds. Due to the fact that vacuum events contain no information about Z and the min-entropy is given according to Alice's key as Bob corrects his key to match Alice, we can substitute $H^{\alpha_1}_\mathrm{min}(Z^\mathrm{l}_\mathrm{v}|Z^\mathrm{l}_\mathrm{s} E\tilde{C}^N)_{\rho|\Omega_\circ} = \log_2 2^{s^\mathrm{l}_{\mathsf{Z},0}} = s^\mathrm{l}_{\mathsf{Z},0}$, where we use the fact that in the case of absolute uncertainty, as is the case for vacuum events, the min-entropy is maximal (as discussed in Sec. 4.1). The smoothing parameter α_1 is a free parameter, and as the bound on the smooth min-entropy for vacuum events is independent of α_1, we set $\alpha_1 = 0$. Thus, interestingly, vacuum events that passed the sifting step contribute to the extractable secure key. Putting everything together yields Lemma 2.

Lemma 2. *Consider the protocol described in Fig. 2 and the following classical registers: the basis choice announcements $\tilde{C}^N$, error correction communications C_EC, hash of Alice's corrected key C'_EV, and choice of hash function for error verification C''_EV, cf. Table 3. Then, we can bound the min-entropy of the state $\rho_{S E\tilde{C}^N C_\mathrm{EC} C'_\mathrm{EV} C''_\mathrm{EV}}$ describing Eve and Alice's key S after privacy amplification,*

$$H^\zeta_\mathrm{min}(Z|E\tilde{C}^N C_\mathrm{EC} C'_\mathrm{EV} C''_\mathrm{EV})_{\rho|\Omega_\circ} \geq s^\mathrm{l}_{\mathsf{Z},0} + H^{\alpha_3}_\mathrm{min}(Z^\mathrm{l}_\mathrm{s}|E\tilde{C}^N)_{\rho|\Omega_\circ} - \log_2 \frac{2}{\alpha_2^2} - \mathrm{leak}_\mathrm{EC} - \log_2 \frac{2}{\epsilon_\mathrm{cor}}\,, \tag{65}$$

where $\mathrm{leak}_\mathrm{EC}$ is the number of bits leaked during error correction, $s^\mathrm{l}_{\mathsf{Z},0}$ is the acceptance bound on the number of vacuum events and $\Omega_\circ$ is defined as the event where the true values of the observed statistics fulfill the acceptance condition, cf. Eq. (47).

[25] A tighter expression for the chain rule for smooth min-entropies can be found in Ref. [86, Theorem 13].

[26] It is also possible to completely remove the vacuum contributions, analogously to the multi-photon contributions, which may slightly increase the secure-key length if their contribution is small (or zero) as the term α_2 then vanishes.

Proof. The proof is given above. □

We note that the bound we derived is slightly tighter than Refs. [26,27] as we remove the multi-photon events using Ref. [63, Lemma 6.17] instead of the chain rule, resulting in fewer smoothing parameters. In the following sections, we address the single-photon min-entropy in Eq. (65) using the entropic uncertainty relation. This term requires more technical arguments than the ones previously discussed.

4.4.2 Source-replacement scheme

In this section, we discuss a technical argument required to apply the entropic uncertainty relation used to bound the single-photon min-entropy from the previous section, cf. Eq. (65). In fact, the single-photon rounds of the *prepare-and-measure scheme* discussed until now, where Alice locally prepares the signal states and sends them to Bob over the quantum channel, can be replaced by an equivalent entanglement-based scenario, following the *source-replacement scheme* [37,87,88]. Essentially, for the rounds where Alice sends single photons, we consider a virtual setup where Alice prepares entangled states

$$|\Psi_+\rangle = \frac{1}{\sqrt{2}} \left(|00\rangle_{AA'} + |11\rangle_{AA'}\right) , \tag{66}$$

keeps system A and sends system A' to Bob. Eve may then intercept system A' and send a system B to Bob. Alice and Bob then share a potentially entangled system ρ_{AB}, where Eve holds a purification of this system. Alice and Bob can estimate how much information Eve holds about A by performing a *von Neumann measurement*, i.e. locally measuring their systems in incompatible bases, the X-basis and Z-basis. This will be formalized in Sec. 4.4.3 when introducing the entropic uncertainty relation, which requires the source replacement. In the following, we may delay Alice's measurements until after Eve has performed her attack.

In the scenario where Alice prepares perfect signal states, her measurement POVMs are given by $\mathbb{X} = \{M_x\}_x$ and $\mathbb{Z} = \{N_z\}_z$ for the X-basis and Z-basis, respectively. Note that one can only view Alice's measurements as having active basis choice if signal preparation is perfect, which is important when using the EUR statement (see Ref. [37, Remark 1]), as it assumes active basis choice on Alice's measurements. For the BB84 protocol with perfectly diagonal bases, considering the single-photon rounds, we have $\mathbb{X} = \{|+\rangle\langle+|, |-\rangle\langle-|\}$ and $\mathbb{Z} = \{|0\rangle\langle 0|, |1\rangle\langle 1|\}$ where $|\pm\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2}$. In the next section, we derive the bounds for the virtual entanglement-based scheme described in this section but note that the bounds equivalently hold for the prepare-and-measure scheme considered throughout this work and described in Sec. 2.1.2.

4.4.3 Entropic uncertainty relation

A lower bound on the single-photon min-entropy $H_{\min}^{\alpha_3}(Z_{\mathrm{s}}^{\mathrm{l}}|E\tilde{C}^N)_{\rho|\Omega_\circ}$ can be found by using the fact that the secrecy of the Z-basis single-photon events is given by how well Bob is able to estimate Alice's key if he would have measured in the X-basis instead[27]. This is expressed by the *entropic uncertainty relation* (EUR) for smooth entropies [42]. The EUR statement considers an arbitrary state $\rho_{ABE'}$, and relates the min-entropy of the state obtained via Z-basis measurements ($\rho_{ZBE'}$) to the max-entropy of the state obtained by X-basis measurements (ρ_{XBE}), on Alice's system. This is given by

$$H_{\min}^{\alpha}(Z|E')_{\rho_{ZBE'}} + H_{\max}^{\alpha}(X|B)_{\rho_{XBE'}^{\mathrm{virt}}} \geq q\,, \tag{67}$$

where $q = -\log_2 c$ and $c = \max_{x,z} \left\|\sqrt{M_x}\sqrt{N_z}\right\|_\infty^2$ is a measure for the incompatibility of the bases. Additionally, E' denotes a generic quantum state of an adversary who also has access to classical communications C'. Here, $\rho_{ZBE'}$ describes the post-measurement state for the actual protocol, given that Alice measures in the Z-basis, and $\rho_{XBE'}^{\mathrm{virt}}$ describes the virtual protocol where Alice measures

[27] This is rather intuitive in the sense that if Eve gathers information about the Z-basis (e.g. through an intercept-and-resend attack), she necessarily induce some error in Bob's detections in the X-basis.

in the X-basis. Considering perfectly diagonal bases, as discussed in the previous section, we have $q = -\log_2 1/2 = 1$ [36, 89][28]. See also Refs. [84, 90] for additional discussions. In the following, we assume that $q = 1$[29].

One advantage of the EUR framework is that the smooth entropies appearing in the entropic uncertainty relation quantify measures beyond the i.i.d. scenario [42]. This approach thus inherently proves security against coherent attacks, the most general form of attack in which Eve can apply any strategy permitted by quantum mechanics on the channel. Thus, it yields tighter finite-size key rates than proof techniques that involve pessimistic lifts from collective to coherent attacks, such as the post-selection technique [43, 44].

We apply the EUR statement on the set of rounds where Alice chose the Z-basis and sent a single photon, and Bob measured in the Z-basis and got a detection. We know that there are exactly $s_{\mathsf{Z},1}$ of such rounds, although the exact value of $s_{\mathsf{Z},1}$ is not known. Since we condition on the event $\Omega_\circ$, we have $s_{\mathsf{Z},1} \geq s^{\mathrm{l}}_{\mathsf{Z},1}$, and we only apply the EUR statement on $s^{\mathrm{l}}_{\mathsf{Z},1}$ rounds. We recall that the key registers were shrunk to match the acceptance bounds in Sec. 4.4.1. Moreover, the state on which the EUR statement is applied can be obtained by reformulating Bob's measurements to consist of several steps, where he first measures to see whether he obtains a detection or not, determines his basis, and only later completes the measurement procedure (see Ref. [37, Section III]). We consider the $s^{\mathrm{l}}_{\mathsf{Z},1}$ rounds where Alice measured in the Z-basis and denote Alice's POVM element for the i-th round as $N_{z_i} \in \mathbb{Z}$ with $z_i \in \{0, 1\}$, cf. Sec. 4.4.2. Then, the POVM describing the full $s^{\mathrm{l}}_{\mathsf{Z},1}$-round measurement is given by $\mathbb{N}^{\mathrm{full}} = \{N^{\mathrm{full}}_{\mathbf{z}}\}_{\mathbf{z}}$, where $\mathbf{z} = (z_1, ..., z_{s^{\mathrm{l}}_{\mathsf{Z},1}})$ and $N^{\mathrm{full}}_{\mathbf{z}} = \bigotimes_i N_{z_i}$. Analogously, we define the $s^{\mathrm{l}}_{\mathsf{Z},1}$-round POVM for the case where Alice measures in the X-basis as $\mathbb{M}^{\mathrm{full}} = \{M^{\mathrm{full}}_{\mathbf{x}}\}_{\mathbf{x}}$. Then we can apply the EUR statement, i.e. Eq. (67), for the multi-round POVMs $\mathbb{N}^{\mathrm{full}}$ and $\mathbb{M}^{\mathrm{full}}$ and obtain

$$H^{\alpha_3}_{\min}(Z^{\mathrm{l}}_{\mathrm{s}}|E)_{\rho_{Z^{\mathrm{l}}_{\mathrm{s}}BE\tilde{C}^N|\Omega_\circ}} + H^{\alpha_3}_{\max}(X^{\mathrm{l}}_{\mathrm{s}}|B)_{\rho^{\mathrm{virt}}_{X^{\mathrm{l}}_{\mathrm{s}}BE\tilde{C}^N|\Omega_\circ}} \geq s^{\mathrm{l}}_{\mathsf{Z},1}\,, \tag{68}$$

where we defined $X^{\mathrm{l}}_{\mathrm{s}} := X^{s^{\mathrm{l}}_{\mathsf{Z},1}}$ and used the fact that

$$-\log_2 \max_{\mathbf{x},\mathbf{z}} \left\| \sqrt{M^{\mathrm{full}}_{\mathbf{x}}} \sqrt{N^{\mathrm{full}}_{\mathbf{z}}} \right\|^2_\infty = -\log_2 \left(\Pi_{i=1}^{s^{\mathrm{l}}_{\mathsf{Z},1}} \max_{x,z} \left\| \sqrt{M_x} \sqrt{N_z} \right\|^2_\infty \right) = s^{\mathrm{l}}_{\mathsf{Z},1}\,, \tag{69}$$

with $\max_{x,z} \left\| \sqrt{M_x} \sqrt{N_z} \right\|^2_\infty = 1/2$. Now, we can use data processing inequalities [63, Theorem 6.19] to make Bob measure his register B in the X-basis and obtain the classical register $\tilde{X}^{\mathrm{l}}_{\mathrm{s}}$. This yields

$$H^{\alpha_3}_{\min}(Z^{\mathrm{l}}_{\mathrm{s}}|E)_{\rho_{Z^{\mathrm{l}}_{\mathrm{s}}BE\tilde{C}^N|\Omega_\circ}} + H^{\alpha_3}_{\max}(X^{\mathrm{l}}_{\mathrm{s}}|\tilde{X}^{\mathrm{l}}_{\mathrm{s}})_{\rho^{\mathrm{virt}}_{X^{\mathrm{l}}_{\mathrm{s}}\tilde{X}^{\mathrm{l}}_{\mathrm{s}}|\Omega_\circ}} \geq s^{\mathrm{l}}_{\mathsf{Z},1}\,. \tag{70}$$

The max-entropy term can now be related to the error rate in the virtual X-basis measurements, which we formalize below. This is known as the *phase error rate*, and we denote it Λ_{Z}. In this way, Eve's uncertainty about the Z-basis detections (quantified by the min-entropy) is related to the correlation between Alice's and Bob's X-basis detections, if they had measured in the X-basis instead (quantified by the max-entropy). Obviously, when measuring in the Z-basis, the correlation in the X-basis is not directly accessible in the protocol. However, if we assume that Eve's attack strategy does not depend on Alice's and Bob's basis choice, we can use the statistics from the events where Alice and Bob choose the X-basis in order to estimate the correlation in the case where they measured in the Z-basis. This is effectively a sampling without replacement problem where one considers a virtual scenario in which Alice and Bob only measure in the X-basis, cf. Refs. [91, Sec. 2.2] and [37, Section 3] for a more thorough discussion. Note that this assumption can be rigorously argued in the scenario where Alice prepares perfect signal states, and Bob's probability of detection is independent of his basis choice (i.e absence of basis-efficiency mismatch).

[28] In practical implementations, the bases might not be perfectly diagonal, leading to a quality factor $q < 1$.

[29] This is required to apply the random sampling argument discussed below.

We note that the EUR is applied to quantum states and is not applicable to a state that was already measured. Intuitively, the virtual scenario described above cannot be assumed if the measurements have already been performed in any basis. Hence, we cannot condition Eq. (70) on Ω_{EC}, Ω_{EV}, Ω_{AT} nor Ω_{B} as these events require the state ρ_{AB} to already be measured. This motivates why we introduced the event $\Omega_\circ$. In Sec. 4.3, we have shown that the bounds derived for Eq. (48) conditioned on $\Omega_\circ$ also hold when conditioning on the other events listed above, resulting in Eq. (57). We defined the *single-photon quantum bit error rate* (QBER) in the X-basis as

$$\Lambda_{\mathsf{X}} \coloneqq \frac{c_{\mathsf{X},1}}{s_{\mathsf{X},1}}\,, \tag{71}$$

where $s_{\mathsf{X},1}$ is the number of single-photon events and $c_{\mathsf{X},1}$ the corresponding number of single-photon errors. We note again that these variables are not directly accessible to Alice and Bob, and it will be the aim of Sec. 5 to bound them and verify that the bounds satisfy the acceptance conditions, cf. Table 1. We can now use Serfling's inequality to bound the virtual single-photon error rate Λ_{Z}, or phase error rate, using the statistics from the X-basis. In fact, following Refs. [92, Corollary 1.1] and [36, Supplementary Notes 2],

$$\Pr\left[\Lambda_{\mathsf{Z}} \geq \Lambda_{\mathsf{X}} + \gamma(\nu, s_{\mathsf{Z},1}, s_{\mathsf{X},1})\right] \leq \nu^2\,, \tag{72}$$

where

$$\gamma(a,b,c) = \sqrt{\frac{b+c}{bc}\frac{c+1}{c}\ln\frac{1}{a}}\,, \tag{73}$$

i.e. the probability that the phase error rate deviates by more than $\gamma(\nu, s_{\mathsf{Z},1}, s_{\mathsf{X},1})$ from the single-photon QBER is bounded by ν^2. The above equation implies

$$\Pr[\Lambda_{\mathsf{Z}} \geq \Lambda_{\mathsf{X}} + \gamma(\nu, s_{\mathsf{Z},1}, s_{\mathsf{X},1}) \wedge \Omega_\circ] \leq \nu^2\,. \tag{74}$$

