arXiv:2210.01058v5 [quant-ph] 30 Dec 2024

Device-independent uncloneable encryption

Srijita Kundu * Ernest Y.-Z. Tan †

December 31, 2024

Abstract

Uncloneable encryption, first introduced by Broadbent and Lord (TQC 2020) is a quantum encryption scheme in which a quantum ciphertext cannot be distributed between two non-communicating parties such that, given access to the decryption key, both parties cannot learn the underlying plaintext. In this work, we introduce a variant of uncloneable encryption in which several possible decryption keys can decrypt a particular encryption, and the security requirement is that two parties who receive independently generated decryption keys cannot both learn the underlying ciphertext. We show that this variant of uncloneable encryption can be achieved device-independently, i.e., without trusting the quantum states and measurements used in the scheme, and that this variant works just as well as the original definition in constructing quantum money. Moreover, we show that a simple modification of our scheme yields a single-decryptor encryption scheme, which was a related notion introduced by Georgiou and Zhandry. In particular, the resulting single-decryptor encryption scheme achieves device-independent security with respect to a standard definition of security against random plaintexts. Finally, we derive an "extractor" result for a two-adversary scenario, which in particular yields a single-decryptor encryption scheme for single bit-messages that achieves perfect anti-piracy security without needing the quantum random oracle model.

1 Introduction

A fundamental difference between classical and quantum information lies in the fact that quantum information cannot be perfectly copied. This property can be used to do cryptography, as was noted by Wiesner [Wie83], who gave the first scheme for *quantum money* which cannot be forged. Later [Got03] considered the question of whether in the context of encryption schemes, one could construct a form of *uncloneable encryption*; i.e. quantum ciphertexts that in some sense cannot be copied. Pursuing this line of reasoning, [Got03] developed an encryption scheme in which an adversary attempting to copy a quantum ciphertext would be caught with high probability by the intended (honest) recipient. Following up on a question posed in that work, [BL20]

*Institute for Quantum Computing and Department of Combinatorics and Optimization, University of Waterloo, Waterloo, Ontario N2L 3G1, Canada. srijita.kundu@uwaterloo.ca

†Institute for Quantum Computing and Department of Physics and Astronomy, University of Waterloo, Waterloo, Ontario N2L 3G1, Canada. yzetan@uwaterloo.ca

subsequently constructed an encryption scheme achieving a slightly different notion of uncloneable encryption[1], namely a quantum ciphertext that cannot be distributed amongst two parties in such a way that they can both decrypt the message with high probability (after obtaining the decryption key).

An uncloneable encryption scheme needs to satisfy a standard notion of indistinguishability (or semantic security) that any encryption scheme needs to satisfy. Aside from this, [BL20] introduced two notions of security that an uncloneable encryption scheme should satisfy: uncloneability and uncloneable-indistinguishability. The uncloneable encryption scheme given [BL20] was a simple construction based on Wiesner states and monogamy of entanglement games. While this scheme achieved uncloneability in the plain model, it did not achieve uncloneable-indistinguishability, even in the quantum random oracle model (QROM).

Following [BL20], there have been several subsequent works on uncloneable cryptography. [MST21] showed that uncloneable-indistinguishability cannot be achieved by schemes using certain kinds of states, and other limitations of the proof techniques employed in [BL20]. [AK21] considered public-key uncloneable encryption; [GMP23] gave a protocol for uncloneable encryption based on the post-quantum hardness of the learning with errors (LWE) problem. Recently, [AKL+22] gave a more complicated uncloneable encryption protocol based on subset coset states that achieves uncloneable-indistinguishability in the QROM. Moreover, [AKL+22] also gave some impossibility results showing that certain kinds of schemes cannot achieve uncloneable-indistinguishability in the plain model. The concept of uncloneable decryption keys, or single-decryptor encryption, was introduced by [GZ20], which takes a reversed perspective compared to uncloneable encryption: here a quantum decryption key is made uncloneable rather than a ciphertext, with the security requirement being only a single party should be able to use the decryption key to decrypt a classical ciphertext. [GZ20] showed that single-decryptor encryption is equivalent to uncloneable encryption under a certain security definition, but other definitions of single-decryptor encryption have also been considered, see e.g. [CLLZ21].

As noted in [BJL+21], uncloneable encryption can be considered the second level in the hierarchy of uncloneable objects, since it makes *information* uncloneable. The first level of the hierarchy only lets us verify the authenticity of objects: this is where private-key quantum money lies. At the top level of the hierarchy, *functionalities* are made uncloneable: this includes quantum copy protection and secure software leasing. It would be natural to ask if higher levels of the hierarchy can be used to achieve lower levels. Indeed, [BL20] showed that uncloneable encryption can be used to construct private-key quantum money. More surprisingly, it has been shown [CMP24, AK21] that uncloneable encryption can be used to construct quantum copy protection of a certain class of functions, although these constructions require either the QROM [CMP24] or additional computational assumptions [AK21].

Device-independence. The results in [Got03, BL20] were derived in a *device-dependent* setting, in which it is assumed that any honest parties can generate trusted states and/or perform trusted measurements. However, it was observed in e.g. [BHK05, AGM06, PAB+09] that in some situations, one can construct protocols that are secure under much weaker assumptions: no assumptions on the states and measurements are made except that the measurements of spatially separated parties are in tensor product (or commute). This strong form of security is referred to as the *device-independent* (DI) paradigm, in that security can be achieved (almost) independently of the

[1] [BL20] refer to the scheme in [Got03] as one that achieves *tamper-detection* rather than uncloneability; in this work we follow their terminology rather than the original terminology in [Got03].

underlying operations being performed by the devices used in the protocol. Device-independent protocols that have information theoretic security are often based on the property of *self-testing* or *rigidity* displayed by some non-local games. Suppose a non-local game is played with some unknown state and measurements. If these measurements and state achieve a winning probability close to the optimal winning probability of the game, then self-testing tells us the state and measurements are close to the ideal state and measurements needed to achieve the optimal winning probability for that game.[2] This means that we can do cryptography with this state and measurements as though they were the ideal state and measurements.

We note that in the specific context of uncloneable encryption, the security proofs in [Got03, BL20] do already have a form of "one-sided device-independent" property, in the sense that for the uncloneable encryption scenario the receiver may be dishonest, and hence the security proof must cover the possibility of the receiver not performing the intended operations. However, our goal in this work is to extend the device-independence to cover the client's devices as well (we briefly elaborate on how the [BL20] scheme is insecure in the fully DI setting in Section 1.1 below). This is somewhat similar to the scenario considered by [GMP23] (for which they achieve polynomial rather than exponential security), except that in their scenario, while the states and measurements are indeed not trusted, it is still assumed that the devices are computationally bounded. Due to this, the security achieved in their scenario is not information theoretic, but under the assumption that the LWE problem cannot be solved by polynomial-time quantum computers. Hence thus far, there has not been an uncloneable encryption scheme in the "standard" fully DI scenario, without computational assumptions.

1.1 Our results

In this work, we develop protocols for a modified version of uncloneable encryption (of classical messages), which we term *uncloneable encryption with variable keys* (VKECM), as well as single-decryptor encryption — see Remark 1 below for comments regarding the security definitions used. Our main contribution is to show that these protocols fulfill a standard notion of DI security, i.e. without computational assumptions, which has not been achieved in any previous work. (As mentioned above, [GMP23] is the only work achieving anything similar to DI security, but their result required computational assumptions; furthermore, our result is also stronger in the sense that it achieves exponential security rather than polynomial security as in that work.) While VKECM differs from the usual notion of uncloneable encryption, we note in particular that it is at least still sufficient to yield a quantum money scheme that is secure in the standard fully DI setting, as we discuss later.

Remark 1. *Currently, there are multiple competing security definitions in the literature for uncloneable encryption and single-decryptor encryption. We do not aim to provide a detailed comparison of the different definitions within the scope of this work, as they are fairly technical, though we discuss some of them briefly in Section 3 when specifying the definitions we chose to use. We highlight however that for uncloneable encryption, we are not studying the standard notion but are instead focusing on the modified version VKECM described below, and hence we have to introduce appropriate new security definitions for VKECM rather than the standard form of uncloneable encryption. Still, we note that they are similar in spirit to those used*

[2] In this work, for simplicity of presentation we use the self-testing results described in [MYS12] which have closed-form expressions; however, there would be no obstacles in principle if one were to instead use the more robust bounds computed in [BNS+15] using semidefinite programming. The latter approach can give bounds that are quite robust to non-maximal winning probabilities on the non-local game.

in the work [GMP23] on uncloneable encryption, and still suffice to yield a DI quantum money scheme as we discuss later. As for single-decryptor encryption, we choose to follow essentially the security definitions used in [CLLZ21, LLQZ22].

Uncloneable encryption with variable keys. In our modified version of uncloneable encryption, the idea is that a particular ciphertext can be decrypted with several possible decryption keys, and each adversary in a cloning attack gets an independently generated decryption key. To further illustrate what we mean, we shall discuss this in the context of the uncloneable encryption scheme based on Wiesner states given by [BL20]. (We stress that this is merely an example to demonstrate the key ideas, and VKECM is not restricted to such a specific implementation — for a general formulation of VKECM, refer to Section 3.1.) For $a, x \in \{0,1\}$, we shall use $|a^x\rangle$ to denote the state $H^x |a\rangle$, where H is the Hadamard matrix that takes the computational basis to the $|+\rangle, |-\rangle$ basis. For $a, x \in \{0,1\}^n$, we shall use $|a^x\rangle$ to denote $\bigotimes_{i=1}^n |(a^i)^{x_i}\rangle$. These $|a^x\rangle$ states are called Wiesner states. The basic encryption scheme (without using the QROM) in [BL20] is as follows: the ciphertext corresponding to a message m of n bits is $(m \oplus a, |a^x\rangle)$, for uniformly random x and a, and the decryption key is x. On getting x, a single party can measure the quantum part of the ciphertext in the bases indicated by x to recover a, and hence m. However, because the Wiesner states satisfy a monogamy of entanglement property [TFKW13], two parties cannot simultaneously do this.

Note that in the scheme described above, the string a which is generated really is a "private key"[3] that is required to do the encryption procedure, but which cannot be revealed to any party if any kind of security is desired. Fortunately, after the encryption procedure is completed, a does not need to be stored; only the string x, which is completely independent of a, needs to be stored and possibly released later as a decryption key.

Now consider the following modification: we still use Wiesner states $|a^x\rangle$, but we cannot use all the bits of a as a one-time-pad for the message — in fact we require that each party that wants to decrypt the message has to learn a different (independently generated) subset of the bits of a in order to do so. The reasons we need to do this are technical and have to do with the proof style based on parallel repetition we use (we shall expand more on this in Section 1.2), but it can be achieved by modifying the protocol in the following way. If the message length is n bits, the Wiesner states will now be l bits, for $l > n$. The ciphertext will be $(m \oplus r, |a^x\rangle)$, where r is a uniformly random string of n bits. (r, a, x) will all need to be stored as private key now, and there will be a "key release" procedure that takes the private key and generates a decryption key with a random subset T of $[l]$ of size n. An instance of the decryption key is $(r \oplus a_T, T, x_T)$, and each time a decryption key is released from the decryption procedure, T is generated independently. Obviously this means there are many possible decryption keys, corresponding to different values of T. A single decryptor given the decryption key and using $|a^x\rangle$ can learn r, and thus can learn m using the classical part of the ciphertext. This also satisfies the property we required, that if two parties both want to learn the message, they have to learn independent subsets of the bits of a.

Our full DI scheme for achieving uncloneable encryption with variable keys is very similar to the modified version of the [BL20] scheme described above, except with a "testing" step to obtain

[3] To avoid confusion: note that here we do not use the term "private key" in the same sense as in a public key encryption procedure.

DI security[4] — basically, we play a nonlocal game on a random subset of the rounds, with the informal goal of ensuring that the devices cannot both win the nonlocal game on those rounds with high probability and still be able to usefully clone the resulting states. (Note, however, that our results are *not* based on parallel self-testing theorems; rather, the only place we invoke self-testing is to study a single protocol round, after which we separately derive a parallel-repetition theorem to analyze the entire protocol. In particular, this means that in principle one could substitute the self-testing argument with other methods for analyzing single protocol rounds.)

We provide a formal definition of uncloneable encryption with variable keys and its related security criteria in Section 3.1. As indicated in the illustrative example above, the main difference between our definition and that introduced by [BL20] is that the whole private key that was used in the encryption needs to be stored, and there is a key release procedure that takes the private key as input, uses additional private randomness, and outputs an independent decryption key each time one is requested (here by independent we mean the additional private randomness is independent for each decryption key). Additionally, since we work in the DI setting, our encryption procedure involves a small amount of interaction[5] to implement the "testing" step, and we include an option to abort the procedure if this test fails. Such features are typically required in DI cryptography protocols, which rely on rigidity properties of various interactive procedures (such as non-local games, taking into account the need to check whether the game is won) to "test" if the device behaviour is close to the ideal case, as mentioned above. For instance, such interaction was also present in the [GMP23] scheme, which was DI under computational assumptions.[6]

Under those definitions, our main result regarding the achievability of DI uncloneable encryption with variable keys is stated in Theorem 14, and the scheme achieving this is described in Scheme 1. Some additional notable features of our scheme are as follows:

- The uncloneable encryption scheme of [GMP23], which is device-independent with computational assumptions, allows for some noise in the devices, but their approach requires the noise parameter to vanish in the limit of large message length n. In contrast, our protocol tolerates a *constant* level of noise in the honest devices. (For the device-dependent uncloneable encryption schemes, to our knowledge none of them have explicitly analyzed noise in the devices, though it should be possible to modify some of the schemes to account for this.)

- Most DI cryptographic protocols that guarantee information theoretic security require that there is no communication between the devices of different parties involved in the protocol. Our security proof is based on the parallel repetition of a form of a non-local game; it was

[4] To see that the [BL20] scheme does not work if the state preparation is untrusted, observe that if the state prepared is simply a classical record of the values (a, x) rather than the Wiesner states $|a^x\rangle$, then it is trivially insecure. If converted to an entanglement-based protocol in which the client performs some choice of measurement x and obtains an output a, observe that if the client's measurements are untrusted, then the devices could just be implementing a completely classical strategy in which for each round the output a is perfectly deterministic for each x, in which case all dishonest parties will know the value of a once given x. (If desired, this deterministic behaviour could be made undetectable by any statistical checks involving only the frequency distribution of a and/or x, by instead making the value of a for each x a function of some classical "hidden variable" Λ, a copy of which is held by all dishonest parties.)

[5] However, this interaction can potentially be removed if the client can impose some additional constraints on their devices; we elaborate on this in Remark 7.

[6] We stress however that despite this interactive aspect, we do *not* assume the receiver has to be honest in our setup. While a dishonest receiver could of course lie about the outputs of their devices, this poses no problems for a DI security proof, because such behaviour can always be absorbed into the operations/measurements performed by the dishonest party — this line of reasoning has been used in many previous works on cryptographic scenarios with some potentially dishonest receiver (including uncloneable encryption) such as [FM18, GMP23, KT23]. (See also Remark 2 later below.)

shown in [JK22] that proofs based on parallel repetition can tolerate a small (but linear in n) amount of communication, or leakage, between the devices of all parties involved. We give a simpler proof, inspired by the lower bound of quantum communication complexity in terms of the quantum partition bound in [LLR12], to show that our scheme tolerates leakage between the client and the receiver during the encryption procedure, and between two parties who are both trying to decrypt the message in a cloning attack. This makes our security criterion qualitatively different from that considered in [BL20] (even after accounting for the fully DI setting we consider), since the two parties in a cloning attack no longer have to be non-communicating — any communication between the parties can obviously also be considered leakage between their devices. We only require that the total number of bits thus leaked be bounded. Our argument could also be adapted to obtain device-dependent schemes for uncloneable encryption that can tolerate some communication between the two parties in a cloning attack.

Application to quantum money. Although our aim in constructing this modification of uncloneable encryption was to be able to prove DI security via proof techniques for parallel repetition, we believe that the modified definition can still be useful. For instance, it can be used just as well as the original notion of uncloneable encryption to get private key quantum money. The approach here is the same as that sketched in [BL20]. Basically, a bank could produce a banknote by encrypting a random string M using our procedure, then storing the private key as well as M in its internal records, and placing the quantum ciphertext in the banknote. To verify a banknote, the bank would use the private key to run the key release procedure and generate a decryption key, then use this to decrypt the state in the banknote and check whether the output matches M. Our security definition for uncloneability immediately implies that if an adversary attempted to clone the banknote and submit it to two separate bank locations for verification (each of which independently runs the key release procedure), the probability of both being accepted[7] is exponentially small.

Since our scheme is secure in the DI setting, this means the above approach yields a method for obtaining DI quantum money.[8] We note that it does seem possible that another approach for DI quantum money would be to slightly modify existing protocols for DI quantum key distribution; however, there may be some benefits to using the approach in this work. In particular, while our analysis above does not say anything about what happens if the bank returns successfully verified banknotes (rather than destroying them and generating fresh ones), the proof techniques we use here should be modifiable to allow a security proof for a scheme that returns successfully verified banknotes a fixed number of times, chosen at the point of generation of the banknote.

Single-decryptor encryption. In single-decryptor encryption of classical messages (SDECM), a key generation process first produces an encryption key and a quantum decryption key; the decryption key is then given to a dishonest party, while the encryption key is stored with the honest party. The requirement is that two parties between whom the dishonest party has distributed the decryption key cannot both decrypt a message (or two independent messages) that have been encrypted with the encryption key. A simple change of perspective in the Wiesner state protocol for uncloneable encryption gives us a single-decryptor encryption protocol: here $|a^x\rangle$ will be the decryption key, (a, x) the encryption key (note here the difference with uncloneable encryption,

[7] More precisely, the probability of both banknotes being accepted *and* the original encryption procedure accepting as well.

[8] This approach avoids an impossibility result for DI quantum money derived in [HS20], because we are considering a somewhat different setup from that work.

where only x needed to be stored), and messages will be encrypted with (a, x) as $(m \oplus a, x)$.

In general the encryption procedure for single-decryptor encryption is allowed to use randomness outside of the encryption key in order to encrypt a message (indeed, this was the case in some of the schemes described in [GZ20]). This has given rise to different possible security definitions, depending on whether the two parties who are challenged to decrypt should receive the same message encrypted using the same additional randomness, or whether the messages and randomness should be independent. Again, we defer the full details to Section 3.2 rather than this introductory section, but to give a brief overview, [CLLZ21, LLQZ22] considered a definition where the two parties receive encryptions of independent messages using independent randomness, i.e. they receive different ciphertexts. On the other hand, [GZ20] considered a definition where the two parties receive encryptions of the same message using the same additional randomness, i.e., when they both receive the same ciphertext, and furthermore showed that this is equivalent to uncloneable encryption under a particular security definition.[9]

We believe that single-decryptor encryption under the security definition of [CLLZ21] should be equivalent to our definition of uncloneable encryption with variable keys, using essentially the same reduction as [GZ20], though we do not attempt to formally prove this claim. Instead, we directly prove that a very straightforward modification of our DI protocol for uncloneable encryption with variable keys, in essentially the same manner as the Wiesner state protocol, achieves single-decryptor encryption under a definition similar to [CLLZ21] (see Section 3.2 for detailed definitions).

Single-decryptor encryption of bits and trits. For single-bit or single-trit messages specifically, we are also able to modify the above single-decryptor encryption scheme in such a way that (under the independent-message security definition) the adversaries' probability of guessing the messages is at most only negligibly larger than the trivial value. This is a stronger security property than that of the above scheme (where the adversary's guessing probability is only exponentially small in the message length — see Section 3.2 for more precise details), and furthermore we obtain it without using the QROM, in contrast to previous work.[10] The idea here is as follows: suppose the probability for two adversarial parties to simultaneously guess some "raw" l-bit strings is exponentially small in l, but larger than 2^{-l}. Now, we would ideally like to "extract" a single bit such that the probability of the two parties simultaneously guessing it is $\frac{1}{2} + \mathrm{negl}(l)$.[11] If there had just been one party instead of two, then this would be achievable by using randomness extractors [TSSR11, DPVR12]; however, the proof techniques in those works do not seem to straightforwardly generalize to two parties. The difficulties with using extractors against two parties were noted in [AKL+22], although using randomness extractors was not ruled out by the impossibility results in the same work.

In the setting of single-decryptor encryption (under the independent-message security defi-

[9] It is actually possible to consider variations of the security definition other than those in [GZ20] and [CLLZ21]: one can make either or both of the message and the additional randomness used in encryption for the two parties independent or identical. We discuss these issues in more detail in Section 3.2.

[10] After the publication of the preprint of this work (in which our focus was on applying this idea for VKECM), a similar result was independently obtained in [AKL23]. We have since identified a flaw in our application of this idea in VKECM, which we elaborate on in this updated manuscript (see Remark 9). However, we found that it could still be used in single-decryptor encryption to obtain a similar result to [AKL23], and present this finding in this updated version.

[11] This part of our analysis does not depend significantly on the exact scaling of the function $\mathrm{negl}(l)$; when applying it in our protocol, it will be an exponentially small function (since we achieve exponential rather than polynomial security), though larger than 2^{-l}.

nition), our method to overcome this difficulty is to design our scheme such that it involves implementing randomness extractors with *different* random seeds for the two parties. Specifically, we shall use the inner product function, which is known to be an extractor. If the two parties cannot guess x with high probability from a shared state $|\rho\rangle_x$, we prove that the probability that one party guesses $x \cdot v^1$ and the other guesses $x \cdot v^2$, where v^1 and v^2 are independently generated from the uniform distribution over $\{0,1\}^l$, is at most $\frac{1}{2} + \text{negl}(l)$.[12] Instead of going via the standard arguments for extractors, our argument for this is done similar to the quantum version of the Goldreich-Levin theorem for hardcore bits [AC02]. The idea is that if the probability of the parties guessing $x \cdot v^1$ and $x \cdot v^2$ averaged over v^1, v^2 is more than $\frac{1}{2} + \text{negl}(l)$, then they can independently run the Bernstein-Vazirani algorithm on their halves of the shared state, to both guess the entire string x with too high a probability. Note that since the two parties need to run the Bernstein-Vazirani algorithm independently, this argument does not work if we consider the probability of both parties learning $x \cdot v$ for the same v.

This argument generalizes to trits as well, but it does not seem to extend to longer bit strings. The implication of this result is that for single-decryptor encryption, we have "perfect" anti-piracy security (see Section 3.2 for formal definitions) for single-bit or single-trit messages, which in turn also implies CPA-style security for such messages. We remark that in principle, one could make a similar modification to our scheme for uncloneable encryption with variable keys, to attempt to obtain uncloneable bits or trits. However, there is a subtle issue that arises in the attempt, and hence we were unable to prove security of the resulting scheme — we discuss this difficulty further in Remark 9 later, along with the relevant properties that would need to be proven in order to obtain such a result.

1.2 Technical overview

In this section, we give an overview of how we construct our DI uncloneable encryption with variable keys (DI-VKECM) scheme, and how we prove its security. All the arguments in this section are for proving uncloneability. In the context of VKECM, uncloneability is the requirement that if the encryption of a uniformly random message gets distributed between two parties, say Bob and Charlie, then the average probability that both of them guess the message given access to independently generated decryption keys, is exponentially small in the number of bits in the message.

Proving security by analyzing a non-local game. The first thing to notice is that the Wiesner states correspond to the states after the measurement of one of the parties (let's say Alice) in the CHSH non-local game. Therefore, we can consider doing something very similar to many protocols for DI quantum key distribution (QKD) [PAB+09]. During the encryption process, the client (who is honest) and the receiver (who may be dishonest) will share states compatible with some l copies of the CHSH game. On some of these copies, the CHSH game will be self-tested, and the rest will be used for encryption. The idea is that, if a random subset is used for self-testing, the dishonest receiver, who had to have prepared the devices beforehand, would have had to actually prepare i.i.d. copies of the ideal CHSH state and measurements (up to some amount of noise per

[12] The argument also works if there are two (possibly correlated) strings x^1 and x^2, and we have a bound on one party learning x^1 and the other party learning x^2 from $|\rho\rangle_{x^1 x^2}$, which will be the case in our actual setting. Here we can upper bound the probability of the parties learning $x^1 \cdot v^1$ and $x^2 \cdot v^2$ respectively.

copy) in order to pass the self-testing check.[13]

However, there is one key aspect in which the situation here differs from that in QKD. In a DIQKD protocol, measurements corresponding to all copies of the game in question can be done at once, and then the Serfling bound can be applied to the resulting input-output distribution, in order to say something about the entire distribution from what is observed in the self-testing subset of inputs and outputs. However, for uncloneable encryption, measurements corresponding to the copies of the game which will be used for encryption cannot be done at the same time as the testing subset; in an honest implementation, these states need to remain unmeasured because the ciphertext needs to be quantum. Thus there is no fixed distribution on which the Serfling bound can be applied.

Because of the above problem, we shall instead use a two-round non-local game[14] whose first round is played between two players Alice and Barlie, and the second round is played between two players Bob and Charlie, between whom Barlie's portion of the state at the end of the first round gets distributed (Alice's portion of the state at the end of the first round remains untouched). We call this game the cloning game CLONE_γ. We describe a single instance of the game first; we shall actually need the parallel-repeated version of the game for the security proof. In the first round of a single instance of the game, Alice will receive a uniformly random single-bit input, and Barlie will receive a trit in $\{0, 1, \text{keep}\}$, with "keep" occuring with probability $(1-\gamma)$. The input "keep" to Barlie indicates that the CHSH game will not be tested, and in this case the first round is automatically won; otherwise, Alice and Barlie's inputs are the same as the inputs of the CHSH game, and they need to produce outputs that satisfy the CHSH winning condition. If Barlie did not get "keep" in the first round, the second round is automatically won; otherwise Bob and Charlie get the same input as Alice did in the first round of the game, and they both have to guess Alice's output bit from the first round. Note that Alice gets the same input regardless of Bob's input, and in the honest case, if she gets input x and produces output a in the first round, the state on Barlie's side is $|a^x\rangle$. If the first round is won with high enough probability, then the state after the first round on Barlie's side is close to $|a^x\rangle$, which means by the monogamy of entanglement property of Wiesner states, we can upper bound the probability that Bob and Charlie can guess a given x. This means that the overall winning probability of CLONE_γ is bounded away from 1. The style of argument we employ here is similar to what was considered in [ACK+14, KST22] for two-party cryptography, although parallel repetition was not considered in those works.

When we consider the parallel-repeated CLONE_γ, i.e., l i.i.d. copies of CLONE_γ, a constant fraction of the instances (in expectation) will be tested in the first round, and the rest can be used for encryption. The ciphertext in this case will be the state after the first round on Barlie's side (which in the honest case is a Wiesner state of the form $|a_S^{x_S}\rangle$, where x and a and Alice's first

[13] In principle, one might be able to use some other non-local game with self-testing properties; however, the CHSH game is particularly convenient since (after Alice's measurement) the ideal strategy produces exactly the Wiesner states. We also note that the monogamy of entanglement game from [TFKW13] (which was used in the [BL20] security proof) was shown to have some self-testing properties as well [BC23]. However, to our knowledge all self-testing properties of that game are derived for the "one-sided DI" scenario where Alice's operations are trusted, and hence it is unclear whether they could be applied to obtain a fully DI protocol.

[14] While we refer to this as a non-local game for brevity, we note that strictly speaking it does not fall within the "standard" framework of non-local games (in which there is no communication between the parties), because in our scenario the player Barlie sends or distributes states to the players Bob and Charlie *after* receiving some inputs. It would be convenient if we could have analyzed some three- or four-player non-local game in the "standard" sense; however, some sort of communication between parties seems unavoidable in order for us to be able to relate this game to the task of uncloneable encryption (similar to the situation for monogamy of entanglement games in [TFKW13, BL20]). We specify the exact order in which the players can share or distribute states in our full game description in Section 4.

round inputs and outputs, and S is the subset on which Barlie's first round input was "keep"), along with the classical string $m \oplus a_S$. If we can prove that the winning probability of the parallel-repeated CLONE$_\gamma$ decreases exponentially in n, then we could prove the uncloneability of this scheme. Note that the scheme as described here is actually an uncloneable encryption scheme in the original sense of [BL20], since x_S is the only decryption key.

Parallel repetition of the cloning game. Unfortunately, we cannot prove a parallel repetition of the game CLONE$_\gamma$ as described. What we can prove a parallel repetition theorem for is a modified version of CLONE$_\gamma$ which is "anchored". The anchoring transformation we use is similar to those used in [Vid17, KT23]. Essentially, the anchoring property requires that Bob and Charlie's second round inputs cannot be perfectly correlated with Alice's first round input, or each other — with some small probability, these distributions need to be product instead. We do this by giving Bob and Charlie independently "blank" inputs rather than x_i on some instances, and then not using those instances for encryption for them (this corresponds to the second round being won for free on these instances of the game) — this forces us to use the additional random string r in the ciphertext as described earlier, with $(r \oplus a_{T\cap S}, x_{T\cap S}, T)$ being a decryption key for random T. This now places us in the setting of VKECM.

We can prove a parallel repetition theorem for the anchored version of CLONE$_\gamma$, which we denote by CLONE$_{\gamma,\alpha}$ for anchoring parameter α, similar to how a parallel repetition theorem for a different two-round game was proved in [KT23]. The game considered in [KT23] had only two players in both rounds, so in our proof we require some additional steps to take care of the two players Bob and Charlie, between whom Barlie's state is divided after the first round. We use the information theoretic framework for parallel repetition that was introduced by [Raz95, Hol07]. In this framework, we consider a strategy for l copies CLONE$_{\gamma,\alpha}$ and condition on the event $\mathcal{E}$ of the winning condition being satisfied on some $C \subseteq [l]$ instances. We show that if $\Pr[\mathcal{E}]$ is not already small, then we can find another coordinate in $i \in \overline{C} = [l] \setminus C$ where the winning probability conditioned on $\mathcal{E}$ is bounded away from 1. The proof is by contradiction: we show that if the probability of $\mathcal{E}$ is large and the probability of winning in i conditioned on $\mathcal{E}$ is not bounded away from 1, then there is a stategy for a single copy of CLONE$_{\gamma,\alpha}$, whose winning probability is higher than the maximum winning probability of CLONE$_{\gamma,\alpha}$. This is done by defining a state representing the inputs, outputs and shared entanglement in the strategy for CLONE$^l_{\gamma,\alpha}$, conditioned on $\mathcal{E}$. When Alice, Barlie, Bob and Charlie's inputs for the i-th instance of CLONE$_{\gamma,\alpha}$ are x_i, u_i, y_i, z_i respectively, we denote this state by $|\varphi\rangle_{x_iu_iy_iz_i}$. The state $|\varphi\rangle_{x_iu_iy_iz_i}$ is such that the distribution obtained by measuring the corresponding i-th output registers on it is the distribution of outputs in the original strategy for the inputs $x_iu_iy_iz_i$, conditioned on the event $\mathcal{E}$. Therefore, if the probability of winning in the original strategy conditioned on $\mathcal{E}$ is too high, and the players are able to output from the state $|\varphi\rangle_{x_iu_iy_iz_i}$ (or close to this distribution) in a single instance of CLONE$_{\gamma,\alpha}$, they can win the single instance with too high probability.

The rest of the proof will thus involve showing how the players can provide outputs that are close to the output distribution in $|\varphi\rangle_{x_iu_iy_iz_i}$ when playing a single instance of CLONE$_{\gamma,\alpha}$. Let us denote the blank inputs to Bob and Charlie in the second round by $\perp$, so that $|\varphi\rangle_{x_iu_i\perp\perp}$ is $|\varphi\rangle_{x_iu_iy_iz_i}$ when they both get this blank input. The first thing to note is that there exists some i such that the distribution of Alice and Barlie's first round outputs is almost the same in $|\varphi\rangle_{x_iu_i\perp\perp}$ and $|\varphi\rangle_{x_iu_iy_iz_i}$ for any y_iz_i. This is because the distributions were exactly the same originally (because the first round outputs were produced without access to y_iz_i), and conditioning on $\mathcal{E}$ does not change the distribution too much (because we have assumed the probability of $\mathcal{E}$ happening is not too small). So in the first round, Alice and Barlie could jointly produce the state $|\varphi\rangle_{x_iu_i\perp\perp}$ on getting inputs

x_i, u_i, and measure its output registers to give their first round outputs. The distribution of $X_i U_i$ conditioned on $Y_i = \perp, Z_i = \perp$ is product, so we can use an argument very similar to that of [JPY14] to prove a parallel repetition theorem for one-round games with product distributions, to argue that there exist unitaries $V_{x_i}^{\mathrm{A}}$ and $V_{u_i}^{\mathrm{BC}}$ that Alice and Barlie can appear on their registers of a shared state $|\varphi\rangle_{\perp\perp}$ (which is the superposition of $|\varphi\rangle_{x_i u_i \perp\perp}$ over all $x_i u_i$) to get close to $|\varphi\rangle_{x_i u_i \perp\perp}$.

In the second round, Barlie then distributes his registers of the shared state (which is close to $|\varphi\rangle_{x_i u_i \perp\perp}$, except with the i-th first-round output registers being measured) between Bob and Charlie, and also gives them u_i. Because Bob and Charlie's inputs are anchored w.r.t. each other, which means that they are product (with each other and with Alice) with some constant probability, we can show by a similar argument that there exist unitaries $V_{u_i y_i}^{\mathrm{B}}$ and $V_{u_i z_i}^{\mathrm{C}}$ that Bob and Charlie can apply on their registers of $|\varphi\rangle_{x_i u_i \perp\perp}$ to get it close to $|\varphi\rangle_{x_i u_i y_i z_i}$. These unitaries do not act on the output registers from the first round, so we can argue that on average, $V_{u_i y_i}^{\mathrm{B}} \otimes V_{u_i z_i}^{\mathrm{C}}$ also takes $|\varphi\rangle_{x_i u_i \perp\perp}$ conditioned on particular first round output values to $|\varphi\rangle_{x_i u_i y_i z_i}$ conditioned on the same values. Therefore, Bob and Charlie can apply these unitaries on the state they get from Barlie, and provide second round outputs by measuring the i-th second round output registers of the resulting state. This completes the stategy for Alice, Barlie, Bob and Charlie for the single instance of $\mathrm{CLONE}_{\gamma,\alpha}$.

1.3 Discussion and future work

The first question left open by our work is whether it is possible to achieve DI security for the original notion of ECM rather than VKECM. We highlight that it seems necessary to do a parallel rather than sequential (which is the setting where parties enter their inputs and get outputs from their devices one by one, instead of all at once) style of proof here. This is because, while we could ensure that the receiver during the encryption procedure enters the inputs for self-testing into their device one by one, simply by sending the inputs one by one and requiring a reply before supplying the next input (thereby giving the protocol many rounds of interaction), it seems fairly unnatural to enforce this constraint on Bob and Charlie. The only proof technique we have for parallel device-independent settings is parallel repetition, so proving a parallel repetition theorem for a game like the CLONE_γ game we described (the version without anchoring) seems necessary. However, it is not known how to prove an exponential parallel repetition theorem for even one-round two-player non-local games where the inputs of the two players are arbitrarily correlated. The most general exponential parallel repetition theorem known here is also for anchored games [BVY17]. Of course, we do not need to prove a parallel repetition theorem for all possible games, only the specific game CLONE_γ. In our parallel repetition theorem $\mathrm{CLONE}_{\gamma,\alpha}$, we did not make use of any structure in the game except for the input distribution. So it may be possible to prove parallel repetition for CLONE_γ by making use of its specific structure.

The second question we leave open is whether it is possible to extend the "randomness extraction" result we have to more than one bit or trit. As we noted before, our style of proof does not work for bit strings, but could some sort of parallel repetition or composability result be used to prove security for a case where instead of one inner product we have several inner products? Also, there remains the question of whether this "extraction" result can be applied in protocols outside of single-decryptor encryption; in particular, whether it could be used in VKECM (see Remark 9 for further discussion) or even the original ECM.

Finally, there is the question of finding more applications for VKECM. For instance, although

we showed that VKECM can be used just as well as ECM for private key quantum money, we have not studied whether the application to quantum copy protection also works with VKECM. Both constructions of copy protection from uncloneable encryption [CMP24, AK21] are schemes for copy-protecting a class of functions known as *multi-bit point functions*. A point function $f_{a,b}$ evaluates to 0 on all inputs except a special input a, on which it evaluates to a string b. When constructing copy protection from uncloneable encryption, the string a is taken as the decryption key of the uncloneable encryption procedure, and b is the encrypted message. The idea is that two parties among whom the copy-protected program has been distributed, should not both be able to evaluate b when they have a as their input — this is guaranteed by the security of the uncloneable encryption scheme. The question then is: what happens if we try to do these constructions with VKECM instead of ECM? Because there are many possible valid decryption keys in VKECM, does this mean we could copy protect a class of functions different from point functions? We leave all of these interesting questions for future work.

1.4 Organization of the paper

In Section 2, we introduce some notation we shall be using throughout the paper, and describe some preliminaries on probability theory and quantum information. In Section 3, we formally define VKECM, SDECM, and related security criteria; we also describe the device-independent setting and assumptions therein in this section. In Section 4, we formally define the two-round cloning games CLONE_γ and $\mathrm{CLONE}_{\gamma,\alpha}$ and prove that the probability of winning a single instance of it is bounded away from 1. In Section 5, we describe our DI-VKECM scheme and prove its security using the parallel repetition theorem for $\mathrm{CLONE}_{\gamma,\alpha}$. In Section 6, we describe our DI-SDECM scheme and prove it satisfies the security definition used in [CLLZ21, LLQZ22]. In Section 7, we describe how the scheme in Section 6 can be modified to "extract" the randomness in the raw keys, producing a stronger security result for single-bit or single-trit messages. Finally, in Section 8, we prove the parallel repetition theorem for $\mathrm{CLONE}_{\gamma,\alpha}$.

2 Preliminaries

2.1 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 1. *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 2. *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 3. *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,*

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

2.2 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 4 (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 5 (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 6. *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 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 7 (Pinsker's Inequality)**.** *For any two states ρ and σ,*

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

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. For CQ states, the expressions for conditional entropy, relative entropy and mutual information for ρ_{XY} and σ_{XY} given by

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

reduce to

$$\mathsf{H}(Y|X)_\rho = \mathop{\mathbb{E}}_{\mathsf{P}_X} \mathsf{H}(Y)_{\rho_x},$$

$$\mathsf{D}(\rho_{XY}\|\sigma_{XY}) = \mathsf{D}(\mathsf{P}_X\|\mathsf{P}_{X'}) + \mathop{\mathbb{E}}_{\mathsf{P}_X} \mathsf{D}(\rho_{Y|x}\|\sigma_{Y|x})$$
$$\mathsf{I}(Y:Z|X) = \mathop{\mathbb{E}}_{\mathsf{P}_X} \mathsf{I}(Y:Z)_{\rho_x}.$$

When talking about entropies of only the classical variables of a CQ state, we shall sometimes omit the state in the subscript. Additionally, for an event $\mathcal{E}$ defined on the classical variable X of a CQ state, we shall use notation like use $\mathsf{H}(X|\mathcal{E})$ and $\mathsf{H}(X_1|X_2;\mathcal{E})$ to talk about entropies of the event when the classical distribution is conditioned on $\mathcal{E}$.

3 Security definitions

In this section, we formally define VKECM and SDECM in the DI setting. We begin by laying out the form of the devices we consider, and making a formal statement of what it means to have DI security. For this statement, we are following fairly standard conventions in the field of DI cryptography. With this perspective, DI security is a notion analogous to information-theoretic security or computational security, in that it describes a class of possible behaviours for dishonest parties.

