Composably secure device-independent encryption with certified deletion

Srijita Kundu[1] and Ernest Y.-Z. Tan[2,3]

[1]Institute for Quantum Computing and Department of Combinatorics and Optimization, University of Waterloo, Waterloo, Ontario N2L 3G1, Canada.

[2]Institute for Theoretical Physics, ETH Zürich, Switzerland.

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

We study the task of encryption with certified deletion (ECD) introduced by Broadbent and Islam [BI20], but in a device-independent setting: we show that it is possible to achieve this task even when the honest parties do not trust their quantum devices. Moreover, we define security for the ECD task in a composable manner and show that our ECD protocol satisfies conditions that lead to composable security. Our protocol is based on device-independent quantum key distribution (DIQKD), and in particular the parallel DIQKD protocol based on the magic square non-local game, given by Jain, Miller and Shi [JMS20]. To achieve certified deletion, we use a property of the magic square game observed by Fu and Miller [FM18], namely that a two-round variant of the game can be used to certify deletion of a single random bit. In order to achieve certified deletion security for arbitrarily long messages from this property, we prove a parallel repetition theorem for two-round non-local games, which may be of independent interest.

1 Introduction

Consider the following scenario: Alice wants to send a message to Bob that is secret from any third party. She may do this by sending Bob a ciphertext which contains the message encrypted with a secret key, such that when the key is revealed to Bob he may learn the message. Now suppose after sending the ciphertext Alice decides that she does not want Bob to learn the message after all, but she cannot prevent the secret key from eventually being revealed to him. So Alice wants to encrypt the message in such a way that she can ask Bob for a *deletion certificate* if she changes her mind. If Bob sends a valid deletion certificate, Alice can be convinced that Bob has indeed deleted his ciphertext and cannot hereafter learn the message even if the secret key is revealed to him. In this scenario Alice is not actually forcing Bob to delete the ciphertext, but she is making sure that he cannot simultaneously convince her that he has deleted the ciphertext, and also learn the message.

Srijita Kundu: srijita.kundu@uwaterloo.ca

Ernest Y.-Z. Tan: yzetan@uwaterloo.ca

An encryption scheme for the above scenario is called *encryption with certified deletion* (ECD) and was introduced by Broadbent and Islam [BI20]. It is easy to see that ECD cannot be achieved with a classical ciphertext: since classical information can always be copied, any deletion certificate Bob sends to Alice can only convince her that he has deleted one copy of it – he may have kept another copy to decrypt from, when he learns the key. However, quantum states cannot in general be copied, and are disturbed by measurements. So if Bob has a quantum ciphertext that he cannot copy, and needs to perform a measurement on it to produce a deletion certificate, the state may be disturbed to such an extent that it is no longer possible to recover the message from it, even with the key.

The no-cloning property and the fact that measurements disturb quantum states have been useful for various cryptographic tasks, such as quantum key distribution (QKD) [BB84] and unforgeable quantum money [Wie83]. The concept of *revocable timed-release encryption* — a task which has some similarities to encryption with certified deletion — was studied by Unruh [Unr14], who showed it can be achieved with quantum encodings. Another related task of tamper-evident delegated quantum storage — here Alice wants to store data that she encrypts using a short key on a remote server, so that she can retrieve it later and also detect if the server has tampered with it — was studied by van der Vecht, Coiteaux-Roy and Škorić [VCRŠ20]. Lütkenhaus, Marwah and Touchette [LMT20] studied a different form of delegated storage, where Alice commits to a single random bit that Bob can learn at some fixed time, or she can erase, using a temporarily trusted third party. Finally, the ECD task itself, as mentioned before, was introduced by Broadbent and Islam, who achieved it using Wiesner's encoding scheme [Wie83].

All of the works mentioned above are in the device-dependent setting, where the honest parties trust either the quantum states that are being used in the protocol, or the measurement devices, or both. However, in general a sufficiently powerful dishonest party may make the quantum state preparation and measurement devices used in a protocol behave however they want. As it turns out, with some mild assumptions it is possible to achieve certain cryptographic tasks even in this scenario. There is a long line of works studying the device-independent security of QKD [PAB+09, AFDF+18, JMS20]. Device-independent protocols for two-party cryptographic tasks such as coin flipping [ACK+14], bit commitment [SCA+11, AMP+16] and XOR oblivious transfer [KST22] have also been shown. Fu and Miller [FM18] studied the task of sharing between two parties a single random bit, which can be certifiably deleted, in the device-independent setting.

A desirable property of cryptographic protocols is that they should be *composable*, meaning that if a protocol is used as part of a larger protocol to achieve some more complex task, then security of the larger protocol should follow from the security of its constituent protocols. While it is possible to achieve composable security of various cryptographic tasks such as QKD [BOHL+05, PR14], this is in general not so easy to achieve for many examples, such as the others mentioned above.

1.1 Our contributions

Informally stated, our main contributions in this work are:

1. We define the ECD task and its security in a composable manner.
2. We give a quantum protocol (with information-theoretic security) for the ECD task that satisfies certain properties of correctness, completeness and secrecy, even when the honest parties

do not trust their own quantum devices.

3. We show how to prove that a protocol that satisfies the above properties achieves the ECD task in a composably secure manner.

The reason we do not combine items 2 and 3 above to make the claim that we give a protocol that achieves the ECD task in a composably secure manner is because the notion of device-independence itself has not been precisely formalized in a composable manner yet. So item 3 in the device-independent setting is conditional on a conjecture that we shall soon explain (though note that even without this conjecture, our proof already shows that the protocol is indeed composably secure in the standard device-dependent setting, i.e. if one imposes the condition that the honest parties are performing trusted measurements). In contrast, our proof that our protocol satisfies the security properties in item 2 holds under standard device-independent conditions, without additional conjectures.

Our composable security definition uses the framework of *Abstract Cryptography* introduced by Maurer and Renner [MR11]. In the Abstract Cryptography framework, a *resource* is an abstract system with an interface available to each party involved, to and from which they can supply some inputs and receive some outputs. A *protocol* uses some resources (meaning it interacts with the interfaces of such resources) in order to construct new resources. The protocol is said to construct the new resource in a composably secure manner if it is not possible to tell the ideal resource apart from the protocol acting on the resources it uses, under certain conditions. As such, a composable security definition for a cryptographic task would be the description of a reasonable (in the sense of being potentially achievable by actual protocols) ideal functionality or resource corresponding to that task, and a composable security proof for a protocol for this task would show that the constructed resource and ideal resource are indistinguishable.

We model the notion of a device-independent resource in the Abstract Cryptography framework as a resource which supplies some black boxes representing quantum states to the honest parties, and the honest parties may press some buttons on these boxes to obtain some classical outputs. However, the resource allows the boxes themselves to be chosen by a dishonest third party Eve, and they produce the outputs by implementing whatever states and measurements Eve wants.

Strictly speaking, to avoid the *memory attack* in the device-independent setting described in [BCK13], some additional constraints need to be placed on the registers that the measurements act on. Namely, one has to impose the condition that the measurements cannot access any registers storing private information from previous (potentially unrelated) protocols. Such a condition is implicitly imposed, albeit not always obvious, in the standard (device-dependent) framework for Abstract Cryptography [MR11, PR14], where the measurements are assumed to be fully characterized (and thus the registers which the measurements act on can be specified to be independent of previous protocols). However, the question of precisely formalizing this condition in the device-independent setting has not been completely resolved, and is currently a topic of active research. For the purposes of this work, we consider the technical treatment of this subject to be beyond our scope, and for ease of presentation we shall proceed under the assumption that it will be possible to find an appropriate such formulation in the device-independent setting. That is, we shall assume the following somewhat informal conjecture and prove our main theorem conditional on it.

Conjecture 1. *The quantum "boxes" typically considered in the device-independent setting can be*

formalized in the Abstract Cryptography framework, in a manner that allows one to impose the conditions we have outlined above (and which we elaborate on in Section 2.3).

We can also introduce a formalization of the notion that Alice cannot prevent the decryption key from leaking to Bob in the ECD setting. We model this as follows: Alice has access to a *trusted temporarily private randomness source* — meaning it supplies random variables with any requested distribution, but after some fixed time it will make public any randomness it provided. Furthermore we impose the constraint that after some point in time (and before decryption takes place), Alice no longer has any communication channels to Bob, and thus her only way for Bob to learn the effective "decryption key" is through the public broadcast made by this temporarily private randomness source — note that this broadcast still occurs even if Alice wants to revoke Bob's ability to learn the message, thereby formalizing the notion that the "decryption key" is eventually leaked. For technical reasons regarding the anchoring-based proof, we also need Alice to have a small supply of local randomness that remains private (it does not need to be announced even for decryption). Overall, our protocol constructs the ECD resource using only these randomness sources, untrusted quantum boxes, and an authenticated classical channel (which only lasts until the aforementioned time) — all of which are fairly weak.

Aside from device-independence and composability, our ECD security definition and protocol construction has the following advantage over the ones in [BI20]: we consider the possibility of Bob being honest and consider security against a third party eavesdropper Eve when this is the case. This helps motivate the encryption aspect of the ECD task: if Alice did not need to conceal the message from Eve, she could have waited until she was sure whether she trusts Bob or not, and then sent the message as plaintext. Security against Eve is not considered in [BI20], and indeed in their protocol Eve may be able to learn the message whenever Bob does.

We note however that making the protocol secure against Eve comes at the cost of making it interactive. In the [BI20] protocol, Bob receives the ciphertext in one round from Alice, whereas in our protocol, Alice sends a message to Bob and Bob replies back with a message before Alice can send the ciphertext (or abort the protocol). Furthermore, to prove this security property we do need to impose a somewhat non-standard condition regarding honest Bob's boxes; however, we highlight that this condition is only used to prove security against Eve, and is not required in any situation where Bob is dishonest (see Sec. 2.3–2.4 for further details).

A more minor difference is that we think it makes more intuitive sense for the ECD task to include a further message from Alice to Bob in which she tells Bob whether she wants him to delete his ciphertext or not (and potentially provides additional information he needs in order to do so), and hence we present our protocol as including this communication from Alice to Bob. However, the protocol and security proof can easily be modified to consider a version in which Alice sends the information required for deletion from the start, and Bob alone makes the decision of whether to delete the ciphertext (this version would essentially match the [BI20] protocol).

1.2 Our techniques

1.2.1 Constructing the DI ECD protocol

All device-independent security proofs are based on non-local games. One approach towards constructing such proofs is to use the property known as *self-testing* or *rigidity* displayed by certain non-local games. Specifically, suppose we play a non-local game with boxes implementing some

unknown state and measurements, and in fact even the dimension of the systems are unspecified. If these state and measurements regardless achieve a winning probability for the game that is close to its optimal winning probability, then self-testing tells us that the state and measurements are close to the ideal state and measurements for that game, up to trivial isometries. For DIQKD, this means in particular that the measurement outputs of the devices given the inputs are random, i.e., they cannot be predicted by a third party even if they have access to the inputs used. This lets us use the outputs of the devices to produce a secret key.

Parallel DIQKD protocol. We make use of the parallel DIQKD protocol given by Jain, Miller and Shi [JMS20], and its subsequent simplification given by Vidick [Vid17], based on the magic square non-local game. In the magic square game, henceforth deonoted by MS, Alice and Bob respectively receive trits x and y, and they are required to output 3-bit strings a and b, which respectively have even parity and odd parity, and satisfy $a[y] = b[x]$. The classical winning probability of MS is $8/9$, whereas the quantum winning probability is 1. The [JMS20] protocol works as follows: Alice and Bob have boxes which can play l many instances of MS. Using trusted private randomness, Alice and Bob generate i.i.d. inputs x, y for each of their boxes and obtain outputs a, b (which are not necessarily i.i.d.). The inputs x, y are then publicly communicated. Alice and Bob select a small subset of instances on which to communicate their outputs and test if the MS winning condition is satisfied (up to some error tolerance) on those instances. If this test passes, then they go ahead and select their common bits $a[y] = b[x]$ from all the instances — they can do this since Alice has a, Bob has b, and they both have x, y — as their raw secret key (some *privacy amplification* of the raw key is required in order to get the final key). Otherwise, the protocol aborts.

If the MS winning condition is satisfied on the test instances with high probability, then self-testing says that the states and measurements are close to the ideal ones for MS; but this property is not directly used in the security proof. In the version of the security proof given by [Vid17], instead a guessing game variant MSE of MS, involving three players Alice, Bob and Eve, is considered. MSE is the same as MS on Alice and Bob's parts, and additionally, Eve also gets Alice and Bob's inputs and has to guess Alice and Bob's common bit. It can be shown that MSE cannot be won with probability 1 by all three players, and in particular if Alice and Bob's winning condition is satisfied, then Eve cannot guess their common bit with high probability. Now making use of a parallel repetition theorem for the MSE game, which first requires a small transformation called *anchoring* in order to make the parallel repetition proof work, we can say that Eve's guessing probability for the shared bit in l many instances of MSE, is exponentially small in l. Since Alice and Bob's winning condition is satisfied on a random subset of instances, we can say it is satisfied on all instances with high probability by making use of a sampling lemma. Hence Eve's guessing probability for the raw key is exponentially small in l. Now using the operational interpretation of min-entropy, this means that the min-entropy of the raw key conditioned on Eve's quantum system is linear in l, and we can use privacy amplification to get a final key that looks almost uniformly random to Eve.

Using DIQKD for ECD. It is easy to see how to use DIQKD to achieve the encryption aspect of ECD — Alice and Bob can perform the DIQKD protocol to share a secret key, and then Alice can encrypt the message by one-time padding it with the key, and send it to Bob. This certainly achieves security against Eve if Bob is honest. However, in the ECD scenario, unlike in the QKD scenario, Bob may not be honest, and hence the QKD security proof may not apply, since it requires him to honestly follow the protocol. Moreover, it is not clear how to achieve the certified deletion aspect of ECD this way. Instead, we do the following for our ECD protocol: we make Alice obtain

the inputs x, y for MS from the trusted temporarily private randomness source, and obtain the raw key by herself using her boxes and the inputs, but she does not reveal the inputs to Bob (who hence does not have the raw key). She then one-time pads the message with the final key obtained from the raw key and sends the resulting ciphertext to Bob. Bob cannot decrypt the message at this time since he does not have the raw key, but he can get the key from his boxes and decrypt as soon as the temporarily private randomness source reveals x, y to him. Hence in order to achieve certified deletion security, Alice needs to make Bob do some operation on his boxes which destroys his ability to learn the raw key even if he gets x, y.

We also note that for technical reasons, Alice actually needs to one-time pad the message with an extra uniformly random string u that she gets from the randomness source, in addition to the final key. This makes no difference to Bob's ability to decrypt the message when all the randomness is revealed by the source or in certified deletion (since u is revealed at the end), but it does potentially make a difference at intermediate stages in the protocol. Such an extra one-time pad is also used by [BI20] in their protocol.

Achieving certified deletion security. Fu and Miller [FM18] made the following observation about the magic square game: suppose Alice does the measurement corresponding to x and Bob does the measurement corresponding to y' on the MS shared state, then if Bob is later given x he can guess $a[y']$ perfectly as $b[x]$ from his output. But if Bob has indeed performed the y' measurement, then he cannot guess the value of $a[y]$ for some $y \neq y'$, even given x. In fact this property holds in a device-independent manner, i.e., if Alice and Bob have boxes implementing some unknown state and measurements which are compatible with MS, and Alice and Bob input x and y' into their boxes and get outputs that satisfy the MS winning condition with probability close to 1, then Bob cannot later perfectly guess $a[y]$ given x, y. Now consider a 2-round variant of MS, which we shall call MSB: in the first round, Alice and Bob are given x, y' and are required to output a, b' that satisfy the MS winning condition; in the second round, Bob is given x, y such that $y \neq y'$ and he is required to produce a bit equal to $a[y]$. We note that Bob can use his first round input, his first round measurement outcome, and his half of the post-measured shared state in order to produce the second round output. The [FM18] observation implies that the winning probability of MSB is less than 1.

Using the same anchoring trick as in MSE, we can prove a parallel repetition theorem for the 2-round MSB game. Now to achieve certified deletion, Alice gets i.i.d. $y' \neq y$ for all l instances from the randomness source, and if she wants Bob to delete his ciphertext, she sends Bob y' and asks for b' as a deletion certificate. If the b' sent by Bob satisfies $a[y'] = b'[x]$ (up to some error tolerance) then Alice accepts his deletion certificate. Due to the parallel repetition theorem for MSB, if Bob's deletion certificate has been accepted, then his guessing probability for $a[y]$, i.e., the raw key, given x, y, is exponentially small in l. Due to privacy amplification, the final key looks uniformly random to Bob, and thus the message is secret from him. We note that certified deletion security should be against Bob and Eve combined rather than just Bob, as a dishonest Bob could collude with Eve in order to try and guess the message. This is fine for our security proof approach, as we can consider Bob and Eve combined as a single party for the purposes of the MSB game.

Remark 1. *Many security proofs for DIQKD work in the sequential rather than parallel setting. In the sequential setting, Alice and Bob provide inputs to and get outputs from each instance of their boxes sequentially, which limits the kinds of correlations that are possible between the whole string of their inputs and outputs. While this is easy to justify for DIQKD when Alice and Bob are both honest, justification is harder for the ECD scenario where Bob may be dishonest and need not use*

his boxes sequentially, so that more general correlations between his inputs and outputs are possible. Hence a parallel rather than sequential security proof is crucial for us.

1.2.2 Proving composable security

To prove composable security for our protocol, we need to show that a *distinguisher* cannot tell the protocol apart from the ideal ECD functionality, when it is constrained to interact with the ideal functionality via a *simulator* acting on the dishonest parties' interfaces. That is, for any possible behaviour of the dishonest parties in the real protocol, we need to construct a simulator such that the above is true. This needs to be done for all possible combinations of honest/dishonest parties involved, and here we only describe the idea for the case when Bob is dishonest and the dishonest third party Eve is present.

Our simulator construction is inspired by the composable security proofs of QKD [BOHL+05, PR14]: it internally simulates the real protocol using whatever outputs it gets from the ideal functionality, so that the distinguisher is able to get states on the dishonest parties' side similar to what it would have gotten in the real protocol. However, the ideal functionality is only supposed to reveal the message m to Bob at the end (if either Alice did not ask for a deletion certificate, or Alice asked for a deletion certificate and Bob did not produce a valid one), and since the simulator needs to simulate the real protocol before this time, it has to instead release a dummy ciphertext that does not depend on the message. Hence we require that the states on the dishonest parties' side corresponding to m and the dummy ciphertext in the protocol be indistinguishable, if the message has not been revealed. This is related to the security notions of *ciphertext indistinguishability* and *certified deletion security* considered in [BI20]. But these properties hold only as long as the protocol does not actually reveal m. If m is actually revealed at the end, the simulator needs to fool the distinguisher into believing it originally released the ciphertext corresponding to m. This is where the extra one-time pad u we use comes in handy: the simulator can edit the value on the one-time pad register to a value compatible with the true message m.

Overall, our security proof is fairly "modular": our simulator construction for dishonest Bob and Eve works for any protocol in which the extra u OTP is used and which satisfies the ciphertext indistinguishability and certified deletion security properties (jointly called *secrecy*). For other combinations of honest/dishonest parties, the proof works for any protocol that satisfies notions of *completeness* and *correctness*, even for devices with some small noise. Completeness here means that if all parties are honest then the protocol aborts with small probability, and Bob's deletion certificate is accepted by Alice with high probability; correctness means that an honest Bob can recover the correct message from the quantum ciphertext with high probability.

1.2.3 Proving parallel repetition for 2-round games

As far as we are aware, our proof of the parallel repetition theorem for the MSB game is the first parallel repetition result for 2-round games, which may be of independent interest. First we clarify what we mean by a 2-round game: in the literature, boxes that play multiple instances of a game, whether sequentially or in parallel, are sometimes referred to as multi-round boxes, and certainly the nomenclature makes sense in the sequential setting. However, the two rounds for us are not two instances of the same game — they both constitute a single game and in particular, the outputs of the second round are required to satisfy a winning condition that depend on the inputs and outputs of the first round. Alice and Bob share a single entangled state at the beginning

of the game, and the second round outputs are obtained by performing a measurement that can depend on the first round inputs and outputs in addition to the second round inputs, on the post-measured state from the first round. This is what we refer to as a 2-round game; it can be viewed as a specific type of interactive game.

We actually prove a parallel repetition theorem for a wider class of 2-round games than just the anchored MSB game; namely, what we call *product-anchored games*. This captures elements of both product games and anchored games, whose parallel repetition has been studied for 1-round games [JPY14, BVY15, BVY17, JK21] (although we consider only a specific form of anchoring which is true of the MSB game — anchored distributions can be more general), and our proof is inspired by techniques from proving parallel repetition for both product and anchored 1-round games. We call a 2-round game product-anchored iff the first round inputs x, y are from a product distribution, and in the second round, only Bob gets an input z which takes a special value $\perp$ with constant probability such that the distribution of x, y conditioned on $z = \perp$ is the same as their marginal distribution, and otherwise $z = (x, y')$ (where y' may be arbitrarily correlated with x, y). The first and second round outputs are (a, b) and b' respectively.[1]

We use the information theoretic framework for parallel repetition established by [Raz95, Hol07]: we consider a strategy $\mathcal{S}$ for l instances of the game G, condition on the event $\mathcal{E}$ of the winning condition being satisfied on some $C \subseteq [l]$ instances, and show that if $\Pr[\mathcal{E}]$ is not already small, then we can find another coordinate in $i \in \overline{C}$ where the winning probability conditioned on $\mathcal{E}$ is bounded away from 1. For 1-round games (where there is no z_i), this is done in the following way: Alice and Bob's overall state in $\mathcal{S}$ conditioned on $\mathcal{E}$ is considered; this state depends on Alice and Bob's inputs — suppose it is $|\varphi\rangle_{x_i y_i}$ when Alice and Bob's inputs in the i-th coordinate are (x_i, y_i). We then argue that there exists some coordinate i and unitaries $\{U_{x_i}\}_{x_i}, \{V_{y_i}\}_{y_i}$ acting on Alice and Bob's registers respectively, such that the operator $U_{x_i} \otimes V_{y_i}$ brings some shared initial state close to the state $|\varphi\rangle_{x_i y_i}$. (In the product case, this shared initial state would be a superposition of the states $|\varphi\rangle_{x_i y_i}$, weighted according to the distributions of x_i and y_i.) Hence, unless the winning probability in the i-th coordinate is bounded away from 1, Alice and Bob can play a single instance of G by sharing this initial state, performing U_{x_i}, V_{y_i} on it on inputs (x_i, y_i), and giving the measurement outcome corresponding to the i-th coordinate on the resulting state; the winning probability of this strategy would then be higher than the optimal winning probability of G — a contradiction.

For 2-round games, the state conditioned on success depends on all three inputs $x_i y_i z_i$, and Alice and Bob obviously cannot perform unitaries U_{x_i} and $V_{y_i z_i}$ in order to produce their first round outputs, since Bob has not received z_i yet. However, we observe that Alice and Bob don't actually need the full $|\varphi\rangle_{x_i y_i z_i}$ state in order to produce their first round outputs — they only need a state whose $A_i B_i$ registers, containing their first round outputs, are close to those of $|\varphi\rangle_{x_i y_i z_i}$. We observe that $|\varphi\rangle_{x_i y_i \perp}$ is indeed such a state. In fact, in the unconditioned state, given $x_i y_i$, all of Alice's registers as well as all of B are independent of z_i, as the second round unitary depending on z_i does not act on these registers (the second round unitary may use B as a control register, but that does not affect the reduced state of B). Conditioning on the high probability event $\mathcal{E}$ does not disturb the state too much, and by chain rule of mutual information, we can argue that there exists an i such that Alice's registers and B in $\varphi_{x_i y_i z_i}$ are close to those in $\varphi_{x_i y_i}$ (i.e., averaged over z_i). Since $z_i = \perp$ with constant probability, this means that these registers are indeed close in $\varphi_{x_i y_i z_i}$

[1] In this notation we switch around the roles of y, y', b, b' as compared to our definition of MSB. We do this in order to make our notation more compatible with standard parallel repetition theorems. As this definition refers to a wider class of games than just MSB, we hope this will not cause any confusion.

and $\varphi_{x_i y_i \perp}$.

Conditioned on $z_i = \perp$, the situation in the first round is identical to the product case; we can argue the same way as in the product parallel repetition proof by [JPY14] that there exist unitaries $\{U_{x_i}\}_{x_i}, \{V_{y_i}\}_{y_i}$ such that $U_{x_i} \otimes V_{y_i}$ takes $|\varphi\rangle_\perp$ close to $|\varphi\rangle_{x_i y_i \perp}$. Now we use the fact that Alice's registers and B are close in $\varphi_{x_i y_i z_i}$ and $\varphi_{x_i y_i \perp}$ once again to argue that there exist unitaries $\{W_{x_i y_i z_i}\}_{x_i y_i z_i}$ acting on Bob's registers except B that take $|\varphi\rangle_{x_i y_i \perp}$ to $|\varphi\rangle_{x_i y_i z_i}$. We notice that $W_{x_i y_i z_i}$ is in fact just $W_{y_i z_i}$, because either z_i contains x_i or it can just be the identity, which means Bob can use $W_{y_i z_i}$ as his second round unitary. Moreover, these unitaries commute with the measurement operator on the $A_i B_i$ registers, hence $W_{y_i z_i}$, acting on the post-measured $|\varphi\rangle_{x_i y_i \perp}$ also takes it to the post-measured $|\varphi\rangle_{x_i y_i z_i}$. Thus the distribution Bob would get by measuring B_i' after applying $W_{y_i z_i}$ on his post $A_i B_i$ measurement state is close to the correct distribution of B_i' conditioned on any values (a_i, b_i) obtained in the first round measurement. This gives a strategy $\mathcal{S}'$ for a single instance of G, where U_{x_i}, V_{y_i} are the first round unitaries and $W_{y_i z_i}$ is Bob's second round unitary.

1.3 Organization of the paper

In Section 2 we formally describe the ideal ECD functionality we consider, and state our precise result regarding it. In Section 3 we provide definitions and known results for the quantities used in our proofs. In Section 4, we describe the variants of the magic square non-local games and state the parallel repetition theorems for them that we use. In Section 5 we give our real ECD protocol and prove various intermediate results that help establish its composable security, which is done in Section 6. Finally, in Section 7 we provide the proofs for the parallel repetition theorems stated in Section 4.

2 Composable security definition for ECD

In this section, we define the precise functionality we aim to achieve, in terms of the Abstract Cryptography framework. We then state our main result regarding achieving this functionality.

2.1 Abstract cryptography

We first briefly state the concepts and definitions we require from the Abstract Cryptography framework. Note that this is not intended to be a complete introduction to all aspects of the framework, as that would be fairly extensive and outside the scope of this work — if more in-depth or pedagogical explanations are required, refer to e.g. [MR11, PR14, VPR19].

2.1.1 Resources, converters, and distinguishers

In this framework, a *resource* is an abstract system with an interface available to each party, to and from which they can supply some inputs and receive some outputs. Qualitatively, the idea of this framework is to model how protocols convert some "real" resources available to the various parties into more "ideal" functionalities for some cryptographic tasks. To formalize this notion, let us lay out the basic setup. We first assume that there is a fixed set Q of parties that can choose

to be either honest or dishonest. As an example, in QKD this set Q can be taken to consist of Eve only, while Alice and Bob are always honest. As another example, for two-party "distrustful" cryptographic tasks such as oblivious transfer or bit commitment, Q consists of both Alice and Bob, who can each potentially be dishonest. For our certified deletion protocol, we will take this set Q to consist of Bob and Eve only; Alice is always honest.

Having fixed this set Q, we introduce the following notation: $(\mathcal{F}_P)_{P\subseteq Q}$ is a tuple indexed by subsets $P \subseteq Q$, where for each $P \subseteq Q$ (i.e. each possible subset of the potentially-dishonest parties), $\mathcal{F}_P$ denotes the resources available when the parties P are behaving dishonestly. Notice that this means we often work with tuples of resources rather than just a single specific resource; this is intended to capture the notion that these resources may have different functionalities depending on whether each of the parties is behaving honestly or dishonestly. (In principle one might want to consider only tuples $(\mathcal{F}_P)_{P\subseteq Q}$ where the resource $\mathcal{F}_P$ is the same regardless of the subset P of dishonest parties. However, this sometimes turns out to be overly restrictive, hence for generality we allow ourselves the flexibility to consider tuples where each resource $\mathcal{F}_P$ is different for different subsets P.)

With this in mind, let $\left(\mathcal{F}_P^{\text{real}}\right)_{P\subseteq Q}$ denote the resource tuple describing the "real" functionalities available to the various parties. Analogously, let $\left(\mathcal{F}_P^{\text{ideal}}\right)_{P\subseteq Q}$ denote the resource tuple describing the "ideal" functionalities we would like to achieve. In order to do so, we would informally like our protocol to "interact with" $\left(\mathcal{F}_P^{\text{real}}\right)_{P\subseteq Q}$ in such a way that it is transformed to $\left(\mathcal{F}_P^{\text{ideal}}\right)_{P\subseteq Q}$. To turn this into a full security definition, we now discuss the notion of *converters*, which can interact with a resource to produce a new resource.

A converter is an abstract system with an "inner" and "outer" interface, with the inner interface being connected to the resource interfaces, and the outer interface becoming the new interface of the resulting resource. If P is a subset of the parties and we have a converter χ^P that connects to their interfaces in a resource $\mathcal{F}$, we shall denote this as $\chi^P\mathcal{F}$ or $\mathcal{F}\chi^P$ (the ordering has no significance except for readability). Each converter describes how that party interacts with its interfaces in $\mathcal{F}$, producing a new set of inputs and outputs "externally" (i.e. at the outer interface). If we have (for instance) a protocol with converters Π^{A} and Π^{B} for parties A and B, for brevity we shall use Π^{AB} to denote the converter obtained by attaching both the converters Π^{A} and Π^{B}. An important basic example of converters arises from protocols themselves, which we shall now describe more thoroughly (also refer to Figure 1 for a schematic depiction).

Explicitly, we shall model a protocol as a tuple $\mathscr{P} = (\Pi^{\mathrm{A}}, \Pi^{\mathrm{B}}, \dots)$ of converters, one for each party. When trying to convert a real resource tuple $\left(\mathcal{F}_P^{\text{real}}\right)_{P\subseteq Q}$ to an ideal resource tuple $\left(\mathcal{F}_P^{\text{ideal}}\right)_{P\subseteq Q}$, these converters would have inner interfaces that connect to $\mathcal{F}_{\{\}}^{\text{real}}$ (i.e. the real resource for the case when all parties choose to behave honestly), while their outer interfaces are required to have the same structure as those in $\mathcal{F}_{\{\}}^{\text{ideal}}$. (For the purposes of formalizing protocols we will not need to consider the resources for the cases where some parties behave dishonestly; we shall return to discussing such behaviour when introducing the security definitions shortly below.) We give a schematic depiction of this in Figure 1.

Finally, we shall require the concept of *distinguishers*. Given two resources $\mathcal{F}$ and $\mathcal{F}'$, a distinguisher is a system that interacts with the interfaces of these resources, and then produces a single bit G (which can be interpreted as a guess of which resource it is interacting with). For a given distinguisher, let $\mathsf{P}_{G|\mathcal{F}}$ be the probability distribution it produces on G when supplied with $\mathcal{F}$, and

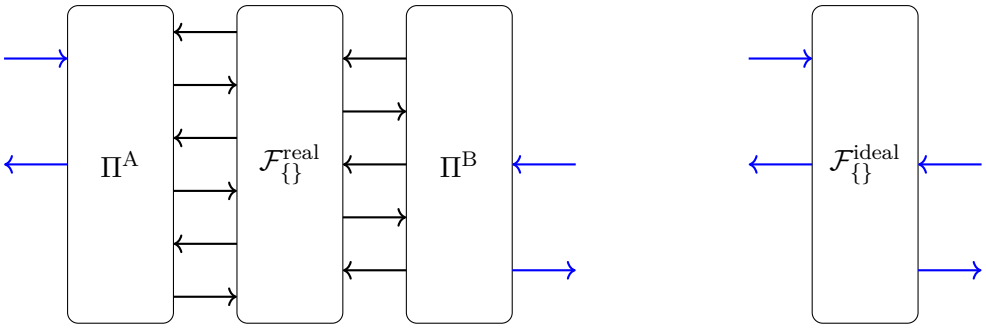


Figure 1: Schematic depiction of protocols interacting with a real resource, in a scenario with only two parties Alice and Bob (labelled as A, B). In the diagram on the left, $\mathcal{F}^{\mathrm{real}}_{\{\}}$ denotes the real resources available when all parties are honest (i.e. the set of dishonest parties P is the empty set $\{\}$). The "inner" interfaces of the protocol converters $\Pi^{\mathrm{A}}, \Pi^{\mathrm{B}}$ attach to the interfaces of $\mathcal{F}^{\mathrm{real}}_{\{\}}$, converting it to a resource with interfaces given by the "outer" interfaces of $\Pi^{\mathrm{A}}, \Pi^{\mathrm{B}}$ (shown in blue here). The resulting resource can be variously denoted as $\Pi^{\mathrm{A}}\mathcal{F}^{\mathrm{real}}_{\{\}}\Pi^{\mathrm{B}}$, $\Pi^{\mathrm{AB}}\mathcal{F}^{\mathrm{real}}_{\{\}}$ or $\mathcal{F}^{\mathrm{real}}_{\{\}}\Pi^{\mathrm{AB}}$, as discussed in the main text. In the diagram on the right, $\mathcal{F}^{\mathrm{ideal}}_{\{\}}$ denotes the desired ideal resource when all parties are honest. We require the outer interfaces of the protocol converters $\Pi^{\mathrm{A}}, \Pi^{\mathrm{B}}$ to have the same structure as those of $\mathcal{F}^{\mathrm{ideal}}_{\{\}}$, i.e. the interfaces shown in blue have the same structure in both the left and right diagrams. We describe more precisely in the rest of this section (see e.g. Definition 1) how to formalize a notion that the resources in the left and right diagrams are "close" to each other.

analogously for $\mathcal{F}'$. Its *distinguishing advantage* λ between these two resources is defined to be

$$\lambda = \left|\mathsf{P}_{G|\mathcal{F}}(0) - \mathsf{P}_{G|\mathcal{F}'}(0)\right| = \frac{1}{2}\left\|\mathsf{P}_{G|\mathcal{F}} - \mathsf{P}_{G|\mathcal{F}'}\right\|_1 .$$

The main way we shall make use of this concept is as a method to formalize how "close" two resources are to each other — if the distinguishing advantage between the two resources is small for any possible distinguisher, it seems reasonable to say these resources are "close". This notion of closeness also has important operational implications, as we shall explain later in Section 2.1.3.

2.1.2 Security definitions

With these concepts, we can now discuss the security definitions in this framework. Suppose that as mentioned above, we have a resource tuple $\left(\mathcal{F}^{\mathrm{real}}_P\right)_{P\subseteq Q}$ describing the real functionalities available to the various parties, and a protocol $\mathscr{P}$ with inner interfaces connecting to $\mathcal{F}^{\mathrm{real}}_{\{\}}$, with the informal goal of constructing a more idealized resource tuple $\left(\mathcal{F}^{\mathrm{ideal}}_P\right)_{P\subseteq Q}$. We would like to formalize the notion of having achieved a sufficiently "good" conversion from $\left(\mathcal{F}^{\mathrm{real}}_P\right)_{P\subseteq Q}$ to $\left(\mathcal{F}^{\mathrm{ideal}}_P\right)_{P\subseteq Q}$. To do so, we use the following approach: for each possible subset $P \subseteq Q$ of the potentially-dishonest parties, consider the scenario where all parties in P choose to behave dishonestly. In such a scenario, it makes sense to consider the resource $\Pi^{\overline{P}}\mathcal{F}^{\mathrm{real}}_P$ (here, $\overline{P}$ denotes the set complement of P with respect to the set of *all* parties, not just with respect to Q)[2] — this is the

[2]For instance in our certified deletion protocol between Alice, Bob and Eve (labelled as $\mathrm{A}, \mathrm{B}, \mathrm{E}$), when considering e.g. $P = \{\mathrm{E}\}$ the notation $\overline{P}$ means the set $\{\mathrm{A}, \mathrm{B}\}$ (despite the fact that only we only consider Bob and Eve to be potentially dishonest, i.e. $Q = \{\mathrm{B}, \mathrm{E}\}$).

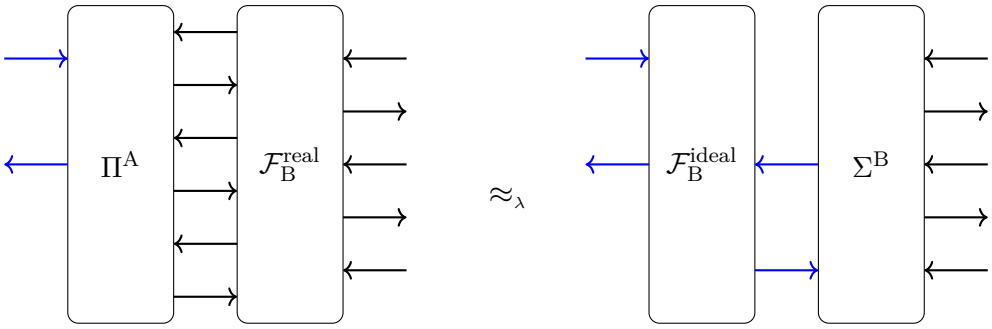


Figure 2: Schematic depiction of one case in Definition 1, in a scenario with only two parties Alice and Bob (labelled as A, B). Shown here is the case where $P = \{\mathrm{B}\}$, i.e. only Bob is being dishonest. On the left, we have the real resource $\mathcal{F}_{\mathrm{B}}^{\mathrm{real}}$ with the protocol Π^{A} attached (this captures the notion that Alice is performing her protocol honestly). On the right, we have the ideal resource $\mathcal{F}_{\mathrm{B}}^{\mathrm{ideal}}$ with a simulator Σ^{B} attached (the role of the simulator is described in the main text). Note that both the left and right sides have outer interfaces with the same structure. Definition 1 requires both sides to be "λ-close" in the sense that the distinguishing advantage between them is at most λ for any distinguisher. Similarly, Definition 1 also requires "λ-closeness" for any other subset P of the potentially dishonest parties and the corresponding analogously defined resources. (In fact the case $P = \{\}$, i.e. none of the parties are dishonest, is basically depicted in Figure 1 — Definition 1 requires the left and right resources in that figure to also be "λ-close".)

resource obtained when the parties in $\overline{P}$ interact with the real resource $\mathcal{F}_P^{\mathrm{real}}$ using the protocol converters $\Pi^{\overline{P}}$ "as intended", while the parties in P do not implement the protocol converters since they are behaving dishonestly. (We give a schematic depiction of this in the left diagram in Figure 2.)

