A Quantum-Proof Non-Malleable Extractor

With Application to Privacy Amplification against Active Quantum Adversaries

Divesh Aggarwal[1]*, Kai-Min Chung[2]**, Han-Hsuan Lin[3]***, and Thomas Vidick[4]†

[1] Center of Quantum Technologies, and Department of Computer Science, NUS, Singapore.
email: dcsdiva@nus.edu.sg.
[2] Institute of Information Science, Academia Sinica, Taipei 11529, Taiwan.
email: kmchung@iis.sinica.edu.tw.
[3] Department of Computer Science, The University of Texas at Austin, Austin, USA.
email: linhh@cs.utexas.edu
[4] Department of Computing and Mathematical Sciences, California Institute of Technology, Pasadena, USA.
email: vidick@cms.caltech.edu.

Abstract. In privacy amplification, two mutually trusted parties aim to amplify the secrecy of an initial shared secret X in order to establish a shared private key K by exchanging messages over an insecure communication channel. If the channel is authenticated the task can be solved in a single round of communication using a strong randomness extractor; choosing a quantum-proof extractor allows one to establish security against quantum adversaries.

In the case that the channel is not authenticated, this simple solution is no longer secure. Nevertheless, Dodis and Wichs (STOC'09) showed that the problem can be solved in two rounds of communication using a non-malleable extractor, a stronger pseudo-random construction than a strong extractor.

We give the first construction of a non-malleable extractor that is secure against quantum adversaries. The extractor is based on a construction by Li (FOCS'12), and is able to extract from source of min-entropy rates larger than $1/2$. Combining this construction with a quantum-proof variant of the reduction of Dodis and Wichs, due to Cohen and Vidick (unpublished) we obtain the first privacy amplification protocol secure against active quantum adversaries.

* This research was further partially funded by the Singapore Ministry of Education and the National Research Foundation under grantR-710-000-012-135.

** This research is partially supported by the 2016 Academia Sinica Career Development Award under Grant no. 23-17. This research is partially supported by MOST QC project, under Grant no. MOST 107-2627-E-002-002 -

*** This material is based on work supported by the Singapore National Research Foundation under NRF RF Award No. NRF-NRFF2013-13.

† Supported by NSF CAREER Grant CCF-1553477, AFOSR YIP award number FA9550-16-1-0495, and the IQIM, an NSF Physics Frontiers Center (NSF Grant PHY-1125565) with support of the Gordon and Betty Moore Foundation (GBMF-12500028).

1 Introduction

Privacy amplification. We study the problem of *privacy amplification* [5, 30, 4, 31] (PA). In this problem, two parties, Alice and Bob, share a weak secret X (a random variable with min-entropy at least k). Using X and an insecure communication channel, Alice and Bob would like to securely agree on a secret key R that is ϵ-close to uniformly random even to an adversary Eve who may have full control over their communication channel. This elegant problem has multiple applications including biometric authentication, leakage-resilient cryptography, and quantum cryptography.

If the adversary Eve is passive, i.e., she is only able to observe the communication but may not alter the messages exchanged, then there is a direct solution based on the use of a strong seeded randomness extractor Ext [33]. This can be done by Alice selecting a uniform seed Y for the extractor, and sending the seed to Bob; Alice and Bob both compute the key $R = \mathrm{Ext}(X, Y)$, which is close to being uniformly random and independent of Y by the strong extractor property. The use of a quantum-proof extractor suffices to protect against adversaries holding quantum side information about the secret X.

Privacy amplification is substantially more challenging when the adversary is active, i.e. Eve can not only read but also modify messages exchanged across the communication channel. This problem has been studied extensively in several works including [31, 35, 16, 19, 8, 17, 13, 27, 25, 26, 20, 2, 28, 9, 12, 3, 29], yielding constructions that are optimal or near-optimal in any of the parameters involved in the problem, including the min-entropy k, the error ϵ, and the communication complexity of the protocol.

Active adversaries with quantum side information. We consider the problem of active attacks by quantum adversaries. This question arises naturally when privacy amplification is used as a sub-protocol, e.g., as a post-processing step in quantum key distribution (QKD), when it may not be safe to assume that the classical communication channel is authenticated.[5] To the best of our knowledge the question was first raised in [7], whose primary focus is privacy amplification with an additional property of source privacy. Although the authors of [7] initially claimed that their construction is secure against quantum side information, they later realized that there was an issue with their argument, and withdrew their claim of quantum security. The only other work we are aware of approaching the question of privacy amplification in the presence of active quantum adversaries is [14]. In this paper it is shown that a classical protocol for PA introduced by Dodis and Wichs [19] remains secure against active quantum attacks when the main tool used in the protocol, a non-malleable extractor, is secure against quantum side information (a notion that is also formally introduced in that paper, and to which we return shortly). Unfortunately, the final contribution of [14], a construction of a quantum-proof non-malleable extractor, also had a flaw in the proof, invalidating the construction. Thus, the problem of quantum-secure active privacy amplification remained open.

[5] QKD relies on an authenticated channel at other stages of the protocol, and here we only address the privacy amplification part: indeed, PA plays an important role in multiple other cryptographic protocols, and it is a fundamental task that it is useful to address first.

It may be useful to discuss the difficulty faced by both these previous works, as it informed our own construction. The issue is related to the modeling of the side information held by the adversary Eve, and how that side information evolves as messages are being exchanged, and possibly modified, throughout the privacy amplification protocol. To explain this, consider the setting for a non-malleable extractor, whose security property can be defined without referring to the way the extractor is used for privacy amplification. Here, Alice initially has a secret X (the source), while Eve holds side information E, a quantum state, correlated with X. Alice selects a uniformly random seed Y and computes $\mathrm{Ext}(X, Y)$. However, in addition to receiving Y (as would already be the case for a strong randomness extractor), Eve is also given the possibility to select an arbitrary $Y' \neq Y$ and receive $\mathrm{Ext}(X, Y')$ as "advice" to help her break the extractor — i.e., distinguish $\mathrm{Ext}(X, Y)$ from uniform. Now, clearly in any practical scenario the adversary may use her side information E in order to guide her choice of Y'; thus Y' should be considered as the outcome of a measurement $\{M_y^{y'}\}$, depending on $Y = y$ and performed on E, which returns an outcome $Y' = y'$ and a post-measurement state E'. This means that the security of the extractor should be considered with respect to the side information E'. But due to the measurement, E' may be correlated with both X and Y in a way that cannot be addressed by standard techniques for the analysis of strong extractors. Indeed, even if E' is classical, so that we can condition on its value, X and Y may not be independent after conditioning on $E' = e'$; due to the lack of independence it is unclear whether extraction works. (Classical proofs condition on $E = e$ at the outset, which does preserve independence.)

The issue seems particularly difficult to accommodate when analyzing extractors based on the technique of "alternate extraction", as was attempted in [7, 14]. In fact, in the original version of [7] the issue is overlooked, resulting in a flawed security proof. In [14] the authors attempted to deal with the difficulty by using the formalism of quantum Markov chains; unfortunately, there is a gap in the argument and it does not seem like the scenario can be modeled using the Markov chain formalism. Note that in the classical setting the issue does not arise: having fixed $E = e$ we can consider Y' to be a fixed, deterministic function of Y — there is no E' to consider, and X is independent of both Y and Y' conditioned on $E = e$. In this paper we do not address the issue, but instead focus on a specific construction of non-malleable extractor whose security can be shown by algebraic techniques sidestepping the difficulty; we explain our approach in more detail below.

Our results. We show that a non-malleable extractor introduced by Li [27] in the classical setting is secure against quantum side information. Combining this construction with the protocol of Dodis and Wichs and its proof of security from [14], we obtain the first protocol for privacy amplification that is secure against active quantum adversaries.

Before describing our results in more detail we summarize Li's construction and its analysis for the case of classical side information. The construction is based on the inner product function. Let p be a prime, $\mathbb{F}_p$ the finite field with p elements, and $\langle \cdot, \cdot \rangle$ the inner product over $\mathbb{F}_p$. Consider the function $\mathrm{Ext} : \mathbb{F}_p^n \times \mathbb{F}_p^n \to \mathbb{F}_p$ given by $\mathrm{Ext}(X, Y) := \langle X, Y \rangle$, where $X \in \mathbb{F}_p^n$ is a weak secret with min-entropy (conditioned on the adversary's side information) assumed to be greater than $(n \log p)/2$, and Y is a uniformly random and independent seed. For this function to be a non-malleable extractor, it is required that $\mathrm{Ext}(X,Y)$ is close to uniform and independent of $\mathrm{Ext}(X, f(Y))$, where f is any adversarially chosen function such that $f(Y) \neq Y$ for all Y. This is clearly not true, since if $f(Y) = cY$ for some $c \in \mathbb{F}_p \setminus \{1\}$, then $\mathrm{Ext}(X, f(Y)) = c\mathrm{Ext}(X,Y)$, and hence we don't get the desired independence. Thus, for such a construction to work, it is necessary to encode the source Y as $\mathsf{Enc}(Y)$, for a well-chosen function Enc, in such a way that $\langle X, \mathsf{Enc}(Y)\rangle - c \cdot \langle X, \mathsf{Enc}(f(Y))\rangle$ is hard to guess. The non-uniform XOR lemma [17, 13, 3] shows that it is sufficient to show that $\langle X, \mathsf{Enc}(Y)\rangle - c \cdot \langle X, \mathsf{Enc}(f(Y))\rangle = \langle X, \mathsf{Enc}(Y) - c \cdot \mathsf{Enc}(f(Y))\rangle$ is close to uniform conditioned on Y and E. The encoding that we use in this paper (which is almost the same as the encoding chosen by Li) is to take $Y \in \mathbb{F}_p^{n/2}$, and encode it as $Y \| Y^2$, which we view as an n-character string over $\mathbb{F}_p$, with the symbol $\|$ denoting concatenation of strings and the square taken by first interpreting Y as an element of $\mathbb{F}_{p^{n/2}}$. Then it is not difficult to show that for any function f such that $f(Y) \neq Y$ and any c, we have that $(Y\|Y^2) - (c \cdot f(Y) \| c \cdot f(Y)^2)$ (taking the addition coordinatewise) has min-entropy almost $(n \log p)/2$. Thus, provided X has sufficiently high min-entropy and using the fact that X and $(Y\|Y^2) - (c \cdot f(Y) \| c \cdot f(Y)^2)$ are independent conditioned on E, the strong extractor property of the inner product function gives the desired result.[6]

Our main technical result is a proof of security of Li's extractor, against quantum side information. We show the following (we refer to Definition 5 for the formal definition of a quantum-proof non-malleable extractor):

Theorem 1. *Let $p \neq 2$ be a prime. Let n be an even integer. Then for any $\epsilon > 0$ the function $\mathrm{nmExt}(X,Y) : \mathbb{F}_p^n \times \mathbb{F}_p^{n/2} \to \mathbb{F}_p$ given by $\langle X, Y\|Y^2\rangle$ is an $\left(\left(\frac{n}{2}+6\right)\log p - 1 + 4\log\frac{1}{\epsilon}, \epsilon\right)$ quantum-proof non-malleable extractor.*

We give the main ideas behind our proof of security for this construction, highlighting the points of departure from the classical analysis. Subsequently, we explain the application to privacy amplification.

Proof ideas. We begin by generalizing the first step of Li's argument, the reduction provided by the non-uniform XOR lemma, to the quantum case. An XOR lemma with quantum side information is already shown in [22], where the lemma is used to show security of the inner product function as a two-source extractor against quantum side information. This version is not sufficient for our purposes, and we establish the following generalization, which may be of independent interest (we refer to Section 3 for relevant definitions):

Lemma 1. *Let p be a prime power and t an integer. Let ρ_{X_0XE} be a ccq state with $X_0 \in \mathbb{F}_p$ and $X = (X_1, \ldots, X_t) \in \mathbb{F}_p^t$. For all $a = (a_1, \ldots, a_t) \in \mathbb{F}_p^t$, define a random variable $Z = X_0 + \langle a, X\rangle = X_0 + \sum_{i=1}^t a_i X_i$. Let $\epsilon \geq 0$ be such that for all*

[6] This description is a little different from Li's description since he was working with a field of size 2^n, but we find it more convenient to work with a prime field.

a, $\frac{1}{2}\left\|\rho^a_{ZE} - U_Z \otimes \rho_E\right\|_1 \leq \epsilon$. Then

$$\frac{1}{2}\left\|\rho_{X_0XE} - U_{X_0} \otimes \rho_{XE}\right\|_1 \leq p^{\frac{t+1}{2}}\sqrt{\frac{\epsilon}{2}}\,. \tag{1.1}$$

XOR lemmas are typically proved via Fourier-based techniques (including the one in [22]). Here we instead rely on a collision probability-based argument inspired from [3]. We prove Lemma 1 by observing that such arguments generalize to the quantum setting, as in the proof of the quantum leftover hash lemma in [36].