Definition 1. *(Device-independent security) Consider any cryptographic scheme involving multiple parties. We say that* devices *for such a scheme consist of objects with the following functionality:*

1. *Initially, each party's device holds a share of some quantum state.*
2. *Each party's device can (possibly more than once) accept a classical input string, which it uses to perform some measurement on its share of the state and produce a classical output string.*
3. *A dishonest party can at any time perform arbitrary quantum operations on its share of the state, including joint operations that involve other registers held by that party.*

We say that a scheme using such devices achieves device-independent (DI) security *(under any security definition required to hold against some class of possible dishonest behaviours) if the class of possible dishonest behaviours includes arbitrary choices of the initial state distributed (and the Hilbert spaces the state is defined on), as well as the measurements performed in point 2,* including *those in honest parties' devices.*

We furthermore say that it achieves DI security against k bits of leakage *if we extend the class of possible dishonest behaviours to allow k occasions at which a classical*[15] *bit is communicated between the devices.*

For brevity, we may refer to a VKECM scheme achieving DI security as a DI-VKECM scheme, and analogously for SDECM, following the same convention as e.g. DIQKD.

Remark 2. *From the perspective of modelling dishonest behaviour, it would seem we should also allow a dishonest party to directly operate on their share of the quantum state in point 2 as well, rather than*

[15]There is essentially no loss of generality in restricting to classical communication, because if quantum communication is desired, the devices can include pre-shared entanglement in the initial quantum state and then use it for quantum teleportation with only classical communication, though this does require 2 classical bits to send 1 qubit of information.

being strictly constrained to supplying inputs to the device in the prescribed fashion. However, the critical observation here is that since we have not placed any constraints on the measurements in the dishonest case, any operations that a dishonest party could perform on the state can equivalently be carried out by the device itself in performing those measurements. Hence there is no loss of generality by focusing on the model presented above.

3.1 Uncloneable encryption with variable keys

We now describe the security definitions we use for uncloneable encryption with variable keys. These definitions are essentially similar to those used in [GMP23], apart from the distinction between the private key and decryption key in our scheme. The definitions in [GMP23] specify a classical client (the honest party). In our case the client will not be classical, but instead needs to have enough quantum capabilities to implement devices as described above (note however that in the honest implementation, the client will only need to perform single-qubit measurements). On the other hand, we shall not be assuming any computational limitations when considering dishonest behaviour (so we can achieve DI security in the sense described above), in contrast to that work.

We remark that while the definitions in [GMP23] differ slightly from those in [BL20], the only differences are basically that the encryption procedure for a message is allowed to be interactive, and are allowed to output an abort symbol, with the protocol not continuing if there is an abort (the probability of not aborting also appears in the security condition).

Definition 2 (Encryption of classical messages with variable keys)**.** *Let λ be a security parameter. An* encryption of classical messages with variable keys *(VKECM) scheme consists of a tuple* $(\mathsf{Enc}, \mathsf{KeyRel}, \mathsf{Dec})$ *such that*

- $\mathsf{Enc}(1^\lambda, m)$ *is a (potentially interactive) protocol between an honest client, who takes as input the security parameter λ and a message m in some message space $\mathcal{M}$, and a potentially dishonest receiver, who takes as input the security parameter λ. The output of the protocol is $(F, K_{\text{priv}}, \rho)$, where F is a flag held by the client which takes values ✓ (accept) or ✗ (reject), K_{priv} is a private key held by the client, and ρ is a quantum ciphertext state held by the receiver on a register we denote as Q.*
- $\mathsf{KeyRel}(k_{\text{priv}})$ *takes as input a private key k_{priv}, and uses some internal randomness to generate and output a decryption key K_{dec}.*
- $\mathsf{Dec}(k_{\text{dec}}, \rho)$ *takes as input a decryption key k_{dec} and a ciphertext state ρ on register Q, and outputs a message value $\widetilde{M} \in \mathcal{M}$.*

We say that a VKECM scheme is efficient if the computations that the client and an honest receiver perform in $\mathsf{Enc}, \mathsf{KeyRel}, \mathsf{Dec}$ *are polynomial time in λ and the length (in bits) of m.*

We require that the VKECM scheme satisfies completeness*: if all steps are carried out honestly, then for any $m \in \mathcal{M}$, we have (in the following statements, terms such as* $\mathsf{Dec} \circ \mathsf{KeyRel} \circ \mathsf{Enc}$ *should be understood as having each procedure acting only on the relevant registers, e.g.* KeyRel *only acts on the private-key output of* Enc*):*

$$\Pr\left[(F = \checkmark) \wedge \left(\mathsf{Dec} \circ \mathsf{KeyRel} \circ \mathsf{Enc}(1^\lambda, m) = m\right)\right] \geq 1 - \text{negl}(\lambda), \tag{1}$$

i.e. the probability of accepting and correctly decrypting the message is high.

Additionally, we impose the condition that for any distribution of a message M, if we let $\sigma_{MQ|F=\text{✗}}$ be the state produced by $\mathsf{Enc}(1^\lambda, M)$ on registers MQ conditioned on $F = \text{✗}$, then we have[16]

$$\sigma_{MQ|F=\text{✗}} = \sigma_{M|F=\text{✗}} \otimes \sigma_{Q|F=\text{✗}}, \tag{2}$$

i.e. when $\mathsf{Enc}(1^\lambda, M)$ aborts, the receiver's state is independent of M.

Remark 3. *In various somewhat similar tasks such as QKD [PR14] or certified deletion with a third-party eavesdropper [KT23], when considering dishonest behaviour we typically also require a* correctness *condition along the following lines: even when the devices are dishonest, the probability that the message is incorrectly decrypted and the protocol accepts is low. In our context however, the only potentially dishonest party is the recipient, and hence it does not make sense to bound this probability for dishonest behaviour: the set of dishonest-receiver behaviours always includes trivial processes where they simply set some random value as the "decrypted message", in which case it is clearly impossible to give any nontrivial bounds on the probability of incorrectly decrypting. (On the other hand, when focusing on the case of honest behaviour, note that the completeness condition (1) indeed incorporates the requirement that the probability of incorrectly decrypting the message is low.)*

We now state the security definitions we use, which are the same as in [GMP23] except with minor modifications to account for the difference in our decryption procedures. First, we aim to capture the notion that an adversary without the decryption key cannot distinguish the message from a "dummy" value:

Definition 3 (Distinguishing attack and indistinguishable security)**.** *A* distinguishing attack *on a VKECM scheme is a process of the following form (here for ease of explanation we take the message space $\mathcal{M}$ to contain a particular value labelled as $\mathbf{0}$ without loss of generality):*

1. *An adversary generates a state on registers ME, where M is a classical register on the message space and E is some (possibly quantum) side-information.*
2. *A uniformly random bit B is independently generated, and used as follows (in which the receiver can behave dishonestly when implementing Enc): if $B = 0$ then $\mathsf{Enc}(1^\lambda, \mathbf{0})$ is performed; if $B = 1$ then $\mathsf{Enc}(1^\lambda, M)$ is performed on the M register produced by the adversary in the previous step. In either case, a flag F, a private key K_{priv}, and a ciphertext state ρ (on a register Q) are produced.*
3. *A measurement is performed on the state on QE to produce a single bit $\hat{B}$.*

A protocol is said to be indistinguishable-secure *if for all distinguishing attacks, we have*

$$\Pr[(F = \text{✓}) \wedge (B = \hat{B})] \leq \frac{1}{2} + \text{negl}(\lambda),$$

where the probability is taken over all randomness in the described procedures.

[16] Here we have differed very slightly from [GMP23], in that for their protocol, when $F = \text{✗}$ the protocol basically stops and no state is produced with the receiver (although in their actual protocol the receiver of course ends up with some quantum state in either case — the state just does not depend on m when $F = \text{✗}$, though it does depend on the key value). The definition we have used is essentially saying the same thing, i.e. ρ does not depend on m if $F = \text{✗}$. In the protocol we design below, when $F = \text{✗}$ the receiver gets the state ρ they would have gotten if $F = \text{✓}$ and the message were some uniformly random "dummy value" m^{fake} which is independent of m. We do this instead of aborting the protocol to simplify the security proof, because this way we do not have to analyze the receiver behaving differently conditioned on the value of F.

Technically, our DI-VKECM protocol in fact satisfies a stronger form of indistinguishability, namely that the ciphertext state is completely independent of the message (because our DI-VCECM protocol basically involves applying a one-time-pad to the message, which serves to perfectly encrypt it). However, we present the definition in the above form for consistency with past work, and also because it is less clear how to formulate an analogous property for cloning and cloning-distinguishing attacks, which we now turn to.

Next, we aim to capture the idea that an adversarial receiver cannot clone the ciphertext such that two parties can later decrypt the message (after receiving decryption keys) without communication:

Definition 4 (Cloning attack and uncloneable security)**.** *A* cloning attack *on a VKECM scheme is a process of the following form:*

1. *A uniformly random message $M \in \mathcal{M}$ is prepared and* Enc *is applied to it (with a potentially dishonest receiver), producing a flag F, a private key K_{priv}, and a ciphertext state ρ (on a register Q).*
2. *An arbitrary channel is applied to the ciphertext state ρ to distribute it between two parties Bob and Charlie.*
3. *Without any further communication between Bob and Charlie except as mediated by leakage via their devices, they receive independently generated decryption keys from $\mathsf{KeyRel}(K_{\text{priv}})$, and use them together with their shares of the state to produce guesses M^{B} and M^{C} respectively for the original message M.*

A protocol is said to be $(t(\lambda), g(\lambda))$-uncloneable-secure *if for all cloning attacks, we have*

$$\Pr[(F = \checkmark) \wedge (M = M^{\text{B}} = M^{\text{C}})] \leq \frac{2^{t(\lambda)}}{|\mathcal{M}|} + g(\lambda),$$

where the probability is taken over the distributions of M and all randomness in the described procedures.

Qualitatively, the smaller the functions $t(\lambda)$ and $g(\lambda)$ are, the "more secure" the protocol is (since the probability of Bob and Charlie guessing the message is smaller). Note that if the protocol also requires that the message is a bitstring of length λ (for instance in the first protocol in [BL20], or the version of our protocol that we describe in Section 5 here), then any $t(\lambda)$ such that $t(\lambda) \geq \lambda$ would be a trivial statement (assuming $g(\lambda)$ is non-negative), since in that case the bound on the guessing probability in the above definition would reach the trivial value of 1. In other words, for such protocols we only have nontrivial results when $t(\lambda) < \lambda$.

Remark 4. *In previous work such as [BL20], the uncloneability definition only required specifying a single function $t(\lambda)$ such that an upper bound of the form $\frac{2^{t(\lambda)}}{|\mathcal{M}|} + \text{negl}(\lambda)$ holds. However, a reviewer has pointed out that such a formulation is not well-posed for the protocols mentioned above where the message is a bitstring of length λ: given any such protocol that achieves $t(\lambda) = \tau\lambda$ for some constant $\tau \in (0, 1)$, the $\frac{2^{t(\lambda)}}{|\mathcal{M}|}$ term would itself be a negligible function of λ, making the split into the $\frac{2^{t(\lambda)}}{|\mathcal{M}|}$ and $\text{negl}(\lambda)$ contributions somewhat ill-defined. We thank the reviewer for pointing out this problem with the previous formulation. For this work, we have chosen to resolve it in our definitions by requiring a specification of* both *the functions $t(\lambda)$ and $g(\lambda)$ in the bound $\frac{2^{t(\lambda)}}{|\mathcal{M}|} + g(\lambda)$. It might perhaps be possible to find a more concise way to address this issue, but we leave this for future work, as it does not affect the qualitative implications of any of our results.*

While the definition of uncloneable security refers to uniformly distributed messages, satisfying the above definition implies analogous properties for messages that are not uniformly distributed; see [BL20].

Finally, for completeness we state a security definition from [BL20] that captures some aspects of both of the preceding properties (though in this work, we will not discuss this security definition in much detail; see Remark 5 below):

Definition 5 (Cloning-distinguishing attack and uncloneable-indistinguishable security)**.** *A* cloning-distinguishing attack *on a VKECM scheme is a process of the following form (here for ease of explanation we take the message space $\mathcal{M}$ to contain a particular value labelled as $\mathbf{0}$ without loss of generality):*

1. *An adversary generates a state on registers ME, where M is a classical register on the message space and E is some (possibly quantum) side-information.*
2. *A uniformly random bit B is independently generated, and used as follows (in which the receiver can behave dishonestly when implementing* Enc*): if $B = 0$ then $\mathsf{Enc}(1^\lambda, \mathbf{0})$ is performed; if $B = 1$ then $\mathsf{Enc}(1^\lambda, M)$ is performed on the M register produced by the adversary in the previous step. In either case, a flag F, a private key K_{priv}, and a ciphertext state ρ (on a register Q) are produced.*
3. *An arbitrary channel is applied to the state on QE to distribute it between two parties Bob and Charlie.*
4. *Without any further communication between Bob and Charlie except as mediated by leakage via their devices, they receive independently generated decryption keys from $\mathsf{KeyRel}(K_{\text{priv}})$, and use them together with their shares of the state to produce bits B' and B'' respectively.*

A protocol is said to be uncloneable-indistinguishable-secure *if for all cloning attacks, we have*

$$\Pr[(F = \checkmark) \wedge (B = B' = B'')] \leq \frac{1}{2} + \mathrm{negl}(\lambda),$$

where the probability is taken over all randomness in the described procedures.

Following [BL20, GMP23], we have stated the above definitions of indistinguishable security and uncloneable-indistinguishable security in terms of the adversary initially generating an arbitrary classical-quantum state on ME, which we shall denote here as ρ^{ini}_{ME}. However, one can argue that without loss of generality, we can restrict to attacks where the value on the M register is deterministic and the state on the E register is trivial (as long as the final measurement in each of the attacks is allowed to be a general POVM). This follows from the following observation: consider any attack that achieves the optimal "success probability" (in the sense of the probability of the event stated at the end of the respective definition). This attack would be based on some initial state ρ^{ini}_{ME}, which is a classical-quantum state and hence equivalent to a classical mixture of states of the form $|m\rangle\langle m|_M \otimes \rho_{E|m}$. Because of this, the success probability of this attack is a convex combination of the success probabilities that would be obtained by preparing the initial state in the form $|m\rangle\langle m|_M \otimes \rho_{E|m}$ for various values of m. By linearity, at least one particular value $m^\star$ must attain the optimal success probability[17], or in other words the same success probability could have been attained by the adversary simply preparing the initial state in the form $|m^\star\rangle\langle m^\star|_M \otimes \rho_{E|m^\star}$.

[17] Furthermore, by observing that if $\rho^{\text{ini}}_{ME} = |\mathbf{0}\rangle\langle\mathbf{0}|_M \otimes \rho_{E|\mathbf{0}}$ then the success probability can only be exactly $1/2$ (since in that case the states produced for either value of B are identical), we see that we can take $m^\star \neq \mathbf{0}$ without loss of generality.

With this attack the state on M is deterministic as claimed; furthermore, since the state on E is now in product with M, we can simply suppose that the state $\rho_{E|m^\star}$ is generated after Enc is applied (and hence absorbed into the subsequent measurements/channels) rather than at the beginning of the attack.

It was shown in [BL20] that the three security properties listed above are somewhat related to each other, as follows:

Lemma 8. *Uncloneable-indistinguishability implies indistinguishability.*

Lemma 9. *If the message space size $|\mathcal{M}|$ is independent of the security parameter λ, then $(0, \mathrm{negl}(\lambda))$-uncloneability implies uncloneable-indistinguishability.*

While the definitions they use differ slightly from ours (because they consider protocols which do not have an abort outcome and do not use variable decryption keys), their arguments carry over straightforwardly to our scenario; we outline the main ideas here.

Proof sketch. For Lemma 8, [BL20] observe that given any distinguishing attack, one can immediately construct a cloning-distinguishing attack that succeeds with the same probability: simply perform the distinguishing attack to produce the classical bit $\hat{B}$, and distribute copies of this value to Bob and Charlie, who output it as their values B', B'' respectively in the cloning-distinguishing attack. Hence the optimal success probability of a distinguishing attack cannot be higher than that for cloning-distinguishing attacks, and referring back to the definitions we see that this means uncloneable-indistinguishability implies indistinguishability.

For Lemma 9, the idea is again similar: given a cloning-distinguishing attack that succeeds with some probability $p \in [0,1]$, [BL20] prove that one can construct a cloning attack that succeeds with probability at least $\frac{2}{|\mathcal{M}|}p$. (We remark that our above observation regarding the structure of optimal cloning-distinguishing attacks can somewhat simplify this proof in [BL20], since without loss of generality we can suppose that the cloning-distinguishing attack starts by simply setting M to a deterministic value.) This implies that the optimal success probability of a cloning-distinguishing attack is at most $\frac{|\mathcal{M}|}{2}$ times greater than that of a cloning attack, and since $(0, \mathrm{negl}(\lambda))$-uncloneability is the statement that the latter is upper bounded by $\frac{1}{|\mathcal{M}|} + \mathrm{negl}(\lambda)$, this gives the desired result as long as $|\mathcal{M}|$ is independent of λ. To see that this approach also applies for our definitions, one simply has to instead consider the states conditioned on $F = \checkmark$, in which case the [BL20] construction gives

$$\Pr[M = M^{\mathrm{B}} = M^{\mathrm{C}} | F = \checkmark] \geq \frac{2}{|\mathcal{M}|} \Pr[B = B' = B'' | F = \checkmark],$$

where the right-hand-side refers to the probabilities in the cloning attack, and the left-hand-side refers to those in the cloning-distinguishing attack constructed from it. Multiplying both sides of this inequality by $\Pr[F = \checkmark]$ and then following the same argument as above gives the desired result for our context. □

Remark 5. *Due to the above reductions, we see that for protocols with $\mathcal{M}$ independent of λ, proving $(0, \mathrm{negl}(\lambda))$-uncloneability would be sufficient to imply the other two properties as well. However, in this work, for messages of arbitrary size (but independent of λ) we only prove $(O(\lambda), \mathrm{negl}(\lambda))$-uncloneability and hence we cannot use this simplification. As for single-bit or single-trit messages, if our result in Section 7 on "extractors" against two adversaries in the single-decryptor encryption setting could be extended*

to the VKECM setting, it might allow a proof of $(0, \mathrm{negl}(\lambda))$*-uncloneability for such messages; however, we were unable to resolve this question within this work (see Remark 9) and hence leave it for future investigation.*

3.2 Single-decryptor encryption

We now describe the security definition we use for device-independent single-decryptor encryption.[18] Like in Definition 2, the syntax will be similar to those in [GZ20, CLLZ21] except the key generation procedure will need to interactive, with the possibility of aborting, in order to achieve device-independence. The notion of security we shall use will be essentially the same as the definition of *random challenge anti-piracy* in [CLLZ21] (Definition 6.5), apart from the modification to account for the abort outcome.

Definition 6 (Device-independent single-decryptor encryption of classical messages)**.** *Let* λ *be a security parameter. A scheme for* single-decryptor encryption of classical messages *(SDECM) consists of a tuple* $(\mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec})$ *such that*

- $\mathsf{KeyGen}(1^\lambda)$ *is a (potentially interactive) protocol between an honest client and a potentially dishonest receiver, both of whom take as input the security parameter* λ*. The output of the protocol is* $(F, K_{\mathrm{enc}}, \rho)$*, where* F *is a flag held by the client that takes values* ✓ *(accept) and* ✗ *(reject),* K_{enc} *is a classical encryption key held by the client, and* ρ *is a quantum decryption key state in a register* Q *held by the receiver.*
- $\mathsf{Enc}(m, k_{\mathrm{enc}}, f)$ *takes as input a message* m *in the message space* $\mathcal{M}$*, an encryption key* k_{enc}*, a flag value* $f \in \{✓, ✗\}$*, and uses additional internal randomness to produce a classical ciphertext* C*.*
- $\mathsf{Dec}(c, \rho)$ *takes as input a ciphertext* c*, a decryption key* ρ*, and outputs a message* $\widetilde{M} \in \mathcal{M}$*.*

We say an SDECM scheme is efficient if the computations that the client and the honest receiver perform in KeyGen, Enc, Dec *are polynomial in* λ *and the length of* m*.*

We require that the SDECM scheme satisfies completeness, i.e., if all steps are carried out honestly, then

$$\Pr\left[(F = ✓) \wedge \left(\mathsf{Dec} \circ \mathsf{Enc}(m, \mathsf{KeyGen}(1^\lambda)) = m\right)\right] \geq 1 - \mathrm{negl}(\lambda), \tag{3}$$

where it is understood that Enc *uses the encryption key and flag produced by* KeyGen*, and* Dec *uses the decryption key state.*

Additionally, we impose the condition that for any value of the encryption key k_{enc}*, the distribution of ciphertexts produced by* $\mathsf{Enc}(m, k_{\mathrm{enc}}, ✗)$ *is independent of* m*; i.e. the ciphertext is independent of the message when* $F = ✗$*.*

SDECM schemes will be required to satisfy indistinguishable security in basically the same way as VKECM, and we shall not define it separately. We now focus on presenting definitions of anti-piracy security (against random challenge plaintexts), based on notions presented in [CLLZ21] (further discussion below).

[18] Similar to the situation for variable-key encryption above, while we use the terms "encryption key" and "decryption key" in the following descriptions, we stress that they do not correspond to the public key and private key respectively in a public-key encryption scheme. In particular, the encryption key in the scheme we design happens to also allow decrypting the ciphertext, so it is certainly not usable as a public-key encryption scheme.

Definition 7 (Pirating attack and anti-piracy security, for identical random challenge plaintexts)**.** *A* pirating attack *on a SDECM scheme is a process of the following form:*

1. $\mathsf{KeyGen}(1^\lambda)$ *is carried out between the client and (dishonest) receiver, producing a flag* F*, an encryption key* K_{enc}*, and a quantum decryption key* ρ*.*
2. *An arbitrary channel is applied to the decryption key state* ρ *to distribute it between two parties Bob and Charlie.*
3. *A uniformly random message* $M \in \mathcal{M}$ *is prepared. Without any further communication between Bob and Charlie except as mediated by leakage via their devices, they receive independently generated instances of* $\mathsf{Enc}(M, K_{\text{enc}}, F)$*, and use them together with their shares of the state to produce guesses* M^{B} *and* M^{C} *respectively for the message* M*.*

A protocol is said to be $(t(\lambda), g(\lambda))$-anti-piracy-secure against identical random challenge plaintexts *if for all such pirating attacks, we have*[19]

$$\Pr[(F = \checkmark) \wedge (M = M^{\text{B}} = M^{\text{C}})] \leq \frac{2^{t(\lambda)}}{|\mathcal{M}|} + g(\lambda),$$

where the probability is taken over the distributions of M *and all randomness in the described procedures.*

Definition 8 (Pirating attack and anti-piracy security, for independent random challenge plaintexts)**.** *The pirating attack as the same as in Definition 7 except in step 3, two independent and uniform messages* M_1 *and* M_2 *are sampled from* $\mathcal{M}$*. Bob and Charlie receive independently generated instances of* $\mathsf{Enc}(M_1, K_{\text{enc}}, F)$ *and* $\mathsf{Enc}(M_2, K_{\text{enc}}, F)$ *respectively, and produce guesses* M^{B} *and* M^{C} *for* M_1 *and* M_2*. The protocol is said to be* $(t(\lambda), g(\lambda))$-anti-piracy-secure against independent random challenge plaintexts *if for all such pirating attacks, we have*

$$\Pr[(F = \checkmark) \wedge (M_1 = M^{\text{B}}) \wedge (M_2 = M^{\text{C}})] \leq \frac{2^{t(\lambda)}}{|\mathcal{M}|} + g(\lambda),$$

If an SDECM scheme with $\mathcal{M}$ independent of λ achieves $t(\lambda) = 0$ and $g(\lambda) = \text{negl}(\lambda)$ under one of the above definitions, we may sometimes qualitatively refer to it as having "perfect" anti-piracy security (with respect to the corresponding definition).

Regarding the definitions above (which we based on [CLLZ21]), we highlight that there were some technical differences between the piracy setups studied in [GZ20] compared to [CLLZ21]. The first difference is in whether Bob and Charlie receive identical copies of a single output of $\mathsf{Enc}(M, K_{\text{enc}}, F)$, versus independently generated outputs of that procedure (put another way: whether the same randomness or independent randomness is used to generate the ciphertexts they receive); here we follow [CLLZ21] and use the latter, as we currently require that property in our security proof. Definition 8 follows [CLLZ21] and has Bob and Charlie also receive encryptions of two independent uniform messages M_1, M_2 (which they have to respectively guess).

[19] Technically, in [CLLZ21] the level of security was instead quantified by writing the upper bound in the form $\frac{1}{|\mathcal{M}|} + \gamma(\lambda) + \text{negl}(\lambda)$ and specifying the function $\gamma(\lambda)$. Here, for a closer analogy to Definition 4 (which was based on [BL20]), we have written it in a form similar to the one used in that definition; the definitions are interconvertible by taking $\gamma(\lambda) = \frac{2^{t(\lambda)}-1}{|\mathcal{M}|}$ or inversely $t(\lambda) = \log(|\mathcal{M}|\gamma(\lambda) + 1)$. Furthermore, we have again required an explicit specification of the function $g(\lambda)$ added to $\frac{2^{t(\lambda)}}{|\mathcal{M}|}$ rather than just requiring it to be negligible, due to the issues pointed out in Remark 4.

Definition 7 is similar to [GZ20] in that it gives Bob and Charlie encryptions of the same message (although independent randomness is still used in the encryption), and this is the definition that has a closer analogy to the uncloneability definition for DI-VKECM. For the protocols we present in this work, we will specify in each case which of the above definition(s) they satisfy.

[CLLZ21] also considered another different notion of anti-piracy security that they called CPA-style security. Here instead of the message to be encrypted being randomly sampled, the adversary chooses two distinct messages (m_0, m_1) which could potentially be encrypted. A uniformly random choice is made between these two messages, and then Bob and Charlie have to guess which of the two messages have been encrypted.[20] The security requirement is that their joint guessing probability should be close to $\frac{1}{2}$. We shall not be considering the CPA-style security definition in this work, but we point out that the CPA-style definition and the random ciphertext definition with $t(\lambda) = 0$ are equivalent for single-bit messages (since a uniform choice is made between the 0 message or the 1 message in either case). Since in this work we present (in Section 7) a protocol that indeed achieves $(0, \text{negl}(\lambda))$-anti-piracy security for single-bit messages, it follows that it also achieves CPA-style security for single-bit messages.

4 Cloning game

For any non-local game G (which includes games with multiple rounds and with a variable number of players, like we shall soon describe), we shall use $\omega^*(G)$ to denote its quantum value, i.e., its maximum winning probability with a quantum strategy. We shall use $\omega^*(G^l)$ to denote the winning probability of l parallel copies of G, and $\omega^*(G^{t/l})$ to denote the winning probability of t copies out of l parallel copies of G.

4.1 The CHSH game

The CHSH game is one of the simplest one-round non-local games between two players Alice and Bob, which is as follows:

- Alice and Bob get inputs $x, y \in \{0, 1\}$ uniformly at random.
- Alice and Bob output $a, b \in \{0, 1\}$.
- The game is won if $a_i \oplus b_i = x_i \cdot y_i$.

The optimal classical winning probability $\omega(\text{CHSH})$ of the game is $\frac{3}{4}$, while the optimal quantum winning probability is $\omega^*(\text{CHSH}) = \frac{1}{2}\left(1 + \frac{1}{\sqrt{2}}\right)$. In the optimal quantum strategy for the CHSH game, Alice and Bob share the maximally entangled state $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. Alice's measurements corresponding to inputs 0 and 1 are $\{|0\rangle\langle 0|, |1\rangle\langle 1|\}$ and $\{|\frac{\pi}{4}\rangle\langle\frac{\pi}{4}|, |-\frac{\pi}{4}\rangle\langle-\frac{\pi}{4}|\}$ respectively, and Bob's measurements corresponding to 0 and 1 are $\{|\frac{\pi}{8}\rangle\langle\frac{\pi}{8}|, |-\frac{3\pi}{8}\rangle\langle-\frac{3\pi}{8}|\}$ and $\{|\frac{3\pi}{8}\rangle\langle\frac{3\pi}{8}|, |-\frac{\pi}{8}\rangle\langle-\frac{\pi}{8}|\}$ respectively, where we are using $|\alpha\rangle$ to denote the state $\cos\alpha\,|0\rangle + \sin\alpha\,|1\rangle$. We shall often refer to these state and measurements as the ideal CHSH state and measurements.

[20] Here again one can have variations depending on whether the message to be encrypted is chosen independently or identically for Bob and Charlie.

The CHSH game satisfies the following *rigidity* property (given by a slight extension of Theorem 2 in [MYS12], by writing the projectors $\Pi, \widetilde{\Pi}$ in the following statement as linear combinations of the hermitian observables described in that work).

Fact 10. *Let $|\phi\rangle, \Pi^{\mathrm{A}}_{a|x}, \Pi^{\mathrm{B}}_{b|y}$ denote the state and measurements used in the ideal CHSH strategy. Suppose a quantum strategy for the CHSH game with shared state $|\widetilde{\phi}\rangle$ and projective measurements $\widetilde{\Pi}^{\mathrm{A}}_{a|x}$ and $\widetilde{\Pi}^{\mathrm{B}}_{b|y}$ of Alice and Bob achieves winning probability $\omega^*(\mathrm{CHSH}) - \mu$. Then there exist isometries $V^{\mathrm{A}}, V^{\mathrm{B}}$ acting only on Alice and Bob's registers in $|\rho\rangle$, and a state $|\mathrm{junk}\rangle$ such that for all x, y, a, b,*

$$\left\| V^{\mathrm{A}} \otimes V^{\mathrm{B}} |\widetilde{\phi}\rangle - |\phi\rangle \otimes |\mathrm{junk}\rangle \right\|_2 \leq O(\mu^{1/4});$$
$$\left\| (V^{\mathrm{A}} \otimes V^{\mathrm{B}})(\widetilde{\Pi}^{\mathrm{A}}_{a|x} \otimes \mathbb{1}) |\widetilde{\phi}\rangle - (\Pi^{\mathrm{A}}_{a|x} \otimes \mathbb{1}) |\phi\rangle \otimes |\mathrm{junk}\rangle \right\|_2 \leq O(\mu^{1/4});$$
$$\left\| (V^{\mathrm{A}} \otimes V^{\mathrm{B}})(\mathbb{1} \otimes \widetilde{\Pi}^{\mathrm{B}}_{b|y}) |\widetilde{\phi}\rangle - (\mathbb{1} \otimes \Pi^{\mathrm{B}}_{b|y}) |\phi\rangle \otimes |\mathrm{junk}\rangle \right\|_2 \leq O(\mu^{1/4}).$$

Alice's ideal measurements in the CHSH game are in the computational and Hadamard basis. Since the ideal shared state between Alice and Bob is the maximally entangled state, Bob's state when Alice does the measurement corresponding to $x = 0$ or 1 and obtains outcome $a = 0$ or 1 is $H^x |a\rangle$. These states are called Wiesner states, and we shall denote the Wiesner state produced when x is the input and a is the output by $|a^x\rangle$. The Wiesner states satisfy the following monogamy of entanglement property, which we shall use in our security proof.

Fact 11 ([TFKW13, BL20])**.** *If $|a^x\rangle$ denotes a Wiesner state, then for any Hilbert spaces $\mathcal{H}^{\mathrm{B}}$ and $\mathcal{H}^{\mathrm{C}}$, any two collection of measurements $\{\Pi^{\mathrm{B}}_{a|x}\}_a$ and $\{\Pi^{\mathrm{C}}_{a|x}\}_a$ (for each x) on $\mathcal{H}^{\mathrm{B}}$ and $\mathcal{H}^{\mathrm{C}}$ respectively, and any CPTP map $\Lambda : \mathbb{C}^2 \to \mathcal{H}^{\mathrm{B}} \otimes \mathcal{H}^{\mathrm{C}}$, we have*

$$\mathop{\mathbb{E}}_{a,x} \mathrm{Tr}\left[\left(\Pi^{\mathrm{B}}_{a|x} \otimes \Pi^{\mathrm{C}}_{a|x} \right) \Lambda(|a^x\rangle\langle a^x|) \right] = \frac{1}{2}\left(1 + \frac{1}{\sqrt{2}}\right).$$

Note that we can also define n-qubit versions of the Wiesner states, and the above result holds with the right-hand side being $\left(\frac{1}{2} + \frac{1}{2\sqrt{2}}\right)^n$ in that case. However, we shall only need the result for single-qubit Wiesner states for our purposes.

4.2 The 2-round cloning game

Using the rigidity or self-testing property of the CHSH game and the monogamy of entanglement property of the Wiesner states, we shall formulate a game that we shall call the 2-round cloning game, which we first qualitatively describe as follows. In a single instance of the game, one of two things will happen probabilistically: either the CHSH game will be played between two players whom we call Alice and Barlie, or Alice will get her input for the CHSH game and produce her output as usual (without knowing what is happening on Barlie's side), but Barlie will split into two players Bob and Charlie, who will both be given the same input as Alice and have to guess her output bit. For technical reasons, we shall actually split the game into two rounds, with the CHSH component happening in the first round and Bob and Charlie guessing Alice's output in the second.

The measurements used by Barlie for the CHSH component may be different from those used by Bob and Charlie for the guessing component. However, Alice's device does not know which

component is taking place, and the shared state between Alice and Barlie or Alice, Bob and Charlie is distributed beforehand, and therefore if the CHSH component is won with probability close to $\omega^*(\text{CHSH})$, then by the self-testing property of CHSH, the shared state and Alice's measurements must be close to the ideal state and measurements. Thus, the state on Bob and Charlie's side post-Alice's measurement must be close to a Wiesner state, which will allow us to use the monogamy of entanglement property to upper bound the probability of Bob and Charlie both guessing Alice's output. We shall define the 2-round cloning game formally below, and formalize the above argument about its winning probability in Section 4.4.

We now give the detailed description. The 2-round cloning game CLONE_γ with parameter γ involves four players Alice, Barlie, Bob and Charlie, although not all of them have to perform actions in each round. At the beginning of the game, there can be some arbitrary entangled state shared between Alice and Barlie.[21] The first round only involves the two players Alice and Barlie, who receive some inputs and produce some outputs (without communication). Specifically, the first round inputs, outputs and the winning condition are as follows:

- Alice receives $x \in \{0,1\}$ uniformly at random. Barlie receives $u \in \{0,1,\text{keep}\}$, such that $u = \text{keep}$ with probability $1-\gamma$, and $u = 0$ or 1 with probability $\frac{\gamma}{2}$ each.
- Alice outputs a and Barlie outputs s.
- The first round win condition is

$$\mathsf{V}_1(x,u,a,s) = \begin{cases} 1 & \text{if } u = \text{keep} \\ 1 & \text{if } (u \neq \text{keep}) \wedge (a \oplus s = x \cdot u) \\ 0 & \text{otherwise.} \end{cases}$$

After Barlie produces his first round output, he can do some further operation on his part of the shared state (though this can also be absorbed into the operation he does to produce s). Then Barlie distributes his state in some arbitrary fashion between two other players, Bob and Charlie. Bob and Charlie do not communicate after this (and Barlie no longer plays any further role in the game, apart from having his first-round values (u,s) being involved in the win condition). In the second round, Alice and Barlie do not receive any inputs and are not required to produce any output; Bob and Charlie receive inputs and have to produce outputs separately. The inputs, outputs and win condition in the second round are as follows:

- Bob and Charlie both receive x as their input and produce b and c as their outputs.
- The second round win condition is

$$\mathsf{V}_2(x,u,a,s,b,c) = \begin{cases} 1 & \text{if } u \neq \text{keep} \\ 1 & \text{if } (u = \text{keep}) \wedge (b = c = a) \\ 0 & \text{otherwise.} \end{cases}$$

For a schematic depiction of the structure of this game, refer to Fig. 1 below (which technically depicts the modified game we describe in the next section, but the overall structure is fairly similar).

[21] For the security analysis, it might seem more general to allow an initial entangled state across all four parties. However, as will become clear from the later description, this does not make any difference since any registers Bob and Charlie might have started with could also be analyzed by initially giving them to Barlie instead.

4.3 Modifying the 2-round cloning game

Although it would be nice to be able to use CLONE_γ directly in our encryption scheme and security proof, in order to be able to prove a parallel repetition theorem, we need to modify the game somewhat, by an "anchoring" transformation similar to [Vid17, KT23]. In our case, this means that Alice's input x will not be revealed with some probability α independently to Bob and Charlie; we can let the second round win condition be automatically satisfied for Bob and Charlie if either of them does not receive x (this will be denoted by the input being $\perp$, and in the protocol will correspond to this instance not being used for key generation). This is needed so that Bob and Charlie's second round inputs and Alice's registers are in product with some probability.

The modified 2-round cloning game $\mathrm{CLONE}_{\gamma,\alpha}$ is the same as CLONE_γ in the first round, and after the first round, Barlie again distributes his state between Bob and Charlie in the same fashion as CLONE_γ. (Refer to Fig. 1 for a schematic diagram of this structure.) However, the second round inputs, outputs and win condition for $\mathrm{CLONE}_{\gamma,\alpha}$ are instead as follows:

- Bob and Charlie receive $y, z \in \{0, 1, \perp\}$ respectively, such that $y = \perp$ and $z = \perp$ independently with probability α, and when y and z are not $\perp$, they are equal to x.
- Bob and Charlie output b and c respectively.
- The second round win condition is

$$\mathsf{V}_2(x,u,y,z,a,s,b,c) = \begin{cases} 1 & \text{if } u \neq \text{keep} \\ 1 & \text{if } (u = \text{keep}) \wedge (y = z = \perp) \\ 1 & \text{if } (u = \text{keep}) \wedge (y = \perp \neq z) \\ 1 & \text{if } (u = \text{keep}) \wedge (z = \perp \neq y) \\ 1 & \text{if } (u = \text{keep}) \wedge (y, z \neq \perp) \wedge (b = c = a) \\ 0 & \text{otherwise.} \end{cases}$$

For later use, we summarize the overall win condition $\mathsf{V}_1(x,u,a,s) \cdot \mathsf{V}_2(x,u,y,z,a,s,b,c) = 1$ as follows:

$$\mathsf{V}_1(x,u,a,s) \cdot \mathsf{V}_2(x,u,y,z,a,s,b,c) = \begin{cases} 1 & \text{if } (u \neq \text{keep}) \wedge (a \oplus s = x \cdot u) \\ 1 & \text{if } (u = \text{keep}) \wedge (y = z = \perp) \\ 1 & \text{if } (u = \text{keep}) \wedge (y = \perp \neq z) \\ 1 & \text{if } (u = \text{keep}) \wedge (z = \perp \neq y) \\ 1 & \text{if } (u = \text{keep}) \wedge (y, z \neq \perp) \wedge (b = c = a) \\ 0 & \text{otherwise.} \end{cases} \tag{4}$$

As qualitatively described above, the various possible win conditions when $u = \text{keep}$ (which arise mainly from the second-round conditions, since the first round is trivially won for that case) can be equivalently rewritten into a single condition

$$(y = \perp) \vee (z = \perp) \vee (b = c = a),$$

i.e. (at least) one of Bob and Charlie got $\perp$ as input, or they both guessed a correctly.