Using the acceptance bounds from Q and the properties of $\gamma(a,b,c)$, which is decreasing in b and c, we obtain

$$\Pr[\Lambda_{\mathsf{Z}} \geq \Lambda^{\mathrm{u}}_{\mathsf{X}} + \gamma(\nu, s^{\mathrm{l}}_{\mathsf{Z},1}, s^{\mathrm{l}}_{\mathsf{X},1}) \,|\, \Omega_\circ] \leq \frac{\nu^2}{\Pr[\Omega_\circ]}\,, \tag{75}$$

where we used that conditioning on $\Omega_\circ$ implies $s_{\mathsf{Z},1} \geq s^{\mathrm{l}}_{\mathsf{Z},1}$, $s_{\mathsf{X},1} \geq s^{\mathrm{l}}_{\mathsf{X},1}$ and $\Lambda_{\mathsf{X}} \leq \Lambda^{\mathrm{u}}_{\mathsf{X}}$. To simplify the notation, we define $\gamma \coloneqq \gamma(\nu, s^{\mathrm{l}}_{\mathsf{Z},1}, s^{\mathrm{l}}_{\mathsf{X},1})$ in the following. Using the results from Ref. [36, Lemma 3], the max-entropy appearing in Eq. (70) can be rewritten in terms of the binary entropy function h[30] and the bound on the phase error rate, namely

$$H^{\alpha_3}_{\min}(Z^{\mathrm{l}}_{\mathrm{s}}|E\tilde{C}^N)_{\rho_{Z^{\mathrm{l}}_{\mathrm{s}}B E\tilde{C}^N|\Omega_\circ}} \geq s^{\mathrm{l}}_{\mathsf{Z},1} - H^{\alpha_3}_{\max}(X^{\mathrm{l}}_{\mathrm{s}}|\tilde{X}^{\mathrm{l}}_{\mathrm{s}})_{\rho^{\mathrm{virt}}_{X^{\mathrm{l}}_{\mathrm{s}}\tilde{X}^{\mathrm{l}}_{\mathrm{s}}E|\Omega_\circ}} \geq s^{\mathrm{l}}_{\mathsf{Z},1} - s^{\mathrm{l}}_{\mathsf{Z},1} h(\Lambda^{\mathrm{u}}_{\mathsf{X}} + \gamma)\,, \tag{76}$$

where

$$\alpha_3 \coloneqq \frac{\nu}{\sqrt{\Pr[\Omega_\circ]}}\,. \tag{77}$$

Intuitively, if $\Lambda^{\mathrm{u}}_{\mathsf{X}} + \gamma$ is small, we can deduce that the correlation between Alice's and Bob's single-photon bit values is high and thus the max-entropy is small. We must distinguish two cases in the following. If $\alpha_3 < 1$, we continue the analysis. However, if $\alpha_3 \geq 1$, we cannot smooth the entropies using α_3, cf. Sec. 4.2. We discuss the latter case below Eq. (80) and assume $\alpha_3 < 1$ for now. Using Lemma 2 and substituting in Eq. (76) yields an operational bound on the smooth min-entropy,

$$\boxed{H^{\zeta}_{\min}(Z|E\tilde{C}^N C_{\mathrm{EC}} C_{\mathrm{EV}})_{\rho|\Omega_\circ} \geq s^{\mathrm{l}}_{\mathsf{Z},0} + s^{\mathrm{l}}_{\mathsf{Z},1}(1 - h(\Lambda^{\mathrm{u}}_{\mathsf{X}} + \gamma)) - \log_2\frac{2}{\alpha_2^2} - \mathrm{leak}_{\mathrm{EC}} - \log_2\frac{2}{\epsilon_{\mathrm{cor}}}\,,} \tag{78}$$

[30] More precisely, h denotes the truncated binary entropy function defined as $h : x \mapsto -x\log_2 x - (1-x)\log_2(1-x)$ if $x \leq 0.5$ and $h(x) = 1$ if $x > 0.5$ [36].

as appearing in Eq. (57). We derived the bound by applying the chain rule for smooth min-entropies to separate the different m-photon event contributions in Z and used the EUR to bound the single-photon contributions with the phase error rate. As discussed above, the conditioning on $\Omega_\circ$ is required to apply the EUR. We have thus derived an upper bound on branch (b), i.e. the first term in Eq. (25), following Eq. (57), in terms of the min-entropy, for which we have derived an operational expression above, cf. Eq. (78). We can now rewrite Eq. (25) by plugging in Eq. (57), yielding

$$\begin{aligned}\Pr[\tilde{\Omega}]d_{\mathrm{sec}}(SEC)_{\rho|\tilde{\Omega}} &\leq \Pr[\tilde{\Omega}\wedge\Omega_{\mathrm{B}}]d_{\mathrm{sec}}(SEC)_{\rho|\tilde{\Omega}\wedge\Omega_{\mathrm{B}}} + \Pr[\tilde{\Omega}\wedge\neg\Omega_{\mathrm{B}}]\,, &(79)\\ &\leq 2(\alpha_2+\nu) + \Delta^{\zeta}_{\mathrm{pa}} + \Pr[\tilde{\Omega}\wedge\neg\Omega_{\mathrm{B}}]\,, &(80)\end{aligned}$$

where we use $\Pr[\Omega_\circ]\leq 1$, and $\alpha_3\Pr[\Omega_\circ]\leq\nu$, cf. Eq. (77). We recall that $\zeta=\alpha_2+\alpha_3$ and we set $\alpha_1=0$ as discussed above. We note that if $\alpha_3\geq 1$, cf. Eq. (77), then we directly have a bound on Eq. (52) without requiring smooth entropies as this implies $\Pr[\Omega_\circ]\leq\nu^2\leq\nu$ and using the fact that the trace distance never exceeds one, we have $\Pr[\tilde{\Omega}\wedge\Omega_{\mathrm{B}}]d_{\mathrm{sec}}(SEC)_{\rho|\tilde{\Omega}\wedge\Omega_{\mathrm{B}}}\leq\nu$, such that all further analyses on Eq. (80) also hold if $\alpha_3\geq 1$. Finally, we recall that the secure-key length l appears in $\Delta^{\zeta}_{\mathrm{pa}}$. We choose an appropriate l to fulfill the security criterion in Sec. 6.1.

Lemma 3. *Consider the protocol described in Fig. 2, the events listed in Table 2 and the classical announcements listed in Table 3. Let ρ_{SEC} be the state describing Eve and Alice's key S after privacy amplification. Then the following bound holds*

$$\Pr[\tilde{\Omega}]d_{\mathrm{sec}}(SEC)_{\rho|\tilde{\Omega}}\leq 2(\alpha_2+\nu)+\Delta^{\zeta}_{\mathrm{pa}}+\Pr[\tilde{\Omega}\wedge\neg\Omega_{\mathrm{B}}]\,, \tag{81}$$

where $\alpha_2,\nu>0$,

$$\Delta^{\zeta}_{\mathrm{pa}}=\frac{1}{2}\sqrt{2^{l-H^{\zeta}_{\min}\left(Z\,|\,E\tilde{C}^{N}C_{\mathrm{EC}}C_{\mathrm{EV}}C_{\mathrm{AT}}\right)_{\rho|\Omega_\circ}}}\,, \tag{82}$$

and the smooth min-entropy is lower bounded by

$$H^{\zeta}_{\min}(Z|E\tilde{C}^{N}C_{\mathrm{EC}}C_{\mathrm{EV}}C_{\mathrm{AT}})_{\rho|\Omega_\circ}\geq s^{\mathrm{l}}_{\mathsf{Z},0}+s^{\mathrm{l}}_{\mathsf{Z},1}(1-h(\Lambda^{\mathrm{u}}_{\mathsf{X}}+\gamma))-\log_2\frac{2}{\alpha_2^2}-\mathrm{leak}_{\mathrm{EC}}-\log_2\frac{2}{\epsilon_{\mathrm{cor}}}\,, \tag{83}$$

where $s^{\mathrm{l}}_{\mathsf{Z},0}$, $s^{\mathrm{l}}_{\mathsf{Z},1}$ and $\Lambda^{\mathrm{u}}_{\mathsf{X}}$ are acceptance parameters fixed before the protocol run, cf. Fig. 2, and $\gamma=\gamma(\nu,s^{\mathrm{l}}_{\mathsf{Z},1},s^{\mathrm{l}}_{\mathsf{X},1})$ is given by Eq. (73).

Proof. The proof is given above. □

Until now, we have assumed that bounds on the number of vacuum events $s^{-}_{\mathsf{Z},0}$, single photon events $s^{-}_{\mathsf{Z},1}$, $s^{-}_{\mathsf{X},1}$ and the single-photon QBER Λ^{+}_{X} exist and can be used by Alice and Bob to perform the acceptance test described in Table 1 and Sec. 2.1.2. The aim of the following section is precisely to derive these bounds in terms of experimentally available parameters. This will also provide us with a bound on $\Pr[\tilde{\Omega}\wedge\neg\Omega_{\mathrm{B}}]$ from Eq. (80), i.e. branch (c), which is the last term we need to bound in Fig. 3.

Remark 13. *The random sampling argument for estimating the phase error rate, formulated in terms of the detection statistics, cf. Eq. (74), assumes no detection-efficiency mismatch, which is experimentally unfeasible, as will be discussed in Sec. 7. A recent work resolves this constraint by adjusting the random sampling arguments for scenarios that do not perfectly satisfy the no-mismatch assumption. In particular, Ref. [37] can produce key rates for scenarios with an imperfectly characterized, bounded amount of mismatch in detector efficiencies and dark count rates.*

5 Decoy bounds

In the last section, the smooth min-entropy has been decomposed so as to yield an expression in terms of the acceptance bounds $s^{\mathrm{l}}_{\mathsf{Z},0}$, $s^{\mathrm{l}}_{\mathsf{Z},1}$, $s^{\mathrm{l}}_{\mathsf{X},1}$ and $\Lambda^{\mathrm{u}}_{\mathsf{X}}$ defined by the acceptance set, cf. Eq (78). The acceptance test is performed by verifying that $s^{-}_{\mathsf{Z},0} \geq s^{\mathrm{l}}_{\mathsf{Z},0}$, $s^{-}_{\mathsf{Z},1} \geq s^{\mathrm{l}}_{\mathsf{Z},1}$, $s^{-}_{\mathsf{X},1} \geq s^{\mathrm{l}}_{\mathsf{X},1}$ and $\Lambda^{+}_{\mathsf{X}} \leq \Lambda^{\mathrm{u}}_{\mathsf{X}}$, cf. Table 1 and Fig. 2. We recall that the number of vacuum events, single-photon events and the phase error rate are not directly accessible to Alice and Bob. Thus, our goal in this section is to determine the decoy bounds $s^{-}_{\mathsf{Z},0}, s^{-}_{\mathsf{Z},1}$, $s^{-}_{\mathsf{X},1}$ and Λ^{+}_{X} solely in terms of experimentally available parameters. The acceptance test is then performed using these bounds. If the decoy bounds hold, the acceptance test passes and error correction was successful, then $s_{\mathsf{Z},0} \geq s^{-}_{\mathsf{Z},0} \geq s^{\mathrm{l}}_{\mathsf{Z},0}$ and analogously for $s^{\mathrm{l}}_{\mathsf{Z},1}$, $s^{\mathrm{l}}_{\mathsf{X},1}$ and $\Lambda^{\mathrm{u}}_{\mathsf{X}}$. Verifying these relations is precisely the aim of the acceptance test on the decoy bounds. We recall that we used $s_{\mathsf{Z},0} \geq s^{\mathrm{l}}_{\mathsf{Z},0}$ and the other relations when deriving an operational expression for the min-entropy in previous section. The methods used in this section are similar to Refs. [26, 27, 91]. The bounds for the 2-decoy state protocol are derived in App. A.2.

5.1 Finite-size photon event statistics

In the 1-decoy state BB84 protocol, similarly to the original BB84 prepare-and-measure protocol, two bases X and Z are chosen to transmit signals over a quantum channel. However, in order to counter so-called photon-number-splitting (PNS) attacks by an eavesdropper Eve, an additionally degree of freedom is introduced in the level of intensity k used to transmit photons with a phase-randomized coherent laser source. A phase-randomized coherent state with intensity k sent by Alice can be represented by [93]

$$\rho_k = \int_0^{2\pi} d\theta f(\theta) \left|\sqrt{k}e^{i\theta}\right\rangle\!\left\langle\sqrt{k}e^{i\theta}\right| , \tag{84}$$

where $f(\theta)$ is the probability density function representing the probability of generating a state with phase θ. Here, $\left|\sqrt{k}e^{i\theta}\right\rangle$ represents a coherent state with mean photon number k and phase θ, defined as a coherent superposition of Fock states $|m\rangle$, where $|m\rangle$ denotes a photon-number (Fock) state containing exactly m photons in the optical mode [94],

$$|\alpha\rangle = \sum_{m=0}^{\infty} e^{-|\alpha|/2} \frac{\alpha^m}{\sqrt{m!}} |m\rangle \ . \tag{85}$$

In the case of uniform phase randomization, i.e. $f(\theta) = \frac{1}{2\pi}$, Eq. (84) simplifies to

$$\rho_k = \sum_{m=0}^{\infty} e^{-k} \frac{k^m}{m!} |m\rangle\langle m| \ . \tag{86}$$

Essentially, with uniform phase randomization, Alice's density operator is diagonal in the Fock-basis, which reduces the analysis to a discussion of the statistics of photon events as Fock states do not carry information about the intensity choice. In contrast, if the phases are not uniformly randomized, then Alice's density operator is not diagonal in the Fock-basis and her signals carry information about the intensity choice. This conflicts with the assumption that Eve has no a priori knowledge about Alice's intensity choices. Note that it is still possible to prove security in this case, but the secure-key length is significantly impacted in current proofs [95–97]. In the following, for simplicity, we assume uniform phase randomization. Following Eq. (86), the photon number of a uniformly phase-randomized coherent photon source follows the Poisson distribution

$$\Pr[m] = e^{-k} \frac{k^m}{m!} , \tag{87}$$

where m is the number of photons sent per signal. In the case of the 1-decoy state protocol, two levels of intensity μ_1 and μ_2 are used at random following pre-configured probabilities p_{μ_1} and p_{μ_2}, with

$\mu_1 > \mu_2$. Often, the states with intensity μ_1 are called *signal states*, and the states with intensity μ_2 are called *decoy states*[31].

It is useful to assume an equivalent virtual scenario in which Alice chooses the mean photon-number after Bob measured an m-photon state. This means that instead of considering the probability of an m-photon event occurring given an intensity $k \in \{\mu_1, \mu_2\}$, we consider the probability that an intensity k was chosen given the detection of an m-photon event. Both scenarios are equivalent as Eve's attack strategy cannot depend on the chosen intensity, meaning that Bob's measurement results are also independent of Alice's intensity choice (for a more thorough discussion, see App. A.6 or Ref. [91, Sec. 3.1]). This follows from the fact that Eve has no a priori knowledge about Alice's intensity choice and that the coherent states are uniformly phase-randomized such that they don't carry any information about the intensity choice, as discussed above.

In the following, solely the Z-basis is considered, but the equations analogously hold for the X-basis. The total number of detections observed by Bob in the Z-basis is given by

$$N_{\mathsf{Z}} = \sum_{m=0}^{\infty} s_{\mathsf{Z},m} \,, \tag{88}$$

where $s_{\mathsf{Z},m}$ is the number of detections of m-photon events in the Z-basis. Alice chooses one of the intensities μ_1 and μ_2 randomly with probabilities $p_{\mu_1|m}$ and $p_{\mu_2|m}$ respectively, given that Bob measures an m-photon state. As such, for a given intensity $k \in \{\mu_1, \mu_2\}$, the expected number of detections is given by

$$n^*_{\mathsf{Z},k} = \sum_{m=0}^{\infty} \Pr[k|m]\, s_{\mathsf{Z},m} \,. \tag{89}$$

Analogously, the total number of errors observed in the Z-basis is given by

$$c_{\mathsf{Z}} = \sum_{m=0}^{\infty} v_{\mathsf{Z},m} \,, \tag{90}$$

where $v_{\mathsf{Z},m}$ is the number of errors associated with $s_{\mathsf{Z},m}$. The expected number of bit errors observed, given a certain intensity k, is given by

$$c^*_{\mathsf{Z},k} = \sum_{m=0}^{\infty} p_{k|m} v_{\mathsf{Z},m} \,. \tag{91}$$

Let $n_{\mathsf{Z},k}$ and $c_{\mathsf{Z},k}$ be the number of detections and errors observed, respectively, given an intensity k. Here, N_{Z}, c_{Z}, $n_{\mathsf{Z},k}$ and $c_{\mathsf{Z},k}$ are known experimental values while the sets $\{s_{\mathsf{Z},m}\}$ and $\{v_{\mathsf{Z},m}\}$ are not. The goal is to derive bounds on $s_{\mathsf{Z},0}$, $s_{\mathsf{Z},1}$, $s_{\mathsf{X},1}$ and Λ_{X} (necessary to perform the acceptance test leading to Eq. (78)) solely in terms of experimentally accessible parameters by taking finite-size effects into account.