Based on the XOR lemma (used with $t = 1$), following Li's arguments it remains to show that the random variable $\langle X, g(Y,Y')\rangle \in \mathbb{F}_p$, where $g(Y,Y') = Y\|Y^2 - c(Y'\|Y'^2) \in \mathbb{F}_p^n$, is close to uniformly distributed from the adversary's point of view, specified by side information E', for every $c \neq 0 \in \mathbb{F}_p$. As already mentioned earlier, this cannot be shown by a reduction to the security proof of the inner product function as a two-source extractor against side information, as X and $g(Y,Y')$ are *not* independent (not even conditioned on the value of E' when E' is classical).

Instead, we are led to a more direct analysis which proceeds by formulating the problem as a communication task.[7] We relate the task of breaking our construction — distinguishing $\langle X, g(Y,Y')\rangle$ from uniform — to success in the following task. Alice is given access to a random variable X, and Bob is given a uniformly random Y. Alice is allowed to send a quantum message E, correlated with X, to Bob. Bob then selects a $Y' \neq Y$ and returns a value $b \in \mathbb{F}_p$. The players win if $b = \langle X, g(Y,Y')\rangle$. Based on our previous reductions it suffices to show that no strategy can succeed with probability substantially higher than random in this game, unless Alice's initial message to Bob contains a large amount of information about X; more precisely, unless the min-entropy of X, conditioned on E, is less than half the length of X.

Note that the problem as we formulated it does not fall in standard frameworks for communication complexity. In particular, it is a relation problem, as Bob is allowed to choose the value Y' to which his prediction b applies. This seems to prevent us from using any prior results on the communication complexity of the inner product function, and we develop an ad-hoc proof which may be of independent interest. We approach the problem using the "reconstruction paradigm" (used in e.g. [15]), which amounts to showing that from any successful strategy of the players one may construct a measurement for Bob which completely "reconstructs" X, given E; if this can be achieved with high enough probability it will contradict the min-entropy assumption on X, via its dual formulation as a guessing probability [23]. We show this by running Bob's strategy "in superposition", and applying a Fourier transform to recover a guess for X. This argument is similar to one introduced in [11, 32]. We refer to Section 4.1 for more detail.

Application to privacy amplification. Finally we discuss the application of our quantum-proof non-malleable extractor to the problem of privacy amplification against active quantum attacks, which is our original motivation. The application is based

[7] The correspondence between security of quantum-proof strong extractors and communication problems has been used repeatedly before, see e.g. [21, 22].

on a breakthrough result by Dodis and Wichs [19], who were first to show the existence of a two-round PA protocol with optimal (up to constant factors) entropy loss $L = \Theta(\log(1/\epsilon))$, for any initial min-entropy k. This was achieved by defining and showing the existence of non-malleable extractors with very good parameters.

The protocol from [19] is recalled in Section 5. The protocol proceeds as follows. Alice sends a uniformly random seed Y to Bob over the communication channel, which is controlled by Eve. Bob receives a possibly modified seed Y'. Then Alice computes a key $K = \mathrm{nmExt}(X, Y)$, and Bob computes $K' = \mathrm{nmExt}(X, Y')$. In the second round, Bob generates another uniformly random seed W', and sends W' together with $T' = \mathrm{MAC}_{K'}(W')$ to Alice, where MAC is a one-time message authentication code. Alice receives a possibly modified T, W and checks whether $T = \mathrm{MAC}_K(W)$. If yes, then the shared secret between Alice and Bob is $\mathrm{Ext}(X, W) = \mathrm{Ext}(X, W')$ with overwhelming probability, where Ext is any strong seeded extractor.

The security of this protocol intuitively follows from the following simple observation. If the adversary does not modify Y, then $K' = K$, and so W' must be equal to W by the security of the MAC. If $Y' \neq Y$, then by the non-malleability property of nmExt, K is uniform and independent of K', and so it is impossible for the adversary to predict $\mathrm{MAC}_K(W)$ for any W even given K' and W'.

Since [19] could not construct an explicit non-malleable extractor, they instead defined and constructed a so called a look-ahead extractor, which can be seen as a weakening of the non-malleability requirement of a non-malleable extractor. This was done by using the alternating extraction protocol by Dziembowski and Pietrzak [18].

In [14], Dodis and Wichs' reduction is extended to the case of quantum side information, provided that the non-malleable Extractor nmExt used in the protocol satisfies the approriate definition of quantum non-malleability, and Ext is a strong quantum-proof extractor. Based on our construction of a quantum-proof non-malleable extractor (Theorem 1) we immediately obtain a PA protocol that is secure as long as the initial secret X has a min-entropy rate of (slightly more than) half. The result is formalized as Corollary 1 in Section 5.

In Section 5.2 we additionally prove security of a one-round protocol due to Dodis et al. [16] against active quantum attacks. The protocol has the advantage of being single-round, but it induces a significantly higher entropy loss, $(n/2) + \log(1/\epsilon)$, than the Dodis-Wichs protocol, for which the loss is independent of n.

Future work. There have been a series of works in the classical setting [17, 13, 27, 25, 20, 28, 9, 12, 3, 29] that have given privacy amplification protocols (via constructing non-malleable extractors or otherwise) that achieve near-optimal parameters. In particular, Li [29] constructed a non-malleable extractor that works for min-entropy $k = \Omega(\log n + \log(1/\epsilon) \log\log(1/\epsilon))$, where ϵ is the error probability.

Our quantum-proof non-malleable extractor requires the min-entropy rate of the initial weak secret to be larger than $1/2$. We leave it as an open question whether one of the above-mentioned protocols that work for min-entropy rate smaller than $1/2$ in the classical setting can be shown secure against quantum side information.

2 Preliminaries

2.1 Notation

For p a prime power we let $\mathbb{F}_p$ denote the finite field with p elements. For any positive integer n, there is a natural bijection $\phi : \mathbb{F}_p^n \mapsto \mathbb{F}_{p^n}$ that preserves group addition and scalar multiplication, i.e., the following hold:

- For all $c \in \mathbb{F}_p$, and for all $x \in \mathbb{F}_p^n$, $\phi(c \cdot x) = c \cdot \phi(x)$.
- For all $x_1, x_2 \in \mathbb{F}_p^n$, $\phi(x_1) + \phi(x_2) = \phi(x_1 + x_2)$.

We use this bijection to define the square of an element in $\mathbb{F}_p^n$, e.g. for $y \in \mathbb{F}_p^n$

$$y^2 = \phi^{-1}\left((\phi(y))^2\right) . \tag{2.1}$$

We write $\langle \cdot, \cdot \rangle$ for the inner product over $\mathbb{F}_p^n$. log denotes the logarithm with base 2.

We write $\mathcal{H}$ for an arbitrary finite-dimensional Hilbert space, $\mathrm{L}(\mathcal{H})$ for the linear operators on $\mathcal{H}$, $\mathrm{Pos}(\mathcal{H})$ for positive semidefinite operators, and $\mathrm{D}(\mathcal{H}) \subset \mathrm{Pos}(\mathcal{H})$ for positive semidefinite operators of trace 1 (*density matrices*). A linear map $T : \mathrm{L}(\mathcal{H}) \to \mathrm{L}(\mathcal{H}')$ is CPTP if it is completely positive, i.e. $T \otimes \mathrm{Id}(A) \geq 0$ for any $d \geq 0$ and $A \in \mathrm{Pos}(\mathcal{H} \otimes \mathbb{C}^d)$, and trace-preserving.

We use capital letters $A, B, E, X, Y, Z, \ldots$ to denote quantum or classical random variables. Generally, the letters near the beginning of the alphabet, such as A, B, E, represent quantum variables (density matrices on a finite-dimensional Hilbert space), while the letters near the end, such as X, Y, Z represent classical variables (ranging over a finite alphabet). We sometimes represent classical random variables as density matrices diagonal in the computational basis, and write e.g. $(A, B, \ldots, E)_\rho$ for the density matrix $\rho_{A,B,\ldots,E}$. For a quantum random variable A, we denote $\mathcal{H}_A$ the Hilbert space on which the associated density matrix ρ_A is supported, and d_A its dimension. If X is classical we loosely identify its range $\{0, \ldots, d_X - 1\}$ with the space $\mathcal{H}_X$ spanned by $\{|0\rangle_X, \ldots, |d_X - 1\rangle_X\}$. We denote I_A the identity operator on $\mathcal{H}_A$. When an identity operator is tensor producted with another matrix, we sometimes omit the identity operator for brevity, e.g. writing $I_A \otimes B$ as B. When a density matrix specifies the states of two random variables, one of which is classical and the other is quantum, we call it a classical-quantum(cq)-state. A cq state $(X, E)_\rho$ takes the form

$$\rho_{XE} = \sum_x |x\rangle\langle x|_X \otimes \rho_E^x ,$$

where the summation is over all x in the range of X and $\{\rho_E^x\}$ are positive semidefinite matrices with $\mathrm{Tr}\,\rho_E^x = p_x$, where p_x is the probability of getting the outcome x when measuring the X register. Similarly, a ccq state $(X, Y, E)_\sigma$ is a density matrix over two classical variables and one quantum variable, e.g. $\sigma_{XYE} = \sum_{x,y} |x\rangle\langle x|_X \otimes |y\rangle\langle y|_Y \otimes \sigma_E^{xy}$. We will sometimes add or remove random variables from an already-specified density matrix. When we omit a random variable, we mean the reduced density matrix, e.g. $(Y, E)_\sigma = \mathrm{Tr}_X(\sigma_{XYE})$. When we introduce a classical variable, we mean that the classical variable is computed into another classical register. For example, for a function $F(\cdot,\cdot)$ on variables X, Y,

$$(F(X,Y),X,Y,E)_\sigma = \sum_{f,x,y} \delta(f,F(x,y))|f\rangle\langle f| \otimes |x\rangle\langle x| \otimes |y\rangle\langle y| \otimes \sigma_E^{xy} \ ,$$

where $\delta(\cdot,\cdot)$ is the Kronecker delta function, and the summation over f is taken over the range of F. When F is a random function, the density matrix is averaged over the appropriate probability distribution.

We use U_Σ to denote the uniform distribution over a set Σ. For m-bit string $\{0,1\}^m$, we abbreviate $U_{\{0,1\}^m}$ as U_m. For a classical random variable X, U_X denote the uniform distribution over the range of X.

For $p \geq 1$ we write $\|\cdot\|_p$ for the Schatten p-norm (this is the p-norm of the vector of singular values). We write $\|\cdot\|$ for the operator norm.

We write $\approx_\epsilon$ to denote that two density matrices are ϵ-close to each other in trace distance. For example, $(X,E)_\rho \approx_\epsilon (U_X,E)_\rho$ means $\frac{1}{2}\left\|\rho_{XE} - U_X \otimes \rho_E\right\|_1 \leq \epsilon$. Note that in case both X and E are classical random variables, this reduces to the statistical distance.

2.2 Quantum information

The min-entropy of a classical random variable X conditioned on quantum side information E is defined as follows.

Definition 1 **(Min-entropy).** *Let $\rho_{XE} \in \mathrm{D}(\mathcal{H}_X \otimes \mathcal{H}_E)$ be a cq state. The* min-entropy *of X conditioned on E is defined as*

$$H_{\min}(X|E)_\rho = \max\{\lambda \geq 0 : \exists \sigma_E \in \mathrm{Pos}(\mathcal{H}_E), \mathrm{Tr}\,(\sigma_E) \leq 1, \text{ s.t. } 2^{-\lambda} I_X \otimes \sigma_E \geq \rho_{XE}\}.$$

When the state ρ with respect to which the entropy is measured is clear from context we simply write $H_{\min}(X|E)$ for $H_{\min}(X|E)_\rho$.