In our actual parallel repetition proof, we shall not need to use any specific structure of $\mathrm{CLONE}_{\gamma,\alpha}$ aside from its input distribution, and thus the parallel repetition result holds for a more general class of games. The specific properties of the input distribution that we shall need to use are:

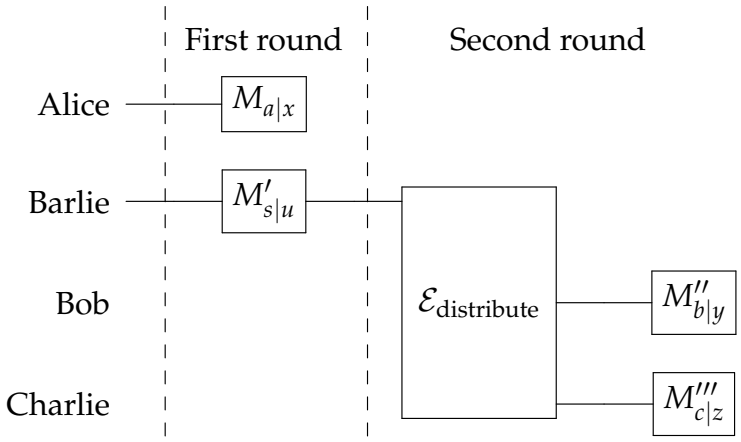

Figure 1: Circuit diagram depicting the game $\text{CLONE}_{\gamma,\alpha}$. Initially, some entangled state is shared between the parties Alice and Barlie. In the first round, Alice measures her register according to her input x to produce an output a, which we depict in the above diagram via its POVM elements $M_{a|x}$; analogously, Barlie measures his register according to some other POVM $M'_{s|u}$. While Alice performs no further operations (so she can discard her state immediately after measuring), Barlie retains his post-measurement register for the second round. In the second round, he redistributes his register to two other parties Bob and Charlie in some arbitrary fashion, which we denote with the channel $\mathcal{E}_{\text{distribute}}$, and Bob and Charlie then respectively perform measurements specified by inputs y and z, producing outputs b and c, which we again represent via POVM elements $M''_{b|y}$ and $M'''_{c|z}$. Note that the simpler game CLONE_{γ} described previously in Section 4.2 also has an essentially similar structure, except that it has a different input distribution (for instance Bob and Charlie's inputs are basically set to $y = z = x$), and a different win condition.

(i) The distribution P_{XU} of the first round inputs is a product distribution; U is also independent of the second round inputs.

(ii) The second round inputs Y, Z are correlated with X in the following way:

$$\mathsf{P}_{XYZ}(x,x,x) = (1-\alpha)^2 \cdot \mathsf{P}_X(x)$$
$$\mathsf{P}_{XYZ}(x,\perp,x) = \mathsf{P}_{XYZ}(x,x,\perp) = \alpha(1-\alpha) \cdot \mathsf{P}_X(x)$$
$$\mathsf{P}_{XYZ}(x,\perp,\perp) = \alpha^2 \cdot \mathsf{P}_X(x).$$

Note that the above implies that conditioned on $Y = Z = \perp$, the conditional distribution $\mathsf{P}_{XU||\perp,\perp}$ of x, u is exactly the same as the marginal distribution of x, u. Similarly, conditioned on $Y = \perp$, the conditional distribution $\mathsf{P}_{XUZ|Y=\perp}$ is the same as the marginal distribution of x, u, z, and conditioned on $Z = \perp$, the conditional distribution $\mathsf{P}_{XUY|Z=\perp}$ is the same as the marginal distribution of x, u, y. Moreover, Y and Z are independent conditioned on X, and since U is independent of everything else, YZ are independent conditioned on XU as well. In fact, if we define random variables DF as follows: D is a uniformly random bit, and $F = XU$ or $F = YZ$ depending on whether $D = 0$ or $D = 1$, then $XUYZ$ are independent conditioned on DF, i.e., $\mathsf{P}_{XUYZ|DF}$ is a product distribution.

4.4 The winning probability of $\mathrm{CLONE}_{\gamma,\alpha}$

We shall now show that $\omega^*(\mathrm{CLONE}_{\gamma,\alpha})$ is strictly less than the trivial upper bound of $(1-\gamma) + \gamma\omega^*(\mathrm{CHSH})$. At first sight, it might appear that this claim holds simply by the following argument sketch: if Bob and Charlie could win perfectly in the second round, then Alice's first-round output must be deterministic conditioned on their side-information, which implies that the devices cannot achieve the maximum quantum CHSH winning probability in the first round. However, this idea has two technical flaws (which we implicitly addressed in previous works [KST22, KT23], though without detailed elaboration). Firstly, for some non-local games it is known that the classical winning probability can be exceeded while still ensuring some inputs give deterministic outputs (see e.g. the *partially deterministic polytope* in [WMP14]); also, in our scenario Bob and Charlie's guesses could potentially depend on Alice's round-1 input, in which case the above argument sketch does not straightforwardly work (see e.g. [Tan21] Appendix B)[22]. Secondly, even if that obstacle were overcome, this argument would only imply that any particular strategy for $\mathrm{CLONE}_{\gamma,\alpha}$ has winning probability less than $(1-\gamma) + \gamma\omega^*(\mathrm{CHSH})$; it would not rule out the possibility of a sequence of strategies achieving winning probabilities *arbitrarily close* to $(1-\gamma) + \gamma\omega^*(\mathrm{CHSH})$. For our later security proof, we really do need the property that the value $\omega^*(\mathrm{CLONE}_{\gamma,\alpha})$ is less than $(1-\gamma) + \gamma\omega^*(\mathrm{CHSH})$, which is a stronger condition (since it means that all strategies have winning probability *bounded away from* $(1-\gamma) + \gamma\omega^*(\mathrm{CHSH})$). Hence the above argument sketch does not work by itself; we now present the actual proof.[23]

[22] Alternatively, observe that the argument clearly fails if we were to consider only a single player Bob instead of both Bob and Charlie, since even if the devices shared the ideal CHSH state in the first round, when the second round occurs Bob could simply (focusing on the $u =$ keep and $y \neq \perp$ case, since otherwise the second round is automatically won) use his knowledge of Alice's first-round input to measure in an appropriate basis and learn her output perfectly.

[23] We also remark that in order to obtain the desired bound, a self-testing result with "nonzero robustness" seems to be necessary, i.e. if Fact 10 had only been proven for $\mu = 0$, it would not have been enough to obtain our desired result (since it leaves open the possibility of devices with CHSH winning probability arbitrarily close to $\omega^*(\mathrm{CHSH})$ while still allowing Bob and Charlie to win the second round with arbitrarily high probability).

Remark 6. *In the proof below, for ease of description we have used the rigidity bound of [MYS12] presented as Fact 10 above, as it has a simple closed-form expression. However, if better bounds on $\omega^*(\mathrm{CLONE}_{\gamma,\alpha})$ are desired, one can instead use the bounds computed in e.g. [BNS+15] using semidefinite programming techniques, which are typically tighter and more noise-robust (but do not have closed-form expressions).*

Theorem 12. *For any $\gamma, \alpha \in (0,1)$, there exists a value $\delta_{\gamma,\alpha} > 0$ such that $\omega^*(\mathrm{CLONE}_{\gamma,\alpha})$ is at most $(1-\gamma) + \gamma\omega^*(\mathrm{CHSH}) - \delta_{\gamma,\alpha}$.*

Proof. Take an arbitrary strategy for playing $\mathrm{CLONE}_{\gamma,\alpha}$. Note that the events listed in (4) that give $\mathsf{V}_1(X,U,A,S) \cdot \mathsf{V}_2(X,U,Y,Z,A,S,B,C) = 1$ are mutually exclusive. Therefore, the winning probability of this strategy on $\mathrm{CLONE}_{\gamma,\alpha}$ is given by summing the probabilities it gives for these events.

We begin by considering the first event. We first note that $\Pr[A \oplus S = X \cdot U | U \neq \text{keep}]$ is just the probability for this strategy to win the CHSH game if it is played in the first round. Therefore, we can denote this value as $\omega^*(\mathrm{CHSH}) - \mu$ for some $\mu \in [0, \omega^*(\mathrm{CHSH})]$ without loss of generality. Putting this together with $\Pr[U \neq \text{keep}] = \gamma$ from the game definition, we have

$$\Pr\left[(U \neq \text{keep}) \wedge (A \oplus S = X \cdot U)\right] = \gamma(\omega^*(\mathrm{CHSH}) - \mu).$$

For the second, third, and fourth events, we apply the game definition to get:

$$\begin{aligned}
\Pr\left[(U = \text{keep}) \wedge (Y = Z = \perp)\right] &= (1-\gamma)\alpha^2, \\
\Pr\left[(U = \text{keep}) \wedge (Y = \perp \neq Z)\right] &= (1-\gamma)\alpha(1-\alpha), \\
\Pr\left[(U = \text{keep}) \wedge (Z = \perp \neq Y)\right] &= (1-\gamma)\alpha(1-\alpha),
\end{aligned}$$

so the sum of their probabilities is

$$(1-\gamma)(\alpha^2 + 2\alpha(1-\alpha)) = (1-\gamma)(1-\tilde{\alpha}), \quad \text{where } \tilde{\alpha} = (1-\alpha)^2.$$

For the last event, first recall that we have parametrized the probability of this strategy winning the CHSH game as $\omega^*(\mathrm{CHSH}) - \mu$. Hence by the CHSH rigidity property (Fact 10), after Alice performs her measurement (chosen uniformly at random), the resulting joint state across her input/output registers and Barlie's register is $O(\mu^{1/4})$-close in trace distance to the "ideal" mixture $\mathbb{E}_{a,x}\left[|x\rangle\langle x| \otimes |a\rangle\langle a| \otimes |a^x\rangle\langle a^x|\right]$ (where $|a^x\rangle\langle a^x|$ again denotes Wiesner states), up to an isometry on Barlie's register.[24] Putting this together with the monogamy of entanglement property (Fact 11), we can conclude that $\Pr\left[B = C = A | (U = \text{keep}) \wedge (Y, Z \neq \perp)\right] \leq \frac{1}{2}\left(1 + \frac{1}{\sqrt{2}}\right) + O(\mu^{1/4})$ (here we implicitly used the fact that the event $(U = \text{keep}) \wedge (Y, Z \neq \perp)$ is independent of Alice's measurement distribution). Combining this with the trivial bound $\Pr\left[B = C = A | (U = \text{keep}) \wedge (Y, Z \neq \perp)\right] \leq 1$, we have overall

$$\begin{aligned}
\Pr\left[(U = \text{keep}) \wedge (Y, Z \neq \perp) \wedge (B = C = A)\right] &\leq (1-\gamma)(1-\alpha)^2 \min\left\{1, \frac{1}{2}\left(1 + \frac{1}{\sqrt{2}}\right) + O(\mu^{1/4})\right\} \\
&= (1-\gamma)\tilde{\alpha} \min\left\{1, \frac{1}{2}\left(1 + \frac{1}{\sqrt{2}}\right) + O(\mu^{1/4})\right\}.
\end{aligned}$$

[24] While that rigidity property is only stated for projective measurements, in this case we are interested only in the classical-quantum state produced after Alice's measurements, which allows us to focus on a suitably chosen Stinespring dilation to projective measurements without loss of generality.

Summing the terms, we get the following upper bound on the winning probability:

$$\begin{aligned}
&(1-\gamma)\left(1-\tilde{\alpha}+\tilde{\alpha}\min\left\{1,\frac{1}{2}\left(1+\frac{1}{\sqrt{2}}\right)+O(\mu^{1/4})\right\}\right)+\gamma(\omega^*(\mathrm{CHSH})-\mu)\\
=&(1-\gamma)\min\left\{1,1-\tilde{\alpha}+\tilde{\alpha}\left(\frac{1}{2}\left(1+\frac{1}{\sqrt{2}}\right)+O(\mu^{1/4})\right)\right\}+\gamma(\omega^*(\mathrm{CHSH})-\mu)\\
=&(1-\gamma)\min\left\{1,\beta+O(\mu^{1/4})\right\}+\gamma(\omega^*(\mathrm{CHSH})-\mu)\quad\text{for }\beta=1-\tilde{\alpha}+\tilde{\alpha}\left(\frac{1}{2}\left(1+\frac{1}{\sqrt{2}}\right)\right)<1,
\end{aligned}$$

absorbing a factor of $\tilde{\alpha}$ into the $O(\mu^{1/4})$ term in the last line (recall α is a constant for the purposes of this proof).

Finally, observe that we have $(1-\gamma)\min\left\{1,\beta+O(\mu^{1/2})\right\}\leq 1-\gamma$ and $\gamma(\omega^*(\mathrm{CHSH})-\mu)\leq\gamma\omega^*(\mathrm{CHSH})$ for any $\mu\in[0,\omega^*(\mathrm{CHSH})]$; however, there is no μ in that interval that simultaneously saturates both inequalities (the only value that saturates the second inequality is $\mu=0$, in which case the first inequality is not saturated since $\beta<1$). Therefore we have a strict inequality

$$(1-\gamma)\min\left\{1,\beta+O(\mu^{1/4})\right\}+\gamma(\omega^*(\mathrm{CHSH})-\mu)<(1-\gamma)+\gamma\omega^*(\mathrm{CHSH}),$$

for all $\mu\in[0,\omega^*(\mathrm{CHSH})]$. To ensure the winning probability is bounded away from $(1-\gamma)+\gamma\omega^*(\mathrm{CHSH})$ by a constant $\delta_{\gamma,\alpha}>0$, we note that $(1-\gamma)\min\left\{1,\beta+O(\mu^{1/4})\right\}+\gamma(\omega^*(\mathrm{CHSH})-\mu)$ is a continuous function of μ on the closed interval $[0,\omega^*(\mathrm{CHSH})]$. Hence it attains its maximum at some value in that interval, and this maximal value will be an upper bound strictly smaller than $(1-\gamma)+\gamma\omega^*(\mathrm{CHSH})$, as desired. □

With this, we give the following parallel repetition theorem upper bounding the winning probability of $\mathrm{CLONE}^{t/l}_{\gamma,\alpha}$:

Theorem 13. *There exists $\kappa>0$ such that for $\delta_{\gamma,\alpha}$ from Theorem 12, and $t=((1-\gamma)+\gamma\omega^*(\mathrm{CHSH})-\delta_{\gamma,\alpha}/2)l$,*

$$\omega^*\left(\mathrm{CLONE}^{t/l}_{\gamma,\alpha}\right)\leq 2^{-\kappa\delta^3_{\gamma,\alpha}\alpha^4 l}.$$

We prove this theorem (in fact, a more general version of it) in Section 8.

5 Uncloneable encryption scheme with variable keys

In this section, we prove our main theorem:

Theorem 14. *There is a scheme for DI-VKECM with message space $\mathcal{M}=\{0,1\}^\lambda$, such that:*

1. *It satisfies the completeness property (1) given i.i.d. honest devices with a constant level of noise;*
2. *It achieves indistinguishable security;*
3. *There exists some $\nu>0$ such that the scheme achieves $(t(\lambda),0)$-uncloneable security against dishonest devices with $\nu\lambda$ bits of leakage, where $t(\lambda)$ is a function satisfying $t(\lambda)<\lambda$ for all sufficiently large λ.*

The protocol achieving Theorem 14 is described in Scheme 1. We prove that Scheme 1 satisfies completeness in Section 5.1, and prove that it satisfies indistinguishability and $(t(\lambda),0)$-uncloneability in Section 5.2, which together constitute the proof of Theorem 14.

Protocol description. Our DI-VKECM scheme is described below — for now, we leave some of the parameters (such as γ and α) to be arbitrary values, with the exact choices that yield Theorem 14 to be specified in the explanations after the protocol. We highlight that when a receiver is dishonest, they do not need to be following their parts as described in the scheme, although we still require them to supply some values to the client at all steps where they are supposed to in the scheme (but these values do not have to be "honestly" produced, of course — recall also that the possibility of a receiver lying about their outputs can be absorbed into the device behaviour without loss of generality).

Informal description of main parameters and notation.

λ: Security parameter (for security definitions from Section 3)

γ: Probability of a "test" instance in the encryption procedure

α: Probability of an instance being eventually "erased" for anchoring purposes

X, A: Input and output strings of client's device in encryption procedure

$\widetilde{X}$, $\widetilde{A}$: Modified versions of X, A in which some instances have been "erased" to account for anchoring

U, S: Input and output strings of receiver's device in encryption procedure

S': Output string of receiver's device in decryption procedure

$\widetilde{S}$: Modified version of S' in which some instances have been "erased" to account for anchoring

R: "One-time-pad" used to encrypt the message

G: Receiver's guess for $\widetilde{A}$

F: Flag for whether the encryption procedure accepted

C: Classical part of ciphertext

K_{dec}: Decryption key

For this scheme, the client and receiver's devices are to have the functionality that the client's device can take an input string $X \in \{0,1\}^l$ and output a string $A \in \{0,1\}^l$, while the receiver's device can take inputs twice: first it takes an input string $U \in \{0,1,\perp\}^l$ and outputs a string $S \in \{0,1\}^l$, then it later takes an input string $\widetilde{X} \in \{2,3,\perp\}^l$ and outputs a string $S' \in \{0,1\}^l$. With this in mind, if we interpret the client and receiver as Alice and Barlie and ignore the second input-output round for the latter, this is exactly the same structure as l parallel instances of the first round of the game $\text{CLONE}_{\gamma,\alpha}$ described in the preceding section. The reason the second round has a different structure is that we only need to consider the second round of the game $\text{CLONE}_{\gamma,\alpha}$ when considering the security definition and constructing the security proof, *not* for defining the protocol itself. (The second-round input and output in the protocol itself is designed to allow an honest receiver to obtain a string that is "highly correlated" to the client's string; this will become clearer when reading the description of the honest device behaviour immediately below the protocol description.) Finally, we remark that for this scheme we take both l and the message length to be equal to the security parameter λ.

Scheme 1 DI-VKECM with security parameter λ and messages in $\mathcal{M} = \{0,1\}^\lambda$

$\mathsf{Enc}(1^\lambda, m)$**:**

1: Devices of the form described above are distributed between the client and receiver, with $l = \lambda$
2: The client samples strings X, U as follows: for each $i \in [l]$, set $X_i \in \{0,1\}$ uniformly at random, and independently set $U_i = \text{keep}, 0, 1$ with probabilities $1-\gamma, \gamma/2, \gamma/2$ respectively
3: The client inputs X into their device and receives an output string $A \in \{0,1\}^l$
4: The client sends U to the receiver
5: The receiver inputs U into their device, interpreting $U_i = \text{keep}$ as $\perp$ for each i, and receives an output string $S \in \{0,1\}^l$
6: The receiver sends S to the client
7: The client tests if the number of $i \in [l]$ such that $U_i \neq \text{keep}$ and $A_i \oplus S_i \neq X_i \cdot U_i$ is at most $(\gamma(1-\omega^*(\text{CHSH})) + \delta_{\gamma,\alpha}/2)l$
8: **if** the test passes **then**
9: The client sets the flag to $F = \checkmark$
10: The client samples $R \in \mathcal{M}$ uniformly at random and sends $C = m \oplus R$ to the receiver
11: **else**
12: The client sets the flag to $F = \times$
13: The client samples $R \in \mathcal{M}$ and $M^{\text{fake}} \in \mathcal{M}$ (independently) uniformly at random and sends $C = M^{\text{fake}} \oplus R$ to the receiver
14: The client stores (X, U, A, R) as the private key; the receiver stores $\rho = \rho' \otimes |C\rangle\langle C|$ as the ciphertext, where ρ' is the quantum state in the receiver's share of the devices

$\mathsf{KeyRel}(k_{\text{priv}})$**:**

15: Interpret the private key as $k_{\text{priv}} = (X, U, A, R)$
16: Sample a string $\widetilde{X} \in \{2, 3, \perp\}^l$ as follows: for each $i \in [l]$, set $\widetilde{X}_i = \perp$ with probability α, and otherwise set $\widetilde{X}_i = X_i + 2$
17: Set a string $\widetilde{A} \in \{0,1\}^l$ as follows: for each $i \in [l]$, set $\widetilde{A}_i = 0$ if $U_i \neq \text{keep}$ or $\widetilde{X}_i = \perp$, and otherwise set $\widetilde{A}_i = A_i$
18: Compute the syndrome $\mathtt{syn}(\widetilde{A})$ following the error-correction procedure described below (see (7))
19: Release the decryption key $K_{\text{dec}} = (R \oplus \widetilde{A}, \mathtt{syn}(\widetilde{A}), \widetilde{X})$

$\mathsf{Dec}(\rho, k)$**:**

20: Interpret ρ as $\rho' \otimes |C\rangle\langle C|$ where ρ' has l qubit registers and $C \in \mathcal{M}$; interpret the decryption key k_{dec} as $(D, \mathtt{syn}(\widetilde{A}), \widetilde{X})$
21: Input $\widetilde{X}$ into the receiver's device and obtain the output string $S' \in \{0,1\}^l$
22: Set a string $\widetilde{S} \in \{0,1\}^l$ as follows: for each $i \in [l]$, set $\widetilde{S}_i = 0$ if $U_i \neq \text{keep}$ or $\widetilde{X}_i = \perp$, and otherwise set $\widetilde{S}_i = S'_i$
23: Use $\widetilde{S}, U, \widetilde{X}$ and $\mathtt{syn}(\widetilde{A})$ to compute a guess G for $\widetilde{A}$
24: Output $\widetilde{M} = C \oplus D \oplus G$

Remark 7. *Qualitatively, the interaction in our encryption procedure arises solely from the fact that we want the receiver to tell the client the output string S, so the client can check whether enough instances win the CHSH game, which later allows us to prove security by invoking the parallel-repetition and rigidity*

results from Section 4. We note however that there is an alternative setup that does not require interaction, if we suppose the client is able to locally impose a particular constraint on the devices. Specifically, we could instead consider a procedure in which the client begins by holding both *the devices and performs steps 1–6 on them, before sending the "receiver's device" over to the receiver (and then proceeding with the rest of the scheme according to the original description), in which case the encryption procedure is non-interactive since it only involves the client sending messages (and devices) to the receiver. For this version, our security proof is still valid as long as the client can enforce that during steps 1–6, the devices are still subject to the bounded-leakage constraint (physically, this might be possible by imposing some "shielding" measures on the devices, keeping them well isolated from each other). Qualitatively, this version can be viewed as having the client locally "test" the devices (while constraining the communication/leakage between them) before using them in the rest of the scheme.*

Honest-device description. We now specify the honest device behaviour. We allow a small amount of noise in the honest behaviour, under a depolarizing-noise model. Specifically, we suppose that the honest devices share l i.i.d. copies of a *Werner state*

$$\rho_q = (1-2q)\,|\Phi^+\rangle\langle\Phi^+| + 2q\frac{\mathbb{1}}{4}, \tag{5}$$

where $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$, and $q \in [0, 1/2]$ will be referred to as the depolarizing-noise parameter. As for the measurements for each input string, we suppose that (for each instance i) the client's device performs Alice's ideal CHSH measurement corresponding to the i-th input bit, on the i-th copy of the shared state. The receiver's measurements are slightly more complicated, though the same in both the first or second input rounds: for each instance i if it obtains an input value in $\{0, 1\}$ then it performs Bob's ideal CHSH measurement corresponding to that value on the i-th copy, whereas if it gets an input value in $\{2, 3\}$ it performs Alice's ideal CHSH measurement corresponding to that value on the i-th copy, and finally if it gets input value $\perp$ then it does nothing to the state and just trivially outputs a fixed value (say, 0). Note that the honest decryption procedure only requires the use of outputs in the second round from those instances i which had input $\perp$ during encryption, which means that in the honest behaviour, all physically relevant outputs are produced by only measuring each qubit once.[25]

This model for the honest devices has the following important properties (for each instance). First, it achieves a CHSH winning probability of $(1-2q)\omega^*(\mathrm{CHSH}) + q$. Second, when the client and receiver's input pairs are $(0, 2)$ or $(1, 3)$, the outputs are equal with probability $1 - q$ (and the marginal output distributions are uniform). In particular, this means that in the decryption step (where the receiver essentially inputs $\widetilde{X}_i = X_i + 2$ into their device for many instances), the honest devices produce outputs that are reasonably "well correlated" between the client and receiver, up to the depolarizing-noise parameter q.

While this noise model is quite simple, we remark that given i.i.d. honest devices with an arbitrary single-instance input-output distribution, it is possible in principle to perform a depolarization procedure (see [MAG06]) to transform their input-output distribution into a form matching the above description (except on the input pairs $(0, 3)$ and $(1, 2)$, which do not occur in the protocol), although this is not necessarily the optimal way to use the devices [MPW22]. Alternatively,

[25] In step 21 of our protocol description, the decryption procedure as presented does technically provide non-trivial inputs to some locations i where we had $U_i \neq$ keep in the first round, i.e., the first round input was not $\perp$. However, this is only for simplicity of description — it can be seen in step 22 that the second-round outputs corresponding to these locations are ignored, so it does not matter what the (honest) device does on these locations in the second round, e.g. even if it is attempting to measure the corresponding qubit a second time.

we note that our subsequent analysis can in fact be phrased entirely in terms of three parameters of the (i.i.d.) honest devices: the probability that they win the CHSH game given uniformly random inputs in $\{0,1\}$, the entropy of Alice's output conditioned on Bob's output for input pair $(0,2)$, and the same for input pair $(1,3)$. Hence if necessary, one could instead specify these three parameters independently, but for ease of presentation in this work we simply use the single-parameter depolarizing-noise model.

Error correction. Because we allow some noise in the honest devices, the client and receiver's output strings from the devices will not be perfectly correlated even in the honest case. We shall accommodate this in our protocol by incorporating standard error correction procedures (see e.g. [Ari10, Ren05, TMPE17]), which we briefly summarize as follows:

Fact 15. *Suppose Alice and Bob hold classical random variables CC' following an i.i.d. distribution $\mathsf{P}_{C_iC_i'}^{\otimes l}$. We shall refer to an error correction procedure as a process in which Alice computes a syndrome value $\mathtt{syn}(C)$ of length $\ell_{\mathtt{syn}}$ (in bits) to send to Bob, who uses it together with C' to produce a guess for C. Then for any $\xi > 1$ and $\beta < 1/2$, there exists an efficient error-correction procedure such that the syndrome length is*

$$\ell_{\mathtt{syn}} = \xi \mathsf{H}(C_i|C_i')l, \tag{6}$$

and the probability of Bob's guess being wrong is upper bounded by a function $p_{\mathrm{err}}(l) = O(2^{-l^\beta})$.

With this in mind, we shall lay out the error correction procedure used in our DI-VKECM scheme. Here we shall describe the error correction procedure in terms of arbitrary values for the protocol parameters γ, α, q. The protocol steps corresponding to the error correction procedure are step 18, in which a syndrome is computed for a string $\widetilde{A}$, and step 23, where the receiver uses it to produce a guess for $\widetilde{A}$. We note that in the honest case, when the full process $\mathsf{Dec} \circ \mathsf{KeyRel} \circ \mathsf{Enc}$ in Scheme 1 is carried out, at the point of step 18 the receiver holds an output string $\widetilde{S}$ from the device along with the values $U, \widetilde{X}$. Furthermore, the device behaviour is i.i.d. in the honest case. With this, we take the error-correction procedure to be performed as specified in Fact 15, interpreting the distribution on (C_i, C_i') in that procedure to be the distribution on $(\widetilde{A}_i, \widetilde{S}_i U_i \widetilde{X}_i)$ for the *honest* devices. Note that this means the value $\mathsf{H}(C_i|C_i')$ in (6) in this context has the following value (letting h_2 denote the binary entropy function):

$$\mathsf{H}(\widetilde{A}_i|\widetilde{S}_i U_i \widetilde{X}_i) = \sum_{u_i \tilde{x}_i} \Pr[U_i\widetilde{X}_i = u_i\tilde{x}_i] \mathsf{H}\Big(\widetilde{A}_i|\widetilde{S}_i; U_i\widetilde{X}_i = u_i\tilde{x}_i\Big) = (1-\gamma)(1-\alpha)h_2(q), \tag{7}$$

where we have used the facts that $\mathsf{H}\Big(\widetilde{A}_i|\widetilde{S}_i; U_i\widetilde{X}_i = u_i\tilde{x}_i\Big) = 0$ whenever $u_i \neq$ keep or $\tilde{x}_i = \perp$ (because $\widetilde{A}_i$ is set to a deterministic value in those cases), and $\mathsf{H}\Big(\widetilde{A}_i|\widetilde{S}_i; U_i\widetilde{X}_i = u_i\tilde{x}_i\Big) = h_2(q)$ otherwise (because in that case we have $u_i =$ keep and $\tilde{x}_i = x_i + 2$, i.e. for the honest devices this corresponds to the client and receiver measuring in the same basis on a Werner state (5), hence their output values $(\widetilde{A}_i, \widetilde{S}_i)$ have uniform marginal distributions, and the probability that they differ is q).

Parameter choices. We now specify the parameter choices for our DI-VKECM scheme. The input/output length l for the devices is set equal to the security parameter λ as mentioned before, and the message is also required to be a bit string of length λ, i.e. we have $\mathcal{M} = \{0,1\}^\lambda$. (This is a slightly redundant parametrization in this case since $\lambda, l, \log|\mathcal{M}|$ are all equal to each other, but

we present it this way to maintain flexibility for potentially choosing l and $\mathcal{M}$ differently in terms of λ, as shall return to in Section 7.) Take any choice of values for $\xi > 1$ and $\gamma, \alpha \in (0,1)$, and set the parameter $\delta_{\gamma,\alpha}$ appearing in the protocol to be the corresponding value from Theorem 12. Letting κ be the constant from Theorem 13, we require the honest devices to have depolarizing-noise values q satisfying

$$q < \frac{\delta_{\gamma,\alpha}}{4}, \qquad 2\xi(1-\gamma)(1-\alpha)h_2(q) < \kappa\delta_{\gamma,\alpha}^3\alpha^4, \tag{8}$$

which is always possible by taking a sufficiently small value of q since $\gamma, \alpha, \delta_{\gamma,\alpha}, \kappa$ have been fixed. With this, all parameters necessary to specify the error correction procedure (in steps 18 and 23) have been fixed; in particular, the length of $\mathtt{syn}(\widetilde{A})$ in that procedure is given by

$$\ell_{\mathtt{syn}} = \xi(1-\gamma)(1-\alpha)h_2(q)l. \tag{9}$$

Note that since the error-correction procedure is based on the honest behaviour, $\ell_{\mathtt{syn}}$ is a protocol parameter, not a random variable.

5.1 Completeness of Scheme 1

It is easy to see that Scheme 1 satisfies the property (2) that when $F = \text{✗}$, the ciphertext state is independent of the message. We now show that it also satisfies the completeness property (1).

Theorem 16. *With the parameter choices as specified in (8)-(9), Scheme 1 satisfies the completeness property (1), with the bound on the right-hand-side being* $1 - \left(e^{-\delta_{\gamma,\alpha}^2\lambda/8} + p_{\text{err}}(\lambda)\right)$ *where* p_{err} *is the function described in Fact 15.*

Proof. Since

$$\begin{aligned}
&\Pr\left[(F = \text{✓}) \wedge \left(\mathsf{Dec} \circ \mathsf{KeyRel} \circ \mathsf{Enc}(1^\lambda, m) = m\right)\right] \\
=&1 - \Pr\left[(F = \text{✗}) \vee \left(\mathsf{Dec} \circ \mathsf{KeyRel} \circ \mathsf{Enc}(1^\lambda, m) \neq m\right)\right] \\
=&1 - \left(\Pr\left[F = \text{✗}\right] + \Pr\left[(F = \text{✓}) \wedge \left(\mathsf{Dec} \circ \mathsf{KeyRel} \circ \mathsf{Enc}(1^\lambda, m) \neq m\right)\right]\right),
\end{aligned}$$

to prove completeness it suffices to bound the two probabilities in the last line when the devices are honest.

To bound $\Pr[F = \text{✗}]$, we recall that our model of the honest devices gives a CHSH winning probability of $(1-2q)\omega^*(\text{CHSH}) + q > \omega^*(\text{CHSH}) - q$. Therefore, by the distribution of U_i in the protocol, in each round we have

$$\begin{aligned}
\Pr[(U_i \neq \text{keep}) \wedge (A_i \oplus S_i \neq X_i \cdot U_i)] &= \gamma \Pr[A_i \oplus S_i \neq X_i \cdot U_i | U_i \neq \text{keep}] \\
&\leq \gamma\left(1 - \omega^*(\text{CHSH}) + q\right) \\
&\leq \gamma\left(1 - \omega^*(\text{CHSH})\right) + \frac{\delta_{\gamma,\alpha}}{4} \quad \text{since } q < \frac{\delta_{\gamma,\alpha}}{4} \text{ and } \gamma < 1.
\end{aligned}$$

Since this value is $\delta_{\gamma,\alpha}/4$ less than the threshold fraction $\gamma(1-\omega^*(\text{CHSH})) + \delta_{\gamma,\alpha}/2$ in the step 7 test, and all the instances are i.i.d. in the honest case, we can apply the Chernoff bound to get that the probability of failing the test (i.e. $F = \text{✗}$) is at most $e^{-\delta_{\gamma,\alpha}^2 l/8}$.

As for $\Pr\left[\mathsf{Dec} \circ \mathsf{Enc}(1^\lambda, m) \neq m\right]$, first observe that when $F = \checkmark$, the honest receiver's decrypted value is equal to m whenever $G = \widetilde{A}$, and hence

$$\Pr\left[(F = \checkmark) \wedge \left(\mathsf{Dec} \circ \mathsf{KeyRel} \circ \mathsf{Enc}(1^\lambda, m) \neq m\right)\right] \leq \Pr\left[(F = \checkmark) \wedge \left(G \neq \widetilde{A}\right)\right] \leq \Pr\left[G \neq \widetilde{A}\right].$$

Since the honest behaviour is i.i.d., and the error-correction step was taken to be as described in Fact 15 based on the honest behaviour, we have that the probability of the receiver's guess G being wrong (i.e. $G \neq \widetilde{A}$) is at most $p_{\text{err}}(l)$ in the honest case. This gives the claimed result, recalling that $l = \lambda$. □

5.2 Security of Scheme 1

We begin with a simple observation about the behaviour of one-time-pads (which can be verified with a straightforward calculation):

Fact 17. *Consider an arbitrary state ρ_{EC_1} where C_1 is a classical n-bit register. Suppose we generate an independent uniformly random n-bit string C_2, and set another register $C_3 = C_1 \oplus C_2$. Then the resulting state $\rho_{EC_1C_2C_3}$ is exactly the same as though we had instead generated C_3 as an independent uniformly random n-bit string, and set $C_2 = C_1 \oplus C_3$.*

In particular, this implies that if we trace out C_2 from that state $\rho_{EC_1C_2C_3}$, the resulting reduced state has the product form $\rho_{EC_1C_3} = \rho_{EC_1} \otimes \mathbb{1}_{C_3}/2^n$, i.e. it could equivalently be generated by setting C_3 to be a uniformly random value independent of ρ_{EC_1}.

From this, we immediately obtain indistinguishable security for our protocol:

Theorem 18. *Scheme 1 is indistinguishable-secure.*

Proof. By definition, indistinguishable security only involves the output of the encryption procedure excluding the private key K_{priv}. We observe that in the encryption procedure, the only step that depends on the message M is step 10 (when $F = \checkmark$), where basically a one-time-pad R is independently generated uniformly at random and applied to the message. Furthermore, since we exclude the private key in analyzing indistinguishable security, we can trace out R immediately after that step. Hence we can apply Fact 17 (identifying M, R with C_1, C_2 respectively) to conclude that the ciphertext register C is completely independent of the message. Since this is the only register that could potentially depend on the message here, it clearly follows that indistinguishable security holds. □

Next, we turn to proving uncloneable security. We begin by first considering a modified version of a cloning attack in which some registers are not provided to the dishonest parties, and proving a bound on the probability that Bob and Charlie can simultaneously guess some parts of the "internal" values $\widetilde{A}$ produced in step 17 of the KeyRel procedure:

Lemma 19. *We introduce the following notation for some registers produced in a cloning attack (as defined in Definition 4): when* KeyRel *is performed for Bob (resp. Charlie), let Y (resp. Z) denote the value of $\widetilde{X}$ produced in step 16, and let $\widetilde{A}^{\mathsf{B}}$ (resp. $\widetilde{A}^{\mathsf{C}}$) denote the value of $\widetilde{A}$ produced in step 17. Let $\mathcal{T}$ denote the subset of instances $i \in [l]$ such that Y_i and Z_i are* both *equal to X_i.*

Now consider a cloning attack, except with the following modifications:

- *When the encryption procedure* Enc *is performed, the receiver is not given the register C in step 10 (or step 13).*
- *When the key-release procedure* KeyRel *is performed for Bob (resp. Charlie), the values $R \oplus \widetilde{A}^{\mathrm{B}}$ and $\mathtt{syn}(\widetilde{A}^{\mathrm{B}})$ (resp. $R \oplus \widetilde{A}^{\mathrm{C}}$ and $\mathtt{syn}(\widetilde{A}^{\mathrm{C}})$) are omitted from the decryption key in step 19.*
- *Instead of Bob (resp. Charlie) producing a guess for the message M, he produces a guess G^{B} (resp. G^{C}) for $\widetilde{A}^{\mathrm{B}}$ (resp. $\widetilde{A}^{\mathrm{C}}$).*

Then if there is no leakage between the client and receiver's devices during $\mathsf{Enc}(1^\lambda, M)$*, or between Bob and Charlie's devices after they receive their decryption keys, the following bound holds:*

$$\Pr[(F = \checkmark) \wedge (\widetilde{A}^{\mathrm{B}}_{\mathcal{T}} = G^{\mathrm{B}}_{\mathcal{T}}) \wedge (\widetilde{A}^{\mathrm{C}}_{\mathcal{T}} = G^{\mathrm{C}}_{\mathcal{T}})] \leq 2^{-\kappa \delta^3_{\gamma,\alpha} \alpha^4 l},$$

where κ is the constant from Theorem 13, and the notation $W_{\mathcal{T}}$ for any string W denotes the substring of W on the instances in $\mathcal{T}$.

Proof. We first briefly summarize the main processes involving the dishonest parties in this modified cloning-attack scenario. The receiver begins with some share of a quantum state in their device, then gets the classical value U from the client and uses it to produce a value S to send to the receiver (in step 6). Without any further communication from the client (since the register C has been omitted), the receiver distributes states between Bob and Charlie. Finally Bob and Charlie receive values Y and Z respectively (since the values $R \oplus \widetilde{A}^{\mathrm{B}}, \mathtt{syn}(\widetilde{A}^{\mathrm{B}}), R \oplus \widetilde{A}^{\mathrm{C}}, \mathtt{syn}(\widetilde{A}^{\mathrm{C}})$ have been omitted from their decryption keys), and measure their states to produce their guesses $G^{\mathrm{B}}, G^{\mathrm{C}}$. Our proof proceeds by comparing this situation to the game $\mathrm{CLONE}^{t/l}_{\gamma,\alpha}$ (with t arbitrary for now; we shall fix a suitable value at the end).

We observe that in terms of the input distribution (and the order in which they are supplied relative to the state distribution step), the distribution of X, U, Y, Z in this scenario is exactly the same as in $\mathrm{CLONE}^{t/l}_{\gamma,\alpha}$. Furthermore, the client's output string A produced during the protocol is produced the same way as Alice's output in $\mathrm{CLONE}^{t/l}_{\gamma,\alpha}$, the receiver's output string S is produced the same way as Barlie's first-round output in $\mathrm{CLONE}^{t/l}_{\gamma,\alpha}$, and Bob and Charlie's guesses $G^{\mathrm{B}}, G^{\mathrm{C}}$ are produced the same way as their second-round outputs in $\mathrm{CLONE}^{t/l}_{\gamma,\alpha}$. Hence we shall treat these values as their outputs in the game $\mathrm{CLONE}^{t/l}_{\gamma,\alpha}$.