As a first attempt, we could try saying that this resource $\Pi^{\overline{P}}\mathcal{F}_P^{\mathrm{real}}$ should be required to be "close to" the resource $\mathcal{F}_P^{\mathrm{ideal}}$, i.e. the ideal resource for the case where all parties in P behave dishonestly. Furthermore, a natural notion of "closeness" between resources is to say that the maximum possible distinguishing advantage is small, as discussed above. Unfortunately, this idea does not quite work by itself, because the interfaces for the dishonest parties P in the resource $\Pi^{\overline{P}}\mathcal{F}_P^{\mathrm{real}}$ are simply those of the real resource $\mathcal{F}_P^{\mathrm{real}}$ (since no converters have been attached to those interfaces), which could generally be very different from those of the ideal resource $\mathcal{F}_P^{\mathrm{ideal}}$. The solution for overcoming this issue turns out to be allowing the attachment of an additional converter Σ^P (referred to as a *simulator*) to the interfaces of the dishonest parties P in $\mathcal{F}_P^{\mathrm{ideal}}$, and only requiring $\Pi^{\overline{P}}\mathcal{F}_P^{\mathrm{real}}$ to be "close to" $\mathcal{F}_P^{\mathrm{ideal}}\Sigma^P$ rather than $\mathcal{F}_P^{\mathrm{ideal}}$. (We depict this in Figure 2.) At first sight, this appears to be a rather contrived approach, since there seems to be no purpose to this simulator other than as an artificial method to make the interfaces of $\mathcal{F}_P^{\mathrm{ideal}}$ the same as those of $\Pi^{\overline{P}}\mathcal{F}_P^{\mathrm{real}}$. However, we shall return to this point in the next section (after formalizing these security notions as Definition 1 below), and explain how this apparently contrived concept in fact leads to powerful operational implications.

We now present the full security definition we use, which formalizes the above discussions and clarifies the quantifier ordering (also see Figure 2 for an example of one case in the definition):

Definition 1. *For a scenario in which there is some set Q of potentially dishonest parties, we say that $\mathscr{P}$* constructs $\left(\mathcal{F}_P^{\mathrm{ideal}}\right)_{P\subseteq Q}$ from $\left(\mathcal{F}_P^{\mathrm{real}}\right)_{P\subseteq Q}$ within distance λ *iff the following holds: for every $P \subseteq Q$, there exists a converter Σ^P which connects to their interfaces in $\mathcal{F}_P^{\mathrm{ideal}}$, such that for every distinguisher, the distinguishing advantage between $\Pi^{\overline{P}}\mathcal{F}_P^{\mathrm{real}}$ and $\mathcal{F}_P^{\mathrm{ideal}}\Sigma^P$ is at most λ. The*

converters Σ^P shall be referred to as simulators.

Remark 2. *We have stated Definition 1 slightly differently from [MR11], in which an individual simulator is required for each dishonest party. A security proof satisfying Definition 1 could be converted into one satisfying the [MR11] definition by modifying the choice of $\left(\mathcal{F}_P^{\text{ideal}}\right)_{P\subseteq Q}$ to one that (for every P containing more than one party) explicitly includes quantum channels between the dishonest parties P, which would allow for individual simulators that communicate using these quantum channels in order to effectively implement the simulator Σ^P in Definition 1. From the perspective of [MR11], this would basically reflect the inability of a protocol to* guarantee *that the dishonest parties cannot communicate with each other. For subsequent ease of describing the simulators, in this work we shall follow Definition 1 as stated, instead of the exact definition in [MR11].*

2.1.3 Operational implications

The operational implications[3] of Definition 1 can be seen by considering the composition of protocols satisfying this definition. Namely, suppose we have a protocol $\mathscr{P}$ that constructs $\left(\mathcal{F}_P^{\text{ideal}}\right)_{P\subseteq Q}$ from $\left(\mathcal{F}_P^{\text{real}}\right)_{P\subseteq Q}$ within distance λ in the sense of Definition 1. Consider any larger protocol $\mathscr{P}'$ that is designed to use the ideal functionality $\left(\mathcal{F}_P^{\text{ideal}}\right)_{P\subseteq Q}$ as a resource. We want to study what happens if this intended functionality $\left(\mathcal{F}_P^{\text{ideal}}\right)_{P\subseteq Q}$ is replaced by the protocol $\mathscr{P}$ applied to $\left(\mathcal{F}_P^{\text{real}}\right)_{P\subseteq Q}$.

To do so, let us pick any $P \subseteq Q$ and focus on the scenario where the parties P are dishonest. Now take any event in this scenario that could be considered a "failure" in the larger protocol (we impose no restrictions on the nature of a failure, except that it be a well-defined event), and suppose the larger protocol also comes with a proof that for any strategy by the dishonest parties, the probability of this failure event is upper-bounded by some p_0 when using the ideal resource $\mathcal{F}_P^{\text{ideal}}$. In that case, one implication of Definition 1 being satisfied is that the probability of this failure event (in the larger protocol) is still at most $p_0 + \lambda$ even when $\left(\mathcal{F}_P^{\text{ideal}}\right)_{P\subseteq Q}$ is replaced by the protocol $\mathscr{P}$ applied to $\left(\mathcal{F}_P^{\text{real}}\right)_{P\subseteq Q}$. This follows from the following observations. Firstly, since the bound p_0 for the functionality $\mathcal{F}_P^{\text{ideal}}$ holds for any strategy by the dishonest parties, it must in particular hold when they implement the simulator Σ^P, i.e. it holds if they are using $\mathcal{F}_P^{\text{ideal}}\Sigma^P$ instead of $\mathcal{F}_P^{\text{ideal}}$. Secondly, since the distinguishing advantage between $\mathcal{F}_P^{\text{ideal}}\Sigma^P$ and $\Pi^{\overline{P}}\mathcal{F}_P^{\text{real}}$ is at most λ according to Definition 1, the probability of the failure event cannot differ by more than λ between them (otherwise the event would serve as a way to distinguish the two cases with advantage greater than λ). In other words, the replacement has not increased the maximum probability of the failure event by more than λ — we highlight again that this failure event could have been chosen to be any arbitrary event; hence this is a very powerful operational statement.

From this argument, we can also gain insight into the purpose of the apparently contrived simulators Σ^P in Definition 1. Basically, they represent some operations that the dishonest parties *could have performed* using only the ideal resource $\mathcal{F}_P^{\text{ideal}}$. While these operations are not necessarily

[3] A more abstract composability notion given by this definition is that if several protocols satisfying this definition are composed, the "error" λ of the resulting larger protocol can be bounded by simply by adding those of the sub-protocols; see [MR11] for further details.

the "optimal" ones they could do in order to "attack" $\mathcal{F}_P^{\text{ideal}}$, the fact remains that they are valid operations for the dishonest parties, and are hence subject to the bound p_0 on the failure probability. Critically, this was enough for the rest of the argument above to carry through, even though the simulator Σ^P may be carrying out some complicated operations that have no correspondence to any sort of reasonable "attack" on $\mathcal{F}_P^{\text{ideal}}$. Such arguments are not uncommon in simulator-based notions of security (even outside the Abstract Cryptography framework), the shared underlying idea being typically that the real behaviour could have been reproduced (or approximated) by taking *only* the ideal behaviour and applying some operations to it, hence it essentially suffices to only consider the ideal behaviour. (In the context of our specific protocol, we shall briefly discuss this further in Remark 8 of Sec. 6.1.)

There is a technicality in the above argument, namely that in order for the reasoning to be valid, the bound p_0 (for the larger protocol $\mathscr{P}'$ using $\mathcal{F}_P^{\text{ideal}}$) must be derived for a class of dishonest-party strategies that includes the simulator Σ^P, in order for the bound to hold for $\mathcal{F}_P^{\text{ideal}}\Sigma^P$ as well. This means that if a more "powerful" simulator is used in Definition 1, then the bound p_0 must be proved against a more "powerful" class of strategies. In particular, for instance the simulators Σ^P we construct in this work assume that the dishonest parties P collaborate to some extent (when there are multiple dishonest parties), which means that to apply the above operational interpretation, the bound p_0 for the larger protocol must be valid against collaborating dishonest parties. However, we note that this is more of a consideration for the larger protocol $\mathscr{P}'$, rather than the protocol $\mathscr{P}$ in Definition 1 itself.

2.2 Ideal ECD functionality

We work in a setting with three parties: Alice who is always honest, and Bob and Eve who may independently be honest or dishonest. The inputs for Alice and honest Bob into the functionality are:

(i) Message $M \in \{0,1\}^n$ from Alice at time t_2

(ii) Deletion decision $D \in \{0,1\}$ from Alice at time t_3

and their outputs are:

(i) Abort decision $O \in \{\top, \bot\}$ to Alice and Bob at time t_1

(ii) Deletion decision D to Bob at time $\dot{t}_3$

(iii) Deletion flag $F \in \{\checkmark, \times\}$ to Alice at time t_4

(iv) $\widetilde{M} = \begin{cases} M & \text{if } D \wedge F = 0 \\ 0^n & \text{if } D \wedge F = 1 \end{cases}$ to Bob at time t_5

where for the purposes of applying the AND function to the binary symbols $\{\times, \checkmark\}$, $\times$ is interpreted as 0.

The times corresponding to the inputs and outputs must satisfy $t_1 \leq t_2 \leq t_3 \leq \dot{t}_3 \leq t_4 < t_5$. In particular, we shall call a functionality an ideal ECD functionality if it produces the above inputs and outputs at any points in time satisfying the above constraints. We have strict inequality only between t_4 and t_5 because this is necessary in any real protocol for achieving the functionality.

We now describe how the honest inputs and outputs are to be interpreted. Alice and Bob's output O is to detect interference by Eve. If $O = \perp$ then the protocol stops and no further inputs are fed in or outputs are received. Alice's input M is self-explanatory: this is the secret message that she potentially wants Bob to learn. Alice's decision D is her later decision about whether she wants Bob to learn M: some time after inputting the message but strictly before the time t_5 when the message is supposed to be revealed, Alice inputs $D = 1$ if she does not want Bob to learn M; otherwise she inputs $D = 0$. D is directly output to Bob some time after Alice inputs it. The output F to Alice is only produced if $D = 1$, and this indicates whether Bob has produced a valid deletion certificate (although the deletion certificate itself is not part of the ideal functionality). If Bob is honest then he always produces a valid certificate if Alice asks him to, and F is always ✓. Finally, the output $\widetilde{M}$ to Bob is a function of M, D and F: if $D = 0$, i.e., Alice wanted him to learn the message, or $F =$ ✗, i.e., he did not produce a valid deletion certificate, then $\widetilde{M} = M$; otherwise it is the dummy string 0^n.

Now we come to the inputs and outputs of dishonest parties, which are the following:

(i) Abort decisions O^{B} and $O^{\mathrm{E}} \in \{\top, \perp\}$ from Bob and Eve at times t_1', t_1'' respectively

(ii) Deletion decision $D \in \{0, 1\}$ to Eve at time $\ddot{t}_3$

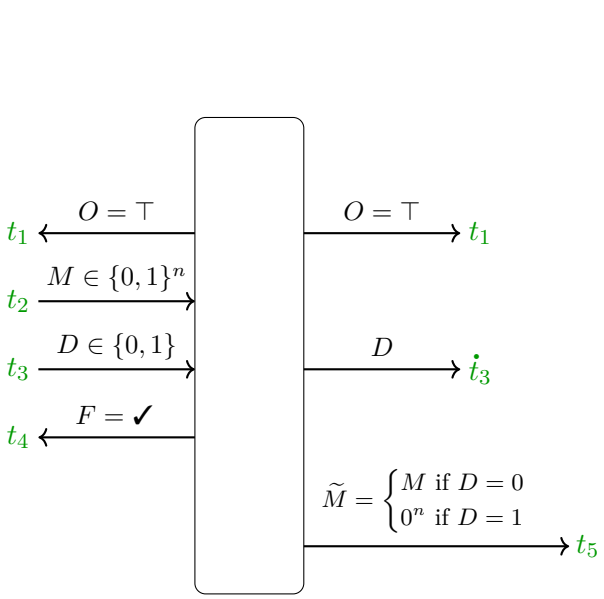
(iii) Deletion flag $F \in \{$✓, ✗$\}$ from Bob at time t_4'.

The times corresponding to these inputs and outputs must satisfy the following ordering with respect to the previously specified times: $t_1', t_1'' \leq t_1$, $t_3 \leq \ddot{t}_3$ and $\dot{t}_3 \leq t_4' \leq t_4$. We remark that we are indifferent about the relative ordering of t_1', t_1'' and $\dot{t}_3, \ddot{t}_3$.

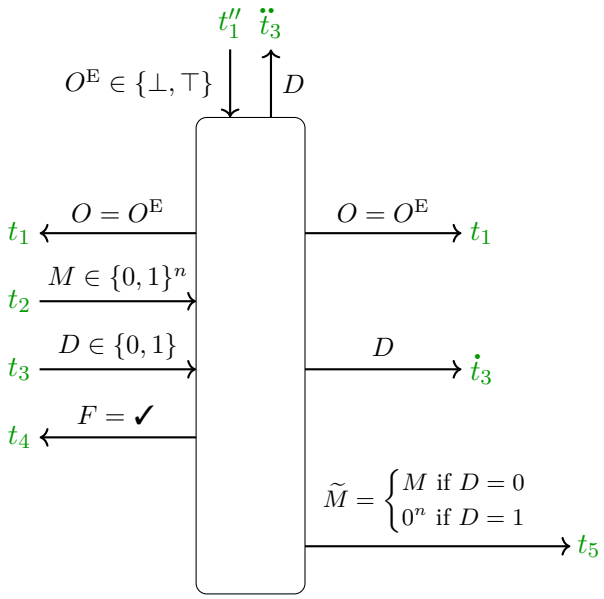
Eve's input O^{E} is similar to what she has in the ideal key distribution functionality that is achieved by quantum key distribution (see e.g. [PR14]). She has the ability to interfere in a way that makes the honest parties abort the protocol. If Bob is honest then Eve's choice of O^{E} directly gets output to Alice and Bob as O and the protocol stops if $O^{\mathrm{E}} = \perp$. However, if $O^{\mathrm{E}} = \top$, then the protocol continues and Eve gets nothing other than D as further outputs, and in particular she is not able to learn the message. We include D as an output for Eve because we cannot prevent her from learning this in our actual protocol. Dishonest Bob also has an input O^{B} that he can use to make the protocol abort: Alice and Bob's output O is $\perp$ if *either one of* Bob and Eve inputs $\perp$. We include this input for Bob because in the real protocol we cannot prevent Bob from deliberately sabotaging whatever test Alice and Bob are supposed to perform in order to detect interference from Eve, so that the output is $O = \perp$.[4] Finally, Bob's input F indicates whether he has decided to produce a valid deletion certificate and hence lose his ability to learn the message or not, and this is directly output to Alice. Honest Bob does not have this functionality, as he simply always deletes his information if requested by Alice.

The final ECD_n functionality, parametrized by the message length n, is depicted in Figure 3 in the four possible combinations of honest and dishonest Bob and Eve. A security proof of a protocol for ECD_n with security parameter λ will consist of showing that the protocol constructs the functionality depicted in Figure 3 within distance λ as per Definition 1.

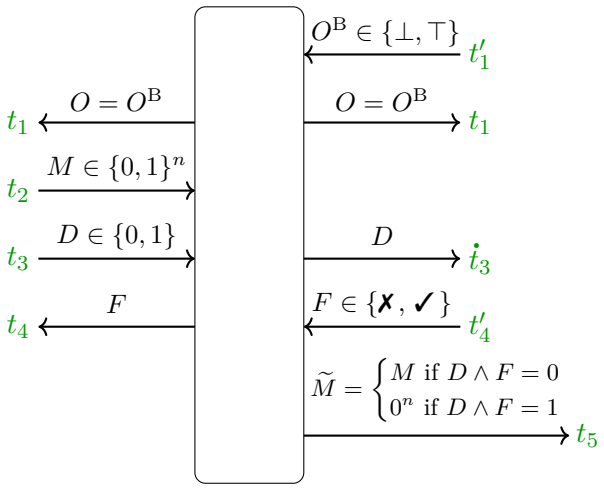
[4] Certainly from the point of view of the ECD functionality such an action by Bob seems pointless, but we cannot exclude this possibility for any composable security proof, since we do not know Bob's motivations in some hypothetical larger protocol in which the real ECD protocol is used, and it may be useful for Bob there if the protocol outputs $\perp$.



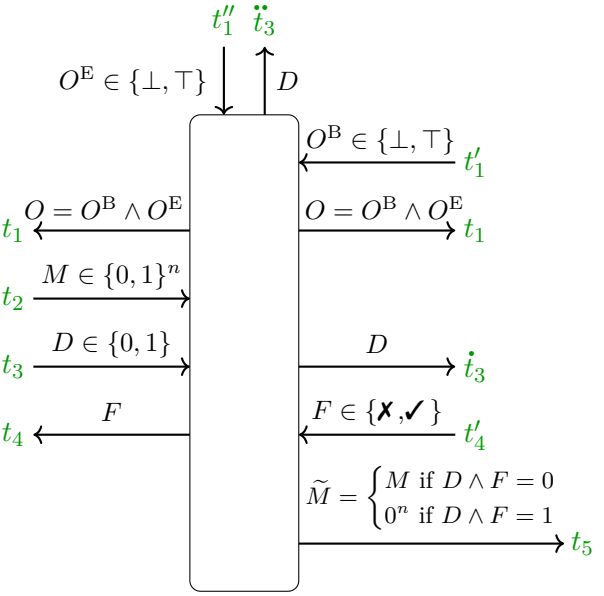
(a) Alice, honest Bob and honest Eve



(b) Alice, honest Bob and dishonest Eve



(c) Alice, dishonest Bob and honest Eve



(d) Alice, dishonest Bob and dishonest Eve

Figure 3: Ideal ECD_n functionality in four cases. The times at which various events occur satisfy $t'_1, t''_1 \leq t_1 \leq t_2 \leq t_3 \leq \dot{t}_3, \ddot{t}_3 \leq t'_4 \leq t_4 < t_5$. All inputs and outputs after O are only provided if $O = \top$; the F input and output are only provided if $D = 1$. $\bot$ and ✗ are interpreted as 0 for the AND function.

2.3 Achievability result

Before stating the result about our protocol constructing the ideal ECD functionality, we clarify what resources are used by the protocol, and what assumptions are needed on said resources.

Resources used.

(i) Boxes $(\mathcal{B}^1, \mathcal{B}^2)$ of the form $(\mathcal{B}^1_1 \dots \mathcal{B}^1_l, \mathcal{B}^2_1 \dots \mathcal{B}^2_l)$, where each $(\mathcal{B}^1_i, \mathcal{B}^2_i)$ is compatible with one instance of the magic square game MS. These boxes are "untrusted", in the sense that Eve[5] supplies them to Alice and Bob after having chosen the states in the boxes and the measurements they perform.

(ii) A trusted temporarily private randomness source $\mathcal{R}$, which if used by Alice by time t_1, makes public all the randomness it supplied at some time $t_4 < t'_5 \leq t_5$.

(iii) A trusted private randomness source $\mathcal{R}^P$ with Alice (which does not make public the randomness it supplies to Alice).

(iv) An authenticated classical channel $\mathcal{C}$ between Alice and Bob, which faithfully transmits all classical messages sent between them, but also supplies copies of the messages to Eve; the channel only needs to be active until time t_4.

Assumptions about quantum boxes. We make the following standard assumptions about the boxes $(\mathcal{B}^1, \mathcal{B}^2)$ for device-independent settings:

(i) The boxes cannot access any registers storing private information from previous protocols, and this restriction continues to hold if the boxes are re-used in future protocols.

(ii) When held by an honest party, the boxes do not broadcast the inputs supplied to them and outputs obtained.

(iii) There is a tripartite tensor-product structure across the state in the $\mathcal{B}^1$ boxes, the state in the $\mathcal{B}^2$ boxes, and Eve's side-information.[6]

(iv) Whenever Bob is dishonest, he can "open" his boxes and directly perform arbitrary operations or measurements on the quantum state they contained. (This matches the allowed dishonest behaviours in other DI protocols for two-party cryptographic tasks [ACK+14, SCA+11, AMP+16, KST22, FM18].)

The first assumption here is to address the memory attack of [BCK13], as mentioned in the introduction (an alternative possibility would be to require that this is the first time the devices are used, and the devices are destroyed afterwards, though this is rather impractical). The second assumption is a basic one that is rather necessary to do any cryptography at all, and the third is a standard nonlocal-game scenario that could be enforced in principle by spatial separation between the parties.

Additionally, however, we also impose the following assumption:

[5] This describes the resource behaviour in the cases where Eve is dishonest. In the case where only Bob is dishonest, we shall consider Bob to be the party choosing the box behaviour.

[6] With the technical exception of the case where both Bob and Eve are dishonest, since they may choose to collaborate in that case; however, this is not too important since even this case can in principle be mapped to a tensor-product structure with quantum communication between Bob and Eve.

(v) Whenever Bob is honest (but the boxes are supplied by a potentially dishonest Eve), he is able to enforce that his l boxes $\mathcal{B}_1^2 \dots \mathcal{B}_l^2$ satisfy no-signalling conditions between them — this could, for instance, be supported by physical "shielding" measures between the boxes that prevent the input to each box from leaking to other boxes. This implies that for any subset $T \subseteq [l]$, there is a well-defined notion of Bob supplying inputs to only the boxes specified by T and immediately receiving the corresponding outputs, with the rest of the inputs to be supplied later (such a procedure is required in our protocol). Furthermore, this no-signalling constraint also implies that the overall output distribution across all the rounds will be unaffected by which subset T of inputs Bob supplies first.

This condition is rather stronger than the typical requirements in the device-independent setting (for non-IID situations, at least). However, it appears to be necessary to ensure security against dishonest Eve in our protocol, though it could be omitted if we instead aim for a more limited functionality similar to [BI20] that does not consider security against an eavesdropper, or potentially it could be worked around using some ideas developed in [KT22]. We defer further discussion of this point to Section 2.4 below.

When Eve and Bob are honest, we assume that the boxes $(\mathcal{B}_1^1 \dots \mathcal{B}_l^1, \mathcal{B}_1^2 \dots \mathcal{B}_l^2)$ play MS^l with an i.i.d. strategy, although they may do so $\varepsilon/2$-noisily. That is, each box independently wins MS with probability $1 - \varepsilon/2$ instead of 1, for some $\varepsilon > 0$.

We shall use $(\mathcal{B}_1^1 \dots \mathcal{B}_l^1, \mathcal{B}_1^2 \dots \mathcal{B}_l^2)_\varepsilon$ to refer to boxes with the above properties.

Theorem 2. *Assuming Conjecture 1, there exists a universal constant $\varepsilon_0 \in (0,1)$ such that for any $\varepsilon \in (0, \varepsilon_0]$, $\lambda \in (0,1]$ and $n \in \mathbb{N}$, there is a protocol that constructs the ECD_n functionality depicted in Figure 3, within distance λ, using only the resources $\mathcal{R}$, $\mathcal{C}$ and $(\mathcal{B}_1^1 \dots \mathcal{B}_l^1, \mathcal{B}_1^2 \dots \mathcal{B}_l^2)_\varepsilon$ for some $l = l(\lambda, \varepsilon, n)$.*

We reiterate here from Section 1.1 that in the above theorem, Conjecture 1 is not required to show intermediate security properties (see Lemmas 25–27), but only to show that these properties lead to composable security. Furthermore, even without that conjecture, our proof is sufficient to show that the protocol is composably secure in the standard device-dependent setting at least.

Remark 3. *The resources we use put some constraints on the timings achievable in the ECD_n functionality. For example, if $\mathcal{R}$ makes the randomness used by Alice public at time t_5', then t_4 and t_5 must satisfy $t_4 < t_5' \leq t_5$. Similarly, the delay between t_3 and $\dot{t}_3$, t_4' and t_4 depend on the time taken to transmit information between Alice and Bob using $\mathcal{C}$.*

2.4 Implications of security definitions and assumptions

A number of points regarding our definition of the ideal functionality, the composable security framework, the resources used, and what they mean for security, need further clarification. We do this below.

- While the message D from Alice indicates whether she would like Bob to delete his ciphertext, the final decision of whether Bob actually does so is entirely up to him. Because of this, one could consider a variant protocol and ideal functionality definition where this message D is omitted. However, it is easy to see that our security proof also proves the security of this variant (one way to see this would be to note that it is basically equivalent to the

distinguisher always selecting $D = 1$, and since our security proof needs to cover any distinguisher strategy, in particular it also includes this possibility).

- In line with the Abstract Cryptography framework, we have defined the ideal functionality above for all four combinations of honest/dishonest Bob and Eve. In particular, we remark that in the case where both Bob and Eve are dishonest, this framework does not explicitly specify whether they collaborate with each other — the framework is *a priori* neutral about this possibility. However, in our proof, the simulator we construct to satisfy Definition 1 for this case does involve some collaboration between them. This does not affect the abstract definition, but we reiterate that it has implications for the operational interpretation as described in Section 2.1. Specifically, to "safely" use our protocol in place of the ideal ECD functionality in a larger protocol, the bounds on failure probabilities in the larger protocol when Bob and Eve are dishonest must at least hold for the case where Bob and Eve collaborate enough to implement the simulator we constructed.

- Our protocol is clearly unable to guarantee the *absence* of communication between Bob and Eve when both are dishonest. Hence while we did not explicitly specify a communication channel between them in the ideal functionality, we do implicitly allow for the possibility. (As previously mentioned, our security proof proceeds without explicitly including such a channel in the ideal functionality, because we have stated Definition 1 using joint simulators for the dishonest parties.)

- We imposed a condition that honest Bob's boxes satisfy no-signalling conditions between them. This is required for our security proof in the case where Bob is honest and Eve is dishonest, because it relies on the existence of a single distribution $\mathsf{P}_{AB|XY}$ that describes the Alice-Bob input-output behaviour regardless of the order in which Bob supplies his inputs (essentially because in our proof here we use a sampling lemma that requires the underlying distribution to be independent of the sampled subset).[7] (An analogous condition is not required for Alice because she supplies all her inputs at once in our protocol.) However, if we were to instead restrict ourselves to a more restricted two-party functionality that omits Eve from the scenario considered here (i.e. similar to [BI20], which does not model a third-party eavesdropper), then this condition would be unnecessary, due to the discussion in the next point.

- In contrast, whenever Bob is dishonest, we do not require an analogous condition — this is consistent with the fact that we allow dishonest Bob to "open" his boxes and perform arbitrary operations on the states within. This is not a problem for our security proof against dishonest Bob, because the distribution $\mathsf{P}_{AB|XY}$ in that context is not quite a fixed input-output distribution for "abstract" boxes, but rather describes the conditional distribution of the strings AB when dishonest Bob produces B using some operation chosen depending on a string Y which he learns over several steps (although Alice is indeed obtaining A by just supplying X as input to her boxes). In particular, in that proof it is acceptable for there to be a different distribution $\mathsf{P}_{AB|XY}$ for each possible order in which Bob learns the string Y. (From a physical standpoint, the order in which Bob learns Y does impose some time-ordering constraints on the parts of B that he produces before learning all of Y; however, it seems difficult to make use of such constraints in the proof. Hence we simply use the fact that

[7] Still, in [KT22] we recently proposed a protocol with a different approach for the random sampling, and it seems possible in principle that the approach there could be adapted to the ECD protocol in order to remove the no-signalling condition on honest Bob's boxes, though that would be beyond the scope of this work.

for each possible order in which Bob learns Y, there is a resulting distribution $\mathsf{P}_{AB|XY}$ which falls within the larger set of correlations captured in the parallel-repetition framework.)

- Ideally, we would like to have a protocol for ECD that does not require private randomness on Alice's side. This is because if Alice had access to randomness that remains private unless she chooses to communicate it, she could simply one-time pad her message with a random string to generate the ciphertext, then refuse to reveal the random string to Bob later if she decides she does not trust him. However, our current protocol does involve some private randomness, due to a technical point in our security proof: we prove security by means of an anchored parallel repetition theorem, where only part of Alice's input is revealed to Bob or Eve. This seems to be a limitation of parallel proof techniques that have been given so far — parallel QKD security proofs also have this requirement [JMS20, Vid17], and for essentially this reason, there have been no parallel security proofs of device-independent randomness expansion. Still, the advantage of our protocol over the trivial protocol with private randomness we just described is that in the trivial protocol, Alice needs to communicate with Bob at the moment when she decides whether the message should be revealed or not, whereas this is not required in our protocol: Alice can simply rely on the temporarily private randomness source to reveal all the information that Bob needs for decryption, and the randomness that Alice got from the private randomness source is not needed for decryption. In other words, we can suppose Alice does not even have a communication channel with Bob after a certain point, in which case the trivial protocol does not work. (Overall, this issue is somewhat due to the formalization we chose here for "leaking the decryption key" in the composable framework — in contrast, in the game-based framework of [BI20], one simply declares what is to be counted as part of the decryption key.)

2.5 Alternative security definition

In order to provide an easier comparison to previous works, we now describe an alternative set of security definitions that could be considered, in a framework that is more similar to that considered in [BI20]. However, as the setup we consider is an extended version of that considered in [BI20], some changes as compared to the definitions in that work are necessary — we elaborate on those changes after presenting these modified definitions. (These security definitions are somewhat similar to some intermediate properties in our composable security analysis, but our purpose in stating them here is mainly to ease comparison with [BI20]. Some features of this definition are similar to [GMP22], which also featured interactive encryption schemes.) As we are aiming for information-theoretic security, we present various conditions below in terms of trace distance (rather than distinguishability with respect to a computationally bounded adversary).

Alternative Definition 1. *A device-independent ECD protocol involves two parties Alice and Bob and a potential third-party "eavesdropper" Eve, out of which Alice always behaves honestly while Bob and Eve might behave dishonestly. It consists of an* encryption *phase, followed by an optional* certified deletion *phase, and finally a* decryption *phase. These phases have the following structure, where we let Q_B denote a register that Bob holds and updates arbitrarily over the course of each phase (there is no loss of generality in using a single register for this purpose, because we do not bound its dimension), and analogously we have a register Q_E for Eve. (As for Alice, she is always honest in this scenario, hence in the following we only state the registers she is supposed to hold at the end of each phase.)*

- *In the encryption phase, Alice and Bob begin with boxes of the form described in Section 2.3, and perform an interactive procedure (over a public authenticated channel) that outputs a classical value $O \in \{\top, \bot\}$ (informally, indicating whether "eavesdropping" was detected). If $O = \bot$, Alice and Bob do not proceed further beyond this point. If $O = \top$, Alice then chooses a message m, and Alice and Bob perform some further interactive steps, during which Alice generates a decryption key R and an additional string P for potential use in the certified deletion phase, while Bob generates some quantum ciphertext state (depending on the message m). At the end, each party has the following registers: Alice holds the classical registers ORP, Bob holds his register Q_B containing the ciphertext state and possibly some other quantum side-information, and Eve holds some quantum side-information in Q_E.*

- *In the certified deletion phase (if it occurs), Alice computes some message using the string P and sends it to Bob. Alice and Bob then perform an interactive procedure (in which Bob can use the register Q_B retained from the encryption phase), at the end of which Alice uses the string P to produce a classical value $F \in \{\checkmark, \text{✗}\}$ (indicating whether she accepted the deletion certificate). At the end, each party has the following registers: Alice holds the classical registers ORF, and Bob and Eve hold some quantum side-information in their respective registers Q_B and Q_E.*

- *In the decryption phase, Alice sends the decryption key R to Bob using the authenticated public channel. Bob then performs some local operations using R and his register Q_B, producing some classical value $\widetilde{M}$ (intended to be a guess for the message m). At the end, each party has the following registers: Alice holds the classical registers OF, Bob's register Q_B contains the classical value $\widetilde{M}$ and possibly some other quantum side-information, and Eve holds some quantum side-information in Q_E.*

We require that the ECD protocol satisfies notions of completeness, correctness, and secrecy, defined as follows (where the parameters $\lambda_{\mathrm{com}}, \lambda_{\mathrm{EC}}, \lambda_{\mathrm{CI}}$ have values in $[0,1]$):

- *The protocol is λ_{com}-complete if, whenever Bob and Eve are behaving honestly, we have*

$$\Pr[O = \bot] \leq \lambda_{\mathrm{com}}, \tag{1}$$

and whenever Bob is honest and the certified deletion phase occurs, we have

$$\Pr[O = \top \wedge F = \text{✗}] \leq \lambda_{\mathrm{com}}. \tag{2}$$

- *The protocol is λ_{EC}-correct if for any choice of message m, whenever Bob is behaving honestly, we have*

$$\Pr[O = \top \wedge \widetilde{M} \neq m] \leq \lambda_{\mathrm{EC}}. \tag{3}$$

- *The protocol is λ_{CI}-secret if for any choice of message m, all of the following conditions hold. Firstly, for any behaviour by Bob and Eve, at all times between the point where O is produced and the point where Alice releases the decryption key R, we have (letting $\omega_{Q_B Q_E|\top}(m)$ denote the state produced at that point in time when the chosen message value is m, conditioned on $O = \top$)*

$$\Pr[O = \top] \left\| \omega_{Q_B Q_E|\top}(m) - \omega_{Q_B Q_E|\top}(0^n) \right\|_1 \leq 2\lambda_{\mathrm{CI}}, \tag{4}$$

and furthermore, if the certified deletion phase occurs, then at all times after F is produced (including after Alice releases the decryption key R), we have (letting $\omega_{Q_B Q_E|\top\checkmark}(m)$ denote the state produced at that point in time when the chosen message value is m, conditioned on $O = \top$ and $F = \checkmark$)

$$\Pr[O = \top \wedge F = \checkmark] \left\| \omega_{Q_B Q_E|\top\checkmark}(m) - \omega_{Q_B Q_E|\top\checkmark}(0^n) \right\|_1 \leq 2\lambda_{\mathrm{CI}}. \tag{5}$$

Secondly, whenever Bob is behaving honestly (while Eve may not be), at all times after O is produced, we have (where $\omega_{Q_E|\top}(m)$ is defined analogously to above)

$$\Pr[O = \top] \left\| \omega_{Q_E|\top}(m) - \omega_{Q_E|\top}(0^n) \right\|_1 \leq 2\lambda_{\mathrm{CI}}. \tag{6}$$

As compared to the security definitions in [BI20], the above definitions may appear somewhat elaborate. However, this is necessary in some form due to the additional features we intend to incorporate here as compared to that work (such as security against an eavesdropper Eve, as well as the DI security guarantee), which in particular have required us to include in our protocol some additional interaction rounds and a flag O to test for eavesdropping, as compared to [BI20]. Since their protocol involves comparatively few rounds of interaction, they were able to present their definitions using an explicitly denoted individual channel for each round; however, such a presentation would quickly become unwieldy for our protocol. Hence in the above definition we have simply described the processes in terms of "interactive procedures", which are to be implicitly understood as some sequence of channels performed by the relevant parties, and we have introduced the registers Q_B, Q_E to account for dishonest Bob and/or Eve arbitrarily updating their registers over that process. (A similar approach has been used in other recent work on encryption protocols with interaction; see for instance Definition 5.8 in [GMP22].) To aid understanding, we now qualitatively describe the intuition behind each of the requirements in the above definition, and compare them to [BI20].

Firstly, the completeness conditions (1)–(2) simply reflect the notion that when various parties are behaving honestly, the corresponding flags should take the "accept" value with high probability. More specifically, (1) states that when there is no eavesdropping, the flag O takes value $\top$ with high probability (this has no counterpart in [BI20], which does not check for eavesdropping); while (2) basically ensures that when Bob validly deletes his information, the flag F takes value ✓ with high probability (this corresponds to Eq. (37) in [BI20], though here we slightly modify the condition to account for the O flag).

Next, the correctness condition (3) is also straightforward: it simply requires that when Bob behaves honestly, then regardless of how Eve acts, the probability that Bob decrypts to the wrong message and the flag O is set to the "accept" value is small. This is the same as the definition of correctness provided in Section 5.2 of [BI20].

Finally, the secrecy condition is the one which appears most different from [BI20]. Qualitatively, (4) and (5) are meant to correspond respectively to the notions of *ciphertext indistinguishability* and *certified deletion security* in [BI20]: each of these notions informally describes some idea of an adversary trying to distinguish between an encryption of the actual message versus an encryption of the all-zero string 0^n.[8] In [BI20], those definitions could be presented using a small

[8] More specifically, ciphertext indistinguishability covers the situation where the adversary does not yet have access to the decryption key, while certified deletion security covers the situation where the certified deletion procedure has taken place and the adversary is then supplied with the decryption key.

number of explicitly denoted channels applied by the adversary, due to the small number of communication rounds in their protocol. However, our protocol involves too many rounds for this to be a practical description. We hence instead impose conditions in terms of the trace distance between the states produced in the two cases, and require these conditions to hold over the relevant timeframes. Due to the operational interpretation of trace distance as distinguishing advantage, this corresponds to a bound on the probability of an adversary successfully distinguishing the two cases (up to some technicalities about conditioning on the OF flag values), hence having implications that are qualitatively similar to the [BI20] definitions of ciphertext indistinguishability and certified deletion security. Lastly, (6) is meant to ensure an analogous notion of indistinguishability from Eve's perspective even if she tries to eavesdrop on the devices, which is an aspect that was not considered in [BI20] and hence has no counterpart in that work.