Note that each signal is independently mapped to a specific intensity, based on the photon number of the pulse. Thus, using suitable concentration inequalities, such as Hoeffding's inequality [98] for independent random variables, we can bound the deviation of the observed number of detections and errors, $n_{\mathsf{Z},k}$ and $c_{\mathsf{Z},k}$, from the expected number of detections and errors, $n^*_{\mathsf{Z},k}$ and $c^*_{\mathsf{Z},k}$, as follows:[32]

$$\boxed{\Pr\left[n^*_{\mathsf{Z},k} > n^+_{\mathsf{Z},k}\right] \leq \epsilon^{n,+}_{\mathsf{Z},k} \,,} \tag{92}$$

$$\boxed{\Pr\left[n^*_{\mathsf{Z},k} < n^-_{\mathsf{Z},k}\right] \leq \epsilon^{n,-}_{\mathsf{Z},k} \,,} \tag{93}$$

where

$$n^{\pm}_{\mathsf{Z},k} \coloneqq n_{\mathsf{Z},k} \pm \delta(N_{\mathsf{Z}}, \epsilon^{n,\pm}_{\mathsf{Z},k}) \,, \tag{94}$$

[31] We note that in our protocol both intensities are used for testing and key generation.

[32] Here, other concentration inequalities such as Azuma's inequality can be used.

and

$$\delta(N_{\mathsf{Z}}, \epsilon^{n,\pm}_{\mathsf{Z},k}) \coloneqq \sqrt{N_{\mathsf{Z}} \ln\left(1/\epsilon^{n,\pm}_{\mathsf{Z},k}\right)/2} \tag{95}$$

is also called Hoeffding delta[33]. In other words, $\epsilon^{n,\pm}_{\mathsf{Z},k}$ is the probability that the number of photons $n_{\mathsf{Z},k}$ detected by Bob deviates by more than $\delta(N_{\mathsf{Z}}, \epsilon^{n,\pm}_{\mathsf{Z},k})$ from the expectation value $n^*_{\mathsf{Z},k}$. For a formal derivation of the expression for the Hoeffding delta using Ref. [98, Eq. (2.1)] as a starting point, refer to App. A.5. Analogously,

$$\boxed{\Pr\left[c^*_{\mathsf{Z},k} > c^+_{\mathsf{Z},k} \,|\, \Omega_{\mathrm{EC}}\right] \leq \epsilon^{c,+}_{\mathsf{Z},k}\,,} \tag{96}$$

$$\boxed{\Pr\left[c^*_{\mathsf{Z},k} < c^-_{\mathsf{Z},k} \,|\, \Omega_{\mathrm{EC}}\right] \leq \epsilon^{c,-}_{\mathsf{Z},k}\,.} \tag{97}$$

where

$$c^{\pm}_{\mathsf{Z},k} \coloneqq c_{\mathsf{Z},k} \pm \delta(c_{\mathsf{Z}}, \epsilon^{c,\pm}_{\mathsf{Z},k})\,, \tag{98}$$

and we additionally condition Eqs. (96) and (97) on error correction succeeding[34] as Bob needs to count the correct number of Z-basis errors $c_{\mathsf{Z},k}$ when comparing the non-corrected key to the corrected key, cf. Fig. 2. The bounds $n^{\pm}_{\mathsf{X},k}$ and $c^{\pm}_{\mathsf{X},k}$ for the X-basis are analogously defined but we don't require any conditioning on Ω_{EC} in this case as the X-basis detections are disclosed. We note that the use of Hoeffding's inequality for independent random variables is subtle in this context and we refer to Refs. [37, Remark 13] and [99] for a more thorough discussion. The goal of the following sections is to determine lower bounds for vacuum and single-photon events as well as an upper bound for the number of vacuum events and single-photon errors, which are required to perform the acceptance test, cf. Fig. 1.

5.1.1 Lower bound on the number of vacuum events

Using Bayes' theorem for the probability of choosing the intensity k given that Bob detected an m-photon event,

$$p_{k|m} = \frac{p_k}{\tau_m} p_{m|k} = \frac{p_k}{\tau_m} \frac{e^{-k} k^m}{m!}\,, \tag{99}$$

where

$$\tau_m = \sum_{k \in \{\mu_1, \mu_2\}} p_k \frac{e^{-k} k^m}{m!} \tag{100}$$

is the average probability for Alice to transmit an m-photon state. Now, using Eqs. (89), (99) and $p_{k|0} = \frac{p_k}{\tau_0} e^{-k}$, we find

$$\frac{\mu_1 e^{\mu_2} n^*_{\mathsf{Z},\mu_2}}{p_{\mu_2}} - \frac{\mu_2 e^{\mu_1} n^*_{\mathsf{Z},\mu_1}}{p_{\mu_1}} = \frac{(\mu_1 - \mu_2) s_{\mathsf{Z},0}}{\tau_0} - \mu_1 \mu_2 \sum_{m=2}^{\infty} \frac{(\mu_1^{m-1} - \mu_2^{m-1}) s_{\mathsf{Z},m}}{\tau_m m!}\,. \tag{101}$$

Now, solving for $s_{\mathsf{Z},0}$ and using $\mu_1 > \mu_2$ yields

$$s_{\mathsf{Z},0} \geq \frac{\tau_0}{(\mu_1 - \mu_2)} \left(\frac{\mu_1 e^{\mu_2} n^*_{\mathsf{Z},\mu_2}}{p_{\mu_2}} - \frac{\mu_2 e^{\mu_1} n^*_{\mathsf{Z},\mu_1}}{p_{\mu_1}} \right)\,. \tag{102}$$

Finally, together with the bounds from Eqs. (92) and (93), we have

$$\boxed{\Pr\left[s_{\mathsf{Z},0} < s^-_{\mathsf{Z},0} \coloneqq \frac{\tau_0}{(\mu_1 - \mu_2)} \left(\frac{\mu_1 e^{\mu_2} n^-_{\mathsf{Z},\mu_2}}{p_{\mu_2}} - \frac{\mu_2 e^{\mu_1} n^+_{\mathsf{Z},\mu_1}}{p_{\mu_1}} \right) \right] \leq \epsilon^{n,-}_{\mathsf{Z},\mu_2} + \epsilon^{n,+}_{\mathsf{Z},\mu_1}\,.} \tag{103}$$

[33] Note that in a QKD protocol, we have an unknown state ρ, that produces random variables such as $n_{\mathsf{Z},k}$ and $s_{\mathsf{Z},m}$. The above expression (and other analogous expressions) should be interpreted such that the probability is over these random variables.

[34] Formally, this can be argued by noting that we can pretend that Alice assigns intensities to pulses only after error correction has succeeded.

The inequalities $n^*_{\mathsf{Z},\mu_2} \geq n^-_{\mathsf{Z},\mu_2}$ and $n^*_{\mathsf{Z},\mu_1} \leq n^+_{\mathsf{Z},\mu_1}$ hold with a probability of at least $1-\epsilon^{n,-}_{\mathsf{Z},\mu_2}$ and $1-\epsilon^{n,+}_{\mathsf{Z},\mu_1}$, respectively (see Eqs. (92) and (93)). Hence, the probability that $s_{\mathsf{Z},0} \geq s^-_{\mathsf{Z},0}$ does not hold, i.e. at least one of the concentration inequalities does not hold, is upper-bounded by $\epsilon^{n,-}_{\mathsf{Z},\mu_2}+\epsilon^{n,+}_{\mathsf{Z},\mu_1}$. This is a consequence of Boole's inequality.

5.1.2 Upper bound on the number of vacuum events

An upper bound on the number of vacuum events is derived in this section and will be needed to derive a lower bound on the number of single-photon events in Sec. 5.1.3. Trivially, following Eq. (90), the total number of errors detected in the Z-basis can be lower bounded by the number of errors detected for vacuum events:

$$c_{\mathsf{Z}} \geq v_{\mathsf{Z},0}\,. \tag{104}$$

Due to the fact that vacuum events carry no information, the average number of vacuum errors $v^*_{\mathsf{Z},0}$ is half of the total number of vacuum events, namely[35] [27]

$$\frac{v^*_{\mathsf{Z},0}}{s_{\mathsf{Z},0}} = \frac{1}{2}\,. \tag{105}$$

By using Hoeffding's inequality, we can in turn bound $v^*_{\mathsf{Z},0}$ as a function of the observed number of errors for vacuum events $v_{\mathsf{Z},0}$ given a certain intensity,

$$\Pr\left[v^*_{\mathsf{Z},0} > v_{\mathsf{Z},0} + \delta(N_{\mathsf{Z}}, \epsilon^{v,+}_{\mathsf{Z},0})\right] \leq \epsilon^{v,+}_{\mathsf{Z},0}\,, \tag{106}$$

using $v_{\mathsf{Z},0}+\delta(s_{\mathsf{Z},0},\epsilon^{v,+}_{\mathsf{Z},0}) \leq v_{\mathsf{Z},0}+\delta(N_{\mathsf{Z}},\epsilon^{v,+}_{\mathsf{Z},0})$. Additionally, we find an upper bound for $v_{\mathsf{Z},0}$ by rewriting

$$c^*_{\mathsf{Z},k} = \sum_{m=0}^{\infty} p_{k|m} v_{\mathsf{Z},m} = \sum_{m=0}^{\infty} \frac{p_k}{\tau_m}\frac{e^{-k}k^m}{m!} v_{\mathsf{Z},m} \geq \frac{p_k}{\tau_0} e^{-k} v_{Z,0} \tag{107}$$

$$\Leftrightarrow v_{\mathsf{Z},0} \leq \frac{c^*_{\mathsf{Z},k}}{p_k}\tau_0 e^k. \tag{108}$$

We can now plug in Eq. (96) and write

$$\Pr\left[v_{\mathsf{Z},0} > \frac{c^+_{\mathsf{Z},k}}{p_k}\tau_0 e^k \,\middle|\, \Omega_{\mathrm{EC}}\right] \leq \epsilon^{c,+}_{\mathsf{Z},k}\,, \tag{109}$$

where any $k \in \{\mu_1,\mu_2\}$ can be chosen, e.g. to maximize the secure-key length. Now, using Eqs. (96), (105) and the bounds from Eqs. (106) and (109), we can determine an upper bound on the number of vacuum events,

$$\boxed{\Pr\left[s_{\mathsf{Z},0} > s^+_{\mathsf{Z},0} := 2\left(\frac{c^+_{\mathsf{Z},k}}{p_k}\tau_0 e^k + \delta(N_{\mathsf{Z}}, \epsilon^{v,+}_{\mathsf{Z},0})\right) \,\middle|\, \Omega_{\mathrm{EC}}\right] \leq \epsilon^{v,+}_{\mathsf{Z},0} + \epsilon^{c,+}_{\mathsf{Z},k}\,,} \tag{110}$$

where we condition on error correction succeeding, i.e. Ω_{EC}, as Bob requires the number of Z-basis errors to compute $c^+_{\mathsf{Z},k}$, which he determines by comparing the verified key to the sifted key, as discussed in Sec. 5.1. In the following, we denote $k^{\mathsf{Z}}_{\min} \in \{\mu_1,\mu_2\}$ the intensity chosen to compute the bound in the inequality above, which can be chosen to maximize the secure-key length.

[35] Here, we implicitly assume that Alice sends each bit with equal probability, both Z-basis detectors have the same properties and no asymmetric losses are present.

5.1.3 Lower bound on the number of single-photon events

Analogously to Sec. 5.1.1, we can write

$$\begin{aligned}\frac{e^{\mu_2} n^*_{\mathsf{Z},\mu_2}}{p_{\mu_2}} - \frac{e^{\mu_1} n^*_{\mathsf{Z},\mu_1}}{p_{\mu_1}} &= \frac{(\mu_2-\mu_1)s_{\mathsf{Z},1}}{\tau_1} + \sum_{m=2}^{\infty} \frac{(\mu_2^m - \mu_1^m)s_{\mathsf{Z},m}}{\tau_m m!} \\ &\leq \frac{(\mu_2-\mu_1)s_{\mathsf{Z},1}}{\tau_1} + \frac{\mu_2^2-\mu_1^2}{\mu_1^2}\sum_{m=2}^{\infty}\frac{\mu_1^m s_{\mathsf{Z},m}}{\tau_m m!},\end{aligned}$$

as

$$\mu_2^m - \mu_1^m = \mu_2^2\mu_2^{m-2} - \mu_1^2\mu_1^{m-2} = \mu_1^{m-2}\left(\mu_2^2\frac{\mu_2^{m-2}}{\mu_1^{m-2}} - \mu_1^2\right) \leq (\mu_2^2-\mu_1^2)\mu_1^{m-2}$$

for $m \geq 2$ and the last inequality holds for $\mu_1 > \mu_2$. Now, writing the sum of multi-photon events ($m \geq 2$) as

$$\sum_{m=2}^{\infty}\frac{\mu_1^m s_{\mathsf{Z},m}}{\tau_m m!} = \sum_{m=2}^{\infty}\frac{e^{\mu_1}e^{-\mu_1}p_{\mu_1}\mu_1^m s_{\mathsf{Z},m}}{p_{\mu_1}\tau_m m!} = \frac{e^{\mu_1}n^*_{\mathsf{Z},\mu_1}}{p_{\mu_1}} - \frac{s_{\mathsf{Z},0}}{\tau_0} - \frac{\mu_1 s_{\mathsf{Z},1}}{\tau_1} \tag{111}$$

by using Equations (89) and (99) yields

$$\frac{e^{\mu_2} n^*_{\mathsf{Z},\mu_2}}{p_{\mu_2}} - \frac{e^{\mu_1} n^*_{\mathsf{Z},\mu_1}}{p_{\mu_1}} \leq \frac{(\mu_2-\mu_1)s_{\mathsf{Z},1}}{\tau_1} + \frac{\mu_2^2-\mu_1^2}{\mu_1^2}\left(\frac{e^{\mu_1}n^*_{\mathsf{Z},\mu_1}}{p_{\mu_1}} - \frac{s_{\mathsf{Z},0}}{\tau_0} - \frac{\mu_1 s_{\mathsf{Z},1}}{\tau_1}\right). \tag{112}$$

Now, solving for $s_{\mathsf{Z},1}$ yields

$$s_{\mathsf{Z},1} \geq \frac{\mu_1\tau_1}{\mu_2(\mu_1-\mu_2)}\left(\frac{e^{\mu_2}n^*_{\mathsf{Z},\mu_2}}{p_{\mu_2}} - \frac{\mu_2^2}{\mu_1^2}\frac{e^{\mu_1}n^*_{\mathsf{Z},\mu_1}}{p_{\mu_1}} - \frac{(\mu_1^2-\mu_2^2)}{\mu_1^2}\frac{s_{\mathsf{Z},0}}{\tau_0}\right). \tag{113}$$

Finally, by substituting Eq. (110) into Eq. (113) and using the lower and upper bounds for the number of detections n^*_{Z,μ_2} and n^*_{Z,μ_1} (see Eqs. (92) and (93)), we can determine a lower bound for the number of single-photon events,[36]

$$\boxed{\Pr\left[s_{\mathsf{Z},1} < s^-_{\mathsf{Z},1} \,|\, \Omega_{\mathrm{EC}}\right] \leq \epsilon^{n,-}_{\mathsf{Z},\mu_2} + \epsilon^{n,+}_{\mathsf{Z},\mu_1} + \Pr\left[s_{\mathsf{Z},0} > s^+_{\mathsf{Z},0} \,|\, \Omega_{\mathrm{EC}}\right],} \tag{114}$$

where

$$s^-_{\mathsf{Z},1} := \frac{\mu_1\tau_1}{\mu_2(\mu_1-\mu_2)}\left(\frac{e^{\mu_2}n^-_{\mathsf{Z},\mu_2}}{p_{\mu_2}} - \frac{\mu_2^2}{\mu_1^2}\frac{e^{\mu_1}n^+_{\mathsf{Z},\mu_1}}{p_{\mu_1}} - \frac{(\mu_1^2-\mu_2^2)}{\mu_1^2}\frac{s^+_{\mathsf{Z},0}}{\tau_0}\right), \tag{115}$$

and we condition on Ω_{EC} for the same reason as in Sec. 5.1.2.