Our goal is to bound the probability of the event $(F = \checkmark) \wedge (\widetilde{A}^{\mathrm{B}}_{\mathcal{T}} = G^{\mathrm{B}}_{\mathcal{T}}) \wedge (\widetilde{A}^{\mathrm{C}}_{\mathcal{T}} = G^{\mathrm{C}}_{\mathcal{T}})$. We shall first argue that this event implies that the game $\mathrm{CLONE}^{t/l}_{\gamma,\alpha}$ is won on all instances $i \in [l]$ where $U_i = \text{keep}$. To do so, consider any such instance i, and observe that if $i \notin \mathcal{T}$ (i.e. at least one of Y_i, Z_i is $\perp$), then $\mathrm{CLONE}^{t/l}_{\gamma,\alpha}$ is automatically won on that instance, recalling the win conditions (4). On the other hand, if $i \in \mathcal{T}$, then the event $(F = \checkmark) \wedge (\widetilde{A}^{\mathrm{B}}_{\mathcal{T}} = G^{\mathrm{B}}_{\mathcal{T}}) \wedge (\widetilde{A}^{\mathrm{C}}_{\mathcal{T}} = G^{\mathrm{C}}_{\mathcal{T}})$ implies that we have $(\widetilde{A}^{\mathrm{B}}_i = G^{\mathrm{B}}_i) \wedge (\widetilde{A}^{\mathrm{C}}_i = G^{\mathrm{C}}_i)$. Furthermore, since $i \in \mathcal{T}$ we have that $\widetilde{A}^{\mathrm{B}}_i$ and $\widetilde{A}^{\mathrm{C}}_i$ are equal to A_i (recalling how they were constructed in step 17 of the protocol). So we see that $\widetilde{A}_i = G^{\mathrm{B}}_i = G^{\mathrm{C}}_i$, i.e. the win condition of $\mathrm{CLONE}^{t/l}_{\gamma,\alpha}$ is indeed fulfilled on all such instances as well.

Hence the only instances on which the win condition of $\mathrm{CLONE}^{t/l}_{\gamma,\alpha}$ might not be fulfilled are those in which $U_i \neq \text{keep}$. Again referring back to the win conditions (4), we see that such instances fail the win condition if and only if $A_i \oplus S_i \neq X_i \cdot U_i$. But recalling the definition of the "testing" step 7 in the protocol, we see that $F = \checkmark$ is the statement that the number of such instances is at most $(\gamma(1 - \omega^*(\mathrm{CHSH})) + \delta_{\gamma,\alpha}/2)l$. Thus overall, we conclude that the event

$(F = \checkmark) \wedge (\widetilde{A}^{\mathrm{B}}_{\mathcal{T}} = G^{\mathrm{B}}_{\mathcal{T}}) \wedge (\widetilde{A}^{\mathrm{C}}_{\mathcal{T}} = G^{\mathrm{C}}_{\mathcal{T}})$ implies the number of instances satisfying the win condition is at least

$$l - \left(\gamma(1 - \omega^*(\mathrm{CHSH})) + \frac{\delta_{\gamma,\alpha}}{2}\right) l = \left((1-\gamma) + \gamma\omega^*(\mathrm{CHSH}) - \frac{\delta_{\gamma,\alpha}}{2}\right) l.$$

Therefore, the probability of $(F = \checkmark) \wedge (\widetilde{A}^{\mathrm{B}}_{\mathcal{T}} = G^{\mathrm{B}}_{\mathcal{T}}) \wedge (\widetilde{A}^{\mathrm{C}}_{\mathcal{T}} = G^{\mathrm{C}}_{\mathcal{T}})$ is at most the probability of having at least $t = ((1-\gamma) + \gamma\omega^*(\mathrm{CHSH}) - \delta_{\gamma,\alpha}/2)\, l$ win instances in $\mathrm{CLONE}^{t/l}_{\gamma,\alpha}$. By Theorem 13, the latter probability is upper bounded by $2^{-\kappa\delta^3_{\gamma,\alpha}\alpha^4 l}$, which gives the desired result. □

With this, we now prove a bound on the probability Bob and Charlie can both guess the values $\widetilde{A}^{\mathrm{B}}, \widetilde{A}^{\mathrm{C}}$ described above, but using all the registers involved in an actual cloning attack. Informally, the idea is that to compensate for the syndromes $\mathtt{syn}(\widetilde{A}^{\mathrm{B}}), \mathtt{syn}(\widetilde{A}^{\mathrm{C}})$ we simply multiply the guessing probability by a factor corresponding to the lengths of the syndromes, whereas for the registers $C, R \oplus \widetilde{A}^{\mathrm{B}}, R \oplus \widetilde{A}^{\mathrm{C}}$ we shall argue that they are mostly "decoupled" from $\widetilde{A}^{\mathrm{B}}\widetilde{A}^{\mathrm{C}}$ and hence have limited effects on the optimal guessing probability.

Lemma 20. *We follow the notation as defined in Lemma 19. Consider a cloning attack with the modification that instead of Bob (resp. Charlie) producing a guess for the message M, he produces a guess G^{B} (resp. G^{C}) for $\widetilde{A}^{\mathrm{B}}$ (resp. $\widetilde{A}^{\mathrm{C}}$). Then if there is no leakage between the client and receiver's devices during $\mathsf{Enc}(1^\lambda, M)$, or between Bob and Charlie's devices after they receive their decryption keys, the following bound holds:*

$$\Pr[(F = \checkmark) \wedge (\widetilde{A}^{\mathrm{B}} = G^{\mathrm{B}}) \wedge (\widetilde{A}^{\mathrm{C}} = G^{\mathrm{C}})] \leq 2^{-\kappa\delta^3_{\gamma,\alpha}\alpha^4 l + 2\ell_{\mathtt{syn}}}, \tag{10}$$

where κ is the constant from Theorem 13, and $\ell_{\mathtt{syn}}$ given by (9).

Proof. The difference between this scenario as compared to that described in Lemma 19 is that here, the dishonest parties have access to more registers: specifically, the receiver is given the register C in the ciphertext, and Bob (resp. Charlie) is given $R \oplus \widetilde{A}^{\mathrm{B}}, \mathtt{syn}(\widetilde{A}^{\mathrm{B}})$ (resp. $R \oplus \widetilde{A}^{\mathrm{C}}, \mathtt{syn}(\widetilde{A}^{\mathrm{C}})$) in his decryption key. For brevity, let D^{B} and H^{B} denote the values $R \oplus \widetilde{A}^{\mathrm{B}}$ and $\mathtt{syn}(\widetilde{A}^{\mathrm{B}})$ for Bob, and define D^{C} and H^{C} analogously for Charlie. To prove the claimed bound (10) in this scenario, we shall analyze a sequence of modified scenarios in which we progressively remove these registers from consideration, finally arriving at the scenario in Lemma 19. (Note that the probability we are bounding in this lemma is also slightly different from that in Lemma 19, because it involves the full strings $\widetilde{A}^{\mathrm{B}}, G^{\mathrm{B}}, \widetilde{A}^{\mathrm{C}}, G^{\mathrm{C}}$ rather than just the substrings on $\mathcal{T}$. We return to this point later in this proof.)

To facilitate this analysis, we introduce the following notation. For any subset Q of the registers mentioned above (i.e. $Q \subseteq \{C, D^{\mathrm{B}}, D^{\mathrm{C}}, H^{\mathrm{B}}, H^{\mathrm{C}}\}$), let $\mathcal{C}_Q$ denote the set of all "modified cloning attacks" in the sense described in the Lemma 19 statement (i.e. at the end Bob and Charlie produce guesses for $\widetilde{A}^{\mathrm{B}}$ and $\widetilde{A}^{\mathrm{C}}$), except that the dishonest parties additionally have access to the registers Q (with the implicit understanding that these registers become available to the dishonest parties at the same points as in a standard cloning attack). In terms of this notation, Lemma 19 is considering all attacks in the set $\mathcal{C}_\emptyset$ ($\emptyset$ denotes the empty set), while this lemma statement we aim to prove here is simply the statement that

$$\max_{\mathcal{C}_{CD^{\mathrm{B}}D^{\mathrm{C}}H^{\mathrm{B}}H^{\mathrm{C}}}} \Pr[\mathcal{E}_{\mathrm{succ}}] \leq 2^{-\kappa\delta^3_{\gamma,\alpha}\alpha^4 l + 2\ell_{\mathtt{syn}}}, \quad \text{where } \mathcal{E}_{\mathrm{succ}} = (F = \checkmark) \wedge (\widetilde{A}^{\mathrm{B}} = G^{\mathrm{B}}) \wedge (\widetilde{A}^{\mathrm{C}} = G^{\mathrm{C}}). \tag{11}$$

As the first step, we argue that Bob and Charlie having access to the registers $H^{\mathrm{B}}H^{\mathrm{C}}$ could only have increased the attack's maximum success probability by at most a factor of $2^{2\ell_{\mathrm{syn}}}$, i.e. in terms of the above notation we have

$$\max_{\mathcal{C}_{CD^{\mathrm{B}}D^{\mathrm{C}}H^{\mathrm{B}}H^{\mathrm{C}}}} \Pr[\mathcal{E}_{\mathrm{succ}}] \leq 2^{2\ell_{\mathrm{syn}}} \max_{\mathcal{C}_{CD^{\mathrm{B}}D^{\mathrm{C}}}} \Pr[\mathcal{E}_{\mathrm{succ}}].$$

This follows from a standard guessing-strategy argument: given any attack in which Bob and Charlie use $H^{\mathrm{B}}H^{\mathrm{C}}$ to achieve $\Pr[\mathcal{E}_{\mathrm{succ}}] = p$ for some $p \in [0,1]$, there is always another attack in which Bob and Charlie achieve $\Pr[\mathcal{E}_{\mathrm{succ}}] \geq 2^{-2\ell_{\mathrm{syn}}} p$ *without* access to $H^{\mathrm{B}}H^{\mathrm{C}}$, as follows: Bob and Charlie independently produce uniformly random guesses for H^{B} and H^{C} respectively, then proceed with the original strategy as though these guesses were the true values of $H^{\mathrm{B}}H^{\mathrm{C}}$. Note that the probability of these guesses being (both) equal to the true syndrome values is always exactly $2^{-2\ell_{\mathrm{syn}}}$, hence the described attack succeeds with probability at least $2^{-2\ell_{\mathrm{syn}}} p$, as claimed.

With this bound we can remove the registers $H^{\mathrm{B}}H^{\mathrm{C}}$ from consideration, in the sense that to prove (11), it would suffice to show that

$$\max_{\mathcal{C}_{CD^{\mathrm{B}}D^{\mathrm{C}}}} \Pr[\mathcal{E}_{\mathrm{succ}}] \leq 2^{-\kappa \delta_{\gamma,\alpha}^3 \alpha^4 l}. \tag{12}$$

To do so, we now proceed to remove the register C as well, by arguing that

$$\max_{\mathcal{C}_{CD^{\mathrm{B}}D^{\mathrm{C}}}} \Pr[\mathcal{E}_{\mathrm{succ}}] = \max_{\mathcal{C}_{D^{\mathrm{B}}D^{\mathrm{C}}}} \Pr[\mathcal{E}_{\mathrm{succ}}].$$

This follows by observing that in the definition of a cloning attack (or modified cloning attack, in this context), the message M is chosen uniformly at random and independently of everything else. This means we can effectively view it as playing the role of a one-time-pad in the process of generating C — note that this is "reversed" from our earlier Theorem 18 proof, in that here we shall view M rather than R as the one-time-pad. To put this rigorously: before step 10, in this context M is a uniformly random value that was generated independently of everything else. Furthermore, for the event $\mathcal{E}_{\mathrm{succ}}$ that we are considering, the only role played by the message M is in generating the value $C = M \oplus R$ in step 10 (focusing on the $F = \checkmark$ case, since otherwise C is produced from a "dummy message" M^{fake} independent of the true message), and hence we can just trace out M immediately after that step. With this, we apply the last statement in Fact 17 (identifying R, M with C_1, C_2 respectively — again, we stress that the roles are "reversed" from our Theorem 18 proof) to conclude that the state produced after step 10 is *exactly* the same as though C was generated as a uniformly random value independent of everything else. Since a dishonest receiver could generate such a C on their own anyway, we can absorb it into the actions of a dishonest receiver when considering the set of attacks $\mathcal{C}_{D^{\mathrm{B}}D^{\mathrm{C}}}$, and conclude that the maximum value of $\Pr[\mathcal{E}_{\mathrm{succ}}]$ over attacks in the set $\mathcal{C}_{CD^{\mathrm{B}}D^{\mathrm{C}}}$ is the same as over the set $\mathcal{C}_{D^{\mathrm{B}}D^{\mathrm{C}}}$.

The last step is to remove the registers $D^{\mathrm{B}}D^{\mathrm{C}}$ and connect $\mathcal{E}_{\mathrm{succ}}$ to the event considered in Lemma 19. We start by observing that whenever Bob and Charlie have access to $D^{\mathrm{B}} = R \oplus \widetilde{A}^{\mathrm{B}}$ and $D^{\mathrm{C}} = R \oplus \widetilde{A}^{\mathrm{C}}$, they can simultaneously guess (respectively) $\widetilde{A}^{\mathrm{B}}$ and $\widetilde{A}^{\mathrm{C}}$ correctly *if and only if* they can simultaneously guess R — this follows by observing that if e.g. Bob guesses R correctly, he can get $\widetilde{A}^{\mathrm{B}}$ by computing $R \oplus D^{\mathrm{B}}$; conversely if he guesses $\widetilde{A}^{\mathrm{B}}$ correctly he can get R from $\widetilde{A}^{\mathrm{B}} \oplus D^{\mathrm{B}}$ (the analysis for Charlie is analogous). To discuss this more easily, let $\widehat{\mathcal{C}}_Q$ denote the set of all modified cloning attacks in a similar fashion to $\mathcal{C}_Q$, except with one further modification that rather than having Bob (resp. Charlie) produce a guess G^{B} (resp. G^{C}) for $\widetilde{A}^{\mathrm{B}}$ (resp. $\widetilde{A}^{\mathrm{C}}$), he is to

produce a guess $\widehat{G}^{\mathrm{B}}$ (resp. $\widehat{G}^{\mathrm{C}}$) for R.[26] (Note that this means Bob and Charlie are both trying to guess the same value in this case.) Then the preceding observation tells us that we have

$$\max_{\mathcal{C}_{D^{\mathrm{B}}D^{\mathrm{C}}}} \Pr[\mathcal{E}_{\mathrm{succ}}] = \max_{\widehat{\mathcal{C}}_{D^{\mathrm{B}}D^{\mathrm{C}}}} \Pr[(F = \checkmark) \wedge (R = \widehat{G}^{\mathrm{B}} = \widehat{G}^{\mathrm{C}})].$$

On the right-hand-side of the above equation, Bob and Charlie are trying to guess R given access to $D^{\mathrm{B}}D^{\mathrm{C}}$. Now consider the set $\mathcal{T}$ as defined in the Lemma 19 statement, and let $\overline{\mathcal{T}} = [l] \setminus \mathcal{T}$. Note that because R is a uniformly random l-bit string, all the bits within it are independent of each other as well, and we can discuss them individually. Suppose that for all the instances $i \in \overline{\mathcal{T}}$, rather than giving Bob (resp. Charlie) the bit D_i^{B} (resp. D_i^{C}) we were to simply give them R_i directly. This would improve their probability of guessing R, hence if we let $\widehat{\mathcal{C}}_{D_{\mathcal{T}}^{\mathrm{B}}R_{\overline{\mathcal{T}}},D_{\mathcal{T}}^{\mathrm{C}}R_{\overline{\mathcal{T}}}}$ denote a scenario where Bob and Charlie get $D_{\mathcal{T}}^{\mathrm{B}}R_{\overline{\mathcal{T}}}$ and $D_{\mathcal{T}}^{\mathrm{C}}R_{\overline{\mathcal{T}}}$ respectively (following the Lemma 19 notation) rather than simply D^{B} and D^{C}, we can write

$$\begin{aligned}
\max_{\widehat{\mathcal{C}}_{D^{\mathrm{B}}D^{\mathrm{C}}}} \Pr[(F = \checkmark) \wedge (R = \widehat{G}^{\mathrm{B}} = \widehat{G}^{\mathrm{C}})] &\leq \max_{\widehat{\mathcal{C}}_{D_{\mathcal{T}}^{\mathrm{B}}R_{\overline{\mathcal{T}}},D_{\mathcal{T}}^{\mathrm{C}}R_{\overline{\mathcal{T}}}}} \Pr[(F = \checkmark) \wedge (R = \widehat{G}^{\mathrm{B}} = \widehat{G}^{\mathrm{C}})] \\
&= \max_{\widehat{\mathcal{C}}_{D_{\mathcal{T}}^{\mathrm{B}}D_{\mathcal{T}}^{\mathrm{C}}}} \Pr[(F = \checkmark) \wedge (R_{\mathcal{T}} = \widehat{G}_{\mathcal{T}}^{\mathrm{B}} = \widehat{G}_{\mathcal{T}}^{\mathrm{C}})] \\
&= \max_{\mathcal{C}_{D_{\mathcal{T}}^{\mathrm{B}}D_{\mathcal{T}}^{\mathrm{C}}}} \Pr[(F = \checkmark) \wedge (\widetilde{A}_{\mathcal{T}}^{\mathrm{B}} = G_{\mathcal{T}}^{\mathrm{B}}) \wedge (\widetilde{A}_{\mathcal{T}}^{\mathrm{C}} = G_{\mathcal{T}}^{\mathrm{C}})],
\end{aligned} \tag{13}$$

where the second line holds because when e.g. Bob has access to $R_{\overline{\mathcal{T}}}$ he can guess R if and only if he can guess $R_{\mathcal{T}}$ (similarly for Charlie), and the third line holds because once again, when e.g. Bob has access to $D_{\mathcal{T}}^{\mathrm{B}} = R_{\mathcal{T}} \oplus \widetilde{A}_{\mathcal{T}}^{\mathrm{B}}$ he can guess $R_{\mathcal{T}}$ if and only if he can guess $\widetilde{A}_{\mathcal{T}}^{\mathrm{B}}$ (similarly for Charlie).

Finally, we observe that for attacks in $\mathcal{C}_{D_{\mathcal{T}}^{\mathrm{B}}D_{\mathcal{T}}^{\mathrm{C}}}$, the dishonest parties do not have access to the register C, and thus the register R is not involved in anything until step 19. We can hence say that R is generated at that point, uniformly at random and independently of everything else, then used to compute $D_{\mathcal{T}}^{\mathrm{B}} = D_{\mathcal{T}}^{\mathrm{C}} = R_{\mathcal{T}} \oplus \widetilde{A}_{\mathcal{T}}$ (recalling steps 17 and 19 of the protocol) and traced out immediately afterwards (since it is not involved in any subsequent steps when considering $\Pr[(F = \checkmark) \wedge (\widetilde{A}_{\mathcal{T}}^{\mathrm{B}} = G_{\mathcal{T}}^{\mathrm{B}}) \wedge (\widetilde{A}_{\mathcal{T}}^{\mathrm{C}} = G_{\mathcal{T}}^{\mathrm{C}})]$). Therefore we can once again apply the last statement in Fact 17 (this time identifying $R_{\mathcal{T}}, \widetilde{A}_{\mathcal{T}}$ with C_1, C_2 respectively, which is more similar to our Theorem 18 proof) to conclude that the state produced after step 19 is exactly the same as though $D_{\mathcal{T}}^{\mathrm{B}}$ was generated as a uniformly random value independent of everything else, and $D_{\mathcal{T}}^{\mathrm{C}}$ set equal to it. Since this is something that a dishonest receiver could have done on their own (before distributing $D_{\mathcal{T}}^{\mathrm{B}}$ and $D_{\mathcal{T}}^{\mathrm{C}}$ to Bob and Charlie), we conclude that

$$\max_{\mathcal{C}_{D_{\mathcal{T}}^{\mathrm{B}}D_{\mathcal{T}}^{\mathrm{C}}}} \Pr[(F = \checkmark) \wedge (\widetilde{A}_{\mathcal{T}}^{\mathrm{B}} = G_{\mathcal{T}}^{\mathrm{B}}) \wedge (\widetilde{A}_{\mathcal{T}}^{\mathrm{C}} = G_{\mathcal{T}}^{\mathrm{C}})] = \max_{\mathcal{C}_{\varnothing}} \Pr[(F = \checkmark) \wedge (\widetilde{A}_{\mathcal{T}}^{\mathrm{B}} = G_{\mathcal{T}}^{\mathrm{B}}) \wedge (\widetilde{A}_{\mathcal{T}}^{\mathrm{C}} = G_{\mathcal{T}}^{\mathrm{C}})].$$

Lemma 19 is precisely the statement that the right-hand-side of the above expression[27] is at most $2^{-\kappa\delta_{\gamma,\alpha}^3\alpha^4 l}$, hence proving the desired bound (12). □

[26] Technically, although we have described G^{B} as a guess for $\widetilde{A}^{\mathrm{B}}$ and $\widehat{G}^{\mathrm{B}}$ as a guess for R (and analogously for Charlie), this is not strictly necessary from a purely mathematical standpoint — abstractly, Bob and Charlie are just producing some values in $\{0,1\}^l$ regardless of whether we are considering $\mathcal{C}_Q$ or $\widehat{\mathcal{C}}_Q$; the only difference is how we choose to label and interpret these values. However, using the notation we have presented makes the argument easier to describe.

[27] Notice that the original event of interest $\mathcal{E}_{\mathrm{succ}}$ is a "stricter" condition than the event we have finally ended up considering, namely $(F = \checkmark) \wedge (\widetilde{A}_{\mathcal{T}}^{\mathrm{B}} = G_{\mathcal{T}}^{\mathrm{B}}) \wedge (\widetilde{A}_{\mathcal{T}}^{\mathrm{C}} = G_{\mathcal{T}}^{\mathrm{C}})$ in Lemma 19 (which only requires Bob and Charlie to guess correctly on $\mathcal{T}$, not all the instances). This distinction is basically reflected in the inequality (13) in our proof here, where informally speaking we have allowed Bob and Charlie to "win for free" on $\overline{\mathcal{T}}$ by simply giving them all the values $R_{\overline{\mathcal{T}}}$.

Remark 8. *In principle, an alternative approach to the above arguments is possible, by instead defining the set $\mathcal{T}$ to also include all the instances with $Y_i = Z_i = \perp$. This does not significantly change the overall structure — Lemma 19 still holds with this definition of $\mathcal{T}$ (because making $\mathcal{T}$ a bigger set just makes $(F = \checkmark) \wedge (\widetilde{A}^{\mathrm{B}}_{\mathcal{T}} = G^{\mathrm{B}}_{\mathcal{T}}) \wedge (\widetilde{A}^{\mathrm{C}}_{\mathcal{T}} = G^{\mathrm{C}}_{\mathcal{T}})$ a stricter condition, i.e. the probability of that event can only decrease), and in the proof of Lemma 20, this definition of $\mathcal{T}$ still has the property that $D^{\mathrm{B}}_{\mathcal{T}} = D^{\mathrm{C}}_{\mathcal{T}} = R_{\mathcal{T}} \oplus \widetilde{A}_{\mathcal{T}}$ (in fact this is precisely the "largest" choice of $\mathcal{T}$ on which we can be sure this property holds). Still, we have chosen our definition of $\mathcal{T}$ as presented because the Lemma 19 proof is slightly easier to describe with that choice.*

Finally, with the above lemma we can straightforwardly bound the probability of Bob and Charlie simultaneously guessing the message, hence obtaining uncloneable security. We first present a version without leakage between the devices:

Theorem 21. *With the parameter choices as specified in (8)-(9), Scheme 1 is $(t(\lambda), 0)$-uncloneable-secure with*

$$t(\lambda) = (1 - \kappa\delta^3_{\gamma,\alpha}\alpha^4 + 2\xi(1-\gamma)(1-\alpha)h_2(q))\lambda,$$

if there is no leakage between the client and the receiver's devices during $\mathsf{Enc}(1^\lambda, M)$, and between the two parties Bob and Charlie after the ciphertext is distributed between them in the cloning attack.

Proof. Uncloneable security is defined in terms of the probability $\Pr[(F = \checkmark) \wedge (M = M^{\mathrm{B}} = M^{\mathrm{C}})]$ only, hence we can focus only on the case where $F = \checkmark$ in the protocol. We note that when this happens, the receiver gets the classical value $C = M \oplus R$, and without loss of generality we suppose they distribute copies of it to Bob and Charlie in the cloning attack. Furthermore, Bob and Charlie get the classical values $D^{\mathrm{B}} = R \oplus \widetilde{A}^{\mathrm{B}}$ and $D^{\mathrm{C}} = R \oplus \widetilde{A}^{\mathrm{C}}$ respectively, where $\widetilde{A}^{\mathrm{B}}, \widetilde{A}^{\mathrm{C}}$ are as described in the statement of Lemma 20. From this, we see that Bob and Charlie can simultaneously guess M correctly if and only if Bob can guess $\widetilde{A}^{\mathrm{B}}$ correctly and Charlie can guess $\widetilde{A}^{\mathrm{C}}$ correctly (because e.g. if Bob guesses M correctly, he can get $\widetilde{A}^{\mathrm{B}}$ from $M \oplus C \oplus D^{\mathrm{B}}$; conversely if he guesses $\widetilde{A}^{\mathrm{B}}$ correctly he can get M from $\widetilde{A}^{\mathrm{B}} \oplus C \oplus D^{\mathrm{B}}$). The probability of them doing the latter (and having $F = \checkmark$) is precisely the probability $\Pr[(F = \checkmark) \wedge (\widetilde{A}^{\mathrm{B}} = G^{\mathrm{B}}) \wedge (\widetilde{A}^{\mathrm{C}} = G^{\mathrm{C}})]$ in Lemma 20. Therefore that lemma gives us (recalling that the message length is $|\mathcal{M}| = 2^l$, and substituting (9) for the syndrome length):

$$\Pr[(F = \checkmark) \wedge (M = M^{\mathrm{B}} = M^{\mathrm{C}})] \leq 2^{-\kappa\delta^3_{\gamma,\alpha}\alpha^4 l + 2\ell_{\mathrm{syn}}} = \frac{2^{l - \kappa\delta^3_{\gamma,\alpha}\alpha^4 l + 2\xi(1-\gamma)(1-\alpha)h_2(q)l}}{|\mathcal{M}|}, \tag{14}$$

which is the desired result since $l = \lambda$. □

We can also obtain a similar statement in the presence of leakage, hence proving Theorem 14:

Theorem 22. *With the parameter choices as specified in (8)-(9), Scheme 1 is $(t(\lambda), 0)$-uncloneable-secure with*

$$t(\lambda) = (1 - \kappa\delta^3_{\gamma,\alpha}\alpha^4 + 2\xi(1-\gamma)(1-\alpha)h_2(q) + \nu)\lambda,$$

if the total leakage between the client and the receiver during $\mathsf{Enc}(1^\lambda, M)$, and between Bob and Charlie during the cloning attack, is νl bits.

Proof. Recall from the description in Section 3 that the leakage can be interactive with arbitrarily many rounds of communication between the client and receiver during $\mathsf{Enc}(1^\lambda, M)$, and between

Bob and Charlie during the cloning attack, as long as the total number of bits leaked is bounded. As stated there, we only consider leakage that happens after the devices receive their inputs — for the client the only input is X, and for the receiver and Bob and Charlie, the inputs can be any information that they get. We shall also take the leakage to happen before the devices produce what we consider their outputs, which is A for the client's device, S for the receiver's device, and $\widetilde{A}^{\mathrm{B}}$ and $\widetilde{A}^{\mathrm{C}}$ for Bob and Charlie's devices. Note that in the protocol description we have the client getting X, A in a single step and the receiver only getting U after that, but these steps need not be so strictly time-ordered — we could have the client inputting X into their device and the receiver inputting U into their device at the same time.[28] Moreover, in each round of communication the following happens: the device that receives the message communicated does some measurement on their quantum state depending on this message, their input, and previous messages and previous measurement outcomes, and sends a message to the other device depending on the output of this measurement and their input. Let the number of bits leaked during the encryption phase be $\nu_1 l$, and the number of bits leaked afterwards (which can be e.g. between Bob and Charlie) be $\nu_2 l$, with $\nu_1 + \nu_2 = \nu$.

To bound $\Pr[(F = \checkmark) \wedge (M = M^{\mathrm{B}} = M^{\mathrm{C}})]$, we use an argument essentially similar to the analysis of the syndromes in the Lemma 20 proof: given any strategy in which the leakage bits are used to achieve $\Pr[(F = \checkmark) \wedge (M = M_B = M_C)] = p$ for some $p \in [0, 1]$, there is always another strategy that achieves $\Pr[(F = \checkmark) \wedge (M = M_B = M_C)] \geq 2^{-\nu l} p$ *without* using the leakage bits, which yields the desired result since we have already proven (under the no-leakage scenario) that the latter probability is upper bounded by (14). Explicitly, the strategy is as follows: the client and receiver's devices will share the same initial state they did in the protocol with leakage, and $\nu_1 l$ extra bits of randomness (which can be simulated by shared entanglement), which will be broken up into blocks corresponding to each round of communication in the situation with leakage. Similarly Bob and Charlie's devices will share the same state and $\nu_2 l$ extra bits of randomness divided into blocks. The idea is that the devices will behave just as they did in the original strategy, by using the shared randomness to simulate the communication received from the other device.

We shall denote the j-th block of randomness shared between the client and receiver's devices by s_j. For the rest of this argument, for the sake of brevity, we shall talk about the client and receiver doing things instead of the client and receiver's devices. Suppose the client was supposed to communicate in the j-th round. In the new strategy, the client assumes that s_{j-1} is the message they received from the receiver in the $(j-1)$-th round, and does the same measurement they would have done in the original strategy for this simulated message (the measurement also depends on the client's input, their previous measurement outcomes, and previous simulated messages). If the outcome of the measurement is not equal to s_j, then the client records a "failure" for this round. The receiver behaves similarly in rounds where they were supposed to communicate. After, all the rounds are done, if the client and receiver have not recorded "failure" at any point, they output as they would have done in the original strategy; otherwise they provide a random output. Once the outputs of the measurements are fixed, the protocol is deterministic, so a transcript of messages that is compatible with the client's outputs, and separately compatible with the receiver's outputs, is compatible with both of them. For any such fixed transcript, the shared

[28] There is a slight complication for the receiver in this leakage model because the receiver actually gets information in two rounds; they first receive U and have to produce S, and then they receive C' — there could also be some leakage from the client to the receiver after the receiver receives C, which the receiver could then pass on to Bob and Charlie. But this kind of leakage can be handled by the simple argument we used to deal with $\mathtt{syn}(\widetilde{A})$, so we are ignoring that here. Nevertheless, if such leakage happens, it should count towards the total number of bits leaked, and the dependence of $t(\lambda)$ on the number of bits leaked would be the same.

randomness between the client and receiver is equal to it with probability $2^{-\nu_1 l}$, and therefore with this probability the client and receiver actually output according to the original strategy.

Bob and Charlie behave similarly during their part of the new strategy, and output according to the old strategy with probability $2^{-\nu_2 l}$. Since the probability of satisfying $(F = \checkmark) \wedge (M = M^{\mathrm{B}} = M^{\mathrm{C}})$ in the old strategy is p, the overall probability of satisfying in the new strategy is at least $2^{-\nu l} p$. □

Recall from the discussion below Definition 4 that in order for $(t(\lambda), 0)$-uncloneability to be a nontrivial property, we require $t(\lambda) < \lambda$. For our scheme with the specified parameter choices, this property indeed holds as long as the leakage fraction ν satisfies (note that the right-hand-side in the expression below is strictly positive due to the condition (8) in the protocol parameter specifications)

$$\nu < \kappa \delta^3_{\gamma,\alpha} \alpha^4 - 2\xi(1-\gamma)(1-\alpha) h_2(q). \tag{15}$$

In other words, regarding the claim in our main theorem (Theorem 14), our scheme achieves nontrivial uncloneable security against dishonest devices with any value of ν up to the bound in (15).

6 Single-decryptor encryption

In this section, we prove the following achievability result for DI-SDECM, via a suitable modification of our above DI-VKECM scheme:

Theorem 23. *There is a scheme for DI-SDECM with message space $\mathcal{M} = \{0,1\}^\lambda$, such that:*

1. *It satisfies the completeness property (3) given i.i.d. honest devices with a constant level of noise;*
2. *It achieves indistinguishable security;*
3. *There exists some $\nu > 0$ such that the scheme achieves $(t(\lambda), 0)$-anti-piracy security as per both Definition 7 and Definition 8, against dishonest devices with $\nu\lambda$ bits of leakage, where $t(\lambda)$ is a function satisfying $t(\lambda) < \lambda$ for all sufficiently large λ.*

Our protocol for achieving this is presented as Scheme 2 below. In the description of Scheme 2, the devices, error-correction procedure, and parameter choices are to be understood as being the same as in Section 5. Informally, the changes as compared to Scheme 1 for DI-VKECM are simple: we have just isolated the parts of the previous encryption procedure that did not involve the message m and placed them into the new key generation procedure $\mathsf{KeyGen}(1^\lambda)$, while the parts that involved m have been placed into the new encryption procedure $\mathsf{Enc}(m, k_{\mathrm{enc}}, f)$ (together with the steps that involved selecting a random subset of the device outputs to XOR with other strings, hence moving this randomness into the encryption procedure rather than the previous "key release" procedure). Another change is that in the new key generation procedure $\mathsf{KeyGen}(1^\lambda)$ we do not have the message m and thus cannot produce a string $m \oplus R$ (in contrast to the previous encryption procedure), so instead we simply output the one-time-pad R by itself, which will be XOR'd with the message m later during the new encryption procedure $\mathsf{Enc}(m, k_{\mathrm{enc}}, f)$.[29]

[29] Intuitively, by the "symmetry" between the one-time-pad and its generated ciphertext as expressed in Fact 17, this change should not modify the actual states produced in any manner that is relevant to the security proofs, as we shall discuss below.

Scheme 2 DI-SDECM with security parameter λ and messages in $\mathcal{M} = \{0,1\}^\lambda$

$\mathsf{KeyGen}(1^\lambda)$**:**

1: Devices of the form described in Section 5 are distributed between the client and receiver, with $l = \lambda$
2: The client samples strings X, U as follows: for each $i \in [l]$, set $X_i \in \{0,1\}$ uniformly at random, and independently set $U_i = \text{keep}, 0, 1$ with probabilities $1-\gamma, \gamma/2, \gamma/2$ respectively
3: The client inputs X into their device and receives an output string $A \in \{0,1\}^l$
4: The client sends U to the receiver
5: The receiver inputs U into their device, interpreting $U_i = \text{keep}$ as $\perp$ for each i, and receives an output string $S \in \{0,1\}^l$
6: The receiver sends S to the client
7: The client tests if the number of $i \in [l]$ such that $U_i \neq \text{keep}$ and $A_i \oplus S_i \neq X_i \cdot U_i$ is at most $(\gamma(1-\omega^*(\text{CHSH})) + \delta_{\gamma,\alpha}/2)l$
8: If the test passes then the client sets the flag to $F = \checkmark$; otherwise the client sets the flag to $F = \text{✗}$
9: The client samples $R \in \mathcal{M}$ uniformly at random and sends it to the receiver
10: The client stores (X, U, A, R) as the encryption key and stores the value of the flag F; the receiver stores $\rho = \rho' \otimes |R\rangle\langle R|$ as the decryption key state, where ρ' is the quantum state in the receiver's share of the devices

$\mathsf{Enc}(m, k_{\text{enc}}, f)$**:**

11: Interpret the encryption key as $k_{\text{enc}} = (X, U, A, R)$
12: Sample a string $\widetilde{X} \in \{0,1,\perp\}^l$ as follows: for each $i \in [l]$, set $\widetilde{X}_i = \perp$ with probability α, and otherwise set $\widetilde{X}_i = X_i + 2$
13: Set a string $\widetilde{A} \in \{0,1\}^l$ as follows: for each $i \in [l]$, set $\widetilde{A}_i = 0$ if $U_i \neq \text{keep}$ or $\widetilde{X}_i = \perp$, and otherwise set $\widetilde{A}_i = A_i$
14: Compute the syndrome $\mathtt{syn}(\widetilde{A})$ following the error-correction procedure described above
15: **if** $f = \checkmark$ **then**
16: Output the ciphertext string $(m \oplus R \oplus \widetilde{A}, \mathtt{syn}(\widetilde{A}), \widetilde{X})$
17: **else**
18: Sample $M^{\text{fake}} \in \mathcal{M}$ uniformly at random and output the ciphertext string $(M^{\text{fake}} \oplus R \oplus \widetilde{A}, \mathtt{syn}(\widetilde{A}), \widetilde{X})$

$\mathsf{Dec}(c, \rho)$**:**

19: Interpret ρ as $\rho' \otimes |R\rangle\langle R|$ where ρ' has l qubit registers and $R \in \mathcal{M}$; interpret the ciphertext string c as $(N, \mathtt{syn}(\widetilde{A}), \widetilde{X})$
20: Input $\widetilde{X}$ into the receiver's device and obtain the output string $S' \in \{0,1\}^l$
21: Set a string $\widetilde{S} \in \{0,1\}^l$ as follows: for each $i \in [l]$, set $\widetilde{S}_i = 0$ if $U_i \neq \text{keep}$ or $\widetilde{X}_i = \perp$, and otherwise set $\widetilde{S}_i = S'_i$
22: Use $\widetilde{S}, U, \widetilde{X}$ and $\mathtt{syn}(\widetilde{A})$ to compute a guess G for $\widetilde{A}$
23: Output $\widetilde{M} = R \oplus N \oplus G$

6.1 Completeness and security of Scheme 2

It is straightforward to see that Scheme 2 satisfies the completeness requirements in Definition 6, since in the honest case the various registers produced are identical to Scheme 1 up to some minor rearrangements regarding R, and hence in the completeness analysis in Section 5.1 carries over directly. As for security, we clearly have indistinguishable security, and it is also not too hard to modify our previous arguments to show anti-piracy security:

Lemma 24. *Scheme 1 is indistinguishable-secure.*

Proof. Indistinguishable security only involves the ciphertext produced by the encryption procedure, without having access to the decryption key K_{dec}. Observe that in the encryption procedure (focusing on the $F = \checkmark$ case, since in the $F = \text{✗}$ case the ciphertext is trivially independent of m), the only part of the ciphertext that depends on the message m is the $m \oplus R \oplus \widetilde{A}$ part. However, recall that R was generated as a uniformly random string independent of everything else (including the other parts of the ciphertext), and hence serves as a perfect one-time-pad. Hence indistinguishable security clearly holds (explicitly: one could e.g. apply Fact 17 to conclude that $m \oplus R \oplus \widetilde{A}$ is completely independent of $m \oplus \widetilde{A}$, which is the only quantity depending on m). □

Lemma 25. *With the parameter choices as specified in (8)-(9), Scheme 2 is $(t(\lambda), 0)$-anti-piracy-secure as per Definition 7 and Definition 8 with*

$$t(\lambda) = (1 - \kappa\delta^3_{\gamma,\alpha}\alpha^4 + 2\xi(1-\gamma)(1-\alpha)h_2(q) + \nu)\lambda,$$

if the total leakage between the client and the receiver during $\mathsf{KeyGen}(1^\lambda)$, and between Bob and Charlie during the pirating attack, is νl bits.

Proof. To show security by Definition 7, observe that for a pirating attack applied to Scheme 2, the steps performed by the dishonest parties and the registers available to them at each step are exactly the same as in a cloning attack applied to Scheme 1, except with the sole modification that the one-time-pad R and the padded message $M \oplus R$ have had their roles interchanged. However, by Fact 17 these two values are precisely interchangeable, and hence our analysis in Section 5.2 for Scheme 1 carries over exactly (noting that the final event of interest is also the same between the definitions of $(t(\lambda), 0)$-anti-piracy security and $(t(\lambda), 0)$-uncloneable security).