In the remainder of this work, we will mostly focus on proving security in the abstract cryptography framework; however, we shall also include discussion of this alternative definition at several points (see Remark 6 and Section 5.5) to aid understanding and comparison to previous work. For instance, when we present our full ECD protocol later (Protocol 1), the descriptions are phrased in terms of the abstract cryptography resources explained in Sections 2.1–2.3, but we also include below the protocol description (in Remark 6) an explanation of how the registers in the protocol correspond to the registers described in this alternative definition. For now, we just highlight and briefly discuss a particularly significant point: in the alternative definition presented above, there is a decryption key R that is revealed in the decryption phase. In the context of the abstract cryptography framework, this register R is instead formalized as the randomness Alice obtains from the temporarily private randomness source described in Section 2.3, which is revealed to all parties at some fixed later time — this is how we have chosen to formalize (in that framework) the notion that this "decryption key" value might be revealed to Bob and/or Eve after the certified deletion phase.

3 Preliminaries

3.1 Probability theory

We shall denote the probability distribution of a random variable X on some set $\mathcal{X}$ by P_X. For any event $\mathcal{E}$ on $\mathcal{X}$, the distribution of X conditioned on $\mathcal{E}$ will be denoted by $\mathsf{P}_{X|\mathcal{E}}$. For joint random variables XY with distribution P_{XY}, P_X is the marginal distribution of X and $\mathsf{P}_{X|Y=y}$ is the conditional distribution of X given $Y = y$; when it is clear from context which variable's value is being conditioned on, we shall often shorten the latter to $\mathsf{P}_{X|y}$. We shall use $\mathsf{P}_{XY}\mathsf{P}_{Z|X}$ to refer to the distribution

$$(\mathsf{P}_{XY}\mathsf{P}_{Z|X})(x,y,z) = \mathsf{P}_{XY}(x,y) \cdot \mathsf{P}_{Z|X=x}(z).$$

Occasionally we shall use notation of the form $\mathsf{P}_{XY}\mathsf{P}_{Z|x^*}$. This denotes the distribution

$$(\mathsf{P}_{XY}\mathsf{P}_{Z|x^*})(x,y,z) = \mathsf{P}_{XY}(x,y) \cdot \mathsf{P}_{Z|X=x^*}(z),$$

which potentially takes non-zero value when $x \neq x^*$. For two distributions P_X and $\mathsf{P}_{X'}$ on the same set $\mathcal{X}$, the ℓ_1 distance between them is defined as

$$\|\mathsf{P}_X - \mathsf{P}_{X'}\|_1 = \sum_{x\in\mathcal{X}} |\mathsf{P}_X(x) - \mathsf{P}_{X'}(x)|.$$

Fact 3. *For joint distributions* P_{XY} *and* $\mathsf{P}_{X'Y'}$ *on the same sets,*

$$\|\mathsf{P}_X - \mathsf{P}_{X'}\|_1 \leq \|\mathsf{P}_{XY} - \mathsf{P}_{X'Y'}\|_1.$$

Fact 4. *For two distributions* P_X *and* $\mathsf{P}_{X'}$ *on the same set and an event* $\mathcal{E}$ *on the set,*

$$|\mathsf{P}_X(\mathcal{E}) - \mathsf{P}_{X'}(\mathcal{E})| \leq \frac{1}{2}\|\mathsf{P}_X - \mathsf{P}_{X'}\|_1.$$

Fact 5. *Suppose probability distributions* $\mathsf{P}_X, \mathsf{P}_{X'}$ *satisfy* $\|\mathsf{P}_X - \mathsf{P}_{X'}\|_1 \leq \varepsilon$*, and an event* $\mathcal{E}$ *satisfies* $\mathsf{P}_X(\mathcal{E}) \geq \alpha$*, where* $\alpha > \varepsilon$*. Then,*

$$\|\mathsf{P}_{X|\mathcal{E}} - \mathsf{P}_{X'|\mathcal{E}}\|_1 \leq \frac{2\varepsilon}{\alpha}.$$

The following result is a consequence of the well-known Serfling bound.

Fact 6 ([TL17])**.** *Let* $Z = Z_1 \dots Z_l$ *be* l *binary random variables with an arbitrary joint distribution, and let* T *be a random subset of size* γl *for* $0 \leq \gamma \leq 1$*, picked uniformly among all such subsets of* $[l]$ *and independently of* Z*. Then,*

$$\Pr\left[\left(\sum_{i\in T} Z_i \geq (1-\varepsilon)\gamma l\right) \wedge \left(\sum_{i\in[l]\setminus T} Z_i < (1-2\varepsilon)(1-\gamma)l\right)\right] \leq 2^{-2\varepsilon^2\gamma l}.$$

3.2 Quantum information

The ℓ_1 distance between two quantum states ρ and σ is given by

$$\|\rho - \sigma\|_1 = \operatorname{Tr}\sqrt{(\rho-\sigma)^\dagger(\rho-\sigma)} = \operatorname{Tr}|\rho - \sigma|.$$

The fidelity between two quantum states is given by

$$\mathsf{F}(\rho,\sigma) = \|\sqrt{\rho}\sqrt{\sigma}\|_1.$$

The Bures distance based on fidelity is given by

$$\mathsf{B}(\rho,\sigma) = \sqrt{1 - \mathsf{F}(\rho,\sigma)}.$$

ℓ_1 distance, fidelity and Bures distance are related in the following way.

Fact 7 (Fuchs-van de Graaf inequality)**.** *For any pair of quantum states* ρ *and* σ*,*

$$2(1 - \mathsf{F}(\rho,\sigma)) \leq \|\rho - \sigma\|_1 \leq 2\sqrt{1 - \mathsf{F}(\rho,\sigma)^2}.$$

Consequently,

$$2\mathsf{B}(\rho,\sigma)^2 \leq \|\rho - \sigma\|_1 \leq 2\sqrt{2}\cdot\mathsf{B}(\rho,\sigma).$$

For two pure states $|\psi\rangle$ *and* $|\phi\rangle$*, we have*

$$\| |\psi\rangle\langle\psi| - |\phi\rangle\langle\phi| \|_1 = \sqrt{1 - \mathsf{F}\left(|\psi\rangle\langle\psi|, |\phi\rangle\langle\phi|\right)^2} = \sqrt{1 - |\langle\psi,\phi\rangle|^2}.$$

Fact 8 (Uhlmann's theorem)**.** *Suppose ρ and σ are mixed states on register X which are purified to $|\rho\rangle$ and $|\sigma\rangle$ on registers XY, then it holds that*

$$\mathsf{F}(\rho,\sigma) = \max_U |\langle\rho|\mathbb{1}_X \otimes U|\sigma\rangle|$$

where the maximization is over unitaries acting only on register Y. Due to the Fuchs-van de Graaf inequality, this implies that there exists a unitary U such that

$$\left\|(\mathbb{1}_X \otimes U)\,|\rho\rangle\langle\rho|\,(\mathbb{1}_X \otimes U^\dagger) - |\sigma\rangle\langle\sigma|\right\|_1 \leq 2\sqrt{\|\rho-\sigma\|_1}.$$

Fact 9. *For a quantum channel $\mathcal{E}$ and states ρ and σ,*

$$\|\mathcal{E}(\rho) - \mathcal{E}(\sigma)\|_1 \leq \|\rho-\sigma\|_1 \qquad \mathsf{F}(\mathcal{E}(\rho),\mathcal{E}(\sigma)) \geq \mathsf{F}(\rho,\sigma).$$

The entropy of a quantum state ρ on a register Z is given by

$$\mathsf{H}(\rho) = -\operatorname{Tr}(\rho\log\rho).$$

We shall also denote this by $\mathsf{H}(Z)_\rho$. For a state ρ_{YZ} on registers YZ, the entropy of Y conditioned on Z is given by

$$\mathsf{H}(Y|Z)_\rho = \mathsf{H}(YZ)_\rho - \mathsf{H}(Z)_\rho$$

where $\mathsf{H}(Z)_\rho$ is calculated w.r.t. the reduced state ρ_Z. The conditional min-entropy of Y given Z is defined as

$$\mathsf{H}_\infty(Y|Z)_\rho = \inf\{\lambda : \exists\sigma_Z \text{ s.t. } \rho_{YZ} \preceq 2^{-\lambda}\mathbb{1}_Y \otimes \sigma_Z\}.$$

The conditional Hartley entropy of Y given Z is defined as

$$\mathsf{H}_0(Y|Z)_\rho = \log\left(\sup_{\sigma_Z} \operatorname{Tr}(\operatorname{supp}(\rho_{YZ})(\mathbb{1}_Y \otimes \sigma_Z))\right)$$

where $\operatorname{supp}(\rho_{YZ})$ is the projector on to the support of ρ_{YZ}. For a classical distribution P_{YZ}, this reduces to

$$\mathsf{H}_0(Y|Z)_{\mathsf{P}_{YZ}} = \log\left(\sup_z |\{y : \mathsf{P}_{YZ}(y,z) > 0\}|\right).$$

For $0 \leq \delta \leq 2$, the δ-smoothed versions of the above entropies are defined as

$$\mathsf{H}^\delta_\infty(Y|Z)_\rho = \sup_{\rho':\|\rho-\rho'\|_1\leq\delta} \mathsf{H}_\infty(Y|Z)_{\rho'} \qquad \mathsf{H}^\delta_0(Y|Z)_{\mathsf{P}_{YZ}} = \inf_{\rho':\|\rho'-\rho\|_1\leq\delta} \inf \mathsf{H}_0(Y|Z)_{\rho'}.$$

Fact 10. *For any state ρ_{XYZ} and any $0 \leq \delta \leq 2$,*

$$\mathsf{H}^\delta_\infty(Y|XZ)_\rho \geq \mathsf{H}^\delta_\infty(Y|Z)_\rho - \log|\mathcal{X}|.$$

The relative entropy between two states ρ and σ of the same dimensions is given by

$$\mathsf{D}(\rho\|\sigma) = \operatorname{Tr}(\rho\log\rho) - \operatorname{Tr}(\rho\log\sigma).$$

Fact 11 (Pinsker's Inequality)**.** *For any two states ρ and σ,*

$$\|\rho-\sigma\|_1^2 \leq 2\ln 2 \cdot \mathsf{D}(\rho\|\sigma) \quad \text{and} \quad \mathsf{B}(\rho,\sigma)^2 \leq \ln 2 \cdot \mathsf{D}(\rho\|\sigma).$$

The mutual information between Y and Z with respect to a state ρ on YZ can be defined in the following equivalent ways:

$$\mathsf{I}(Y:Z)_\rho = \mathsf{D}(\rho_{YZ}\|\rho_Y \otimes \rho_Z) = \mathsf{H}(Y)_\rho - \mathsf{H}(Y|Z)_\rho = \mathsf{H}(Z)_\rho - \mathsf{H}(Z|Y)_\rho.$$

The conditional mutual information between Y and Z conditioned on X is defined as

$$\mathsf{I}(Y:Z|X)_\rho = \mathsf{H}(Y|X)_\rho - \mathsf{H}(Y|XZ)_\rho = \mathsf{H}(Z|X)_\rho - \mathsf{H}(Z|XY)_\rho.$$

Mutual information can be seen to satisfy the chain rule

$$\mathsf{I}(XY:Z)_\rho = \mathsf{I}(X:Z)_\rho + \mathsf{I}(Y:Z|X)_\rho.$$

A state of the form

$$\rho_{XY} = \sum_x \mathsf{P}_X(x)\,|x\rangle\langle x|_X \otimes \rho_{Y|x}$$

is called a CQ (classical-quantum) state, with X being the classical register and Y being quantum. We shall use X to refer to both the classical register and the classical random variable with the associated distribution. As in the classical case, here we are using $\rho_{Y|x}$ to denote the state of the register Y conditioned on $X = x$, or in other words the state of the register Y when a measurement is done on the X register and the outcome is x. Hence $\rho_{XY|x} = |x\rangle\langle x|_X \otimes \rho_{Y|x}$. When the registers are clear from context we shall often write simply ρ_x.

Fact 12. *For a CQ state ρ_{XY} where X is the classical register, $\mathsf{H}_\infty(X|Y)_\rho$ is equal to the negative logarithm of the maximum probability of guessing X from the quantum system $\rho_{Y|x}$, i.e.,*

$$\mathsf{H}_\infty(X|Y)_\rho = -\log\left(\sup_{\{M_x\}_x} \sum_x \mathsf{P}_X(x)\,\mathrm{Tr}(M_x\rho_{Y|x})\right)$$

where the maximization is over the set of POVMs with elements indexed by x.

For CQ states, the expression for relative entropy for ρ_{XY} and σ_{XY} given by

$$\rho_{XY} = \sum_x \mathsf{P}_X(x)\,|x\rangle\langle x|_X \otimes \rho_{Y|x} \qquad \sigma_{XY} = \sum_x \mathsf{P}_{X'}(x)\,|x\rangle\langle x|_X \otimes \sigma_{Y|x},$$

reduces to

$$\mathsf{S}(\rho_{XY}\|\sigma_{XY}) = \mathsf{S}(\mathsf{P}_X\|\mathsf{P}_{X'}) + \mathop{\mathbb{E}}_{\mathsf{P}_X} \mathsf{S}(\rho_{Y|x}\|\sigma_{Y|x}). \tag{7}$$

Accordingly, the conditional mutual information between Y and Z conditioned on a classical register X, is simply

$$\mathsf{I}(Y:Z|X) = \mathop{\mathbb{E}}_{\mathsf{P}_X} \mathsf{I}(Y:Z)_{\rho_x}. \tag{8}$$

3.3 2-universal hashing

Definition 2. *A family $\mathfrak{H}$ of functions from $\mathcal{X}$ to $\mathcal{Z}$ is called a* 2-universal family of hash functions *iff*

$$\forall x \neq x' \qquad \Pr[h(x) = h(x')] \leq \frac{1}{|\mathcal{Z}|}$$

where the probability is taken over the choice of h uniformly over $\mathfrak{H}$.

2-universal hash function families always exist if $|\mathcal{X}|$ and $|\mathcal{Z}|$ are powers of 2, i.e., bit strings of some fixed length (see e.g. [CW79]). We shall denote a family of 2-universal hash functions from $\{0,1\}^s$ to $\{0,1\}^n$ by $\mathfrak{H}(s,n)$.[9]

2-universal hash functions are used for privacy amplification in cryptography. For privacy amplification against an adversary with quantum side information, the following lemma is used.

Fact 13 (Leftover Hashing Lemma, [Ren05]). *The CQ state $\rho_{CKH\widetilde{E}}$, where C is an n-bit classical register, K is an s-bit classical register, and H is a classical register of dimension $|\mathfrak{H}(s,n)|$, is defined as*

$$\rho_{CKH\widetilde{E}} = \sum_{k\in\{0,1\}^s} \sum_{h\in\mathfrak{H}(s,n)} \frac{1}{|\mathfrak{H}(s,n)|} \mathsf{P}_K(k) \otimes |h(k),k,h\rangle\langle h(k),k,h|_{CKH} \otimes \rho_{\widetilde{E}|k}.$$

Then for any $\varepsilon \in [0,1)$,

$$\left\| \rho_{CH\widetilde{E}} - \frac{\mathbb{1}_C}{2^n} \otimes \rho_{H\widetilde{E}} \right\|_1 \leq 2^{-\frac{1}{2}(\mathsf{H}_\infty^\varepsilon(K|\widetilde{E})-n)} + 2\varepsilon.$$

4 The magic square game & its parallel repetition

In a 2-player k-round game G, Alice and Bob share an entangled state at the beginning of the game. In the j-th round, they receive inputs (x^j, y^j) and produce outputs (a^j, b^j) respectively. They can do this by performing measurements that depend on the inputs and outputs of all rounds up to the j-th, on the post-measured state from the previous round. Each round has an associated predicate V^j which is a function of all inputs and outputs up to the j-th round. Alice and Bob win the game iff

$$\bigwedge_{j=1}^{k} \mathsf{V}^j(x^1 \dots x^j, y^1 \dots y^j, a^1 \dots a^j, b^1 \dots b^j) = 1.$$

For a k-round game G, let G^l denote the l-fold parallel repetition of it, and let $G^{t/l}$ denote the following game:

- For $j = 1$ to k, in the j-th round, Alice and Bob receive $x_1^j, \dots, x_l^j$ and $y_1^j, \dots, y_l^j$ as inputs.
- For $j = 1$ to k, in the j-th round, Alice and Bob output $a_1^j, \dots, a_l^j$ and $y_1^j \dots, y_l^j$.
- Alice and Bob win the game iff $(x_i^1 \dots x_i^k, y_i^1 \dots y_i^k, a_i^1 \dots a_i^k, b_i^1 \dots b_i^k)$ win G for at least t many i-s.

A parallel repetition threshold theorem gives an upper bound on the winning probability of $G^{t/l}$ which is exponentially small in l, for sufficiently high values of t/l.

In the magic square game,

[9] Strictly speaking, in our applications of this concept we shall need to use bitstrings of variable length (up to some upper bound l) as inputs to the hash functions. This can be handled simply by noting that there are $2^{l+1}-1$ bitstrings of length less than or equal to l. Hence there is an injective mapping from such bitstrings to bitstrings of length $l+1$, and we can then apply 2-universal hash families designed for the latter (note that the mapping leaves all conditional entropies invariant because it is injective).

- Alice and Bob receive respective inputs $x \in \{0,1,2\}$ and $y \in \{0,1,2\}$ independently and uniformly at random.
- Alice outputs $a \in \{0,1\}^3$ such that $a[0] \oplus a[1] \oplus a[2] = 0$ and Bob outputs $b \in \{0,1\}^3$ such that $b[0] \oplus b[1] \oplus b[2] = 1$.
- Alice and Bob win the game if $a[y] = b[x]$.

The classical value of the magic square game is $\omega(\mathrm{MS}) = 8/9$, whereas the quantum value is $\omega^*(\mathrm{MS}) = 1$.

We introduce two variants of the magic square game: a 3-player 1-round version where Alice and Bob's distributions are product and are anchored w.r.t. the third player Eve's input, and a 2-player 2-round version where Alice and Bob's first round inputs are product and anchored w.r.t. Bob's second round input. We shall make use of parallel repetition threshold theorems for both these kinds of games.

4.1 2-player 2-round MSB_α

MSB_α is defined as follows:

- In the first round, Alice and Bob receive inputs $x \in \{0,1,2\}$ and $y' \in \{0,1,2\}$ independently and uniformly at random.
- Alice outputs $a \in \{0,1\}^3$ such that $a[0] \oplus a[1] \oplus a[2] = 0$, and Bob outputs $b' \in \{0,1\}^3$ such that $b'[0] \oplus b'[1] \oplus b'[2] = 1$.
- In the second round, Bob gets input $z = \perp$ (indicating no input) with probability α, and otherwise $z = (x, y)$ where y is uniformly distributed on $\{0,1,2\} \setminus y'$. (Alice has no input.)
- Bob outputs $c \in \{0,1\}$. (Alice has no output.)
- Alice and Bob win the game if $a[y'] = b'[x]$, and either Bob gets input $\perp$ or $a[y] = c$.

Lemma 14. *There exists a constant $0 < c^{\mathrm{B}} < 1$ such that $\omega^*(\mathrm{MSB}_\alpha) = 1 - c^{\mathrm{B}}(1-\alpha)$.*

In order to prove Lemma 14, we shall make use of a result due to [FM18].

Fact 15 ([FM18])**.** *Suppose Alice and Bob have a state and measurements that can win the* MS *game with probability $1-\delta$. Consider any $x, y, y' \in \{0,1,2\}$ such that $y' \neq y$, and suppose Alice and Bob perform the aforementioned measurements for inputs x, y', receiving outputs a, b'. Then if Bob is subsequently given y and Alice's input x, the probability that he can guess $a[y]$ is at most $\frac{1}{2} + 9\sqrt{\delta}$.*

Proof of Lemma 14. Since $z = (x, y)$ with probability $1 - \alpha > 0$, it suffices to show that the probability of winning the game for $z = (x, y)$ is at most $1 - c^{\mathrm{B}}$ for some $c^{\mathrm{B}} > 0$. If $z = \perp$, the game being played is just the standard magic square game, which can be won with probability 1.

The probability of winning the game if $z = (x, y)$ can be written as $\Pr[(a[y'] = b'[x]) \wedge (a[y] = c) | z = (x, y)]$, which is upper bounded by

$$\min\{\Pr[a[y'] = b'[x] | z = (x, y)], \Pr[a[y] = c | z = (x, y)]\}.$$

Denote $\Pr[a[y'] = b'[x]|z = (x,y)] = 1-\delta$. Then by Fact 15 we have $\Pr[a[y] = c|z = (x,y)] \leq \frac{1}{2}+9\sqrt{\delta}$, hence the above expression is upper bounded by the maximum value of $\min\{1-\delta, \frac{1}{2}+9\sqrt{\delta}\}$ over all possible δ. Since $\frac{1}{2}+9\sqrt{\delta}$ is continuous in δ and has value less than 1 at $\delta = 0$, this maximum must be less than 1. In fact the maximum is obtained at the intersection of $1-\delta$ and $\frac{1}{2}+9\sqrt{\delta}$ for $\delta \in [0,1]$, where the value is ~ 0.997. □

Theorem 16. *For $c_\alpha^{\mathrm{B}} = c^{\mathrm{B}}(1-\alpha)$ from Lemma 14, δ such that $t = (1-c_\alpha^{\mathrm{B}}+\eta)l \in ((1-c_\alpha^{\mathrm{B}})l, l]$, there exists $d^{\mathrm{B}} > 0$ such that*

$$\omega^*(\mathrm{MSB}_\alpha^{t/l}) \leq 2^{-d^{\mathrm{B}}\eta^3\alpha^2 l}.$$

We prove more a general version of Theorem 16 in Section 7.

4.2 3-player MSE_α game

MSE_α is defined as follows:

- Alice and Bob receive inputs $x \in \{0,1,2\}$ and $y \in \{0,1,2\}$ independently and uniformly at random.
- Eve receives an input $z = \perp$ (indicating no input) with probability α, and $z = (x,y)$ with probability $1-\alpha$.
- Alice outputs $a \in \{0,1\}^3$ such that $a[0] \oplus a[1] \oplus a[2] = 0$, Bob outputs $b \in \{0,1\}^3$ such that $b[0] \oplus b[1] \oplus b[2] = 1$ and Eve outputs $c \in \{0,1\}$.
- Alice, Bob and Eve win the game if $a[y] = b[x]$, and either Eve gets input $\perp$ or she outputs $c = a[y] = b[x]$.

Fact 17 ([KKM+08], and modification described in [Vid17])**.** *There exists a constant $0 < c^{\mathrm{E}} < 1$ such that $\omega^*(\mathrm{MSE}_\alpha) = 1 - c^{\mathrm{E}}(1-\alpha)$.*

Theorem 18. *For $c_\alpha^{\mathrm{E}} = c^{\mathrm{E}}(1-\alpha)$ from Fact 17, δ such that $t = (1-c_\alpha^{\mathrm{E}}+\eta)l \in ((1-c_\alpha^{\mathrm{E}})l, l]$, there exists a constant $d^{\mathrm{E}} > 0$ such that*

$$\omega^*(\mathrm{MSE}_\alpha^{t/l}) \leq 2^{-d^{\mathrm{E}}\eta^3\alpha^2 l}.$$

We prove a more general version of Theorem 18 in Section 7. Note that it is possible to use the result of [BVY15, BVY17] for k-player anchored games to get a version of Theorem 18 with worse parameters; we provide a different proof in order to improve the parameters.

5 ECD protocol

Our ECD protocol, which uses the resources $\mathcal{C}, \mathcal{R}, \mathcal{R}^P$ and $(\mathcal{B}_1^1 \dots \mathcal{B}_l^1, \mathcal{B}_1^2 \dots \mathcal{B}_l^2)_\varepsilon$, is given in Protocol 1. To be specific, Protocol 1 describes the steps performed by Alice and honest Bob; we have highlighted the steps that a dishonest Bob need not perform in red.[10] We have also indicated

[10] We assume Bob sends $b_{\overline{T}}$ and $b'_{\overline{T}}$ generated in some arbitrary manner to Alice in lines 7 and 25 even if he is dishonest, so as not to give himself away as dishonest, which is why these have not been highlighted in red.

in green steps that occur at specific times corresponding to the ideal functionality. The parameters l, α, γ in the protocol need to satisfy conditions specified in Section 5.4. The function $\mathtt{syn}$ used in the protocol is specified by Fact 20 later (it is basically the syndrome of an appropriate error-correcting code).

Remark 4. *In the Protocol 1 description, for readability we present the various steps as being performed by the parties Alice and Bob themselves; for instance we say that (amongst various other steps) Alice performs various checks and outputs values O and F. However, strictly speaking this does not perfectly match the formal descriptions required in the Abstract Cryptography framework, where many of those steps should instead be stated (in the honest case) as being performed by the* protocols Π^{A} *and* Π^{B} *(recall that these are converters with inner interfaces attached to the real resources and outer interfaces interacting with the parties Alice and Bob). In that framework, technically we should instead say for instance that it is the* protocol Π^{A} *that performs those checks and outputs the values O and F to Alice (who is viewed as a sort of "external agent" who only plays the roles of supplying the values M, D and receiving the outputs O, F). However, in the Protocol 1 description and the subsequent analysis in this section, it is awkward to constantly describe the various actions as being performed by abstract protocols/converters, and hence for brevity we gloss over the distinction in this section and just describe all these actions as being performed by Alice and Bob themselves. (Though in Section 6 where we prove security in the full Abstract Cryptography picture, we will return to being more explicit about this distinction.)*

Protocol 1 ECD protocol

Phase 1: Encryption

Alice and Bob receive $\mathcal{B}_1^1 \dots \mathcal{B}_l^1$ and $\mathcal{B}_1^2 \dots \mathcal{B}_l^2$ respectively from Eve
Alice gets $S \subseteq [l]$ obtained by choosing each index independently with probability $(1-\alpha)$, and $T \subseteq S$ (or $\subseteq [l]$ if $|S| < \gamma l$) of size γl uniformly at random, from $\mathcal{R}$
Alice gets x_S, y_S and $y'_{\overline{T}}$ uniformly at random such that $y_i \neq y'_i$ for each i, from $\mathcal{R}$
Alice supplies x_S as inputs to her boxes corresponding to S and uniformly random inputs from $\mathcal{R}^P$ to the rest of her boxes, recording the outputs from the subset S as a string a_S
Alice sends (T, y_T) to Bob using $\mathcal{C}$
Bob inputs y_T into his boxes corresponding to T and gets output b_T
Bob sends b_T to Alice using $\mathcal{C}$
Alice tests if $|S| \geq \gamma l$ and $a_i[y_i] = b_i[x_i]$ for at least $(1-\varepsilon)|T|$ many i-s in T
if the test passes **then**
    Alice sends $O = \top$ to Bob
    At time t_1, Alice and Bob output $O = \top$
    Alice sets $K^{\mathrm{A}} = (a_i[y_i])_{i \in S}$
    Alice gets $h \in \mathfrak{H}(l+1, n)$, $U_1 \in \{0,1\}^n$, $U_2 \in \{0,1\}^{|\mathtt{syn}(K^{\mathrm{A}})|}$ uniformly at random from $\mathcal{R}$
    At time t_2, Alice selects input $M \in \{0,1\}^n$
    Alice sends $C = (C_1, C_2) = (M \oplus h(K^{\mathrm{A}}) \oplus U_1, \mathtt{syn}(K^{\mathrm{A}}) \oplus U_2)$ to Bob using $\mathcal{C}$
else
    Alice sends $O = \perp$ to Bob
    At time t_1, Alice and Bob output $O = \perp$ and the protocol ends

Phase 2: Certified deletion

At time t_3, Alice selects input $D \in \{0,1\}$
if $D = 0$ **then**
    Alice sends 0 to Bob using $\mathcal{C}$
else
    Alice sends $(1, y'_{\overline{T}})$ to Bob using $\mathcal{C}$
    Bob inputs $y'_{\overline{T}}$ into his boxes corresponding to $\overline{T}$ and gets output $b'_{\overline{T}}$
    Bob sends $b'_{\overline{T}}$ to Alice using $\mathcal{C}$
    Alice tests if $a_i[y'_i] = b'_i[x_i]$ for at least $(1-2\varepsilon)|S \setminus T|$ many i-s in $S \setminus T$
    if the test passes **then**
        At time t_4, Alice outputs $F = \checkmark$
    else
        At time t_4, Alice outputs $F = \boldsymbol{\times}$

Phase 3: Decryption

$\mathcal{R}$ reveals $R = (x_S, y_S, y'_{\overline{T}}, S, T, h, u_1, u_2)$
if $D = 0$ **then**
    Bob inputs $y_{S \cap \overline{T}}$ to his boxes corresponding to $S \cap \overline{T}$, uniformly random inputs to the boxes corresponding to S, and records the outputs from $S \cap \overline{T}$ as $b_{S \cap \overline{T}}$
    Bob sets $K^{\mathrm{B}} = (b_i[x_i])_{i \in S}$
    Bob uses K^{B} and $\mathtt{syn}(K^{\mathrm{A}}) = C_2 \oplus u_2$ to compute a guess $\widetilde{K}^{\mathrm{A}}$ for K^{A}
    At time t_5, Bob outputs $\widetilde{M} = C_1 \oplus h(\widetilde{K}^{\mathrm{A}}) \oplus u_1$
else
    At time t_5, Bob outputs $\widetilde{M} = 0^n$

Remark 5. *Protocol 1 can be modified so that instead of step 23, Alice sends $y'_{\overline{T}}$ to Bob in either step 5 or 15. It may be desirable to do this if we want to achieve the alternative ECD task discussed in Section 2.4, where Bob makes the deletion decision himself, so as not to include an unnecessary round of interaction (since that version will not include the communication in steps 21 and 23 at all). Because of the OTPs with u_1 and u_2, as we discuss later, sending $y'_{\overline{T}}$ earlier has no effect on security.*

Remark 6. *We explain here how the above Protocol 1 description should be viewed in the context of the alternative security definitions in Section 2.5.*

In the encryption phase of that definition, Alice is supposed to produce and store registers O, R and P. With respect to the Protocol 1 description, these should be viewed as follows: O is simply the value O generated in step 9, R consists of the values $(x_S, y_S, y'_{\overline{T}}, S, T, h, u_1, u_2)$ obtained from the temporarily private randomness source $\mathcal{R}$ over the course of the encryption phase (which are later revealed in step 31 for decryption, as we would expect), and P consists of the values $(y'_{\overline{T}}, x_S, y_S, a_S)$ (for potential later use in the certified deletion phase). As for Bob, he is supposed to end up with a ciphertext state in his register Q_B: with respect to the Protocol 1 description, this ciphertext state consists of the register C in step 15 together with the quantum state in his half of the boxes. (If Bob is honest, he holds no other registers in Q_B; if he is dishonest then Q_B holds a state which he has been updating arbitrarily over the course of the encryption phase using the messages exchanged.) Eve's side-information register Q_E consists of her original quantum side-information on the boxes, as well as all messages exchanged between Alice and Bob.

In the certified deletion phase of that definition, the register P used by Alice and Bob is as described above, and the register F produced by Alice is simply the flag F generated in step 27 of the Protocol 1 description.

Finally, in the decryption phase of that definition, the decryption key R is again as described above, and similarly for the ciphertext state that Bob uses to decrypt the message. His decrypted value $\widetilde{M}$ for the message corresponds to step 36 of the Protocol 1 description.

5.1 Notation

We shall introduce some notation that will be used in the rest of the section and the composable security proof. Firstly, note that even though for ease of presentation in the protocol, we have indicated Alice getting R step by step from $\mathcal{R}$, in reality she could have gotten it all in step 3 and here we shall consider her having done so. We do not use any registers for the randomness Alice got from $\mathcal{R}^P$ as this is not relevant in the protocol or the security proof.

Consider the following state shared by Alice, Bob and Eve after step 8 of the protocol, when Alice has produced the abort decision O but has not sent it to Bob yet:

$$\varphi_{CFORK^{\mathrm{A}}\widetilde{A}\widetilde{B}B_T\widetilde{E}} = |0^n\rangle\!\langle 0^n|_{CF} \otimes \sum_{ork^{\mathrm{A}}} \mathsf{P}_{ORK^{\mathrm{A}}}(ork^{\mathrm{A}})\, |ork^{\mathrm{A}}\rangle\!\langle ork^{\mathrm{A}}|_{ORK^{\mathrm{A}}} \otimes \varphi_{\widetilde{A}\widetilde{B}B_T\widetilde{E}|ork^{\mathrm{A}}}.$$

Here the ciphertext register $C = C_1C_2$ and the flag register F — which are initialized to default values — are with Alice, as is the randomness R received from $\mathcal{R}$. The answer B_T Alice got from Bob is with both Alice and Eve, but for the sake of brevity we only explicitly specify the copy with Eve. $\widetilde{A}, \widetilde{B}, \widetilde{E}$ are the quantum registers held by Alice, Bob and Eve. We shall assume $\widetilde{B}\widetilde{E}$ includes TY_T that Bob (and Eve) got from Alice, and $\widetilde{A}\widetilde{B}$ includes Alice and Bob's copies of B_T. Finally, we shall assume $\widetilde{B}$ contains the register K^{B} on which Bob would obtain his raw key, if he were

honest. Further states in the protocol are obtained from φ by passing some registers from Alice to Bob (and Eve) and local operations on the registers possessed by Alice or jointly Bob and Eve.

At times t_2 and t_3 the message $M = m$ and the deletion decision $D = 0/1$ enter the protocol, and we shall specify these parameters when talking about states from these points on — although the message dependence is only on the C register, so we may drop the M dependence when talking about other registers. We use the following notation to denote states at various times in the protocol conditioned on various events (all the states are conditioned on outputting $\top$ at time t_1, though we only mention this in the first one, since the protocol only continues after t_1 under this condition):

$$\begin{aligned}
&\rho_{CFORK^{\mathrm{A}}\widetilde{A}\widetilde{B}B_T\widetilde{E}} &&: \varphi_{CFORK^{\mathrm{A}}\widetilde{A}\widetilde{B}B_T\widetilde{E}} \text{ conditioned on } O = \top \\
&\rho^1_{CFORK^{\mathrm{A}}\widetilde{A}\widetilde{B}B_T\widetilde{E}}(m,0) &&: \text{state after honest Bob's measurement in step 33} \\
&\rho^2_{CFORK^{\mathrm{A}}\widetilde{A}\widetilde{B}B_T\widetilde{E}}(m,1) &&: \text{state at time } t_4 \text{ when Alice has produced the flag } F \\
&\sigma_{CFORK^{\mathrm{A}}\widetilde{A}\widetilde{B}B_T\widetilde{E}}(m,1) &&: \rho^2_{CFORK^{\mathrm{A}}\widetilde{A}\widetilde{B}B_T\widetilde{E}}(m,1) \text{ conditioned on } F = \checkmark
\end{aligned}$$

We shall use $p_\top$ to denote the probability of outputting $\top$ at time t_1, which is clearly the probability of ρ within φ.[11] Let $p_{\checkmark|\top}$ denote the probability of Alice outputting $\checkmark$ at time t_4 conditioned on outputting $\top$ at time t_1, for message $M = m$ and $D = 1$, i.e., the probability of $\sigma(m,1)$ within $\rho^2(m,1)$. This probability is independent of m, as we shall argue in Lemma 24.

5.2 Completeness and correctness

We now prove some lemmas which, in the context of the alternative security definitions in Section 2.5, will imply the completeness and correctness properties (as we shall discuss in Section 5.5). In the context of our composable security analysis (in Section 6), however, these will just be intermediate results in the full composable security proof.

Lemma 19. *Suppose $\alpha, \gamma < \frac{1}{2}$ and $l \geq \frac{4}{(1-2\gamma)^2}$. If Bob and Eve are honest (so Alice and Bob's boxes are $\varepsilon/2$-noisy, i.e., able to win each instance of* MS *with probability $1 - \varepsilon/2$) then*

$$p_\top \geq \left(1 - 2^{-(1-2\gamma)^2 l/8}\right)\left(1 - 2^{-\varepsilon^2\gamma l/8}\right) \geq 1 - 2^{-(1-2\gamma)^2 l/8} - 2^{-\varepsilon^2\gamma l/8}.$$

Moreover, if Bob is honest and $D = 1$ (i.e. Alice requests a deletion certificate), then regardless of Eve, we have

$$p_\top(1 - p_{\checkmark|\top}) \leq 2^{-2\varepsilon^2\gamma l}.$$

Proof. Since each element of $[l]$ is included in S independently with probability $(1-\alpha)$, we see from the Chernoff bound that the probability of outputting $\perp$ due to $|S| < \gamma l$ is bounded by

$$\Pr[|S| < \gamma l] \leq 2^{-\frac{(1-\alpha-\gamma)^2}{2(1-\alpha)} l} \leq 2^{-\frac{(1-2\gamma)^2}{8} l},$$

for the choice of α. Moreover, for our choice of l the above quantity is at most $\frac{1}{2}$. Conditioned on $|S| \geq \gamma l$, the behaviour of the boxes on T is independent of S. For any $i \in [l]$, let W_i denote the indicator variable for the event $a_i[y_i] = b_i[x_i]$. Since each instance of MS is won with probability

[11] By this we mean that $\varphi = p_\top \rho + (1 - p_\top)\rho'$, where ρ' is the state conditioned on $O = \perp$ instead.

at least $1-\varepsilon/2$ by honest boxes, the probability of aborting due to $a_i[y_i] \neq b_i[y_i]$ in at least $\varepsilon|T|$ boxes in T, i.e., $\sum_{i\in T} W_i \leq (1-\varepsilon)|T|$, is

$$\Pr\left[\sum_{i\in T} W_i < (1-\varepsilon)|T| \middle| |S| \geq \gamma l\right] \leq 2^{-\frac{\varepsilon^2|T|}{8}} = 2^{-\frac{\varepsilon^2\gamma l}{8}}.$$

Hence overall,

$$p_\top \geq \left(1-2^{-(1-2\gamma)^2 l/8}\right)\left(1-2^{-\varepsilon^2\gamma l/8}\right).$$

$p_{\checkmark|\top}$ is independent of m in general (see Lemma 24 below), but it is easy to see why this is so for honest Bob: his behaviour in Phase 2 is entirely independent of m. To lower bound $p_{\checkmark|\top}$, let W_i be defined as before, and let W_i' be the indicator variable for the event that when Bob inputs y_i' into his box and gets output b_i', they satisfy $a_i[y_i'] = b_i'[x_i]$. As the marginal distributions of y_i and y_i' are exactly the same, W_i' and W_i are identically distributed.