5.1.4 Upper bound on the number of single-photon errors

Finally, an upper bound for the number of single-photon errors is required to determine an upper bound on the single-photon QBER Λ_{X} (and thus the phase error rate Λ_{Z}) in Sec. 5.2. It can easily be derived, similarly to the other bounds, by rewriting

$$\frac{e^{\mu_1}c^*_{\mathsf{X},\mu_1}}{p_{\mu_1}} - \frac{e^{\mu_2}c^*_{\mathsf{X},\mu_2}}{p_{\mu_2}} = \frac{\mu_1-\mu_2}{\tau_1}v_{\mathsf{X},1} + \sum_{m=2}^{\infty}\frac{\mu_1^m}{\tau_m m!}v_{\mathsf{X},m} - \sum_{m=2}^{\infty}\frac{\mu_2^m}{\tau_m m!}v_{\mathsf{X},m}.$$

Using $\mu_1 > \mu_2$, we have

$$\frac{e^{\mu_1}c^*_{\mathsf{X},\mu_1}}{p_{\mu_1}} - \frac{e^{\mu_2}c^*_{\mathsf{X},\mu_2}}{p_{\mu_2}} \geq \frac{\mu_1-\mu_2}{\tau_1}v_{\mathsf{X},1}$$

[36] This bound is tight as $s^+_{\mathsf{Z},0}$ does not depend on $\epsilon^{n,-}_{\mathsf{Z},\mu_2}$ nor $\epsilon^{n,+}_{\mathsf{Z},\mu_1}$.

and thus

$$\frac{\tau_1}{\mu_1-\mu_2}\left(\frac{e^{\mu_1}c^*_{\mathsf{X},\mu_1}}{p_{\mu_1}}-\frac{e^{\mu_2}c^*_{\mathsf{X},\mu_2}}{p_{\mu_2}}\right)\geq v_{\mathsf{X},1}\,.$$

Finally, using Eqs. (96) and (97) yields an upper bound on the number of single-photon errors

$$\boxed{\Pr\left[v_{\mathsf{X},1}>v^+_{\mathsf{X},1}\coloneqq\frac{\tau_1}{\mu_1-\mu_2}\left(\frac{e^{\mu_1}c^+_{\mathsf{X},\mu_1}}{p_{\mu_1}}-\frac{e^{\mu_2}c^-_{\mathsf{X},\mu_2}}{p_{\mu_2}}\right)\right]\leq\epsilon^{c,+}_{\mathsf{X},\mu_1}+\epsilon^{c,-}_{\mathsf{X},\mu_2}} \tag{116}$$

Remark 14. *Ineqs.* (103), (110), (114) *and* (116) *are equivalent to the bounds derived in Ref. [27], except for the conditioning on* Ω_{EC} *in Eqs.* (110) *and* (114)*, which was not mentioned in Ref. [27]. For the derivation of the bounds for the 2-decoy protocol based on Ref. [26], we refer to App. A.2.*

Remark 15. *All equations from this section remain valid if the bases used for the key distribution and parameter estimation are swapped. For example, although not explicitly shown,* $s^-_{\mathsf{X},1}$ *is given by replacing* Z *by* X *in Eq.* (114)*. This is needed to calculate the upper bound on the single-photon QBER* Λ_{X} *and thus the phase error rate* Λ_{Z}*.*

5.2 Upper bound on the phase error rate

We recall that in Sec. 4.4 we have derived a bound on the phase error rate in terms of the single-photon QBER using Serfling's inequality, cf. Eq. (74). The acceptance test requires to verify $\Lambda^+_{\mathsf{X}}\leq\Lambda^{\mathrm{u}}_{\mathsf{X}}$. An upper bound on the single-photon QBER is explicitly given by[37]

$$\boxed{\Pr\left[\Lambda_{\mathsf{X}}>\Lambda^+_{\mathsf{X}}\coloneqq\frac{v^+_{\mathsf{X},1}}{s^-_{\mathsf{X},1}}\right]\leq\Pr\left[v_{\mathsf{X},1}>v^+_{\mathsf{X},1}\right]+\Pr\left[s_{\mathsf{X},1}<s^-_{\mathsf{X},1}\right]\,,} \tag{117}$$

which corresponds to an upper bound on the probability that one of the bounds, $v^+_{\mathsf{X},1}$ or $s^-_{\mathsf{X},1}$, fails. We note that $s^-_{\mathsf{X},1}$ is given by replacing Z by X in Eq. (114). Now that we have operational expressions for the decoy bounds $s^-_{\mathsf{Z},0}$, $s^-_{\mathsf{Z},1}$, $s^-_{\mathsf{X},1}$ and Λ^+_{X}, the acceptance test described in Sec. 2.1.2 and Fig 2 can be performed on these bounds.

6 Extractable secure-key length

The first term in Eq. (20) has been treated in Sec. 3.1 by bounding branch (a) from Fig. 3 using the properties of universal$_2$ hashing. In Sec. 2.3.4, we have split the second term in terms of the decoy concentration inequalities holding (branch (b)) and not holding (branch (c)). As seen in Sec. 4, the quantum leftover hash lemma provides a bound on branch (b) in terms of the smooth min-entropy and the secure-key length, cf. Eq. (80). Hence, the last term we need to bound is branch (c) and will be addressed in Sec. 6.1 using the decoy bounds derived in last section. We then derive an operational expression on the secure-key length solely in terms of the acceptance parameters, which we further simplify in Sec. 6.2.

6.1 Operational expression for the secure-key length

After the error correction, error verification steps and acceptance test, Alice and Bob disclosed $\mathrm{leak}_{\mathrm{EC}}+\log_2\frac{2}{\epsilon_{\mathrm{cor}}}$ bits of information through the classical channel and possess a verified key pair Z_A and Z_B, cf. Sec 3.1. During the acceptance test, they check the observed statistics derived in Sec. 5 against pre-defined parameters, namely they verify that $s^-_{\mathsf{Z},0}\geq s^{\mathrm{l}}_{\mathsf{Z},0}$, $s^-_{\mathsf{Z},1}\geq s^{\mathrm{l}}_{\mathsf{Z},1}$, $s^-_{\mathsf{X},1}\geq s^{\mathrm{l}}_{\mathsf{X},1}$ and $\Lambda^+_{\mathsf{X}}\leq\Lambda^{\mathrm{u}}_{\mathsf{X}}$, cf.

[37] We note that this bound is not tight if $k^{\mathsf{X}}_{\min}=\mu_1$ as then $v^+_{\mathsf{X},1}$ is not independent of $s^-_{\mathsf{X},1}$. In this case, the expression can be optimized by removing one contribution $\epsilon^{c,+}_{\mathsf{X},\mu_1}$.

Sec. 5.2 and Table 1. If at least one of the conditions does not hold, the protocol aborts, as discussed in Sec. 2.1 and Fig. 2.

In order to derive the decoy bounds, Hoeffding's inequalities, cf. Eqs. (92) to (97), have been used multiple times. Hence, as discussed in Sec. 5, the resulting bounds have a probability of not holding upper-bounded by Eqs. (103), (114) and (117). An illustration visualizing the different contributions is depicted in Fig. 6. Using this, we can determine an upper-bound on branch (c), i.e. for the probability for at least one of the Hoeffding inequalities failing, cf. Eq. (25), by summing over all contributions, yielding

$$\Pr[\neg\Omega_{\mathrm{B}}\wedge\Omega_{\mathrm{EC}}] \leq \epsilon^{n,-}_{\mathsf{Z},\mu_2}+\epsilon^{n,+}_{\mathsf{Z},\mu_1}+\epsilon^{c,+}_{\mathsf{Z},k^{\mathsf{Z}}_{\min}}+\epsilon^{v,+}_{\mathsf{Z},0}+\epsilon^{c,+}_{\mathsf{X},k^{\mathsf{X}}_{\min}}+\epsilon^{v,+}_{\mathsf{X},0}+\epsilon^{n,-}_{\mathsf{X},\mu_2}+\epsilon^{n,+}_{\mathsf{X},\mu_1}+\epsilon^{c,+}_{\mathsf{X},\mu_1}+\epsilon^{c,-}_{\mathsf{X},\mu_2} =: \Delta_{\mathrm{ci}}\,, \tag{118}$$

where contributions appearing twice are only counted once because if a Hoeffding inequality holds, it holds for all occurences. We implicitly used that $\Pr[\neg\Omega_{\mathrm{B}}\wedge\Omega_{\mathrm{EC}}] \leq \Pr[\neg\Omega_{\mathrm{B}}\,|\,\Omega_{\mathrm{EC}}]$ and $\Pr[\neg\Omega_{\mathrm{B}}\wedge\Omega_{\mathrm{EC}}] \leq \Pr[\neg\Omega_{\mathrm{B}}]$. We thus directly have a bound on branch (c) as $\Pr[\tilde{\Omega}\wedge\neg\Omega_{\mathrm{B}}] \leq \Pr[\neg\Omega_{\mathrm{B}}\wedge\Omega_{\mathrm{EC}}]$. Substituting Eq. (118) in Eq. (80), we can write

$$\Pr[\tilde{\Omega}]d_{\mathrm{sec}}(SEC)_{\rho|\tilde{\Omega}} \leq 2(\alpha_2+\nu)+\Delta^{\zeta}_{\mathrm{pa}}+\Delta_{\mathrm{ci}} \leq \epsilon'_{\mathrm{sec}}\,, \tag{119}$$

and the parameter ϵ'_{sec} is similarly defined to the secrecy parameter ϵ_{sec}, which corresponds to the second term in the expanded definition of security, cf. Eq. (20), as discussed in Remark 6. An operational expression for ϵ'_{sec} is given by adding the contributions, yielding

$$\epsilon'_{\mathrm{sec}} = \underbrace{2\nu}_{\text{Serfling's inequality}} + \underbrace{2\alpha_2}_{\text{Chain rule}} + \underbrace{\Delta^{\zeta}_{\mathrm{pa}}}_{\text{Privacy amplification}} + \underbrace{\Delta_{\mathrm{ci}}}_{\text{Concentration inequalities}}\,. \tag{120}$$

The term ν results from the use of Serfling's inequality to bound the single-photon phase error rate using the single-photon QBER, cf. Sec. 4.4.3. The terms α_2 and ν result from optimizing the min-entropy in an ζ-ball around ρ_{ZE} (see Sec. 4.4) and thus represent the probability that the optimized density operator $\bar{\rho}_{ZE}$ can be distinguished from ρ_{ZE}. The term $\Delta^{\zeta}_{\mathrm{pa}}$ results from the privacy amplification itself and originates from the quantum leftover hash lemma for min-entropies, cf. Eq. (50). Finally, Δ_{ci} represents the probability that the decoy bounds, as derived in Sec. 5 and discussed above, fail.

Substituting the definition of $\Delta^{\zeta}_{\mathrm{pa}}$, cf. Eq. (50), into Eq. (119), using the bound on the min-entropy, cf. Eq. (78), and isolating l yields an expression for the maximum extractable secure-key length, as given in Theorem 2. We have thus bounded both terms in the expanded definition in security, cf. Eq. (20), i.e. all branches in Fig. 3, such that the protocol described in Sec. 2.1.2, which either aborts or generates a key of length l, is ϵ-secure. We recall that the length l of the key should be fixed before the protocol run, during the parameter agreement step.

Theorem 2. *The protocol described in Fig. 2 is ϵ-secure, where $\epsilon_{\mathrm{cor}}+\epsilon'_{\mathrm{sec}} \leq \epsilon$, if the length of the secure key output when the protocol does not abort is*

$$\boxed{l = \left\lfloor s^{\mathrm{l}}_{\mathsf{Z},0}+s^{\mathrm{l}}_{\mathsf{Z},1}(1-h(\Lambda^{\mathrm{u}}_{\mathsf{X}}+\gamma))-\mathrm{leak}_{\mathrm{EC}}-\log_2\frac{4}{\epsilon_{\mathrm{cor}}\alpha_2^2}-2\log_2\frac{1}{2(\epsilon'_{\mathrm{sec}}-2\zeta'-\Delta_{\mathrm{ci}})}\right\rfloor}\,, \tag{121}$$

where $\zeta'=\alpha_2+\nu$, the acceptance parameters $s^{\mathrm{l}}_{\mathsf{Z},0}$, $s^{\mathrm{l}}_{\mathsf{Z},1}$ and $\Lambda^{\mathrm{u}}_{\mathsf{X}}$ are fixed before the protocol run, cf. Fig. 2, $\gamma=\gamma(\nu,s^{\mathrm{l}}_{\mathsf{Z},1},s^{\mathrm{l}}_{\mathsf{X},1})$ is given by Eq. (73), and $\mathrm{leak}_{\mathrm{EC}}$ is the number of bits leaked for error correction. The terms appearing in the above expression can be set to arbitrary values (e.g. to the maximize the secure-key length) such that $2\zeta'+\Delta^{\zeta}_{\mathrm{pa}}+\Delta_{\mathrm{ci}} \leq \epsilon'_{\mathrm{sec}}$ and $\epsilon_{\mathrm{cor}}+\epsilon'_{\mathrm{sec}} \leq \epsilon$.

Proof. The proof for ϵ'_{sec}-secrecy is given above, cf. Eq. (119), while the ϵ_{cor}-correctness follows from Theorem 1. Then the protocol is ϵ-secure following Eq. (20). □

For each term appearing in the above equation, we have plugged in the value minimizing the secure-key length that satisfies the conditions imposed by the acceptance set Q. In our case, this can be done

analytically as the secure-key length is monotonously dependent on the observed statistics. As such, the value minimizing the secure-key length is either a lower or upper bound on the observed statistics. This also explains why the acceptance set has been specifically chosen as described in Fig. 2. We can see that the smooth min-entropy has an operational meaning in the sense that it is an upper bound on the number of secret bits Alice can extract from Z.

Note that the expression for secure-key length in Eq. (121) may in principle be negative for certain parameters. However, without loss of generality, we assume that the parameters defining the protocol are chosen such that the resulting secure-key length is strictly positive (which can always be evaluated in advance using Eq. (121) as we are considering a fixed-length protocol).

6.2 Simplified expression for the secure-key length

We may simplify Eq. (121) by setting the terms α_2, ν, $\Delta^{\zeta}_{\mathrm{pa}}$ and error terms in Δ_{ci} to a common value ϵ_0. This reduces Eq. (120) to $\epsilon'_{\mathrm{sec}} = 15\epsilon_0$. This expression can be plugged back into Eq. (121), where

$$\epsilon'_{\mathrm{sec}} - 2\zeta' - \Delta_{\mathrm{ci}} = \epsilon_0 = \frac{\epsilon'_{\mathrm{sec}}}{15}\,, \tag{122}$$

yielding

$$\boxed{l = s^{\mathrm{l}}_{\mathsf{Z},0} + s^{\mathrm{l}}_{\mathsf{Z},1}(1 - h(\Lambda^{\mathrm{u}}_{\mathsf{X}} + \gamma)) - \mathrm{leak}_{\mathrm{EC}} - \log_2 \frac{2}{\epsilon_{\mathrm{cor}}} - 4\log_2 \frac{15}{\epsilon'_{\mathrm{sec}}\sqrt[4]{2}}\,,} \tag{123}$$

where we have set $\zeta' = 2\epsilon_0$ and $\Delta_{\mathrm{ci}} = 10\epsilon_0$. We note that the bound on the secure-key length is slightly tighter than in the original works [26, 27], as we have directly removed the multi-photon event register in the min-entropy in Eq. (62) without using the chain rule, leading to $\epsilon'_{\mathrm{sec}} = 15\epsilon_0$ instead of $\epsilon'_{\mathrm{sec}} = 19\epsilon_0$ [27] and the last term in Eq. (122) instead of $6\log_2(19/\epsilon'_{\mathrm{sec}})$ [27]. The same optimization is done for the 2-decoy state protocol and an expression for the secure-key length of the 2-decoy variant is derived in App. A.2. Essentially, the security proof for the 2-decoy state protocol only differs from the 1-decoy state protocol in the decoy bounds used to perform the acceptance test.