To show security by Definition 8, we also just need to basically repeat the analysis in Section 5.2, although we need to modify specific parts of the proofs rather than simply invoking the symmetry between R and $M \oplus R$ as in the preceding case (since in this case the two independent messages make the register values somewhat different as compared to a cloning attack on Scheme 1). To highlight the key points: first observe that following the Theorem 21 proof, we again have that the maximum probability that $F = \checkmark$ and Bob and Charlie can simultaneously guess their respective message values is the same as the maximum probability that $F = \checkmark$ and they can simultaneously guess $\widetilde{A}^{\text{B}}$ and $\widetilde{A}^{\text{C}}$ respectively. Hence it suffices to bound the latter, which can be done by following a similar argument as the Lemma 20 proof, now defining the sets $\mathcal{C}_{RP^{\text{B}}P^{\text{C}}H^{\text{B}}H^{\text{C}}}, \ldots, \mathcal{C}_{\emptyset}$ with respect to pirating attacks rather than cloning attacks (and letting P^{B} denote the value $M_1 \oplus R \oplus \widetilde{A}^{\text{B}}$ Bob receives in his ciphertext, and analogously $P^{\text{C}} = M_2 \oplus R \oplus \widetilde{A}^{\text{C}}$ for Charlie); our aim is then to bound $\max_{\mathcal{C}_{RP^{\text{B}}P^{\text{C}}H^{\text{B}}H^{\text{C}}}} \Pr[\mathcal{E}_{\text{succ}}]$. To do so, we handle the syndromes $H^{\text{B}}H^{\text{C}}$ by the same argument, to get an upper bound in terms of $\max_{\mathcal{C}_{RP^{\text{B}}P^{\text{C}}}} \Pr[\mathcal{E}_{\text{succ}}]$. This time however, handling the registers $RP^{\text{B}}P^{\text{C}}$ is actually easier: in this scenario P^{B} is just a value $R \oplus \widetilde{A}^{\text{B}}$

one-time-padded with the value M_1 (which is not involved with any other register in this scenario), hence Fact 17 implies Bob could have generated it locally, and it can be removed in the sense that we have $\max_{\mathcal{C}_{RP^{\mathrm{B}}P^{\mathrm{C}}}} \Pr[\mathcal{E}_{\mathrm{succ}}] = \max_{\mathcal{C}_{RP^{\mathrm{C}}}} \Pr[\mathcal{E}_{\mathrm{succ}}]$.[30] Similarly, P^{C} is just a value $R \oplus \widetilde{A}^{\mathrm{C}}$ one-time-padded with the value M_2 and can also be removed. This leaves only R, which (with $P^{\mathrm{B}}P^{\mathrm{C}}$ excluded from consideration) is just a register that could have been generated locally by the receiver before distributing states to Bob and Charlie, and hence can also be removed. Summarizing, this gives $\max_{\mathcal{C}_{RP^{\mathrm{B}}P^{\mathrm{C}}}} \Pr[\mathcal{E}_{\mathrm{succ}}] = \max_{\mathcal{C}_{\varnothing}} \Pr[\mathcal{E}_{\mathrm{succ}}]$, yielding the desired bound via Lemma 19 (recalling that $\mathcal{E}_{\mathrm{succ}}$ is a "stricter" event than the one considered in that lemma). □

7 Single-decryptor encryption of bits and trits

We now describe how Scheme 2 can be modified to achieve "perfect" anti-piracy security under Definition 8 for the cases where the message space is a single bit or trit (i.e. $\mathcal{M} = \mathbb{F}_2$ or $\mathbb{F}_3$; later in this section we describe some obstacles faced in generalizing this result to larger $\mathbb{F}_p$, as well as a technical difficulty in applying it to DI-VKECM or Definition 7 of anti-piracy security). Specifically, we obtain the following result:

Theorem 26. *There is a scheme for DI-SDECM with message space $\mathcal{M} = \mathbb{F}_2$ or $\mathcal{M} = \mathbb{F}_3$ which achieves the first two properties as in Theorem 23 and $(0, \mathrm{negl}(\lambda))$-anti-piracy security as per Definition 8, against dishonest devices with $v\lambda$ bits of leakage, as long as*

$$3v < \kappa\delta^3_{\gamma,\alpha}\alpha^4 - 2(1-\gamma)(1-\alpha)h_2(q). \tag{16}$$

Qualitatively, the idea is to implement a form of randomness extraction or privacy amplification [TSSR11, DPVR12]. In our setting, from Lemma 20 we have a bound on the probability of Bob and Charlie being able to simultaneously guess the "raw key" strings $\widetilde{A}^{\mathrm{B}}, \widetilde{A}^{\mathrm{C}}$. Our goal here to process $\widetilde{A}^{\mathrm{B}}, \widetilde{A}^{\mathrm{C}}$ into shorter strings such that their probability of being able to simultaneously guess the shorter strings is only negligibly larger than the trivial guessing probability, from which we could achieve $(0, \mathrm{negl}(\lambda))$-anti-piracy security.

Explicitly, the modification to Scheme 2 is as follows. The input/output string length l for the devices is still set equal to the security parameter λ as before, but the message space is now $\mathcal{M} = \mathbb{F}_p$ for $p = 2$ or 3. The following steps in the protocol are modified:

- In step 9 of KeyGen, the "one-time-pad" R is instead drawn uniformly at random in $\mathbb{F}_p$.
- In step 16 of Enc, instead of setting $(m \oplus R \oplus \widetilde{A}, \mathtt{syn}(\widetilde{A}), \widetilde{X})$ as the ciphertext, the following procedure is performed: a uniformly random value $V \in \mathbb{F}_p^l$ is generated (independently of everything else), and the ciphertext is set as $(m \oplus R \oplus \widetilde{A} \cdot V, \mathtt{syn}(\widetilde{A}), \widetilde{X}, V)$, where $\widetilde{A} \cdot V$ denotes inner product with respect to $\mathbb{F}_p$, and $\oplus$ is computed modulo p. Note that the random value V is included in the ciphertext.
- In step 23 of Dec, the final output is instead computed as $\widetilde{M} = R \oplus D \oplus G \cdot V$, where $G \cdot V$ is computed using the value of V included in the ciphertext.

[30] This proof structure did not work for the Lemma 20 proof because the values $D^{\mathrm{B}} = R \oplus \widetilde{A}^{\mathrm{B}}$, $D^{\mathrm{C}} = R \oplus \widetilde{A}^{\mathrm{C}}$ were padded with a *common* value R, preventing us from applying Fact 17. This issue was handled in that proof via the more elaborate argument where we allowed Bob and Charlie to "win for free" on $\overline{T}$ by giving them all the values $R_{\overline{T}}$.

Qualitatively, the randomized value V serves as a method to "extract" the randomness in $\widetilde{A}$. We highlight that similar to the standard setting for strong extractors (viewing V as the extractor seed), V can be revealed to the party trying to guess the inner-product value (and this is a necessary property in our context, since an honest receiver would need to use it in decrypting the message).

To show that this modified protocol indeed achieves $(0, \mathrm{negl}(\lambda))$-anti-piracy security, we basically need to show that if Bob and Charlie try to simultaneously guess their corresponding inner-product values, they only have a negligible advantage over the trivial success probability of $1/p$. This brings us to the main technical result of this section, which can be thought of as a simultaneous non-local version of the quantum Goldreich-Levin theorem [AC02]:

Lemma 27. *Consider a CQ state $\rho_{X^{\mathrm{B}}X^{\mathrm{C}}BC}$, where X^{B} and X^{C} are both classical registers taking values in $\mathbb{F}_p^l$, while B and C are quantum registers held by Bob and Charlie respectively. Further, suppose for any measurements Bob and Charlie can do on their quantum registers to produce outputs G^{B} and G^{C}, we have*

$$\Pr[(G^{\mathrm{B}} = X^{\mathrm{B}}) \wedge (G^{\mathrm{C}} = X^{\mathrm{C}})] \leq \delta,$$

where the probability is taken over the distribution of $X^{\mathrm{B}}X^{\mathrm{C}}$. Consider $V^{\mathrm{B}}, V^{\mathrm{C}}$ which are indepedently and uniformly distributed in $\mathbb{F}_p^l$. If V^{B} and V^{C} are given to Bob and Charlie respectively, and they do measurements on their quantum registers depending on V^{B} and V^{C}, to produce outputs $G^{\mathrm{B}}(V^{\mathrm{B}})$ and $G^{\mathrm{C}}(V^{\mathrm{C}})$, then we have for $p = 2, 3$,

$$\Pr\left[\bigvee_{\substack{j,k:\\ j+k=0 \mod p}} (G^{\mathrm{B}}(V^{\mathrm{B}}) = X^{\mathrm{B}} \cdot V^{\mathrm{B}} + j) \wedge (G^{\mathrm{C}}(V^{\mathrm{C}}) = X^{\mathrm{C}} \cdot V^{\mathrm{C}} + k)\right] \leq \frac{1}{p} + O(\delta^{1/3}),$$

where the probability is taken over the distribution of $X^{\mathrm{B}}X^{\mathrm{C}}, V^{\mathrm{B}}V^{\mathrm{C}}$.

Note that the event whose probability is being upper bounded in the lemma for $p = 2$ is that Bob and Charlie both guess $X^{\mathrm{B}} \cdot V^{\mathrm{B}}$ and $X^{\mathrm{C}} \cdot V^{\mathrm{C}}$ respectively right, or they both guess wrong. If $p = 3$, the event is that they both guess right, or one of their guesses is off by 1, and the other's guess is off by 2. An upper bound on the probability of this event obviously implies an upper bound on the probability of them both guessing right. But as we shall see later, in order to prove a version of this lemma with leakage, we shall actually need the fact that we can prove an upper bound on the probability of this larger event in the case without leakage.

Proof of Lemma 27. We shall assume that for any fixed $X^{\mathrm{B}}X^{\mathrm{C}} = x^{\mathrm{B}}x^{\mathrm{C}}$, $\rho_{BC|x^{\mathrm{B}}x^{\mathrm{C}}}$ is a pure state $|\rho\rangle\langle\rho|_{BC|x^{\mathrm{B}}x^{\mathrm{C}}}$. This is without loss of generality, because we can always consider a purification of the state — Bob and Charlie may not have access to the purifying registers, but that will not matter for the purposes of our argument.

The proof will be via contradiction: supposing Bob and Charlie have a strategy in which they use V^{B} and V^{C} to produce outputs $G^{\mathrm{B}}(V^{\mathrm{B}})$ and $G^{\mathrm{C}}(V^{\mathrm{C}})$ such that

$$\Pr_{X^{\mathrm{B}}X^{\mathrm{C}}V^{\mathrm{B}}V^{\mathrm{C}}}\left[\bigvee_{\substack{j,k:\\ j+k=0 \mod p}} (G^{\mathrm{B}}(V^{\mathrm{B}}) = X^{\mathrm{B}} \cdot V^{\mathrm{B}} + j) \wedge (G^{\mathrm{C}}(V^{\mathrm{C}}) = X^{\mathrm{C}} \cdot V^{\mathrm{C}} + k)\right] > \frac{1}{p} + \varepsilon, \tag{17}$$

we shall construct a procedure for Bob and Charlie to learn X^{B} and X^{C} with probability greater than $\Omega(\varepsilon^3)$. To begin, note that for each value of $x^{\mathrm{B}}, x^{\mathrm{C}}, v^{\mathrm{B}}, v^{\mathrm{C}}$, without loss of generality we can model Bob and Charlie's procedure to obtain their guesses for $x^{\mathrm{B}} \cdot v^{\mathrm{B}}$ and $x^{\mathrm{C}} \cdot v^{\mathrm{C}}$ (using $|\rho\rangle_{BC|x^{\mathrm{B}}x^{\mathrm{C}}}$ and $v^{\mathrm{B}}, v^{\mathrm{C}}$) as follows: they each attach a p-dimensional ancilla, which is to be their output register, to their halves of $|\rho\rangle_{BC|x^{\mathrm{B}}x^{\mathrm{C}}}$, and apply unitaries controlled on v^{B} and v^{C} respectively to the state and ancillas. The output value is then obtained by measuring their ancilla registers in the computational basis. Suppose the action of the unitaries, which we shall call $U_{\mathrm{IP}}^{\mathrm{B}}$ and $U_{\mathrm{IP}}^{\mathrm{C}}$, is as follows:

$$\begin{aligned} &U_{\mathrm{IP}}^{\mathrm{B}} \otimes U_{\mathrm{IP}}^{\mathrm{C}} \, |v^{\mathrm{B}}v^{\mathrm{C}}\rangle_{V^{\mathrm{B}}V^{\mathrm{C}}} \, |00\rangle_{Z^{\mathrm{B}}Z^{\mathrm{C}}} \, |\rho\rangle_{BC|x^{\mathrm{B}}x^{\mathrm{C}}} \\ &= |v^{\mathrm{B}}v^{\mathrm{C}}\rangle_{V^{\mathrm{B}}V^{\mathrm{C}}} \sum_{j,k \in \mathbb{F}_p} \alpha_{x^{\mathrm{B}}x^{\mathrm{C}}jk}^{v^{\mathrm{B}}v^{\mathrm{C}}} \, |x^{\mathrm{B}} \cdot v^{\mathrm{B}} + j\rangle_{Z^{\mathrm{B}}} \, |x^{\mathrm{C}} \cdot v^{\mathrm{C}} + k\rangle_{Z^{\mathrm{C}}} \, |\sigma^{v^{\mathrm{B}}v^{\mathrm{C}}}\rangle_{BC|x^{\mathrm{B}}x^{\mathrm{C}}jk} . \end{aligned}$$

In the above, $U_{\mathrm{IP}}^{\mathrm{B}}$ acts on the registers $V^{\mathrm{B}}Z^{\mathrm{B}}B$ and $U_{\mathrm{IP}}^{\mathrm{C}}$ acts on $V^{\mathrm{C}}Z^{\mathrm{C}}C$. After their action, the $V^{\mathrm{B}}V^{\mathrm{C}}$ registers remain unchanged; there is some superposition of answers of the form $x^{\mathrm{B}} \cdot v^{\mathrm{B}} + j$ and $x^{\mathrm{C}} \cdot v^{\mathrm{C}} + k$ (where all additions are modulo p) on the answer registers $Z^{\mathrm{B}}, Z^{\mathrm{C}}$, and corresponding to these answers, the state on the BC registers is $|\sigma^{v^{\mathrm{B}}v^{\mathrm{C}}}\rangle_{BC|x^{\mathrm{B}}x^{\mathrm{C}}jk}$. The probability of getting answers $x^{\mathrm{B}} \cdot x^{\mathrm{C}} + j$ and $x^{\mathrm{C}} \cdot v^{\mathrm{C}} + k$ is $|\alpha_{x^{\mathrm{B}}x^{\mathrm{C}}jk}^{v^{\mathrm{B}}v^{\mathrm{C}}}|^2$.

Also, note that by applying Markov's inequality on (17) we have that

$$\begin{aligned} &\Pr_{X^{\mathrm{B}}X^{\mathrm{C}}} \left[\Pr_{V^{\mathrm{B}}V^{\mathrm{C}}} \left[\bigvee_{\substack{j,k: \\ j+k=0 \mod p}} (G^{\mathrm{B}}(V^{\mathrm{B}}) = X^{\mathrm{B}} \cdot V^{\mathrm{B}} + j) \wedge (G^{\mathrm{C}}(V^{\mathrm{C}}) = X^{\mathrm{C}} \cdot V^{\mathrm{C}} + k) \right] \leq \frac{1}{p} + \frac{\varepsilon}{2} \right] \\ \leq &\frac{1 - \frac{1}{p} - \varepsilon}{1 - \frac{1}{p} - \frac{\varepsilon}{2}} \leq 1 - \frac{\varepsilon}{2}. \end{aligned}$$

This means that with probability at least $\frac{\varepsilon}{2}$ over the distribution of $X^{\mathrm{B}}X^{\mathrm{C}}$, Bob and Charlie's average probability (over the distribution of $V^{\mathrm{B}}V^{\mathrm{C}}$) of outputting $x^{\mathrm{B}} \cdot v^{\mathrm{B}} + j$ and $x^{\mathrm{C}} \cdot v^{\mathrm{C}} + k$ for $j + k = 0 \mod p$ is at least $\frac{1}{p} + \frac{\varepsilon}{2}$. We shall call pairs $x^{\mathrm{B}}x^{\mathrm{C}}$ for which this is true "good" pairs. We shall now concentrate on a good pair $x^{\mathrm{B}}x^{\mathrm{C}}$, and henceforth in the analysis, we shall drop the $x^{\mathrm{B}}x^{\mathrm{C}}$ dependence from $|\rho\rangle_{BC|x^{\mathrm{B}}x^{\mathrm{C}}}$ and $|\sigma^{v^{\mathrm{B}}v^{\mathrm{C}}}\rangle_{BC|x^{\mathrm{B}}x^{\mathrm{C}}jk}$ and $\alpha_{x^{\mathrm{B}}x^{\mathrm{C}}jk}^{v^{\mathrm{B}}v^{\mathrm{C}}}$ (with the understanding that we are now only focusing on a fixed good pair $x^{\mathrm{B}}x^{\mathrm{C}}$).

Since $x^{\mathrm{B}}x^{\mathrm{C}}$ is a good pair, we have that

$$\frac{1}{p^{2l}} \sum_{v^{\mathrm{B}}v^{\mathrm{C}}} \sum_{j+k=0} \left| \alpha_{jk}^{v^{\mathrm{B}}v^{\mathrm{C}}} \right|^2 \geq \frac{1}{p} + \frac{\varepsilon}{2}. \tag{18}$$

We shall now show there exists a procedure independent of $x^{\mathrm{B}}x^{\mathrm{C}}$ that Bob and Charlie can perform on $|\rho\rangle_{BC}$, such that (given that $x^{\mathrm{B}}x^{\mathrm{C}}$ is a good pair) Bob and Charlie output $x^{\mathrm{B}}x^{\mathrm{C}}$ with probability at least $\Omega(\varepsilon^2)$. Essentially, Bob and Charlie will carry out the Bernstein-Vazirani algorithm independently, using $U_{\mathrm{IP}}^{\mathrm{B}}$ and $U_{\mathrm{IP}}^{\mathrm{C}}$ as noisy oracles. The circuit for doing so is depicted below in Figure 2.

Bob's registers in this circuit are $V^{\mathrm{B}}Z^{\mathrm{B}}\widetilde{Z}^{\mathrm{B}}B$, and Charlie's registers are $V^{\mathrm{C}}Z^{\mathrm{C}}\widetilde{Z}^{\mathrm{C}}B$. The circuit essentially does the following: it prepares a uniform superposition of v^{B} and v^{C} by applying $F_p^{\otimes l}$

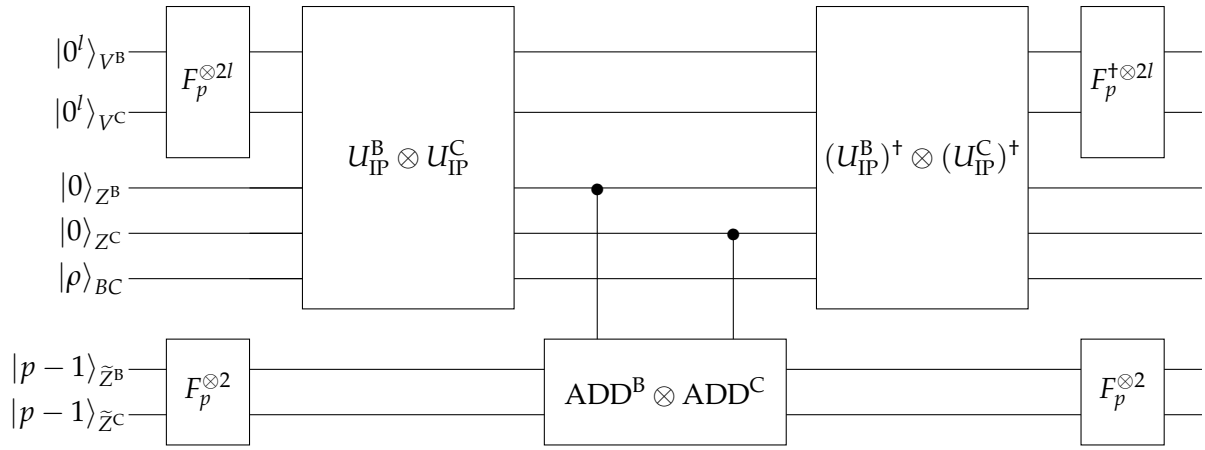

Figure 2: Circuit to compute x^B, x^C in good set

on the $|0^l\rangle$ state in the V^B and V^C registers respectively. Here F_p is the $\mathbb{F}_p$ Fourier transform, whose action on computational basis states is given by

$$F_p |j\rangle = \frac{1}{\sqrt{p}} \sum_{k \in \mathbb{F}_p} \omega^{jk} |k\rangle ,$$

with ω being the p-th root of unity. At the same time as $F_p^{\otimes l}$, the circuit applies $F_p^{\otimes 2}$ to the registers $\widetilde{Z}^B$ and $\widetilde{Z}^C$, which are initialized with $|p-1\rangle |p-1\rangle$. The effect of the Fourier transforms on these registers is

$$F_p^{\otimes 2} |p-1\rangle_{\widetilde{Z}^B} |p-1\rangle_{\widetilde{Z}^C} = \frac{1}{p} \sum_{j',k' \in \mathbb{F}_p} \omega^{(p-1)j'+(p-1)k'} |j'k'\rangle_{\widetilde{Z}^B\widetilde{Z}^C} = \frac{1}{p} \sum_{j',k' \in \mathbb{F}_p} \omega^{-j'-k'} |j'k'\rangle_{\widetilde{Z}^B\widetilde{Z}^C} .$$

After this, the unitaries $U_{\mathrm{IP}}^B \otimes U_{\mathrm{IP}}^C$ are acted on the registers $V^B V^C Z^B Z^C BC$, and then the ADD^B and ADD^C gates acting on the registers $Z^B\widetilde{Z}^B$ and $Z^C\widetilde{Z}^C$ registers respectively are applied. The ADD^B gate essentially adds (modulo p) the value in the Z^B register to the value in the $\widetilde{Z}^B$ register, and similarly, the ADD^C gate adds the value in the Z^C register to the $\widetilde{Z}^C$ register. After this, the inverses of the $U_{\mathrm{IP}}^B \otimes U_{\mathrm{IP}}^C$ gates and the $F_p^{\otimes(2l+2)}$ gates are added on their respective registers. Finally, Bob measures the V^B register and Charlie measures the V^C register, both in the computational basis. Note that all these steps can be carried out by Bob acting only on his registers, and Charlie acting only on his registers.

The probability that Bob and Charlie measure the $V^B V^C$ registers and both get the correct values x^B and x^C is at least

$$\left| \langle x^B x^C|_{V^B V^C} \langle 00|_{Z^B Z^C} \langle \rho|_{BC} \langle p-1, p-1|_{\widetilde{Z}^B\widetilde{Z}^C} U_5 U_4 U_3 U_2 U_1 |0^l 0^l\rangle_{V^B V^C} |00\rangle_{Z^B Z^C} |\rho\rangle_{BC} |p-1, p-1\rangle_{\widetilde{Z}^B\widetilde{Z}^C} \right|^2 ,$$

where $U_1 = F_p^{\otimes(2l+2)}$, $U_2 = U_{\mathrm{IP}}^B \otimes U_{\mathrm{IP}}^C$, $U_3 = \mathrm{ADD}^B \otimes \mathrm{ADD}^C$, $U_4 = (U_{\mathrm{IP}}^B)^\dagger \otimes (U_{\mathrm{IP}}^C)^\dagger$ and $U_5 = F_p^{\otimes(2l+2)}$. To calculate this, we observe

$$\begin{aligned} &U_3 U_2 U_1 |0^l 0^l\rangle_{V^B V^C} |00\rangle_{Z^B Z^C} |\rho\rangle_{BC} |p-1, p-1\rangle_{\widetilde{Z}^B\widetilde{Z}^C} \\ =&U_3 U_2 \left(\frac{1}{p^{l+1}} \sum_{v^B, v^C \in \mathbb{F}_p^l} |v^B v^C\rangle_{V^B V^C} |00\rangle_{Z^B Z^C} |\rho\rangle_{BC} \sum_{j',k' \in \mathbb{F}_p} \omega^{-j'-k'} |j', k'\rangle_{\widetilde{Z}^B\widetilde{Z}^C} \right) \end{aligned}$$

$$
\begin{aligned}
=&U_3\left(\frac{1}{p^{l+1}}\sum_{v^{\mathrm{B}},v^{\mathrm{C}}\in\mathbb{F}_p^l}|v^{\mathrm{B}}v^{\mathrm{C}}\rangle\sum_{j,k\in\mathbb{F}_p}\alpha_{jk}^{v^{\mathrm{B}}v^{\mathrm{C}}}|x^{\mathrm{B}}\cdot v^{\mathrm{B}}+j,x^{\mathrm{C}}\cdot v^{\mathrm{C}}+k\rangle|\sigma^{v^{\mathrm{B}}v^{\mathrm{C}}}\rangle_{jk}\sum_{j',k'\in\mathbb{F}_p}\omega^{-j'-k'}|j',k'\rangle\right)\\
=&\frac{1}{p^{l+1}}\sum_{v^{\mathrm{B}},v^{\mathrm{C}}}|v^{\mathrm{B}}v^{\mathrm{C}}\rangle\sum_{j,k}\alpha_{jk}^{v^{\mathrm{B}}v^{\mathrm{C}}}|x^{\mathrm{B}}\cdot v^{\mathrm{B}}+j,x^{\mathrm{C}}\cdot v^{\mathrm{C}}+k\rangle|\sigma^{v^{\mathrm{B}}v^{\mathrm{C}}}\rangle_{jk}\sum_{j',k'}\omega^{-j'-k'}|x^{\mathrm{B}}\cdot v^{\mathrm{B}}+j+j',x^{\mathrm{C}}\cdot v^{\mathrm{C}}+k+k'\rangle\\
=&\frac{1}{p^{l+1}}\sum_{v^{\mathrm{B}},v^{\mathrm{C}}}|v^{\mathrm{B}}v^{\mathrm{C}}\rangle\sum_{j,k}\alpha_{jk}^{v^{\mathrm{B}}v^{\mathrm{C}}}\omega^{x^{\mathrm{B}}\cdot v^{\mathrm{B}}+j+x^{\mathrm{C}}\cdot v^{\mathrm{C}}+k}|x^{\mathrm{B}}\cdot v^{\mathrm{B}}+j,x^{\mathrm{C}}\cdot v^{\mathrm{C}}+k\rangle|\sigma^{v^{\mathrm{B}}v^{\mathrm{C}}}\rangle_{jk}\sum_{j',k'}\omega^{-j'-k'}|j',k'\rangle\,.
\end{aligned}
$$

Similarly,

$$
\begin{aligned}
&\langle x^{\mathrm{B}}x^{\mathrm{C}}|_{V^{\mathrm{B}}V^{\mathrm{C}}}\langle 00|_{Z^{\mathrm{B}}Z^{\mathrm{C}}}\langle\rho|_{BC}\langle p-1,p-1|_{\widetilde{Z}^{\mathrm{B}}\widetilde{Z}^{\mathrm{C}}}U_5U_4\\
=&\left(\frac{1}{p^{l+1}}\sum_{v^{\mathrm{B}},v^{\mathrm{C}}}\omega^{-x^{\mathrm{B}}\cdot v^{\mathrm{B}}-x^{\mathrm{C}}\cdot v^{\mathrm{C}}}\langle v^{\mathrm{B}}v^{\mathrm{C}}|\langle 00|_{Z^{\mathrm{B}}Z^{\mathrm{C}}}\langle\rho|_{BC}\sum_{j',k'}\omega^{j'+k'}\langle j',k'|_{\widetilde{Z}^{\mathrm{B}}\widetilde{Z}^{\mathrm{C}}}\right)U_4\\
=&\frac{1}{p^{l+1}}\sum_{v^{\mathrm{B}},v^{\mathrm{C}}}\omega^{-x^{\mathrm{B}}\cdot v^{\mathrm{B}}-x^{\mathrm{C}}\cdot v^{\mathrm{C}}}\langle v^{\mathrm{B}}v^{\mathrm{C}}|\sum_{j,k}(\alpha_{jk}^{v^{\mathrm{B}}v^{\mathrm{C}}})^*\langle x^{\mathrm{B}}\cdot v^{\mathrm{B}}+j,x^{\mathrm{C}}\cdot v^{\mathrm{C}}+k|\langle\sigma^{v^{\mathrm{B}}v^{\mathrm{C}}}|_{jk}\sum_{j',k'}\omega^{j'+k'}\langle j',k'|_{\widetilde{Z}^{\mathrm{B}}\widetilde{Z}^{\mathrm{C}}}\,.
\end{aligned}
$$

Note that the states $|v^{\mathrm{B}}v^{\mathrm{C}}\rangle|x^{\mathrm{B}}\cdot v^{\mathrm{B}}+j,x^{\mathrm{C}}\cdot v^{\mathrm{C}}+k\rangle|\sigma^{v^{\mathrm{B}}v^{\mathrm{C}}}\rangle_{jk}$ are orthogonal for different values of $v^{\mathrm{B}},v^{\mathrm{C}},j$ and k. Therefore we have,

$$
\begin{aligned}
&\langle x^{\mathrm{B}}x^{\mathrm{C}}|\langle 00|\langle\rho|\langle p-1,p-1|U_5U_4U_3U_2U_1|0^l0^l\rangle|00\rangle|\rho\rangle|p-1,p-1\rangle\\
=&\frac{1}{p^{2l}}\sum_{v^{\mathrm{B}},v^{\mathrm{C}}}\sum_{j,k\in\mathbb{F}_p}\left|\alpha_{jk}^{v^{\mathrm{B}}v^{\mathrm{C}}}\right|^2\omega^{j+k}\\
=&\sum_{k'\in\mathbb{F}_p}\left(\sum_{j'\in\mathbb{F}_p}\frac{1}{p^{2l}}\sum_{v^{\mathrm{B}},v^{\mathrm{C}}}\left|\alpha_{j',k'-j'}^{v^{\mathrm{B}}v^{\mathrm{C}}}\right|^2\right)\omega^{k'},
\end{aligned}
\tag{19}
$$

where $k'-j'$ in the subscript of $\alpha_{j',k'-j'}^{v^{\mathrm{B}}v^{\mathrm{C}}}$ is meant to be interpreted modulo p.

For $p=2$, $\omega=-1$, so the above expression is

$$
\frac{1}{2^{2l}}\sum_{v^{\mathrm{B}}v^{\mathrm{C}}}\left|\alpha_{00}^{v^{\mathrm{B}}v^{\mathrm{C}}}\right|^2+\frac{1}{2^{2l}}\sum_{v^{\mathrm{B}}v^{\mathrm{C}}}\left|\alpha_{11}^{v^{\mathrm{B}}v^{\mathrm{C}}}\right|^2-\frac{1}{2^{2l}}\sum_{v^{\mathrm{B}}v^{\mathrm{C}}}\left|\alpha_{01}^{v^{\mathrm{B}}v^{\mathrm{C}}}\right|^2-\frac{1}{2^{2l}}\sum_{v^{\mathrm{B}}v^{\mathrm{C}}}\left|\alpha_{10}^{v^{\mathrm{B}}v^{\mathrm{C}}}\right|^2
$$

For a good $x^{\mathrm{B}}x^{\mathrm{C}}$, by (18), we have $\frac{1}{2^{2l}}\sum_{v^{\mathrm{B}}v^{\mathrm{C}}}(|\alpha_{00}^{v^{\mathrm{B}}v^{\mathrm{C}}}|^2+|\alpha^{v^{\mathrm{B}}v^{\mathrm{C}}}|^2)\geq\frac{1}{2}+\frac{\varepsilon}{2}$, which means that $\frac{1}{2^{2l}}\sum_{v^{\mathrm{B}}v^{\mathrm{C}}}(|\alpha_{01}^{v^{\mathrm{B}}v^{\mathrm{C}}}|^2+|\alpha_{10}^{v^{\mathrm{B}}v^{\mathrm{C}}}|^2)$ is at most $\frac{1}{2}-\frac{\varepsilon}{2}$. Therefore, the probability of Bob and Charlie learning $x^{\mathrm{B}}x^{\mathrm{C}}$ from the good set is at least

$$
\left|\frac{1}{2}+\frac{\varepsilon}{2}-\frac{1}{2}+\frac{\varepsilon}{2}\right|^2\geq\varepsilon^2.
$$

Since the probability of $X^{\mathrm{B}}X^{\mathrm{C}}$ being from the good set is at least $\frac{\varepsilon}{2}$, the overall probability of Bob and Charlie learning $X^{\mathrm{B}}X^{\mathrm{C}}$ is at least $\frac{\varepsilon^3}{2}=\Omega(\varepsilon^3)$ as claimed.

For $p=3$, (19) instead becomes

$$
\frac{1}{3^{2l}}\sum_{v^{\mathrm{B}}v^{\mathrm{C}}}\left(\left|\alpha_{00}^{v^{\mathrm{B}}v^{\mathrm{C}}}\right|^2+\left|\alpha_{12}^{v^{\mathrm{B}}v^{\mathrm{C}}}\right|^2+\left|\alpha_{21}^{v^{\mathrm{B}}v^{\mathrm{C}}}\right|^2+\omega\left(\left|\alpha_{01}^{v^{\mathrm{B}}v^{\mathrm{C}}}\right|^2+\left|\alpha_{10}^{v^{\mathrm{B}}v^{\mathrm{C}}}\right|^2+\left|\alpha_{22}^{v^{\mathrm{B}}v^{\mathrm{C}}}\right|^2\right)\right.
$$

$$+ \omega^2 \left(\left| \alpha_{11}^{v^B v^C} \right|^2 + \left| \alpha_{02}^{v^B v^C} \right|^2 + \left| \alpha_{20}^{v^B v^C} \right|^2 \right) \Bigg).$$

We can thus write the probability of learning a good $x^B x^C$ as

$$|a_0 + a_1\omega + a_2\omega^2|^2 = a_0^2 + a_1^2 + a_2^2 - a_0a_1 - a_0a_2 - a_1a_2,$$

where $a_0 + a_1 + a_2 = 1$, and we know from (18) that $a_0 = \frac{1}{3^{2l}} \sum_{v^B v^C} \left(\left| \alpha_{00}^{v^B v^C} \right|^2 + \left| \alpha_{12}^{v^B v^C} \right|^2 + \left| \alpha_{21}^{v^B v^C} \right|^2 \right)$ $\geq \frac{1}{3} + \frac{\varepsilon}{2}$. Writing a_2 in terms of a_0, a_1, the above expression attains its minimum value w.r.t. a_1 when its derivative w.r.t. a_1 is 0. This happens at $a_1 = \frac{1-a_0}{2}$, and the corresponding value of the expression is $\frac{1}{4}(3a_0 - 1)^2$. Substituting $a_0 \geq \frac{1}{3} + \frac{\varepsilon}{2}$, we get that the probability is always at least $\frac{9\varepsilon^2}{16}$ for $x^B x^C$ in the good set. Thus the probability of learning $X^B X^C$ overall is at least $\frac{9\varepsilon^3}{32} = \Omega(\varepsilon^3)$. □

We make some observations from the proof of Lemma 27. First, the lower bound for learning a good $x^B x^C$ in the general case is $\left| \sum_{j=0}^{p-1} a_j \omega^j \right|^2$, where the a_j-s form a probability distribution, and $a_0 \geq \frac{1}{p} + \frac{\varepsilon}{2}$. Our proof works for $p = 2, 3$ because we can show the quantity is bounded away from zero under the two constraints on the a_j-s that we have. However, this does not seem to hold for $p > 3$, and hence our proof approach here does not work straightforwardly for such p. In particular, for any even-valued $p > 3$, note that one of the powers of ω is -1; hence, if we make the a_j-s corresponding to the -1 root have the same value as a_0, and give the rest of the a_j-s equal values, then $\sum_{j=0}^{p-1} a_j \omega^j = 0$. As for odd-valued $p > 3$, we note that for $p = 5$, viewing the terms $a_j\omega^j$ as vectors in the complex plane lets us see geometrically that (as long as ε is not too large) there is also a feasible choice of a_j values such that $\sum_{j=0}^{p-1} a_j \omega^j = 0$, and the construction should also generalize to all other odd-valued $p > 3$. Explicitly[31]: set $a_0 = \frac{1}{5} + \frac{\varepsilon}{2}$, and let $a_1 = a_4 = \frac{1-a_0-t}{4}$, $a_2 = a_3 = \frac{1-a_0+t}{4}$ for a parameter $t \in [0, 1 - a_0]$ whose exact value we shall choose later. Observe that since $a_1 = a_4$ and $a_2 = a_3$, these values always sum to a value with zero imaginary part, i.e. $\Im\left(\sum_{j=0}^{p-1} a_j \omega^j\right) = 0$. Furthermore, if $t = 0$ (i.e. $a_1 = a_2 = a_3 = a_4 = \frac{1-a_0}{4} < \frac{1}{5}$) then $\Re\left(\sum_{j=0}^{p-1} a_j \omega^j\right) > 0$, whereas if $t = 1 - a_0$ (i.e. $a_1 = a_4 = 0$ and $a_2 = a_3 = \frac{1-a_0}{2}$) then $\Re\left(\sum_{j=0}^{p-1} a_j \omega^j\right) < 0$ (as long as ε is not too large). Hence by continuity in t, there exists some $t \in [0, 1 - a_0]$ such that $\Re\left(\sum_{j=0}^{p-1} a_j \omega^j\right) = 0$ exactly, yielding the desired counterexample.[32] Still, we currently do not know whether this difficulty for the $p > 3$ case is simply a limitation of this proof approach, or whether Lemma 27 fundamentally does not hold in that case.

Additionally, we note that it is fine for the purposes of the proof if the initial upper bound on Bob and Charlie being able to guess X^B and X^C was obtained in the presence of some leakage between Bob and Charlie. The bound on the probability of Bob and Charlie guessing $X^B \cdot V^B$

[31] The geometric intuition here is that $\sum_{j=0}^{p-1} a_j \omega^j$ is the point in the complex plane given by head-to-tail summation of the vectors $a_j\omega^j$, which basically form a "non-closed pentagon" with side lengths a_j. The specified a_j values yield an endpoint of this vector sum that (due to the symmetry in the a_1, a_2, a_3, a_4 choices) always lies on the real axis, and moves from the positive half to the negative half as t ranges from 0 to $1 - a_0$.

[32] We remark that this argument basically relies on having (at least) one "free parameter" t to adjust the vector sum endpoint; therefore, it should generalize to larger odd-valued p as well, but an analogous construction is not available in the $p = 3$ case because if e.g. we were to try setting $a_0 = \frac{1}{3} + \frac{\varepsilon}{2}$ and $a_1 = a_2$, there are no "degrees of freedom" left after accounting for normalization.

and $X^C \cdot V^C$ holds in the presence of the same amount of leakage about X^B and X^C, as long as additional leakage about V^B and V^C does not happen. Note however that the above proof really does not work if V^B is fully leaked to Charlie and V^C is fully leaked to Bob. This is because, in the contradiction step of the proof, we would then have to assume that U_{IP}^B also takes a copy of V^C as input and U_{IP}^C takes a copy of R^B as input. But to run the Bernstein-Vazirani algorithm, Bob needs to have a uniform superposition of over V^B, which is uncorrelated with everything else, and Charlie needs to have a uniform superposition over V^C which is uncorrelated with everything else. Of course, for similar reasons, the proof does not work if we try to take inner product with the same V for both Bob and Charlie.

However, for a bounded amount of leakage about X^B, X^C or V^B, V^C, similar to Theorem 22, we can still come up with a new strategy for guessing $X^B \cdot V^B$ and $X^C \cdot V^C$ without leakage, given a strategy to guess them with leakage. This allows us to convert an upper bound on the "success probability" for the latter to an upper bound for the former. The analysis needs to be more fine-grained here however, since the kind of bound we are hoping to get with leakage is $\frac{1}{p} + \mathrm{negl}(l)$, instead of $\mathrm{negl}(l)$, and we need to make use of the fact that the final bound in Lemma 27 is an upper bound on the probability of Bob and Charlie both guessing right *or* both guessing wrong (that is, for $p = 2$, as described previously; the $p = 3$ case is similar but involves the $j + k = 0 \mod p$ condition more directly). We do this analysis in the following corollary.