Definition 2 **((n,k)-source).** *A cq state ρ_{XE} is an (n,k)-source if $n = \log d_X$ and $H_{\min}(X|E))_\rho \geq k$.*

Rather than using Definition 1, we will most often rely on an operational expression for the min-entropy stated in the following lemma from [23].

Lemma 2 **(Min-entropy and guessing probability).** *For a cq state $\rho_{XE} \in \mathrm{D}(\mathcal{H}_X \otimes \mathcal{H}_E)$, the guessing probability is defined as the probability to correctly guess X with the optimal strategy to measure E, i.e.*

$$p_{guess}(X|E)_\rho = \sup_{\{M_x\}} \sum_x p_x \, \mathrm{Tr}\left(M_x \rho_E^x\right) \ , \qquad (2.2)$$

where $\{M_x\}$ is a positive operator-valued measure (POVM) on $\mathcal{H}_E$. Then the guessing probability is related to the min-entropy by

$$p_{guess}(X|E)_\rho = 2^{-H_{\min}(X|E)_\rho} \ . \qquad (2.3)$$

2.3 Extractors

We first give the definition of a strong quantum-proof extractor. Recall the notation $(X, E)_\rho \approx_\epsilon (X', E')_\rho$ for $\frac{1}{2}\|\rho_{XE} - \rho_{X'E'}\|_1 \leq \epsilon$, and U_m for a random variable uniformly distributed over m-bit strings.

Definition 3. *Let k be an integer and $\epsilon \geq 0$. A function* $\mathrm{Ext} : \mathcal{H}_X \times \mathcal{H}_Y \to \mathcal{H}_Z$ *is a strong (k, ϵ) quantum-proof extractor if for all cq states $\rho_{XE} \in \mathrm{D}(\mathcal{H}_X \otimes \mathcal{H}_E)$ with $H_{\min}(X|E) \geq k$, and for a classical uniform $Y \in \mathcal{H}_Y$ independent of ρ_{XE},*

$$(\mathrm{Ext}(X, Y), Y, E)_\rho \approx_\epsilon (U_Z, Y, E)_\rho \,.$$

There are known explicit constructions of strong quantum-proof extractors.

Theorem 2 **([36]).** *For any integers d_X, k and for any $\epsilon > 0$ there exists an explicit strong (k, ϵ) quantum-proof extractor* $\mathrm{Ext}\colon \{0, \ldots, d_X - 1\} \times \{0, \ldots, d_Y - 1\} \to \{0, \ldots, d_Z - 1\}$ *with $\log d_Y = O(\log d_X)$ and $\log d_Z = k - O(\log(1/\epsilon) - O(1)$.*

We use the same definition of non-malleable extractor against quantum side information that was introduced in the work [14]. The definition is a direct generalization of the classical notion of non-malleable extractor introduced in [19]. The first step is to extend the notion that the adversary may query the extractor on any *different* seed Y' than the seed Y actually used to the case where Y' may be generated from Y as well as quantum side information held by the adversary.

Definition 4 **(Map with no fixed points).** *Let $\mathcal{H}_Y$, $\mathcal{H}_E$ and $\mathcal{H}_{E'}$ be finite-dimensional Hilbert spaces. We say that a CPTP map $T : \mathrm{L}(\mathcal{H}_Y \otimes \mathcal{H}_E) \to \mathrm{L}(\mathcal{H}_Y \otimes \mathcal{H}_{E'})$ has* no fixed points *if for all $\rho_E \in \mathrm{D}(\mathcal{H}_E)$ and all computational basis states $|y\rangle \in \mathcal{H}_Y$ it holds that*

$$\langle y|_Y \, \mathrm{Tr}_{\mathcal{H}_{E'}} \big(T\big(|y\rangle\langle y|_Y \otimes \rho_E\big)\big) \, |y\rangle_Y \;=\; 0 \,.$$

The following definition is given in [14]:

Definition 5 **(Non-mallleable extractor).** *Let $\mathcal{H}_X$, $\mathcal{H}_Y$, $\mathcal{H}_Z$ be finite-dimensional Hilbert spaces, of respective dimension d_X, d_Y, and d_Z. Let $k \leq \log d_X$ and $\epsilon > 0$. A function*

$$\mathrm{nmExt} \,:\, \{0, \ldots, d_X - 1\} \times \{0, \ldots, d_Y - 1\} \to \{0, \ldots, d_Z - 1\}$$

is a (k, ϵ) quantum-proof non-malleable extractor if for every cq-state $(X, E)_\rho$ on $\mathcal{H}_X \otimes \mathcal{H}_E$ such that $H_{\min}(X|E)_\rho \geq k$ and any CPTP map $\mathrm{Adv} : \mathrm{L}(\mathcal{H}_Y \otimes \mathcal{H}_E) \to \mathrm{L}(\mathcal{H}_Y \otimes \mathcal{H}_{E'})$ *with no fixed points,*

$$\big\|\sigma_{\mathrm{nmExt}(X,Y)\mathrm{nmExt}(X,Y')YY'E'} - U_Z \otimes \sigma_{\mathrm{nmExt}(X,Y')YY'E'}\big)\big\|_1 \leq \epsilon \,,$$

where

$$\sigma_{YY'XE'} \;=\; \frac{1}{d_Y} \sum_y |y\rangle\langle y|_Y \otimes (I_X \otimes \mathrm{Adv})(|y\rangle\langle y|_Y \otimes \rho_{XE}) \tag{2.4}$$

and $\sigma_{\mathrm{nmExt}(X,Y)\mathrm{nmExt}(X,Y')YY'E'}$ is obtained from $\sigma_{YY'XE'}$ by (classically) computing $\mathrm{nmExt}(X, Y)$ *and* $\mathrm{nmExt}(X, Y')$ *in ancilla registers and tracing out X.*

2.4 Hölder's inequality

We use the following Hölder's inequality for matrices. For a proof, see e.g. [6].

Lemma 3 (Hölder's inequality). *For any $n \times n$ matrices A, B, C with complex entries, and real numbers $r, s, t > 0$ satisfying $\frac{1}{r} + \frac{1}{s} + \frac{1}{t} = 1$,*

$$\|ABC\|_1 \leq \left\||A|^r\right\|_1^{1/r} \left\||B|^s\right\|_1^{1/s} \left\||C|^t\right\|_1^{1/t} . \tag{2.5}$$

3 Quantum XOR lemma

In this section we prove two XOR lemmas with quantum side information. We prove a non-uniform version, Lemma 1, in Section 3.1. In the full version of the paper [1], we also prove a more standard XOR lemma with quantum side indformation for completeness.[8] Since XOR lemmas often play a fundamental role, they might be of independent interest. Our proofs are based on quantum collision probability techniques[9] from [36] to transform a classical collision probability-based proof into one that also allows for quantum side information. The idea of non-uniform XOR lemma is natural in the context of non-malleable extractors, and has been explored in [27, 13, 3]. Our non-uniform XOR lemma generalizes a restricted version of Lemma 3.15 of [27] to $\mathbb{F}_p$ with quantum side information.[10]

The quantum collision probability is defined as follows.

Definition 6 (Quantum collision probability). *Let $\rho_{AB} \in \mathrm{D}(\mathcal{H}_A \otimes \mathcal{H}_B)$ and $\sigma_B \in \mathrm{D}(\mathcal{H}_B)$. The collision probability of ρ_{AB}, conditioned on σ_B, is defined as*

$$\Gamma_c(\rho_{AB}|\sigma_B) \equiv \mathrm{Tr}\left(\rho_{AB}(I_A \otimes \sigma_B^{-1/2})\right)^2 , \tag{3.1}$$

where $\sigma_B \in \mathrm{D}(\mathcal{H}_B)$.

A careful reader might notice that $\Gamma_c \leq 1$ is not generally true, so calling Γ_c collision *probability* seems misleading. We give a general definition which allows arbitrary states ρ_{AB} and σ_B to match the existing literature, but here we always consider cq states ρ_{AB} and take $\sigma_B = \rho_B$. We prove in the full version [1] that $\Gamma_c \leq 1$ in such cases. $\Gamma_c(\rho_{AB}|\sigma_B)$ also reduces to the classical collision probability when both of A, B are classical and $\sigma_B = \rho_B$.

We will often use the following relation, also taken from [36], valid for any $\rho_{AB} \in \mathrm{D}(\mathcal{H}_A \otimes \mathcal{H}_B)$:

$$\mathrm{Tr}\left((\rho_{AB} - U_A \otimes \rho_B)(I_A \otimes \rho_B^{-1/2})\right)^2 = \Gamma_c(\rho_{AB}|\rho_B) - \frac{1}{d_A} , \tag{3.2}$$

[8] When restricted to $\mathbb{F}_2$, our standard XOR lemma is very similar to Lemma 10 of [22], although the result from [22] provides a tighter bound in this case. [22] provides a bound of $p^{2^t}\epsilon^2$, while ours scales as $p^t\epsilon$, a quadratic loss. However our result applies to $\mathbb{F}_p$, while it is unclear whether the proof of [22] generalizes to $p > 2$. [22] obtains ther result by Fourier analysis.

[9] The term "quantum collision probability" is ours.

[10] Compared to [27, Lemma 3.15], we have $m = 1$ and $n = t$.

which can be verified by expanding the square:

$$\begin{aligned}
&\operatorname{Tr}\left((\rho_{AB} - U_A \otimes \rho_B)(I_A \otimes \rho_B^{-1/2})\right)^2 \\
&= \operatorname{Tr}\left(\rho_{AB}\,\rho_B^{-1/2}\right)^2 - 2\operatorname{Tr}\left(\rho_{AB}\,\rho_B^{-1/2}(U_A\rho_B)\rho_B^{-1/2}\right) + \operatorname{Tr}\left((U_A\rho_B)\rho_B^{-1/2}\right)^2 \\
&= \Gamma_c(\rho_{AB}|\rho_B) - \frac{1}{d_A}\,.
\end{aligned}$$

3.1 Non-uniform XOR lemma

Our non-uniform XOR lemma bounds the distance to uniform of a ccq state, a state with two classical registers and one quantum register. Roughly speaking, the lemma states that given two random variables $X_0 \in \mathbb{F}_p$ and $X \in \mathbb{F}_p^t$, if $X_0 + \langle a, X\rangle$ is close to uniform, then X_0 is close to uniform given X.

Lemma 1 (restated)**.** *Let p be a prime power, t an integer and $\epsilon \geq 0$. Let ρ_{X_0XE} be a ccq state with $X_0 \in \mathbb{F}_p$ and $X = (X_1, \ldots, X_t) \in \mathbb{F}_p^t$. For all $a = (a_1, \ldots, a_t) \in \mathbb{F}_p^t$, define a random variable $Z = X_0 + \langle a, X\rangle = X_0 + \sum_{i=1}^t a_i X_i$. If for all a, $\frac{1}{2}\left\|\rho_{ZE}^a - U_Z \otimes \rho_E\right\|_1 \leq \epsilon$, then*

$$\frac{1}{2}\left\|\rho_{X_0XE} - U_{X_0} \otimes \rho_{XE}\right\|_1 \leq \frac{p^{(t+1)/2}}{\sqrt{2}}\sqrt{\epsilon}\,. \tag{3.3}$$

The proof of the non-uniform XOR lemma has the following structure: we bound the collision probability by the trace distance in Lemma 5, then prove the non-uniform XOR lemma based on that. First we establish that for any ccq state ρ_{XZE}:

$$\begin{aligned}
&\operatorname{Tr}\left((\rho_{XZE} - U_X \otimes \rho_{ZE})(I_{XZ} \otimes \rho_E^{-1/2})\right)^2 \\
&= \operatorname{Tr}\left(\rho_{XZE}\,\rho_E^{-1/2}\right)^2 - 2\operatorname{Tr}\left(\rho_{XZE}\,\rho_E^{-1/2}(U_X\rho_{ZE})\rho_E^{-1/2}\right) + \operatorname{Tr}\left((U_X\rho_{ZE})\rho_E^{-1/2}\right)^2 \\
&= \Gamma_c(\rho_{XZE}|\rho_E) - \frac{1}{d_X}\Gamma_c(\rho_{ZE}|\rho_E)\,.
\end{aligned} \tag{3.4}$$

We need the following lemma to bound the collision probability by the trace distance in Lemma 5.