The secure-key rate is simulated using the simplified expression, Eq. (123), and depicted as a function of the channel attenuation for various numbers of signals sent N and for various block sizes N_{Z}, cf. Fig. 5. We recall that the block size is defined as the number of Z-basis detections remaining after sifting, i.e. the size of the block used for post-processing. In this case, either N is fixed and N_{Z} variable or the other way around[38]. At each point, the free parameters μ_1, μ_2, p_{μ_1} and p^A_{X} are optimized to maximize the secure-key rate, cf. Fig. 2. For simplicity, we set Alice's and Bob's basis choice probabilities to be equal. We assume a 625 MHz repetition rate for Alice, 200 Hz dark-count rate for Bob and a probability of error (i.e. misalignment) of 2 %. We use Eq. (31) to simulate the error correction cost and set the error correction inefficiency to $f_{\mathrm{EC}} = 1.16$. Finally, we set the security parameters to $\epsilon_{\mathrm{sec}} = \epsilon_{\mathrm{cor}} = 10^{-12}$. Under these conditions, we observe that we can reach about 50 dB attenuation for a block size of $N_{\mathsf{Z}} = 10^7$, which corresponds to about 250 km at 0.2 dB/km. The asymptotic case, $N = \infty$, directly follows from Eq. (123) as all correction terms which do not scale with N disappear, cf. Appendix A.7.

Remark 16. *We can observe that for a given ϵ'_{sec} and ϵ_{cor}, multiple variables can be optimized in Eqs. (120) and (121), namely ν, α_2 and the different ϵ-terms. They can be adjusted individually to maximize l as long as $2\zeta' + \Delta^{\zeta}_{\mathrm{pa}} + \Delta_{\mathrm{ci}} \leq \epsilon'_{\mathrm{sec}}$.*

Remark 17. *A comparison of the mathematical tools underlying different proof techniques, i.e. entropic uncertainty relation, entropy-accumulation-theorem-based and post-selection technique, is provided in Ref. [100]. A comparison of the performance of our work with the recently published marginal-constrained entropy accumulation theorem (MEAT) framework [101] can be found in Ref. [102], while a comparison with both the MEAT and the post-selection technique can be found in Ref. [103].*

[38] We recall that in practice N and N_{Z} must be fixed prior to running the protocol.

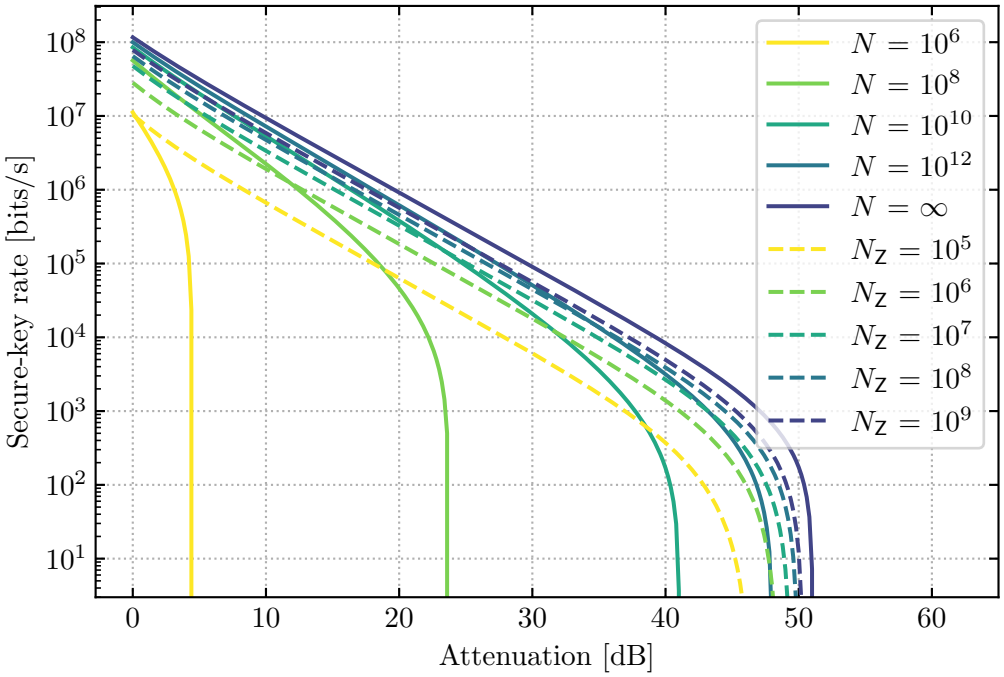


Figure 5: Secure-key rate as a function of the attenuation for various numbers of signals sent N and block sizes N_Z, computed using Eq. (123). At each point, the parameters μ_1, μ_2, p_{μ_1} and p_X^A are optimized to maximize the secure-key rate. The values for the various protocol parameters are listed in the main text.

7 Discussion

This section serves as a general discussion about the 1-decoy and 2-decoy state BB84 protocols as well as Renner's EUR framework and dwelves into insights often omitted from security proofs.

Impact of noise on performance. One notable difference between the 1-decoy and 2-decoy state protocols, which was not discussed in Ref. [27], is their resilience in regards to noise. In fact, for the 1-decoy state protocol, the upper bound on the number of vacuum events, i.e. Eq. (110), directly depends on the number of errors in the basis. This means that the advantage of this approach, which avoids sending the vacuum state itself, is best achieved in experiments with low noise. In fact, an increase in noise impacts this protocol twice; first in the single-photon QBER, Eq. (117), and second in the lower bound on the number of single-photon events, Eq. (114). In contrast, for the 2-decoy state protocol, the number of errors only appears once, namely in the bound for the single-photon QBER, cf. App. A.2.

Numerical analysis. When performing numerical simulations, particular caution should be taken regarding the accepted range for the bounds on the number of photon events and errors as well as the phase error rate. In fact, the bounds should be clipped when exceeding their allowed range. The lower bounds, Eqs. (93), (97), (103), (114), can, in theory, be negative and should, in this case, be clipped to zero. Additionally, in numerical simulations, one usually optimized the parameters from the parameter agreement step to maximize the secure-key rate, cf. Sec. 2.1.2. For this optimization, the error terms fom Eq. (118) are often set to a common value, which significantly reduced the degrees of freedom and results in Eq. (123). However, in principle, one can use the more general expression, cf. Eq. (121), and optimize the full set of error terms to yield higher secure-key rates, albeit increasing the complexity of the numerical optimizations.

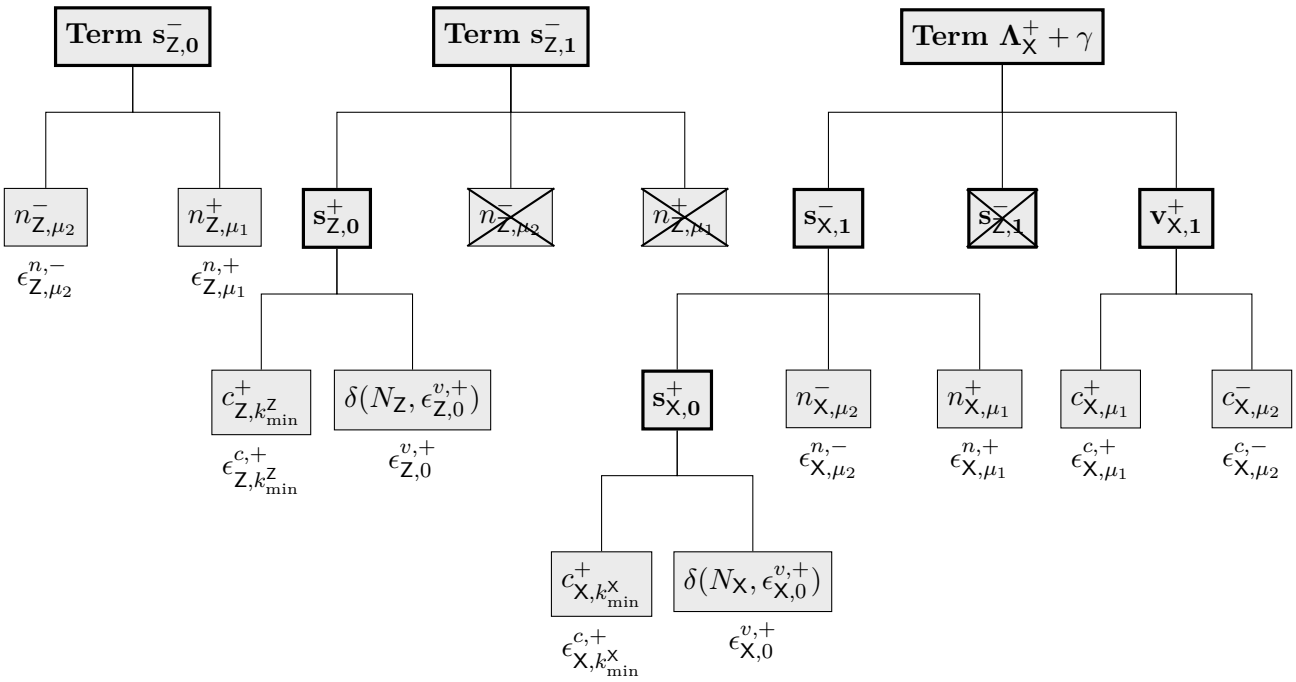


Figure 6: Illustration of finite-size effects appearing in the bound on the min-entropy (Eq. (78)) and their contribution to Eq. (118). The crossed-out boxes correspond to terms that appear twice and are thus only counted once.

EUR framework limitations. Two important considerations must be kept in mind when applying the EUR in Sec. 4.4.3. First, in order to write down the EUR statement, we require an active basis choice on Alice's side. Second, we assume that Eve's attack strategy does not depend on Alice's and Bob's basis choice to estimate the phase error rate in the Z-basis from the single-photon QBER in the X-basis using statistical sampling. This requires that Alice prepares perfect states, i.e. her basis choice is not leaked to Eve via the state she prepares. This also requires that the detection probabilities are equal on Bob's side. Various implementation designs and device imperfections lead to exploitable asymmetric losses between the bases, which conflicts with this assumption. Examples include detection-efficiency mismatch or dark count rate mismatch. We note that a recent work resolves this long-standing limitation of the EUR framework on the detector side for active basis choices [37].

Reverse error correction. Finally, we note that reverse error correction, a commonly used post-processing variant where Alice corrects her key to match Bob's, is not straightforward to incorporate in this security proof framework. Indeed, Eve can influence Bob's detection outcomes and thus directly affect the sifted key if reverse error correction is used. Throughout the analysis, the number of m-photon events refers to the photon number distribution leaving Alice's system, cf. Sec. 5.1. Now, if reverse error correction is used, this discussion does not hold anymore. For example, in this context it is not possible to assume that Eve has no information about the vacuum events, which was used in Sec. 4.4.1, as she may influence Bob's detections and Alice corrects her key to match Bob's. Even if the vacuum events are assumed to be unsafe, and thus the vacuum term left out, the use of the EUR is not directly justified in this context. In contrast, with forward error correction, the verified key is effectively Alice's sifted key, as Bob corrects his key to match hers, simplifying the theoretical analysis as Eve cannot influence Alice's state preparation under the assumptions listed in App. A.1. Therefore, we advise practical implementations based on this framework (which also include the works [26,27,36]) to employ forward error correction.

8 Conclusion

In this work, we consolidate the security proof for the 1-decoy and 2-decoy state BB84 protocol by formulating it in a rigorous yet accessible manner in Renner's entropic uncertainty relation framework. By addressing technical inconsistencies and unclarities in existing works, we refine the proof with a unified language, rigorously handling the conditioning on states and thoroughly discussing the error terms. Additionally, we provide a rigorous treatment for fixed-length protocols, an aspect overlooked in previous analyses [26, 27]. An important distinction, previously unaddressed, concerns the 1-decoy state protocol's acceptance test, which is performed after error correction. We rigorously discuss and resolve these issues in our analysis. By providing a constructive approach, beginning with the general definition of security, and, bounding each term separately, we offer a clear outline and step-by-step framework for the proof. We unify the ideas developed in various works to form a robust reference for practical implementations of the protocol, and a basis for further discussions of the underlying assumptions and potential vulnerabilities.

While this security proof serves as a solid starting point for any practical implementation wishing to use the decoy-state BB84 protocol, it is important to note that side-channel attacks, resulting from device imperfections, are not modeled in the security proof. Prominent attacks such as the Trojan-horse attack [104, 105] or detector-efficiency mismatch attack [37, 106] can be incorporated into the security proof by relaxing the assumptions about the devices. On the hardware side, QKD systems often either require adjustments or additional components, such as optical isolators and filters, that need to be precisely characterized[39]. A recent study by the German Federal Office for Information Security (BSI) [38] lists most known side-channel attacks and their countermeasures. Unfortunately, these attacks are often neglected [40, 41] and thus compromise the security claims. Incorporating the most critical side-channel attacks into a complete security proof would form the natural next step towards bridging the gap between theory and experiment. While significant effort has been devoted to combining different countermeasures, developing a security proof encompassing most of today's known attacks is far from trivial and remains an open task.

Acknowledgements

We would like to thank Shlok Nahar, Víctor Zapatero, Davide Orsucci, Jonas Treplin and Benedikt Leible for valuable comments on the first version of the manuscript. We thank Ernest Y.-Z. Tan for pointing out that reverse error correction may not be trivial to apply in this framework. We also thank Andy Schreier and Hermann Kampermann for engaging in fruitful discussions. For semantical polishing of the introduction and conclusion, large language models were used. This research was conducted within the scope of the QuNET-initiative, funded by the German Federal Ministry of Education and Research (BMBF). D.R. thanks the Galician Regional Government (consolidation of Research Units: AtlantTIC), MICIN with funding from the European Union NextGenerationEU (PRTR-C17.I1) and the Galician Regional Government with own funding through the "Planes Complementarios de I+D+I con las Comunidades Autónomas" in Quantum Communication and The European Union's Horizon Europe Framework Programme under the project "Quantum Security Networks Partnership" (QSNP, grant agreement No 101114043). This work was also funded by the NSERC Discovery Grant, and was partially conducted at the Institute for Quantum Computing, University of Waterloo, which is funded by Government of Canada through ISED. D.T. is partially funded by the Mike and Ophelia Lazaridis Fellowship.

[39] Alternatively, one can opt for a different protocol, such as measurement-device-independent QKD [32] or device-independent QKD [76].

Author contributions

J.K. and N.W. proposed and supervised the research. J.W. and J.K. performed the research for the first version of the manuscript. J.W. wrote the first draft of the manuscript. J.W. and J.K. edited the manuscript. J.W., J.K., D.R. and N.W. discussed and reviewed the first version of the manuscript. N.L. and D.T. were brought onto the project during the second version of the manuscript to address subtleties and enhance its rigor. J.W. and D.T. led the editing of the second version, implementing a series of improvements that clarified and strengthened the arguments. All authors reviewed and approved the updated manuscript for finalization.

Software availability

The code used to generate Fig. 5 is openly available at [107].

A Appendix

A.1 Model assumptions

This section provides a list of assumptions that have been used in the security proof. References to further readings are provided for most items. We recall the fundamental assumptions of quantum key distribution [12, Sec. IV]:

1. Quantum physics is a correct and complete theory.
2. The classical channel used by Alice and Bob is authenticated.
3. The devices used during the protocol behave in a fully predictable and controllable manner.