Corollary 28. *In the same setting as Lemma 27, if the bound δ for Bob and Charlie guessing X^B and X^C holds without any leakage, then with vl bits of leakage, we have,*

$$\Pr\left[\bigvee_{\substack{j,k:\\ j+k=0 \mod p}} (G^B(V^B) = X^B \cdot V^B + j) \wedge (G^C(V^C) = X^C \cdot V^C + k)\right] \leq \frac{1}{p} + 2^{vl} \cdot O(\delta^{1/3}).$$

Proof. We shall only present the analysis for $p = 2$; the $p = 3$ analysis is very similar. As before, if vl bits were leaked in the original strategy $\mathcal{P}$, then to obtain a new strategy without leakage, Bob and Charlie will share vl bits of randomness, which they will use to simulate messages of $\mathcal{P}$ without communicating. At the end, if the randomness is consistent with all their measurement outcomes, they will output according to $\mathcal{P}$, otherwise they will output uniformly at random (using independent uniform bits). This means there are three different possibilities: Bob and Charlie both output a uniformly at random, one of them outputs uniformly at random and the other outputs according to $\mathcal{P}$, and both of them output according to $\mathcal{P}$.

We now compute the probability of Bob and Charlie both being right or being wrong in this new strategy without leakage. The probability that they both output according to $\mathcal{P}$ is of course 2^{-vl}, and conditioned on them doing so, the probability of them both being right or both being wrong is the same as in $\mathcal{P}$, which is, say, $\frac{1}{2} + \varepsilon$. Now suppose the probability that they both output uniformly at random is q_1, and the probability that one of them outputs uniformly at random and the other according to $\mathcal{P}$ is q_2, where $q_1 + q_2 = 1 - 2^{-vl}$. In the first case, the probability that they both output right or they both output wrong is $\frac{1}{2} \cdot \frac{1}{2} + \frac{1}{2} \cdot \frac{1}{2} = \frac{1}{2}$. In the latter case, let us first focus on the party who outputs according to $\mathcal{P}$: we don't know the actual value of the probability that their output is correct, but call this value β. With this (and using the fact that the other party simply produces an independent uniform output in this case), the probability of both the parties outputting right or both of them outputting wrong in this case is $\frac{1}{2} \cdot \beta + \frac{1}{2} \cdot (1 - \beta) = \frac{1}{2}$. Thus, their overall probability of both outputting right or both outputting wrong in this strategy

without leakage is

$$q_1 \cdot \frac{1}{2} + q_2 \cdot \frac{1}{2} + 2^{-\nu l} \cdot \left(\frac{1}{2} + \varepsilon\right) = \frac{1}{2} + 2^{-\nu l} \cdot \varepsilon.$$

Since we know from Lemma 27 that this probability is at most $\frac{1}{2} + O(\delta^{1/3})$, this gives us $\varepsilon \leq 2^{\nu l} \cdot O(\delta^{1/3})$. □

7.1 $(0, \mathrm{negl}(\lambda))$-anti-piracy security for bits and trits

With the above result, we can now prove fairly straightforwardly that the modified protocol achieves $(0, \mathrm{negl}(\lambda))$-anti-piracy security under Definition 8 (independent random challenge plaintexts), thus achieving Theorem 26 (the fact that it also satisfies completeness and indistinguishable security is easily seen from similar arguments as in Section 6.1).

Lemma 29. *Let the total number of leaked bits between the client and the receiver during* $\mathsf{Enc}(1^\lambda, M)$*, and between Bob and Charlie during the pirating attack, be* νl*. Then with the parameter choices as specified in* (8)-(9)*, Scheme 2 with the modifications described in this section is* $(0, \mathrm{negl}(\lambda))$*-anti-piracy-secure under Definition 8, as long as* ν *satisfies*

$$3\nu < \kappa \delta^3_{\gamma,\alpha} \alpha^4 - 2(1-\gamma)(1-\alpha) h_2(q). \tag{20}$$

Proof. The structure of this proof is basically the same as our analysis in Section 5.2 for DI-VKECM, except we invoke Corollary 28 to "amplify" the bounds on the guessing probabilities, and also we make some modifications to fit the pirating-attack scenario (analogous to the modifications described in the Lemma 25 proof).

Consider a pirating attack as described in Definition 8. Let the number of bits leaked during the key generation phase be $\nu_1 l$, and the number of bits leaked afterwards be $\nu_2 l$, with $\nu_1 + \nu_2 = \nu$. In order to properly apply Corollary 28 later, we suppose without loss of generality that all the $\nu_2 l$ bits leaked in the second part occur after Bob and Charlie get their ciphertexts (as remarked in the Theorem 22 proof, any leakage in the second part before they get their ciphertexts can be handled via the same form of argument as for the first $\nu_1 l$ bits, or alternatively by simply absorbing such leakage into the dishonest receiver's actions before distributing the state between Bob and Charlie). Let the ciphertext value that Bob receives during the encryption phase be denoted as $(P^{\mathrm{B}}, \mathtt{syn}(\widetilde{A}^{\mathrm{B}}), \widetilde{X}^{\mathrm{B}}, V^{\mathrm{B}})$ where $P^{\mathrm{B}} = M_1 \oplus R \oplus \widetilde{A}^{\mathrm{B}} \cdot V^{\mathrm{B}}$; analogously, let Charlie's values be denoted as $(P^{\mathrm{C}}, \mathtt{syn}(\widetilde{A}^{\mathrm{C}}), \widetilde{X}^{\mathrm{C}}, V^{\mathrm{C}})$ where $P^{\mathrm{C}} = M_2 \oplus R \oplus \widetilde{A}^{\mathrm{C}} \cdot V^{\mathrm{C}}$.

To begin, let us first prove a rough analogue of Lemma 20; specifically, consider a scenario that is defined the same way as a pirating attack on this protocol, except with the following modifications:

- Bob and Charlie's goal is instead to guess their respective "raw key" strings $\widetilde{A}^{\mathrm{B}}$ and $\widetilde{A}^{\mathrm{C}}$ (rather than their messages).
- During the encryption phase, we only give them the values $(\mathtt{syn}(\widetilde{A}^{\mathrm{B}}), \widetilde{X}^{\mathrm{B}})$ and $(\mathtt{syn}(\widetilde{A}^{\mathrm{C}}), \widetilde{X}^{\mathrm{C}})$ in their respective ciphertexts (i.e. $(P^{\mathrm{B}}, V^{\mathrm{B}})$ and $(P^{\mathrm{C}}, V^{\mathrm{C}})$ are omitted), and also require them to produce their guesses "immediately" after receiving these values, *without* performing the subsequent $\nu_2 l$ bits of leakage.

We aim to upper bound the probability that their guesses are correct in this scenario. To do so, we note that for the special case $\nu_1 = 0$ (i.e. no bits are leaked up until their guesses for $\widetilde{A}^{\mathrm{B}}, \widetilde{A}^{\mathrm{C}}$ are produced), by the same arguments as the Lemma 20 proof, the probability that $F = \checkmark$ and they both guess correctly is at most $2^{-\kappa\delta^3_{\gamma,\alpha}\alpha^4 l + 2\xi(1-\gamma)(1-\alpha)h_2(q)l}$, substituting in the formula (9) for the syndrome length $\ell_{\mathtt{syn}}$. (Here we have invoked the fact that in this scenario Bob and Charlie do not get $P^{\mathrm{B}}, V^{\mathrm{B}}$ and $P^{\mathrm{C}}, V^{\mathrm{C}}$, in which case the register R they received in the key generation phase is something they could have generated on their own using shared randomness, so the only "useful" classical information they receive to produce their guesses are $(\mathtt{syn}(\widetilde{A}^{\mathrm{B}}), \widetilde{X}^{\mathrm{B}})$ and $(\mathtt{syn}(\widetilde{A}^{\mathrm{C}}), \widetilde{X}^{\mathrm{C}})$.) Now, to handle the general case where $\nu_1 > 0$, we can again use the same arguments as in the Theorem 22 proof to conclude that this probability is instead upper bounded by $2^{-\kappa\delta^3_{\gamma,\alpha}\alpha^4 l + 2\xi(1-\gamma)(1-\alpha)h_2(q)l + \nu_1 l}$. This means we have that the probability they both guess correctly *conditioned* on $F = \checkmark$ satisfies

$$\begin{aligned}\Pr[(\widetilde{A}^{\mathrm{B}} = G^{\mathrm{B}}) \wedge (\widetilde{A}^{\mathrm{C}} = G^{\mathrm{C}}) | F = \checkmark] &= \frac{1}{\Pr[F = \checkmark]} \Pr[(F = \checkmark) \wedge (\widetilde{A}^{\mathrm{B}} = G^{\mathrm{B}}) \wedge (\widetilde{A}^{\mathrm{C}} = G^{\mathrm{C}})] \\ &\leq \frac{2^{-\kappa\delta^3_{\gamma,\alpha}\alpha^4 l + 2\xi(1-\gamma)(1-\alpha)h_2(q)l + \nu_1 l}}{\Pr[F = \checkmark]}. \end{aligned} \tag{21}$$

We now use the above bound to study another modified pirating attack scenario, where now the only modification from an actual pirating attack is that Bob and Charlie try to respectively produce guesses for $\widetilde{A}^{\mathrm{B}} \cdot V^{\mathrm{B}}$ and $\widetilde{A}^{\mathrm{C}} \cdot V^{\mathrm{C}}$ instead of their messages (i.e. here we allow them to have access to their full ciphertexts and leakage bits). First note that because the messages M_1, M_2 were initially chosen uniformly and independently of everything else (by Definition 8 for pirating attacks), and play no further role in this modified scenario after being used to produce P^{B} and P^{C}, we can invoke Fact 17 to say that P^{B} could have been locally generated by Bob, and analogously P^{C} by Charlie, which means we can omit them from consideration. (This is the same argument as in the Lemma 25 proof with respect to Definition 8.) With this, we are precisely in a scenario where Lemma 27 applies, identifying $X^{\mathrm{B}}, X^{\mathrm{C}}$ in the lemma statement with $\widetilde{A}^{\mathrm{B}}, \widetilde{A}^{\mathrm{C}}$ respectively in this scenario: the above bound (21) upper-bounds the probability that (for the state conditioned on $F = \checkmark$) Bob and Charlie can guess the "raw key" values $\widetilde{A}^{\mathrm{B}}, \widetilde{A}^{\mathrm{C}}$, and we are interested in bounding the probability that they can guess $\widetilde{A}^{\mathrm{B}} \cdot V^{\mathrm{B}}$ and $\widetilde{A}^{\mathrm{C}} \cdot V^{\mathrm{C}}$ after receiving $V^{\mathrm{B}}, V^{\mathrm{C}}$ and having $\nu_2 l$ bits of leakage. Explicitly, Lemma 27 tells us that this probability (for the conditional state) is at most

$$\frac{1}{p} + \frac{2^{\nu_2 \lambda}}{\Pr[F = \checkmark]^{\frac{1}{3}}} O\left(2^{-\frac{1}{3}(\kappa\delta^3_{\gamma,\alpha}\alpha^4 - 2\xi(1-\gamma)(1-\alpha)h_2(q) + \nu_1)\lambda}\right),$$

substituting $l = \lambda$.

Finally, we turn to the actual pirating attack scenario. We make the simple observation that while Bob's goal here is to guess his message M_1, the fact that he has the values R and $P^{\mathrm{B}} = M_1 \oplus R \oplus \widetilde{A}^{\mathrm{B}} \cdot V^{\mathrm{B}}$ means that this is equivalent to producing a guess for $\widetilde{A}^{\mathrm{B}} \cdot V^{\mathrm{B}}$; an analogous statement holds for Charlie. Hence the above bound also holds for the probability that they can both guess their messages (conditioned on $F = \checkmark$), which lets us write

$$\begin{aligned} &\Pr[(F = \checkmark) \wedge (M_1 = M^{\mathrm{B}}) \wedge (M_2 = M^{\mathrm{C}})] \\ &= \Pr[F = \checkmark] \Pr[(M_1 = M^{\mathrm{B}}) \wedge (M_2 = M^{\mathrm{C}}) | F = \checkmark] \\ &\leq \Pr[F = \checkmark] \left(\frac{1}{p} + \frac{2^{\nu_2 \lambda}}{\Pr[F = \checkmark]^{\frac{1}{3}}} O\left(2^{-\frac{1}{3}(\kappa\delta^3_{\gamma,\alpha}\alpha^4 - 2\xi(1-\gamma)(1-\alpha)h_2(q) + \nu_1)\lambda}\right)\right) \end{aligned}$$

$$\leq \frac{1}{p} + O\left(2^{-\frac{1}{3}(\kappa\delta_{\gamma,\alpha}^3\alpha^4 - 2\xi(1-\gamma)(1-\alpha)h_2(q)-3\nu)\lambda}\right).$$

Given the condition (16), the $O\left(2^{-\frac{1}{3}(\kappa\delta_{\gamma,\alpha}^3\alpha^4 - 2\xi(1-\gamma)(1-\alpha)h_2(q)-3\nu)\lambda}\right)$ term is a negligible function of λ, yielding the desired result. □

Remark 9. *Unlike the previous section, we were not able to prove here that this protocol satisfies $(0, \mathrm{negl}(\lambda))$-anti-piracy security in the sense of Definition 7, due to a subtle issue in handling the information available to Bob and Charlie. Specifically, under that definition, the values P^{B} and P^{C} in the above analysis would instead be $P^{\mathrm{B}} = M \oplus R \oplus \widetilde{A}^{\mathrm{B}} \cdot V^{\mathrm{B}}$ and $P^{\mathrm{C}} = M \oplus R \oplus \widetilde{A}^{\mathrm{B}} \cdot V^{\mathrm{C}}$ where the message M is the same in both terms. Due to this, we no longer have the property that $P^{\mathrm{B}}P^{\mathrm{C}}$ can be locally generated by Bob and Charlie without access to the client's registers, and the above argument no longer straightforwardly works.[33] A similar obstacle is encountered when trying to obtain a DI-VKECM protocol with $(0, \mathrm{negl}(\lambda))$-uncloneability via this approach.[34]*

Still, we note that it does seem possible that the protocol may in fact satisfy Definition 7; it is just that the above proof technique does not suffice to show this. If a proof of this were to be found, it seems likely that it would also yield an uncloneable encryption protocol with $(0, \mathrm{negl}(\lambda))$-uncloneability for single bits or trits. (A property that may be convenient in a prospective proof is the fact that e.g. for the bit-valued case (i.e. $\mathcal{M} = \mathbb{F}_2$), the values $P^{\mathrm{B}}P^{\mathrm{C}}$ can be equivalently viewed as a pair of bits uniformly distributed across the two values satisfying $P^{\mathrm{B}} \oplus P^{\mathrm{C}} = \widetilde{A}^{\mathrm{B}} \cdot V^{\mathrm{B}} \oplus \widetilde{A}^{\mathrm{B}} \cdot V^{\mathrm{C}}$. Put another way, in some sense they encode the XOR of the "secret" values $\widetilde{A}^{\mathrm{B}} \cdot V^{\mathrm{B}}$ and $\widetilde{A}^{\mathrm{B}} \cdot V^{\mathrm{C}}$, but in a "distributed" way across Bob and Charlie rather than being available to either of them locally. If it could be shown that supplying Bob and Charlie with these values does not increase their joint probability of guessing the message M, then it would be sufficient to obtain the desired result.)

8 Parallel repetition of the cloning game

In this section, we prove the following theorem.

Theorem 30. *Let G_α be a game as described in Section 4.3, satisfying properties (i)-(ii), and with $\omega^*(G_\alpha) = 1 - \varepsilon$. Let $\mathcal{A}, \mathcal{S}, \mathcal{B}, \mathcal{C}$ be the output sets of G_α. Then for $t = (1 - \varepsilon + \eta)l$, the parallel-repeated G_α satisfies*

$$\omega^*(G_\alpha^l) = \left(1 - \frac{\varepsilon}{2}\right)^{\Omega\left(\frac{\varepsilon^2\alpha^4 l}{\log(|\mathcal{A}|\cdot|\mathcal{S}|\cdot|\mathcal{B}|\cdot|\mathcal{C}|)}\right)}$$
$$\omega^*(G_\alpha^{t/l}) = \left(1 - \frac{\eta}{2}\right)^{\Omega\left(\frac{\eta^2\alpha^4 l}{\log(|\mathcal{A}|\cdot|\mathcal{S}|\cdot|\mathcal{B}|\cdot|\mathcal{C}|)}\right)}.$$

Theorem 13 is a simplified version of the second bound after applying the inequality $1 - \kappa \leq 2^{-\kappa}$.

We shall use the following results in our proof.

[33] Qualitatively, one way to understand this issue is that in our above proof, we have basically treated the messages M_1 and M_2 as independent one-time-pads on the quantities $R \oplus \widetilde{A}^{\mathrm{B}} \cdot V^{\mathrm{B}}$ and $R \oplus \widetilde{A}^{\mathrm{B}} \cdot V^{\mathrm{C}}$, but attempting an analogous argument under Definition 7 with M as the "one-time-pad" runs into the issue that it is reused across the two terms, which disrupts the usual security properties of one-time-padding.

[34] In the context of the previous protocols without the "extraction" step, our security proofs overcame this issue via the bound (13), in which we essentially exploited the fact that the dishonest parties' goal in the security definition is a somewhat "stricter" win condition than the parallel-repeated game we actually bound the winning probability of. This approach does not seem to straightforwardly work after the extraction step has taken place.

Fact 31 ([Hol07]). *Let* $\mathsf{P}_{QM_1\ldots M_lN} = \mathsf{P}_Q\mathsf{P}_{M_1|Q}\mathsf{P}_{M_2|Q}\ldots\mathsf{P}_{M_l|Q}\mathsf{P}_{N|QM_1\ldots M_l}$ *be a probability distribution over* $\mathcal{Q}\times\mathcal{M}^l\times\mathcal{N}$*, and let* $\mathcal{E}$ *be any event. Then,*

$$\sum_{i=1}^{l}\|\mathsf{P}_{QM_iN|\mathcal{E}}-\mathsf{P}_{QN|\mathcal{E}}\mathsf{P}_{M_i|Q}\|_1\leq\sqrt{l\left(\log(|\mathcal{N}|)+\log\left(\frac{1}{\Pr[\mathcal{E}]}\right)\right)}.$$

Fact 32 ([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 33 (Quantum Raz's Lemma, [BVY17]). *Let* ρ_{XY} *and* σ_{XY} *be two CQ states with* $X=X_1\ldots X_l$ *being classical, and* σ *being product across all registers. Then,*

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

Fact 34 ([KT23], Lemma 32). *Suppose* P_{ST} *and* $\mathsf{P}_{S'T'R'}$ *are distributions such that for some* t^**, we have* $\mathsf{P}_{ST}(s,t^*)=\beta\cdot\mathsf{P}_S(s)$ *for all* s*. If* $\|\mathsf{P}_{ST}-\mathsf{P}_{S'T'}\|_1\leq\beta$*, then,*

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

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

8.1 Setup

Consider a protocol $\mathcal{P}$ for l copies of G_α. Alice and Barlie have inputs $X=X_1\ldots X_l$ and $U=U_1\ldots U_l$ in the first round. Before the game starts, they share some entangled state; we shall assume that after they receive their outputs, they do some unitaries and then measure in the computational basis to produce their outputs $A=A_1\ldots A_l$ and $S=S_1\ldots S_l$. Suppose the state held by Alice and Barlie after they produce the outputs is $|\sigma\rangle$ on registers $A\widetilde{A}S\widetilde{S}E^{\mathrm{A}}E^{\mathrm{BC}}$, with Alice holding $A\widetilde{A}E^{\mathrm{A}}$ and Barlie holding the rest.[35] Here $A=A_1\ldots A_l$ and $S=S_1\ldots S_l$ will be the registers in which Alice and Barlie's outputs are measured in the computational basis; $\widetilde{A},\widetilde{S}$ are registers onto which the contents of A,S are copied — we can always assume the outputs are copied since they are classical. We define the following pure state to represent the inputs, outputs and other registers in the protocol at this stage:

$$|\rho\rangle_{X\widetilde{X}U\widetilde{U}Y\widetilde{Y}Z\widetilde{Z}A\widetilde{A}S\widetilde{S}E^{\mathrm{A}}E^{\mathrm{BC}}}=\sum_{x,u,y,z}\sqrt{\mathsf{P}_{XUYZ}(x,u,y,z)}\,|xx\rangle_{X\widetilde{X}}\,|uu\rangle_{U\widetilde{U}}\,|yy\rangle_{Y\widetilde{Y}}\,|zz\rangle_{Z\widetilde{Z}}\otimes\sum_{a,s}\sqrt{\mathsf{P}_{AS|xu}(as)}\,|aa\rangle_{A\widetilde{A}}\,|ss\rangle_{S\widetilde{S}}\,|\rho\rangle_{E^{\mathrm{A}}E^{\mathrm{BC}}|xuas}.$$

[35] Barlie can do an additional unitary on his registers before passing them on to Bob and Charlie — here we are absorbing that unitary, which does not change the distribution of AS, into $|\sigma\rangle$.

Here we have included the $Y\widetilde{Y}Z\widetilde{Z}$ registers in this state even though they have not been revealed yet or used in the protocol; the state in the entangled registers has no dependence on z because of this. Here $\mathsf{P}_{AS|xu}(a,s)$ is the probability of Alice and Barlie obtaining outputs (a,s) on inputs (x,u) in the first round. In the actual protocol, the registers A and S would be measured at this stage, and the outputs can be used as classical inputs for the next round, but for the sake of this analysis we shall keep everything coherent.

In the second round, the registers $S\widetilde{S}E^{\mathrm{BC}}$ are distributed in some way between Bob and Charlie. They will then receive inputs Y, Z respectively, and additionally have access to U. Now Bob and Charlie again do some unitaries and produce their outputs by measuring in the computational basis. Suppose their shared state when they produce their outputs is $|\sigma\rangle$ on registers $BCE^{\mathrm{B}}E^{\mathrm{C}}$, with Bob holding BE^{B} and Charlie holding the rest. For convenience, we shall also divide up the classical information that they both have copies of in the following way: Bob gets US, and Charlie gets $\widetilde{U}\widetilde{S}$. We denote the state of the protocol at this stage by

$$\begin{aligned}|\sigma\rangle_{X\widetilde{X}U\widetilde{U}Y\widetilde{Y}Z\widetilde{Z}A\widetilde{A}S\widetilde{S}BCE^{\mathrm{A}}E^{\mathrm{B}}E^{\mathrm{C}}} = \sum_{x,u,y,z} \sqrt{\mathsf{P}_{XUYZ}(x,u,y,z)}\,|xx\rangle_{X\widetilde{X}}\,|uu\rangle_{U\widetilde{U}}\,|yy\rangle_{Y\widetilde{Y}}\,|zz\rangle_{Z\widetilde{Z}} \otimes \\ \sum_{a,s} \sqrt{\mathsf{P}_{AS|xu}(as)}\,|aa\rangle_{A\widetilde{A}}\,|ss\rangle_{S\widetilde{S}} \sum_{bc} \sqrt{\mathsf{P}_{BC|xuyzas}(bc)}\,|b\rangle_B\,|c\rangle_C \otimes \\ |\sigma\rangle_{E^{\mathrm{A}}E^{\mathrm{B}}E^{\mathrm{C}}|xuyzasbc}\,.\end{aligned}$$

Note that to get $|\rho\rangle$ to $|\sigma\rangle$, the $A\widetilde{A}$ registers are not touched at all, and $S\widetilde{S}$ are used only as a control registers for Bob and Charlie's unitaries, which is why the marginal distribution of AS is the same in $|\rho\rangle$ and $|\sigma\rangle$.

We shall use the following lemma, whose proof is given later, to prove Theorem 30.

Lemma 35. *Let $\omega^*(G) = 1-\varepsilon$. For $i \in [l]$, let $J_i = \mathsf{V}_1(X_iU_i, A_iS_i)\cdot\mathsf{V}_2(X_iU_iY_iZ_i, A_iS_iB_iC_i)$ in a protocol $\mathcal{P}$ for l copies of G (here V_1 and V_2 are the first and second round predicates respectively). If $\mathcal{E}_T$ is the event $\prod_{i\in T} J_i = 1$ and $\overline{T}$ denotes $[l]\setminus T$ for $T \subseteq [l]$, then*

$$\mathop{\mathbb{E}}_{i\in\overline{T}} \Pr[J_i = 1|\mathcal{E}_T] \leq 1-\varepsilon+O\left(\frac{\sqrt{\delta_T}}{\alpha^2}\right),$$

where

$$\delta_T = \frac{|T|\cdot\log(|\mathcal{A}|\cdot|\mathcal{S}|\cdot|\mathcal{B}|\cdot|\mathcal{C}|)+\log(1/\Pr[\mathcal{E}_T])}{l}.$$

It is possible to give an explicit constant in place of the big O in the above lemma statement, by tracking all the constants in the proof. We shall not be doing so here, but it can be seen from our proof that the constant we get is certainly bigger than 4. Therefore, it is sufficient to prove the lemma when $\delta_T \leq \alpha^4/8$, as the lemma statement is trivial otherwise.

To prove the bound on $\omega^*(G^l)$ in Theorem 30, we shall use the above lemma to choose a random subset T of $[l]$, such that the probability of winning in the random subset is

$$\left(1-\frac{\varepsilon}{2}\right)^{\left(\frac{\Omega(\varepsilon^2\alpha^4)}{\log(|\mathcal{A}|\cdot|\mathcal{S}|\cdot|\mathcal{B}|\cdot|\mathcal{C}|)}\right)l},$$

which immediately implies that the same bound holds for $\omega^*(G_\alpha^l)$. We start with $T=\emptyset$, and construct T by choosing a uniformly random element outside the current T, until the final set

satisfies $\delta_T \geq \varepsilon^2\alpha^4/4K^2$, where K is the constant in the big O of Lemma 35. Every instance added by this procedure, except the very last one, satisfies the bound in Lemma 35 with $K \cdot \frac{\sqrt{\delta_T}}{\alpha^2} \leq \frac{\varepsilon}{2}$. If the final picked set has $\log(1/\Pr[\mathcal{E}_T]) \geq \left(\frac{\varepsilon^2\alpha^4}{4K^2}\right) \cdot \frac{l}{2\log(|\mathcal{A}|\cdot|\mathcal{S}|\cdot|\mathcal{B}|\cdot|\mathcal{C}|)}$, then we are already done. Otherwise we have,

$$|T| \geq \left(\frac{\varepsilon^2\alpha^4}{4K^2} - \log(1/\Pr[\mathcal{E}_T])\right) \cdot \frac{l}{\log(|\mathcal{A}|\cdot|\mathcal{S}|\cdot|\mathcal{B}|\cdot|\mathcal{C}|)},$$

which makes $\Pr[\mathcal{E}_T] \leq \left(1-\frac{\varepsilon}{2}\right)^{|T|-1} \leq \left(1-\frac{\varepsilon}{2}\right)^{\left(\frac{\varepsilon^2\alpha^4}{8K^2}\right)\cdot\frac{l}{\log(|\mathcal{A}|\cdot|\mathcal{S}|\cdot|\mathcal{B}|\cdot|\mathcal{C}|)}}$, which is the required bound.

Next, to prove the bound on $\omega^*(G^{t/l})$, where $t = (1-\varepsilon+\eta)l$, for some γ to be determined later, suppose T is such that $\Pr[\mathcal{E}_T] \geq 2^{-\gamma^2 l - |T|\cdot\log(|\mathcal{A}|\cdot|\mathcal{S}|\cdot|\mathcal{B}|\cdot|\mathcal{C}|)}$. Then we have, $\delta_T \leq \gamma^2$. Let

$$n = \frac{\gamma^2 l}{\log\left(\frac{\log(|\mathcal{A}|\cdot|\mathcal{S}|\cdot|\mathcal{B}|\cdot|\mathcal{C}|)}{1-\varepsilon+\frac{K\gamma}{\alpha^2}}\right)},$$

which satisfies $2^{-\gamma^2 l - n\cdot\log(|\mathcal{A}|\cdot|\mathcal{S}|\cdot|\mathcal{B}|\cdot|\mathcal{C}|)} = \left(1-\varepsilon+\frac{K\gamma}{\alpha^2}\right)^n$. For a random set of size n, we can then say by the previous inductive argument that its winning probability is upper bounded by $\left(1-\varepsilon+\frac{K\gamma}{\alpha^2}\right)^n$, i.e.,

$$\sum_{T\subseteq[l]:|T|=n} \frac{1}{\binom{l}{n}} \Pr[\mathcal{E}_T] \leq \left(1-\varepsilon+\frac{K\gamma}{\alpha^2}\right)^n. \tag{22}$$

Now set $\gamma = \frac{\alpha^2\eta}{4K}$, which makes $n < (1-\varepsilon+\eta)l$. If $(1-\varepsilon+\eta)l$ games are won, we can pick a random subset of n instances out of the $(1-\varepsilon+\eta)l$ instances on which the game is won, and say that the probability of winning the $(1-\varepsilon+\eta)l$ instances is upper bounded by the probability of winning these n instances. Using (22) we therefore have,

$$\omega^*(G^{t/l}) \leq \sum_{T\subseteq[(1-\varepsilon+\eta)l]:|T|=n} \frac{1}{\binom{(1-\varepsilon+\eta)l}{n}} \Pr[\mathcal{E}_T] \leq \left(1-\varepsilon+\frac{\eta}{4}\right)^n \cdot \frac{\binom{l}{n}}{\binom{(1-\varepsilon+\eta)l}{n}}. \tag{23}$$

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 definition of n. Putting this into (23) we get,

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

which proves the theorem after substituting the value of n.

8.2 Proof of Lemma 35

From this section onwards, for the sake of brevity, we shall drop the subscript T from δ_T and $\mathcal{E}_T$ as defined in Lemma 35, and refer to these quantities as simply δ and $\mathcal{E}$.

For each $i \in [l]$, we define the random variable $D_i F_i$ as described in Section 4.3: for each i D_i is a uniformly random bit; $F_i = X_i U_i$ if $D_i = 0$ and $F_i = Y_i Z_i$ if $D_i = 1$. We can consider the states $|\rho\rangle$ and $|\sigma\rangle$ conditioned on particular values of $DF = d_1 \dots d_l f_1 \dots f_l = df$, and this simply means that the distributions of $XUYZ$ are conditioned on $DF = df$.

Conditioned on $DF = df$, we define the state $|\varphi\rangle_{df}$, which is $|\sigma\rangle_{df}$ conditioned on success in T:

$$|\varphi\rangle_{X\tilde{X}U\tilde{U}Y\tilde{Y}Z\tilde{Z}A\tilde{A}S\tilde{S}BCE^{\mathrm{A}}E^{\mathrm{B}}E^{\mathrm{C}}|df} = \frac{1}{\sqrt{\gamma_{df}}} \sum_{x,u,y,z} \sqrt{\mathsf{P}_{XUYZ|df}(x,u,y,z)}\, |xx\rangle_{X\tilde{X}} |uu\rangle_{U\tilde{U}} |yy\rangle_{Y\tilde{Y}} |zz\rangle_{Z\tilde{Z}} \otimes \sum_{\substack{a,s,b,c: \\ (x_T,u_T,y_T,z_T,a_T,s_T,b_T,c_T) \\ \text{win } G^{|T|}}} \sqrt{\mathsf{P}_{ASBC|xuyz}(asbc)}\, |aa\rangle_{A\tilde{A}} |ss\rangle_{S\tilde{S}} |b\rangle_B |c\rangle_C \otimes |\sigma\rangle_{E^{\mathrm{A}}E^{\mathrm{B}}E^{\mathrm{C}}|xuyzasbc}$$

where γ_{df} is the probability of winning in T conditioned on $DF = df$, in $\mathcal{P}$. It is easy to see that $\mathsf{P}_{XUYZASBC|\mathcal{E},df}$ is the distribution on the registers $XUYZASBC$ in $|\varphi\rangle_{df}$. For $i \in [l]$, we shall use $|\varphi\rangle_{x_i u_i y_i z_i d_{-i} f_{-i}}$ (where d_{-i} stands for $d_1 \dots d_{i-1} d_{i+1} \dots d_l$ and similar notation is used for f), $|\varphi\rangle_{u_i y_i z_i d_{-i} f_{-i}}$, $|\varphi\rangle_{x_i y_i z_i d_{-i} f_{-i}}$, $|\varphi\rangle_{y_i z_i d_{-i} f_{-i}}$ to refer to $|\varphi\rangle$ with values of $X_i U_i Y_i Z_i D_{-i} F_{-i}$, $U_i Y_i Z_i D_{-i} F_{-i}$, $X_i Y_i Z_i D_{-i} F_{-i}$ and $Y_i Z_i D_{-i} F_{-i}$ respectively conditioned on, and similar notation for other variables and subsets of $[l]$ as well. $|\varphi\rangle_{\perp,\perp,d_{-i}f_{-i}}$ will be used to refer to a state where at an index implied from context (in this case i), $Y_i Z_i$ are both conditioned on the value $\perp$; when only one of Y_i or Z_i are conditioned on, we shall write the state explicitly as $|\varphi\rangle_{Y_i=\perp,d_{-i}f_{-i}}$ or $|\varphi\rangle_{Z_i=\perp,d_{-i}f_{-i}}$.

We shall use the following lemma, whose proof we give later, to prove Lemma 35.

Lemma 36. *If $\delta \leq \alpha^4/8$ for δ as defined in Lemma 35 (called δ_T in the lemma statement), then using $R_i = X_T U_T Y_T Z_T A_T S_T B_T C_T D_{-i} F_{-i}$, the following conditions hold:*

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

(ii) For each $i \in \overline{T}$, there exist unitaries $\{V^{\mathrm{A}}_{i,x_i r_i}\}_{x_i r_i}$ acting on $X_{\overline{T}} \widetilde{X}_{\overline{T}} E^{\mathrm{A}} A_{\overline{T}} \widetilde{A}_{\overline{T}}$, and $\{V^{\mathrm{BC}}_{i,y_i r_i}\}_{y_i r_i}$ acting on $U_{\overline{T}} \widetilde{U}_{\overline{T}} Y_{\overline{T}} \widetilde{Y}_{\overline{T}} Z_{\overline{T}} \widetilde{Z}_{\overline{T}} S_{\overline{T}} \widetilde{S}_{\overline{T}} B_{\overline{T}} C_{\overline{T}} E^{\mathrm{B}} E^{\mathrm{C}}$ such that

$$\mathop{\mathbb{E}}_{i\in\overline{T}} \mathop{\mathbb{E}}_{\mathsf{P}_{X_i U_i R_i|\mathcal{E}}} \left\| V^{\mathrm{A}}_{i,x_i r_i} \otimes V^{\mathrm{BC}}_{i,u_i r_i} |\varphi\rangle\langle\varphi|_{\perp\perp r_i} (V^{\mathrm{A}}_{i,x_i r_i})^\dagger \otimes (V^{\mathrm{BC}}_{i,u_i r_i})^\dagger - |\varphi\rangle\langle\varphi|_{x_i u_i \perp\perp r_i} \right\|_1 \leq O\left(\frac{\sqrt{\delta}}{\alpha^2}\right);$$

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

(iv) For each $i \in \overline{T}$, there exist unitaries $\{V^{\mathrm{B}}_{i,u_i y_i r_i}\}_{u_i y_i r_i}$ acting on the registers $Y_{\overline{T}} \widetilde{Y}_{\overline{T}} U_{\overline{T}} S_{\overline{T}} E^{\mathrm{B}} B_{\overline{T}}$ and $\{V^{\mathrm{C}}_{i,u_i z_i r_i}\}_{u_i z_i r_i}$ acting on $Z_{\overline{T}} \widetilde{Z}_{\overline{T}} \widetilde{U}_{\overline{T}} \widetilde{S}_{\overline{T}} E^{\mathrm{C}} C_{\overline{T}}$ such that

$$\mathop{\mathbb{E}}_{i\in\overline{T}} \mathop{\mathbb{E}}_{\mathsf{P}_{X_i U_i Y_i Z_i A_i S_i R_i|\mathcal{E}}} \left\| V^{\mathrm{B}}_{i,u_i y_i r_i} \otimes V^{\mathrm{C}}_{i,u_i z_i r_i} |\varphi\rangle\langle\varphi|_{x_i u_i \perp\perp a_i s_i r_i} (V^{\mathrm{B}}_{i,u_i y_i r_i})^\dagger \otimes (V^{\mathrm{C}}_{i,u_i z_i r_i})^\dagger - |\varphi\rangle\langle\varphi|_{x_i u y_i z_i a_i s_i r_i} \right\|_1 \leq O\left(\frac{\sqrt{\delta}}{\alpha^2}\right).$$

As noted before, the statement of Lemma 35 is trivial if $\delta \geq \alpha^4/8$, so we shall use Lemma 36 to prove Lemma 35 in the case that $\delta \leq \alpha^4/8$. Making use of the conditions in Lemma 36, we give a strategy for a single copy of G_α as follows:

- Alice and Barlie share $\log|\overline{T}|$ uniform bits, for each $i \in \overline{T}$, $\mathsf{P}_{R_i|\mathcal{E},\perp\perp}$ as randomness, and for each $R_i = r_i$, the state $|\varphi\rangle_{\perp\perp r_i}$ as entanglement, with Alice holding registers $X_{\overline{T}}\widetilde{X}_{\overline{T}}A_{\overline{T}}\widetilde{A}_{\overline{T}}E^{\mathrm{A}}$ and Barlie holding registers $U_{\overline{T}}\widetilde{U}_{\overline{T}}Y_{\overline{T}}\widetilde{Y}_{\overline{T}}Z_{\overline{T}}\widetilde{Z}_{\overline{T}}S_{\overline{T}}\widetilde{S}_{\overline{T}}B_{\overline{T}}C_{\overline{T}}E^{\mathrm{B}}E^{\mathrm{C}}$ (the rest of the registers have fixed values due to r_i).
- Alice and Barlie use their shared randomness to sample $i \in \overline{T}$ uniformly, and in the first round, apply $V^{\mathrm{A}}_{i,x_ir_i}$, $V^{\mathrm{BC}}_{i,u_ir_i}$ on their parts of the shared entangled state according to their shared randomness from $\mathsf{P}_{R_i|\mathcal{E},\perp\perp}$ and their first round inputs.
- Alice and Bob measure the A_i, S_i registers of the resulting state to give their first round outputs.
- Before the second round starts, Barlie passes the registers $Y_{\overline{T}}\widetilde{Y}_{\overline{T}}U_{\overline{T}}S_{\overline{T}}BE^{\mathrm{B}}$ to Bob, and $Z_{\overline{T}}\widetilde{Z}_{\overline{T}}\widetilde{U}_{\overline{T}}\widetilde{S}_{\overline{T}}CE^{\mathrm{C}}$ to Charlie. He also gives each of them his first round input u_i, and the i, r_i he sampled in the first round.
- After receiving the second round inputs, Bob and Charlie apply $V^{\mathrm{B}}_{i,u_iy_ir_i}$ and $V^{\mathrm{C}}_{i,u_iz_ir_i}$ respectively to their registers according to their inputs and u_ir_i received from Barlie.
- Bob and Charlie measure the B_i, C_i registers of the resulting state to give their second round outputs.