Lemma 4. *Let ρ_{XZE} be a ccq state. Then*

$$-\frac{1}{d_X}I_{XZE} \leq \left(I_{XZ} \otimes \rho_E^{-\frac{1}{2}}\right)(\rho_{XZE} - U_X \otimes \rho_{ZE})\left(I_{XZ} \otimes \rho_E^{-\frac{1}{2}}\right) \leq \left(1 - \frac{1}{d_X}\right)I_{XZE}\,. \tag{3.5}$$

Proof. We bound the eigenvalues of the middle expression. Since ρ_{XZE} is a ccq state, we know that the middle expression

$$\begin{aligned}&\left(I_{XZ}\otimes\rho_E^{-1/2}\right)(\rho_{XZE}-U_X\otimes\rho_{ZE})\left(I_{XZ}\otimes\rho_E^{-1/2}\right)\\&=\sum_{x,z}|x\rangle\langle x|\otimes|z\rangle\langle z|\otimes\rho_E^{-1/2}\left(\rho_E^{xz}-\frac{1}{d_X}\rho_E^z\right)\rho_E^{-1/2}\end{aligned}\tag{3.6}$$

is block diagonal, where $\rho_E^z=\sum_x\rho_E^{xz}$ and $\rho_E=\sum_{x,z}\rho_E^{xz}$. For any state $|\phi\rangle\in\mathcal{H}_E$ and x,z in the range of X,Z,

$$\langle\phi|\rho_E^{-1/2}\left(\rho_E^{xz}-\frac{1}{d_X}\rho_E^z\right)\rho_E^{-1/2}|\phi\rangle\geq\langle\phi|\rho_E^{-1/2}\left(-\frac{1}{d_X}\rho_E^z\right)\rho_E^{-1/2}|\phi\rangle\geq-\frac{1}{d_X}\,.\tag{3.7}$$

This proves the first inequality. We also have

$$\begin{aligned}&\langle\phi|\rho_E^{-1/2}\left(\rho_E^{xz}-\frac{1}{d_X}\rho_E^z\right)\rho_E^{-1/2}|\phi\rangle\\&=\langle\phi|\rho_E^{-1/2}\left(\rho_E^{xz}-\frac{1}{d_X}\sum_{x'}\rho_E^{x'z}\right)\rho_E^{-1/2}|\phi\rangle\\&=\left(1-\frac{1}{d_X}\right)\langle\phi|\rho_E^{-1/2}\rho_E^{xz}\rho_E^{-1/2}|\phi\rangle-\frac{1}{d_X}\sum_{x'\neq x}\langle\phi|\rho_E^{-1/2}\rho_E^{xz}\rho_E^{-1/2}|\phi\rangle\\&\leq\left(1-\frac{1}{d_X}\right)\,.\end{aligned}\tag{3.8}$$

This proves the second inequality. □

We then bound the collision probability by the trace distance.

Lemma 5 (Bounding collision probability with trace distance, non-uniform). *Let ρ_{XZE} be a ccq state. If*

$$\frac{1}{2}\left\|\rho_{XZE}-U_X\rho_{ZE}\right\|_1=\epsilon\,,\tag{3.9}$$

then

$$\frac{4\epsilon^2}{d_Xd_Z}\leq\Gamma_c(\rho_{XZE}|\rho_E)-\frac{1}{d_X}\Gamma_c(\rho_{ZE}|\rho_E)\leq2\epsilon\left(1-\frac{1}{d_X}\right)\,.\tag{3.10}$$

Proof. For the first inequality, we use Hölder's inequality (Lemma 3) with $r=t=4, s=2, A=C=I_{XZ}\otimes\rho_E^{1/4}$, and $B=$

$\left(I_{XZ} \otimes \rho_E^{-1/4}\right)\left(\rho_{XZE} - U_X \rho_{ZE}\right)\left(I_{XZ} \otimes \rho_E^{-1/4}\right)$. This leads to

$$
\begin{aligned}
2\epsilon &= \left\|\rho_{XZE} - U_X \rho_{ZE}\right\|_1 \\
&= \|ABC\|_1 \\
&\leq \left\|A^4\right\|_1^{1/4} \left\|B^2\right\|_1^{1/2} \left\|C^4\right\|_1^{1/4} \\
&= \sqrt{d_X d_Z \operatorname{Tr}\left(\left(\rho_{XZE} - U_X \otimes \rho_{ZE}\right)\left(I_{XZ} \otimes \rho_E^{-1/2}\right)\right)^2} \\
&= \sqrt{d_X d_Z \left(\Gamma_c(\rho_{XZE}|\rho_E) - \frac{1}{d_X}\Gamma_c(\rho_{ZE}|\rho_E)\right)}\,, \qquad (3.11)
\end{aligned}
$$

where we used Eq. (3.4) in the last line. Squaring both sides and dividing by $d_X d_Z$, we get the desired inequality. For the second inequality, we use Lemma 4 to show that

$$
\begin{aligned}
&-\frac{1}{d_X} I_{XZE} \leq \left(I_{XZ} \otimes \rho_E^{-\frac{1}{2}}\right)\left(\rho_{XZE} - U_X \otimes \rho_{ZE}\right)\left(I_{XZ} \otimes \rho_E^{-\frac{1}{2}}\right) \leq \left(1 - \frac{1}{d_X}\right) I_{XZE} \\
&\Rightarrow \left|\left(I_{XZ} \otimes \rho_E^{-1/2}\right)\left(\rho_{XZE} - U_X \otimes \rho_{ZE}\right)\left(I_{XZ} \otimes \rho_E^{-1/2}\right)\right| \leq \left(1 - \frac{1}{d_X}\right) I_{XZE}\,. \qquad (3.12)
\end{aligned}
$$

Starting with Eq. (3.4), we have

$$
\begin{aligned}
&\Gamma_c(\rho_{XZE}|\rho_E) - \frac{1}{d_X}\Gamma_c(\rho_{ZE}|\rho_E) \\
&= \operatorname{Tr}\left(\left(\rho_{XZE} - U_X \otimes \rho_{ZE}\right)\left(I_{XZ} \otimes \rho_E^{-1/2}\right)\right)^2 \\
&\leq \operatorname{Tr}\left(\left|\rho_{XZE} - U_X \rho_{ZE}\right| \left|\left(I_{XZ} \otimes \rho_E^{-1/2}\right)\left(\rho_{XZE} - U_X \otimes \rho_{ZE}\right)\left(I_{XZ} \otimes \rho_E^{-1/2}\right)\right|\right) \\
&\leq \operatorname{Tr}\left(\left|\rho_{XZE} - U_X \rho_{ZE}\right| \left(1 - \frac{1}{d_X}\right) I_{XZE}\right) \\
&= 2\epsilon\left(1 - \frac{1}{d_X}\right), \qquad (3.13)
\end{aligned}
$$

where we used Eq. (3.12) on the fourth line. □

Now we restate and prove the non-uniform XOR lemma. The proof idea is to start from the trace distance of X_0 given X to uniform, apply Lemma 5 to get an upper bound in terms of the collision probability of X_0 given X, apply Eq. (3.4) and expand the square to express the collision probability of X_0 given X in terms of the collision probability of $X_0 + \langle a, X\rangle$, and finally apply Lemma 5 again to get an upper bound in terms of the trace distance of $X_0 + \langle a, X\rangle$ to uniform.

Lemma 1 (restated)**.** *Let p be a prime power, t an integer and $\epsilon \geq 0$. Let ρ_{X_0XE} be a ccq state with $X_0 \in \mathbb{F}_p$ and $X = (X_1, \ldots, X_t) \in \mathbb{F}_p^t$. For all $a = (a_1, \ldots, a_t) \in$*

$\mathbb{F}_p^t$, define a random variable $Z = X_0 + \langle a, X\rangle = X_0 + \sum_{i=1}^t a_i X_i$. If for all a, $\frac{1}{2}\left\|\rho_{ZE}^a - U_Z \otimes \rho_E\right\|_1 \leq \epsilon$, then

$$\frac{1}{2}\left\|\rho_{X_0XE} - U_{X_0} \otimes \rho_{XE}\right\|_1 \leq \frac{p^{(t+1)/2}}{\sqrt{2}}\sqrt{\epsilon}\,. \tag{3.14}$$

Proof. We start by relating the collision probability of Z and $X_0 + \langle a, X\rangle$:

$$\begin{aligned}
&\Gamma_c(\rho_{ZE}^a|\rho_E) - \frac{1}{p}\\
&= \mathrm{Tr}\left[(\rho_{ZE}^a - U_Z\rho_E)I_Z \otimes \rho_E^{-1/2}\right]^2\\
&= \mathrm{Tr}\left[\sum_z |z\rangle\langle z| \sum_{x,x_0}\left(\delta\left(z - x_0 - \langle a,x\rangle, 0\right) - \frac{1}{p}\right)\rho_E^{x_0x} I_Z \rho_E^{-1/2}\right]^2\\
&= \sum_z \mathrm{Tr}\left[\sum_{x_0x}\left(\delta\left(z - x_0 - \langle a,x\rangle, 0\right) - \frac{1}{p}\right)\rho_E^{x_0x}\rho_E^{-1/2}\right]^2\\
&= \sum_{z,x_0,x_0',x,x'}\Big[\delta\left(z - x_0 - \langle a,x\rangle, 0\right)\delta\left(z - x_0' - \langle a,x'\rangle, 0\right)\\
&\quad - \frac{2}{p}\delta\left(z - x_0 - \langle a,x\rangle, 0\right) + \frac{1}{p^2}\Big]\,\mathrm{Tr}\left(\rho_E^{x_0x}\rho_E^{-1/2}\rho_E^{x_0'x'}\rho_E^{-1/2}\right)\\
&= \sum_{x_0,x_0',x,x'}\left[\delta\left(x_0 - x_0' + \langle a, x - x'\rangle, 0\right) - \frac{1}{p}\right]\mathrm{Tr}\left(\rho_E^{x_0x}\rho_E^{-1/2}\rho_E^{x_0'x'}\rho_E^{-1/2}\right)\\
&= \sum_{x_0,x_0',x}\left(\delta\left(x_0 - x_0', 0\right) - \frac{1}{p}\right)\mathrm{Tr}\left(\rho_E^{x_0x}\rho_E^{-1/2}\rho_E^{x_0'x}\rho_E^{-1/2}\right)\\
&\quad + \sum_{x_0,x_0',x\neq x'}\left[\delta\left(x_0 - x_0' + \langle a, x - x'\rangle, 0\right) - \frac{1}{p}\right]\mathrm{Tr}\left(\rho_E^{x_0x}\rho_E^{-1/2}\rho_E^{x_0'x'}\rho_E^{-1/2}\right)\\
&= \sum_{x_0,x}\mathrm{Tr}\left(\rho_E^{x_0x}\rho_E^{-1/2}\rho_E^{x_0x}\rho_E^{-1/2}\right) - \frac{1}{p}\sum_{x_0,x_0',x}\mathrm{Tr}\left(\rho_E^{x_0x}\rho_E^{-1/2}\rho_E^{x_0'x}\rho_E^{-1/2}\right)\\
&\quad + \sum_{x_0,x_0',x\neq x'}\left[\delta\left(x_0 - x_0' + \langle a, x - x'\rangle, 0\right) - \frac{1}{p}\right]\mathrm{Tr}\left(\rho_E^{x_0x}\rho_E^{-1/2}\rho_E^{x_0'x'}\rho_E^{-1/2}\right)\\
&= \Gamma_c(\rho_{X_0XE}|\rho_E) - \frac{1}{p}\Gamma_c(\rho_{XE}|\rho_E)\\
&\quad + \sum_{x_0,x_0',x\neq x'}\left[\delta\left(x_0 - x_0' + \langle a, x - x'\rangle, 0\right) - \frac{1}{p}\right]\mathrm{Tr}\left(\rho_E^{x_0x}\rho_E^{-1/2}\rho_E^{x_0'x'}\rho_E^{-1/2}\right).
\end{aligned} \tag{3.15}$$

When we average over a, the last term vanishes,

$$\mathrm{E}_a\left(\Gamma_c(\rho_{ZE}^a|\rho_E) - \frac{1}{p}\right) = \Gamma_c(\rho_{X_0XE}|\rho_E) - \frac{1}{p}\Gamma_c(\rho_{XE}|\rho_E)\,. \tag{3.16}$$

With the heavy work done, we put everything together and prove the lemma

$$\begin{aligned}\frac{\left\|\rho_{X_0XE} - U_{X_0}\rho_{XE}\right\|_1^2}{p^{t+1}} &\le \Gamma_c(\rho_{X_0XE}|\rho_E) - \frac{1}{p}\Gamma_c(\rho_{XE}|\rho_E) \\ &= \mathrm{E}_a\left(\Gamma_c(\rho^a_{ZE}|\rho_E) - \frac{1}{p}\right) \\ &\le 2\epsilon\,, \end{aligned} \tag{3.17}$$

where we used Lemma 5 one the first line, Eq. (3.16) on the second line, Lemma 5 and the assumption of the lemma on the third line. Multiplying both sides by $\frac{p^{t+1}}{2}$ and take a square root, we get the desired result:

$$\frac{1}{2}\left\|\rho_{X_0XE} - U_{X_0}\rho_{XE}\right\|_1 \le \frac{p^{(t+1)/2}}{\sqrt{2}}\sqrt{\epsilon}\,. \tag{3.18}$$

□

4 Quantum-Proof Non-malleable Extractor

In this section we introduce our non-malleable extractor and prove its security. The extractor was first considered by Li [27]. We use the symbol $\|$ for concatenation of strings, and for $a, b \in \mathbb{F}_p^n$ write $\langle a, b\rangle$ for the standard inner product over $\mathbb{F}_p^n$.