Following the last point, we assume that no device imperfections and thus no side-channels are present [38, 40, 41]. Specifically, we make the following adversarial and model assumptions:

1. Eve has only access to the classical and quantum channel, but not to the sender and receiver devices, nor to their environment. She may perform any attack allowed by quantum mechanics, i.e. including coherent attacks.
2. The transmitted signals are uniformly phase-randomized and coherent [108]. Eve has no a priori information about Alice's intensity choice. Thus, we can write Alice's signals as a coherent superposition of Fock states [93]

$$\rho_k = \sum_{m=0}^{\infty} e^{-k} \frac{k^m}{m!} |m\rangle\langle m| \ . \tag{124}$$

3. The X and Z bases are perfectly diagonal, i.e. the quality factor is $q = 1$, cf. [36].
4. Eve's attack strategy does not depend on Alice and Bob's basis choices. Eve has no a priori knowledge about the basis choices. This implies basis-independent losses, i.e. no detection-efficiency mismatch nor dark-count rate mismatch [37].
5. Alice has access to a true randomness source (e.g. when choosing the error verification and privacy amplification hash functions or for state encoding).

A.2 Bounds for the 2-decoy state protocol

In the case where two decoy states are used, also known as *2-decoy state protocol*, Alice can choose between three intensities when preparing her states, namely μ_1, μ_2 and μ_3, for which $\mu_1 > \mu_2 + \mu_3$ and $\mu_2 > \mu_3 \geq 0$ [26, 91]. The security proof is done analogously to the 1-decoy security proof with the exception that the bounds on photon events and errors differ, leading to different terms for Δ_{ci} in Eq. (118). In this section, we will first derive the relevant bounds and finally determine Δ_{ci} in the case of two decoy states. The derivation of the bounds is based on Ref. [91, Sec. 3.1].

A.2.1 Lower bound for the vacuum events

In full analogy to Sec. 5.1.1, by replacing μ_1 by μ_2 and μ_2 by μ_3, we can derive a lower bound for the number of vacuum event

$$\frac{\mu_2 e^{\mu_3} n^*_{\mathsf{Z},\mu_3}}{p_{\mu_3}} - \frac{\mu_3 e^{\mu_2} n^*_{\mathsf{Z},\mu_2}}{p_{\mu_2}} = \frac{(\mu_2 - \mu_3) s_{\mathsf{Z},0}}{\tau_0} - \mu_2 \mu_3 \sum_{m=2}^{\infty} \frac{(\mu_2^{m-1} - \mu_3^{m-1}) s_{\mathsf{Z},m}}{\tau_m m!}\,, \tag{125}$$

yielding

$$\boxed{\Pr\left[s_{\mathsf{Z},0} < s^-_{\mathsf{Z},0}\right] \leq \epsilon^{n,-}_{\mathsf{Z},\mu_3} + \epsilon^{n,+}_{\mathsf{Z},\mu_2}\,,} \tag{126}$$

where

$$s^-_{\mathsf{Z},0} \coloneqq \frac{\tau_0}{(\mu_2 - \mu_3)} \left(\frac{\mu_2 e^{\mu_3} n^-_{\mathsf{Z},\mu_3}}{p_{\mu_3}} - \frac{\mu_3 e^{\mu_2} n^+_{\mathsf{Z},\mu_2}}{p_{\mu_2}} \right). \tag{127}$$

A.2.2 Lower bound for the vacuum events

Analogously to Sec. 5.1.3, we can write

$$\begin{aligned} \frac{e^{\mu_2} n^*_{\mathsf{Z},\mu_2}}{p_{\mu_2}} - \frac{e^{\mu_3} n^*_{\mathsf{Z},\mu_3}}{p_{\mu_3}} &= \frac{(\mu_2 - \mu_3) s_{\mathsf{Z},1}}{\tau_1} + \sum_{m=2}^{\infty} \frac{(\mu_2^m - \mu_3^m) s_{\mathsf{Z},m}}{\tau_m m!} \\ &\leq \frac{(\mu_2 - \mu_3) s_{\mathsf{Z},1}}{\tau_1} + \frac{\mu_2^2 - \mu_3^2}{\mu_1^2} \sum_{m=2}^{\infty} \frac{\mu_1^m s_{\mathsf{Z},m}}{\tau_m m!} \end{aligned}$$

as we can write

$$\mu_2^m - \mu_3^m = \frac{\mu_2^2 - \mu_3^2}{\mu_2 + \mu_3} \sum_{i=0}^{m-1} \mu_2^{m-i-1} \mu_3^i \leq (\mu_2^2 - \mu_3^2)(\mu_2 + \mu_3)^{m-2} \leq (\mu_2^2 - \mu_3^2)\mu_1^{m-2}\,,$$

for $m \geq 2$ where the last inequality holds for $\mu_2 + \mu_3 \leq \mu_1$ and $\sum_{i=0}^{m-1} \mu_2^{m-i-1}\mu_3^i \leq (\mu_2 + \mu_3)^{m-1}$ for $m \geq 2$ has been used, which directly follows from the binomial theorem. This can easily be proven by induction. Now, writing the sum of multi-photon events ($m \geq 2$) as

$$\sum_{m=2}^{\infty} \frac{\mu_1^m s_{\mathsf{Z},m}}{\tau_m m!} = \sum_{m=2}^{\infty} \frac{e^{\mu_1} e^{-\mu_1} p_{\mu_1} \mu_1^m s_{\mathsf{Z},m}}{p_{\mu_1} \tau_m m!} = \frac{e^{\mu_1} n^*_{\mathsf{Z},\mu_1}}{p_{\mu_1}} - \frac{s_{\mathsf{Z},0}}{\tau_0} - \frac{\mu_1 s_{\mathsf{Z},1}}{\tau_1} \tag{128}$$

by using Eqs. (99) and (89) yields

$$\frac{e^{\mu_2} n^*_{\mathsf{Z},\mu_2}}{p_{\mu_2}} - \frac{e^{\mu_3} n^*_{\mathsf{Z},\mu_3}}{p_{\mu_3}} \leq \frac{(\mu_2 - \mu_3) s_{\mathsf{Z},1}}{\tau_1} + \frac{\mu_2^2 - \mu_3^2}{\mu_1^2} \left(\frac{e^{\mu_1} n^*_{\mathsf{Z},\mu_1}}{p_{\mu_1}} - \frac{s_{\mathsf{Z},0}}{\tau_0} - \frac{\mu_1 s_{\mathsf{Z},1}}{\tau_1} \right). \tag{129}$$

Finally, solving for $s_{\mathsf{Z},1}$ yields

$$s_{\mathsf{Z},1} \geq \frac{\mu_1 \tau_1}{\mu_1(\mu_2 - \mu_3) - (\mu_2^2 - \mu_3^2)} \left(\frac{e^{\mu_2} n^*_{\mathsf{Z},\mu_2}}{p_{\mu_2}} - \frac{e^{\mu_3} n^*_{\mathsf{Z},\mu_3}}{p_{\mu_3}} + \frac{\mu_2^2 - \mu_3^2}{\mu_1^2} \left(\frac{s_{\mathsf{Z},0}}{\tau_0} - \frac{e^{\mu_1} n^*_{\mathsf{Z},\mu_1}}{p_{\mu_1}} \right) \right) \tag{130}$$

and using $\mu_1(\mu_2-\mu_3)-(\mu_2^2-\mu_3^2)=(\mu_1-\mu_3+\mu_2)(\mu_2-\mu_3)>0$ we find

$$\boxed{\Pr\left[s_{\mathsf{Z},1}<s^-_{\mathsf{Z},1}\right]\leq \epsilon^{n,-}_{\mathsf{Z},\mu_2}+\epsilon^{n,+}_{\mathsf{Z},\mu_3}+\epsilon^{n,+}_{\mathsf{Z},\mu_1}+\epsilon^{n,-}_{\mathsf{Z},\mu_3}+\epsilon^{n,+}_{\mathsf{Z},\mu_2}\,,} \tag{131}$$

where

$$s^-_{\mathsf{Z},1}\coloneqq \frac{\mu_1\tau_1}{\mu_1(\mu_2-\mu_3)-(\mu_2^2-\mu_3^2)}\left(\frac{e^{\mu_2}n^-_{\mathsf{Z},\mu_2}}{p_{\mu_2}}-\frac{e^{\mu_3}n^+_{\mathsf{Z},\mu_3}}{p_{\mu_3}}+\frac{\mu_2^2-\mu_3^2}{\mu_1^2}\left(\frac{s^-_{\mathsf{Z},0}}{\tau_0}-\frac{e^{\mu_1}n^+_{\mathsf{Z},\mu_1}}{p_{\mu_1}}\right)\right). \tag{132}$$

A.2.3 Upper bound on the number of single-photon events

In complete analogy to Sec. 5.1.4, we can derive an upper bound on the number of single-photon events by replacing $\mu_1\to\mu_2$ and $\mu_2\to\mu_3$, leading to

$$\boxed{\Pr\left[v_{\mathsf{X},1}>v^+_{\mathsf{X},1}\right]\leq \epsilon^{c,+}_{\mathsf{X},\mu_2}+\epsilon^{c,-}_{\mathsf{X},\mu_3}\,,} \tag{133}$$

where

$$v^+_{\mathsf{X},1}\coloneqq \frac{\tau_1}{\mu_2-\mu_3}\left(\frac{e^{\mu_2}c^+_{\mathsf{X},\mu_2}}{p_{\mu_2}}-\frac{e^{\mu_3}c^-_{\mathsf{X},\mu_3}}{p_{\mu_3}}\right). \tag{134}$$

A.2.4 Security analysis

As discussed above, the security proof of the 2-decoy protocol solely differs from that of the 1-decoy regarding the bounds on the photon events and errors. As such, for the 2-decoy state protocol, the protocol description from Fig. 2 can be used with an additional intensity μ_3 and where the bounds derived above are used for the acceptance test. The proof can be performed analogously to the 1-decoy state protocol yielding

$$\Pr[\tilde{\Omega}]d_{\mathrm{sec}}(SEC)_{\rho|\tilde{\Omega}}\leq 2(\alpha_2+\nu)+\Delta^{\zeta}_{\mathrm{pa}}+\Delta_{\mathrm{ci}}\leq\epsilon'_{\mathrm{sec}}\,, \tag{135}$$

where we adjust the concentration inequality term using the bounds derived above,

$$\begin{aligned}\Delta_{\mathrm{ci}}=\;&\epsilon^{n,-}_{\mathsf{Z},\mu_2}+\epsilon^{n,+}_{\mathsf{Z},\mu_3}+\epsilon^{n,+}_{\mathsf{Z},\mu_1}+\epsilon^{n,-}_{\mathsf{Z},\mu_3}+\epsilon^{n,+}_{\mathsf{Z},\mu_2}+\epsilon^{n,-}_{\mathsf{X},\mu_2}+\epsilon^{n,+}_{\mathsf{X},\mu_3}\\&+\epsilon^{n,+}_{\mathsf{X},\mu_1}+\epsilon^{n,-}_{\mathsf{X},\mu_3}+\epsilon^{n,+}_{\mathsf{X},\mu_2}+\epsilon^{c,+}_{\mathsf{X},\mu_2}+\epsilon^{c,-}_{\mathsf{X},\mu_3}\,.\end{aligned} \tag{136}$$

Now, in analogy to Sec. 6, using Eq. (136) and setting all error terms to a common value yields an expression for the maximum extractable secure-key length in terms of ϵ_{cor} and ϵ'_{sec},

$$\boxed{l=s^{\mathrm{l}}_{\mathsf{Z},0}+s^{\mathrm{l}}_{\mathsf{Z},1}(1-h(\Lambda^{\mathrm{u}}_{\mathsf{X}}+\gamma))-\mathrm{leak}_{\mathrm{EC}}-\log_2\frac{2}{\epsilon_{\mathrm{cor}}}-4\log_2\frac{17}{\epsilon'_{\mathrm{sec}}\sqrt[4]{2}}\,.} \tag{137}$$

A.3 Intuition on the trace distance

Given two probability distributions P_Z and Q_Z, the probability of an event $z\in\mathcal{Z}$ occurring is given by $P_Z(z)$ and $Q_Z(z)$ respectively. The goal is to distinguish both probability distributions by correctly assigning a random sample $s\in\{z\}$ to the probability distribution it originated from. For this purpose, we introduce the *total variation distance* (called trace distance when generalized to density operators), defined as

$$TV(P_Z,Q_Z)\coloneqq\frac{1}{2}\sum_z|P_Z(z)-Q_Z(z)|\leq 1\,. \tag{138}$$

The definition above can be rewritten as (see Ref. [51, Eq. (9.3)])

$$TV(P_Z,Q_Z)=\max_{\Omega}\left|\sum_{z\in\Omega}P_Z(z)-\sum_{z\in\Omega}Q_Z(z)\right|, \tag{139}$$

where the maximization is taken over all subsets $\Omega \subseteq \{x\}$. In other words, the Ω for which the difference is maximized is the optimal event to consider when one wants to distinguish P_Z and Q_Z as it describes the event for which the probabilities of both probability distributions differ the most.

If the total variation distance is upper-bounded by ζ, i.e. $TV(P_Z, Q_Z) \leq \zeta$, it can be shown that the probability of assigning a sample s to the correct probability distribution is upper-bounded by (see Refs. [65, Sec. 9.1.4], [66, Sec. 2.4.2] and [64, Sec. 3.2.1])

$$P_{\text{distinguish}}(P_Z, Q_Z) \leq \frac{1}{2} + \frac{\zeta}{2}\,. \tag{140}$$

In other words, ζ describes the *distinguishing advantage* when trying to distinguish two probability distributions. In the special case where $\zeta = 0$, and thus both probability distributions yield equal results, one can only randomly assign s with a success rate of 50 %. In this case, both probability distributions are indistinguishable.

This concept also applies when density operators ρ and σ are considered instead of classical probability distributions. The generalization of the total variation distance to quantum states is discussed in Refs. [51, Sec. 9.2] and [64, Sec. 3.2].

A.4 Comparison between the von Neumann entropy and min-entropy

As a more conservative measure of entropy than the von Neumann entropy, the min-entropy outputs the entropy in the case where Eve is the most likely to guess the secure key. As an example, let n be the number of possible bit string combinations, $n = \dim \mathcal{S}$. Now, assuming that the j-th combination occurs 50% of the time and that the remaining $n-1$ strings are uniformly distributed with $p_i = \frac{1/2}{n-1}$, $i \neq j$. The von Neumann entropy yields

$$\begin{aligned} S(\rho) &= -\operatorname{Tr}\{\rho \log_2 \rho\} \\ &= -\sum_{i=1}^{n} p_i \log_2 p_i \\ &= -\frac{1}{2}\log_2 \frac{1}{2} - \sum_{i=1, i\neq j} \frac{1}{2(n-1)} \log_2 \frac{1}{2(n-1)} \\ &= \frac{1}{2}\log_2 \left(2(n-1)\right) + \frac{1}{2}\,. \end{aligned}$$

For $n = 2^{64}$, i.e. a 64-bit string, we find $S(\rho) \approx 33$. In contrast, the min-entropy Eq. (41) yields

$$H_{\min}(\rho) = -\log_2 p_{\text{guess}} = 1\,,$$

independently of n, where $p_{\text{guess}} = \frac{1}{2}$. The von Neumann entropy describes the average uncertainty of a system equivalently to the Shannon entropy, while the min-entropy solely assumes the outcome with highest probability, i.e. the case where the observer has the smallest uncertainty about the system and thus accounts for a more conservative entropy measure, which is assumed in the realm of quantum cryptography.