We shall first analyse the success probability of this strategy assuming the inputs and shared randomness are distributed according to $\mathsf{P}_{X_iY_iZ_iR_i|\mathcal{E}}$ for i. Let $\mathsf{P}_{\widehat{A}_i\widehat{S}_i|X_iU_iY_iZ_iR_i}$ denote the conditional distribution Alice and Barlie get after the first round (note that $\widehat{A}_i\widehat{S}_i$ are actually independent of Y_iZ_i given X_iU_i, but we are still writing Y_iZ_i in the conditioning), and $\mathsf{P}_{\widehat{B}_i\widehat{C}_i|X_iU_iY_iZ_iR_i\widehat{A}_i\widehat{S}_i}$ denote their conditional distribution after the second round. Since $\mathsf{P}_{\widehat{A}_i\widehat{S}_i|X_iY_iZ_iR_i}$ is obtained by measuring the A_iS_i registers of the state $V^{\mathrm{A}}_{i,x_ir_i} \otimes V^{\mathrm{BC}}_{i,u_ir_i}|\varphi\rangle_{\perp\perp r_i}$, and $\mathsf{P}_{A_iS_i|\mathcal{E},X_iU_i,\perp\perp,R_i}$ is obtained by measuring the same registers of $|\varphi\rangle_{x_iu_i\perp\perp r_i}$, from item (ii) of Lemma 36 and Fact 6 we have,

$$\mathop{\mathbb{E}}_{i\in\overline{T}} \left\| \mathsf{P}_{X_iU_iY_iZ_iR_i|\mathcal{E}} \left(\mathsf{P}_{\widehat{A}_i\widehat{S}_i|X_iU_iY_iZ_iR_i} - \mathsf{P}_{A_iS_i|\mathcal{E},X_iU_i,\perp\perp,R_i} \right) \right\|_1 \leq O\left(\frac{\sqrt{\delta}}{\alpha^2}\right).$$

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

$$\mathop{\mathbb{E}}_{i\in\overline{T}} \left\| \mathsf{P}_{X_iU_iY_iZ_iR_i|\mathcal{E}} \left(\mathsf{P}_{\widehat{A}_i\widehat{S}_i|X_iU_iY_iZ_iR_i} - \mathsf{P}_{A_iS_i|\mathcal{E},X_iU_iY_iZ_iR_i} \right) \right\|_1 \leq O\left(\frac{\sqrt{\delta}}{\alpha^2}\right).$$

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

$$\mathop{\mathbb{E}}_{i\in\overline{T}} \left\| \mathsf{P}_{X_iU_iY_iZ_iR_iA_iS_i} \left(\mathsf{P}_{\widehat{B}_i\widehat{C}_i|X_iU_iY_iZ_iR_i\widehat{A}_i\widehat{S}_i} - \mathsf{P}_{B_iC_i|\mathcal{E},X_iY_iZ_iR_iA_iS_i} \right) \right\|_1 \leq O\left(\frac{\sqrt{\delta}}{\alpha^2}\right).$$

Now, since our actual distribution of inputs and randomness if $\mathsf{P}_{X_iU_iY_iZ_i}\mathsf{P}_{R_i|\mathcal{E},\perp\perp}$, our actual input, randomness and output distribution is $\mathsf{P}_{X_iU_iY_iZ_i}\mathsf{P}_{R_i|\mathcal{E},\perp\perp}\mathsf{P}_{\widehat{A}_i\widehat{S}_i\widehat{B}_i\widehat{C}_i|X_iY_iZ_iR_i}$. Combing the above equations with item (i), we get that this distribution satisfies,

$$\mathop{\mathbb{E}}_{i\in\overline{T}}\left\|\mathsf{P}_{X_iU_iY_iZ_i}\mathsf{P}_{R_i|\mathcal{E},\perp\perp}\mathsf{P}_{\widehat{A}_i\widehat{S}_i\widehat{B}_i\widehat{C}_i|X_iU_iY_iZ_iR_i}-\mathsf{P}_{X_iU_iY_iZ_iR_iA_iS_iB_iC_i|\mathcal{E}}\right\|_1\leq O\left(\frac{\sqrt{\delta}}{\alpha^2}\right).$$

Suppose the constant in the above big O is K. Since $\Pr[J_i=1|\mathcal{E}]$ is the probability that the distribution $\mathsf{P}_{X_iU_iY_iZ_iR_iA_iS_iB_iC_i|\mathcal{E}}$ wins a single copy of the game G_α, if $\mathbb{E}_{i\in\overline{T}}\Pr[J_i=1|\mathcal{E}]>1-\varepsilon+\frac{K}{2}\cdot\frac{\sqrt{\delta}}{\alpha^2}$, then the winning probability of our constructed strategy is more than

$$1-\varepsilon+\frac{K}{2}\cdot\frac{\sqrt{\delta}}{\alpha^2}-\frac{1}{2}\mathop{\mathbb{E}}_{i\in\overline{T}}\left\|\mathsf{P}_{X_iU_iY_iZ_i}\mathsf{P}_{R_i|\mathcal{E},\perp\perp}\mathsf{P}_{\widehat{A}_i\widehat{S}_i\widehat{B}_i\widehat{C}_i|X_iU_iY_iZ_iR_i}-\mathsf{P}_{X_iU_iY_iZ_iR_iA_iS_iB_iC_i|\mathcal{E}}\right\|_1\geq\omega^*(G),$$

which is a contradiction. Therefore we must have $\mathbb{E}_{i\in\overline{T}}\Pr[J_i=1|\mathcal{E}]\leq 1-\varepsilon+O\left(\frac{\sqrt{\delta}}{\alpha^2}\right)$.

8.3 Proof of Lemma 36

Closeness of distributions. Applying Fact 31 with Q, N being trivial and $M_i = X_iU_iY_iZ_i$ we get,

$$\mathop{\mathbb{E}}_{i\in\overline{T}}\|\mathsf{P}_{X_iU_iY_iZ_i|\mathcal{E}}-\mathsf{P}_{X_iU_iY_iZ_i}\|_1\leq\frac{1}{l-|T|}\sqrt{(l-|T|)\cdot\log(1/\Pr[\mathcal{E}])}\leq\sqrt{2\delta},\tag{24}$$

recalling we are taking δ to be the value δ_T defined in Lemma 35. In particular, the last line of the above equation is obtained by recalling that we have required $\delta\leq\alpha^4/8$, which implies $|T|\leq l/2$.

Also, applying Fact 31 again with M_i the same, $Q = X_TU_TY_TZ_TDF$ and $N = A_TS_TB_TC_T$, we get

$$\begin{aligned}
\sqrt{2\delta}&\geq\frac{1}{l-|T|}\sqrt{(l-|T|)(\log(1/\Pr[\mathcal{E}])+|T|\cdot\log(|\mathcal{A}|\cdot|\mathcal{S}|\cdot|\mathcal{B}|\cdot|\mathcal{C}|)}\\
&\geq\mathop{\mathbb{E}}_{i\in\overline{T}}\left\|\mathsf{P}_{X_iU_iY_iZ_iX_TU_TY_TZ_TDFA_TS_TB_TC_T|\mathcal{E}}-\mathsf{P}_{X_TU_TY_TZ_TA_TS_TB_TC_TDF|\mathcal{E}}\mathsf{P}_{X_iU_iY_iZ_i|X_TU_TY_TZ_TDF}\right\|_1\\
&=\mathop{\mathbb{E}}_{i\in\overline{T}}\|\mathsf{P}_{X_iU_iY_iZ_iD_iF_iR_i|\mathcal{E}}-\mathsf{P}_{D_iF_iR_i|\mathcal{E}}\mathsf{P}_{X_iU_iY_iZ_i|D_iF_i}\|_1\\
&=\frac{1}{2}\mathop{\mathbb{E}}_{i\in\overline{T}}\left(\|\mathsf{P}_{X_iU_iY_iZ_iR_i|\mathcal{E}}-\mathsf{P}_{X_iU_iR_i|\mathcal{E}}\mathsf{P}_{Y_iZ_i|X_iU_i}\|_1+\|\mathsf{P}_{X_iU_iY_iZ_iR_i|\mathcal{E}}-\mathsf{P}_{Y_iZ_iR_i|\mathcal{E}}\mathsf{P}_{X_iU_i|Y_iZ_i}\|_1\right),
\end{aligned}\tag{25}$$

where in the third line we have used the definition of $R_i = X_TU_TY_TZ_TA_TS_TB_TC_TD_{-i}G_{-i}$, and the last line is obtained by conditioning on values $D_i = 0$ and $D_i = 1$ (which happen with probability $\frac{1}{2}$ even after conditioning on $\mathcal{E}$).

Note that for all x_i, u_i, we have $\mathsf{P}_{X_iU_iY_iZ_i}(x_i,u_i,\perp,\perp)=\alpha^2\cdot\mathsf{P}_{X_iU_i}(x_iu_i)$. This and the bound (24) allows us to apply item (ii) of Fact 34, with $X_iU_i = S$, $Y_iZ_i = T$, $R_i = R$, and the corresponding variables conditioned on $\mathcal{E}$ being the primed variables in the lemma statement. This gives

$$\begin{aligned}
\mathop{\mathbb{E}}_{i\in\overline{T}}\left\|\mathsf{P}_{X_iU_iY_iZ_iR_i|\mathcal{E}}-\mathsf{P}_{X_iU_iY_iZ_i}\mathsf{P}_{R_i|\mathcal{E},\perp\perp}\right\|_1\leq\frac{2}{\alpha^2}\mathop{\mathbb{E}}_{i\in\overline{T}}&\left(\|\mathsf{P}_{X_iU_iY_iZ_iR_i|\mathcal{E}}-\mathsf{P}_{X_iU_iR_i|\mathcal{E}}\mathsf{P}_{Y_iZ_i|X_iU_i}\|_1\right.\\
&\left.+\|\mathsf{P}_{X_iU_iY_iZ_iR_i|\mathcal{E}}-\mathsf{P}_{Y_iZ_iR_i|\mathcal{E}}\mathsf{P}_{X_iU_i|Y_iZ_i}\|_1\right)
\end{aligned}$$

$$+\frac{7}{\alpha^2}\mathop{\mathbb{E}}_{i\in\overline{T}}\|\mathsf{P}_{X_iU_iY_iZ_i|\mathcal{E}}-\mathsf{P}_{X_iU_iY_iZ_i}\|_1.$$

Applying (24) and (25) to the terms on the right-hand side yields item (i) of the lemma.

To show item (iii) of the lemma, we shall apply Fact 32 to the states $\varphi_{YZX\widetilde{X}U\widetilde{U}A_{\overline{T}}\widetilde{A}_{\overline{T}}S_{\overline{T}}\widetilde{S}_{\overline{T}}|a_Ts_Tb_Tc_Tdf}$ and $\sigma_{YZX\widetilde{X}U\widetilde{U}A_{\overline{T}}\widetilde{A}_{\overline{T}}S_{\overline{T}}\widetilde{S}_{\overline{T}}|df}$ (with z being $a_Ts_Tb_Tc_T$) to get,

$$\begin{aligned}
&\mathop{\mathbb{E}}_{\mathsf{P}_{Y_TZ_TX_TU_TA_TS_TC_TC_TDF|\mathcal{E}}}\mathsf{D}\Big(\varphi_{Y_{\overline{T}}Z_{\overline{T}}X_{\overline{T}}\widetilde{X}_{\overline{T}}U_{\overline{T}}\widetilde{U}_{\overline{T}}A_{\overline{T}}\widetilde{A}_{\overline{T}}S_{\overline{T}}\widetilde{S}_{\overline{T}}|x_Tu_Ty_Tz_Ta_Ts_Tb_Tc_Tdf}\Big\|\sigma_{Y_{\overline{T}}Z_{\overline{T}}X_{\overline{T}}\widetilde{X}_{\overline{T}}U_{\overline{T}}\widetilde{U}_{\overline{T}}A_{\overline{T}}\widetilde{A}_{\overline{T}}S_{\overline{T}}\widetilde{S}_{\overline{T}}|x_Tu_Ty_Tz_Tdf}\Big)\\
\leq&\mathop{\mathbb{E}}_{\mathsf{P}_{A_TS_TB_TC_TDF}}\mathsf{D}\left(\varphi_{YZX\widetilde{X}U\widetilde{U}A_{\overline{T}}\widetilde{A}_{\overline{T}}S_{\overline{T}}\widetilde{S}_{\overline{T}}|a_Ts_Tb_Tc_Tdf}\Big\|\sigma_{YZX\widetilde{X}U\widetilde{U}A_{\overline{T}}\widetilde{A}_{\overline{T}}S_{\overline{T}}\widetilde{S}_{\overline{T}}|df}\right)\\
\leq&\mathop{\mathbb{E}}_{\mathsf{P}_{DF|\mathcal{E}}}(\log(1/\gamma_{df})+\log(|\mathcal{A}|^{|T|}\cdot|\mathcal{S}|^{|T|}\cdot|\mathcal{B}|^{|T|}\cdot|\mathcal{C}|^{|T|}))\\
\leq&\log\left(1/\mathop{\mathbb{E}}_{\mathsf{P}_{DF|\mathcal{E}}}\gamma_{df}\right)+|T|\cdot\log(|\mathcal{A}|\cdot|\mathcal{S}|\cdot|\mathcal{B}|\cdot|\mathcal{C}|)\\
=&\log(1/\Pr[\mathcal{E}])+|T|\cdot\log(|\mathcal{A}|\cdot|\mathcal{S}|\cdot|\mathcal{B}|\cdot|\mathcal{C}|)=\delta l.
\end{aligned}$$

Now we notice that the state $\sigma_{Y_{\overline{T}}Z_{\overline{T}}X_{\overline{T}}\widetilde{X}_{\overline{T}}U_{\overline{T}}\widetilde{U}_{\overline{T}}A_{\overline{T}}\widetilde{A}_{\overline{T}}S_{\overline{T}}\widetilde{S}_{\overline{T}}|x_Tu_Ty_Tz_Tdf}$ is product across $Y_{\overline{T}}Z_{\overline{T}}$ and the rest of the registers. This is because conditioned on df, YZ is independent of XY, and YZ was not involved in the first round at all, so YZ is definitely in product with $A\widetilde{A}S\widetilde{S}E^{\mathrm{A}}$ in ρ. The unitary that produced σ from ρ does not touch the registers $X\widetilde{X}A\widetilde{A}E^{\mathrm{A}}$ at all, and only uses $U\widetilde{U}S\widetilde{S}$ as control registers. Therefore, there are no correlations between YZ and these registers conditioned on df in σ either. The product structure obviously also holds true if we trace out the $X_{\overline{T}}\widetilde{X}_{\overline{T}}U_{\overline{T}}\widetilde{U}_{\overline{T}}$ registers. Therefore, we can apply Quantum Raz's lemma (Fact 33) to the above bound to say

$$\begin{aligned}
\delta l\geq&\mathop{\mathbb{E}}_{\mathsf{P}_{X_TU_TY_TZ_TA_TS_TB_TC_TDF|\mathcal{E}}}\mathsf{D}\Big(\varphi_{Y_{\overline{T}}Z_{\overline{T}}A_{\overline{T}}\widetilde{A}_{\overline{T}}S_{\overline{T}}\widetilde{S}_{\overline{T}}|x_Tu_Ty_Tz_Ta_Ts_Tb_Tc_Tdf}\Big\|\sigma_{Y_{\overline{T}}Z_{\overline{T}}A_{\overline{T}}\widetilde{A}_{\overline{T}}S_{\overline{T}}\widetilde{S}_{\overline{T}}|x_Tu_Ty_Tz_Tdf}\Big)\\
\geq&\sum_{i\in\overline{T}}\mathsf{I}(Y_iZ_i:A_{\overline{T}}\widetilde{A}_{\overline{T}}S_{\overline{T}}\widetilde{S}_{\overline{T}}|X_TU_TY_TZ_TA_TS_TB_TC_TDF)_{\varphi}\\
\geq&\frac{l}{2}\mathop{\mathbb{E}}_{i\in\overline{T}}\mathop{\mathbb{E}}_{\mathsf{P}_{D_iF_iR_i|\mathcal{E}}}\mathsf{I}(Y_iZ_i:A_{\overline{T}}\widetilde{A}_{\overline{T}}S_{\overline{T}}\widetilde{S}_{\overline{T}})_{\varphi_{d_if_ir_i}}\\
\geq&\frac{l}{2}\cdot\frac{1}{2}\mathop{\mathbb{E}}_{i\in\overline{T}}\mathop{\mathbb{E}}_{\mathsf{P}_{X_iU_iR_i|\mathcal{E}}}\mathsf{I}(Y_iZ_i:A_{\overline{T}}\widetilde{A}_{\overline{T}}S_{\overline{T}}\widetilde{S}_{\overline{T}})_{\varphi_{x_iu_ir_i}}\\
=&\frac{l}{4}\mathop{\mathbb{E}}_{i\in\overline{T}}\mathop{\mathbb{E}}_{\mathsf{P}_{X_iU_iY_iZ_iR_i|\mathcal{E}}}\mathsf{D}\left(\varphi_{A_{\overline{T}}\widetilde{A}_{\overline{T}}S_{\overline{T}}\widetilde{S}_{\overline{T}}|x_iy_iz_ir_i}\Big\|\varphi_{A_{\overline{T}}\widetilde{A}_{\overline{T}}S_{\overline{T}}\widetilde{S}_{\overline{T}}|x_iu_ir_i}\right)\\
\geq&\frac{l}{4}\mathop{\mathbb{E}}_{i\in\overline{T}}\mathop{\mathbb{E}}_{\mathsf{P}_{X_iY_iZ_iR_i|\mathcal{E}}}\mathsf{B}\left(\varphi_{A_{\overline{T}}\widetilde{A}_{\overline{T}}S_{\overline{T}}\widetilde{S}_{\overline{T}}|x_iu_iy_iz_ir_i},\varphi_{A_{\overline{T}}\widetilde{A}_{\overline{T}}S_{\overline{T}}\widetilde{S}_{\overline{T}}|x_iu_ir_i}\right)^2,
\end{aligned}$$

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

$$\mathop{\mathbb{E}}_{i\in\overline{T}}\mathop{\mathbb{E}}_{\mathsf{P}_{X_iY_iZ_iR_i|\mathcal{E}}}\mathsf{B}\left(\varphi_{A_{\overline{T}}\widetilde{A}_{\overline{T}}S_{\overline{T}}\widetilde{S}_{\overline{T}}|x_iy_iz_ir_i},\varphi_{A_{\overline{T}}\widetilde{A}_{\overline{T}}S_{\overline{T}}\widetilde{S}_{\overline{T}}|x_iu_ir_i}\right)\leq 2\sqrt{\delta}. \tag{26}$$

Now (24) implies

$$\mathop{\mathbb{E}}_{i\in\overline{T}}\left\|\mathsf{P}_{X_iU_iY_iZR_i|\mathcal{E}}-\mathsf{P}_{Y_iZ_i}\mathsf{P}_{X_iU_iR_i|\mathcal{E},Y_iZ_i}\right\|_1=\mathop{\mathbb{E}}_{i\in\overline{T}}\left\|\mathsf{P}_{Y_iZ_i|\mathcal{E}}-\mathsf{P}_{Y_iZ_i}\right\|_1\leq\sqrt{2\delta}.$$

Therefore,

$$\begin{aligned}
&\mathop{\mathbb{E}}_{i\in\overline{T}} \mathsf{P}_{Y_iZ_i} \mathop{\mathbb{E}}_{\mathsf{P}_{X_iR_i|\mathcal{E},Y_iZ_i}} \mathsf{B}\left(\varphi_{A_{\overline{T}}\widetilde{A}_{\overline{T}}S_{\overline{T}}\widetilde{S}_{\overline{T}}|x_iu_iy_iz_ir_i}, \varphi_{A_{\overline{T}}\widetilde{A}_{\overline{T}}S_{\overline{T}}\widetilde{S}_{\overline{T}}|x_iu_ir_i}\right) \\
\leq &\mathop{\mathbb{E}}_{i\in\overline{T}} \mathsf{P}_{X_iU_iR_i|\mathcal{E},Y_iZ_i} \mathop{\mathbb{E}} \mathsf{B}\left(\varphi_{A_{\overline{T}}\widetilde{A}_{\overline{T}}S_{\overline{T}}\widetilde{S}_{\overline{T}}|x_iu_iy_iz_ir_i}, \varphi_{A_{\overline{T}}\widetilde{A}_{\overline{T}}S_{\overline{T}}\widetilde{S}_{\overline{T}}|x_iu_ir_i}\right) + \mathop{\mathbb{E}}_{i\in\overline{T}} \left\|\mathsf{P}_{X_iU_iY_iZR_i|\mathcal{E}} - \mathsf{P}_{Y_iZ_i}\mathsf{P}_{X_iU_iR_i|\mathcal{E},Y_iZ_i}\right\|_1 \\
\leq &4\sqrt{\delta}.
\end{aligned}$$

Since $\mathsf{P}_{Y_iZ_i}(\perp,\perp) = \alpha^2$, we have,

$$\mathop{\mathbb{E}}_{i\in\overline{T}} \mathop{\mathbb{E}}_{\mathsf{P}_{X_iU_iR_i|\mathcal{E},\perp,\perp}} \mathsf{B}\left(\varphi_{A_{\overline{T}}\widetilde{A}_{\overline{T}}S_{\overline{T}}\widetilde{S}_{\overline{T}}|x_iu_i\perp\perp r_i}, \varphi_{A_{\overline{T}}\widetilde{A}_{\overline{T}}S_{\overline{T}}\widetilde{S}_{\overline{T}}|x_iu_ir_i}\right) \leq \frac{4\sqrt{\delta}}{\alpha^2}. \tag{27}$$

Applying the Fuchs-van de Graaf inequality to (26) and (27), and tracing out registers besides the i-th one we get,

$$\mathop{\mathbb{E}}_{i\in\overline{T}} \left\|\mathsf{P}_{X_iU_iY_iZ_iR_i|\mathcal{E}}(\mathsf{P}_{A_iS_i|\mathcal{E},X_iU_iY_iZ_iR_i} - \mathsf{P}_{A_iS_i|\mathcal{E},X_iU_iR_i})\right\|_1 \leq 4\sqrt{2\delta}, \tag{28}$$

$$\mathop{\mathbb{E}}_{i\in\overline{T}} \left\|\mathsf{P}_{X_iU_iR_i|\mathcal{E},\perp\perp}(\mathsf{P}_{A_iS_i|\mathcal{E},X_iU_i\perp\perp,R_i} - \mathsf{P}_{A_iS_i|\mathcal{E},X_iU_iR_i})\right\|_1 \leq \frac{8\sqrt{2\delta}}{\alpha^2}. \tag{29}$$

Finally, we can apply item (i) of Fact 34 with $X_iU_i = S$, $Y_iZ_i = T$, $R_i = R$, and the variables conditioned on $\mathcal{E}$ being the corresponding primed variables, since $\mathsf{P}_{X_iU_iY_iZ_i}(x_i,u_i,\perp,\perp) = \alpha^2 \cdot \mathsf{P}_{X_iU_i}(x_i,u_i)$ for all x_i, u_i. Using (24) and (25), this gives us

$$\begin{aligned}
&\mathop{\mathbb{E}}_{i\in\overline{T}} \left\|\mathsf{P}_{X_iU_iR_i|\mathcal{E}} - \mathsf{P}_{X_iU_iR_i|\mathcal{E},\perp\perp}\right\|_1 \\
\leq &\frac{2}{\alpha^2} \mathop{\mathbb{E}}_{i\in\overline{T}} \left\|\mathsf{P}_{X_iU_iY_iZ_iR_i|\mathcal{E}} - \mathsf{P}_{X_iU_iR_i|\mathcal{E}}\mathsf{P}_{Y_iZ_i|X_iU_i}\right\|_1 + \frac{5}{\alpha^2} \mathop{\mathbb{E}}_{i\in\overline{T}} \left\|\mathsf{P}_{X_iU_iY_iZ_i|\mathcal{E}} - \mathsf{P}_{X_iU_iY_iZ_i}\right\|_1 \\
\leq &O\left(\frac{\sqrt{\delta}}{\alpha^2}\right).
\end{aligned} \tag{30}$$

Applying the triangle inequality to the above, as well as (28) and (29) we get,

$$\begin{aligned}
&\mathop{\mathbb{E}}_{i\in\overline{T}} \left\|\mathsf{P}_{X_iU_iY_iZ_iR_i|\mathcal{E}}\left(\mathsf{P}_{A_iS_i|\mathcal{E},X_iU_iY_iZ_iR_i} - \mathsf{P}_{A_iS_i|\mathcal{E},X_iU_i,\perp\perp,R_i}\right)\right\|_1 \\
\leq &\mathop{\mathbb{E}}_{i\in\overline{T}} \Big(\left\|\mathsf{P}_{X_iU_iY_iZ_iR_i|\mathcal{E}}(\mathsf{P}_{A_iS_i|\mathcal{E},X_iU_iY_iZ_iR_i} - \mathsf{P}_{A_iS_i|\mathcal{E},X_iU_iR_i})\right\|_1 \\
&\quad + \left\|\mathsf{P}_{X_iU_iR_i|\mathcal{E},\perp\perp}(\mathsf{P}_{A_iS_i|\mathcal{E},X_iU_i\perp\perp,R_i} - \mathsf{P}_{A_iS_i|\mathcal{E},X_iU_iR_i})\right\|_1 + 2\left\|\mathsf{P}_{X_iU_iR_i|\mathcal{E}} - \mathsf{P}_{X_iU_iR_i|\mathcal{E},\perp\perp}\right\|_1 \Big) \\
\leq &O\left(\frac{\sqrt{\delta}}{\alpha^2}\right).
\end{aligned}$$

This shows item (iii) of the lemma.

For later calculations, we note that the state $\sigma_{YZ\widetilde{Z}A\widetilde{A}S\widetilde{S}|df}$ is also product across Y and the rest of the registers. Therefore, it is possible to get bounds on $\mathbb{E}_{i\in\overline{T}} \mathbb{E}_{\mathsf{P}_{D_iF_iR_i}} \mathsf{I}(Y_i : Z_{\overline{T}}\widetilde{Z}_{\overline{T}}A_{\overline{T}}\widetilde{A}_{\overline{T}})_{\varphi_{d_if_ir_i}}$ in the

exact same way. Doing the same calculation as above with this quantity and conditioning $Y_i = \perp$ (which happens with probability α under P_{Y_i}), we can get

$$\mathop{\mathbb{E}}_{i\in\overline{T}} \left\| \mathsf{P}_{X_iU_iY_iR_i|\mathcal{E}} (\mathsf{P}_{Z_iA_iS_i|\mathcal{E},X_iU_iY_iR_i} - \mathsf{P}_{Z_iA_iS_i|\mathcal{E},X_iU_i,Y_i=\perp,R_i}) \right\|_1 \leq O\left(\frac{\sqrt{\delta}}{\alpha}\right). \tag{31}$$

Note that we have had to apply Fact 34 with $X_iU_iZ_i = S, Y_i = T$ and $R_i = R$ to get the above inequality, which is possible because $\mathsf{P}_{X_iU_iY_iZ_i}(x_i, u_i, \perp, z_i) = \alpha \cdot \mathsf{P}_{X_iU_iZ_i}(x_i, u_i, z_i)$ for all x_i, u_i, z_i. Similarly, on Charlie's side we have,

$$\mathop{\mathbb{E}}_{i\in\overline{T}} \left\| \mathsf{P}_{X_iU_iZ_iR_i|\mathcal{E}} (\mathsf{P}_{Y_iA_iS_i|\mathcal{E},X_iU_iZ_iR_i} - \mathsf{P}_{Y_iA_iS_i|\mathcal{E},X_iU_i,Z_i=\perp,R_i}) \right\|_1 \leq O\left(\frac{\sqrt{\delta}}{\alpha}\right). \tag{32}$$

Existence of unitaries $V^{\mathrm{A}}_{i,x_ir_i}$ and $V^{\mathrm{BC}}_{i,u_ir_i}$. The proof of item (ii) of the lemma will be very similar to the analogous step in the proof of the parallel repetition theorem in [KT23]. Applying Fact 32 on the states $\varphi_{XU\tilde{U}Y\tilde{Y}Z\tilde{Z}S_{\overline{T}}\tilde{S}_{\overline{T}}B_{\overline{T}}C_{\overline{T}}E^{\mathrm{B}}E^{\mathrm{C}}|a_Ts_Tb_Tc_Tdf}$ and $\sigma_{XU\tilde{U}Y\tilde{Y}Z\tilde{Z}S_{\overline{T}}\tilde{S}_{\overline{T}}B_{\overline{T}}\tilde{C}_{\overline{T}}E^{\mathrm{B}}E^{\mathrm{C}}|df}$ with z being $a_Ts_Tb_Tc_T$ as before, we get,

$$\begin{aligned}
&\mathop{\mathbb{E}}_{\mathsf{P}_{X_TU_TY_TZ_TA_TS_TB_TC_TDF|\mathcal{E}}} \mathsf{D}\left(\varphi_{X_{\overline{T}}U_{\overline{T}}\tilde{U}_{\overline{T}}Y_{\overline{T}}\tilde{Y}_{\overline{T}}Z_{\overline{T}}\tilde{Z}_{\overline{T}}S_{\overline{T}}\tilde{S}_{\overline{T}}B_{\overline{T}}C_{\overline{T}}E^{\mathrm{B}}E^{\mathrm{C}}|x_Tu_Ty_Tz_Ta_Ts_Tb_Tc_Tdf} \middle\| \sigma_{X_{\overline{T}}U_{\overline{T}}\tilde{U}_{\overline{T}}Y_{\overline{T}}\tilde{Y}_{\overline{T}}Z_{\overline{T}}\tilde{Z}_{\overline{T}}S_{\overline{T}}\tilde{S}_{\overline{T}}B_{\overline{T}}\tilde{C}_{\overline{T}}E^{\mathrm{B}}E^{\mathrm{C}}|x_Tu_Ty_Tz_Tdf}\right) \\
\leq &\mathop{\mathbb{E}}_{\mathsf{P}_{A_TS_TB_TC_TDF|\mathcal{E}}} \mathsf{D}\left(\varphi_{XU\tilde{U}Y\tilde{Y}Z\tilde{Z}S_{\overline{T}}\tilde{S}_{\overline{T}}B_{\overline{T}}C_{\overline{T}}E^{\mathrm{B}}E^{\mathrm{C}}|a_Ts_Tb_Tc_Tdf} \middle\| \sigma_{XU\tilde{U}Y\tilde{Y}Z\tilde{Z}S_{\overline{T}}\tilde{S}_{\overline{T}}B_{\overline{T}}\tilde{C}_{\overline{T}}E^{\mathrm{B}}E^{\mathrm{C}}|df}\right) \\
\leq &\mathop{\mathbb{E}}_{\mathsf{P}_{DF|\mathcal{E}}} (\log(1/\gamma_{df}) + \log(|\mathcal{A}|^{|T|} \cdot |\mathcal{S}|^{|T|} \cdot |\mathcal{B}|^{|T|} \cdot |\mathcal{C}|^{|T|})) \\
\leq &\delta l.
\end{aligned}$$

Notice that $\sigma_{X_{\overline{T}}U_{\overline{T}}\tilde{U}_{\overline{T}}Y_{\overline{T}}\tilde{Y}_{\overline{T}}Z_{\overline{T}}\tilde{Z}_{\overline{T}}S_{\overline{T}}\tilde{S}_{\overline{T}}B_{\overline{T}}\tilde{C}_{\overline{T}}E^{\mathrm{B}}E^{\mathrm{C}}|x_Tu_Ty_Tz_Tdf}$ is product across $X_{\overline{T}}$ and the rest of the registers. This is because conditioned on df, $X_{\overline{T}}$ is in product with the rest of the input registers, and the registers $S_{\overline{T}}\tilde{S}_{\overline{T}}B_{\overline{T}}\tilde{C}_{\overline{T}}E^{\mathrm{B}}E^{\mathrm{C}}$ are acted upon by unitaries that are conditioned on the rest of the input registers only. Henceforth, we shall use $\tilde{E}^{\mathrm{BC}}$ to refer to the registers $U_{\overline{T}}\tilde{U}_{\overline{T}}Y_{\overline{T}}\tilde{Y}_{\overline{T}}Z_{\overline{T}}\tilde{Z}_{\overline{T}}S_{\overline{T}}\tilde{S}_{\overline{T}}B_{\overline{T}}C_{\overline{T}}E^{\mathrm{B}}E^{\mathrm{C}}$ for brevity. We can apply Quantum Raz's Lemma (Fact 33) to say as before,

$$\begin{aligned}
\delta l &\geq \mathop{\mathbb{E}}_{\mathsf{P}_{X_TU_TY_TZ_TA_TS_TB_TC_TDF|\mathcal{E}}} \mathsf{D}\left(\varphi_{X_{\overline{T}}\tilde{E}^{\mathrm{BC}}|x_Tu_Ty_Tz_Ta_Ts_Tb_Tc_Tdf} \middle\| \sigma_{X_{\overline{T}}\tilde{E}^{\mathrm{BC}}|x_Tu_Ty_Tz_Tdf}\right) \\
&\geq \sum_{i\in\overline{T}} \mathsf{I}(X_i : \tilde{E}^{\mathrm{BC}}|X_TU_TY_TZ_TA_TS_TB_TC_TDF)_\varphi \\
&\geq \frac{l}{4} \mathop{\mathbb{E}}_{i\in\overline{T}} \mathop{\mathbb{E}}_{\mathsf{P}_{X_iY_iZ_iR_i|\mathcal{E}}} \mathsf{B}\left(\varphi_{\tilde{E}^{\mathrm{BC}}|x_iy_iz_ir_i}, \varphi_{\tilde{E}^{\mathrm{BC}}|y_iz_ir_i}\right)^2.
\end{aligned}$$

Using Jensen's inequality on the above, we then have,

$$\mathop{\mathbb{E}}_{i\in\overline{T}} \mathop{\mathbb{E}}_{\mathsf{P}_{X_iY_iZ_iR_i|\mathcal{E}}} \mathsf{B}\left(\varphi_{\tilde{E}^{\mathrm{BC}}|x_iy_iz_ir_i}, \varphi_{\tilde{E}^{\mathrm{BC}}|y_iz_ir_i}\right) \leq 2\sqrt{\delta}.$$

Shifting the expectation from $\mathsf{P}_{X_iY_iZ_iR_i|\mathcal{E}}$ to $\mathsf{P}_{Y_iZ_i}\mathsf{P}_{X_iU_iR_i|\mathcal{E},Y_iZ_i}$ and conditioning on $Y_iZ_i = (\perp, \perp)$ as before, we then have,

$$\mathop{\mathbb{E}}_{i\in\overline{T}} \mathop{\mathbb{E}}_{\mathsf{P}_{X_iR_i|\mathcal{E},\perp,\perp}} \mathsf{B}\left(\varphi_{\tilde{E}^{\mathrm{BC}}|x_i\perp\perp r_i}, \varphi_{\tilde{E}^{\mathrm{BC}}|\perp\perp r_i}\right) \leq \frac{4\sqrt{\delta}}{\alpha^2}.$$

Finally, since $|\varphi\rangle_{x_i\perp\perp r_i}$ and $|\varphi\rangle_{\perp\perp r_i}$ are purifications of $\varphi_{\widetilde{E}^{\mathrm{BC}}|x_i\perp\perp r_i}$ and $\varphi_{\widetilde{E}^{\mathrm{BC}}|\perp\perp r_i}$, by Uhlmann's theorem and the Fuchs-van de Graaf inequality, there exist unitaries $V^{\mathrm{A}}_{i,x_ir_i}$ acting on registers outside of $\widetilde{E}^{\mathrm{BC}}$, i.e., on $X_{\overline{T}}\widetilde{X}_{\overline{T}}E^{\mathrm{A}}A_{\overline{T}}\widetilde{A}_{\overline{T}}$ (the values in other registers are fixed by r_i) such that

$$\mathop{\mathbb{E}}_{i\in\overline{T}}\mathop{\mathbb{E}}_{\mathsf{P}_{X_iR_i|\mathcal{E},\perp\perp}}\left\|V^{\mathrm{A}}_{i,x_ir_i}\otimes\mathbb{1}\,|\varphi\rangle\langle\varphi|_{\perp\perp r_i}\,(V^{\mathrm{A}}_{i,x_ir_i})^\dagger\otimes\mathbb{1}-|\varphi\rangle\langle\varphi|_{x_i\perp\perp r_i}\right\|_1\leq\frac{8\sqrt{2\delta}}{\alpha^2}. \tag{33}$$

By the same analysis on Barlie's side, we can say that there exist unitaries $V^{\mathrm{BC}}_{i,u_ir_i}$ acting on $U_{\overline{T}}\widetilde{U}_{\overline{T}}Y_{\overline{T}}\widetilde{Y}_{\overline{T}}Z_{\overline{T}}\widetilde{Z}_{\overline{T}}S_{\overline{T}}\widetilde{S}_{\overline{T}}B_{\overline{T}}C_{\overline{T}}E^{\mathrm{B}}E^{\mathrm{C}}$ such that

$$\mathop{\mathbb{E}}_{i\in\overline{T}}\mathop{\mathbb{E}}_{\mathsf{P}_{U_iR_i|\mathcal{E},\perp\perp}}\left\|\mathbb{1}\otimes V^{\mathrm{BC}}_{i,u_ir_i}\,|\varphi\rangle\langle\varphi|_{\perp\perp r_i}\,\mathbb{1}\otimes(V^{\mathrm{BC}}_{i,u_ir_i})^\dagger-|\varphi\rangle\langle\varphi|_{u_i\perp\perp r_i}\right\|_1\leq\frac{8\sqrt{2\delta}}{\alpha^2}. \tag{34}$$

Now, if $\mathcal{O}_{X_i}$ is the channel that measures the X_i register and records the outcome, this commutes with the $V^{\mathrm{BC}}_{i,u_ir_i}$ unitaries. So,

$$\mathcal{O}_{X_i}\left(\mathbb{1}\otimes V^{\mathrm{BC}}_{i,u_ir_i}\,|\varphi\rangle\langle\varphi|_{\perp\perp r_i}\,\mathbb{1}\otimes(V^{\mathrm{BC}}_{i,u_ir_i})^\dagger\right)=\mathop{\mathbb{E}}_{\mathsf{P}_{X_i|\mathcal{E},\perp\perp r_i}}|x_i\rangle\langle x_i|\otimes\left(\mathbb{1}\otimes V^{\mathrm{BC}}_{i,u_ir_i}\,|\varphi\rangle\langle\varphi|_{x_i\perp\perp r_i}\,\mathbb{1}\otimes(V^{\mathrm{BC}}_{i,u_ir_i})^\dagger\right)$$
$$\mathcal{O}_{X_i}\left(|\varphi\rangle\langle\varphi|_{u_i\perp\perp r_i}\right)=\mathop{\mathbb{E}}_{\mathsf{P}_{X_i|\mathcal{E},u_i\perp\perp r_i}}|x_i\rangle\langle x_i|\otimes|\varphi\rangle\langle\varphi|_{x_iu_i\perp\perp r_i}.$$

Therefore, applying Fact 1 to (34) with the $\mathcal{O}_{X_i}$ channel we get,

$$\mathop{\mathbb{E}}_{i\in\overline{T}}\mathop{\mathbb{E}}_{\mathsf{P}_{U_iR_i|\mathcal{E},\perp\perp}}\left\|\mathop{\mathbb{E}}_{\mathsf{P}_{X_i|\mathcal{E},\perp\perp r_i}}|x_i\rangle\langle x_i|\otimes\left(\mathbb{1}\otimes V^{\mathrm{BC}}_{i,u_ir_i}\,|\varphi\rangle\langle\varphi|_{x_i\perp\perp r_i}\,\mathbb{1}\otimes(V^{\mathrm{BC}}_{i,u_ir_i})^\dagger\right)-\mathop{\mathbb{E}}_{\mathsf{P}_{X_i|\mathcal{E},u_i\perp\perp r_i}}|x_i\rangle\langle x_i|\otimes|\varphi\rangle\langle\varphi|_{x_iy_i\perp r_i}\right\|_1$$
$$\leq\frac{8\sqrt{2\delta}}{\alpha^2}.$$

Therefore,

$$\mathop{\mathbb{E}}_{i\in\overline{T}}\mathop{\mathbb{E}}_{\mathsf{P}_{X_iU_iR_i|\mathcal{E},\perp\perp}}\left\|\mathbb{1}\otimes V^{\mathrm{BC}}_{i,u_ir_i}\,|\varphi\rangle\langle\varphi|_{x_i\perp\perp r_i}\,\mathbb{1}\otimes(V^{\mathrm{BC}}_{i,u_ir_i})^\dagger-|\varphi\rangle\langle\varphi|_{x_iu_i\perp\perp r_i}\right\|_1$$
$$\leq\frac{8\sqrt{2\delta}}{\alpha^2}+2\mathop{\mathbb{E}}_{i\in\overline{C}}\left\|\mathsf{P}_{X_iU_iR_i|\mathcal{E},\perp\perp}-\mathsf{P}_{R_i|\mathcal{E},\perp\perp}\mathsf{P}_{X_i|\mathcal{E},\perp\perp,R_i}\mathsf{P}_{U_i|\mathcal{E},\perp\perp,R_i}\right\|_1. \tag{35}$$