Definition 7 (Inner product-based non-malleable extractor). *Let $p \neq 2$ be a prime. For any even integer n, define a function $\mathrm{nmExt} : \mathbb{F}_p^n \times \mathbb{F}_p^{n/2} \to \mathbb{F}_p$ by $\mathrm{nmExt}(X, Y) = \langle X, Y||Y^2\rangle$, where Y^2 is defined as in Section 2.1.*

Theorem 1. *Let $p \neq 2$ be a prime. Let n be an even integer. Then for any $\epsilon > 0$ the function $\mathrm{nmExt}(X, Y) = \langle X, Y\|Y^2\rangle$ is an $\left(\left(\frac{n}{2}+6\right)\log p - 1 + 4\log\frac{1}{\epsilon}, \epsilon\right)$ quantum-proof non-malleable extractor.*

The proof of Theorem 1 is based on a reduction showing that any successful attack for an adversary to nmExt leads to a good strategy for the players in a certain communication game, that we introduce next.

4.1 A communication game

Let $p \neq 2$ be a prime. Let n be an even integer, and $g : \mathbb{F}_p^{n/2} \times \mathbb{F}_p^{n/2} \to \mathbb{F}_p^n$ an arbitrary function such that for any $z \in \mathbb{F}_p^n$ there are at most two possible pairs (y, y') such that $y \neq y'$ and $g(y, y') = z$. Consider the following communication game, called $\mathrm{GUESS}(n, p, g)$, between two players Alice and Bob.

1. Bob receives $y \in \mathbb{F}_p^{n/2}$ from the referee.
2. Alice creates a cq state ρ_{XE}, where $X \in \mathbb{F}_p^n$, and sends the quantum register E to Bob.

3. Bob returns $y' \in \mathbb{F}_p^{n/2}$ and $b \in \mathbb{F}_p$.

The players win if and only if $b = \langle x, g(y,y')\rangle$ and $y' \neq y$.

Note that Alice does not receive anything from the referee and is completely free in what state she wants to create, so it is easy for the players to win with probability 1 by creating a trivial state, e.g. $\rho_{XE} = |0\rangle\langle 0| \otimes |0\rangle\langle 0|$. Therefore we benchmark the success probability of a strategy by the min-entropy of Alice's "input" X, conditioned on her message E to Bob. The following lemma bounds the players' maximum success probability in this game over uniformly random input y and quantum measurements as a function of the min-entropy of Alice's input X, conditioned on her message E to Bob.

Lemma 6 (Success probability of the communication game). *Suppose there exists a communication protocol for Alice and Bob in* GUESS(n,p,g) *that succeeds with probability at least $\frac{1}{p}+\epsilon$, on average over a uniformly random choice of input y to Bob. Then $H_{\min}(X|E)_\rho \leq \frac{n}{2}\log p + 1 + 2\log\frac{1}{\epsilon}$.*

Proof. Let $\rho_{XE} = \sum_x |x\rangle\langle x|_X \otimes \rho_E^x$ be the cq state prepared by Alice. A strategy for Bob is a family of POVM $\{M_y^{y',b}\}_{y',b}$, indexed by $y \in \mathbb{F}_p^{n/2}$ and with outcomes $(y',b) \in \mathbb{F}_p^{n/2} \times \mathbb{F}_p$. We can assume that $\{M_y^{y',b}\}_{y',b}$ is projective, since Alice can send ancilla qubits along with ρ and allow Bob to apply Naimark's theorem to his POVM in order to obtain a projective measurement; this will change neither his success probability nor the min-entropy of Alice's state. By definition, the players' success probability in GUESS(n,p,g) is

$$\frac{1}{p}+\epsilon = \sum_x p^{-\frac{n}{2}} \sum_y \sum_{y'} \sum_b \delta(b, \langle x, g(y,y')\rangle)\, \mathrm{Tr}\big(M_y^{y',b}\rho_E^x\big)\ . \tag{4.1}$$

For each $u \in \mathbb{F}_p$ let $A_{y,u}^{y'} = \sum_b \omega^{ub} M_y^{y',b}$, where $\omega = e^{\frac{2i\pi}{p}}$. By inversion, $M_y^{y',b} = \frac{1}{p}\sum_u \omega^{-ub} A_{y,u}^{y'}$. Replacing this into (4.1) we obtain

$$\begin{aligned}\frac{1}{p}+\epsilon &= \frac{1}{p}\sum_u p^{-\frac{n}{2}} \sum_y \sum_{y'} \sum_b \delta(b, \langle x, g(y,y')\rangle)\, \omega^{-ub}\, \mathrm{Tr}\big(A_{y,u}^{y'}\rho_E^x\big)\\ &\leq \frac{1}{p} + \Big(1-\frac{1}{p}\Big) \max_{u\neq 0} \Big| p^{-\frac{n}{2}} \sum_y \sum_{y'} \sum_b \delta(b, \langle x, g(y,y')\rangle)\, \omega^{-ub}\, \mathrm{Tr}\big(A_{y,u}^{y'}\rho_E^x\big)\Big|\ ,\end{aligned} \tag{4.2}$$

where for the second line we used that $\sum_{y'} A_{y,0}^{y'} = \sum_{y',b} M_y^{y',b} = I_E$.

Fix $u \neq 0$ that achieves the maximum in (4.2). For fixed y, define the map $T_{y,u}$ on $\mathcal{H}_E$ by

$$T_{y,u} : |\psi\rangle \mapsto \sum_{y'} |y'\rangle A_{y,u}^{y'} |\psi\rangle\ . \tag{4.3}$$

$T_{y,u}$ has norm at most 1, since

$$T_{y,u}^{\dagger} T_{y,u} = \sum_{y'} (A_{y,u}^{y'})^{\dagger} A_{y,u}^{y'} = \sum_{y'} \sum_{b} \left(M_y^{y',b} \right)^2 = I_E \ .$$

For the second equality we used that $\{M_y^{y',b}\}_{y',b}$ is projective. Therefore $T_{y,u}$ is a physical operation.

Consider the following guessing strategy for an adversary holding side information ρ_E^x about x. The adversary first prepares a uniform superposition over y. Conditioned on y, it applies the map $T_{y,u}$. It computes $g(y,y')$ in an ancilla register, and erases (y,y'), except for one bit of information $r(y,y') \in \{0,1\}$, which specifies which pre-image (y,y') is, given $g(y,y')$ (this is possible by the 2-to-1 assumption on g). The adversary applies a Fourier transform on the register containing $g(y,y')$, using $\omega_u = \omega^{-u}$ as primitive p-th root of unity (this is possible since $u \neq 0$ and p is prime). It measures the result and outputs it as a guess for x. Formally, the transformation this implements is

$$\begin{aligned} |\psi\rangle &\mapsto p^{-\frac{n}{4}} \sum_{y} |y\rangle \sum_{y'} |y'\rangle A_{y,u}^{y'} |\psi\rangle \\ &\mapsto p^{-\frac{n}{4}} \sum_{y,y'} \big|g(y,y')\big\rangle \big|r(y,y')\big\rangle A_{y,u}^{y'} |\psi\rangle \\ &\mapsto \sum_{v} |v\rangle \Big(p^{-\frac{3n}{4}} \sum_{y,y'} \omega_u^{\langle v, g(y,y')\rangle} \big|r(y,y')\big\rangle A_{y,u}^{y'} \Big) |\psi\rangle \ . \end{aligned}$$

The adversary's success probability in guessing $v = x$ on input ρ_E^x is therefore

$$\begin{aligned} p_s &= \sum_{x} \mathrm{Tr}\Big(\Big(p^{-\frac{3n}{4}} \sum_{y,y'} \omega_u^{\langle x, g(y,y')\rangle} \big|r(y,y')\big\rangle \otimes A_{y,u}^{y'} \Big) \rho_E^x \\ &\quad \cdot \Big(p^{-\frac{3n}{4}} \sum_{y,y'} \omega_u^{-\langle x, g(y,y')\rangle} \big\langle r(y,y')\big| \otimes (A_{y,u}^{y'})^{\dagger} \Big) \Big) \\ &= \frac{1}{p^{\frac{3n}{2}}} \sum_{x} \sum_{r \in \{0,1\}} \mathrm{Tr}\Big(\Big(\sum_{y,y' : r(y,y') = r} \omega_u^{\langle x, g(y,y')\rangle} A_{y,u}^{y'} \Big)^{\dagger} \\ &\quad \cdot \Big(\sum_{y,y' : r(y,y') = r} \omega_u^{\langle x, g(y,y')\rangle} A_{y,u}^{y'} \Big) \rho_E^x \Big) \\ &\geq \frac{1}{p^{\frac{3n}{2}}} \sum_{x} \frac{1}{2} \mathrm{Tr}\Big(\Big(\sum_{y,y'} \omega_u^{\langle x, g(y,y')\rangle} A_{y,u}^{y'} \Big)^{\dagger} \Big(\sum_{y,y'} \omega_u^{\langle x, g(y,y')\rangle} A_{y,u}^{y'} \Big) \rho_E^x \Big) \ , \end{aligned} \tag{4.4}$$

where for the last line we used $\mathrm{Tr}(A^\dagger A\rho) + \mathrm{Tr}(B^\dagger B\rho) \geq \frac{1}{2}\mathrm{Tr}((A+B)^\dagger(A+B)\rho)$ if ρ is positive semidefinite. Now, recall from (4.2) and our choice of u that

$$\begin{aligned}\epsilon &\leq p^{-\frac{n}{2}} \Big| \sum_{x,y,y'} \omega^{-u(\langle x, g(y,y')\rangle)} \,\mathrm{Tr}\big(A^{y'}_{y,u}\,\rho_E^x\big)\Big| \\ &\leq p^{-\frac{n}{2}} \Big(\sum_x \mathrm{Tr}(\rho_E^x)\Big)^{1/2} \\ &\cdot \Big(\sum_x \mathrm{Tr}\Big(\Big(\sum_{y,y'} \omega^{-u(\langle x,g(y,y')\rangle)}\, A^{y'}_{y,u}\Big)\,\rho_E^x\,\Big(\sum_{y,y'} \omega^{-u(\langle x,g(y,y')\rangle)}\, A^{y'}_{y,u}\Big)^\dagger\Big)\Big)^{1/2}, \end{aligned} \tag{4.5}$$

where the inequality is Cauchy-Schwarz. Comparing (4.4) and (4.5) gives

$$p_s \;\geq\; \frac{1}{2} p^{-\frac{n}{2}} \epsilon^2 \,.$$

We conclude using that by Lemma 2, $H_{\min}(X|E) \leq -\log p_s$. □

4.2 Proof of Theorem 1

In this section we give the proof of Theorem 1. Towards this we first prove a preliminary lemma showing that a certain function, based on the definition of nmExt, has few collisions.