Recall that W_i is the same variable regardless of when the inputs are provided and the outputs obtained, so we can consider doing the $y'_{\overline{T}}$ measurement on φ. $p_\top$ is the probability of the event

$$(|S| \geq \gamma l) \wedge \left(\sum_{i\in T} W_i \geq (1-\varepsilon)|T|\right), \tag{9}$$

when all the measurements are done on φ. Let $p_\checkmark$ denote the probability of

$$(|S| \geq \gamma l) \wedge \left(\sum_{i\in T} W_i \geq (1-\varepsilon)|T|\right) \wedge \left(\sum_{i\in S\setminus T} W_i' \geq (1-2\varepsilon)|S\setminus T|\right). \tag{10}$$

Since the distribution of S is independent of the W_i-s and W_i'-s, from Lemma 6,

$$\begin{aligned}
&\Pr\left[\left(\sum_{i\in T} W_i \geq (1-\varepsilon)|T|\right) \wedge \left(\sum_{i\in S\setminus T} W_i' < (1-2\varepsilon)|S\setminus T|\right) \middle| |S| \geq \gamma l\right] \\
&= \Pr\left[\left(\sum_{i\in T} W_i \geq (1-\varepsilon)|T|\right) \wedge \left(\sum_{i\in S\setminus T} W_i < (1-2\varepsilon)|S\setminus T|\right) \middle| |S| \geq \gamma l\right] \\
&\leq 2^{-2\varepsilon^2 \frac{\gamma l}{|S|}\cdot|S|} = 2^{-2\varepsilon^2\gamma l}.
\end{aligned}$$

This gives us

$$\begin{aligned}
p_\checkmark &= p_\top - \Pr\left[(|S| \geq \gamma l) \wedge \left(\sum_{i\in T} W_i \geq (1-\varepsilon)|T|\right) \wedge \left(\sum_{i\in S\setminus T} W_i' < (1-2\varepsilon)|S\setminus T|\right)\right] \\
&\geq p_\top - 2^{-2\varepsilon^2\gamma l} \Pr\left[|S| \geq \gamma l\right] \\
&\geq p_\top - 2^{-2\varepsilon^2\gamma l}.
\end{aligned}$$

Now simply observe that $p_\checkmark = p_\top p_{\checkmark|\top}$, which gives us the required result. Note that here we required that upon receiving $y'_{\overline{T}}$, Bob produces $b'_{\overline{T}}$ by the same procedure by which he produced b_T upon receiving y_T, which is his honest behaviour (even though the boxes themselves are untrusted), but we did not assume that the procedure actually implements anything close to the ideal MS measurements. A dishonest Bob, on the other hand, may produce $b'_{\overline{T}}$ by some different procedure, and hence this bound does not apply to him. □

Further analysis will be done assuming α, γ, l satisfy the conditions of Lemma 19, though we shall not state it explicitly in each case.

The correctness of Protocol 1, i.e., the fact that Bob is able to produce the correct message if $D = 0$ and he is honest, uses the following fact.

Fact 20 ([Ren05], Lemma 6.3.4)**.** *Suppose Alice and Bob respectively hold random variables $K^{\mathrm{A}}, K^{\mathrm{B}} \in \{0,1\}^s$. Then for $0 < \delta \leq 1$, there exists a protocol in which Alice communicates a single message $\mathtt{syn}(K^{\mathrm{A}})$ of at most $\mathsf{H}_0^\delta(K^{\mathrm{A}}|K^{\mathrm{B}}) + \log(1/\lambda_{\mathrm{EC}})$ bits to Bob, after which Bob can produce a guess $\widetilde{K}^{\mathrm{A}}$ that is equal to K^{A} with probability at least $1 - (\delta + \lambda_{\mathrm{EC}})/2$.*

Lemma 21. *There is a choice of $C_2 = \mathtt{syn}(K^{\mathrm{A}})$ of length $h_2(2\varepsilon)l + \log(1/\lambda_{\mathrm{EC}})$ bits, such that $\widetilde{K}^{\mathrm{A}}$ produced by honest Bob in step 35 of Phase 3 of the protocol is equal to K^{A} with probability at least $1 - (2 \cdot 2^{-2\varepsilon^2\gamma l}/p_\top + \lambda_{\mathrm{EC}}/2)$, where h_2 is the binary entropy function.*

Proof. Define the random variables W_i as in the proof of Lemma 19. First observe that ρ^1 is the state conditioned on the event (9) after the measurements are done on φ.[12] Let $\widetilde{\rho}^1$ be the state conditioned on the event

$$\widetilde{\mathcal{E}} = (|S| \geq \gamma l) \wedge \left(\sum_{i \in T} W_i \geq (1-\varepsilon)|T| \right) \wedge \left(\sum_{i \in S \setminus T} W_i \geq (1-2\varepsilon)|S \setminus T| \right), \tag{11}$$

when all the measurements are done on φ. Note that $\widetilde{\rho}^1$ is also equal to ρ^1 conditioned on the event $\widetilde{\mathcal{E}}$ (since the event $\widetilde{\mathcal{E}}$ is a stricter condition than the event (9)). We shall now argue that ρ^1 and $\widetilde{\rho}^1$ are close in trace distance, by showing that the event $\widetilde{\mathcal{E}}$ occurs with some sufficiently high probability in the state ρ^1.

To do so, we follow exactly the same argument structure as in the proof of Lemma 19, except with the event $\widetilde{\mathcal{E}}$ in place of the event (10). With respect to the state immediately after the measurements are done on φ, let $p_{\widetilde{\mathcal{E}}}$ denote the probability of the event $\widetilde{\mathcal{E}}$, and let $p_{\widetilde{\mathcal{E}}|\top}$ denote the probability of the event $\widetilde{\mathcal{E}}$ conditioned on the event (9). (Note that $p_{\widetilde{\mathcal{E}}|\top}$ is also precisely the probability of the event $\widetilde{\mathcal{E}}$ with respect to the state ρ^1.) With this notation, we obtain analogous inequalities to the Lemma 19 proof:

$$\begin{aligned} p_{\widetilde{\mathcal{E}}} &= p_\top - \Pr\left[(|S| \geq \gamma l) \wedge \left(\sum_{i \in T} W_i \geq (1-\varepsilon)|T| \right) \wedge \left(\sum_{i \in S \setminus T} W_i < (1-2\varepsilon)|S \setminus T| \right) \right] \\ &\geq p_\top - 2^{-2\varepsilon^2\gamma l} \Pr\left[|S| \geq \gamma l\right] \\ &\geq p_\top - 2^{-2\varepsilon^2\gamma l}, \end{aligned}$$

where the inequality in the second line is again due to Lemma 6. Since we also again have $p_{\widetilde{\mathcal{E}}} = p_{\widetilde{\mathcal{E}}|\top} p_\top$, the above bound gives $p_{\widetilde{\mathcal{E}}|\top} \geq (p_\top - 2^{-2\varepsilon^2\gamma l})/p_\top = 1 - 2^{-2\varepsilon^2\gamma l}/p_\top$. In other words, we have shown that the probability of the event (11) in the state ρ^1 is at least $1 - 2^{-2\varepsilon^2\gamma l}/p_\top$. Recalling that

[12] Note that we previously defined ρ^1 to be the state produced by the following sequence of steps: perform the measurements on T, then condition on a particular event, then perform the measurements on $\overline{T}$. However, this is where we use the condition imposed on honest Bob's boxes that the order of measurements does not change the distribution: because of that condition, we can equivalently consider ρ^1 to be the state where all the measurements are performed before the event is conditioned on.

$\widetilde{\rho}^1$ is the state conditioned on that event, from the definition of the 1-norm distance it immediately follows that $\|\rho^1 - \widetilde{\rho}^1\|_1 \leq 2(1 - p_{\widetilde{\mathcal{E}}|\top}) \leq 2 \cdot 2^{-2\varepsilon^2\gamma l}/p_\top$.

In $\widetilde{\rho}^1$, the K^{B} thus obtained differs from K^{A} in at most $2\varepsilon|S|$ many indices. The number of $|S|$-bit binary strings that can disagree with K^{B} in at most $2\varepsilon|S|$ places is at most $2^{h_2(2\varepsilon)|S|} \leq 2^{h_2(2\varepsilon)l}$. Hence,

$$\mathsf{H}_0(K^{\mathrm{A}}|K^{\mathrm{B}})_{\widetilde{\rho}^1} \leq h_2(2\varepsilon)l$$

and this implies that the $(2 \cdot 2^{-2\varepsilon^2\gamma l}/p_\top)$-smoothed entropy of ρ^1 is at most $h_2(2\varepsilon)l$. Hence by Fact 20, we get the required result.[13] □

5.3 Secrecy

We now prove some lemmas which, in the context of the alternative security definitions in Section 2.5, will imply the secrecy property (as we shall discuss in Section 5.5). In the context of our composable security analysis (in Section 6), however, these will just be intermediate results in the full composable security proof.

Specifically, we prove two lower bounds for the (smoothed) min-entropy of K^{A} in the states ρ and σ, conditioned on Bob and Eve's side information and the randomness R. These will later allow us to show secrecy of the protocol via the Leftover Hashing Lemma.

Lemma 22. *If Bob plays honestly and $p_\top \geq 2 \cdot 2^{-2\varepsilon^2\gamma l}$, then the state $\rho^1_{C_2RK^{\mathrm{A}}\widetilde{B}B_T\widetilde{E}}$ satisfies*

$$\mathsf{H}_\infty^{\delta_\top}(K^{\mathrm{A}}|C_2RB_T\widetilde{E})_{\rho^1} \geq d^{\mathrm{E}}(c_\alpha^{\mathrm{E}} - 2\varepsilon)^3\alpha^2 l - 2\varepsilon^2\gamma l - 2\gamma l - h_2(2\varepsilon)l - \log(1/\lambda_{\mathrm{EC}}),$$

where $c_\alpha^{\mathrm{E}}, d^{\mathrm{E}}$ are the constants from Theorem 18, and $\delta_\top = \frac{2\cdot 2^{-2\varepsilon^2\gamma l}}{p_\top}$.

Proof. We follow the proof approach of [Vid17] for the protocol in [JMS20]. First we shall bound $\mathsf{H}_\infty^{\delta_\top}(K^{\mathrm{A}}|SX_SY_S\widetilde{E})_{\rho^1}$. Consider the $\mathrm{MSE}^{t/l}$ game with $t = (1 - 2\varepsilon)l$ being played on the shared state between Alice, Bob and Eve. Let W_i denote the indicator variable for the event $a_i[y_i] = b_i[x_i]$ and V_i denote the indicator variable for the event $a_i[y_i] = c_i$ (Eve's guess for the i-th bit). The winning condition for the i-th game is $W_i \wedge V_i = 1$.

By Theorem 18, the winning probability of $\mathrm{MSE}^{t/l}$ on the original state shared by Alice, Bob and Eve is at most $2^{-d^{\mathrm{E}}(c_\alpha^{\mathrm{E}}-2\varepsilon)^3\alpha^2 l}$. We first consider the state $\widetilde{\rho}^1$ defined in the proof of Lemma 21, i.e. this original state conditioned on the event (11). Denoting the probability of this conditioning event as $p_{\widetilde{\mathcal{E}}}$, we can bound the winning probability of $\mathrm{MSE}^{t/l}$ on the state $\widetilde{\rho}^1$ as

$$\Pr_{\widetilde{\rho}^1}[\text{Win } \mathrm{MSE}^{t/l}] \leq \frac{2^{-d^{\mathrm{E}}(c_\alpha^{\mathrm{E}}-2\varepsilon)^3\alpha^2 l}}{p_{\widetilde{\mathcal{E}}}}.$$

[13] Strictly speaking, in order to actually implement the [Ren05] protocol (Fact 20), it is not sufficient to only have the upper bound $\mathsf{H}_0^\delta(K^{\mathrm{A}}|K^{\mathrm{B}}) \leq h_2(2\varepsilon)l$. Rather, for each value of K^{B} Bob needs to know the set of K^{A} values such that $\Pr[K^{\mathrm{A}}|K^{\mathrm{B}}] > 0$, where the probability is with respect to some distribution in the δ-ball that attains $\mathsf{H}_0(K^{\mathrm{A}}|K^{\mathrm{B}}) = h_2(2\varepsilon)l$. The proof we give here indeed characterizes this set, namely the set of K^{A} that differ from K^{B} in at most $2\varepsilon l$ indices, so it is possible to apply that protocol.

By construction, in $\widetilde{\rho}^1$ there is always some subset of S with size at least $(1-2\varepsilon)|S|$ on which $W_i = 1$ for each i. Hence whenever $V_i = 1$ for all $i \in S$, $\mathrm{MSE}^{t/l}$ is won. This implies

$$\Pr_{\widetilde{\rho}^1}\left[\sum_{i\in S} V_i = |S|\right] \leq \Pr_{\widetilde{\rho}^1}[\text{Win MSE}^{t/l}].$$

But the probability of $V_i = 1$ for all $i \in S$ is the probability that Eve is able to guess $a_i[y_i]$ given $x_i y_i$ for all $i \in S$. Hence from Fact 12,

$$\begin{aligned} H_\infty(K^{\mathrm{A}}|SX_SY_S\widetilde{E})_{\widetilde{\rho}^1} &= \log\left(\frac{1}{\Pr_{\widetilde{\rho}^1}\left[\sum_{i\in S} V_i = |S|\right]}\right) \\ &\geq d^{\mathrm{E}}(c_\alpha^{\mathrm{E}} - 2\varepsilon)^3\alpha^2 l - \log(1/p_{\widetilde{\mathcal{E}}}). \end{aligned}$$

We now relate this to the state of interest ρ^1 (i.e. the state conditioned only on the event $(|S| \geq \gamma l) \wedge (\sum_{i\in T} W_i \geq (1-\varepsilon)|T|)$) by recalling that $\|\rho^1 - \widetilde{\rho}^1\|_1 \leq \delta_\top$ as shown in the proof of Lemma 21, and hence the $\delta_\top$-smoothed min-entropy of ρ^1 is at least the above value as well. Furthermore, since the Serfling bound in the form of Lemma 6 also implies $p_{\widetilde{\mathcal{E}}} \geq p_\top - 2^{-2\varepsilon^2\gamma l}$ (this addresses a minor issue in the [Vid17] proof, which just replaced $p_{\widetilde{\mathcal{E}}}$ with $p_\top$ directly), we have

$$\begin{aligned} H_\infty^{\delta_\top}(K^{\mathrm{A}}|SX_SY_S\widetilde{E})_{\rho^1} &\geq d^{\mathrm{E}}(c_\alpha^{\mathrm{E}} - 2\varepsilon)^3\alpha^2 l - \log\frac{1}{p_\top - 2^{-2\varepsilon^2\gamma l}} \\ &\geq d^{\mathrm{E}}(c_\alpha^{\mathrm{E}} - 2\varepsilon)^3\alpha^2 l - 2\varepsilon^2\gamma l, \end{aligned}$$

using the condition $p_\top \geq 2\cdot 2^{-2\varepsilon^2\gamma l}$.

Finally, the other parts of R besides SX_SY_S are T (which Eve already has in $\widetilde{E}$), $Y'_{\overline{T}}$, H and U_1U_2. But K^{A} is independent of $Y'_{\overline{T}}$ given SY_S (since K^{A} is produced by a measurement in Alice's boxes only, which has no relation to Bob's string $Y'_{\overline{T}}$ apart from the values SY_S used to specify which bits of Alice's input to include in K^{A}), and H and U_1U_2 are independent of everything else (since by construction they are drawn uniformly and independently of all other registers here). Hence giving Eve these extra registers in R makes no difference. Lastly, to handle C_2 and B_T (which are not independent of K^{A}), we simply note that C_2 is at most $h_2(2\varepsilon)l + \log(1/\lambda_{\mathrm{EC}})$ bits and B_T is at most $2\gamma l$ bits, hence by Fact 10 we get the desired result. □

For proving the next bound, we shall need the following fact, which is easily proven by a summation relabelling:

Fact 23. *Consider a CQ state ρ_{ZQ} where Z is an s-bit classical register. If we select an independent uniformly random $U \in \{0,1\}^s$ and generate a register $C = Z \oplus U$, then the resulting global state,*

$$\sum_{z\in\{0,1\}^s}\sum_{u\in\{0,1\}^s} \frac{1}{2^s}\mathsf{P}_Z(z)\,|z\oplus u\rangle\langle z\oplus u|_C \otimes |u\rangle\langle u|_U \otimes |z\rangle\langle z|_Z \otimes \rho_{Q|z}, \tag{12}$$

is equal to

$$\sum_{z\in\{0,1\}^s}\sum_{u\in\{0,1\}^s} \frac{1}{2^s}\mathsf{P}_Z(z)\,|u\rangle\langle u|_C \otimes |z\oplus u\rangle\langle z\oplus u|_U \otimes |z\rangle\langle z|_Z \otimes \rho_{Q|z}. \tag{13}$$

When applying this fact, we shall take U to correspond to (U_1, U_2) in Protocol 5, which is basically a one-time pad. Intuitively, Fact 23 expresses a symmetry[14] between the "ciphertext" and the "padding string" when applying a one-time pad — while we usually think of the ciphertext as taking the value $Z \oplus U$ and the padding string as taking the independent uniform value U, this fact implies that we have an exactly equivalent situation by thinking of the ciphertext as taking the value U and the padding string as taking the value $Z \oplus U$. We use this to prove the following lemma (for all possible behaviours by Bob and Eve — note that while dishonest Bob does not have to honestly report the "raw" outcomes of measurements on his states, such behaviour can simply be absorbed into the strategy he uses to generate $\widetilde{B}$ and B_T):

Lemma 24. *The probability $p_{\checkmark|\top}$ is independent of the message m. Furthermore, letting R' denote all the registers in R except U_1, the state $\sigma_{K^{\mathrm{A}}CR'\widetilde{B}B_T\widetilde{E}}$ satisfies*

$$\mathsf{H}_\infty(K^{\mathrm{A}}|CR'\widetilde{B}B_T\widetilde{E})_\sigma \geq d^{\mathrm{B}}(c_\alpha^{\mathrm{B}} - \varepsilon)^3\alpha^2(1-\gamma)l - \log(1/p_\top p_{\checkmark|\top}) - \gamma l - h_2(2\varepsilon)l - \log(1/\lambda_{\mathrm{EC}}),$$

where $c_\alpha^{\mathrm{B}}, d^{\mathrm{B}}$ are the constants from Theorem 16.

Proof. Recall that U was initially generated as a uniformly random value independent of all the other registers, and that it is not revealed to Bob and Eve until the final time t_5. Also, by Fact 23, we know that at the point at which C is generated, the global state remains the same if we swap the roles of the registers C and U. This means that it is perfectly equivalent to instead consider the following "virtual" process: Bob and Eve generate an independent uniformly random value in the register C, and this is used to generate a register $U = (M \oplus h(K^{\mathrm{A}}) \oplus C_1, \mathtt{syn}(K^{\mathrm{A}}) \oplus C_2)$ which is given to Alice only (until time t_5). We stress that this virtual process does not correspond to a physical procedure which is actually performed, but it produces exactly the same state as the original protocol, so it is valid to study it in place of the original protocol.

With this process in mind, it is clear that $p_{\checkmark|\top}$ is independent of m, since the only register that depends on m at that point is always with Alice and not acted upon. We shall now prove

$$\mathsf{H}_\infty(K^{\mathrm{A}}|CR''\widetilde{B}B_T\widetilde{E})_\sigma \geq d^{\mathrm{B}}(c_\alpha^{\mathrm{B}} - \varepsilon)^3\alpha^2(1-\gamma)l - \log(1/p_\top p_{\checkmark|\top}) - \gamma l,$$

where R'' denotes all the registers in R except U_1U_2. From there the desired bound would follow by subtracting the number of bits in U_2, via Fact 10.

Under the virtual process, the register C is locally generated from the joint system of Bob and Eve, without access to any of Alice's registers. Hence we can proceed as in the proof of Lemma 22, this time by considering the game $\mathrm{MSB}_\alpha^{t/(1-\gamma)l}$ for $t = (1-\varepsilon)(1-\gamma)l$ on the set $\overline{T} = [l] \setminus T$ between Alice and the joint system of Bob and Eve. In this case, however, an important difference is that we allow the output distribution to depend on which subset T is supplied first (this information is implicitly included in R''). This works because Alice's accept condition at this point is directly the condition that enough rounds are won on the entire set, instead of a small test subset. In particular, this means that for each input order we can directly study the corresponding state conditioned on accepting, without relating it to some "nearby" state that is independent of the input order (this

[14] For the purposes of our proof, we technically do not need such an exact symmetry — it would suffice to have functions f and g such that (12) and (13) are equal when register C in (12) is set to $f(z,u)$ and register U in (13) is set to $g(z,u)$. However, our proof is easier to describe using the formulation shown. Furthermore, in principle our proofs also hold using a relaxed version of this statement in which (12) and (13) are only λ_{OTP}-close in ℓ_1 distance for some value $\lambda_{\mathrm{OTP}} > 0$, at the cost of increasing our composable security parameter by $O(\lambda_{\mathrm{OTP}})$.

was the only part of the Lemma 22 proof that required the condition on honest Bob's boxes, in order to apply the Serfling bound).

However, even apart from the $|S| \geq \gamma l$ conditioning (whose probability is included in $p_\top$), the input distribution in $\overline{T}$ is not quite right for $\mathrm{MSB}^{t/(1-\gamma)l}$. To see this, let us recap the distribution in the actual protocol of the sets S and T conditioned on $|S| \geq \gamma l$, according to step 2:

- Let P_{ST} denote the distribution of the variables S and T in the actual protocol, where $S \subseteq [l]$ is generated by choosing each index independently with probability $(1-\alpha)$. Let $\mathcal{E}_1$ denote the event that $|S| \geq \gamma l$ when S is drawn according to P_S, and $\mathsf{P}_{ST|\mathcal{E}_1}$ is the joint distribution of S and T conditioned on this event (in which case T is a uniformly random subset of S).

To relate this to the game $\mathrm{MSB}_\alpha^{t/(1-\gamma)l}$ (for arbitrary t), we would like to consider the game to be played on $\overline{T}$, and consider $S \cap \overline{T}$ to specify the subset of $\overline{T}$ on which Alice and Bob get nontrivial inputs. However, since in $\mathsf{P}_{ST|\mathcal{E}_1}$ the subset S was drawn first and T was then drawn as a subset of it, this somewhat affects the distribution of $S \cap \overline{T}$ within $\overline{T}$ (in that $S \cap \overline{T}$ is not distributed according to choosing each index in $\overline{T}$ independently with probability $(1-\alpha)$). To obtain sets ST with a distribution suitable for $\mathrm{MSB}_\alpha^{t/(1-\gamma)l}$ in the preceding sense, we could instead consider the following distribution:

- Let Q_{ST} denote the distribution obtained as follows: choose T as a uniformly random subset of $[l]$ with size γl; independently generate $S \subseteq [l]$ by choosing each index independently with probability $(1-\alpha)$. Since S and T are chosen independently, it can be seen that Q_{ST} indeed gives the right input distribution for $\mathrm{MSB}_\alpha^{t/(1-\gamma)l}$ played on $\overline{T}$ with Alice and Bob getting nontrivial inputs on $S \cap \overline{T}$.

Now let $\mathcal{E}_2$ be the event that when S and T are drawn according to Q_{ST}, T is a subset of S; $\mathsf{Q}_{ST|\mathcal{E}_2}$ is the distribution conditioned on this event. Since S and T are independent in Q_{ST}, the distribution $\mathsf{Q}_{ST|\mathcal{E}_2}$ can be equivalently described as first choosing S followed by T according to their respective distributions, and then conditioning on $T \subseteq S$ — but from this, we see that in fact $\mathsf{Q}_{ST|\mathcal{E}_2}$ is just the same distribution as $\mathsf{P}_{ST|\mathcal{E}_1}$ (note that $T \subseteq S$ implicitly includes the condition $|S| \geq \gamma l$, since T always has size γl).

Since conditioning on an event with probability q cannot increase probabilities by more than a factor of $1/q$, we see that when studying the protocol we can compensate for using the actual distribution $\mathsf{P}_{ST|\mathcal{E}_1}$ (i.e. $\mathsf{Q}_{ST|\mathcal{E}_2}$) instead of the "correct game distribution" Q_{ST} by rescaling all upper bounds on probabilities by $1/\Pr_{\mathsf{Q}}[T \subseteq S]$. From the definition of Q_{ST}, we can easily compute that $\Pr_{\mathsf{Q}}[T \subseteq S] = (1-\alpha)^{\gamma l}$, hence we shall include this factor when bounding the winning probability of $\mathrm{MSB}_\alpha^{t/(1-\gamma)l}$ under the actual protocol's input distribution.

With this, we return to the topic of bounding the min-entropy. The state σ is conditioned on the first round of $\mathrm{MSB}_\alpha^{t/(1-\gamma)l}$ winning, as well as the initial conditioning of outputting $\top$. The probability of winning both the first and second rounds on an unconditioned state with an unconditioned input distribution is at most $2^{-d^{\mathrm{B}}(c_\alpha^{\mathrm{B}}-\varepsilon)^3\alpha^2(1-\gamma)l}$. Hence,

$$\mathsf{H}_\infty(K^{\mathrm{A}}|R''\widetilde{B}B_T\widetilde{E})_\sigma = \log\left(\frac{1}{\Pr_\sigma\left[\mathrm{Win}\ \mathrm{MSB}_\alpha^{t/(1-\gamma)l}\right]}\right) \geq \log\left(\frac{(1-\alpha)^{\gamma l}p_\top p_{\checkmark|\top}}{2^{-d^{\mathrm{B}}(c_\alpha^{\mathrm{B}}-\varepsilon)^3\alpha^2(1-\gamma)l}}\right),$$

which yields the desired bound (noting that $\log(1-\alpha) > -1$ since we took the condition $\alpha < \frac{1}{2}$ in Lemma 19 to be satisfied). We get the min-entropy instead of smoothed min-entropy here (and

we do not need an explicit lower bound on $p_\top p_{\checkmark|\top}$, unlike Lemma 22) because Alice checks the condition on the entire $\overline{T}$ instead of a test subset, so we do not need to consider a "nearby" state in place of the actual conditional state. □

5.4 Parameter choices

Take any values of $\alpha \in (0, \frac{1}{2})$ and $\varepsilon \in (0, 1)$ satisfying

$$\min\{d^{\mathrm{E}}(c_\alpha^{\mathrm{E}} - 2\varepsilon)^3\alpha^2 \ , \ d^{\mathrm{B}}(c_\alpha^{\mathrm{B}} - \varepsilon)^3\alpha^2\} > h_2(2\varepsilon). \tag{14}$$

To construct this more explicitly, we could focus on a fixed choice of α (say, $\alpha = 0.4$), in which case there clearly exists ε_0 such that $\min\{d^{\mathrm{E}}(c_\alpha^{\mathrm{E}} - 2\varepsilon_0)^3\alpha^2 \ , \ d^{\mathrm{B}}(c_\alpha^{\mathrm{B}} - \varepsilon_0)^3\alpha^2\} > h_2(2\varepsilon_0)$ (by noting the behaviour of both sides as $\varepsilon_0 \to 0$). This value is then a valid choice of ε_0 in Theorem 2, since (14) would then be satisfied for any $\varepsilon \in (0, \varepsilon_0]$ (using that fixed choice of α).

Now take some $\lambda_{\mathrm{com}}, \lambda_{\mathrm{CI}}, \lambda_{\mathrm{EC}} \in (0, 1]$ and some desired message length n, and choose l large enough such that when setting

$$\gamma = \frac{1}{\varepsilon^2 l} \max\left\{8 \log \frac{2}{\lambda_{\mathrm{com}}} \ , \ \frac{1}{2} \log \frac{8}{\lambda_{\mathrm{CI}}} \ , \ \frac{1}{2} \log \frac{8}{\lambda_{\mathrm{EC}}}\right\}, \tag{15}$$

the following conditions are satisfied: firstly, $\gamma < \frac{1}{2}$, secondly,

$$2^{-(1-2\gamma)^2 l/8} \leq \frac{\lambda_{\mathrm{com}}}{2}, \tag{16}$$

and lastly,

$$\begin{aligned} n &\leq d^{\mathrm{E}}(c_\alpha^{\mathrm{E}} - 2\varepsilon)^3\alpha^2 l - 2\varepsilon^2\gamma l - 2\gamma l - h_2(2\varepsilon)l - \log(1/\lambda_{\mathrm{EC}}) - 2\log(2/\lambda_{\mathrm{CI}}), \\ n &\leq d^{\mathrm{B}}(c_\alpha^{\mathrm{B}} - \varepsilon)^3\alpha^2(1-\gamma)l - \gamma l - h_2(2\varepsilon)l - \log(1/\lambda_{\mathrm{EC}}) - 2\log(2/\lambda_{\mathrm{CI}}). \end{aligned} \tag{17}$$

The conditions $\gamma < \frac{1}{2}$ and (16) ensure that the conditions on γ, l for Lemma 19 are satisfied. Since the choice of γ in (15) satisfies $\gamma \to 0$ as $l \to \infty$, these conditions can always be satisfied by taking sufficiently large l. Furthermore, given that (14) holds, for any n the conditions (17) will be satisfied at sufficiently large l, because all the γl terms are independent of l for this choice of γ.

For these parameter choices, together with a choice of syndrome satisfying Lemma 21 for the specified λ_{EC} value, the described ECD protocol satisfies the following security properties (which hold independently of Conjecture 1). They are qualitatively similar to the notions of completeness, correctness and secrecy laid out in the alternative definition in Section 2.5: we discuss in Section 5.5 how they imply that the properties in that alternative definition are indeed satisfied, whereas in Section 6 we use these results to prove composable security.

Lemma 25. *Given parameter choices satisfying (14)–(17), if Bob and Eve are honest, then*

$$1 - p_\top \leq \lambda_{\mathrm{com}}.$$

Also, if Bob is honest and $D = 1$ (i.e. Alice requests a deletion certificate), then

$$p_\top(1 - p_{\checkmark|\top}) \leq \lambda_{\mathrm{com}}.$$

Proof. This follows immediately from Lemma 19, recalling that we chose parameters such that $2^{-(1-2\gamma)^2 l/8} \leq \lambda_{\mathrm{com}}/2$ and $\gamma \geq 8\log(2/\lambda_{\mathrm{com}})/(\varepsilon^2 l) \geq \log(1/\lambda_{\mathrm{com}})/(2\varepsilon^2 l)$. □

Lemma 26. *Given parameter choices satisfying (14)–(17), if Bob is honest, then for any specific message value $M = m$ we have*

$$p_\top \Pr[\widetilde{M} \neq m | O = \top] \leq \lambda_{\mathrm{EC}}.$$

Proof. Observe that conditioned on $O = \top$ in step 10 of the protocol (so that Bob gets the value $C_1 = m \oplus h(K^{\mathrm{A}}) \oplus U_1$ from Alice, where m is the specific message value we discuss here), honest Bob's final value $\widetilde{M} = C_1 \oplus h(\widetilde{K}^{\mathrm{A}}) \oplus U_1$ will be equal to m whenever his guess $\widetilde{K}^{\mathrm{A}}$ matches Alice's value K^{A}. Hence conditioned on $O = \top$, the probability that his final value $\widetilde{M}$ differs from m (i.e. $\Pr[\widetilde{M} \neq m | O = \top]$) is at most the probability that his guess was wrong, i.e. $\widetilde{K}^{\mathrm{A}} \neq K^{\mathrm{A}}$. Recalling that we chose parameters such that $\gamma \geq \log(8/\lambda_{\mathrm{EC}})/(2\varepsilon^2 l)$, Lemma 21 tells us for honest Bob, the probability that $\widetilde{K}^{\mathrm{A}} \neq K^{\mathrm{A}}$ is at most

$$\frac{2 \cdot 2^{-2\varepsilon^2 \gamma l}}{p_\top} + \frac{\lambda_{\mathrm{EC}}}{2} \leq \frac{\lambda_{\mathrm{EC}}}{2p_\top} + \frac{\lambda_{\mathrm{EC}}}{2} \leq \frac{\lambda_{\mathrm{EC}}}{p_\top},$$

which gives the desired result. □

Lemma 27. *Given parameter choices satisfying (14)–(17), we have for any specific message value $M = m$:*

$$p_\top p_{\checkmark | \top} \left\| \sigma_{C R \widetilde{B} B_T \widetilde{E}}(m, 1) - \sigma_{C R \widetilde{B} B_T \widetilde{E}}(0^n, 1) \right\|_1 \leq 2\lambda_{\mathrm{CI}},$$

and if Bob plays honestly,

$$p_\top \left\| \rho^1_{C R B_T \widetilde{E}}(m, 0) - \rho^1_{C R B_T \widetilde{E}}(0^n, 0) \right\|_1 \leq 2\lambda_{\mathrm{CI}}.$$

Proof. We first prove the expression for ρ^1, which is under the assumption that Bob plays honestly. Observe that if $p_\top < 2 \cdot 2^{-2\varepsilon^2 \gamma l}$, then we are already done since we chose $\gamma \geq \log(8/\lambda_{\mathrm{CI}})/(2\varepsilon^2 l)$. Hence we can take $p_\top \geq 2 \cdot 2^{-2\varepsilon^2 \gamma l}$, in which case we can put together the bound in Lemma 22 with the first of the bounds on n in (17) to get

$$\frac{1}{2}\left(\mathsf{H}_\infty^{\delta_\top}(K^{\mathrm{A}} | C_2 R B_T \widetilde{E})_{\rho^1} - n \right) \geq \log(2/\lambda_{\mathrm{CI}}).$$

Let S be a register storing the value of the hash $h(K^{\mathrm{A}})$. Recalling that $\gamma \geq \log(8/\lambda_{\mathrm{CI}})/(2\varepsilon^2 l)$, the Leftover Hashing Lemma then implies

$$\left\| \rho^1_{S C_2 R B_T \widetilde{E}} - \frac{\mathbb{1}_S}{2^n} \otimes \rho^1_{C_2 R B_T \widetilde{E}} \right\|_1 \leq 2^{-\log(2/\lambda_{\mathrm{CI}})} + 2\frac{2 \cdot 2^{-2\varepsilon^2 \gamma l}}{p_\top} \leq \frac{\lambda_{\mathrm{CI}}}{2} + \frac{\lambda_{\mathrm{CI}}}{2p_\top} \leq \frac{\lambda_{\mathrm{CI}}}{p_\top}.$$

The state on these registers is independent of the value of M. Now for any message value m, let $\mathcal{E}^m$ denote the map that generates the ciphertext register $C_1 = m \oplus s$ by reading s off the register S and then tracing it out. By the properties of the one-time pad, we know that

$$\mathcal{E}^m\left(\frac{\mathbb{1}_S}{2^n} \otimes \rho^1_{C_2 R B_T \widetilde{E}} \right) = \mathcal{E}^{0^n}\left(\frac{\mathbb{1}_S}{2^n} \otimes \rho^1_{C_2 R B_T \widetilde{E}} \right).$$

This yields the desired result:

$$\begin{aligned}
&\left\|\rho^1_{CRB_T\widetilde{E}}(m,0) - \rho^1_{CRB_T\widetilde{E}}(0^n,1)\right\|_1 \\
=&\left\|\mathcal{E}^m\left(\rho^1_{SC_2RB_T\widetilde{E}}\right) - \mathcal{E}^{0^n}\left(\rho^1_{SC_2RB_T\widetilde{E}}\right)\right\|_1 \\
\leq&\left\|\mathcal{E}^m\left(\rho^1_{SC_2RB_T\widetilde{E}}\right) - \mathcal{E}^m\left(\frac{\mathbb{1}_S}{2^n}\otimes\rho^1_{C_2RB_T\widetilde{E}}\right)\right\|_1 + \left\|\mathcal{E}^{0^n}\left(\frac{\mathbb{1}_S}{2^n}\otimes\rho^1_{C_2RB_T\widetilde{E}}\right) - \mathcal{E}^{0^n}\left(\rho^1_{SC_2RB_T\widetilde{E}}\right)\right\|_1 \\
\leq&\frac{2\lambda_{\mathrm{CI}}}{p_\top},
\end{aligned}$$

using Fact 9 in the last line.