A.5 Derivation of the expression for the Hoeffding-delta

Hoeffding's inequality [98, Eq. (2.1)] states that for independent and identically distributed random variables $V_1, \ldots, V_n$, such that $0 \leq V_i \leq 1$,

$$P\left(\frac{1}{n}\sum_{i=1}^{n} V_i - E[V] > t\right) \leq \exp\left(-2nt^2\right), \tag{141}$$

where $E[V]$ is the common expectation value of each variables V_i and $t > 0$. In other words, Hoeffding's inequality states that, for a finite number of events n, the measured mean $\frac{1}{n}\sum_{i=1}^{n} V_i$ deviates by

more than t from the common expectation value with a probability no more than $\exp(-2nt^2)$. The expectation value is common to all variables V_i as they are independent and identically distributed. The expectation value for the sum of all random variables is then $nE[V]$, where n is the number of events considered. Now, if we choose $t = \tilde{\delta}(n,\epsilon) \coloneqq \sqrt{\frac{1}{2n}\ln\frac{1}{\epsilon}}$, then Hoeffding's inequality holds since

$$P\left(\frac{1}{n}\sum_{i=1}^{n} V_i - E[V] > \tilde{\delta}(n,\epsilon)\right) \leq \exp\left(-2n\tilde{\delta}(n,\epsilon)^2\right) \tag{142}$$

$$= \exp\left(-2n\frac{1}{2n}\ln\frac{1}{\epsilon}\right) \tag{143}$$

$$= \epsilon\,. \tag{144}$$

Note, however, that we are considering the expectation value of the sum of all variables and not the expectation value of each variable in Sec. 5.1. As the expectation value is common to all variables, we can use Ref. [98, Eq. (1.3)], effectively multiplying each term with n, yielding

$$P\left(\sum_{i=1}^{n} V_i - nE[V] > n\tilde{\delta}(n,\epsilon)\right) \leq \epsilon\,. \tag{145}$$

We can then define a new Hoeffding-delta

$$\delta(n,\epsilon) \coloneqq n\tilde{\delta}(n,\epsilon) = \sqrt{\frac{n}{2}\ln\frac{1}{\epsilon}}\,, \tag{146}$$

which fulfills the above equation. This choice of $\delta(n,\epsilon)$ is precisely the one introduced in Sec. 5.1. Note that from Ref. [98, Eq. (1.4)], using the symmetry of the bounds, we can state that

$$P\left(-\sum_{i=1}^{n} V_i + nE[V] > \delta(n,\epsilon)\right) \leq \epsilon \tag{147}$$

As an example, this corresponds to the cases

$$P\left(n_{\mathsf{Z},\mu_1} - n^*_{\mathsf{Z},\mu_1} > \delta(N_{\mathsf{Z}},\epsilon)\right) \leq \epsilon \tag{148}$$

and

$$P\left(n^*_{\mathsf{Z},\mu_1} - n_{\mathsf{Z},\mu_1} > \delta(N_{\mathsf{Z}},\epsilon)\right) \leq \epsilon \tag{149}$$

or, equivalently,

$$P\left(\left|n^*_{\mathsf{Z},\mu_1} - n_{\mathsf{Z},\mu_1}\right| > \delta(N_{\mathsf{Z}},\epsilon)\right) \leq 2\epsilon\,. \tag{150}$$

A.6 Scenario where Alice chooses the intensity after detection

If Alice sends m photons, then Eve's and Bob's detections are independent of the intensity μ_1 or μ_2 the m-photon event originates from. To illustrate this, consider the probability tree diagram depicted in Fig. 7. Let $p_e(m)$ represent Eve's influence on Bob's photon detections. Intuitively, as Eve cannot base her attack strategy on the intensity chosen, this term only depends on the number of photons sent m. Note that this is a simplification as $p_e(m)$ can also depend on other variables that are however not relevant for this discussion.

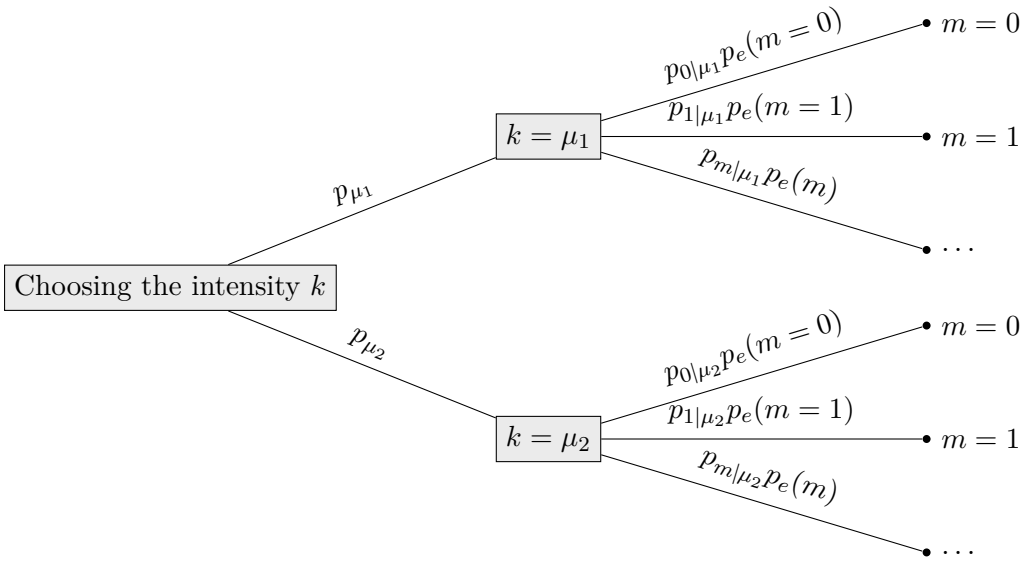


Figure 7: Probability tree diagram representing the different paths leading to an m-photon detection on Bob's side given the intensities μ_1 and μ_2. Here, $p_e(m)$ represents Eve's influence on Bob's detections due to her attack strategy.

In the case where Eve cannot base her attack strategy on the intensity chosen, the probability of the intensity μ_1 being chosen given that Bob detects m photons is given by using Bayes' theorem, cf. Eq. (99),

$$p_{\mu_1|m} = \frac{p_e(m) p_{\mu_1} p_{m|\mu_1}}{p_e(m) p_{\mu_1} p_{m|\mu_1} + p_e(m) p_{\mu_2} p_{m|\mu_2}} \tag{151}$$

$$= \frac{p_{\mu_1} p_{m|\mu_1}}{p_{\mu_1} p_{m|\mu_1} + p_{\mu_2} p_{m|\mu_2}} . \tag{152}$$

Intuitively, this represents the fraction of the paths originating from an intensity μ_1, given that m photons where detected, compared to all paths leading to the detection of an m-photon event.

This shows that assuming that Alice chooses the intensity k after an m-photon event was detected is mathematically equivalent to choosing the intensity before measuring an m-photon event. Now, if we were to assume that Eve could base her attack strategy on the level of intensity k chosen, then her influence $p_e(m, k)$ would depend on the level of intensity k in additional to m, yielding a new expression for $p_{\mu_1|m}$, namely

$$p_{\mu_1|m} = \frac{p_e(m, \mu_1) p_{\mu_1} p_{m|\mu_1}}{p_e(m, \mu_1) p_{\mu_1} p_{m|\mu_1} + p_e(m, \mu_2) p_{\mu_2} p_{m|\mu_2}} . \tag{153}$$

Here, the $p_e(m, k)$ terms do not cancel out and we could not determine $p_{k|m}$ solely as a function of $p_{m|k}$ and p_k using Bayes' theorem effectively meaning that both scenarios would not be equivalent.

A.7 Asymptotic secure-key rate

An expression for the asymptotic secure-key rate can be found based on the finite-size case. In the following, we use the simplified finite-size expression, cf. Eq. (123), but the same argument holds for Eq. (121). For a given channel and detection model, we denote the probability, each round, to detect a click in a basis a (which is not discarded) with intensity choice k as $p_{a,k}$. Similarly, we denote the probability for an error in a basis a with intensity choice k as $e_{a,k}$. As we are considering the asymptotic case, and therefore directly dealing with probabilities, concentration inequalities are not needed and the deviation terms from Eqs. (94) and (98) do not appear. Then, analogously to Sec. 5, we can derive

bounds on the probabilities for vacuum and single-photon events

$$Y^-_{\mathsf{Z},0} \coloneqq \frac{\tau_0}{(\mu_1-\mu_2)}\left(\frac{\mu_1 e^{\mu_2} p_{\mathsf{Z},\mu_2}}{p_{\mu_2}} - \frac{\mu_2 e^{\mu_1} p_{\mathsf{Z},\mu_1}}{p_{\mu_1}}\right), \tag{154}$$

$$Y^+_{a,0} \coloneqq 2\frac{e_{a,k}}{p_k}\tau_0 e^k, \tag{155}$$

$$Y^-_{a,1} \coloneqq \frac{\mu_1\tau_1}{\mu_2(\mu_1-\mu_2)}\left(\frac{e^{\mu_2} p_{a,\mu_2}}{p_{\mu_2}} - \frac{\mu_2^2}{\mu_1^2}\frac{e^{\mu_1} p_{a,\mu_1}}{p_{\mu_1}} - \frac{(\mu_1^2-\mu_2^2)}{\mu_1^2}\frac{Y^+_{a,0}}{\tau_0}\right), \tag{156}$$

where any $k \in \{\mu_1, \mu_2\}$ can be chosen, e.g. to maximize the secure-key rate. Analogously to the discussion in Sec. 5, the probability for a single-photon error is given by

$$E^+_{\mathsf{X},1} = \frac{\tau_1}{\mu_1-\mu_2}\left(\frac{e^{\mu_1} e_{\mathsf{X},\mu_1}}{p_{\mu_1}} - \frac{e^{\mu_2} e_{\mathsf{X},\mu_2}}{p_{\mu_2}}\right). \tag{157}$$

Then, the asymptotic secure-key rate is given by

$$r = Y^-_{\mathsf{Z},0} + Y^-_{\mathsf{Z},1}\left(1 - h\left(\frac{E^+_{\mathsf{X},1}}{Y^-_{\mathsf{X},1}}\right)\right) - h\left(e_{\mathsf{Z}}\right), \tag{158}$$

where the last term follows from Eq. (28) and e_{Z} is the probability of an error in the Z-basis, which is given by the channel and detection model. The asymptotic secure-key rate is plotted in Fig. 5 and compared to the finite-size regime.

References

[1] 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, 1978, doi:10.1145/359340.359342.

[2] W. Diffie and M. Hellman. New directions in cryptography. *IEEE Transactions on Information Theory*, 22(6):644–654, 1976, doi:10.1109/TIT.1976.1055638.

[3] N. Koblitz. Elliptic curve cryptosystems. *Mathematics of Computation*, 48(177):203–209, 1987, doi:10.1090/S0025-5718-1987-0866109-5.

[4] V. S. Miller. Use of elliptic curves in cryptography. In H. C. Williams, editor, *Advances in Cryptology — CRYPTO '85 Proceedings*, pages 417–426, Berlin, Heidelberg, 1986. Springer Berlin Heidelberg, doi:10.1007/3-540-39799-X_31.

[5] C. E. Shannon. Communication theory of secrecy systems. *The Bell System Technical Journal*, 28(4):656–715, 1949, doi:10.1002/j.1538-7305.1949.tb00928.x.

[6] W. K. Wootters and W. H. Zurek. A single quantum cannot be cloned. *Nature*, 299(5886):802–803, 1982, doi:10.1038/299802a0.

[7] P. Shor and J. Preskill. Simple Proof of Security of the BB84 Quantum Key Distribution Protocol. *Physical Review Letters*, 85:441–444, 2000, doi:10.1103/PhysRevLett.85.441.

[8] R. Canetti. Universally composable security: a new paradigm for cryptographic protocols. In *Proceedings 42nd IEEE Symposium on Foundations of Computer Science*, pages 136–145, 2001, doi:10.1109/SFCS.2001.959888.

[9] D. Mayers. Unconditional security in quantum cryptography. *J. ACM*, 48(3):351–406, 2001, doi:10.1145/382780.382781.

[10] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden. Quantum Cryptography. *Reviews of Modern Physics*, 74(1):145–195, 2002, doi:10.1103/RevModPhys.74.145.

[11] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dusek, N. Lütkenhaus, and M. Peev. The Security of Practical Quantum Key Distribution. *Reviews of Modern Physics*, 81(3):1301–1350, 2009, doi:10.1103/RevModPhys.81.1301.

[12] C. Portmann and R. Renner. Security in Quantum Cryptography. *Reviews of Modern Physics*, 94(2):025008, 2022, doi:10.1103/RevModPhys.94.025008.

[13] G. Brassard. Brief history of quantum cryptography: a personal perspective. In *IEEE Information Theory Workshop on Theory and Practice in Information-Theoretic Security*, page 19–23. IEEE, 2005, doi:10.1109/itwtpi.2005.1543949.

[14] C. H. Bennett and G. Brassard. Quantum cryptography: Public key distribution and coin tossing. *Theoretical Computer Science*, 560:7–11, 1984, doi:10.1016/j.tcs.2014.05.025.

[15] A. Boaron, G. Boso, D. Rusca, C. Vulliez, C. Autebert, M. Caloz, M. Perrenoud, G. Gras, F. Bussières, M.-J. Li, D. Nolan, A. Martin, and H. Zbinden. Secure Quantum Key Distribution over 421 km of Optical Fiber. *Physical Review Letters*, 121(19):190502, 2018, doi:10.1103/PhysRevLett.121.190502.

[16] C. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin. Experimental quantum cryptography. *Journal of Cryptology*, 1992, doi:10.1007/BF00191318.

[17] B. Huttner, N. Imoto, N. Gisin, and T. Mor. Quantum cryptography with coherent states. *Physical Review A*, 51(3):1863–1869, 1995, doi:10.1103/PhysRevA.51.1863.

[18] N. Lütkenhaus and M. Jahma. Quantum key distribution with realistic states: photon-number statistics in the photon-number splitting attack. *New Journal of Physics*, 4:44–44, 2002, doi:10.1088/1367-2630/4/1/344.

[19] W.-Y. Hwang. Quantum Key Distribution with High Loss: Toward Global Secure Communication. *Physical Review Letters*, 91(5):057901, 2003, doi:10.1103/PhysRevLett.91.057901.

[20] X.-B. Wang. Beating the photon-number-splitting attack in practical quantum cryptography. *Physical Review Letters*, 94(23):230503, 2005, doi:10.1103/PhysRevLett.94.230503.

[21] H.-K. Lo, X. Ma, and K. Chen. Decoy State Quantum Key Distribution. *Physical Review Letters*, 94(23):230504, 2005, doi:10.1103/PhysRevLett.94.230504.

[22] N. Lütkenhaus. Security against individual attacks for realistic quantum key distribution. *Physical Review A*, 61(5):052304, 2000, doi:10.1103/PhysRevA.61.052304.

[23] V. Scarani, A. Acín, G. Ribordy, and N. Gisin. Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations. *Physical Review Letters*, 92(5), 2004, doi:10.1103/physrevlett.92.057901.

[24] R. Renner. Security of quantum key distribution, 2005, doi:10.48550/arXiv.quant-ph/0512258.

[25] L. Kamin, A. Arqand, I. George, N. Lütkenhaus, and E. Y.-Z. Tan. Finite-Size Analysis of Prepare-and-Measure and Decoy-State Quantum Key Distribution via Entropy Accumulation. *PRX Quantum*, 6(2):020342, 2025, doi:10.1103/PRXQuantum.6.020342.

[26] 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(2):022307, 2014, doi:10.1103/PhysRevA.89.022307.

[27] D. Rusca, A. Boaron, F. Grünenfelder, A. Martin, and H. Zbinden. Finite-key analysis for the 1-decoy state QKD protocol. *Applied Physics Letters*, 112(17):171104, 2018, doi:10.1063/1.5023340.

[28] 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.

[29] X. Ma, B. Qi, Y. Zhao, and H.-K. Lo. Practical decoy state for quantum key distribution. *Physical Review A*, 72(1):012326, 2005, doi:10.1103/PhysRevA.72.012326.

[30] L. Kamin and N. Lütkenhaus. Improved decoy-state and flag-state squashing methods. *Physical Review Research*, 6(4):043223, 2024, doi:10.1103/PhysRevResearch.6.043223.

[31] A. Ekert. Quantum cryptography based on Bell's theorem. *Physical Review Letters*, 67:661–663, 1991, doi:10.1103/PhysRevLett.67.661.

[32] H.-K. Lo, M. Curty, and B. Qi. Measurement-device-independent quantum key distribution. *Physical Review Letters*, 108(13), 2012, doi:10.1103/physrevlett.108.130503.

[33] M. Lucamarini, Z. L. Yuan, J. F. Dynes, and A. J. Shields. Overcoming the rate–distance limit of quantum key distribution without quantum repeaters. *Nature*, 557(7705):400–403, 2018, doi:10.1038/s41586-018-0066-6.