Lemma 7. *Let $p \neq 2$ be a prime and n an even integer. For $a \in \mathbb{F}_p$ define a function $g_a : \mathbb{F}_p^{n/2} \times \mathbb{F}_p^{n/2} \to \mathbb{F}_p^n$ by*

$$g_a(y,y') \;=\; y + ay' \| y^2 + ay'^2 \,, \tag{4.6}$$

where y^2 is defined in Section 2.1. Then for any $a \in \mathbb{F}_p, a \neq 0$ and $z \in \mathbb{F}_p^n$ there are at most 2 distinct pairs (y,y') such that $y' \neq y$ and $g_a(y,y') = z$.

Proof. We use the bijection defined in Section 2.1 to interpret y and y' in $\mathbb{F}_{p^{n/2}}$. For $a \neq 0$, we fix an image $g_a = (c,d)$, where c,d are interpreted as elements of $\mathbb{F}_{p^{n/2}}$, and solve for (y,y') in $\mathbb{F}_{p^{n/2}} \times \mathbb{F}_{p^{n/2}}$ satisfying

$$y + ay' = c\,, \tag{4.7}$$

$$y^2 + ay'^2 = d\,. \tag{4.8}$$

Using (4.7) to eliminate y we get

$$\begin{aligned} &(c - ay')^2 + ay'^2 = d \\ &\Rightarrow (a + a^2)y'^2 + (-2ca)y' + (c^2 - d) = 0\,. \end{aligned} \tag{4.9}$$

Since (4.9) is a quadratic equation, there are at most two solutions unless all coefficients are zero. Since $p \neq 2$, $-2 \neq 0$. If all coefficients are zero, $-2 \neq 0$, and $a \neq 0$, then $c = d = 0, a = -1$, which implies $y' = y$ by (4.7) and contradicts our assumption. So there are at most two different y' that can be mapped to (c,d). By (4.7) each y' corresponds to a unique y, so there are at most two pre-images. □

We are ready to give the proof of Theorem 1. The proof depends on a simple lemma relating trace distance and guessing measurements, Lemma 8, which is stated and proved after the proof of the theorem.

Proof of Theorem 1. Let $k = \left(\frac{n}{2}+6\right)\log p - 1 + 4\log\frac{1}{\epsilon}$ and $\rho_{XE} \in \mathrm{D}(\mathbb{C}^{p^n} \otimes \mathcal{H}_E)$ an $(n\log p, k)$-source. Fix a CPTP map $\mathrm{Adv} : \mathrm{L}(\mathbb{C}^{p^{n/2}} \otimes \mathcal{H}_E) \to \mathrm{L}(\mathbb{C}^{p^{n/2}} \otimes \mathcal{H}_{E'})$ with no fixed points, and define $\sigma_{\mathrm{nmExt}(X,Y)\mathrm{nmExt}(X,Y')YY'E'}$ as in Definition 5. Given the definition of nmExt, to prove the theorem we need to show that

$$(\langle X, Y\|Y^2\rangle, \langle X, Y'\|Y'^2\rangle, Y', Y, E')_\sigma \approx_\epsilon (U_{\mathbb{F}_p}, \langle X, Y'\|Y'^2\rangle, Y', Y, E')_\sigma \,. \tag{4.10}$$

Applying the XOR lemma, Lemma 1, with $X_0 = \langle X, Y||Y^2\rangle$, $X = \langle X, Y'||Y'^2\rangle$, $E = (Y', Y, E')$ and $t = 1$, (4.10) will follow once it is shown that

$$(\langle X, Y||Y^2\rangle + a\langle X, Y'\|Y'^2\rangle, Y', Y, E')_\sigma \approx_{\frac{2\epsilon^2}{p^2}} (U_{\mathbb{F}_p}, Y', Y, E')_\sigma \,, \tag{4.11}$$

for all $a \in \mathbb{F}_p$. For $a = 0$, (4.11) follows from the fact that inner product is a quantum-proof two source extractor, which can be shown by the combination of Theorem 5.3 of [10] and Lemma 1 in [24]. For non-zero $a \in \mathbb{F}_p$, recall the function $g_a : \mathbb{F}_p^{n/2} \times \mathbb{F}_p^{n/2} \to \mathbb{F}_p^n$ defined in (4.6). Lemma 7 shows that for any $a \neq 0$, the restriction of g_a to $\{(y, y') : y \neq y'\}$ is at most 2-to-1, and $y \neq y'$ is ensured by the fact that Adv has no fixed points. We establish (4.11) by contradiction. Assume thus that

$$(\langle X, g_a(Y, Y')\rangle, Y', Y, E')_\sigma \approx_{\frac{2\epsilon^2}{p^2}} (U_{\mathbb{F}_p}, Y', Y, E')_\sigma \tag{4.12}$$

does not hold, for some non-zero $a \in \mathbb{F}_p$. Fix such an a and write g_a for g. From Lemma 8 it follows that there exists a POVM measurement $\{M^z\}_{z\in\mathbb{F}_p}$ on $\sigma_{Y'YE'}$ such that

$$\sum_{z\in\mathbb{F}_p} \mathrm{Tr}\big(M^z \sigma^z_{YY'E}\big) \geq \frac{1}{p} + \frac{2\epsilon^2}{p^3} \,, \tag{4.13}$$

where $\sigma^z_{YY'E}$ is the reduced density of σ on $YY'E$ conditioned on $\langle X, g(Y, Y')\rangle = z$. To conclude the proof of the theorem we show that the adversary's map Adv and the POVM $\{M^z\}$ can be combined to give a "successful" strategy for the players in the communication game introduced in Section 4.1. To see this, consider the state ρ_{XE} that is instantiated as the source for the extractor; by definition $H_{\min}(X|E)_\rho = k = \left(\frac{n}{2}+6\right)\log p - 1 + 4\log\frac{1}{\epsilon}$. In the third step of the game, Bob applies the map Adv to the registers Y and E containing his input Y and the state sent by Alice, and measures to obtain an outcome Y'. He then applies the measurement $\{M^z\}$ on his registers (Y, Y', E) to obtain a value $b = z \in \mathbb{F}_p$ that he provides as his output in the game. By (4.13) it follows that this strategy succeeds in the game with probability at least $\frac{1}{p} + \frac{2\epsilon^2}{p^3}$, which by Lemma 6 implies $H_{\min}(X|E) \leq \frac{n}{2}\log p + 1 + 2\log\frac{p^3}{2\epsilon^2}$, contradicting our choice of k. This proves (4.11) and thus the theorem. □

The following lemma is used in the proof of the theorem.

Lemma 8. *Let $\rho_{XE} = \sum_x |x\rangle\langle x| \otimes \rho_E^x$ be such that*

$$\frac{1}{2}\|(X,E)-(U,E)\|_1 \;=\; \frac{1}{2}\left\|\rho_{XE} - U_X \otimes \rho_E\right\|_1 \;=\; \epsilon\;,$$

where U_X is the totally mixed state on X and $\rho_E = \sum_x \rho_E^x$. Then there exists a POVM $\{M_x\}$ on ρ_E such that

$$\sum_x \mathrm{Tr}(M_x \rho_E^x) = \frac{1}{d_X} + \frac{\epsilon}{d_X}\;.$$

Proof. Since ρ_{XE} is a cq state, $\|\rho_{XE} - U_X \otimes \rho_E\|_1 = \sum_x \|\rho_E^x - \frac{1}{d_X}\rho_E\|_1$. For each x, let M'_x be the projector onto the positive eigenvalues of $\rho_E^x - \frac{1}{d_X}\rho_E$, so

$$\sum_x \mathrm{Tr}(M'_x(\rho_E^x - \frac{1}{d_X}\rho_E)) = \frac{1}{2}\sum_x \|\rho_E^x - \frac{1}{d_X}\rho_E\|_1\;. \tag{4.14}$$

Let $M' = \sum_x M'_x$ and $M_x = \frac{1}{d_X}(M'_x + (I_E - \frac{1}{d_X}M'))$. Then $M_x \geq 0$ and $\sum_x M_x = \frac{1}{d_X}(M' + d_X I_E - M') = I_E$. Moreover,

$$\begin{aligned}
\sum_x \mathrm{Tr}(M_x\rho_E^x) &= \sum_x \mathrm{Tr}\left[\frac{1}{d_X}(M'_x + (I_E - \frac{1}{d_X}M'))\rho_E^x\right]\\
&= \frac{1}{d_X}\left[\sum_x \left(\mathrm{Tr}(M'_x\rho_E^x)\right) + \mathrm{Tr}\left((I_E - \frac{1}{d_X}M')\rho_E\right)\right]\\
&= \frac{1}{d_X} + \frac{1}{d_X}\sum_x\left(\mathrm{Tr}(M'_x\rho_E^x) - \frac{1}{d_X}\mathrm{Tr}(M'_x\rho_E)\right)\\
&= \frac{1}{d_X} + \frac{1}{d_X}\left(\sum_x \mathrm{Tr}\left(M'_x(\rho_E^x - \frac{1}{d_X}\rho_E)\right)\right)\\
&= \frac{1}{d_X} + \frac{1}{2d_X}\sum_x \left\|\rho_E^x - \frac{1}{d_X}\rho_E\right\|_1
\end{aligned}$$

by (4.14). □

5 Privacy amplification

Dodis and Wichs [19] introduced a framework for constructing a two-message privacy amplification protocol from any non-malleable extractor. In [14] it is shown that the same framework, when instantiated with a quantum-proof non-malleable extractor nmExt as defined in Definition 5, leads to a protocol that is secure against active quantum adversaries. In Section 5.1 we recall the Dodis-Wichs protocol, and state the security guarantees that follow by plugging in our non-malleable extractor construction. The guarantees follows from the quantum extension of the Dodis-Wichs results in [14]; since that work has not been published we include their results regarding the Dodis-Wichs protocol in Appendix A.

In Section 5.2 we show that a different protocol for privacy amplification due to Dodis et al. [16], whose main advantage is of being a one-round protocol, is also quantum-proof. The construction and analysis of the protocol of [16] is simple, with the drawback of a large entropy loss.

We start with the definition of a quantum-secure privacy amplification protocol against active adversaries. A privacy amplification protocol (P_A, P_B) is defined as follows. The protocol is executed by two parties Alice and Bob sharing a secret $X \in \{0,1\}^n$, whose actions are described by P_A, P_B respectively.[11] In addition there is an active, computationally unbounded adversary Eve, who might have some quantum side information E correlated with X but satisfying $H_{\min}(X|E)_\rho \geq k$, where ρ_{XE} denotes the initial state at beginning of the protocol.

Informally, the goal for the protocol is that whenever a party (Alice or Bob) does not reject, the key R output by this party is random and statistically independent of Eve's view. Moreover, if both parties do not reject, they must output the same keys $R_A = R_B$ with overwhelming probability.

More formally, we assume that Eve is in full control of the communication channel between Alice and Bob, and can arbitrarily insert, delete, reorder or modify messages sent by Alice and Bob to each other. At the end of the protocol, Alice outputs a key $R_A \in \{0,1\}^m \cup \{\perp\}$, where $\perp$ is a special symbol indicating rejection. Similarly, Bob outputs a key $R_B \in \{0,1\}^m \cup \{\perp\}$. The following definition generalizes the classical definition in [17].

Definition 8. *Let k, m be integer and $\epsilon \geq 0$. A privacy amplification protocol (P_A, P_B) is a (k, m, ϵ)-*privacy amplification protocol secure against active quantum adversaries *if it satisfies the following properties for any initial state ρ_{XE} such that $H_{\min}(X|E)_\rho \geq k$, and where σ be the joint state of Alice, Bob, and Eve at the end of the protocol:*

1. Correctness. *If the adversary does not interfere with the protocol, then* $\Pr[R_A = R_B \wedge\ R_A \neq \perp \wedge R_B \neq \perp] = 1$.
2. Robustness. *This property comes in two flavors. The first is* pre-application *robustness, which states that even in the presence of an active adversary,* $\Pr[R_A \neq R_B \wedge\ R_A \neq \perp \wedge R_B \neq \perp] \leq \epsilon$*. The second is* post-application *robustness, which is defined similarly, except the adversary is additionally given the key R_A that is the result of the interaction (P_A, P_E), and the key R_B that results from the interaction (P_E, P_B), where P_E denotes the adversary's actions in its interaction with Alice and Bob.*
3. Extraction. *Given a string $r \in \{0,1\}^m \cup \{\perp\}$, let* $\mathsf{purify}(r)$ *be a random variable on m-bit strings that is deterministically equal to $\perp$ if $r = \perp$, and is otherwise uniformly distributed. Let V denotes the transcript of an execution of the protocol execution, and $\rho_{E'}$ the final quantum state possessed by Eve. Then the following*

[11] It is not necessary for the definition to specify exactly how the protocols are formulated; informally, each player's actions is described by a sequence of efficient algorithms that compute the player's next message, given the past interaction.

should hold:

$$(R_A, V, E')_\sigma \approx_\epsilon (\mathsf{purify}(R_A), V, E')_\sigma \quad \textit{and} \quad (R_B, V, E')_\sigma \approx_\epsilon (\mathsf{purify}(R_B), V, E')_\sigma \ .$$

In other words, whenever a party does not reject, the party's key is indistinguishable from a fresh random string to the adversary.