For σ, it is again easier to analyze the situation by using Fact 23 to switch to the virtual process of C being a uniformly random value and U being set to $U = (M \oplus h(K^{\mathrm{A}}) \oplus C_1, \mathtt{syn}(K^{\mathrm{A}}) \oplus C_2)$. We then follow a similar argument as above: by Lemma 24 and the second bound on n in (17), we have

$$\frac{1}{2}\left(\mathsf{H}_\infty(K^{\mathrm{A}}|CR'\widetilde{B}B_T\widetilde{E})_\sigma - n\right) \geq \log(2/\lambda_{\mathrm{CI}}) - \frac{1}{2}\log(1/p_\top p_{\checkmark|\top}) \geq \log(2/\lambda_{\mathrm{CI}}) - \log(1/p_\top p_{\checkmark|\top}),$$

where R' denotes all the registers in R except U_1. Defining $\hat{\mathcal{E}}^m$ the same way as $\mathcal{E}^m$ above, except with the output register being U_1 instead of C_1, we follow the same line of reasoning and obtain

$$\left\|\sigma_{CR\widetilde{B}B_T\widetilde{E}}(m,1) - \sigma_{CR\widetilde{B}B_T\widetilde{E}}(0^n,1)\right\|_1 = \left\|\hat{\mathcal{E}}^m\left(\sigma_{CR'\widetilde{B}B_T\widetilde{E}}\right) - \hat{\mathcal{E}}^{0^n}\left(\sigma_{CR'\widetilde{B}B_T\widetilde{E}}\right)\right\|_1 \leq \frac{2\lambda_{\mathrm{CI}}}{p_\top p_{\checkmark|\top}}.$$

(In fact, a tighter bound of $\lambda_{\mathrm{CI}}/(p_\top p_{\checkmark|\top})$ holds here since the min-entropy bound for σ is not smoothed, but we shall not track this detail.) □

5.5 Security under the alternative definition

From the above properties, it is not difficult to show that the required properties for the alternative security definition in Section 2.5 are satisfied. Firstly, the completeness requirements (1)–(2) are precisely the properties shown in Lemma 25. Next, the correctness requirement (3) is precisely the property shown in Lemma 26.

As for the secrecy requirements (4)–(6), we first observe that (4) trivially holds over the required duration (i.e. until the decryption key is released), because the only point in the encryption phase that potentially depends on the message is the value $M \oplus h(K^{\mathrm{A}}) \oplus U_1$ in step 15, but by Fact 23 this register is in fact also independent of the message (until U_1 is released) since U_1 serves as a one-time-pad that is kept secret until being released in the decryption key R. As for the requirement (5), it also trivially holds before the decryption key R is released, for the same reason; whereas after that point, it is ensured by the first bound in the Lemma 27 statement (together with the fact that any further processing of Bob and/or Eve's registers cannot increase that trace distance, by the data-processing inequality). Finally, an analogous argument holds for the requirement (6): it trivially holds before the decryption key R is released, and afterwards it is ensured by the second bound in the Lemma 27 statement.

6 Composable security proof

In this section, we prove our main security result, which implies Theorem 2. The argument essentially only depends on Fact 23 and Lemmas 25–27, without requiring the details of the analysis leading up to those lemmas.

Theorem 28. *Assuming Conjecture 1, there exists a universal constant $\varepsilon_0 \in (0,1)$ such that for any $\varepsilon \in (0,\varepsilon_0]$, $\lambda_{\mathrm{com}}, \lambda_{\mathrm{CI}}, \lambda_{\mathrm{EC}} \in (0,1]$ and $n \in \mathbb{N}$, there exist parameter choices for Protocol 1 such that it constructs the ECD_n functionality from the resources $\mathcal{R}$, $\mathcal{C}$ and $(\mathcal{B}_1^1 \dots \mathcal{B}_l^1, \mathcal{B}_1^2 \dots \mathcal{B}_l^2)_\varepsilon$, within distance $\lambda = 2\lambda_{\mathrm{com}} + \lambda_{\mathrm{CI}} + \lambda_{\mathrm{EC}}$.*

As noted in the previous section, using the value of ε_0 specified there allows us to choose parameters such that (14)–(17) are satisfied, in which case Lemmas 25–27 hold and we can use them in our subsequent proof. To prove composable security according to Definition 1, we need to consider the four possible combinations of honest/dishonest Bob and Eve's behaviours, and for each case bound the distinguishing probability between the real functionality with the honest parties performing the honest protocol, versus the ideal functionality with some simulator attached to the dishonest parties' interfaces. We shall construct appropriate simulators and argue that for a distinguisher interacting with either scenario, the states held by the distinguisher in the two scenarios differ in ℓ_1 distance by at most $2\lambda = 4\lambda_{\mathrm{com}} + 2\lambda_{\mathrm{CI}} + 2\lambda_{\mathrm{EC}}$ at all times. This implies the distinguishing advantage is bounded by λ via Fact 9, since the process of the distinguisher producing a value on the guess register G can be viewed as a channel applied to the states it holds.

Note that it suffices to consider only the points where output registers are released to the distinguisher, since by Fact 9, any operations the distinguisher performs between these points cannot increase the ℓ_1 distance. Furthermore, we observe that for classical inputs, it is not necessary to bound the distinguishability for all possible input distributions that the distinguisher could supply — it suffices to find a bound that holds for all specific values that could be supplied as input, since by convexity of the ℓ_1 norm, the same bound would hold when considering arbitrary distributions over those input values. In particular, for the subsequent arguments we shall assume the distinguisher supplies a specific value m for the input M, and we shall split the analysis into different cases for the two possible values for the input D.

Remark 7. *In the following proofs, we shall construct simulators by explicitly using Fact 23, but an alternative approach appears possible, which we sketch out here. First, observe that the use of the one-time pad U in Protocol 1 is in fact a composably secure realization of a functionality we could call a* trusted-sender channel with delay*, which is defined in exactly the same way as the* channel with delay *in [VPR19], except that only the recipient is potentially dishonest.*[15] *If we now view Protocol 1 as sending the value $(M \oplus h(K^{\mathrm{A}}), \mathtt{syn}(K^{\mathrm{A}}))$ through a composably secure implementation of a trusted-sender channel with delay, we can safely assume that the C register gives no information to the dishonest parties about Alice's outputs until the final step, which may be a helpful perspective to keep in mind when considering the proofs below. Essentially, our approach below has the simulator in the composable security proof for the trusted-sender channel with delay "built into" the argument directly, by repeated use of Fact 23.*

Since in this section we are proving results in the Abstract Cryptography framework, we shall

[15] Proving this would be fairly simple: just follow the argument in the composable security proof for the one-time pad [PR14], except with appropriate changes in timing.

now explicitly refer to various actions in the Protocol 1 description as being performed by the protocols Π^{A} and Π^{B} rather than Alice and Bob (recall the discussion in Remark 4).

6.1 Dishonest Bob and Eve

The distinguisher's task in this case is to distinguish $\Pi^{\mathrm{A}}\mathcal{F}_{\mathrm{BE}}^{\mathrm{real}}$ and $\mathcal{F}_{\mathrm{BE}}^{\mathrm{ideal}}\Sigma^{\mathrm{BE}}$. As mentioned in the introduction, intuitively speaking we shall choose the simulator Σ^{BE} here to run the honest protocol internally with a "virtual" simulated instance of the protocol Π^{A} (and a "dummy" version of the protocol's inputs on Alice's interfaces, which we shall soon describe) — the construction here is in fact rather similar to the QKD analysis in [PR14]; the example described there may be instructive in helping to understand our construction.

To give a broad overview (the detailed description will subsequently follow; see also Figure 4), the simulator begins by following the actions of Π^{A} in Protocol 1: it accepts the boxes from Eve, generates S and T the same way as step 2, generates inputs the same way as in step 3 and supplies them to the boxes, etc — in particular, on step 7 it accepts some value of b_T supplied at Bob's interface[16], then performs the checks in step 8, and so on. A small difference occurs in step 10, where an output value O is produced by Π^{A} that would normally be sent out to Alice's interface on Π^{A}; here however the simulator is instead supposed to be connected to $\mathcal{F}_{\mathrm{BE}}^{\mathrm{ideal}}$ on that interface, and hence we shall instead make the simulator supply the value O as the input values O^{B} and O^{E} on the relevant interfaces in the ideal functionality (this is again a very similar construction to the QKD analysis in [PR14]). Upon reaching step 14 we encounter a notable obstacle: the simulator does not have access to the true message value m supplied to Alice's interface on $\mathcal{F}_{\mathrm{BE}}^{\mathrm{ideal}}\Sigma^{\mathrm{BE}}$ (since the simulator is only attached to Bob and Eve's interfaces in $\mathcal{F}_{\mathrm{BE}}^{\mathrm{ideal}}$). Hence what it does at that step is that it instead acts as though the message had a dummy value 0^n, and releases a corresponding ciphertext $C_1 = 0^n \oplus u_1$ (where u_1 is the uniformly random value drawn in step 13). In our security proof below, we will be showing that despite this substitution, the distinguisher still cannot easily distinguish $\Pi^{\mathrm{A}}\mathcal{F}_{\mathrm{BE}}^{\mathrm{real}}$ and $\mathcal{F}_{\mathrm{BE}}^{\mathrm{ideal}}\Sigma^{\mathrm{BE}}$. Proceeding onwards in a similar fashion, the last notable point is that if in the final steps the values of D and F are such that ideal functionality releases the true message value m, then the simulator will use m to set the value on the register U_1 to $m \oplus h(k^{\mathrm{A}}) \oplus u_1$ instead, before releasing it as part of R[17] — the idea here is that by setting U_1 to this value, the simulator makes it "retroactively" consistent with having encrypted the true message value m in the previously released ciphertext C_1 using U_1 as a one-time-pad, despite the fact that C_1 was originally generated as a dummy value $C_1 = 0^n \oplus u_1$. At the end of this section (see Remark 8), we briefly discuss some informal intuition of some concepts captured by this simulator construction.

With the broad picture in mind, we now give the full description of the simulator's actions, with a schematic depiction in Figure 4. Furthermore, after each step in the description, we derive bounds on the distinguishability of the real and ideal functionalities up to that point.

- The simulator accepts the input states from the outer interface corresponding to Eve, and performs an internal simulated instance of Π^{A} from the ECD protocol (producing a value

[16] For the purpose of the distinguishability argument, the value supplied here is chosen by the distinguisher; our full security analysis below will cover any possible such choice when trying to distinguish $\Pi^{\mathrm{A}}\mathcal{F}_{\mathrm{BE}}^{\mathrm{real}}$ and $\mathcal{F}_{\mathrm{BE}}^{\mathrm{ideal}}\Sigma^{\mathrm{BE}}$.

[17] Note that the simulator is not constrained to use the actual resources of the ECD protocol. In particular, it does not have to use a temporarily private randomness source, which is why in some of the cases we describe, the value of R the simulator reveals at the outer interface does not describe the randomness used by the simulated Π^{A}.

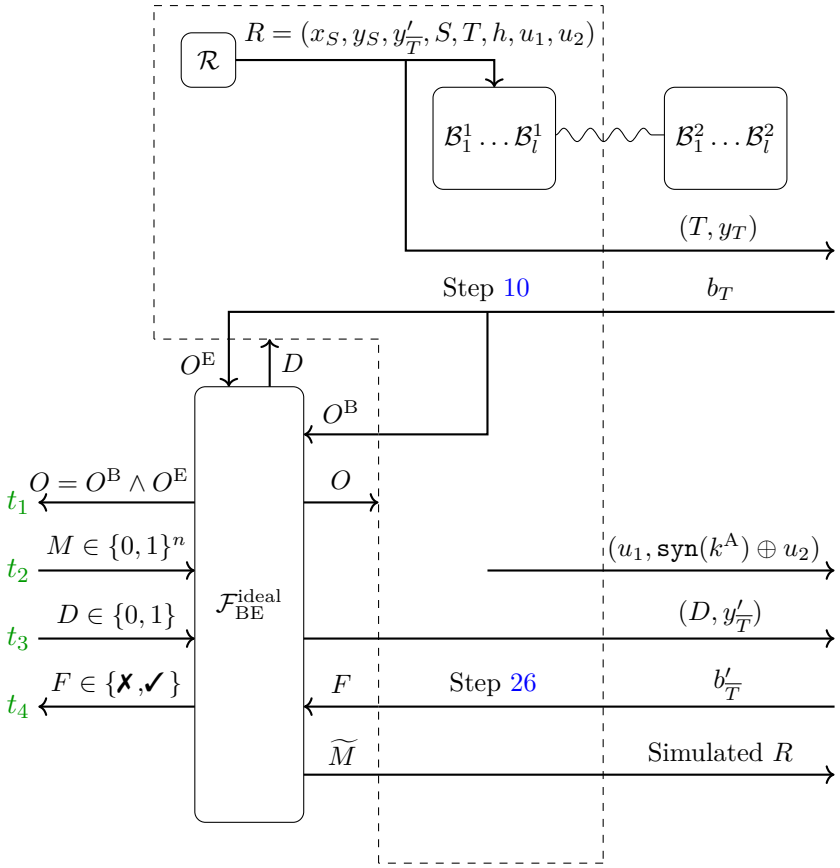


Figure 4: Schematic for the case of dishonest Bob and Eve, in which we require a simulator Σ^{BE} (depicted as the dashed region; refer to the main text for more description of the simulator's actions) acting on the ideal functionality $\mathcal{F}^{\mathrm{ideal}}_{\mathrm{BE}}$. As before in the honest functionality, the F input and output is provided only if $D = 1$, and the simulator only sends $y'_{\overline{T}}$ if $D = 1$ as well. The version of R the simulator releases has U_1 set to $\widetilde{m} \oplus h(k^{\mathrm{A}}) \oplus u_1$.

(T, y_T) which it outputs at the outer interfaces for Bob and/or Eve, and accepting a value b_T supplied at the outer interface for Bob, which it uses in its simulated instance of Π^{A}), until step 10. The inner interface of the simulator then feeds the output O of that step as the values O^{B} and O^{E} to the ideal functionality, which releases the same value O to the distinguisher (and also the simulator, though the simulator does not need it).

$\Pi^{\mathrm{A}}\mathcal{F}^{\mathrm{real}}_{\mathrm{BE}}$ and $\mathcal{F}^{\mathrm{ideal}}_{\mathrm{BE}}\Sigma^{\mathrm{BE}}$ are perfectly indistinguishable throughout this process, since no message value has been chosen yet, and hence the states produced by $\Pi^{\mathrm{A}}\mathcal{F}^{\mathrm{real}}_{\mathrm{BE}}$ and $\mathcal{F}^{\mathrm{ideal}}_{\mathrm{BE}}\Sigma^{\mathrm{BE}}$ are identical.

- If $O = \perp$, the simulator stops here, apart from releasing its register R at the end. Otherwise, it continues on with its simulated instance of Π^{A} from the ECD protocol, except that at the step where C_1 is to be generated, it instead prepares C_1 by generating an independent and uniformly random u_1 and setting $C_1 = u_1$. Furthermore, the simulator does not initialize a register U_1 yet — this is valid because after generating C_1, the register U_1 is not needed at any point in the ECD protocol until the last step. The simulator then proceeds until it receives D from the ideal functionality at the inner interface.

By Fact 23, it is easily seen that the states produced by $\Pi^{\mathrm{A}}\mathcal{F}_{\mathrm{BE}}^{\mathrm{real}}$ and $\mathcal{F}_{\mathrm{BE}}^{\mathrm{ideal}}\Sigma^{\mathrm{BE}}$ remain perfectly indistinguishable throughout these steps: we can equivalently consider the virtual process where $\Pi^{\mathrm{A}}\mathcal{F}_{\mathrm{BE}}^{\mathrm{real}}$ initializes the register C_1 with the independent uniform value u_1, exactly as $\mathcal{F}_{\mathrm{BE}}^{\mathrm{ideal}}\Sigma^{\mathrm{BE}}$ did. (The distinguisher does not yet have access to U_1, the only register which differs between $\Pi^{\mathrm{A}}\mathcal{F}_{\mathrm{BE}}^{\mathrm{real}}$ and $\mathcal{F}_{\mathrm{BE}}^{\mathrm{ideal}}\Sigma^{\mathrm{BE}}$ under this virtual process.)

- If $D = 0$, the simulator receives the message m at the inner interface and sets $U_1 = m \oplus h(k^{\mathrm{A}}) \oplus u_1$, then it outputs the register R at the outer interfaces.

  Through this process, the distinguisher only receives D followed by R. Since it already knows D, the former is trivial, and we only need to bound the distinguishability after receiving R. At this point, the state produced by $\Pi^{\mathrm{A}}\mathcal{F}_{\mathrm{BE}}^{\mathrm{real}}$ is such that U_1 was initialized with the independent uniform value u_1, and C_1 with the value $m \oplus h(k^{\mathrm{A}}) \oplus u_1$. In comparison, the state produced by $\mathcal{F}_{\mathrm{BE}}^{\mathrm{ideal}}\Sigma^{\mathrm{BE}}$ is such that C_1 was initialized with the independent uniform value u_1 and U_1 was initialized with the value $m \oplus h(k^{\mathrm{A}}) \oplus u_1$. Applying Fact 23, the situations for $\Pi^{\mathrm{A}}\mathcal{F}_{\mathrm{BE}}^{\mathrm{real}}$ and $\mathcal{F}_{\mathrm{BE}}^{\mathrm{ideal}}\Sigma^{\mathrm{BE}}$ are hence exactly equivalent.

- If $D = 1$, the simulator releases $y'_{\overline{T}}$ at the outer interfaces, then receives an input $b'_{\overline{T}}$. Using this value, it runs step 26, and feeds the output F of that step to the ideal functionality. Depending on the value of F, it performs one of the following actions:
  - If $F =$ ✗, the simulator does the same as in the $D = 0$ case: it receives the message m at the inner interface and sets $U_1 = m \oplus h(k^{\mathrm{A}}) \oplus u_1$, then it outputs the register R at the outer interfaces.
  - If $F =$ ✓, the simulator sets $U_1 = 0^n \oplus h(k^{\mathrm{A}}) \oplus u_1$, then it outputs the register R at the outer interfaces.

  Through this process, the distinguisher receives $(D, y'_{\overline{T}})$, supplies an input $b'_{\overline{T}}$, then receives F followed by R. By Fact 23, it is again easily seen that the states produced by $\Pi^{\mathrm{A}}\mathcal{F}_{\mathrm{BE}}^{\mathrm{real}}$ and $\mathcal{F}_{\mathrm{BE}}^{\mathrm{ideal}}\Sigma^{\mathrm{BE}}$ remain perfectly indistinguishable up until R is released, because as long as the distinguisher does not have access to R (and hence U_1), we can consider the virtual process where both $\Pi^{\mathrm{A}}\mathcal{F}_{\mathrm{BE}}^{\mathrm{real}}$ and $\mathcal{F}_{\mathrm{BE}}^{\mathrm{ideal}}\Sigma^{\mathrm{BE}}$ initialized C_1 with the independent uniform value u_1.

  After R is released, we note that the conditional states for the $O = \perp$ component are perfectly indistinguishable, because in that component all the registers are independent of the message (possibly by being set to "blank" values). Also, the conditional states for $F =$ ✗ are perfectly indistinguishable, by the same argument as in the $D = 0$ case above. As for the conditional states for $F =$ ✓, the states produced by $\Pi^{\mathrm{A}}\mathcal{F}_{\mathrm{BE}}^{\mathrm{real}}$ and $\mathcal{F}_{\mathrm{BE}}^{\mathrm{ideal}}\Sigma^{\mathrm{BE}}$ are $\sigma_{CR\widetilde{B}B_T\widetilde{E}}(m, 1)$ and $\sigma_{CR\widetilde{B}B_T\widetilde{E}}(0^n, 1)$ respectively — the former holds by definition, while the latter can be understood by noting the simulator set the values $C_1 = u_1$ and $U_1 = 0^n \oplus h(k^{\mathrm{A}}) \oplus u_1$, but by Fact 23 the values on C_1 and U_1 can be swapped, which would then result in the state $\sigma_{CR\widetilde{B}B_T\widetilde{E}}(0^n, 1)$.

  Overall, the distinguisher's states produced by $\Pi^{\mathrm{A}}\mathcal{F}_{\mathrm{BE}}^{\mathrm{real}}$ and $\mathcal{F}_{\mathrm{BE}}^{\mathrm{ideal}}\Sigma^{\mathrm{BE}}$ at this point are respectively of the form

  $$(1 - p_\top) \left|\perp\right\rangle\!\left\langle\perp\right|_O \otimes \omega_{CR\widetilde{B}B_T\widetilde{E}}$$

$$+ p_{\top} |\top\rangle\langle\top|_O \otimes \Big((1 - p_{\checkmark|\top}) |\text{✗}\rangle\langle\text{✗}|_F \otimes \psi_{CR\widetilde{B}B_T\widetilde{E}} + p_{\checkmark|\top} |\checkmark\rangle\langle\checkmark|_F \otimes \sigma_{CR\widetilde{B}B_T\widetilde{E}}(m, 1) \Big),$$
$$(1 - p_{\top}) |\bot\rangle\langle\bot|_O \otimes \omega_{CR\widetilde{B}B_T\widetilde{E}}$$
$$+ p_{\top} |\top\rangle\langle\top|_O \otimes \Big((1 - p_{\checkmark|\top}) |\text{✗}\rangle\langle\text{✗}|_F \otimes \psi_{CR\widetilde{B}B_T\widetilde{E}} + p_{\checkmark|\top} |\checkmark\rangle\langle\checkmark|_F \otimes \sigma_{CR\widetilde{B}B_T\widetilde{E}}(0^n, 1) \Big),$$

where ω and ψ are appropriate conditional states for $O = \bot$ and $F = \text{✗}$ (as argued above, these states are the same in the two scenarios), and $p_{\checkmark|\top}$ is the same in both scenarios (by Lemma 24). The only components that differ in the two scenarios are the σ terms, hence by Lemma 27 we see that the ℓ_1 distance between the states is bounded by $2\lambda_{\mathrm{CI}}$.

Remark 8. *Informally, one piece of intuition captured by the above simulator construction is that we are showing there exists a process that can (given access to Bob and Eve's interfaces in* $\mathcal{F}_{\mathrm{BE}}^{\mathrm{ideal}}$*) closely reproduce the real behaviour* $\Pi^{\mathrm{A}}\mathcal{F}_{\mathrm{BE}}^{\mathrm{real}}$*, without having access to Alice's actual message* m *until/unless the ideal resource* $\mathcal{F}_{\mathrm{BE}}^{\mathrm{ideal}}$ *reveals it in the final steps. This in particular serves to formalize the notion that the real behaviour* $\Pi^{\mathrm{A}}\mathcal{F}_{\mathrm{BE}}^{\mathrm{real}}$ *does not "leak unwanted information about* m*" (though we highlight that as discussed in Section 2.1.3, satisfying the full Definition 1 condition automatically guards against a much broader class of possible "flaws"). This form of reasoning also lies behind other simulator-based arguments outside of Abstract Cryptography, for instance in the security analysis of protocols for zero-knowledge proofs.*

6.2 Dishonest Bob and honest Eve

Since Eve has no inputs to the protocol after the initial step, the argument for this case is essentially the same as the preceding section, just with $\widetilde{E}$ traced out.

6.3 Honest Bob and dishonest Eve

- The simulator accepts the input states from the outer interface corresponding to Eve, and performs internal simulated instances of Π^{A} and Π^{B} from the ECD protocol until step 10. The inner interface of the simulator then feeds the output O of that step as the value O^{E} to the ideal functionality, which releases the same value O to the distinguisher (and also the simulator, though the simulator does not need it).

  $\Pi^{\mathrm{AB}}\mathcal{F}_{\mathrm{E}}^{\mathrm{real}}$ and $\mathcal{F}_{\mathrm{E}}^{\mathrm{ideal}}\Sigma^{\mathrm{E}}$ are perfectly indistinguishable throughout this process, since no message value has been chosen yet, and hence the states produced by $\Pi^{\mathrm{AB}}\mathcal{F}_{\mathrm{E}}^{\mathrm{real}}$ and $\mathcal{F}_{\mathrm{E}}^{\mathrm{ideal}}\Sigma^{\mathrm{E}}$ are identical.

- If $O = \bot$, the simulator stops here, apart from releasing its register R at the end. Otherwise, it continues on with its simulated instance of Π^{A} from the ECD protocol, except that at the step where C_1 is to be generated, it instead prepares C_1 by generating an independent and uniformly random u_1 and setting $C_1 = u_1$. Furthermore, the simulator does not initialize a register U_1 yet. The simulator then proceeds until it receives D from the ideal functionality at the inner interface.

  By Fact 23, it is easily seen that the states produced by $\Pi^{\mathrm{AB}}\mathcal{F}_{\mathrm{E}}^{\mathrm{real}}$ and $\mathcal{F}_{\mathrm{E}}^{\mathrm{ideal}}\Sigma^{\mathrm{E}}$ remain perfectly indistinguishable throughout these steps: we can equivalently consider the virtual process where $\Pi^{\mathrm{AB}}\mathcal{F}_{\mathrm{E}}^{\mathrm{real}}$ initializes the register C_1 with the independent uniform

value u_1, exactly as $\mathcal{F}_{\mathrm{E}}^{\mathrm{ideal}}\Sigma^{\mathrm{E}}$ did. (The distinguisher does not yet have access to U_1, the only register which differs between $\Pi^{\mathrm{AB}}\mathcal{F}_{\mathrm{E}}^{\mathrm{real}}$ and $\mathcal{F}_{\mathrm{E}}^{\mathrm{ideal}}\Sigma^{\mathrm{E}}$ under this virtual process.)

- If $D = 0$, the simulator continues on with its simulated instances of Π^{A} and Π^{B} until those protocols are finished, upon which the simulator sets $U_1 = 0^n \oplus h(k^{\mathrm{A}}) \oplus u_1$ and releases R at the outer interface.

  Through this process, the distinguisher receives D followed by $R\widetilde{M}$. (There is no F output for $D = 0$.) The distinguisher supplies no inputs, so we can suppose without loss of generality that it applies no operations on its systems through this process, and we only need to bound the distinguishability after $R\widetilde{M}$ is released.

  We note that the conditional states for the $O = \perp$ component at this point are perfectly indistinguishable, because in that component all the registers are independent of the message (possibly by being set to "blank" values). For the $O = \top$ component, the conditional states produced by $\Pi^{\mathrm{AB}}\mathcal{F}_{\mathrm{E}}^{\mathrm{real}}$ and $\mathcal{F}_{\mathrm{E}}^{\mathrm{ideal}}\Sigma^{\mathrm{E}}$ are $\rho^1_{\widetilde{M}CRB_T\widetilde{E}}(m,0)$ and $\rho^1_{\widetilde{M}CRB_T\widetilde{E}}(0^n,0)$ respectively, where the latter can be understood by again using Fact 23 to swap the values on the C_1 and U_1 registers.

  Overall, the distance between the states from $\Pi^{\mathrm{AB}}\mathcal{F}_{\mathrm{E}}^{\mathrm{real}}$ and $\mathcal{F}_{\mathrm{E}}^{\mathrm{ideal}}\Sigma^{\mathrm{E}}$ at this point is

$$\begin{aligned}
&p_\top \left\| \rho^1_{\widetilde{M}CRB_T\widetilde{E}}(m,0) - |m\rangle\langle m|_{\widetilde{M}} \otimes \rho^1_{CRB_T\widetilde{E}}(0^n,0) \right\|_1 \\
\leq &p_\top \left\| \rho^1_{\widetilde{M}CRB_T\widetilde{E}}(m,0) - |m\rangle\langle m|_{\widetilde{M}} \otimes \rho^1_{CRB_T\widetilde{E}}(m,0) \right\|_1 \\
&\quad + p_\top \left\| |m\rangle\langle m|_{\widetilde{M}} \otimes \rho^1_{CRB_T\widetilde{E}}(m,0) - |m\rangle\langle m|_{\widetilde{M}} \otimes \rho^1_{CRB_T\widetilde{E}}(0^n,0) \right\|_1 .
\end{aligned}$$

  By Lemma 27, the second term is bounded by $2\lambda_{\mathrm{CI}}$. As for the first term, we have

$$\begin{aligned}
&p_\top \left\| \rho^1_{\widetilde{M}CRB_T\widetilde{E}}(m,0) - |m\rangle\langle m|_{\widetilde{M}} \otimes \rho^1_{CRB_T\widetilde{E}}(m,0) \right\|_1 \\
\leq &p_\top \sum_{\widetilde{m}} \Pr[\widetilde{M} = \widetilde{m} | O = \top] \left\| |\widetilde{m}\rangle\langle\widetilde{m}|_{\widetilde{M}} \otimes \rho^1_{CRB_T\widetilde{E}|\widetilde{M}=\widetilde{m}}(m,0) - |m\rangle\langle m|_{\widetilde{M}} \otimes \rho^1_{CRB_T\widetilde{E}|\widetilde{M}=\widetilde{m}}(m,0) \right\|_1 \\
\leq &p_\top \sum_{\widetilde{m}\neq m} 2 \Pr[\widetilde{M} = \widetilde{m} | O = \top] \leq 2\lambda_{\mathrm{EC}},
\end{aligned}$$

  applying Lemma 26 in the last line. Adding the two bounds, we arrive at a final bound of $2\lambda_{\mathrm{CI}} + 2\lambda_{\mathrm{EC}}$.

- If $D = 1$, the simulator continues on with its simulated instances of Π^{A} and Π^{B}: it releases $y'_{\overline{T}}$ and $b'_{\overline{T}}$, then sets $U_1 = 0^n \oplus h(k^{\mathrm{A}}) \oplus u_1$ and finally releases R at the outer interface.

  Through this process, the distinguisher receives $(D, y'_{\overline{T}})$ (at t_3), then $b'_{\overline{T}}$ followed by F (at t_4), and finally $R\widetilde{M}$ (at t_5). The distinguisher supplies no inputs, so we can suppose without loss of generality that it applies no operations on its systems through this process, and we only need to bound the distinguishability after $R\widetilde{M}$ is released. Also, D is trivial since the distinguisher chose it, and so is $\widetilde{M}$ since here it is always set to 0^n, so we shall ignore these registers.

We note that the conditional states for the $O = \perp$ component at this point are perfectly indistinguishable, because in that component all the registers are independent of the message (possibly by being set to "blank" values). Also, for the $F = \checkmark$ component the conditional states produced by $\Pi^{\mathrm{A}}\mathcal{F}_{\mathrm{BE}}^{\mathrm{real}}$ and $\mathcal{F}_{\mathrm{BE}}^{\mathrm{ideal}}\Sigma^{\mathrm{BE}}$ are $\sigma_{RCY'_{\overline{T}}B'_{\overline{T}}B_T\widetilde{E}}(m,1)$ and $\sigma_{RCY'_{\overline{T}}B'_{\overline{T}}B_T\widetilde{E}}(0^n,1)$ respectively, where the latter can be understood by again using Fact 23 to swap the values on the C_1 and U_1 registers.

Overall, the states produced by $\Pi^{\mathrm{AB}}\mathcal{F}_{\mathrm{E}}^{\mathrm{real}}$ and $\mathcal{F}_{\mathrm{E}}^{\mathrm{ideal}}\Sigma^{\mathrm{E}}$ at this point are respectively of the form

$$(1-p_\top)\,|\perp\rangle\langle\perp|_O \otimes \omega_{FRCY'_{\overline{T}}B'_{\overline{T}}B_T\widetilde{E}} + p_\top \rho^2_{FRCY'_{\overline{T}}B'_{\overline{T}}B_T\widetilde{E}}(m,1),$$
$$(1-p_\top)\,|\perp\rangle\langle\perp|_O \otimes \omega_{FRCY'_{\overline{T}}B'_{\overline{T}}B_T\widetilde{E}} + p_\top\,|\checkmark\rangle\langle\checkmark|_F \otimes \rho^2_{RCY'_{\overline{T}}B'_{\overline{T}}B_T\widetilde{E}}(0^n,1),$$

where ω is an appropriate conditional state (as argued above, it is the same in both scenarios), and

$$\begin{aligned}\rho^2_{FRCY'_{\overline{T}}B'_{\overline{T}}B_T\widetilde{E}}(m,1) &= (1-p_{\checkmark|\top})\,|\text{✗}\rangle\langle\text{✗}|_F \otimes \psi_{RCY'_{\overline{T}}B'_{\overline{T}}B_T\widetilde{E}}(m,1)\\ &\quad + p_{\checkmark|\top}\,|\checkmark\rangle\langle\checkmark|_F \otimes \sigma_{RCY'_{\overline{T}}B'_{\overline{T}}B_T\widetilde{E}}(m,1),\\ |\checkmark\rangle\langle\checkmark|_F \otimes \rho^2_{RCY'_{\overline{T}}B'_{\overline{T}}B_T\widetilde{E}}(0^n,1) &= |\checkmark\rangle\langle\checkmark|_F \otimes \Big((1-p_{\checkmark|\top})\psi_{RCY'_{\overline{T}}B'_{\overline{T}}B_T\widetilde{E}}(0^n,1)\\ &\quad + p_{\checkmark|\top}\sigma_{RCY'_{\overline{T}}B'_{\overline{T}}B_T\widetilde{E}}(0^n,1)\Big).\end{aligned}$$

where ψ are appropriate conditional states, and $p_{\checkmark|\top}$ is the same in both scenarios (by Lemma 24). The ℓ_1 distance between the two expressions is bounded by

$$2p_\top(1-p_{\checkmark|\top}) + p_\top p_{\checkmark|\top}\left\|\sigma_{RCY'_{\overline{T}}B'_{\overline{T}}B_T\widetilde{E}}(m,1) - \sigma_{RCY'_{\overline{T}}B'_{\overline{T}}B_T\widetilde{E}}(0^n,1)\right\|_1 \leq 2\lambda_{\mathrm{com}} + 2\lambda_{\mathrm{CI}},$$

where we have applied Lemmas 25 and 27 (for the latter we use the fact that $\widetilde{B}$ can contain a copy of $Y'_{\overline{T}}B'_{\overline{T}}$, and apply Fact 9).

6.4 Honest Bob and Eve

In this case there are no dishonest parties, so the simulator is trivial and our task is simply to bound the distinguishability between $\Pi^{\mathrm{ABE}}\mathcal{F}^{\mathrm{real}}$ and $\mathcal{F}^{\mathrm{ideal}}$.

- We first consider the situation up until D is supplied.

Through this process, the distinguisher releases O, then supplies M and D. When O is released, the states produced by $\Pi^{\mathrm{ABE}}\mathcal{F}^{\mathrm{real}}$ and $\mathcal{F}^{\mathrm{ideal}}$ are $(1-p_\top)\,|\perp\rangle\langle\perp|_O + p_\top\,|\top\rangle\langle\top|_O$ and $|\top\rangle\langle\top|_O$ respectively, where $p_\top$ is computed with respect to the honest behaviour in the ECD protocol. Then Lemma 25 implies the ℓ_1 distance between them is bounded by

$$2(1-p_\top) \leq 2\lambda_{\mathrm{com}}.$$

After that, $\Pi^{\mathrm{ABE}}\mathcal{F}^{\mathrm{real}}$ and $\mathcal{F}^{\mathrm{ideal}}$ do not release any outputs during the steps described here, hence the distance between the states cannot increase.

- If $D = 0$:

The distinguisher receives D followed by $\widetilde{M}$. (There is no F output for $D = 0$.) D is trivial since the distinguisher chose it, so we only need to bound the distinguishability after $\widetilde{M}$ is released. The states produced by $\Pi^{\mathrm{ABE}}\mathcal{F}^{\mathrm{real}}$ and $\mathcal{F}^{\mathrm{ideal}}$ at this point are respectively (filling in the register $\widetilde{M}$ with a "blank value" ϕ in the case where $O = \perp$ for $\Pi^{\mathrm{ABE}}\mathcal{F}^{\mathrm{real}}$):

$$(1-p_\top)\,|\perp\rangle\langle\perp|_O \otimes |\phi\rangle\langle\phi|_{\widetilde{M}} + p_\top\,|\top\rangle\langle\top|_O \otimes \sum_{\widetilde{m}} \Pr[\widetilde{M}=\widetilde{m}|O=\top]\,|\widetilde{m}\rangle\langle\widetilde{m}|_{\widetilde{M}},$$
$$|\top\rangle\langle\top|_O \otimes |m\rangle\langle m|_{\widetilde{M}},$$

and the ℓ_1 distance between them is upper bounded by

$$\begin{aligned}&2(1-p_\top) + p_\top \left\| |\top\rangle\langle\top|_O \otimes \sum_{\widetilde{m}} \Pr[\widetilde{M}=\widetilde{m}|O=\top]\,|\widetilde{m}\rangle\langle\widetilde{m}|_{\widetilde{M}} - |\top\rangle\langle\top|_O \otimes |m\rangle\langle m|_{\widetilde{M}} \right\|_1 \\ \leq &2(1-p_\top) + p_\top \sum_{\widetilde{m}\neq m} 2\Pr[\widetilde{M}=\widetilde{m}|O=\top] \leq 2\lambda_{\mathrm{com}} + 2\lambda_{\mathrm{EC}},\end{aligned}$$

applying Lemmas 25 and 26 in the last line.

- If $D = 1$:

The distinguisher receives D, followed by F and $\widetilde{M}$. D is trivial, and no inputs occur between F and $\widetilde{M}$, so we only need to bound the distinguishability after $\widetilde{M}$ is released. The states produced by $\Pi^{\mathrm{ABE}}\mathcal{F}^{\mathrm{real}}$ and $\mathcal{F}^{\mathrm{ideal}}$ at this point are respectively (filling in the registers $\widetilde{M}F$ with a "blank value" ϕ in the case where $O = \perp$ for $\Pi^{\mathrm{ABE}}\mathcal{F}^{\mathrm{real}}$):

$$(1-p_\top)\,|\perp\rangle\langle\perp|_O \otimes |\phi\rangle\langle\phi|_F \otimes |\phi\rangle\langle\phi|_{\widetilde{M}} + p_\top\,|\top\rangle\langle\top|_O \otimes \rho_F^2 \otimes |0^n\rangle\langle 0^n|_{\widetilde{M}},$$
$$|\top\rangle\langle\top|_O \otimes |\text{✓}\rangle\langle\text{✓}|_F \otimes |0^n\rangle\langle 0^n|_{\widetilde{M}},$$

where $\rho_F^2 = (1-p_{\text{✓}|\top})\,|\text{✗}\rangle\langle\text{✗}|_F + p_{\text{✓}|\top}\,|\text{✓}\rangle\langle\text{✓}|_F$. The ℓ_1 distance between them is upper bounded by

$$2(1-p_\top) + 2p_\top(1-p_{\text{✓}|\top}) \leq 4\lambda_{\mathrm{com}},$$

applying Lemma 25.