Combining (33) and (35) we get,

$$\mathop{\mathbb{E}}_{i\in\overline{T}}\mathop{\mathbb{E}}_{\mathsf{P}_{X_iU_iR_i|\mathcal{E},\perp\perp}}\left\|V^{\mathrm{A}}_{i,x_ir_i}\otimes V^{\mathrm{BC}}_{i,u_ir_i}\,|\varphi\rangle\langle\varphi|_{\perp\perp r_i}\,(V^{\mathrm{A}}_{i,x_ir_i})^\dagger\otimes(V^{\mathrm{BC}}_{i,u_ir_i})^\dagger-|\varphi\rangle\langle\varphi|_{x_iu_i\perp\perp r_i}\right\|_1$$
$$\leq\mathop{\mathbb{E}}_{i\in\overline{T}}\mathop{\mathbb{E}}_{\mathsf{P}_{X_iU_iR_i|\mathcal{E},\perp\perp}}\left\|\mathbb{1}\otimes V^{\mathrm{BC}}_{i,u_ir_i}\left(V^{\mathrm{A}}_{i,x_ir_i}\otimes\mathbb{1}\,|\varphi\rangle\langle\varphi|_{\perp\perp r_i}\,(V^{\mathrm{A}}_{i,x_ir_i})^\dagger\otimes\mathbb{1}-|\varphi\rangle\langle\varphi|_{x_i\perp\perp r_i}\right)\mathbb{1}\otimes(V^{\mathrm{BC}}_{i,u_ir_i})^\dagger\right\|_1$$
$$+\mathop{\mathbb{E}}_{i\in\overline{T}}\mathop{\mathbb{E}}_{\mathsf{P}_{X_iU_iR_i|\mathcal{E},\perp\perp}}\left\|\mathbb{1}\otimes V^{\mathrm{BC}}_{i,u_ir_i}\,|\varphi\rangle\langle\varphi|_{x_i\perp\perp r_i}\,\mathbb{1}\otimes(V^{\mathrm{BC}}_{i,u_ir_i})^\dagger-|\varphi\rangle\langle\varphi|_{x_iu_i\perp\perp r_i}\right\|_1$$
$$\leq\frac{8\sqrt{2\delta}}{\alpha^2}+\frac{8\sqrt{2\delta}}{\alpha^2}+2\mathop{\mathbb{E}}_{i\in\overline{T}}\left\|\mathsf{P}_{X_iU_iR_i|\mathcal{E},\perp\perp}-\mathsf{P}_{R_i|\mathcal{E},\perp\perp}\mathsf{P}_{X_i|\mathcal{E},\perp\perp,R_i}\mathsf{P}_{U_i|\mathcal{E},\perp\perp,R_i}\right\|_1. \tag{36}$$

By Fact 3 we have,

$$\begin{aligned}\mathop{\mathbb{E}}_{i\in\overline{T}}\left\|\mathsf{P}_{X_iU_iR_i|\mathcal{E},\perp\perp}-\mathsf{P}_{X_iU_i|\perp\perp}\mathsf{P}_{R_i|\mathcal{E},\perp\perp}\right\|_1 &\leq \frac{2}{\mathsf{P}_{Y_iZ_i}(\perp,\perp)}\mathop{\mathbb{E}}_{i\in\overline{T}}\left\|\mathsf{P}_{X_iU_iY_iZ_iR_i|\mathcal{E}}-\mathsf{P}_{X_iU_i|Y_iZ_i}\mathsf{P}_{Y_iZ_iR_i|\mathcal{E}}\right\|_1\\ &\leq \frac{4\sqrt{2\delta}}{\alpha^2},\end{aligned}$$

where we have used (25) in the last line. Noting that $\mathsf{P}_{X_iU_i|\perp\perp}=\mathsf{P}_{X_iU_i}=\mathsf{P}_{X_i}\mathsf{P}_{U_i}=\mathsf{P}_{X_i|\perp\perp}\mathsf{P}_{U_i|\perp\perp}$, we then have,

$$\begin{aligned}&\mathop{\mathbb{E}}_{i\in\overline{T}}\left\|\mathsf{P}_{X_iU_iR_i|\mathcal{E},\perp\perp}-\mathsf{P}_{R_i|\mathcal{E},\perp\perp}\mathsf{P}_{X_i|\mathcal{E},\perp\perp,R_i}\mathsf{P}_{U_i|\mathcal{E},\perp\perp,R_i}\right\|_1\\ \leq&\mathop{\mathbb{E}}_{i\in\overline{T}}\Big(\left\|\mathsf{P}_{X_iU_iR_i|\mathcal{E},\perp\perp}-\mathsf{P}_{X_iU_i|\perp\perp}\mathsf{P}_{R_i|\mathcal{E},\perp\perp}\right\|_1+\left\|(\mathsf{P}_{X_i|\perp\perp}\mathsf{P}_{R_i|\mathcal{E},\perp\perp}-\mathsf{P}_{X_iR_i|\mathcal{E},\perp\perp})\mathsf{P}_{U_i|\perp\perp}\right\|_1\\ &\quad+\left\|(\mathsf{P}_{U_i|\perp\perp}\mathsf{P}_{R_i|\mathcal{E},\perp\perp}-\mathsf{P}_{U_iR_i|\mathcal{E},\perp\perp})\mathsf{P}_{X_i|\mathcal{E},\perp\perp,R_i}\right\|_1\Big)\\ \leq&\mathop{\mathbb{E}}_{i\in\overline{T}}\Big(\left\|\mathsf{P}_{X_iU_iR_i|\mathcal{E},\perp\perp}-\mathsf{P}_{X_iU_i|\perp\perp}\mathsf{P}_{R_i|\mathcal{E},\perp\perp}\right\|_1+\left\|\mathsf{P}_{X_i|\perp\perp}\mathsf{P}_{R_i|\mathcal{E},\perp\perp}-\mathsf{P}_{X_iR_i|\mathcal{E},\perp\perp}\right\|_1\\ &\quad+\left\|\mathsf{P}_{U_i|\perp\perp}\mathsf{P}_{R_i|\mathcal{E},\perp\perp}-\mathsf{P}_{U_iR_i|\mathcal{E},\perp\perp}\right\|_1\Big)\\ \leq&3\mathop{\mathbb{E}}_{i\in\overline{T}}\left\|\mathsf{P}_{X_iU_iR_i|\mathcal{E},\perp\perp}-\mathsf{P}_{X_iU_i|\perp\perp}\mathsf{P}_{R_i|\mathcal{E},\perp\perp}\right\|_1\leq\frac{12\sqrt{2\delta}}{\alpha^2}.\end{aligned}$$

Putting the above in (36) we get,

$$\begin{aligned}&\mathop{\mathbb{E}}_{i\in\overline{T}}\mathop{\mathbb{E}}_{\mathsf{P}_{X_iU_iR_i|\mathcal{E},\perp\perp}}\left\|V^{\mathrm{A}}_{i,x_ir_i}\otimes V^{\mathrm{BC}}_{i,u_ir_i}|\varphi\rangle\langle\varphi|_{\perp\perp r_i}(V^{\mathrm{A}}_{i,x_ir_i})^\dagger\otimes(V^{\mathrm{BC}}_{i,u_ir_i})^\dagger-|\varphi\rangle\langle\varphi|_{x_iu_i\perp\perp r_i}\right\|_1\\ \leq&O\left(\frac{\sqrt{\delta}}{\alpha^2}\right).\end{aligned}\tag{37}$$

Finally, from (30) and (37) we get,

$$\begin{aligned}&\mathop{\mathbb{E}}_{i\in\overline{T}}\mathop{\mathbb{E}}_{\mathsf{P}_{X_iU_iR_i|\mathcal{E}}}\left\|V^{\mathrm{A}}_{i,x_ir_i}\otimes V^{\mathrm{BC}}_{i,u_ir_i}|\varphi\rangle\langle\varphi|_{\perp\perp r_i}(V^{\mathrm{A}}_{i,x_ir_i})^\dagger\otimes(V^{\mathrm{BC}}_{i,u_ir_i})^\dagger-|\varphi\rangle\langle\varphi|_{x_iu_i\perp\perp r_i}\right\|_1\\ \leq&\mathop{\mathbb{E}}_{i\in\overline{T}}\mathop{\mathbb{E}}_{\mathsf{P}_{X_iU_iR_i|\mathcal{E},\perp\perp}}\left\|V^{\mathrm{A}}_{i,x_ir_i}\otimes V^{\mathrm{BC}}_{i,u_ir_i}|\varphi\rangle\langle\varphi|_{\perp\perp r_i}(V^{\mathrm{A}}_{i,x_ir_i})^\dagger\otimes(V^{\mathrm{BC}}_{i,u_ir_i})^\dagger-|\varphi\rangle\langle\varphi|_{x_iu_i\perp\perp r_i}\right\|_1\\ &\quad+\mathop{\mathbb{E}}_{i\in\overline{T}}\left\|\mathsf{P}_{X_iU_iR_i|\mathcal{E}}-\mathsf{P}_{X_iU_iR_i|\mathcal{E},\perp\perp}\right\|_1\\ \leq&O\left(\frac{\sqrt{\delta}}{\alpha^2}\right).\end{aligned}$$

This completes the proof of item (ii) of the lemma.

Existence of unitaries $V^{\mathrm{B}}_{i,y_ir_i}$ and $V^{\mathrm{C}}_{i,z_ir_i}$. We observe that $\sigma_{Y_{\overline{T}}X_{\overline{T}}\widetilde{X}_{\overline{T}}\widetilde{U}_{\overline{T}}\widetilde{S}_{\overline{T}}Z_{\overline{T}}\widetilde{Z}_{\overline{T}}A_{\overline{T}}\widetilde{A}_{\overline{T}}C_{\overline{T}}E^{\mathrm{A}}E^{\mathrm{C}}|x_Tu_Ty_Tz_Tdf}$ is product across $Y_{\overline{T}}$ and the rest of the registers. $Y_{\overline{T}}$ is in product with Alice's registers conditioned on $x_Tu_Ty_Tz_Tdf$ here because that was the case in the state ρ at the end of the first round; Alice's registers don't change from the first round, and $Y_{\overline{T}}$ is only acted upon as a control register to get σ from ρ. $Y_{\overline{T}}$ was also in product with Barlie's input and output registers as well as Charlie's

registers in ρ conditioned on $x_t u_T y_T z_T df$, and remain so after Bob and Charlie's unitaries. Hence using $\widetilde{E}^{\mathrm{AC}}$ to denote the registers $X_{\overline{T}}\widetilde{X}_{\overline{T}}\widetilde{U}_{\overline{T}}\widetilde{S}_{\overline{T}}Z_{\overline{T}}\widetilde{Z}_{\overline{T}}A_{\overline{T}}\widetilde{A}_{\overline{T}}C_{\overline{T}}E^{\mathrm{A}}E^{\mathrm{C}}$ and applying Facts 32 and 33 again on $\varphi_{Y_{\overline{T}}\widetilde{E}^{\mathrm{AC}}|x_T u_T y_T z_T a_t s_t b_t c_T df}$ and $\sigma_{Y_{\overline{T}}\widetilde{E}^{\mathrm{AC}}|x_T u_T y_T z_T df}$we get,

$$\begin{aligned}
2\delta &\geq \mathop{\mathbb{E}}_{i\in\overline{T}} \mathsf{I}(Y_i : \widetilde{E}^{\mathrm{AC}}|D_i F_i R_i)_{\varphi} \\
&= \mathop{\mathbb{E}}_{i\in\overline{T}} \mathop{\mathbb{E}}_{\mathsf{P}_{Y_i F_i R_i|\mathcal{E}}} \mathsf{D}\left(\varphi_{\widetilde{E}^{\mathrm{AC}}|y_i d_i f_i r_i}\middle\|\varphi_{\widetilde{E}^{\mathrm{AC}}|d_i f_i r_i}\right) \\
&\geq \frac{1}{2}\mathop{\mathbb{E}}_{i\in\overline{T}} \mathop{\mathbb{E}}_{\mathsf{P}_{X_i U_i Y_i R_i|\mathcal{E}}} \mathsf{D}\left(\varphi_{\widetilde{E}^{\mathrm{AC}}|x_i u_i y_i r_i}\middle\|\varphi_{\widetilde{E}^{\mathrm{AC}}|x_i u_i r_i}\right) \\
&\geq \frac{1}{2}\mathop{\mathbb{E}}_{i\in\overline{T}} \mathop{\mathbb{E}}_{\mathsf{P}_{X_i U_i Y_i R_i|\mathcal{E}}} \mathsf{B}\left(\varphi_{\widetilde{E}^{\mathrm{AC}}|x_i u_i y_i r_i}, \varphi_{\widetilde{E}^{\mathrm{AC}}|x_i u_i r_i}\right)^2.
\end{aligned}$$

Applying Jensen's inequality on the above, we get

$$\mathop{\mathbb{E}}_{i\in\overline{T}} \mathop{\mathbb{E}}_{\mathsf{P}_{X_i U_i Y_i R_i|\mathcal{E}}} \mathsf{B}\left(\varphi_{\widetilde{E}^{\mathrm{AC}}|x_i u_i y_i r_i}, \varphi_{\widetilde{E}^{\mathrm{AC}}|x_i u_i r_i}\right) \leq 2\sqrt{\delta}. \tag{38}$$

Moreover, shifting the expectation from $\mathsf{P}_{X_i U_i Y_i R_i|\mathcal{E}}$ to $\mathsf{P}_{Y_i}\mathsf{P}_{X_i U_i R_i|\mathcal{E},Y_i}$ and conditioning on $Y_i = \perp$ (which happens with probability α under P_{Y_i}) like before, we get,

$$\mathop{\mathbb{E}}_{i\in\overline{T}} \mathop{\mathbb{E}}_{\mathsf{P}_{X_i U_i R_i|\mathcal{E},Y_i=\perp}} \mathsf{B}\left(\varphi_{\widetilde{E}^{\mathrm{AC}}|x_i u_i, Y_i=\perp r_i}, \varphi_{\widetilde{E}^{\mathrm{AC}}|x_i u_i r_i}\right) \leq \frac{4\sqrt{\delta}}{\alpha}. \tag{39}$$

Using the triangle inequality on (38) and (39), we get,

$$\begin{aligned}
&\mathop{\mathbb{E}}_{i\in\overline{T}} \mathop{\mathbb{E}}_{\mathsf{P}_{X_i U_i Y_i R_i|\mathcal{E}}} \mathsf{B}\left(\varphi_{\widetilde{E}^{\mathrm{AC}}|x_i u_i y_i r_i}, \varphi_{\widetilde{E}^{\mathrm{AC}}|x_i u_i, Y_i=\perp, r_i}\right) \\
\leq &\mathop{\mathbb{E}}_{i\in\overline{T}} \mathop{\mathbb{E}}_{\mathsf{P}_{X_i U_i Y_i R_i|\mathcal{E}}} \mathsf{B}\left(\varphi_{\widetilde{E}^{\mathrm{AC}}|x_i u_i y_i r_i}, \varphi_{\widetilde{E}^{\mathrm{AC}}|x_i u_i r_i}\right) \\
&\quad + \mathop{\mathbb{E}}_{i\in\overline{T}} \mathop{\mathbb{E}}_{\mathsf{P}_{X_i U_i R_i|\mathcal{E},Y_i=\perp}} \mathsf{B}\left(\varphi_{\widetilde{E}^{\mathrm{AC}}|x_i u_i, Y_i=\perp, r_i}, \varphi_{\widetilde{E}^{\mathrm{AC}}|x_i u_i r_i}\right) \\
&\quad + \mathop{\mathbb{E}}_{i\in\overline{T}} \left\|(\mathsf{P}_{X_i U_i R_i|\mathcal{E}} - \mathsf{P}_{X_i U_i R_i|\mathcal{E},Y_i=\perp})\mathsf{P}_{Y_i|\mathcal{E},X_i U_i R_i}\right\|_1 \\
\leq &2\sqrt{\delta} + \frac{4\sqrt{\delta}}{\alpha} + \frac{2}{\alpha}\mathop{\mathbb{E}}_{i\in\overline{T}} \left\|\mathsf{P}_{X_i U_i Y_i R_i|\mathcal{E}} - \mathsf{P}_{X_i U_i R_i|\mathcal{E}}\mathsf{P}_{Y_i|X_i U_i}\right\|_1 + \frac{5}{\alpha}\mathop{\mathbb{E}}_{i\in\overline{T}} \left\|\mathsf{P}_{X_i U_i Y_i|\mathcal{E}} - \mathsf{P}_{X_i U_i Y_i}\right\|_1 \\
\leq &2\sqrt{\delta} + \frac{4\sqrt{\delta}}{\alpha} + \frac{4\sqrt{2\delta}}{\alpha} + \frac{5\sqrt{2\delta}}{\alpha} \\
\leq &O\left(\frac{\sqrt{\delta}}{\alpha}\right).
\end{aligned}$$

In the third line of the above calculation, we have noted that we can apply item (i) of Fact 34 to bound the distance $\left\|\mathsf{P}_{X_i U_i R_i|\mathcal{E}} - \mathsf{P}_{X_i U_i R_i|\mathcal{E},Y_i=\perp}\right\|_1$ with $T = Y_i$, since we have $\mathsf{P}_{X_i U_i Y_i}(x_i, u_i, \perp)$ $= \alpha \cdot \mathsf{P}_{X_i U_i}(x_i, u_i)$ for all x_i, u_i. In the fourth line, we have used (25) and (24) to bound the trace distances. Finally, using Uhlmann's theorem and the Fuchs-van de Graaf inequality on the above,

we get that there exist unitaries $V^{\mathrm{B}}_{i,x_iu_iy_ir_i}$ acting on the registers outside $\widetilde{E}^{\mathrm{AC}}$, i.e., on $Y_{\overline{T}}\widetilde{Y}_{\overline{T}}U_{\overline{T}}S_{\overline{T}}BE^{\mathrm{B}}$, such that

$$\mathop{\mathbb{E}}_{i\in\overline{T}}\mathop{\mathbb{E}}_{\mathsf{P}_{X_iU_iY_iR_i|\mathcal{E}}}\left\|V^{\mathrm{B}}_{i,x_iu_iy_ir_i}\otimes\mathbb{1}\,|\varphi\rangle\langle\varphi|_{x_iu_i,Y_i=\perp,r_i}\,(V^{\mathrm{B}}_{i,x_iu_iy_ir_i})^\dagger\otimes\mathbb{1}-|\varphi\rangle\langle\varphi|_{x_iu_iy_ir_i}\right\|_1\leq O\left(\frac{\sqrt{\delta}}{\alpha}\right). \tag{40}$$

Since y_i is either $\perp$, in which case the unitary $V^{\mathrm{B}}_{i,x_iu_iy_ir_i}$ is just the identity, or y_i is equal to x_i, $V^{\mathrm{B}}_{i,x_iu_iy_ir_i}$ is in fact just $V^{\mathrm{B}}_{i,u_iy_ir_i}$.

Let $\mathcal{O}_{Z_iA_iS_i}$ be the channel which measures the $Z_iA_i\widetilde{S}_i$ registers and records the outcome, which commutes with $V^{\mathrm{B}}_{i,u_iy_ir_i}$. We have,

$$\begin{aligned}
&\mathcal{O}_{Z_iA_iS_i}\left(V^{\mathrm{B}}_{i,u_iy_ir_i}\otimes\mathbb{1}\,|\varphi\rangle\langle\varphi|_{x_iu_i,Y_i=\perp,r_i}\,(V^{\mathrm{B}}_{i,u_iy_ir_i})^\dagger\otimes\mathbb{1}\right)\\
=&\mathop{\mathbb{E}}_{\mathsf{P}_{Z_iA_iS_i|\mathcal{E},x_iu_i,Y_i=\perp,r_i}}|z_ia_is_i\rangle\langle z_ia_is_i|\otimes\left(V^{\mathrm{B}}_{i,u_iy_ir_i}\otimes\mathbb{1}\,|\varphi\rangle\langle\varphi|_{x_iu_i,Y_i=\perp,z_ia_is_ir_i}\,(V^{\mathrm{B}}_{i,u_iy_ir_i})^\dagger\otimes\mathbb{1}\right)\\
&\mathcal{O}_{Z_iA_iS_i}\left(|\varphi_{x_iu_iy_ir_i}\rangle\langle\varphi_{x_iu_iy_ir_i}|\right)=\mathop{\mathbb{E}}_{\mathsf{P}_{Z_iA_iS_i|\mathcal{E},x_iu_iy_ir_i}}|z_ia_is_i\rangle\langle z_ia_is_i|\otimes|\varphi\rangle\langle\varphi|_{x_iu_iy_iz_ia_is_ir_i}.
\end{aligned}$$

Applying Fact 6 on (40) we thus get,

$$\begin{aligned}
&\mathop{\mathbb{E}}_{i\in\overline{T}}\mathop{\mathbb{E}}_{\mathsf{P}_{X_iU_iY_iZ_iA_iS_iR_i|\mathcal{E}}}\left\|V^{\mathrm{B}}_{i,u_iy_ir_i}\otimes\mathbb{1}\,|\varphi\rangle\langle\varphi|_{x_iu_i,Y_i=\perp,z_ia_is_ir_i}\,(V^{\mathrm{B}}_{i,u_iy_ir_i})^\dagger\otimes\mathbb{1}-|\varphi\rangle\langle\varphi|_{x_iu_iy_iz_ia_is_ir_i}\right\|_1\\
\leq&\mathop{\mathbb{E}}_{i\in\overline{T}}\mathop{\mathbb{E}}_{\mathsf{P}_{X_iU_iY_iR_i|\mathcal{E}}}\left\|V^{\mathrm{B}}_{i,u_iy_ir_i}\otimes\mathbb{1}\,|\varphi\rangle\langle\varphi|_{x_iu_i,Y_i=\perp,r_i}\,(V^{\mathrm{B}}_{i,u_iy_ir_i})^\dagger\otimes\mathbb{1}-|\varphi\rangle\langle\varphi|_{x_iu_iy_ir_i}\right\|_1\\
&\quad+2\mathop{\mathbb{E}}_{i\in\overline{T}}\left\|\mathsf{P}_{X_iU_iY_iR_i|\mathcal{E}}(\mathsf{P}_{Z_iA_iS_i|\mathcal{E},X_iU_iY_iR_i}-\mathsf{P}_{Z_iA_iS_i|\mathcal{E},X_iU_i,Y_i=\perp,R_i})\right\|_1\\
\leq&O\left(\frac{\sqrt{\delta}}{\alpha}\right),
\end{aligned} \tag{41}$$

where to bound the second term of the second line, we have used (31).

Repeating the same steps as above on Charlie's side and using (32) this time, we get that there exist unitaries $V^{\mathrm{C}}_{i,u_iz_ir_i}$ acting on $Z_{\overline{T}}\widetilde{Z}_{\overline{T}}\widetilde{U}_{\overline{T}}\widetilde{S}_{\overline{T}}CE^{\mathrm{C}}$ such that

$$\mathop{\mathbb{E}}_{i\in\overline{T}}\mathop{\mathbb{E}}_{\mathsf{P}_{X_iU_iY_iZ_iA_iS_iR_i|\mathcal{E}}}\left\|\mathbb{1}\otimes V^{\mathrm{C}}_{i,u_iz_ir_i}\,|\varphi\rangle\langle\varphi|_{x_iu_iy_i,Z_i=\perp,a_is_ir_i}\,\mathbb{1}\otimes(V^{\mathrm{C}}_{i,u_iz_ir_i})^\dagger-|\varphi\rangle\langle\varphi|_{x_iu_iy_iz_ia_is_ir_i}\right\|_1\leq O\left(\frac{\sqrt{\delta}}{\alpha}\right).$$

We can use (24) again to shift the expectation in the above expression from $\mathsf{P}_{X_iU_iY_iZ_iR_i|\mathcal{E}}$ to $\mathsf{P}_{Y_i}\mathsf{P}_{X_iU_iZ_iR_i|\mathcal{E},Y_i}$, with only a $\sqrt{2\delta}$ loss. We can then condition on $Y_i=\perp$ (which happens with probability α under P_{Y_i}) to get,

$$\begin{aligned}
&\mathop{\mathbb{E}}_{i\in\overline{T}}\mathop{\mathbb{E}}_{\mathsf{P}_{X_iU_iZ_iA_iS_iR_i|\mathcal{E},Y_i=\perp}}\left\|\mathbb{1}\otimes V^{\mathrm{C}}_{i,u_iz_ir_i}\,|\varphi\rangle\langle\varphi|_{x_iu_i,\perp\perp,a_is_ir_i}\,\mathbb{1}\otimes(V^{\mathrm{C}}_{i,u_iz_ir_i})^\dagger-|\varphi\rangle\langle\varphi|_{x_iu_i,Y_i=\perp,z_ia_is_ir_i}\right\|_1\\
\leq&O\left(\frac{\sqrt{\delta}}{\alpha^2}\right).
\end{aligned} \tag{42}$$

Now, tracing out the Y_i register from (31) we get,

$$\mathop{\mathbb{E}}_{i\in\overline{T}}\left\|\mathsf{P}_{X_iU_iR_i|\mathcal{E}}(\mathsf{P}_{Z_iA_iS_i|\mathcal{E},X_iU_iR_i}-\mathsf{P}_{Z_iA_iS_i|\mathcal{E},X_iU_i,Y_i=\perp,R_i})\right\|_1\leq O\left(\frac{\sqrt{\delta}}{\alpha}\right),$$

and moreover, as we have seen before, we can use Fact 34 to bound $\mathbb{E}_{i\in\overline{T}} \left\| \mathsf{P}_{X_iU_iR_i|\mathcal{E}} - \mathsf{P}_{X_iU_iR_i|\mathcal{E},Y_i=\perp} \right\|_1$. Therefore,

$$\begin{aligned}\mathop{\mathbb{E}}_{i\in\overline{T}} \left\| \mathsf{P}_{X_iU_iZ_iA_iS_iR_i|\mathcal{E},Y_i=\perp} - \mathsf{P}_{X_iU_iZ_iA_iS_iR_i|\mathcal{E}} \right\|_1 &\leq \mathop{\mathbb{E}}_{i\in\overline{T}} \left\| (\mathsf{P}_{X_iU_iR_i|\mathcal{E}} - \mathsf{P}_{X_iU_iR_i|\mathcal{E},Y_i=\perp}) \mathsf{P}_{Z_iA_iS_i|\mathcal{E},X_iU_i,Y_i=\perp,R_i} \right\|_1 \\ &\quad + \mathop{\mathbb{E}}_{i\in\overline{T}} \left\| \mathsf{P}_{X_iU_iR_i|\mathcal{E}} (\mathsf{P}_{Z_iA_iS_i|\mathcal{E},X_iU_iR_i} - \mathsf{P}_{Z_iA_iS_i|\mathcal{E},X_iU_i,Y_i=\perp,R_i}) \right\|_1 \\ &\leq O\left(\frac{\sqrt{\delta}}{\alpha}\right).\end{aligned}$$

Using this along with (42) we get,

$$\begin{aligned}&\mathop{\mathbb{E}}_{i\in\overline{T}} \mathop{\mathbb{E}}_{\mathsf{P}_{X_iU_iZ_iA_iS_iR_i|\mathcal{E}}} \left\| \mathbb{1} \otimes V^{\mathrm{C}}_{i,u_iz_ir_i} |\varphi\rangle\langle\varphi|_{x_iu_i,\perp\perp,a_is_ir_i} \mathbb{1} \otimes (V^{\mathrm{C}}_{i,u_iz_ir_i})^\dagger - |\varphi\rangle\langle\varphi|_{x_iu_i,Y_i=\perp,z_ia_is_ir_i} \right\|_1 \\ \leq & O\left(\frac{\sqrt{\delta}}{\alpha^2}\right). \end{aligned} \tag{43}$$

Finally, combining (41) and (43) we get,

$$\begin{aligned}&\mathop{\mathbb{E}}_{i\in\overline{T}} \mathop{\mathbb{E}}_{\mathsf{P}_{X_iU_iY_iZ_iA_iS_iR_i|\mathcal{E}}} \left\| V^{\mathrm{B}}_{i,u_iy_ir_i} \otimes V^{\mathrm{C}}_{i,u_iz_ir_i} |\varphi\rangle\langle\varphi|_{x_iu_i,\perp\perp,a_is_ir_i} (V^{\mathrm{B}}_{i,u_iy_ir_i})^\dagger \otimes (V^{\mathrm{C}}_{i,u_iz_ir_i})^\dagger - |\varphi\rangle\langle\varphi|_{x_iu_iy_iz_ia_is_ir_i} \right\|_1 \\ \leq & \mathop{\mathbb{E}}_{i\in\overline{T}} \mathop{\mathbb{E}}_{\mathsf{P}_{X_iU_iZ_iA_iS_iR_i|\mathcal{E}}} \left\| V^{\mathrm{B}}_{i,u_iy_ir_i} \left(\mathbb{1} \otimes V^{\mathrm{C}}_{i,u_iz_ir_i} |\varphi\rangle\langle\varphi|_{x_iu_i,\perp\perp,a_is_ir_i} \mathbb{1} \otimes (V^{\mathrm{C}}_{i,u_iz_ir_i})^\dagger - |\varphi\rangle\langle\varphi|_{x_iu_i,Y_i=\perp,z_ia_is_ir_i} \right) V^{\mathrm{B}}_{i,u_iy_ir_i} \right\|_1 \\ &+ \mathop{\mathbb{E}}_{i\in\overline{T}} \mathop{\mathbb{E}}_{\mathsf{P}_{X_iU_iY_iZ_iA_iS_iR_i|\mathcal{E}}} \left\| V^{\mathrm{B}}_{i,u_iy_ir_i} \otimes \mathbb{1} |\varphi\rangle\langle\varphi|_{x_iu_i,Y_i=\perp,z_ia_is_ir_i} (V^{\mathrm{B}}_{i,u_iy_ir_i})^\dagger \otimes \mathbb{1} - |\varphi\rangle\langle\varphi|_{x_iu_iy_iz_ia_is_ir_i} \right\|_1 \\ \leq & O\left(\frac{\sqrt{\delta}}{\alpha^2}\right).\end{aligned}$$

This completes the proof of item (iv) of the lemma.

Acknowledgements

We thank Eric Culf, Mads Friis Frand-Madsen, Rahul Jain, Sébastien Lord, and Joseph Renes for helpful discussions. We also thank a reviewer for pointing out the issue described in Remark 4 regarding previous security definitions. S. K. is funded by the Natural Sciences and Engineering Research Council of Canada (NSERC) Discovery Grants Program and Fujitsu Labs America. E. Y.-Z. T. is funded by NSERC Alliance and Huawei Technologies Canada Co., Ltd. Research at the Institute for Quantum Computing (IQC) is supported by Innovation, Science and Economic Development (ISED) Canada.

References

[AC02] Mark Adcock and Richard Cleve. A Quantum Goldreich-Levin Theorem with Cryptographic Applications. In *STACS 2002*, pages 323–334, 2002.

[ACK+14] Nati Aharon, André Chailloux, Iordanis Kerenidis, Serge Massar, Stefano Pironio, and Jonathan Silman. Weak coin flipping in a device-independent setting. In *Theory of Quantum Computation, Communication, and Cryptography*, pages 1–12, 2014.

[AGM06] Antonio Acín, Nicolas Gisin, and Lluis Masanes. From Bell's Theorem to Secure Quantum Key Distribution. *Physical Review Letters*, 97:120405, 2006.

[AK21] Prabhanjan Ananth and Fatih Kaleoglu. Unclonable Encryption, Revisited. In *Theory of Cryptography: 19th International Conference, TCC 2021, Raleigh, NC, USA, November 8–11, 2021, Proceedings, Part I*, page 299–329, Berlin, Heidelberg, 2021. Springer-Verlag.

[AKL+22] Prabhanjan Ananth, Fatih Kaleoglu, Xingjian Li, Qipeng Liu, and Mark Zhandry. On the Feasibility of Unclonable Encryption, and More. In *Advances in Cryptology – CRYPTO 2022*, page 212–241. Springer Nature Switzerland, 2022.

[AKL23] Prabhanjan Ananth, Fatih Kaleoglu, and Qipeng Liu. Cloning Games: A General Framework For Unclonable Primitives. In *Proceedings of Advances in Cryptology – CRYPTO 2023: 43rd Annual International Cryptology Conference (CRYPTO 2023)*, page 66–98, 2023.

[Ari10] Erdal Arikan. Source polarization. In *2010 IEEE International Symposium on Information Theory*, pages 899–903, 2010.

[BC23] Anne Broadbent and Eric Culf. Rigidity for Monogamy-Of-Entanglement Games. In *14th Innovations in Theoretical Computer Science Conference (ITCS 2023)*, volume 251 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 28:1–28:29, Dagstuhl, Germany, 2023. Schloss Dagstuhl – Leibniz-Zentrum für Informatik.

[BHK05] Jonathan Barrett, Lucien Hardy, and Adrian Kent. No Signaling and Quantum Key Distribution. *Physical Review Letters*, 95:010503, 2005.

[BJL+21] Anne Broadbent, Stacey Jeffery, Sébastien Lord, Supartha Podder, and Aarthi Sundaram. Secure Software Leasing Without Assumptions. In Kobbi Nissim and Brent Waters, editors, *Theory of Cryptography*, pages 90–120, Cham, 2021.

[BL20] Anne Broadbent and Sébastien Lord. Uncloneable Quantum Encryption via Oracles. In *15th Conference on the Theory of Quantum Computation, Communication and Cryptography (TQC 2020)*, pages 4:1–4:22, 2020.

[BNS+15] Jean-Daniel Bancal, Miguel Navascués, Valerio Scarani, Tamás Vértesi, and Tzyh Haur Yang. Physical characterization of quantum devices from nonlocal correlations. *Physical Review A*, 91:022115, 2015.

[BVY17] Mohammad Bavarian, Thomas Vidick, and Henry Yuen. Hardness Amplification for Entangled Games via Anchoring. In *Proceedings of the 49th Annual ACM SIGACT Symposium on Theory of Computing*, STOC '17, page 303–316, 2017.

[CLLZ21] Andrea Coladangelo, Jiahui Liu, Qipeng Liu, and Mark Zhandry. Hidden Cosets and Applications to Unclonable Cryptography. In *Advances in Cryptology – CRYPTO 2021*, pages 556–584. Springer International Publishing, 2021.

[CMP24] Andrea Coladangelo, Christian Majenz, and Alexander Poremba. Quantum copy-protection of compute-and-compare programs in the quantum random oracle model. *Quantum*, 8:1330, 2024.

[DPVR12] Anindya De, Christopher Portmann, Thomas Vidick, and Renato Renner. Trevisan's Extractor in the Presence of Quantum Side Information. *SIAM Journal on Computing*, 41(4):915–940, 2012.

[FM18] Honghao Fu and Carl A. Miller. Local randomness: Examples and application. *Physical Review A*, 97:032324, 2018.

[GMP23] Alexandru Gheorghiu, Tony Metger, and Alexander Poremba. Quantum Cryptography with Classical Communication: Parallel Remote State Preparation for Copy-Protection, Verification, and More. In *50th International Colloquium on Automata, Languages, and Programming (ICALP 2023)*, volume 261 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 67:1–67:17, Dagstuhl, Germany, 2023. Schloss Dagstuhl – Leibniz-Zentrum für Informatik.

[Got03] Daniel Gottesman. Uncloneable Encryption. *Quantum Information and Computation*, 3(6):581–602, 2003.

[GZ20] Marios Georgiou and Mark Zhandry. Unclonable Decryption Keys. IACR Cryptology ePrint, 2020.

[Hol07] Thomas Holenstein. Parallel Repetition: Simplifications and the No-Signaling Case. In *Proceedings of the Thirty-Ninth Annual ACM Symposium on Theory of Computing*, STOC '07, page 411–419, 2007.

[HS20] Karol Horodecki and Maciej Stankiewicz. Semi-device-independent quantum money. *New Journal of Physics*, 22(2):023007, 2020.

[JK22] R. Jain and S. Kundu. A direct product theorem for quantum communication complexity with applications to device-independent QKD. In *2021 IEEE 62nd Annual Symposium on Foundations of Computer Science (FOCS)*, pages 1285–1295, 2022.

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

[KST22] Srijita Kundu, Jamie Sikora, and Ernest Y.-Z. Tan. A device-independent protocol for XOR oblivious transfer. *Quantum*, 6:725, 2022.

[KT23] Srijita Kundu and Ernest Y.-Z. Tan. Composably secure device-independent encryption with certified deletion. *Quantum*, 7:1047, 2023.

[LLQZ22] Jiahui Liu, Qipeng Liu, Luowen Qian, and Mark Zhandry. Collusion Resistant Copy-Protection for Watermarkable Functionalities. In Eike Kiltz and Vinod Vaikuntanathan, editors, *Theory of Cryptography*, pages 294–323, Cham, 2022. Springer Nature Switzerland.

[LLR12] Sophie Laplante, Virginie Lerays, and Jérémie Roland. Classical and Quantum Partition Bound and Detector Inefficiency. In *Automata, Languages, and Programming*, pages 617–628, Berlin, Heidelberg, 2012.

[MAG06] Ll. Masanes, A. Acin, and N. Gisin. General properties of nonsignaling theories. *Physical Review A*, 73:012112, 2006.

[MPW22] Michele Masini, Stefano Pironio, and Erik Woodhead. Simple and practical DIQKD security analysis via BB84-type uncertainty relations and Pauli correlation constraints. *Quantum*, 6:843, October 2022.

[MST21] Christian Majenz, Christian Schaffner, and Mehrdad Tahmasbi. Limitations on Uncloneable Encryption and Simultaneous One-Way-to-Hiding. arXiv:2103.14510v3, 2021.

[MYS12] Matthew McKague, Tzyh Haur Yang, and Valerio Scarani. Robust self-testing of the singlet. *Journal of Physics A: Mathematical and Theoretical*, 45(45):455304, 2012.

[PAB+09] Stefano Pironio, Antonio Acín, Nicolas Brunner, Nicolas Gisin, Serge Massar, and Valerio Scarani. Device-independent quantum key distribution secure against collective attacks. *New Journal of Physics*, 11(4):045021, 2009.

[PR14] Christopher Portmann and Renato Renner. Cryptographic security of quantum key distribution. arXiv:1409.3525v1, 2014.

[Raz95] Ran Raz. A Parallel Repetition Theorem. In *Proceedings of the Twenty-Seventh Annual ACM Symposium on Theory of Computing*, page 447–456, 1995.

[Ren05] Renato Renner. Security of Quantum Key Distribution. arXiv:0512258v2, 2005.

[Tan21] Ernest Y.-Z. Tan. Prospects for device-independent quantum key distribution. arXiv:2111.11769v1, 2021.

[TFKW13] Marco Tomamichel, Serge Fehr, Jędrzej Kaniewski, and Stephanie Wehner. A monogamy-of-entanglement game with applications to device-independent quantum cryptography. *New Journal of Physics*, 15(10):103002, 2013.

[TMPE17] Marco Tomamichel, Jesus Martinez-Mateo, Christoph Pacher, and David Elkouss. Fundamental finite key limits for one-way information reconciliation in quantum key distribution. *Quantum Information Processing*, 16(11), 2017.

[TSSR11] Marco Tomamichel, Christian Schaffner, Adam Smith, and Renato Renner. Leftover Hashing Against Quantum Side Information. *IEEE Transactions on Information Theory*, 57(8):5524–5535, 2011.

[Vid17] Thomas Vidick. Parallel DIQKD from parallel repetition. arXiv:1703.08508v1, 2017.

[Wie83] Stephen Wiesner. Conjugate Coding. *SIGACT News*, 15(1):78–88, 1983.

[WMP14] E. Woodhead, S. Massar, and S. Pironio. Imperfections and self testing in prepare-and-measure quantum key distribution, 2014.