The quantity $k - m$ is called the entropy loss.

5.1 Dodis-Wichs protocol with non-malleable extractor

Here we first recall the Dodis-Wichs protocol for privacy amplification (hereafter called *Protocol DW*), which is summarized in Figure 5.1, and the required security definitions, taken from [14]. We then state the result obtained by instantiating the protocol with the quantum-proof non-malleable extractor from Theorem 1.

Protocol DW

Let $d_X, d_Y, d_2, \ell, d_Z, t, k$ be integers and $\epsilon_{\text{MAC}}, \epsilon_{\text{Ext}}, \epsilon_{\text{nmExt}} > 0$.
Let $\text{MAC} : \{0, \dots, d_Z - 1\} \times \{0,1\}^{d_2} \rightarrow \{0,1\}^t$ be a one-time ϵ_{MAC}-information-theoretically secure message authentication code.
Let $\text{Ext} : \{0, \dots, d_X - 1\} \times \{0,1\}^{d_2} \rightarrow \{0,1\}^m$ be a strong $(k - \ell - \log(1/\epsilon_{\text{Ext}}), \epsilon_{\text{Ext}})$ quantum-proof extractor.
Let $\text{nmExt} : \{0, \dots, d_X - 1\} \times \{0,, \dots, d_Y - 1\} \rightarrow \{0, \dots, d_Z - 1\}$ be a $(k, \epsilon_{\text{nmExt}})$ quantum-proof non-malleable extractor.
It is assumed that both parties, Alice and Bob, have access to a shared random variable $X \in \{0, \dots, d_X - 1\}$.

1. Alice samples a Y_A uniformly from $\{0,, \dots, d_Y - 1\}$. She sends Y_A to Bob. She computes $Z = \text{nmExt}(X, Y_A)$.
2. Bob receives Y'_A from Alice. He samples a uniform $Y_B \sim U_{d_2}$, and computes $Z' = \text{nmExt}(X, Y'_A)$ and $W = \text{MAC}(Z', Y_B)$. He sends (Y_B, W) to Alice. Bob then reaches the KEYDERIVED state and outputs $R_B = \text{Ext}(X, Y_B)$.
3. Alice receives (Y'_B, W') from Bob. If $W' = \text{MAC}(Z, Y'_B)$ she reaches the KEYCONFIRMED state and outputs $R_A = \text{Ext}(X, Y'_B)$. Otherwise she outputs $R_A = \perp$.

Fig. 5.1. The Dodis-Wichs privacy amplification protocol.

Aside from the use of a strong quantum-proof extractor (Definition 3) and a quantum-proof non-malleable extractor (Definition 5), the protocol relies on an information-theoretically secure one-time message authentication codes, or MAC. This security notion is defined as follows.

Definition 9. *A function* $\text{MAC} : \{0, \dots, d_Z - 1\} \times \{0,1\}^d \rightarrow \{0,1\}^t$ *is an* ϵ_{MAC}-information-theoretically secure one-time message authentication code *if for any function* $\mathcal{A} : \{0,1\}^d \times \{0,1\}^t \rightarrow \{0,1\}^d \times \{0,1\}^t$ *it holds that for all* $m \in \{0,1\}^d$

$$\Pr_{k \leftarrow U_Z} \left[(\text{MAC}(k, m') = \sigma') \wedge (m' \neq m) : (m', \sigma') \leftarrow \mathcal{A}(m, \text{MAC}(k, m)) \right] \leq \epsilon_{\text{MAC}}.$$

Efficient constructions of MAC satisfying the conditions of Definition 9 are known. The following proposition summarizes some parameters that are achievable using a construction based on polynomial evaluation.

Proposition 1 (Proposition 1 in [34]). *For any $\epsilon_{\mathrm{MAC}} > 0$, integer $d > 0$, $d_Z \geq \frac{d^2}{\epsilon_{\mathrm{MAC}}^2}$, there exists an efficient family of ϵ_{MAC}-information-theoretically secure one-time message authentication codes*

$$\{\mathrm{MAC} : \{0, \ldots, d_Z - 1\} \times \{0,1\}^d \to \{0,1\}^t\}_{d \in \mathbb{N}}$$

with $t \leq \log d + \log(1/\epsilon_{\mathrm{MAC}})$.

The correctness and security requirements for the protocol are natural extensions of the classical case (see Definition 18 in [19]). Informally, the adversary has the following control over the outcome of the protocol. First, it possess initial quantum side information E about the weak secret X shared by Alice and Bob. That is, it has a choice of a cq source ρ_{XE}, under the condition that $H_{\min}(X|E)$ is sufficiently large. Second, the adversary may intercept and modify any of the messages exchanged. In Protocol DW there are only two messages exchanged, Y_A from Alice to Bob and (Y_B, σ) from Bob to Alice. To each of these messages the adversary may apply an arbitrary transformation, that may depend on its side information E. We model the two possible attacks, one for each message, as CPTP maps $T_1 : \mathrm{L}(\mathcal{H}_Y \otimes \mathcal{H}_E) \to \mathrm{L}(\mathcal{H}_Y \otimes \mathcal{H}_{E'})$ and $T_2 : \mathrm{L}(\mathbb{C}^{2^{d_2}} \otimes \mathcal{H}_{2^t} \otimes \mathcal{H}_{E'}) \to \mathrm{L}(\mathbb{C}^{2^{d_2}} \otimes \mathbb{C}^{2^t} \otimes \mathcal{H}_{E''})$, where $\mathcal{H}$ denotes the Hilbert space associated with system E. Note that we may always assume that $\mathcal{H}$ is large enough for the adversary to keep a local copy of the messages it sees, if it so desires.

The following result on the security of protocol DW is shown in [14]. We include the proof in Appendix A.

Theorem 3. *Let k, t, d_Z and $\epsilon_{\mathrm{MAC}}, \epsilon_{\mathrm{Ext}}, \epsilon_{\mathrm{nmExt}}$ be parameters of Protocol DW, as specified in Figure 5.1. Let* nmExt *be a $(k, \epsilon_{\mathrm{nmExt}})$ quantum-proof non-malleable extractor,* Ext *a strong $(k - \log d_Z - \log(1/\epsilon_{\mathrm{Ext}}), \epsilon_{\mathrm{Ext}})$ quantum-proof extractor, and* MAC *an ϵ_{MAC}-information-theoretically secure one-time message authentication code. Then for any active attack (ρ_{XE}, T_1, T_2) such that $H_{\min}(X|E)_\rho \geq k$, the DW privacy amplification protocol described in Figure 5.1 is (k, m, ϵ)-secure as defined in Definition 8 with $\epsilon = O(\epsilon_{\mathrm{Ext}} + \epsilon_{\mathrm{nmExt}} + \epsilon_{\mathrm{MAC}})$.*

Combined with Theorem 1 stating the security of our construction of a quantum-proof non-malleable extractor, Theorem 3 provides a means to obtain privacy amplification protocol secure against active attacks for a range of parameters. Due to the limitations of our non-malleable extractor we are only able to extract from sources whose entropy rate is at least $\frac{1}{2}$. This is a typical setting in the case of quantum key distribution, where the initial min-entropy satisfies $H_{\min}(X|E) \geq \alpha \log d_X$ for some constant α which depends on the protocol and the noise tolerance, but is generally larger than $3/4$. Specifically, we obtain the following:

Corollary 1. *For any $\epsilon > 0$, there exists a constant $c > 0$, such that the following holds. For any active attack (ρ_{XE}, T_1, T_2) such that $H_{\min}(X|E)_\rho = k \geq \frac{1}{2} \log d_X + c \cdot \log(1/\epsilon)$, there is an $O(\epsilon)$-secure DW protocol that outputs a key of length $m = k - O(\log(1/\epsilon))$.*

Proof. Let p be a prime and n a positive integer such that $\log p = \Theta(\log(1/\epsilon))$ and $d_X = p^n$. Let $d_Y = p^{n/2}$, and $d_Z = p$. Also, let $d_2 = O(\log d_X)$, $m = k - O(\log(1/\epsilon))$, and $t = O(\log(1/\epsilon))$. We instantiate Theorem 3 with the following.

- Let $\mathrm{Ext} : \{0,\ldots,d_X - 1\} \times \{0,1\}^{d_2} \to \{0,1\}^m$ be the $(k - O(\log(1/\epsilon)), \epsilon)$ strong quantum-proof extractor from Theorem 2.
- Let $\mathrm{nmExt} : \{0,\ldots,d_X - 1\} \times \{0,,\ldots,d_Y - 1\} \to \{0,\ldots,d_Z - 1\}$ be the $(\frac{1}{2} \cdot \log d_X + O(\log(1/\epsilon)), \epsilon)$ non-malleable extractor from Theorem 1.
- Let $\mathrm{MAC} : \{0,\ldots,d_Z - 1\} \times \{0,1\}^{d_2} \to \{0,1\}^t$ be the one-time ϵ-information-theoretically secure message authentication code from Proposition 1.

The result follows. □

5.2 One-round Privacy Amplification Protocol

In this section we show that the one-round protocol of Dodis et al. [16] is also quantum-proof. This protocol has significantly higher entropy loss, $(n/2) + \log(1/\epsilon)$, than the DW protocol we presented in the previous section.

One-round Privacy Amplification Protocol

Let n, k be integers and $\epsilon > 0$. Let $v = n - k + \log(1/\epsilon)$ and $m = (n/2) - v$.

It is assumed that both parties, Alice and Bob, have access to a shared random variable $X \in \{0,1\}^n$. They interpret X as a pair $X = (X_1, X_2)$ where X_1, X_2 are identified as elements in $\mathbb{F}_{2^{n/2}}$.

1. Alice samples a Y uniformly from $\mathbb{F}_{2^{n/2}}$ and computes $Z = YX_1 + X_2$. Let $W = [Z]_1^v$ be the first v bits of Z. She sends (Y, W) to Bob and outputs $R_A = [Z]_{v+1}^{n/2}$, the remaining part of Z.
2. Bob receives (Y', W') from Alice and computes $Z' = Y'X_1 + X_2$. If $W' = [Z']_1^v$, then Bob outputs $R_B = [Z']_{v+1}^{n/2}$. Otherwise he outputs $\perp$.

Fig. 5.2. The one-round privacy amplification protocol from [16].

Theorem 4. *For any integer n and $k > n/2$, and any $\epsilon > 0$, the protocol in Figure 5.2 is a one-round (k, m, ϵ)-quantum secure privacy amplification protocol with post-application robustness and entropy loss $k - m = (n/2) + \log(1/\epsilon)$.*

Proof. Correctness and extraction follow as in the classical proof by observing that $\mathrm{Ext}(X,Y) = YX_1 + X_2$ is a quantum-proof extractor since $h_Y(X_1, X_2) = YX_1 + X_2$ is a family of universal hash function, which is shown to be a quantum-proof strong extractor in [36]. For robustness, the classical proof does not generalize directly. We prove post-application robustness as follows.