7 Parallel repetition theorems

7.1 Parallel repetition theorem for 2-round 2-player product-anchored game

Definition 3. *A 2-round 2-player non-local game is called a* product-anchored game *with* anchoring probability α *iff*

- *Alice and Bob get $(x, y) \in \mathcal{X} \times \mathcal{Y}$ from a product distribution as their first round inputs.*
- *Alice and Bob produce $(a, b) \in \mathcal{A} \times \mathcal{B}$ as their first round outputs.*
- *Bob gets $z = \perp$ with probability α and $z = (x, y')$ with probability $1 - \alpha$, as his second round input, such that the distribution of (x, y) conditioned on $z = \perp$ is the same as the marginal distribution of (x, y). (Alice has no input.)*
- *Bob produces b' as his second round output. (Alice has no output.)*
- *Alice and Bob win the game iff $\mathsf{V}(x, y, a, b)$ and $\mathsf{V}'(x, y, z, a, b, b')$ are both satisfied.*

Theorem 29. *Let G be a 2-round 2-player non-local product-anchored game satisfying the conditions above with parameter α. Then for $\delta > 0$ and $t = (\omega^*(G) + \eta)l$,*

$$\omega^*(G^l) = \left(1 - (1 - \omega^*(G))^3\right)^{\Omega\left(\frac{\alpha^2 l}{\log(|\mathcal{A}|\cdot|\mathcal{B}|\cdot|\mathcal{B}'|)}\right)}$$
$$\omega^*(G^{t/l}) = \left(1 - \eta^3\right)^{\Omega\left(\frac{\alpha^2 l}{\log(|\mathcal{A}|\cdot|\mathcal{B}|\cdot|\mathcal{B}'|)}\right)}.$$

We shall use the following results in order to prove the theorem.

Fact 30 ([Hol07])**.** *Let $\mathsf{P}_{TU_1\ldots U_l V} = \mathsf{P}_T \mathsf{P}_{U_1|T} \mathsf{P}_{U_2|T} \ldots \mathsf{P}_{U_l|T} \mathsf{P}_{V|TU_1\ldots U_l}$ be a probability distribution over $\mathcal{T} \times \mathcal{U}^l \times \mathcal{V}$, and let $\mathcal{E}$ be any event. Then,*

$$\sum_{i=1}^{l} \|\mathsf{P}_{TU_i V|\mathcal{E}} - \mathsf{P}_{TV|\mathcal{E}} \mathsf{P}_{U_i|T}\|_1 \leq \sqrt{l\left(\log(|\mathcal{V}|) + \log\left(\frac{1}{\Pr[\mathcal{E}]}\right)\right)}.$$

Fact 31 ([BVY15], Lemma 16)**.** *Suppose TVW are random variables such that for some w^*, we have $\mathsf{P}_{VW}(v, w^*) = \alpha \cdot \mathsf{P}_V(v)$ for all v. Then,*

$$\left\|\mathsf{P}_{TVW} - \mathsf{P}_{VW}\mathsf{P}_{T|V,w^*}\right\|_1 \leq \frac{2}{\alpha}\left\|\mathsf{P}_{TVW} - \mathsf{P}_{VW}\mathsf{P}_{T|V}\right\|_1.$$

Using the above fact, we prove the following lemma that we shall use later.

Lemma 32. *Suppose P_{ST} and $\mathsf{P}_{S'T'R'}$ are distributions such that for some t^*, we have for some t^*, $\mathsf{P}_{ST}(s, t^*) = \alpha \cdot \mathsf{P}_S(s)$ for all s. If $\|\mathsf{P}_{ST} - \mathsf{P}_{S'T'}\|_1 \leq \alpha$, then,*

(i) $\|\mathsf{P}_{S'R'|t^*} - \mathsf{P}_{S'R'}\|_1 \leq \frac{2}{\alpha}\|\mathsf{P}_{S'T'R'} - \mathsf{P}_{S'R'}\mathsf{P}_{T|S}\|_1 + \frac{5}{\alpha}\|\mathsf{P}_{S'T'} - \mathsf{P}_{ST}\|_1$;

(ii) $\left\|\mathsf{P}_{S'T'R'} - \mathsf{P}_{ST}\mathsf{P}_{R'|t^*}\right\|_1 \leq \frac{2}{\alpha}\left(\left\|\mathsf{P}_{S'T'R'} - \mathsf{P}_{T'R'}\mathsf{P}_{S|T}\right\|_1 + \left\|\mathsf{P}_{S'T'R'} - \mathsf{P}_{S'R'}\mathsf{P}_{T|S}\right\|_1\right) + \frac{7}{\alpha}\|\mathsf{P}_{S'T'} - \mathsf{P}_{ST}\|_1.$

Proof. Note that

$$\|\mathsf{P}_{S|t^*} - \mathsf{P}_{S'|t^*}\|_1 \leq \frac{2}{\alpha}\|\mathsf{P}_{S'T'} - \mathsf{P}_{ST}\|_1$$

by Fact 5. Let $\mathsf{P}_{STR''}$ denote the distribution $\mathsf{P}_{ST}\mathsf{P}_{R'|S'T'}$, i.e., $\mathsf{P}_{STR''}(s, t, r) = \mathsf{P}_{ST}(st)\mathsf{P}_{R'|S'=s,T'=t}(r)$.

$$\|\mathsf{P}_{S'R'} - \mathsf{P}_{SR''}\|_1 = \sum_{s,r}\left|\mathsf{P}_{S'}(s)\sum_t \mathsf{P}_{T'|s}(t)\mathsf{P}_{R'|st}(r) - \mathsf{P}_S(s)\sum_t \mathsf{P}_{T|s}(t)\mathsf{P}_{R'|st}(r)\right|$$

$$\leq \sum_{s,t,r} \left| \mathsf{P}_{S'}(s)\mathsf{P}_{T'|s}(t) - \mathsf{P}_{S}(s)\mathsf{P}_{T|s}(t) \right| \mathsf{P}_{R'|st}(r)$$
$$= \|\mathsf{P}_{S'T'} - \mathsf{P}_{ST}\|_1.$$

Similarly,

$$\begin{aligned}
\left\|\mathsf{P}_{SR''} - \mathsf{P}_{SR''|t^*}\right\|_1 &\leq \left\|\mathsf{P}_{ST}\mathsf{P}_{R'|S'T'} - \mathsf{P}_{ST}\mathsf{P}_{R'|S',t^*}\right\|_1 \\
&\leq \frac{2}{\alpha}\left\|\mathsf{P}_{ST}\mathsf{P}_{R'|S'T'} - \mathsf{P}_{ST}\mathsf{P}_{R'|S'}\right\|_1 \\
&\leq \frac{2}{\alpha}\left(\left\|\mathsf{P}_{ST}\mathsf{P}_{R'|S'T'} - \mathsf{P}_{T|S}\mathsf{P}_{S'R'}\right\|_1 + \|\mathsf{P}_{S'T'} - \mathsf{P}_{ST}\|_1\right)
\end{aligned}$$

where in the second inequality we have used Fact 31. Combining all this, and using Fact 5,

$$\begin{aligned}
\|\mathsf{P}_{S'R'|t^*} - \mathsf{P}_{S'R'}\|_1 &\leq \|\mathsf{P}_{S'R'|t^*} - \mathsf{P}_{SR''|t^*}\|_1 + \|\mathsf{P}_{SR''|t^*} - \mathsf{P}_{SR''}\|_1 + \|\mathsf{P}_{SR''} - \mathsf{P}_{S'R'}\|_1 \\
&\leq \frac{2}{\alpha}\|\mathsf{P}_{S'T'R'} - \mathsf{P}_{STR''}\|_1 + \frac{2}{\alpha}\left(\left\|\mathsf{P}_{ST}\mathsf{P}_{R'|S'T'} - \mathsf{P}_{T|S}\mathsf{P}_{S'R'}\right\|_1 + \|\mathsf{P}_{S'T'} - \mathsf{P}_{ST}\|_1\right) \\
&\quad + \|\mathsf{P}_{S'T'} - \mathsf{P}_{ST}\|_1 \\
&= \frac{2}{\alpha}\left\|(\mathsf{P}_{S'T'} - \mathsf{P}_{ST})\mathsf{P}_{R'|S'T'}\right\|_1 + \frac{2}{\alpha}\|\mathsf{P}_{S'T'R'} - \mathsf{P}_{S'R'}\mathsf{P}_{T|S}\|_1 + \frac{3}{\alpha}\|\mathsf{P}_{S'T'} - \mathsf{P}_{ST}\|_1 \\
&= \frac{2}{\alpha}\|\mathsf{P}_{S'T'} - \mathsf{P}_{ST}\|_1 + \frac{2}{\alpha}\|\mathsf{P}_{S'T'R'} - \mathsf{P}_{S'R'}\mathsf{P}_{T|S}\|_1 + \frac{3}{\alpha}\|\mathsf{P}_{S'T'} - \mathsf{P}_{ST}\|_1 \\
&= \frac{2}{\alpha}\|\mathsf{P}_{S'T'R'} - \mathsf{P}_{S'R'}\mathsf{P}_{T|S}\|_1 + \frac{5}{\alpha}\|\mathsf{P}_{S'T'} - \mathsf{P}_{ST}\|_1 .
\end{aligned}$$

This proves item (i).

We have $\mathsf{P}_{T'}(t^*) \geq \mathsf{P}_T(t^*) - \frac{1}{2}\|\mathsf{P}_{S'T'} - \mathsf{P}_{ST}\|_1 \geq \alpha/2$. Therefore we have,

$$\left\|\mathsf{P}_{S'T'R'} - \mathsf{P}_{S|T}\mathsf{P}_{T'R'}\right\|_1 \geq \mathsf{P}_{T'}(t^*)\left\|\mathsf{P}_{S'R'|t^*} - \mathsf{P}_{S|t^*}\mathsf{P}_{R'|t^*}\right\|_1 \geq \frac{\alpha}{2}\left\|\mathsf{P}_{S'R'|t^*} - \mathsf{P}_{S|t^*}\mathsf{P}_{R'|t^*}\right\|_1 .$$

Using this we get,

$$\begin{aligned}
\left\|\mathsf{P}_{S}\mathsf{P}_{R'|S',t^*} - \mathsf{P}_{S}\mathsf{P}_{R'|t^*}\right\|_1 &\leq \left\|\mathsf{P}_{S'R'|t^*} - \mathsf{P}_{S|t^*}\mathsf{P}_{R'|t^*}\right\|_1 + \left\|(\mathsf{P}_{S'|t^*} - \mathsf{P}_{S|t^*})\mathsf{P}_{R'|S',t^*}\right\|_1 \\
&\leq \frac{2}{\alpha}\left\|\mathsf{P}_{S'T'R'} - \mathsf{P}_{S|T}\mathsf{P}_{T'R'}\right\|_1 + \left\|\mathsf{P}_{S'|t^*} - \mathsf{P}_{S|t^*}\right\|_1 \\
&\leq \frac{2}{\alpha}\left\|\mathsf{P}_{S'T'R'} - \mathsf{P}_{S|T}\mathsf{P}_{T'R'}\right\|_1 + \frac{2}{\alpha}\|\mathsf{P}_{S'T'} - \mathsf{P}_{ST}\|_1 , \qquad (18)
\end{aligned}$$

where we have used Fact 5 in the last inequality.

Next, note that we can apply Fact 31 to get a bound

$$\left\|\mathsf{P}_{STR''} - \mathsf{P}_{ST}\mathsf{P}_{R''|S,t^*}\right\|_1 \leq \frac{2}{\alpha}\left\|\mathsf{P}_{STR''} - \mathsf{P}_{ST}\mathsf{P}_{R''|S}\right\|_1 ,$$

because the marginal distribution on the first two variables is P_{ST} in both terms, which satisfies $\mathsf{P}_{ST}(s,t^*) = \mathsf{P}_T(t^*)\mathsf{P}_S(s) = \alpha\cdot\mathsf{P}_S(s)$ for all s. But since by definition we have $\mathsf{P}_{STR''} = \mathsf{P}_{ST}\mathsf{P}_{R'|S'T'}$, we can rewrite the bound as follows:

$$\left\|\mathsf{P}_{ST}\mathsf{P}_{R'|S'T'} - \mathsf{P}_{ST}\mathsf{P}_{R'|S',t^*}\right\|_1 \leq \frac{2}{\alpha}\left\|\mathsf{P}_{ST}\mathsf{P}_{R'|S'T'} - \mathsf{P}_{ST}\mathsf{P}_{R'|S'}\right\|_1 .$$

Using this we get,

$$\begin{aligned}
\left\|\mathsf{P}_{S'T'R'} - \mathsf{P}_{ST}\mathsf{P}_{R'|S',t^*}\right\|_1 &\leq \left\|\mathsf{P}_{ST}\mathsf{P}_{R'|S'T'} - \mathsf{P}_{ST}\mathsf{P}_{R'|S',t^*}\right\|_1 + \left\|\mathsf{P}_{S'T'R'} - \mathsf{P}_{ST}\mathsf{P}_{R'|S'T'}\right\|_1 \\
&\leq \frac{2}{\alpha}\left\|\mathsf{P}_{ST}\mathsf{P}_{R'|S'T'} - \mathsf{P}_{ST}\mathsf{P}_{R'|S'}\right\|_1 + \left\|\mathsf{P}_{S'T'} - \mathsf{P}_{ST}\right\|_1 \\
&\leq \frac{2}{\alpha}\Big(\left\|\mathsf{P}_{S'T'R'} - \mathsf{P}_{S'R'}\mathsf{P}_{T|S}\right\|_1 + \left\|\mathsf{P}_{ST} - \mathsf{P}_{S'T'}\right\|_1 + \left\|\mathsf{P}_{S'} - \mathsf{P}_{S}\right\|_1\Big) \\
&\quad + \left\|\mathsf{P}_{S'T'} - \mathsf{P}_{ST}\right\|_1 \\
&\leq \frac{2}{\alpha}\left\|\mathsf{P}_{S'T'R'} - \mathsf{P}_{S'R'}\mathsf{P}_{T|S}\right\|_1 + \frac{5}{\alpha}\left\|\mathsf{P}_{S'T'} - \mathsf{P}_{ST}\right\|_1. \qquad (19)
\end{aligned}$$

Therefore, using (18) and (19),

$$\begin{aligned}
\left\|\mathsf{P}_{S'T'R'} - \mathsf{P}_{ST}\mathsf{P}_{R'|t^*}\right\|_1 &\leq \left\|\mathsf{P}_{S'T'R'} - \mathsf{P}_{ST}\mathsf{P}_{R'|S',t^*}\right\|_1 + \left\|\mathsf{P}_{S}\mathsf{P}_{R'|S',t^*} - \mathsf{P}_{S}\mathsf{P}_{R'|t^*}\right\|_1 \\
&\leq \frac{2}{\alpha}\Big(\left\|\mathsf{P}_{S'T'R'} - \mathsf{P}_{T'R'}\mathsf{P}_{S|T}\right\|_1 + \left\|\mathsf{P}_{S'T'R'} - \mathsf{P}_{S'R'}\mathsf{P}_{T|S}\right\|_1\Big) \\
&\quad + \frac{7}{\alpha}\left\|\mathsf{P}_{S'T'} - \mathsf{P}_{ST}\right\|_1.
\end{aligned}$$

This proves item (ii). □

Finally, we shall use the following two facts.

Fact 33 ([JPY14], Lemma III.1)**.** *Suppose ρ and σ are CQ states satisfying $\rho = \delta\sigma + (1-\delta)\sigma'$ for some other state σ'. Suppose Z is a classical register of size $|\mathcal{Z}|$ in ρ and σ such that the distribution on Z in σ is P_Z, then*

$$\mathop{\mathbb{E}}_{\mathsf{P}_Z} \mathsf{D}(\sigma_z\|\rho) \leq \log(1/\delta) + \log|\mathcal{Z}|.$$

Fact 34 (Quantum Raz's Lemma, [BVY15])**.** *Let ρ_{XY} and σ_{XY} be two CQ states with $X = X_1 \dots X_l$ being classical, and σ being product across all registers. Then,*

$$\sum_{i=1}^{l} \mathsf{I}(X_i : Y)_\rho \leq \mathsf{D}(\rho_{XY}\|\sigma_{XY}).$$

Proof of Theorem 29. Consider a strategy $\mathcal{S}$ for l copies of G (it may correspond to G^l or $G^{t/l}$ — it doesn't really matter): before the game starts, Alice and Bob share an entangled state on registers $A\widetilde{A}B\widetilde{B}B'\widetilde{B}'E^{\mathrm{A}}E^{\mathrm{B}}$. Here A, B, B' will be the registers in which the outputs are measured in the computational basis, and $\widetilde{A}, \widetilde{B}, \widetilde{B}'$ are registers onto which the contents of A, B, B' are copied — we can always assume the outputs are copied since they are classical. Alice and Bob apply unitaries based on their first round inputs XY to their respective halves of this entangled state and measure in the computational basis to obtain their first round outputs. We define the following pure state to represent the inputs, outputs and other registers in the protocol at this stage:

$$\begin{aligned}
&|\rho\rangle_{X\widetilde{X}Y\widetilde{Y}Z\widetilde{Z}A\widetilde{A}B\widetilde{B}B'\widetilde{B}'E^{\mathrm{A}}E^{\mathrm{B}}} \\
&= \sum_{x,y,z} \sqrt{\mathsf{P}_{XYZ}(x,y,z)}\,|xx\rangle_{X\widetilde{X}}\,|yy\rangle_{Y\widetilde{Y}}\,|zz\rangle_{Z\widetilde{Z}} \sum_{a,b} \sqrt{\mathsf{P}_{AB|xy}(ab)}\,|aa\rangle_{A\widetilde{A}}\,|bb\rangle_{B\widetilde{B}}\,|\rho\rangle_{B'\widetilde{B}'E^{\mathrm{A}}E^{\mathrm{B}}|xyab}
\end{aligned}$$

where we have used Z to denote Bob's second round input, which is either $\perp$ or (x, y'). We have included the $Z\widetilde{Z}$ registers in this state even though Bob has not received the z input yet; the state

in the entangled registers has no dependence on z however. Here $\mathsf{P}_{AB|xy}(a,b)$ is the probability of Alice and Bob obtaining outputs (a,b) on inputs (x,y) in the first round.

In the actual protocol, the AB registers are measured on $|\rho\rangle$, and the subsequent unitary Bob applies on the $B'\widetilde{B}'E^{\mathrm{B}}$ registers can depend on his first round output, as well as both his inputs. We represent the state of the protocol at this state by:

$$\begin{aligned}&|\sigma\rangle_{X\widetilde{X}Y\widetilde{Y}Z\widetilde{Z}A\widetilde{A}B\widetilde{B}B'\widetilde{B}'E^{\mathrm{A}}E^{\mathrm{B}}}\\ =&\sum_{x,y,z}\sqrt{\mathsf{P}_{XYZ}(x,y,z)}\,|xx\rangle_{X\widetilde{X}}\,|yy\rangle_{Y\widetilde{Y}}\,|zz\rangle_{Z\widetilde{Z}}\sum_{a,b}\sqrt{\mathsf{P}_{AB|xy}(ab)}\,|aa\rangle_{A\widetilde{A}}\,|bb\rangle_{B\widetilde{B}}\otimes\\ &\sum_{b'}\sqrt{\mathsf{P}_{B'|xyzab}(b')}\,|b'b'\rangle_{B'\widetilde{B}'}\,|\sigma\rangle_{E^{\mathrm{A}}E^{\mathrm{B}}|xyzabb'}\,.\end{aligned}$$

Note that $|\sigma\rangle$ is related to $|\rho\rangle$ by a unitary on the $B'\widetilde{B}'E^{\mathrm{B}}$ registers that is controlled on the registers YZB, which is why the marginal distribution of AB is the same in $|\rho\rangle$ and $|\sigma\rangle$. Note that even though no operations explicitly dependent on x are done in the second round, the distribution of B' obtained in σ depends on x, because the state $|\rho\rangle_{B'\widetilde{B}'E^{\mathrm{A}}E^{\mathrm{B}}|xyab}$ depended on x.

Let $\omega^*(G)=1-\varepsilon$. To prove the theorem, we shall use the following lemma (whose proof is given later).

Lemma 35. *For $i\in[l]$, let $T_i=\mathsf{V}(A_iB_i,X_iY_i)\wedge\mathsf{V}'(A_iB_iB_i',X_iY_iZ_i)$ in a strategy $\mathcal{S}$ for l copies of G (here X,Y are the first round inputs, A,B first round outputs, and V the first round predicate; Z is the second round input, B' the second round output, and V' the second round predicate). If $\mathcal{E}_C$ is the event $\prod_{i\in C}T_i=1$ for $C\subseteq[l]$, then*

$$\mathop{\mathbb{E}}_{i\in\overline{C}}\Pr[T_i=1|\mathcal{E}_C]\leq 1-\varepsilon+\frac{191\sqrt{\delta_C}}{\alpha}$$

where

$$\delta_C=\frac{|C|\cdot\log(|\mathcal{A}|\cdot|\mathcal{B}|\cdot|\mathcal{B}'|)+\log(1/\Pr[\mathcal{E}_C])}{l}.$$

The theorem follows from the above lemma using standard arguments as in e.g. [Rao08] — we shall reproduce here the proof given in that work, with some additional elaborations. We only need to prove the upper bound on $\omega^*(G^{t/l})$; the one for $\omega^*(G^l)$ then follows immediately by setting $\eta=1-\omega^*(G^l)$.

Consider any strategy for playing l parallel instances of G. We begin by proving the following claim: for any $\gamma\in(0,1)$, if we set n to be a value satisfying

$$2^{-\gamma^2 l+n\cdot\log(|\mathcal{A}|\cdot|\mathcal{B}|\cdot|\mathcal{B}'|)}=\left(1-\varepsilon+\frac{191\gamma}{\alpha}\right)^n \tag{20}$$

and pick a uniformly random subset $C\subseteq[l]$ of size n, the expected probability of winning all the instances on the chosen subset satisfies

$$\mathop{\mathbb{E}}_{C}\Pr[\mathcal{E}_C]=\sum_{C\subseteq[l]:|C|=n}\frac{1}{\binom{l}{n}}\Pr[\mathcal{E}_C]\leq 2\left(1-\varepsilon+\frac{191\gamma}{\alpha}\right)^n. \tag{21}$$

Note that there is indeed a (unique) value of n satisfying the required condition, specifically

$$n=\frac{\gamma^2 l}{\log\left(\frac{|\mathcal{A}|\cdot|\mathcal{B}|\cdot|\mathcal{B}'|}{1-\varepsilon+\frac{191\gamma}{\alpha}}\right)}.$$

To prove this claim, let $\mathbf{I}_1, \mathbf{I}_2, \ldots \mathbf{I}_n$ be a sequence of random variables obtained by drawing elements from $[l]$ uniformly at random without replacement (in this argument, random variables will be denoted in bold, while specific values they can take will be denoted without bolding). For each $j \in [n]$, we define a random variable $\mathbf{C}_j = (\mathbf{I}_1, \mathbf{I}_2, \ldots \mathbf{I}_j)$, i.e. its value is the tuple formed by the first j elements of the sequence. In a minor abuse of terminology, we will sometimes call the tuple $\mathbf{C}_j$ a subset of $[l]$, and we define $\mathcal{W}_j$ to be the event that all instances in $\mathbf{C}_j$ are won. With this interpretation, observe that $\mathbf{C}_n$ is a uniformly random subset of size n, and hence our goal is just to prove a bound on $\Pr[\mathcal{W}_n]$ (since this would be equal to $\mathbb{E}_C \Pr[\mathcal{E}_C]$ in (21)). Next, for each $j \in [n]$ we define $\mathcal{L}_j$ to be an event on $\mathbf{C}_j$, as follows: it is the event that $\mathbf{C}_j$ takes a value C_j such that $\Pr[\mathcal{E}_{C_j}] \leq (1 - \varepsilon + 191\gamma/\alpha)^n$, i.e. the probability of winning all games on that particular subset C_j is "low".[18] Also, let $\mathcal{H}_j$ be the complementary event that $\mathbf{C}_j$ takes a value C_j such that $\Pr[\mathcal{E}_{C_j}] > (1 - \varepsilon + 191\gamma/\alpha)^n$, i.e. the winning probability is "high".

With these events, we can write $\Pr[\mathcal{W}_n] = \Pr[\mathcal{W}_n \wedge \mathcal{L}_n] + \Pr[\mathcal{W}_n \wedge \mathcal{H}_n]$ and bound the individual terms. The first term is simply upper bounded by $(1 - \varepsilon + 191\gamma/\alpha)^n$ due to the definition of $\mathcal{L}_n$. To bound the second term, we argue as follows for each $j \in [n]$. Observe that if we consider any fixed value C_j for the random variable $\mathbf{C}_j$, this also fixes a value C_{j-1} for the "preceding" tuple $\mathbf{C}_{j-1}$, and furthermore, winning all instances of the game on C_j implies winning all instances on C_{j-1}. With this, the event $\mathcal{W}_j$ always implies the event $\mathcal{W}_{j-1}$, and so we can write $\mathcal{W}_j = \mathcal{W}_j \wedge \mathcal{W}_{j-1}$. It also tells us that for each value C_j we have $\Pr[\mathcal{E}_{C_j}] \leq \Pr[\mathcal{E}_{C_{j-1}}]$, from which we see that the event $\mathcal{H}_j$ always implies the event $\mathcal{H}_{j-1}$, and we can write $\mathcal{H}_j = \mathcal{H}_j \wedge \mathcal{H}_{j-1}$. Hence for each $j \in [n]$ we have

$$\Pr[\mathcal{W}_j \wedge \mathcal{H}_j] = \Pr[\mathcal{W}_j \wedge \mathcal{W}_{j-1} \wedge \mathcal{H}_j \wedge \mathcal{H}_{j-1}] = \Pr[\mathcal{W}_j \wedge \mathcal{H}_j | \mathcal{W}_{j-1} \wedge \mathcal{H}_{j-1}] \Pr[\mathcal{W}_{j-1} \wedge \mathcal{H}_{j-1}],$$

where for ease of notation we introduce trivial "always-true" events $\mathcal{W}_0$ and $\mathcal{H}_0$. Applying this relation repeatedly, we arrive at

$$\Pr[\mathcal{W}_n \wedge \mathcal{H}_n] = \prod_{j=1}^{n} \Pr[\mathcal{W}_j \wedge \mathcal{H}_j | \mathcal{W}_{j-1} \wedge \mathcal{H}_{j-1}] \Pr[\mathcal{W}_{j-1} \wedge \mathcal{H}_{j-1}].$$

Hence it suffices to bound $\Pr[\mathcal{W}_j \wedge \mathcal{H}_j | \mathcal{W}_{j-1} \wedge \mathcal{H}_{j-1}]$ for each j, which we shall do by upper bounding it with $\Pr[\mathcal{W}_j | \mathcal{W}_{j-1} \wedge \mathcal{H}_{j-1}]$ and applying Lemma 35. In more detail: note that conditioned on $\mathcal{H}_{j-1}$, by definition $\mathbf{C}_{j-1}$ takes a value C_{j-1} satisfying $\Pr[\mathcal{E}_{C_{j-1}}] > (1 - \varepsilon + 191\gamma/\alpha)^n$, and this is the same as $\log(1/\Pr[\mathcal{E}_{C_{j-1}}]) < \gamma^2 l - n \cdot \log(|\mathcal{A}| \cdot |\mathcal{B}| \cdot |\mathcal{B}'|)$ by the defining property (20) for n. Substituting this into the bound in Lemma 35 gives (since $|C_{j-1}| \leq n$)

$$1 - \varepsilon + \frac{191\sqrt{\delta_{C_{j-1}}}}{\alpha} \leq 1 - \varepsilon + \frac{191}{\alpha} \sqrt{\frac{n \log(|\mathcal{A}| \cdot |\mathcal{B}| \cdot |\mathcal{B}'|) + \log(1/\Pr[\mathcal{E}_{C_{j-1}}])}{l}} \leq 1 - \varepsilon + \frac{191\gamma}{\alpha}.$$

With this, we can apply Lemma 35 to write $\Pr[\mathcal{W}_j | \mathcal{W}_{j-1} \wedge \mathcal{H}_{j-1}] \leq 1 - \varepsilon + 191\gamma/\alpha$ (recalling that $\mathbf{C}_j$ can be viewed as being generated from $\mathbf{C}_{j-1}$ by drawing a uniformly random $i \notin \mathbf{C}_{j-1}$ and appending it). Since this bound holds for every $j \in [n]$, we get $\Pr[\mathcal{W}_n \wedge \mathcal{H}_n] \leq (1 - \varepsilon + 191\gamma/\alpha)^n$, which yields the claimed bound (21).

[18] A slightly different perspective that may help in understanding the definition of this event is that for each $j \in [n]$, we can define an indicator variable $\mathbf{V}_j^{\mathcal{L}}$ as follows: $\mathbf{V}_j^{\mathcal{L}}$ is a function of $\mathbf{C}_j$, taking value 1 if $\mathbf{C}_j$ takes a value C_j such that $\Pr[\mathcal{E}_{C_j}] \leq (1 - \varepsilon + 191\gamma/\alpha)^n$, and taking value 0 otherwise. (Note that this is a well-defined function of C_j because we have fixed a particular strategy for playing the game, and hence $\Pr[\mathcal{E}_{C_j}]$ is a function of C_j only.) The event $\mathcal{L}_j$ is then exactly the event $\mathbf{V}_j^{\mathcal{L}} = 1$.

Finally, to use this to prove the bound on $\omega^*(G^{t/l})$ for $t = (1-\varepsilon+\eta)l$, we set $\gamma = \frac{\alpha\eta}{764}$, which gives $n < (1-\varepsilon+\eta)l$. If $t = (1-\varepsilon+\eta)l$ games are won, we can pick a random subset of size n out of the $(1-\varepsilon+\eta)l$ won games, and say that the probability of winning $(1-\varepsilon+\eta)l$ games is upper bounded by the probability of winning on this random subset. Therefore we have,

$$\omega^*(G^{t/l}) \leq \sum_{C\subseteq[(1-\varepsilon+\eta)l]:|C|=n} \frac{1}{\binom{(1-\varepsilon+\eta)l}{n}} \Pr[\mathcal{E}_C] \leq 2\left(1-\varepsilon+\frac{\eta}{4}\right)^n \cdot \frac{\binom{l}{n}}{\binom{(1-\varepsilon+\eta)l}{n}}, \tag{22}$$

where the last inequality follows from the bound (21) (note that the binomial-coefficient terms are independent of the summations and could hence be factored out). We can simplify the second factor in the above expression as

$$\frac{\binom{l}{n}}{\binom{(1-\varepsilon+\eta)l}{n}} \leq \left(\frac{l}{(1-\varepsilon+\eta)l-n}\right)^n \leq \left(\frac{1}{1-\varepsilon+\frac{3\eta}{4}}\right)^n,$$

where in the last inequality we have used the expression for n. Putting this into (22) we get,

$$\omega^*(G^{t/l}) \leq 2\left(\frac{1-\varepsilon+\frac{\eta}{4}}{1-\varepsilon+\frac{3\eta}{4}}\right)^n = 2\left(1-\frac{\frac{\eta}{2}}{1-\varepsilon+\frac{3\eta}{4}}\right)^n \leq 2\left(1-\frac{\eta}{2}\right)^n,$$

which proves the theorem after substituting the value of n. □

To prove Lemma 35, we shall first define the correlation-breaking random variables D_iG_i for each $i \in [l]$ as follows: D_i is a uniformly random bit, and G_i takes value X_iY_i or Z_i respectively depending on whether D_i is 0 or 1. With this, XYZ are independent conditioned on DG: to see this, first note that the distribution on $XYZDG$ is independent across instances, so it suffices to prove that for each i, $X_iY_iZ_i$ are independent conditioned on D_iG_i. Observe that conditioned on $D_i = 0$, the value of X_iY_i is fixed by G_i, so X_iY_i are trivially independent conditioned on G_i. Whereas conditioned on $D_i = 1$, the value of Z_i is fixed by G_i, so it suffices to show that X_iY_i is independent conditioned on Z_i. This is indeed true because conditioned on $Z_i = \perp$, the distribution of X_iY_i is equal to their marginal distribution, which is product; whereas conditioned on any other value of Z_i, the value of X_i is fixed by Z_i, so X_i is trivially independent of Y_i.

Let $|\rho\rangle_{dg}$ and $|\sigma\rangle_{dg}$ denote the states $|\rho\rangle$ and $|\sigma\rangle$ conditioned on $DG = dg$, which simply means that the distribution of XYZ used is conditioned on dg.

Conditioned on $DG = dg$, we define the state $|\varphi\rangle_{dg}$, which is $|\sigma\rangle_{dg}$ conditioned on success in C, i.e., the event $\mathcal{E}_C$ as defined in Lemma 35:

$$\begin{aligned}
&|\varphi\rangle_{X\widetilde{X}Y\widetilde{Y}Z\widetilde{Z}A\widetilde{A}B\widetilde{B}B'\widetilde{B}'E^{\mathrm{A}}E^{\mathrm{B}}|dg} \\
=&\frac{1}{\sqrt{\gamma_{dg}}} \sum_{x,y,z} \sqrt{\mathsf{P}_{XYZ|dg}(xyz)}\, |xx\rangle_{X\widetilde{X}} |yy\rangle_{Y\widetilde{Y}} |zz\rangle_{Z\widetilde{Z}} \sum_{\substack{a,b,b':\\(x_C,y_C,z_C,a_C,b_C,b'_C)\\ \text{win } G^{|C|}}} \sqrt{\mathsf{P}_{ABB'|xyz}(ab)}\, |aa\rangle_{A\widetilde{A}} |bb\rangle_{B\widetilde{B}} \otimes \\
&|b'b'\rangle_{B'\widetilde{B}'} |\sigma\rangle_{E^{\mathrm{A}}E^{\mathrm{B}}|xyzabb'}
\end{aligned}$$

where γ_{dg} is the probability of winning in C conditioned on $DG = dg$, in $\mathcal{S}$; γ_{dg} averaged over dg is then $\Pr[\mathcal{E}_C]$. It is easy to see that $\mathsf{P}_{XYZABB'|\mathcal{E}_C,dg}$ is the distribution on the registers $XYZABB'$ in $|\varphi\rangle_{dg}$, and $\mathbb{E}_{\mathsf{P}_{DG|\mathcal{E}_C}} \mathsf{P}_{XYZABB'|\mathcal{E}_C,dg}$ is $\mathsf{P}_{XYZABB'|\mathcal{E}_C}$.

In the remainder of the proof, we shall use the following notation. For $i \in [l]$, we shall use $|\varphi\rangle_{x_i y_i z_i d_{-i} g_{-i}}$ (where d_{-i} stands for $d_1 \dots d_{i-1} d_{i+1} \dots d_l$ and g_{-i} is defined similarly), $|\varphi\rangle_{x_i d_{-i} g_{-i}}$, $|\varphi\rangle_{y_i d_{-i} g_{-i}}$, $|\varphi\rangle_{x_i y_i d_{-i} g_{-i}}$ to refer to $|\varphi\rangle$ with values of $X_i Y_i Z_i D_{-i} G_{-i}$, $X_i D_{-i} G_{-i}$, $Y_i D_{-i} G_{-i}$ and $X_i Y_i D_{-i} G_{-i}$ respectively conditioned on. We shall use similar notation for other variables and subsets of $[l]$ as well. $|\varphi\rangle_{\perp, d_{-i} g_{-i}}$ will be used to refer to $|\varphi\rangle$ conditioned on $Z_i = \perp, D_{-i} G_{-i} = d_{-i} g_{-i}$.

We shall use the following lemma, whose proof we give later, to prove Lemma 35. In the statement of this lemma, and in the proofs henceforth, we shall refer to δ_C and $\mathcal{E}_C$ as just δ and $\mathcal{E}$ for brevity.