[34] P. Zeng, H. Zhou, W. Wu, and X. Ma. Mode-pairing quantum key distribution. *Nature Communications*, 13(1):3903, 2022, doi:10.1038/s41467-022-31534-7.

[35] 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.

[36] M. Tomamichel, C. C. W. Lim, N. Gisin, and R. Renner. Tight finite-key analysis for quantum cryptography. *Nature Communications*, 3(1), 2012, doi:10.1038/ncomms1631.

[37] D. Tupkary, S. Nahar, P. Sinha, and N. Lütkenhaus. Phase error rate estimation in QKD with imperfect detectors. *Quantum*, 9:1937, 2025, doi:10.22331/q-2025-12-11-1937.

[38] German Federal Office for Information Security. Implementation Attacks against QKD Systems, 2024. `https://www.bsi.bund.de/EN/Service-Navi/Publikationen/Studien/QKD-Systems/Implementation_Attacks_QKD_Systems_node.html` Last accessed on 18-05-24.

[39] N. Jain, B. Stiller, I. Khan, D. Elser, C. Marquardt, and G. Leuchs. Attacks on practical quantum key distribution systems (and how to prevent them). *Contemporary Physics*, 57(3):366–387, 2016, doi:10.1080/00107514.2016.1148333.

[40] S. Sajeed, P. Chaiwongkhot, A. Huang, H. Qin, V. Egorov, A. Kozubov, A. Gaidash, V. Chistiakov, A. Vasiliev, A. Gleim, and V. Makarov. An approach for security evaluation and certification of a complete quantum communication system. *Scientific Reports*, 11(1):5110, 2021, doi:10.1038/s41598-021-84139-3.

[41] V. Makarov, A. Abrikosov, P. Chaiwongkhot, A. K. Fedorov, A. Huang, E. Kiktenko, M. Petrov, A. Ponosova, D. Ruzhitskaya, A. Tayduganov, D. Trefilov, and K. Zaitsev. Preparing a commercial quantum key distribution system for certification against implementation loopholes. *Physical Review Applied*, 22(4):044076, 2024, doi:10.1103/PhysRevApplied.22.044076.

[42] M. Tomamichel and R. Renner. The Uncertainty Relation for Smooth Entropies. *Physical Review Letters*, 106(11):110506, 2011, doi:10.1103/PhysRevLett.106.110506.

[43] S. Nahar, D. Tupkary, Y. Zhao, N. Lütkenhaus, and E. Y.-Z. Tan. Postselection technique for optical quantum key distribution with improved de finetti reductions. *PRX Quantum*, 5:040315, 2024, doi:10.1103/PRXQuantum.5.040315.

[44] M. Christandl, R. König, and R. Renner. Postselection Technique for Quantum Channels with Applications to Quantum Cryptography. *Physical Review Letters*, 102(2):020504, 2009, doi:10.1103/PhysRevLett.102.020504.

[45] T. Metger and R. Renner. Security of quantum key distribution from generalised entropy accumulation. *Nature Communications*, 14(1):5272, 2023, doi:10.1038/s41467-023-40920-8.

[46] M. Koashi. Simple security proof of quantum key distribution based on complementarity. *New Journal of Physics*, 11(4):045018, 2009, doi:10.1088/1367-2630/11/4/045018.

[47] S. Pirandola, U. L. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck, D. Englund, T. Gehring, C. Lupo, C. Ottaviani, J. Pereira, M. Razavi, J. S. Shaari, M. Tomamichel, V. C. Usenko, G. Vallone, P. Villoresi, and P. Wallden. Advances in Quantum Cryptography. *Advances in Optics and Photonics*, 12(4):1012, 2020, doi:10.1364/AOP.361502.

[48] R. Wolf. *Quantum Key Distribution: An Introduction with Exercises*, volume 988. Springer International Publishing, Cham, 2021, doi:10.1007/978-3-030-73991-1.

[49] F. Grasselli. *Quantum Cryptography: From Key Distribution to Conference Key Agreement*. Quantum Science and Technology. Springer International Publishing, Cham, 2021, doi:10.1007/978-3-030-64360-7.

[50] J. Audretsch. *Entangled Systems: New Directions in Quantum Physics*. John Wiley & Sons, Ltd, 2007, doi:10.1002/9783527619153.

[51] M. Nielsen and I. Chuang. *Quantum Computation and Quantum Information: 10th Anniversary Edition*. Cambridge University Press, 2010, doi:10.1017/CBO9780511976667.

[52] M. N. Wegman and J. L. Carter. New hash functions and their use in authentication and set equality. *Journal of Computer and System Sciences*, 22(3):265–279, 1981, doi:10.1016/0022-0000(81)90033-7.

[53] D. R. Stinson. Universal hashing and authentication codes. *Designs, Codes and Cryptography*, 4(3):369–380, 1994, doi:10.1007/BF01388651.

[54] C. Portmann. Key recycling in authentication. *IEEE Transactions on Information Theory*, 60(7):4383–4396, 2014, doi:10.1109/TIT.2014.2317312.

[55] D. Tupkary, E. Y.-Z. Tan, and N. Lütkenhaus. Security proof for variable-length quantum key distribution. *Phys. Rev. Res.*, 6:023002, 2024, doi:10.1103/PhysRevResearch.6.023002.

[56] M. Hayashi and T. Tsurumaru. Concise and tight security analysis of the Bennett–Brassard 1984 protocol with finite key lengths. *New Journal of Physics*, 14(9):093014, 2012, doi:10.1088/1367-2630/14/9/093014.

[57] S. Kawakami, T. Sasaki, and M. Koashi. Finite-key analysis for quantum key distribution with weak coherent pulses based on Bernoulli sampling. *Physical Review A*, 96(1):012305, 2017, doi:10.1103/PhysRevA.96.012305.

[58] G. Currás-Lorenzo, A. Navarrete, K. Azuma, G. Kato, M. Curty, and M. Razavi. Tight finite-key security for twin-field quantum key distribution. *npj Quantum Information*, 7(1):1–9, 2021, doi:10.1038/s41534-020-00345-3.

[59] I. George, J. Lin, and N. Lütkenhaus. Numerical calculations of the finite key rate for general quantum key distribution protocols. *Physical Review Research*, 3(1):013274, 2021, doi:10.1103/PhysRevResearch.3.013274.

[60] V. Mannalath, V. Zapatero, and M. Curty. Sharp Finite Statistics for Quantum Key Distribution. *Physical Review Letters*, 135(2):020803, 2025, doi:10.1103/l735-x48g.

[61] C. Pfister, N. Lütkenhaus, S. Wehner, and P. J. Coles. Sifting attacks in finite-size quantum key distribution. *New Journal of Physics*, 18(5):053001, 2016, doi:10.1088/1367-2630/18/5/053001.

[62] K. Tamaki, H.-K. Lo, A. Mizutani, G. Kato, C. C. W. Lim, K. Azuma, and M. Curty. Security of quantum key distribution with iterative sifting. *Quantum Science and Technology*, 3(1):014002, 2018, doi:10.1088/2058-9565/aa89bd.

[63] Marco Tomamichel. *Quantum Information Processing with Finite Resources*. Springer International Publishing, 2016, doi:10.1007/978-3-319-21891-5.

[64] M. Tomamichel. A Framework for Non-Asymptotic Quantum Information Theory, 2012, doi:10.48550/arxiv.1203.2142.

[65] M. Wilde. *From Classical to Quantum Shannon Theory*. Cambridge University Press, 2016, doi:10.1017/9781316809976.001.

[66] A. Tsybakov. *Introduction to Nonparametric Estimation*. Springer series in statistics. Springer, Dordrecht, 2009, doi:10.1007/b13794.

[67] N. Smart. *Cryptography: An Introduction, 3rd Edition*. Mcgraw-Hill College, 2004.

[68] G. S. Vernam. Cipher printing telegraph systems: For secret wire and radio telegraphic communications. *Journal of the A.I.E.E.*, 45(2):109–115, 1926, doi:10.1109/JAIEE.1926.6534724.

[69] M. Herrero-Collantes and J. C. Garcia-Escartin. Quantum random number generators. *Reviews of Modern Physics*, 89(1):015004, 2017, doi:10.1103/RevModPhys.89.015004.

[70] R. Colbeck and R. Renner. No extension of quantum theory can have improved predictive power. *Nature Communications*, 2(1):411, 2011, doi:10.1038/ncomms1416.

[71] Carla Ferradini, Martin Sandfuchs, Ramona Wolf, and Renato Renner. Defining security in quantum key distribution, 2025, doi:10.48550/arXiv.2509.13405.

[72] D. Tupkary, S. Nahar, and E. Y.-Z. Tan. Authentication in Security Proofs for Quantum Key Distribution, 2026, doi:10.48550/arXiv.2601.17960.

[73] N. Mosca, D. Stebila, and B. Ustaoglu. Quantum key distribution in the classical authenticated key exchange framework, 2012, doi:10.48550/arXiv.1206.6150.

[74] G. Currás-Lorenzo, M. Pereira, G. Kato, M. Curty, and K. Tamaki. Security framework for quantum key distribution with imperfect sources. *Optica Quantum*, 3(6):525–534, 2025, doi:10.1364/OPTICAQ.569424.

[75] V. Zapatero, Á. Navarrete, and M. Curty. Implementation security in quantum key distribution. *Advanced Quantum Technologies*, 8(2):2300380, 2025, doi:https://doi.org/10.1002/qute.202300380.

[76] S. Pironio, A. Acín, N. Brunner, N. Gisin, S. Massar, and V. Scarani. Device-independent quantum key distribution secure against collective attacks. *New Journal of Physics*, 11(4):045021, 2009, doi:10.1088/1367-2630/11/4/045021.

[77] E. Biham, M. Boyer, P. O. Boykin, T. Mor, and V. Roychowdhury. A Proof of the Security of Quantum Key Distribution, 2005, doi:10.48550/arXiv.quant-ph/0511175.

[78] J. Müller-Quade and R. Renner. Composability in quantum cryptography. *New Journal of Physics*, 11(8):085006, 2009, doi:10.1088/1367-2630/11/8/085006.

[79] B. Schneier. *Applied Cryptography: Protocols, Algorithms, and Source Code in C*. John Wiley & Sons Inc, 1996.

[80] J. Carter and M. Wegman. Universal classes of hash functions. *Journal of Computer and System Sciences*, 18(2):143–154, 1979, doi:10.1016/0022-0000(79)90044-8.

[81] M. Tomamichel, J. Martinez-Mateo, C. Pacher, and D. Elkouss. Fundamental Finite Key Limits for One-Way Information Reconciliation in Quantum Key Distribution. *Quantum Information Processing*, 16(11):280, 2017, doi:10.1007/s11128-017-1709-5.

[82] H. Tyagi and A. Vardy. Universal Hashing for Information-Theoretic Security. *Proceedings of the IEEE*, 103(10):1781–1795, 2015, doi:10.1109/JPROC.2015.2462774.

[83] R. Renner and R. König. Universally composable privacy amplification against quantum adversaries. In Joe Kilian, editor, *Theory of Cryptography*, pages 407–425, Berlin, Heidelberg, 2005. Springer Berlin Heidelberg, doi:10.1007/978-3-540-30576-7_22.

[84] R. Konig, 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.

[85] 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.

[86] A. Vitanov, F. Dupuis, M. Tomamichel, and R. Renner. Chain rules for smooth min- and max-entropies. *IEEE Transactions on Information Theory*, 59(5):2603–2612, 2013, doi:10.1109/tit.2013.2238656.

[87] M. Curty, M. Lewenstein, and N. Lütkenhaus. Entanglement as a precondition for secure quantum key distribution. *Phys. Rev. Lett.*, 92:217903, 2004, doi:10.1103/PhysRevLett.92.217903.

[88] A. Ferenczi and N. Lütkenhaus. Symmetries in quantum key distribution and the connection between optimal attacks and optimal cloning. *Phys. Rev. A*, 85:052310, 2012, doi:10.1103/PhysRevA.85.052310.

[89] P. J. Coles, R. M. Metodiev, and N. Lütkenhaus. Numerical approach for unstructured quantum key distribution. *Nature Communications*, 7(1):11712, 2016, doi:10.1038/ncomms11712.

[90] A. Ekert and R. Renner. The ultimate physical limits of privacy. *Nature*, 507(7493):443–447, 2014, doi:10.1038/nature13132.

[91] C. C. W. Lim. *Tight security bounds for quantum key distribution*. PhD thesis, Université de Genève, 2014.

[92] R. J. Serfling. Probability Inequalities for the Sum in Sampling without Replacement. *The Annals of Statistics*, 2(1):39–48, 1974, doi:10.1214/aos/1176342611.

[93] H.-K. Lo and J. Preskill. Security of quantum key distribution using weak coherent states with nonrandom phases, 2007, doi:10.48550/arXiv.quant-ph/0610203.

[94] M. O. Scully and M. S. Zubairy. *Quantum Optics*. Cambridge University Press, 1997.

[95] G. Currás-Lorenzo, S. Nahar, N. Lütkenhaus, K. Tamaki, and M. Curty. Security of quantum key distribution with imperfect phase randomisation. *Quantum Science and Technology*, 9(1):015025, 2024, doi:10.1088/2058-9565/ad141c.

[96] X. Sixto, G. Currás-Lorenzo, K. Tamaki, and M. Curty. Secret key rate bounds for quantum key distribution with faulty active phase randomization. *EPJ Quantum Technology*, 10(1):53, 2023, doi:10.1140/epjqt/s40507-023-00210-0.

[97] S. Nahar, T. Upadhyaya, and N. Lütkenhaus. Imperfect phase randomization and generalized decoy-state quantum key distribution. *Phys. Rev. Appl.*, 20:064031, 2023, doi:10.1103/PhysRevApplied.20.064031.

[98] W. Hoeffding. Probability Inequalities for Sums of Bounded Random Variables. *Journal of the American Statistical Association*, 58(301):13–30, 1963, doi:10.2307/2282952.

[99] M. Curty, F. Xu, W. Cui, C. Lim, K. Tamaki, and H.-K. Lo. Finite-key analysis for measurement-device-independent quantum key distribution. *Nature Communications*, 5(1), 2014, doi:10.1038/ncomms4732.

[100] D. Tupkary, E. Y.-Z. Tan, S. Nahar, L. Kamin, and N. Lütkenhaus. QKD security proofs for decoy-state BB84: protocol variations, proof techniques, gaps and limitations, 2025, doi:10.48550/arXiv.2502.10340.

[101] A. Arqand and E. Y.-Z. Tan. Marginal-constrained entropy accumulation theorem, 2025, doi:10.48550/arXiv.2502.02563.

[102] L. Kamin, J. Burniston, and E. Y.-Z. Tan. Rényi security framework against coherent attacks applied to decoy-state QKD, 2025, doi:10.48550/arXiv.2504.12248.

[103] L. Kamin. *From Asymptotic to Finite-Size Security in Decoy-State Quantum Key Distribution*. PhD thesis, University of Waterloo, 2026. In preparation.

[104] M. Lucamarini, I. Choi, M. B. Ward, J. F. Dynes, Z. L. Yuan, and A. J. Shields. Practical Security Bounds Against the Trojan-Horse Attack in Quantum Key Distribution. *Physical Review X*, 5(3):031030, 2015, doi:10.1103/PhysRevX.5.031030.

[105] W. Wang, K. Tamaki, and M. Curty. Finite-key security analysis for quantum key distribution with leaky sources. *New Journal of Physics*, 20(8):083027, 2018, doi:10.1088/1367-2630/aad839.

[106] Y. Zhang, P. J. Coles, A. Winick, J. Lin, and N. Lütkenhaus. Security proof of practical quantum key distribution with detection-efficiency mismatch. *Physical Review Research*, 3(1):013076, 2021, doi:10.1103/PhysRevResearch.3.013076.

[107] G. Wiesemann. Quantum key distribution secure-key rate simulation (1-decoy BB84). https://github.com/JeromeWiesemann/Quantum-key-distribution-secure-key-rate-simulation-1-decoy-BB84, 2025. Accessed: 2025-12-03.

[108] H.-K. Lo and J. Preskill. Phase randomization improves the security of quantum key distribution, 2005, doi:10.48550/arXiv.quant-ph/0504209.