Lemma 36. *Let δ be δ_C as defined in Lemma 35. If $\delta \leq \frac{\alpha^2}{8}$, then using $R_i = X_C Y_C Z_C A_C B_C B'_C D_{-i} G_{-i}$, the following conditions hold:*

(i) $\mathbb{E}_{i \in \overline{C}} \left\| \mathsf{P}_{X_i Y_i Z_i R_i | \mathcal{E}} - \mathsf{P}_{X_i Y_i Z_i} \mathsf{P}_{R_i | \mathcal{E}, \perp} \right\|_1 \leq \frac{11\sqrt{2\delta}}{\alpha}$;

(ii) For each i, there exist unitaries $\{U^i_{x_i r_i}\}_{x_i r_i}$ acting on $X_{\overline{C}} \widetilde{X}_{\overline{C}} E^{\mathrm{A}} A_{\overline{C}} \widetilde{A}_{\overline{C}}$, and $\{V^i_{y_i r_i}\}_{y_i r_i}$ acting on $Y_{\overline{C}} \widetilde{Y}_{\overline{C}} E^{\mathrm{B}} B_{\overline{C}} \widetilde{B}_{\overline{C}} B'_{\overline{C}} \widetilde{B}'_{\overline{C}}$ such that

$$\mathop{\mathbb{E}}_{i \in \overline{C}} \mathop{\mathbb{E}}_{\mathsf{P}_{X_i Y_i R_i | \mathcal{E}}} \left\| U^i_{x_i r_i} \otimes V^i_{y_i r_i} |\varphi\rangle\langle\varphi|_{\perp r_i} (U^i_{x_i r_i})^\dagger \otimes (V^i_{y_i r_i})^\dagger - |\varphi\rangle\langle\varphi|_{x_i y_i \perp r_i} \right\|_1 \leq \frac{58\sqrt{2\delta}}{\alpha};$$

(iii) $\mathbb{E}_{i \in \overline{C}} \left\| \mathsf{P}_{X_i Y_i Z_i R_i | \mathcal{E}} \left(\mathsf{P}_{A_i B_i | \mathcal{E}, X_i Y_i Z_i R_i} - \mathsf{P}_{A_i B_i | \mathcal{E}, X_i Y_i, \perp, R_i} \right) \right\|_1 \leq \frac{30\sqrt{2\delta}}{\alpha}$;

(iv) There exist unitaries $\{W^i_{y_i z_i r_i}\}_{y_i z_i r_i}$ acting on the registers $Y_{\overline{C}} \widetilde{Y}_{\overline{C}} Z_{\overline{C}} \widetilde{Z}_{\overline{C}} E^{\mathrm{B}} B'_{\overline{C}} \widetilde{B}'_{\overline{C}}$ such that

$$\mathop{\mathbb{E}}_{i \in \overline{C}} \mathop{\mathbb{E}}_{\mathsf{P}_{X_i Y_i Z_i A_i B_i R_i | \mathcal{E}}} \left\| \mathbb{1} \otimes W^i_{y_i z_i r_i} |\varphi\rangle\langle\varphi|_{x_i y_i \perp a_i b_i r_i} \mathbb{1} \otimes (W^i_{y_i z_i r_i})^\dagger - |\varphi\rangle\langle\varphi|_{x_i y_i z_i a_i b_i r_i} \right\|_1 \leq \frac{90\sqrt{2\delta}}{\alpha}.$$

Proof of Lemma 35. Note that if $\delta \geq \alpha^2/8$, the upper bound in Lemma 35 is trivial. So we shall only prove the lemma in the case that $\delta \leq \alpha^2/8$ using Lemma 36. Using Lemma 36, we give a strategy $\mathcal{S}'$ for a single copy of G as follows:

- Alice and Bob share $\log |\overline{C}|$ uniform bits, for each $i \in \overline{C}$, $\mathsf{P}_{R_i | \mathcal{E}, \perp}$ as randomness, and for each $R_i = r_i$, the state $|\varphi\rangle_{\perp r_i}$ as entanglement, with Alice holding registers $X_{\overline{C}} \widetilde{X}_{\overline{C}} E^{\mathrm{A}} A_{\overline{C}} \widetilde{A}_{\overline{C}}$ and Bob holding registers $Y_{\overline{C}} \widetilde{Y}_{\overline{C}} Z_{\overline{C}} \widetilde{Z}_{\overline{C}} E^{\mathrm{B}} B_{\overline{C}} \widetilde{B}_{\overline{C}} B'_{\overline{C}} \widetilde{B}'_{\overline{C}}$.
- Alice and Bob use their shared randomness to sample $i \in \overline{C}$ uniformly, and in the first round, apply $U^i_{x_i r_i}$, $V^i_{y_i r_i}$ on their parts of the shared entangled state according to their shared randomness from $\mathsf{P}_{R_i | \mathcal{E}, \perp}$ and their first round inputs.
- Alice and Bob measure the A_i, B_i registers of the resulting state to give their first round outputs.
- Bob applies $W^i_{y_i z_i r_i}$ to his half of the shared entangled state after the first round according to his second round input and the shared randomness.
- Bob measures the B'_i register of the resulting state to give his second round output.

We shall first do the analysis assuming Alice and Bob have the distribution $\mathsf{P}_{X_iY_iZ_iR_i|\mathcal{E}}$ exactly. Let $\mathsf{P}_{\widehat{A}_i\widehat{B}_i|X_iY_iZ_iR_i}$ denote the conditional distribution Alice and Bob get after the first round (note that $\widehat{A}_i\widehat{B}_i$ are actually independent of Z_i given X_iY_i, but we are still writing Z_i in the conditioning), and $\mathsf{P}_{\widehat{B}'_i|X_iY_iZ_iR_i\widehat{A}_i\widehat{B}_i}$ denote their conditional distribution after the second round. Since $\mathsf{P}_{\widehat{A}_i\widehat{B}_i|X_iY_iZ_iR_i}$ is obtained by measuring the A_iB_i registers of the state $U^i_{x_ir_i}\otimes V^i_{y_ir_i}|\varphi\rangle_{\perp r_i}$, and $\mathsf{P}_{A_iB_i|\mathcal{E},X_iY_i,\perp,R_i}$ is obtained by measuring the same registers of $|\varphi\rangle_{x_iy_i\perp r_i}$, from item (ii) of Lemma 36 and Fact 9 we have,

$$\mathop{\mathbb{E}}_{i\in\overline{C}}\left\|\mathsf{P}_{X_iY_iZ_iR_i|\mathcal{E}}\left(\mathsf{P}_{\widehat{A}_i\widehat{B}_i|X_iY_iZ_iR_i}-\mathsf{P}_{A_iB_i|\mathcal{E},X_iY_i,\perp,R_i}\right)\right\|_1\leq\frac{58\sqrt{2\delta}}{\alpha}.$$

Combining this with item (iii) of the lemma we have,

$$\mathop{\mathbb{E}}_{i\in\overline{C}}\left\|\mathsf{P}_{X_iY_iZ_iR_i|\mathcal{E}}\left(\mathsf{P}_{\widehat{A}_i\widehat{B}_i|X_iY_iZ_iR_i}-\mathsf{P}_{A_iB_i|\mathcal{E},X_iY_iZ_iR_i}\right)\right\|_1\leq\frac{58\sqrt{2\delta}}{\alpha}+\frac{30\sqrt{2\delta}}{\alpha}.$$

By similar reasoning, we have from item (iv),

$$\mathop{\mathbb{E}}_{i\in\overline{C}}\left\|\mathsf{P}_{X_iY_iZ_iR_iA_iB_i}\left(\mathsf{P}_{\widehat{B}'_i|X_iY_iZ_iR_i\widehat{A}_i\widehat{B}_i}-\mathsf{P}_{B'_i|\mathcal{E},X_iY_iZ_iR_iA_iB_i}\right)\right\|_1\leq\frac{90\sqrt{2\delta}}{\alpha}.$$

Combining these with item (i), then we overall have,

$$\mathop{\mathbb{E}}_{i\in\overline{C}}\left\|\mathsf{P}_{X_iY_iZ_i}\mathsf{P}_{R_i|\mathcal{E},\perp}\mathsf{P}_{\widehat{A}_i\widehat{B}_i\widehat{B}'_i|X_iY_iZ_iR_i}-\mathsf{P}_{X_iY_iZ_iR_iA_iB_iB'_i|\mathcal{E}}\right\|_1\leq\frac{11\sqrt{2\delta}}{\alpha}+\frac{58\sqrt{2\delta}}{\alpha}+\frac{120\sqrt{2\delta}}{\alpha}\leq\frac{382\sqrt{\delta}}{\alpha}.$$

Since $\Pr[T_i=1|\mathcal{E}]$ is the probability of that the distribution $\mathsf{P}_{X_iY_iZ_iR_iA_iB_iB'_i|\mathcal{E}}$ wins a single copy of the game, if $\mathbb{E}_{i\in\overline{C}}\Pr[T_i=1|\mathcal{E}]>1-\varepsilon+\frac{191\sqrt{\delta}}{\alpha}$, then the winning probability of our constructed strategy is more than

$$1-\varepsilon+\frac{191\sqrt{\delta}}{\alpha}-\frac{1}{2}\mathop{\mathbb{E}}_{i\in\overline{C}}\left\|\mathsf{P}_{X_iY_iZ_i}\mathsf{P}_{R_i|\mathcal{E},\perp}\mathsf{P}_{\widehat{A}_i\widehat{B}_i\widehat{B}'_i|X_iY_iZ_iR_i}-\mathsf{P}_{X_iY_iZ_iR_iA_iB_iB'_i|\mathcal{E}}\right\|_1\geq\omega^*(G),$$

which is a contradiction. Therefore we must have $\mathbb{E}_{i\in\overline{C}}\Pr[T_i=1|\mathcal{E}]\leq1-\varepsilon+\frac{191\sqrt{\delta}}{\alpha}$. □

Proof of Lemma 36. **Closeness of distributions.** Applying Fact 30 with T,V being trivial and $U_i=X_iY_iZ_i$ we get,

$$\mathop{\mathbb{E}}_{i\in\overline{C}}\|\mathsf{P}_{X_iY_iZ_i|\mathcal{E}}-\mathsf{P}_{X_iY_iZ_i}\|_1\leq\frac{1}{l-|C|}\sqrt{(l-|C|)\cdot\log(1/\Pr[\mathcal{E}])}\leq\sqrt{2\delta},\tag{23}$$

recalling we are taking δ to be the value δ_C defined in Lemma 35. In particular, the last line of the above equation is obtained by recalling that we have required $\delta\leq\alpha^2/8$, which implies $|C|\leq l/2$.

Also, applying Fact 30 again with U_i the same, $T=X_CY_CZ_CDG$ and $V=A_CB_CB'_C$, and using $R_i=X_CY_CZ_CA_CB_CB'_CD_{-i}G_{-i}$, we get

$$\begin{aligned}\sqrt{2\delta}&\geq\frac{1}{l-|C|}\sqrt{(l-|C|)(\log(1/\Pr[\mathcal{E}])+|C|\cdot\log(|\mathcal{A}|\cdot|\mathcal{B}|\cdot|\mathcal{B}'|)}\\&\geq\mathop{\mathbb{E}}_{i\in\overline{C}}\left\|\mathsf{P}_{X_iY_iZ_iX_CY_CZ_CDGA_CB_CB'_C|\mathcal{E}}-\mathsf{P}_{X_CY_CZ_CA_CB_CB'_CDG|\mathcal{E}}\mathsf{P}_{X_iY_iZ_i|X_CY_CZ_CDG}\right\|_1\end{aligned}$$

$$= \mathop{\mathbb{E}}_{i\in\overline{C}} \|\mathsf{P}_{X_iY_iZ_iD_iG_iR_i|\mathcal{E}} - \mathsf{P}_{D_iG_iR_i|\mathcal{E}}\mathsf{P}_{X_iY_iZ_i|D_iG_i}\|_1$$
$$= \frac{1}{2}\mathop{\mathbb{E}}_{i\in\overline{C}} \left(\|\mathsf{P}_{X_iY_iZ_iR_i|\mathcal{E}} - \mathsf{P}_{X_iY_iR_i|\mathcal{E}}\mathsf{P}_{Z_i|X_iY_i}\|_1 + \|\mathsf{P}_{X_iY_iZ_iR_i|\mathcal{E}} - \mathsf{P}_{Z_iR_i|\mathcal{E}}\mathsf{P}_{X_iY_i|Z_i}\|_1\right), \tag{24}$$

where the last line is obtained by conditioning on values $D_i = 0$ and $D_i = 1$.

Now, the bound (23) allows us to apply item (ii) of Lemma 32, with $X_iY_i = S$, $Z_i = T$, $R_i = R$, and the corresponding variables conditioned on $\mathcal{E}$ being the primed variables in the lemma statement. This gives

$$\mathop{\mathbb{E}}_{i\in\overline{C}} \left\|\mathsf{P}_{X_iY_iZ_iR_i|\mathcal{E}} - \mathsf{P}_{X_iY_iZ_i}\mathsf{P}_{R_i|\mathcal{E},\perp}\right\|_1 \leq \frac{2}{\alpha}\mathop{\mathbb{E}}_{i\in\overline{C}} (\|\mathsf{P}_{X_iY_iZ_iR_i|\mathcal{E}} - \mathsf{P}_{X_iY_iR_i|\mathcal{E}}\mathsf{P}_{Z_i|X_iY_i}\|_1$$
$$+ \|\mathsf{P}_{X_iY_iZ_iR_i|\mathcal{E}} - \mathsf{P}_{Z_iR_i|\mathcal{E}}\mathsf{P}_{X_iY_i|Z_i}\|_1) + \frac{7}{\alpha}\mathop{\mathbb{E}}_{i\in\overline{C}} \|\mathsf{P}_{X_iY_iZ_i|\mathcal{E}} - \mathsf{P}_{X_iY_iZ_i}\|_1.$$

Applying (23) and (24) to the terms on the right-hand side yields item (i) of the lemma.

Existence of unitaries $U^i_{x_ir_i}$ and $V^i_{y_ir_i}$. We first note

$$\mathop{\mathbb{E}}_{\mathsf{P}_{X_CY_CZ_CA_CB_CB'_CDG|\mathcal{E}}} \mathsf{D}\left(\varphi_{X_{\overline{C}}Y_{\overline{C}}\widetilde{Y}_{\overline{C}}Z_{\overline{C}}\widetilde{Z}_{\overline{C}}B_{\overline{C}}\widetilde{B}_{\overline{C}}B'_{\overline{C}}\widetilde{B}'_{\overline{C}}E^{\mathrm{B}}|x_Cy_Cz_Ca_Cb_Cb'_Cdg}\middle\|\sigma_{X_{\overline{C}}Y_{\overline{C}}\widetilde{Y}_{\overline{C}}Z_{\overline{C}}\widetilde{Z}_{\overline{C}}B_{\overline{C}}\widetilde{B}_{\overline{C}}B'_{\overline{C}}\widetilde{B}'_{\overline{C}}E^{\mathrm{B}}|x_Cy_Cz_Cdg}\right)$$
$$\leq \mathop{\mathbb{E}}_{\mathsf{P}_{A_CB_CB'_CDG|\mathcal{E}}} \mathsf{D}\left(\varphi_{XY\widetilde{Y}Z\widetilde{Z}B_{\overline{C}}\widetilde{B}_{\overline{C}}B'_{\overline{C}}\widetilde{B}'_{\overline{C}}E^{\mathrm{B}}|a_Cb_Cb'_Cdg}\middle\|\sigma_{XY\widetilde{Y}Z\widetilde{Z}B_{\overline{C}}\widetilde{B}_{\overline{C}}B'_{\overline{C}}\widetilde{B}'_{\overline{C}}E^{\mathrm{B}}|dg}\right)$$
$$\leq \mathop{\mathbb{E}}_{\mathsf{P}_{DG|\mathcal{E}}} (\log(1/\gamma_{dg}) + \log(|\mathcal{A}|^{|C|}\cdot|\mathcal{B}|^{|C|}\cdot|\mathcal{B}'|^{|C|}))$$
$$\leq \log\left(1/\mathop{\mathbb{E}}_{\mathsf{P}_{DG|\mathcal{E}}}\gamma_{dg}\right) + |C|\cdot\log(|\mathcal{A}|\cdot|\mathcal{B}|\cdot|\mathcal{B}'|)$$
$$= \log(1/\Pr[\mathcal{E}]) + |C|\cdot\log(|\mathcal{A}|\cdot|\mathcal{B}|\cdot|\mathcal{B}'|) = \delta l,$$

where the first inequality is from (7), and to get the second inequality we have used Fact 33 on the states φ_{dg} and σ_{dg} (with z being $a_Cb_Cb'_C$).

Note that $\sigma_{X_{\overline{C}}Y_{\overline{C}}\widetilde{Y}_{\overline{C}}Z_{\overline{C}}\widetilde{Z}_{\overline{C}}E^{\mathrm{B}}B_{\overline{C}}\widetilde{B}_{\overline{C}}B'_{\overline{C}}\widetilde{B}'_{\overline{C}}|x_Cy_Cz_Cdg}$ is product across $X_{\overline{C}}$ and the rest of the registers, since dg is being conditioned on. Hence using Quantum Raz's Lemma,

$$\begin{aligned}
\delta l &\geq \mathop{\mathbb{E}}_{\mathsf{P}_{X_CY_CZ_CA_CB_CB'_CDG|\mathcal{E}}} \mathsf{D}\left(\varphi_{X_{\overline{C}}Y_{\overline{C}}\widetilde{Y}_{\overline{C}}Z_{\overline{C}}\widetilde{Z}_{\overline{C}}B_{\overline{C}}\widetilde{B}_{\overline{C}}B'_{\overline{C}}\widetilde{B}'_{\overline{C}}E^{\mathrm{B}}|x_Cy_Cz_Ca_Cb_Cb'_Cdg}\middle\|\sigma_{X_{\overline{C}}Y_{\overline{C}}\widetilde{Y}_{\overline{C}}Z_{\overline{C}}\widetilde{Z}_{\overline{C}}B_{\overline{C}}\widetilde{B}_{\overline{C}}B'_{\overline{C}}\widetilde{B}'_{\overline{C}}E^{\mathrm{B}}|x_Cy_Cz_Cdg}\right)\\
&\geq \sum_{i\in\overline{C}} \mathsf{I}(X_i : Y_{\overline{C}}\widetilde{Y}_{\overline{C}}Z_{\overline{C}}\widetilde{Z}_{\overline{C}}B_{\overline{C}}\widetilde{B}_{\overline{C}}B'_{\overline{C}}\widetilde{B}'_{\overline{C}}E^{\mathrm{B}}|X_CY_CZ_CA_CB_CB'_CDG)_{\varphi}\\
&= \sum_{i\in\overline{C}} \mathsf{I}(X_i : Y_{\overline{C}}\widetilde{Y}_{\overline{C}}Z_{\overline{C}}\widetilde{Z}_{\overline{C}}B_{\overline{C}}\widetilde{B}_{\overline{C}}B'_{\overline{C}}\widetilde{B}'_{\overline{C}}E^{\mathrm{B}}|D_iG_iR_i)_{\varphi}\\
&= \sum_{i\in\overline{C}} \mathop{\mathbb{E}}_{\mathsf{P}_{D_iG_iR_i|\mathcal{E}}} \mathsf{I}(X_i : Y_{\overline{C}}\widetilde{Y}_{\overline{C}}Z_{\overline{C}}\widetilde{Z}_{\overline{C}}B_{\overline{C}}\widetilde{B}_{\overline{C}}B'_{\overline{C}}\widetilde{B}'_{\overline{C}}E^{\mathrm{B}})_{\varphi_{d_ig_ir_i}}\\
&\geq \frac{l}{2}\mathop{\mathbb{E}}_{i\in\overline{C}}\mathop{\mathbb{E}}_{\mathsf{P}_{D_iG_iR_i|\mathcal{E}}} \mathsf{I}(X_i : Y_{\overline{C}}\widetilde{Y}_{\overline{C}}Z_{\overline{C}}\widetilde{Z}_{\overline{C}}B_{\overline{C}}\widetilde{B}_{\overline{C}}B'_{\overline{C}}\widetilde{B}'_{\overline{C}}E^{\mathrm{B}})_{\varphi_{d_ig_ir_i}}\\
&\geq \frac{l}{2}\cdot\frac{1}{2}\mathop{\mathbb{E}}_{i\in\overline{C}}\mathop{\mathbb{E}}_{\mathsf{P}_{Z_iR_i|\mathcal{E}}} \mathsf{I}(X_i : Y_{\overline{C}}\widetilde{Y}_{\overline{C}}Z_{\overline{C}}\widetilde{Z}_{\overline{C}}B_{\overline{C}}\widetilde{B}_{\overline{C}}B'_{\overline{C}}\widetilde{B}'_{\overline{C}}E^{\mathrm{B}})_{\varphi_{g_ir_i|D_i=1}}
\end{aligned}$$

$$
\begin{aligned}
&= \frac{l}{2} \cdot \frac{1}{2} \mathop{\mathbb{E}}_{i\in\overline{C}} \mathsf{P}_{Z_iR_i|\mathcal{E}} \mathsf{I}(X_i : Y_{\overline{C}}\widetilde{Y}_{\overline{C}}Z_{\overline{C}}\widetilde{Z}_{\overline{C}}B_{\overline{C}}\widetilde{B}_{\overline{C}}B'_{\overline{C}}\widetilde{B}'_{\overline{C}}E^{\mathrm{B}})_{\varphi_{z_ir_i}} \\
&= \frac{l}{4} \mathop{\mathbb{E}}_{i\in\overline{C}} \mathsf{P}_{X_iZ_iR_i|\mathcal{E}} \mathsf{D}\left(\varphi_{Y_{\overline{C}}\widetilde{Y}_{\overline{C}}Z_{\overline{C}}\widetilde{Z}_{\overline{C}}E^{\mathrm{B}}B_{\overline{C}}\widetilde{B}_{\overline{C}}B'_{\overline{C}}\widetilde{B}'_{\overline{C}}|x_iz_ir_i} \middle\| \varphi_{Y_{\overline{C}}\widetilde{Y}_{\overline{C}}Z_{\overline{C}}\widetilde{Z}_{\overline{C}}E^{\mathrm{B}}B_{\overline{C}}\widetilde{B}_{\overline{C}}B'_{\overline{C}}\widetilde{B}'_{\overline{C}}|z_ir_i}\right) \\
&\geq \frac{l}{4} \mathop{\mathbb{E}}_{i\in\overline{C}} \mathsf{P}_{X_iZ_iR_i|\mathcal{E}} \mathsf{B}\left(\varphi_{Y_{\overline{C}}\widetilde{Y}_{\overline{C}}Z_{\overline{C}}\widetilde{Z}_{\overline{C}}E^{\mathrm{B}}B_{\overline{C}}\widetilde{B}_{\overline{C}}B'_{\overline{C}}\widetilde{B}'_{\overline{C}}|x_iz_ir_i}, \varphi_{Y_{\overline{C}}\widetilde{Y}_{\overline{C}}Z_{\overline{C}}\widetilde{Z}_{\overline{C}}E^{\mathrm{B}}B_{\overline{C}}\widetilde{B}_{\overline{C}}B'_{\overline{C}}\widetilde{B}'_{\overline{C}}|z_ir_i}\right)^2
\end{aligned}
$$

where we have used Pinsker's inequality in the final step. Using Jensen's inequality on the above we then have,

$$
2\sqrt{\delta} \geq \mathop{\mathbb{E}}_{i\in\overline{C}} \mathsf{P}_{X_iZ_iR_i|\mathcal{E}} \mathsf{B}\left(\varphi_{Y_{\overline{C}}\widetilde{Y}_{\overline{C}}Z_{\overline{C}}\widetilde{Z}_{\overline{C}}E^{\mathrm{B}}B_{\overline{C}}\widetilde{B}_{\overline{C}}B'_{\overline{C}}\widetilde{B}'_{\overline{C}}|x_iz_ir_i}, \varphi_{Y_{\overline{C}}\widetilde{Y}_{\overline{C}}Z_{\overline{C}}\widetilde{Z}_{\overline{C}}E^{\mathrm{B}}B_{\overline{C}}\widetilde{B}_{\overline{C}}B'_{\overline{C}}\widetilde{B}'_{\overline{C}}|z_ir_i}\right).
$$

Since $\mathsf{B}(\cdot,\cdot)$ always lies between 0 and 1, changing the distribution over which its expectation value is taken can only increase the expectation value by at most the ℓ_1-distance between the distributions. This lets us write

$$
\begin{aligned}
&\mathop{\mathbb{E}}_{i\in\overline{C}} \mathsf{P}_{Z_i} \mathsf{P}_{X_iR_i|\mathcal{E},Z_i} \mathsf{B}\left(\varphi_{Y_{\overline{C}}\widetilde{Y}_{\overline{C}}Z_{\overline{C}}\widetilde{Z}_{\overline{C}}E^{\mathrm{B}}B_{\overline{C}}\widetilde{B}_{\overline{C}}B'_{\overline{C}}\widetilde{B}'_{\overline{C}}|x_iz_ir_i}, \varphi_{Y_{\overline{C}}\widetilde{Y}_{\overline{C}}Z_{\overline{C}}\widetilde{Z}_{\overline{C}}E^{\mathrm{B}}B_{\overline{C}}\widetilde{B}_{\overline{C}}B'_{\overline{C}}\widetilde{B}'_{\overline{C}}|z_ir_i}\right) \\
\leq &\mathop{\mathbb{E}}_{i\in\overline{C}} \mathsf{P}_{X_iZ_iR_i|\mathcal{E}} \mathsf{B}\left(\varphi_{Y_{\overline{C}}\widetilde{Y}_{\overline{C}}Z_{\overline{C}}\widetilde{Z}_{\overline{C}}E^{\mathrm{B}}B_{\overline{C}}\widetilde{B}_{\overline{C}}B'_{\overline{C}}\widetilde{B}'_{\overline{C}}|x_iz_ir_i}, \varphi_{Y_{\overline{C}}\widetilde{Y}_{\overline{C}}Z_{\overline{C}}\widetilde{Z}_{\overline{C}}E^{\mathrm{B}}B_{\overline{C}}\widetilde{B}_{\overline{C}}B'_{\overline{C}}\widetilde{B}'_{\overline{C}}|z_ir_i}\right) \\
&\quad + \mathop{\mathbb{E}}_{i\in\overline{C}} \left\|\mathsf{P}_{X_iZ_iR_i|\mathcal{E}} - \mathsf{P}_{Z_i}\mathsf{P}_{X_iR_i|\mathcal{E},Z_i}\right\|_1 \\
\leq &2\sqrt{\delta} + \sqrt{2\delta},
\end{aligned}
$$

where to get the last step we use the fact that (23) implies

$$
\begin{aligned}
\mathop{\mathbb{E}}_{i\in\overline{C}} \left\|\mathsf{P}_{X_iY_iZ_iR_i|\mathcal{E}} - \mathsf{P}_{Z_i}\mathsf{P}_{X_iY_iR_i|\mathcal{E},Z_i}\right\|_1 &= \mathop{\mathbb{E}}_{i\in\overline{C}} \left\|\mathsf{P}_{X_iY_iR_i|\mathcal{E},Z_i}(\mathsf{P}_{Z_i|\mathcal{E}} - \mathsf{P}_{Z_i})\right\|_1 \\
&= \mathop{\mathbb{E}}_{i\in\overline{C}} \left\|\mathsf{P}_{Z_i|\mathcal{E}} - \mathsf{P}_{Z_i}\right\|_1 \\
&\leq \sqrt{2\delta}.
\end{aligned}
$$

Finally, since $\mathsf{P}_{Z_i}(\perp) = \alpha$, we have,

$$
\mathop{\mathbb{E}}_{i\in\overline{C}} \mathsf{P}_{X_iR_i|\mathcal{E},\perp} \mathsf{B}\left(\varphi_{Y_{\overline{C}}\widetilde{Y}_{\overline{C}}Z_{\overline{C}}\widetilde{Z}_{\overline{C}}E^{\mathrm{B}}B_{\overline{C}}\widetilde{B}_{\overline{C}}B'_{\overline{C}}\widetilde{B}'_{\overline{C}}|x_i\perp r_i}, \varphi_{Y_{\overline{C}}\widetilde{Y}_{\overline{C}}Z_{\overline{C}}\widetilde{Z}_{\overline{C}}E^{\mathrm{B}}B_{\overline{C}}\widetilde{B}_{\overline{C}}B'_{\overline{C}}\widetilde{B}'_{\overline{C}}|\perp r_i}\right) \leq \frac{2\sqrt{\delta}+\sqrt{2\delta}}{\alpha} \leq \frac{4\sqrt{\delta}}{\alpha}.
$$

By Uhlmann's theorem, there exist unitaries $\{U^i_{x_ir_i}\}_{x_ir_i}$ acting on the registers $X_{\overline{C}}\widetilde{X}_{\overline{C}}E^{\mathrm{A}}A_{\overline{C}}\widetilde{A}_{\overline{C}}$ such that

$$
\begin{aligned}
&\mathop{\mathbb{E}}_{i\in\overline{C}} \mathsf{P}_{X_iR_i|\mathcal{E},\perp} \mathsf{B}\left(U^i_{x_ir_i} \otimes \mathbb{1} \left|\varphi\right\rangle\!\left\langle\varphi\right|_{\perp r_i} (U^i_{x_ir_i})^\dagger \otimes \mathbb{1}, \left|\varphi\right\rangle\!\left\langle\varphi\right|_{x_i\perp r_i}\right) \\
= &\mathop{\mathbb{E}}_{i\in\overline{C}} \mathsf{P}_{X_iR_i|\mathcal{E},\perp} \mathsf{B}\left(\varphi_{Y_{\overline{C}}\widetilde{Y}_{\overline{C}}Z_{\overline{C}}\widetilde{Z}_{\overline{C}}E^{\mathrm{B}}B_{\overline{C}}\widetilde{B}_{\overline{C}}B'_{\overline{C}}\widetilde{B}'_{\overline{C}}|x_i\perp r_i}, \varphi_{Y_{\overline{C}}\widetilde{Y}_{\overline{C}}Z_{\overline{C}}\widetilde{Z}_{\overline{C}}E^{\mathrm{B}}B_{\overline{C}}\widetilde{B}_{\overline{C}}B'_{\overline{C}}\widetilde{B}'_{\overline{C}}|\perp r_i}\right) \\
\leq &\frac{4\sqrt{\delta}}{\alpha}.
\end{aligned}
$$

Now using the Fuchs-van de Graaf inequality we get,

$$\mathop{\mathbb{E}}_{i\in\overline{C}}\mathop{\mathbb{E}}_{\mathsf{P}_{X_iR_i|\mathcal{E},\perp}}\left\|U^i_{x_ir_i}\otimes\mathbb{1}\,|\varphi\rangle\langle\varphi|_{\perp r_i}\,(U^i_{x_ir_i})^\dagger\otimes\mathbb{1}-|\varphi\rangle\langle\varphi|_{x_i\perp r_i}\right\|_1\leq\frac{8\sqrt{2\delta}}{\alpha}. \tag{25}$$

Similarly, $\sigma_{Y_{\overline{C}}X_{\overline{C}}\widetilde{X}_{\overline{C}}E^{\mathrm{A}}A_{\overline{C}}\widetilde{A}_{\overline{C}}|x_Cy_Cz_Cdg}$ is product across $Y_{\overline{C}}$ and the rest of the registers. Hence by using the same analysis as above, we get that there exist unitaries $\{V^i_{y_ir_i}\}_{y_ir_i}$ acting only on the registers $Y_{\overline{C}}\widetilde{Y}_{\overline{C}}Z_{\overline{C}}\widetilde{Z}_{\overline{C}}E^{\mathrm{B}}B_{\overline{C}}\widetilde{B}_{\overline{C}}B'_{\overline{C}}\widetilde{B}'_{\overline{C}}$ such that,

$$\mathop{\mathbb{E}}_{i\in\overline{C}}\mathop{\mathbb{E}}_{\mathsf{P}_{Y_iR_i|\mathcal{E},\perp}}\left\|\mathbb{1}\otimes V^i_{y_ir_i}\,|\varphi\rangle\langle\varphi|_{\perp r_i}\,\mathbb{1}\otimes(V^i_{y_ir_i})^\dagger-|\varphi\rangle\langle\varphi|_{y_i\perp r_i}\right\|_1\leq\frac{8\sqrt{2\delta}}{\alpha}. \tag{26}$$

Now, if $\mathcal{O}_{X_i}$ is the channel that measures the X_i register and records the outcome, then

$$\mathcal{O}_{X_i}\left(\mathbb{1}\otimes V^i_{y_ir_i}\,|\varphi\rangle\langle\varphi|_{\perp r_i}\,\mathbb{1}\otimes(V^i_{y_ir_i})^\dagger\right)=\mathop{\mathbb{E}}_{\mathsf{P}_{X_i|\mathcal{E},\perp r_i}}|x_i\rangle\langle x_i|\otimes\left(\mathbb{1}\otimes V^i_{y_ir_i}\,|\varphi\rangle\langle\varphi|_{x_i\perp r_i}\,\mathbb{1}\otimes(V^i_{y_ir_i})^\dagger\right)$$
$$\mathcal{O}_{X_i}\left(|\varphi\rangle\langle\varphi|_{y_i\perp r_i}\right)=\mathop{\mathbb{E}}_{\mathsf{P}_{X_i|\mathcal{E},y_i\perp r_i}}|x_i\rangle\langle x_i|\otimes|\varphi\rangle\langle\varphi|_{x_iy_i\perp r_i}\,.$$

Therefore, applying Fact 9 to (26) with the $\mathcal{O}_{X_i}$ channel we get,

$$\mathop{\mathbb{E}}_{i\in\overline{C}}\mathop{\mathbb{E}}_{\mathsf{P}_{Y_iR_i|\mathcal{E},\perp}}\left\|\mathop{\mathbb{E}}_{\mathsf{P}_{X_i|\mathcal{E},\perp r_i}}|x_i\rangle\langle x_i|\otimes\left(\mathbb{1}\otimes V^i_{y_ir_i}\,|\varphi\rangle\langle\varphi|_{x_i\perp r_i}\,\mathbb{1}\otimes(V^i_{y_ir_i})^\dagger\right)-\mathop{\mathbb{E}}_{\mathsf{P}_{X_i|\mathcal{E},y_i\perp r_i}}|x_i\rangle\langle x_i|\otimes|\varphi\rangle\langle\varphi|_{x_iy_i\perp r_i}\right\|_1$$
$$\leq\frac{8\sqrt{2\delta}}{\alpha}.$$

From this we have,

$$\begin{aligned}
&\mathop{\mathbb{E}}_{i\in\overline{C}}\mathop{\mathbb{E}}_{\mathsf{P}_{X_iY_iR_i|\mathcal{E},\perp}}\left\|\mathbb{1}\otimes V^i_{y_ir_i}\,|\varphi\rangle\langle\varphi|_{x_i\perp r_i}\,\mathbb{1}\otimes(V^i_{y_ir_i})^\dagger-|\varphi\rangle\langle\varphi|_{x_iy_i\perp r_i}\right\|_1\\
&=\mathop{\mathbb{E}}_{i\in\overline{C}}\mathop{\mathbb{E}}_{\mathsf{P}_{Y_iR_i|\mathcal{E},\perp}}\left\|\mathop{\mathbb{E}}_{\mathsf{P}_{X_i|\mathcal{E},y_i\perp r_i}}|x_i\rangle\langle x_i|\otimes\left(\mathbb{1}\otimes V^i_{y_ir_i}\,|\varphi\rangle\langle\varphi|_{x_i\perp r_i}\,\mathbb{1}\otimes(V^i_{y_ir_i})^\dagger-|\varphi\rangle\langle\varphi|_{x_iy_i\perp r_i}\right)\right\|_1\\
&\leq\mathop{\mathbb{E}}_{i\in\overline{C}}\mathop{\mathbb{E}}_{\mathsf{P}_{Y_iR_i|\mathcal{E},\perp}}\left\|\mathop{\mathbb{E}}_{\mathsf{P}_{X_i|\mathcal{E},\perp r_i}}|x_i\rangle\langle x_i|\otimes\left(\mathbb{1}\otimes V^i_{y_ir_i}\,|\varphi\rangle\langle\varphi|_{x_i\perp r_i}\,\mathbb{1}\otimes(V^i_{y_ir_i})^\dagger\right)-\mathop{\mathbb{E}}_{\mathsf{P}_{X_i|\mathcal{E},y_i\perp r_i}}|x_i\rangle\langle x_i|\otimes|\varphi\rangle\langle\varphi|_{x_iy_i\perp r_i}\right\|_1\\
&\quad+\mathop{\mathbb{E}}_{i\in\overline{C}}\mathop{\mathbb{E}}_{\mathsf{P}_{Y_iR_i|\mathcal{E},\perp}}\left\|\left(\mathop{\mathbb{E}}_{\mathsf{P}_{X_i|\mathcal{E},y_i\perp r_i}}|x_i\rangle\langle x_i|-\mathop{\mathbb{E}}_{\mathsf{P}_{X_i|\mathcal{E},\perp r_i}}|x_i\rangle\langle x_i|\right)\otimes\left(\mathbb{1}\otimes V^i_{y_ir_i}\,|\varphi\rangle\langle\varphi|_{x_i\perp r_i}\,\mathbb{1}\otimes(V^i_{y_ir_i})^\dagger\right)\right\|_1\\
&\leq\frac{8\sqrt{2\delta}}{\alpha}+2\mathop{\mathbb{E}}_{i\in\overline{C}}\left\|\mathsf{P}_{X_iY_iR_i|\mathcal{E},\perp}-\mathsf{P}_{R_i|\mathcal{E},\perp}\mathsf{P}_{X_i|\mathcal{E},\perp,R_i}\mathsf{P}_{Y_i|\mathcal{E},\perp,R_i}\right\|_1.
\end{aligned}\tag{27}$$

Combining equations (25) and (27) we then get,

$$\begin{aligned}
&\mathop{\mathbb{E}}_{i\in\overline{C}}\mathop{\mathbb{E}}_{\mathsf{P}_{X_iY_iR_i|\mathcal{E},\perp}}\left\|U^i_{x_ir_i}\otimes V^i_{y_ir_i}\,|\varphi\rangle\langle\varphi|_{\perp r_i}\,(U^i_{x_ir_i})^\dagger\otimes(V^i_{y_ir_i})^\dagger-|\varphi\rangle\langle\varphi|_{x_iy_i\perp r_i}\right\|_1\\
&\leq\mathop{\mathbb{E}}_{i\in\overline{C}}\mathop{\mathbb{E}}_{\mathsf{P}_{X_iY_iR_i|\mathcal{E},\perp}}\left\|\mathbb{1}\otimes V^i_{y_ir_i}\left(U^i_{x_ir_i}\otimes\mathbb{1}\,|\varphi\rangle\langle\varphi|_{\perp r_i}\,(U^i_{x_ir_i})^\dagger\otimes\mathbb{1}-|\varphi\rangle\langle\varphi|_{x_i\perp r_i}\right)\mathbb{1}\otimes(V^i_{y_ir_i})^\dagger\right\|_1\\
&\quad+\mathop{\mathbb{E}}_{i\in\overline{C}}\mathop{\mathbb{E}}_{\mathsf{P}_{X_iY_iR_i|\mathcal{E},\perp}}\left\|\mathbb{1}\otimes V^i_{y_ir_i}\,|\varphi\rangle\langle\varphi|_{x_i\perp r_i}\,\mathbb{1}\otimes(V^i_{y_ir_i})^\dagger-|\varphi\rangle\langle\varphi|_{x_iy_i\perp r_i}\right\|_1
\end{aligned}$$

$$
\begin{aligned}
&= \mathop{\mathbb{E}}_{i\in\overline{C}} \mathop{\mathbb{E}}_{\mathsf{P}_{X_iY_iR_i|\mathcal{E},\perp}} \left\| U^i_{x_ir_i} \otimes \mathbb{1} \left|\varphi\right\rangle\!\left\langle\varphi\right|_{\perp r_i} (U^i_{x_ir_i})^\dagger \otimes \mathbb{1} - \left|\varphi\right\rangle\!\left\langle\varphi\right|_{x_i\perp r_i} \right\|_1 \\
&\quad + \mathop{\mathbb{E}}_{i\in\overline{C}} \mathop{\mathbb{E}}_{\mathsf{P}_{X_iY_iR_i|\mathcal{E},\perp}} \left\| \mathbb{1} \otimes V^i_{y_ir_i} \left|\varphi\right\rangle\!\left\langle\varphi\right|_{x_i\perp r_i} \mathbb{1} \otimes (V^i_{y_ir_i})^\dagger - \left|\varphi\right\rangle\!\left\langle\varphi\right|_{x_iy_i\perp r_i} \right\|_1 \\
&\leq \frac{16\sqrt{2\delta}}{\alpha} + 2 \mathop{\mathbb{E}}_{i\in\overline{C}} \left\| \mathsf{P}_{X_iY_iR_i|\mathcal{E},\perp} - \mathsf{P}_{R_i|\mathcal{E},\perp} \mathsf{P}_{X_i|\mathcal{E},\perp,R_i} \mathsf{P}_{Y_i|\mathcal{E},\perp,R_i} \right\|_1 . \qquad (28)
\end{aligned}
$$

Now note that we have an upper bound of $2\sqrt{2\delta}$ on $\mathbb{E}_{i\in\overline{C}} \left\| \mathsf{P}_{X_iY_iZ_iR_i|\mathcal{E}} - \mathsf{P}_{X_iY_i|Z_i} \mathsf{P}_{Z_iR_i|\mathcal{E}} \right\|_1$. Thus, by Fact 5,

$$
\begin{aligned}
\mathop{\mathbb{E}}_{i\in\overline{C}} \left\| \mathsf{P}_{X_iY_iR_i|\mathcal{E},\perp} - \mathsf{P}_{X_iY_i|\perp} \mathsf{P}_{R_i|\mathcal{E},\perp} \right\|_1 &\leq \frac{2}{\mathsf{P}_{Z_i}(\perp)} \mathop{\mathbb{E}}_{i\in\overline{C}} \left\| \mathsf{P}_{X_iY_iZ_iR_i|\mathcal{E}} - \mathsf{P}_{X_iY_i|Z_i} \mathsf{P}_{Z_iR_i|\mathcal{E}} \right\|_1 \\
&\leq \frac{4\sqrt{2\delta}}{\alpha}.
\end{aligned}
$$

Using this we get, and the fact that $\mathsf{P}_{X_iY_i|\perp} = \mathsf{P}_{X_iY_i} = \mathsf{P}_{X_i}\mathsf{P}_{Y_i} = \mathsf{P}_{X_i|\perp}\mathsf{P}_{Y_i|\perp}$, we get,

$$
\begin{aligned}
&\mathop{\mathbb{E}}_{i\in\overline{C}} \left\| \mathsf{P}_{X_iY_iR_i|\mathcal{E},\perp} - \mathsf{P}_{R_i|\mathcal{E},\perp} \mathsf{P}_{X_i|\mathcal{E},\perp,R_i} \mathsf{P}_{Y_i|\mathcal{E},\perp,R_i} \right\|_1 \\
&\leq \mathop{\mathbb{E}}_{i\in\overline{C}} \left(\left\| \mathsf{P}_{X_iY_iR_i|\mathcal{E},\perp} - \mathsf{P}_{X_iY_i|\perp} \mathsf{P}_{R_i|\mathcal{E},\perp} \right\|_1 + \left\| \mathsf{P}_{X_i|\perp} \mathsf{P}_{Y_i|\perp} \mathsf{P}_{R_i|\mathcal{E},\perp} - \mathsf{P}_{Y_iR_i|\mathcal{E},\perp} \mathsf{P}_{X_i|\mathcal{E},\perp,R_i} \right\|_1 \right) \\
&\leq \frac{4\sqrt{2\delta}}{\alpha} + \mathop{\mathbb{E}}_{i\in\overline{C}} \left(\left\| (\mathsf{P}_{X_i|\perp} \mathsf{P}_{R_i|\mathcal{E},\perp} - \mathsf{P}_{X_iR_i|\mathcal{E},\perp}) \mathsf{P}_{Y_i|\perp} \right\|_1 + \left\| \mathsf{P}_{X_i|\mathcal{E},\perp,R_i} (\mathsf{P}_{Y_i|\perp} \mathsf{P}_{R_i|\mathcal{E},\perp} - \mathsf{P}_{Y_iR_i|\mathcal{E},\perp}) \right\|_1 \right) \\
&\leq \frac{4\sqrt{2\delta}}{\alpha} + \mathop{\mathbb{E}}_{i\in\overline{C}} \left(\left\| \mathsf{P}_{X_i|\perp} \mathsf{P}_{R_i|\mathcal{E},\perp} - \mathsf{P}_{X_iR_i|\mathcal{E},\perp} \right\|_1 + \left\| \mathsf{P}_{Y_i|\perp} \mathsf{P}_{R_i|\mathcal{E},\perp} - \mathsf{P}_{Y_iR_i|\mathcal{E},\perp} \right\|_1 \right) \\
&\leq \frac{4\sqrt{2\delta}}{\alpha} + 2 \mathop{\mathbb{E}}_{i\in\overline{C}} \left\| \mathsf{P}_{X_iY_i|\perp} \mathsf{P}_{R_i|\mathcal{E},\perp} - \mathsf{P}_{X_iY_iR_i|\mathcal{E},\perp} \right\|_1 \leq \frac{12\sqrt{2\delta}}{\alpha}.
\end{aligned}
$$

In the fourth line of the above calculation, we have upper bounded $\left\| \mathsf{P}_{X_i|\perp} \mathsf{P}_{R_i|\mathcal{E},\perp} - \mathsf{P}_{X_iR_i|\mathcal{E},\perp} \right\|_1$ by $\left\| \mathsf{P}_{X_iY_i|\perp} \mathsf{P}_{R_i|\mathcal{E},\perp} - \mathsf{P}_{X_iY_iR_i|\mathcal{E},\perp} \right\|_1$ since we get the distributions $\mathsf{P}_{X_i|\perp} \mathsf{P}_{R_i|\mathcal{E},\perp}$ and $\mathsf{P}_{X_iR_i|\mathcal{E},\perp}$ respectively by tracing out the Y_i registers of $\mathsf{P}_{X_iY_i|\perp} \mathsf{P}_{R_i|\mathcal{E},\perp}$ and $\mathsf{P}_{X_iY_iR_i|\mathcal{E},\perp}$; also, we have upper bounded $\left\| \mathsf{P}_{Y_i|\perp} \mathsf{P}_{R_i|\mathcal{E},\perp} - \mathsf{P}_{Y_iR_i|\mathcal{E},\perp} \right\|_1$ by similar reasoning. Putting the above bound in (28) we get,

$$
\mathop{\mathbb{E}}_{i\in\overline{C}} \mathop{\mathbb{E}}_{\mathsf{P}_{X_iY_iR_i|\mathcal{E},\perp}} \left\| U^i_{x_ir_i} \otimes V^i_{y_ir_i} \left|\varphi\right\rangle\!\left\langle\varphi\right|_{\perp r_i} (U^i_{x_ir_i})^\dagger \otimes (V^i_{y_ir_i})^\dagger - \left|\varphi\right\rangle\!\left\langle\varphi\right|_{x_iy_i\perp r_i} \right\|_1 \leq \frac{16\sqrt{2\delta}}{\alpha} + \frac{24\sqrt{2\delta}}{\alpha}.
$$

Now, the quantity we actually want to bound is almost the same as the above expression, except we have to take the expectation over the distribution $\mathsf{P}_{X_iY_iR_i|\mathcal{E}}$ rather than $\mathsf{P}_{X_iY_iR_i|\mathcal{E},\perp}$. Since the ℓ_1-distance term always lies between 0 and 2, changing the distribution over which the expectation is taken can only increase the expectation value by at most 2 times the distance between the two distributions. Thus we can write

$$
\begin{aligned}
&\mathop{\mathbb{E}}_{i\in\overline{C}} \mathop{\mathbb{E}}_{\mathsf{P}_{X_iY_iR_i|\mathcal{E}}} \left\| U^i_{x_ir_i} \otimes V^i_{y_ir_i} \otimes \mathbb{1} \left|\varphi\right\rangle\!\left\langle\varphi\right|_{\perp r_i} (U^i_{x_ir_i})^\dagger \otimes (V^i_{y_ir_i})^\dagger \otimes \mathbb{1} - \left|\varphi\right\rangle\!\left\langle\varphi\right|_{x_iy_i\perp r_i} \right\|_1 \\
&\leq \mathop{\mathbb{E}}_{i\in\overline{C}} \mathop{\mathbb{E}}_{\mathsf{P}_{X_iY_iR_i|\mathcal{E},\perp}} \left\| U^i_{x_ir_i} \otimes V^i_{y_ir_i} \left|\varphi\right\rangle\!\left\langle\varphi\right|_{\perp r_i} (U^i_{x_ir_i})^\dagger \otimes (V^i_{y_ir_i})^\dagger - \left|\varphi\right\rangle\!\left\langle\varphi\right|_{x_iy_i\perp r_i} \right\|_1 \\
&\quad + 2 \mathop{\mathbb{E}}_{i\in\overline{C}} \left\| \mathsf{P}_{X_iY_iR_i|\mathcal{E}} - \mathsf{P}_{X_iY_iR_i|\mathcal{E},\perp} \right\|_1
\end{aligned}
$$

$$\leq \frac{40\sqrt{2\delta}}{\alpha} + \frac{4}{\alpha}\mathop{\mathbb{E}}_{i\in\overline{C}}\left\|\mathsf{P}_{X_iY_iZ_iR_i|\mathcal{E}} - \mathsf{P}_{X_iY_iR_i|\mathcal{E}}\mathsf{P}_{Z_i|X_iY_i}\right\|_1 + \frac{10}{\alpha}\mathop{\mathbb{E}}_{i\in\overline{C}}\left\|\mathsf{P}_{X_iY_iZ_i|\mathcal{E}} - \mathsf{P}_{X_iY_iZ_i}\right\|_1$$
$$\leq \frac{40\sqrt{2\delta}}{\alpha} + \frac{18\sqrt{2\delta}}{\alpha} = \frac{58\sqrt{2\delta}}{\alpha}, \tag{29}$$

where to get the third line we used item (i) of Lemma 32 to bound $\left\|\mathsf{P}_{X_iY_iR_i|\mathcal{E}} - \mathsf{P}_{X_iY_iR_i|\mathcal{E},\perp}\right\|_1$, and in the next line we have used (24) and (23) to bound the trace distances. This proves item (ii) of the lemma.

Existence of unitaries $W^i_{y_iz_ir_i}$. Note that $\sigma_{Z_{\overline{C}}X_{\overline{C}}\widetilde{X}_{\overline{C}}A_{\overline{C}}\widetilde{A}_{\overline{C}}B_{\overline{C}}\widetilde{B}_{\overline{C}}E^{\mathrm{A}}|dg}$ is product across $Z_{\overline{C}}$ and the rest of the registers, since they were product in ρ, and σ is obtained from ρ by a unitary that acts on the other registers, only using $Z_{\overline{C}}$ as a control register (this is also true if we include $Y_{\overline{C}}\widetilde{Y}_{\overline{C}}$ along with $X_{\overline{C}}\widetilde{X}_{\overline{C}}A_{\overline{C}}\widetilde{A}_{\overline{C}}B_{\overline{C}}\widetilde{B}_{\overline{C}}E^{\mathrm{A}}$, but we don't need to do this). Therefore, by the same analysis as in the case of $X_{\overline{C}}$ and $Y_{\overline{C}}$,

$$\begin{aligned}
2\delta &\geq \mathop{\mathbb{E}}_{i\in\overline{C}}\mathsf{P}_{Z_iD_iG_iR_i|\mathcal{E}}\mathop{\mathbb{E}}\mathsf{D}\left(\varphi_{X_{\overline{C}}\widetilde{X}_{\overline{C}}A_{\overline{C}}\widetilde{A}_{\overline{C}}B_{\overline{C}}\widetilde{B}_{\overline{C}}E^{\mathrm{A}}|z_id_ig_ir_i}\middle\|\varphi_{X_{\overline{C}}\widetilde{X}_{\overline{C}}A_{\overline{C}}\widetilde{A}_{\overline{C}}B_{\overline{C}}\widetilde{B}_{\overline{C}}E^{\mathrm{A}}|d_ig_ir_i}\right)\\
&\geq \frac{1}{2}\mathop{\mathbb{E}}_{i\in\overline{C}}\mathsf{P}_{X_iY_iZ_iR_i|\mathcal{E}}\mathop{\mathbb{E}}\mathsf{D}\left(\varphi_{X_{\overline{C}}\widetilde{X}_{\overline{C}}A_{\overline{C}}\widetilde{A}_{\overline{C}}B_{\overline{C}}\widetilde{B}_{\overline{C}}E^{\mathrm{A}}|x_iy_iz_ir_i}\middle\|\varphi_{X_{\overline{C}}\widetilde{X}_{\overline{C}}A_{\overline{C}}\widetilde{A}_{\overline{C}}B_{\overline{C}}\widetilde{B}_{\overline{C}}E^{\mathrm{A}}|x_iy_ir_i}\right)\\
&\geq \frac{1}{2}\mathop{\mathbb{E}}_{i\in\overline{C}}\mathsf{P}_{X_iY_iZ_iR_i|\mathcal{E}}\mathop{\mathbb{E}}\mathsf{B}\left(\varphi_{X_{\overline{C}}\widetilde{X}_{\overline{C}}A_{\overline{C}}\widetilde{A}_{\overline{C}}B_{\overline{C}}\widetilde{B}_{\overline{C}}E^{\mathrm{A}}|x_iy_iz_ir_i},\varphi_{X_{\overline{C}}\widetilde{X}_{\overline{C}}A_{\overline{C}}\widetilde{A}_{\overline{C}}B_{\overline{C}}\widetilde{B}_{\overline{C}}E^{\mathrm{A}}|x_iy_ir_i}\right)^2.
\end{aligned}$$

Using Jensen's inequality on the last inequality, we get,

$$\mathop{\mathbb{E}}_{i\in\overline{C}}\mathsf{P}_{X_iY_iZ_iR_i|\mathcal{E}}\mathop{\mathbb{E}}\mathsf{B}\left(\varphi_{X_{\overline{C}}\widetilde{X}_{\overline{C}}A_{\overline{C}}\widetilde{A}_{\overline{C}}B_{\overline{C}}\widetilde{B}_{\overline{C}}E^{\mathrm{A}}|x_iy_iz_ir_i},\varphi_{X_{\overline{C}}\widetilde{X}_{\overline{C}}A_{\overline{C}}\widetilde{A}_{\overline{C}}B_{\overline{C}}\widetilde{B}_{\overline{C}}E^{\mathrm{A}}|x_iy_ir_i}\right) \leq 2\sqrt{\delta}. \tag{30}$$

Moreover, shifting the expectation from $\mathsf{P}_{X_iY_iZ_iR_i|\mathcal{E}}$ to $\mathsf{P}_{Z_i}\mathsf{P}_{X_iY_iR_i|\mathcal{E},Z_i}$ and conditioning on $Z_i = \perp$ (which happens with probability α under P_{Z_i}), like we did when showing the existence of $U^i_{x_ir_i}, V^i_{y_ir_i}$, we get,

$$\mathop{\mathbb{E}}_{i\in\overline{C}}\mathsf{P}_{X_iY_iR_i|\mathcal{E},\perp}\mathop{\mathbb{E}}\mathsf{B}\left(\varphi_{X_{\overline{C}}\widetilde{X}_{\overline{C}}A_{\overline{C}}\widetilde{A}_{\overline{C}}B_{\overline{C}}\widetilde{B}_{\overline{C}}E^{\mathrm{A}}|x_iy_i\perp r_i},\varphi_{X_{\overline{C}}\widetilde{X}_{\overline{C}}A_{\overline{C}}\widetilde{A}_{\overline{C}}B_{\overline{C}}\widetilde{B}_{\overline{C}}E^{\mathrm{A}}|x_iy_ir_i}\right) \leq \frac{4\sqrt{\delta}}{\alpha}. \tag{31}$$

Now using the triangle inequality on (30) and (31), we get,

$$\begin{aligned}
&\mathop{\mathbb{E}}_{i\in\overline{C}}\mathsf{P}_{X_iY_iZ_iR_i|\mathcal{E}}\mathop{\mathbb{E}}\mathsf{B}\left(\varphi_{X_{\overline{C}}\widetilde{X}_{\overline{C}}A_{\overline{C}}\widetilde{A}_{\overline{C}}B_{\overline{C}}\widetilde{B}_{\overline{C}}E^{\mathrm{A}}|x_iy_iz_ir_i},\varphi_{X_{\overline{C}}\widetilde{X}_{\overline{C}}A_{\overline{C}}\widetilde{A}_{\overline{C}}B_{\overline{C}}\widetilde{B}_{\overline{C}}E^{\mathrm{A}}|x_iy_i\perp r_i}\right)\\
\leq &\mathop{\mathbb{E}}_{i\in\overline{C}}\mathsf{P}_{X_iY_iZ_iR_i|\mathcal{E}}\mathop{\mathbb{E}}\mathsf{B}\left(\varphi_{X_{\overline{C}}\widetilde{X}_{\overline{C}}A_{\overline{C}}\widetilde{A}_{\overline{C}}B_{\overline{C}}\widetilde{B}_{\overline{C}}E^{\mathrm{A}}|x_iy_iz_ir_i},\varphi_{X_{\overline{C}}\widetilde{X}_{\overline{C}}A_{\overline{C}}\widetilde{A}_{\overline{C}}B_{\overline{C}}\widetilde{B}_{\overline{C}}E^{\mathrm{A}}|x_iy_ir_i}\right)\\
&+\mathop{\mathbb{E}}_{i\in\overline{C}}\mathsf{P}_{X_iY_iR_i|\mathcal{E},\perp}\mathop{\mathbb{E}}\mathsf{B}\left(\varphi_{X_{\overline{C}}\widetilde{X}_{\overline{C}}A_{\overline{C}}\widetilde{A}_{\overline{C}}B_{\overline{C}}\widetilde{B}_{\overline{C}}E^{\mathrm{A}}|x_iy_i\perp r_i},\varphi_{X_{\overline{C}}\widetilde{X}_{\overline{C}}A_{\overline{C}}\widetilde{A}_{\overline{C}}B_{\overline{C}}\widetilde{B}_{\overline{C}}E^{\mathrm{A}}|x_iy_ir_i}\right)\\
&+\mathop{\mathbb{E}}_{i\in\overline{C}}\left\|(\mathsf{P}_{X_iY_iR_i|\mathcal{E}} - \mathsf{P}_{X_iY_iR_i|\mathcal{E},\perp})\mathsf{P}_{Z_i|\mathcal{E},X_iY_iR_i}\right\|_1\\
\leq &2\sqrt{\delta} + \frac{4\sqrt{\delta}}{\alpha} + \frac{2}{\alpha}\mathop{\mathbb{E}}_{i\in\overline{C}}\left\|\mathsf{P}_{X_iY_iR_iZ_i|\mathcal{E}} - \mathsf{P}_{X_iY_iR_i|\mathcal{E}}\mathsf{P}_{Z_i|X_iY_i}\right\|_1 + \frac{5}{\alpha}\mathop{\mathbb{E}}_{i\in\overline{C}}\left\|\mathsf{P}_{X_iY_iZ_i|\mathcal{E}} - \mathsf{P}_{X_iY_iZ_i}\right\|_1
\end{aligned}$$

$$\leq 2\sqrt{\delta} + \frac{4\sqrt{\delta}}{\alpha} + \frac{4\sqrt{2\delta}}{\alpha} + \frac{5\sqrt{2\delta}}{\alpha}$$
$$\leq \frac{15\sqrt{\delta}}{\alpha}. \tag{32}$$

In the third line of the above calculation, we have noted that $\left\|(\mathsf{P}_{X_iY_iR_i|\mathcal{E}} - \mathsf{P}_{X_iY_iR_i|\mathcal{E},\perp})\mathsf{P}_{Z_i|\mathcal{E},X_iY_iR_i}\right\|_1 = \left\|\mathsf{P}_{X_iY_iR_i|\mathcal{E}} - \mathsf{P}_{X_iY_iR_i|\mathcal{E},\perp}\right\|_1$, and we have used item (i) of Lemma 32 (with $X_iY_i = S, Z_i = T, R_i = R$, and the conditioned variables being the corresponding primed variables) to bound the latter. In the fourth line, we have used (24) and (23) to bound the trace distances.

Applying the Fuchs-van de Graaf inequality on (32) and tracing out registers besides A_iB_i gives us

$$\mathop{\mathbb{E}}_{i\in\overline{C}} \mathop{\mathbb{E}}_{\mathsf{P}_{X_iY_iZ_iR_i|\mathcal{E}}} \left\|\varphi_{A_iB_i|x_iy_iz_ir_i} - \varphi_{A_iB_i|x_iy_i\perp r_i}\right\|_1 \leq \frac{30\sqrt{2\delta}}{\alpha}.$$

Since the A_iB_i registers are classical, the trace distance in the above expression can be interpreted as the distance between the distributions $\mathsf{P}_{A_iB_i|\mathcal{E},x_iy_iz_ir_i}$ and $\mathsf{P}_{A_iB_i|\mathcal{E},x_iy_i\perp r_i}$. Therefore we have,

$$\begin{aligned}\mathop{\mathbb{E}}_{i\in\overline{C}} \left\|\mathsf{P}_{X_iY_iZ_iR_i|\mathcal{E}}(\mathsf{P}_{A_iB_i|\mathcal{E},X_iY_iZ_iR_i} - \mathsf{P}_{A_iB_i|\mathcal{E},X_iY_i,\perp,R_i})\right\|_1 &= \mathop{\mathbb{E}}_{i\in\overline{C}} \mathop{\mathbb{E}}_{\mathsf{P}_{X_iY_iZ_iR_i|\mathcal{E}}} \left\|\mathsf{P}_{A_iB_i|\mathcal{E},x_iy_iz_ir_i} - \mathsf{P}_{A_iB_i|\mathcal{E},x_iy_i\perp r_i}\right\|_1 \\ &\leq \frac{30\sqrt{2\delta}}{\alpha},\end{aligned}$$

which is item (iii) of the lemma.

To get item (iv) of the lemma, we use the Fuchs-van de Graaf inequality on (32) but don't trace out any registers, and then we use Uhlmann's theorem as before, which gives us unitaries $\{W^i_{x_iy_iz_ir_i}\}_{x_iy_iz_ir_i}$ acting on $Y_{\overline{C}}\widetilde{Y}_{\overline{C}}Z_{\overline{C}}\widetilde{Z}_{\overline{C}}E^{\mathrm{B}}B'_{\overline{C}}\widetilde{B}'_{\overline{C}}$ such that

$$\mathop{\mathbb{E}}_{i\in\overline{C}} \mathop{\mathbb{E}}_{\mathsf{P}_{X_iY_iZ_iR_i|\mathcal{E}}} \left\|\mathbb{1}\otimes W^i_{x_iy_iz_ir_i}\,|\varphi\rangle\langle\varphi|_{x_iy_i,\perp r_i}\,\mathbb{1}\otimes (W^i_{x_iy_iz_ir_i})^\dagger - |\varphi\rangle\langle\varphi|_{x_iy_iz_ir_i}\right\|_1 \leq \frac{30\sqrt{2\delta}}{\alpha}. \tag{33}$$

Since z_i is either $\perp$, in which case the unitary $W^i_{x_iy_iz_ir_i}$ can just be identity, or z_i contains x_i, $W^i_{x_iy_iz_ir_i}$ is in fact just $W^i_{y_iz_ir_i}$.

Let $\mathcal{O}_{A_iB_i}$ be the channel that measures the A_iB_i registers and records the outcomes. This clearly commutes with $W^i_{y_iz_ir_i}$. Therefore,

$$\begin{aligned}&\mathcal{O}_{A_iB_i}\left(\mathbb{1}\otimes W^i_{y_iz_ir_i}\,|\varphi\rangle\langle\varphi|_{x_iy_i\perp r_i}\,\mathbb{1}\otimes (W^i_{y_iz_ir_i})^\dagger\right) \\ =&\mathop{\mathbb{E}}_{\mathsf{P}_{A_iB_i|\mathcal{E},x_iy_i\perp r_i}} |a_ib_i\rangle\langle a_ib_i|\otimes\left(\mathbb{1}\otimes W^i_{y_iz_ir_i}\,|\varphi\rangle\langle\varphi|_{x_iy_i\perp a_ib_ir_i}\,\mathbb{1}\otimes (W^i_{y_iz_ir_i})^\dagger\right) \\ &\mathcal{O}_{A_iB_i}\left(|\varphi\rangle\langle\varphi|_{x_iy_iz_ir_i}\right) \\ =&\mathop{\mathbb{E}}_{\mathsf{P}_{A_iB_i|x_iy_iz_ir_i}} |a_ib_i\rangle\langle a_ib_i|\otimes|\varphi\rangle\langle\varphi|_{x_iy_iz_ia_ib_ir_i}\end{aligned}$$

Using this and Fact 9 on (33) along with item (iii) we get,

$$\begin{aligned}&\mathop{\mathbb{E}}_{i\in\overline{C}} \mathop{\mathbb{E}}_{\mathsf{P}_{X_iY_iZ_iA_iB_iR_i|\mathcal{E}}} \left\|\mathbb{1}\otimes W^i_{y_iz_ir_i}\,|\varphi\rangle\langle\varphi|_{x_iy_i\perp a_ib_ir_i}\,\mathbb{1}\otimes (W^i_{y_iz_ir_i})^\dagger - |\varphi\rangle\langle\varphi|_{x_iy_iz_ia_ib_ir_i}\right\|_1 \\ \leq&\frac{30\sqrt{2\delta}}{\alpha} + 2\mathop{\mathbb{E}}_{i\in\overline{C}} \left\|\mathsf{P}_{X_iY_iZ_iR_i|\mathcal{E}}\left(\mathsf{P}_{A_iB_i|\mathcal{E},X_iY_iZ_iR_i} - \mathsf{P}_{A_iB_i|\mathcal{E},X_iY_i,\perp,R_i}\right)\right\|_1\end{aligned}$$

$$\leq \frac{90\sqrt{2\delta}}{\alpha}$$

This proves item (iv). □

7.2 Parallel repetition theorem for 1-round 3-player product-anchored game

We call a 1-round 3-player product-anchored iff Alice and Bob's marginal input distribution is a product distribution, and Eve's input takes value either $z = (x, y)$ or $z = \perp$ such that $p(x, y, \perp) = \alpha \cdot p(x, y)$. Note that this is also a special type of anchoring on Charlie's side, but this definition will be sufficient for our purposes.

Theorem 37. *Let G be a 1-round 3-player non-local product-anchored game with parameter α. Then for $\delta > 0$ and $t = (\omega^*(G) + \eta)l$,*

$$\omega^*(G^l) = \left(1 - (1 - \omega^*(G))^3\right)^{\Omega\left(\frac{\alpha^2 l}{\log(|\mathcal{A}|\cdot|\mathcal{B}|\cdot|\mathcal{C}|)}\right)}$$
$$\omega^*(G^{t/l}) = \left(1 - \eta^3\right)^{\Omega\left(\frac{\alpha^2 l}{\log(|\mathcal{A}|\cdot|\mathcal{B}|\cdot|\mathcal{C}|)}\right)}.$$

Proof sketch. Defining the correlation-breaking variables $D_i G_i$ the same way as in the 2-player 2-round case, we have that conditioned on $DG = dg$, Alice's inputs are in product with Bob and Eve's systems in the state of a strategy for l copies of G; the analogous statements hold for Bob and Eve's inputs as well. As in the case of the 2-round game, we condition on the success event $\mathcal{E}$ on a subset C, and define $|\varphi\rangle$ to be the state of the protocol conditioned on $\mathcal{E}$. Defining R_i and the quantity δ the same way, the lemma analogous to Lemma 36 in this case is the following.

Lemma 38. *If $\delta = O(\varepsilon^2\alpha^2)$, the following conditions hold:*

(i) $\mathbb{E}_{i\in\overline{C}} \left\| \mathsf{P}_{X_iY_iZ_iR_i|\mathcal{E}} - \mathsf{P}_{X_iY_iZ_i}\mathsf{P}_{R_i|\mathcal{E},\perp} \right\|_1 \leq \frac{9\sqrt{2\delta}}{\alpha}$;

(ii) For each $i \in \overline{C}$, there exist unitaries $U^i_{x_ir_ix_ir_i}, \{V^i_{y_ir_i}\}_{y_ir_i}, \{W^i_{z_ir_i}\}_{z_ir_i}$ acting on Alice, Bob and Charlie's systems such that

$$\mathop{\mathbb{E}}_{i\in\overline{C}} \mathop{\mathbb{E}}_{\mathsf{P}_{X_iY_iZ_iR_i|\mathcal{E}}} \left\| U^i_{x_ir_i} \otimes V^i_{y_ir_i} \otimes W^i_{z_ir_i} |\varphi\rangle\langle\varphi|_{\perp r_i} (U^i_{x_ir_i})^\dagger \otimes (V^i_{y_ir_i})^\dagger \otimes (W^i_{z_ir_i})^\dagger - |\varphi\rangle\langle\varphi|_{x_iy_iz_ir_i} \right\|_1$$
$$\leq \frac{88\sqrt{2\delta}}{\alpha}.$$

The proof of item (i) in Lemma 38 is exactly the same as in Lemma 36. The existence of unitaries $U^i_{x_ir_i}$ and $V^i_{y_ir_i}$ in item (ii) is shown in exactly the same way. The existence of Eve's unitaries $W^i_{z_ir_i}$ is shown in a way similar to the existence of the second round unitaries in Lemma 36, and using the fact that Eve's inputs are in product with Alice and Bob's systems in the original state, conditioned on dg.

Using Lemma 38, we can give a strategy for a single copy of G where Alice, Bob and Eve share $\mathsf{P}_{R_i|\mathcal{E},\perp}$ as randomness and $|\varphi\rangle_{\perp r_i}$ as entanglement, and apply the unitaries $U^i_{x_ir_i}, V^i_{y_ir_i}$ and $W^i_{z_ir_i}$ on receiving inputs (x_i, y_i, z_i). □

Acknowledgements

We thank Anne Broadbent for discussions on the result in [BI20], as well as Lídia del Rio, Christopher Portmann, Renato Renner and Vilasini Venkatesh for discussions on composable security. We also thank Serge Fehr and anonymous reviewers on an earlier version of this manuscript for pointing out the additional required conditions on Bob's boxes.

This work was prepared while S. K. was at the Centre for Quantum Technologies (National University of Singapore), supported by the National Research Foundation, including under NRF RF Award No. NRF-NRFF2013-13, the Prime Minister's Office, Singapore; the Ministry of Education, Singapore, under the Research Centres of Excellence program and by Grant No. MOE2012-T3-1-009; and in part by the NRF2017-NRF-ANR004 VanQuTe Grant. E. Y.-Z. T. was at the Institute for Theoretical Physics (ETH Zürich), supported by the Swiss National Science Foundation (SNSF) grant number 20QT21_187724 via the National Center for Competence in Research for Quantum Science and Technology (QSIT), the Air Force Office of Scientific Research (AFOSR) via grant FA9550-19-1-0202, and the QuantERA project eDICT.

References

[ACK+14] N. Aharon, A. Chailloux, I. Kerenidis, S. Massar, S. Pironio, and J. Silman. Weak coin flipping in a device-independent setting. *Theory of Quantum Computation, Communication, and Cryptography*. 2014, pp. 1–12. ISBN: 978-3-642-54429-3.

[AFDF+18] R. Arnon-Friedman, F. Dupuis, O. Fawzi, R. Renner, and T. Vidick. Practical device-independent quantum cryptography via entropy accumulation. En. *Nature Communications* 9.1 (2018), p. 459. ISSN: 2041-1723.

[AMP+16] N. Aharon, S. Massar, S. Pironio, and J. Silman. Device-independent bit commitment based on the CHSH inequality. *New Journal of Physics* 18.2 (2016), p. 025014.

[BB84] C. H. Bennett and G. Brassard. Quantum cryptography: Public key distribution and coin tossing. *Proceedings of International Conference on Computers, Systems and Signal Processing*. 1984, p. 175.

[BCK13] J. Barrett, R. Colbeck, and A. Kent. Memory Attacks on Device-Independent Quantum Cryptography. *Physical Review Letters* 110 (2013), p. 010503.

[BI20] A. Broadbent and R. Islam. Quantum Encryption with Certified Deletion. *Theory of Cryptography*. 2020, pp. 92–122.

[BOHL+05] M. Ben-Or, M. Horodecki, D. W. Leung, D. Mayers, and J. Oppenheim. The Universal Composable Security of Quantum Key Distribution. *Theory of Cryptography*. 2005, pp. 386–406. ISBN: 978-3-540-30576-7.

[BVY15] M. Bavarian, T. Vidick, and H. Yuen. *Anchoring Games for Parallel Repetition*. https://arxiv.org/abs/1509.07466. 2015.

[BVY17] M. Bavarian, T. Vidick, and H. Yuen. Hardness Amplification for Entangled Games via Anchoring. *Proceedings of the 49th Annual ACM SIGACT Symposium on Theory of Computing*. STOC '17. Montreal, Canada, 2017, 303–316. ISBN: 9781450345286.

[CW79] J. L. Carter and M. N. Wegman. Universal classes of hash functions. *Journal of Computer and System Sciences* 18.2 (1979), pp. 143–154.

[FM18] H. Fu and C. A. Miller. Local randomness: Examples and application. *Physical Review A* 97 (2018), p. 032324.

[GMP22] A. Gheorghiu, T. Metger, and A. Poremba. *Quantum cryptography with classical communication: parallel remote state preparation for copy-protection, verification, and more*. https://arxiv.org/abs/2201.13445. 2022.

[Hol07] T. Holenstein. Parallel Repetition: Simplifications and the No-Signaling Case. *Proceedings of the Thirty-Ninth Annual ACM Symposium on Theory of Computing*. STOC '07. San Diego, California, USA, 2007, 411–419. ISBN: 9781595936318.

[JK21] R. Jain and S. Kundu. A Direct Product Theorem for One-Way Quantum Communication. *Proceedings of the 36th IEEE Annual Computational Complexity Conference (CCC 2021)*. 2021, 27:1–27:28. ISBN: 978-3-95977-193-1.

[JMS20] R. Jain, C. A. Miller, and Y. Shi. Parallel Device-Independent Quantum Key Distribution. *IEEE Transactions on Information Theory* 66.9 (2020), pp. 5567–5584.

[JPY14] R. Jain, A. Pereszlényi, and P. Yao. A Parallel Repetition Theorem for Entangled Two-Player One-Round Games under Product Distributions. *2014 IEEE 29th Conference on Computational Complexity (CCC '14)*. 2014, pp. 209–216.

[KKM+08] J. Kempe, H. Kobayashi, K. Matsumoto, B. Toner, and T. Vidick. Entangled Games are Hard to Approximate. *2008 49th Annual IEEE Symposium on Foundations of Computer Science*. 2008, pp. 447–456.

[KST22] S. Kundu, J. Sikora, and E. Y.-Z. Tan. A device-independent protocol for XOR oblivious transfer. *Quantum* 6 (2022), p. 725. ISSN: 2521-327X.

[KT22] S. Kundu and E. Y.-Z. Tan. *Device-independent uncloneable encryption*. https://arxiv.org/abs/2210.01058. 2022.

[LMT20] N. Lütkenhaus, A. Marwah, and D. Touchette. Erasable Bit Commitment From Temporary Quantum Trust. *IEEE Journal on Selected Areas in Information Theory* 1.2 (2020), pp. 536–554.

[MR11] U. Maurer and R. Renner. Abstract Cryptography. *The Second Symposium on Innovations in Computer Science, ICS 2011*. Tsinghua University Press, 2011, pp. 1–21.

[PAB+09] 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 (2009), p. 045021. ISSN: 1367-2630.

[PR14] C. Portmann and R. Renner. *Cryptographic security of quantum key distribution*. https://arxiv.org/abs/1409.3525. 2014.

[Rao08] A. Rao. Parallel Repetition in Projection Games and a Concentration Bound. *Proceedings of the Fortieth Annual ACM Symposium on Theory of Computing*. STOC '08. Association for Computing Machinery, 2008, 1–10. ISBN: 9781605580470.

[Raz95] R. Raz. A Parallel Repetition Theorem. *Proceedings of the Twenty-Seventh Annual ACM Symposium on Theory of Computing*. Las Vegas, Nevada, USA, 1995, 447–456. ISBN: 0897917189.

[Ren05] R. Renner. Security of Quantum Key Distribution. PhD thesis. ETH Zürich, 2005.

[SCA+11] J. Silman, A. Chailloux, N. Aharon, I. Kerenidis, S. Pironio, and S. Massar. Fully distrustful quantum bit commitment and coin flipping. *Physical Review Letters* 106 (2011), p. 220501.

[TL17] M. Tomamichel and A. Leverrier. A largely self-contained and complete security proof for quantum key distribution. *Quantum* 1 (2017), p. 14. ISSN: 2521-327X.

[Unr14] D. Unruh. Revocable Quantum Timed-Release Encryption. *Advances in Cryptology – EUROCRYPT 2014*. 2014, pp. 129–146. ISBN: 978-3-642-55220-5.

[VCRŠ20] B. van der Vecht, X. Coiteaux-Roy, and B. Škorić. *Can't Touch This: unconditional tamper evidence from short keys*. https://arxiv.org/abs/2006.02476. 2020.

[Vid17] T. Vidick. *Parallel DIQKD from parallel repetition*. https://arxiv.org/abs/1703.08508. 2017.

[VPR19] V. Venkatesh, C. Portmann, and L. del Rio. Composable security in relativistic quantum cryptography. *New Journal of Physics* 21.4 (2019), p. 043057.

[Wie83] S. Wiesner. Conjugate Coding. *SIGACT News* 15.1 (1983), 78–88. ISSN: 0163-5700.