We proceed by contradiction. Suppose post-application robustness is violated, i.e. $\Pr[R_A \neq R_B \wedge\ R_A \neq \perp\ \wedge R_B \neq \perp] > \epsilon$. Then there is an initial state ρ_{XE} with

$H_{\min}(X|E)_\rho \geq k$ and a CPTP map $T : \mathrm{L}(\mathcal{H}_Y \otimes \mathcal{H}_W \otimes \mathcal{H}_{R_A} \otimes \mathcal{H}_E) \to \mathrm{L}(\mathcal{H}_Y \otimes \mathcal{H}_W \otimes \mathcal{H}_{E'})$ that can be applied by an adversary Eve to produce a modified message that is accepted by Bob with probability greater than ϵ. Note that T has R_A as input since we consider post-application robustness. Let $(Y', W', E') = T(Y, W, R_A, E)$. If post-application robustness is violated, then $\Pr[W' = [Y'X_1 + X_2]_1^v] > \epsilon$.

Consider the following communication game: Alice has access to a cq-state ρ_{XE}. Alice samples a uniformly random Y, computes $W = [YX_1 + X_2]_1^v$, $R_A = [YX_1 + X_2]_{v+1}^{n/2}$, and sends E, Y, W, and R_A to Bob. They win if Bob guesses X correctly from E, Y, W, and R_A. Using the map T introduced above, Bob can execute the following strategy. First, apply T on Alice's message to generate a guess (Y', W'). Second, guess a uniformly random R'_B. Third, use $Y, Y', (W, R_A) = YX_1 + X_2$, and $(W', R'_B) = Y'X_1 + X_2$ to solve for a unique $X = (X_1, X_2)$. Note that Bob succeeds if the guesses (Y', W') and R'_B in the first two steps are both correct (i.e., $(W', R'_B) = Y'X_1 + X_2$), which has probability greater than $\epsilon \cdot 2^{-((n/2)-v)}$. On the other hand, we can upper bound the winning probability of the communication game using the min entropy assumption $H(X|E)_\rho \geq k$. Since Y is independent of X and the length of (W, R_A) is $n/2$, $H_{\min}(X|E, Y, W)_\rho \geq k - (n/2)$. Thus the winning probability is less than $2^{-(k-(n/2))}$. Putting the two calculations together we have

$$\epsilon \cdot 2^{-((n/2)-v)} \leq \Pr[\text{ Bob wins }] \leq 2^{-(k-(n/2))},$$

which implies $v < n - k - \log(1/\epsilon)$, a contradiction. □

References

1. Divesh Aggarwal, Kai-Min Chung, Han-Hsuan Lin, and Thomas Vidick. A quantum-proof non-malleable extractor, with application to privacy amplification against active quantum adversaries. *arXiv preprint arXiv:1710.00557*, 2017.
2. Divesh Aggarwal, Yevgeniy Dodis, Zahra Jafargholi, Eric Miles, and Leonid Reyzin. Amplifying privacy in privacy amplification. In *Advances in Cryptology - CRYPTO 2014 - 34th Annual Cryptology Conference, Santa Barbara, CA, USA, August 17-21, 2014, Proceedings, Part II*, pages 183–198, 2014.
3. Divesh Aggarwal, Kaave Hosseini, and Shachar Lovett. Affine-malleable extractors, spectrum doubling, and application to privacy amplification. In *Information Theory (ISIT), 2016 IEEE International Symposium on*, pages 2913–2917. Ieee, 2016.
4. Charles H. Bennett, Gilles Brassard, Claude Crépeau, and Ueli M. Maurer. Generalized privacy amplification. *IEEE Transactions on Information Theory*, 41(6):1915–1923, 1995.
5. Charles H. Bennett, Gilles Brassard, and Jean-Marc Robert. Privacy amplification by public discussion. *SIAM Journal on Computing*, 17(2):210–229, 1988.
6. Rajendra Bhatia. *Matrix Analysis*. Graduate Texts in Mathematics, Springer, 1997.
7. Niek J. Bouman and Serge Fehr. Secure authentication from a weak key, without leaking information. In *Advances in Cryptology - EUROCRYPT 2011 - 30th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Tallinn, Estonia, May 15-19, 2011. Proceedings*, pages 246–265, 2011.
8. Nishanth Chandran, Bhavana Kanukurthi, Rafail Ostrovsky, and Leonid Reyzin. Privacy amplification with asymptotically optimal entropy loss. In *Proceedings of the 42nd ACM Symposium on Theory of Computing, STOC 2010, Cambridge, Massachusetts, USA, 5-8 June 2010*, pages 785–794, 2010.

9. Eshan Chattopadhyay, Vipul Goyal, and Xin Li. Non-malleable extractors and codes, with their many tampered extensions. *arXiv preprint arXiv:1505.00107*, 2015.
10. Kai-Min Chung, Xin Li, and Xiaodi Wu. Multi-source randomness extractors against quantum side information, and their applications. 2014.
11. Richard Cleve, Wim van Dam, Michael Nielsen, and Alain Tapp. Quantum entanglement and the communication complexity of the inner product function. In *Williams C.P. (eds) Quantum Computing and Quantum Communications. Lecture Notes in Computer Science*, volume 1509, pages 61–74. Springer, Berlin, Heidelberg, 1999.
12. Gil Cohen. Non-malleable extractors - new tools and improved constructions. *Electronic Colloquium on Computational Complexity (ECCC)*, 22:183, 2015.
13. Gil Cohen, Ran Raz, and Gil Segev. Non-malleable extractors with short seeds and applications to privacy amplification. In *Computational Complexity (CCC), 2012 IEEE 27th Annual Conference on*, pages 298–308. IEEE, 2012.
14. Gil Cohen and Thomas Vidick. Privacy amplification against active quantum adversaries. 2016.
15. Anindya De, Christopher Portmann, Thomas Vidick, and Renato Renner. Trevisan's extractor in the presence of quantum side information. 41(4):915–940, 2012.
16. Yevgeniy Dodis, Bhavana Kanukurthi, Jonathan Katz, Leonid Reyzin, and Adam Smith. Robust fuzzy extractors and authenticated key agreement from close secrets. *IEEE Transactions on Information Theory*, 58(9):6207–6222, 2012.
17. Yevgeniy Dodis, Xin Li, Trevor D. Wooley, and David Zuckerman. Privacy amplification and nonmalleable extractors via character sums. *SIAM J. Comput.*, 43(2):800–830, 2014.
18. Yevgeniy Dodis and Prashant Puniya. Feistel networks made public, and applications. In Moni Naor, editor, *Advances in Cryptology - EUROCRYPT 2007*, volume 4515 of *Lecture Notes in Computer Science*, pages 534–554. Springer-Verlag, 2007.
19. Yevgeniy Dodis and Daniel Wichs. Non-malleable extractors and symmetric key cryptography from weak secrets. In Michael Mitzenmacher, editor, *Proceedings of the 41st Annual ACM Symposium on Theory of Computing*, pages 601–610, Bethesda, MD, USA, 2009. ACM.
20. Yevgeniy Dodis and Yu Yu. Overcoming weak expectations. In *TCC*, pages 1–22, 2013.
21. Dmitry Gavinsky, Julia Kempe, Iordanis Kerenidis, Ran Raz, and Ronald De Wolf. Exponential separations for one-way quantum communication complexity, with applications to cryptography. In *Proceedings of the thirty-ninth annual ACM symposium on Theory of computing*, pages 516–525. ACM, 2007.
22. Roy Kasher and Julia Kempe. Two-source extractors secure against quantum adversaries. *Theory of Computing*, 8(1):461–486, 2012.
23. Robert Koenig, Renato Renner, and Christian Schaffner. *IEEE Transactions on Information Theory*, 55(9), 2009.
24. Chia-Jung Lee, Chi-Jen Lu, Shi-Chun Tsai, and Wen-Guey Tzeng. Extracting randomness from multiple independent sources. *IEEE Transactions on Information Theory*, 51(6):2224–2227, 2005.
25. Xin Li. Design extractors, non-malleable condensers and privacy amplification. In *Proceedings of the 44th Symposium on Theory of Computing Conference, STOC 2012, New York, NY, USA, May 19 - 22, 2012*, pages 837–854, 2012.
26. Xin Li. Non-malleable condensers for arbitrary min-entropy, and almost optimal protocols for privacy amplification. *CoRR*, abs/1211.0651, 2012.
27. Xin Li. Non-malleable extractors, two-source extractors and privacy amplification. In *FOCS*, pages 688–697, 2012.
28. Xin Li. Non-malleable condensers for arbitrary min-entropy, and almost optimal protocols for privacy amplification. In *Theory of Cryptography - 12th Theory of Cryptography Confer-*

ence, TCC 2015, Warsaw, Poland, March 23-25, 2015, Proceedings, Part I, pages 502–531, 2015.
29. Xin Li. Improved non-malleable extractors, non-malleable codes and independent source extractors. In *Proceedings of the 49th Annual ACM SIGACT Symposium on Theory of Computing, STOC 2017, Montreal, QC, Canada, June 19-23, 2017*, pages 1144–1156, 2017.
30. Ueli Maurer. Conditionally-perfect secrecy and a provably-secure randomized cipher. *Journal of Cryptology*, 5(1):53–66, 1992.
31. Ueli Maurer and Stefan Wolf. Privacy amplification secure against active adversaries. In Burton S. Kaliski, Jr., editor, *Advances in Cryptology—CRYPTO '97*, volume 1294 of *LNCS*, pages 307–321. Springer-Verlag, 1997.
32. Ashwin Nayak and Julia Salzman. Limits on the ability of quantum states to convey classical messages. *Journal of the ACM (JACM)*, 53(1):184–206, 2006.
33. Noam Nisan and David Zuckerman. Randomness is linear in space. *Journal of Computer and System Sciences*, 52(1):43–53, 1996.
34. Renato Renner and Robert König. Universally composable privacy amplification against quantum adversaries. In *Theory of Cryptography*, pages 407–425. Springer, 2005.
35. Renato Renner and Stefan Wolf. Unconditional authenticity and privacy from an arbitrarily weak secret. In Dan Boneh, editor, *Advances in Cryptology—CRYPTO 2003*, volume 2729 of *LNCS*, pages 78–95. Springer-Verlag, 2003.
36. Marco Tomamichel, Christian Schaffner, Adam D. Smith, and Renato Renner. Leftover hashing against quantum side information. *IEEE Trans. Information Theory*, 57(8):5524–5535, 2011.
37. Alexander Vitanov, Frederic Dupuis, Marco Tomamichel, and Renato Renner. Chain rules for smooth min-and max-entropies. *Information Theory, IEEE Transactions on*, 59(5):2603–2612, 2013.

A The Dodis-Wichs Protocol

In this appendix we reproduce the proof of Theorem 3, taken from [14].

Proof of Theorem 3. Let an *active attack* on Protocol DW be specified by

- A cq state $\rho_{XE} \in \mathrm{D}(\mathcal{H}_X \otimes \mathcal{H}_E)$ such that $H_{\min}(X|E)_\rho \geq k$;
- A CPTP map $T_1 : \mathrm{L}(\mathcal{H}_Y \otimes \mathcal{H}_E) \to \mathrm{L}(\mathcal{H}_Y \otimes \mathcal{H}_{E'})$ whose output on the first registered is systematically decohered in the computational basis; formally, for any ρ_{YE}, $T_1(\rho_{YE}) = \sum_y (|y\rangle\langle y|_Y \otimes \mathrm{Id}_E) T_1(\rho_{YE}) (|y\rangle\langle y|_Y$
$\otimes \mathrm{Id}_E)$;
- A CPTP map $T_2 : \mathrm{L}(\mathbb{C}^{2^{d_2}} \otimes \mathbb{C}^{2^t} \otimes \mathcal{H}_{E'}) \to \mathrm{L}(\mathbb{C}^{2^{d_2}} \otimes \mathbb{C}^{2^t} \otimes \mathcal{H}_{E''})$.

Given an active attack (ρ_{XE}, T_1, T_2) we instantiate random variables Y_A, Z, Y'_A, Y_B, Z', σ, Y'_B, σ' and R_A, R_B in the obvious way, as defined in the protocol and taking into account the maps T_1 and T_2, applied successively to determine Y'_A and (Y'_B, σ').

The correctness of the protocol is clear.

To show robustness, let $\sigma_{Y'_A Y_A XE'}$ denote the joint state of Y'_A, Y_A (which represents a local copy of Y_A kept by Alice), X, and Eve's registers after her first map T_1 has been applied. Further decompose ρ as a sum of sub-normalized densities $\sigma^{=}_{Y'_A Y_A XE'}$, corresponding to conditioning on $Y'_A = Y_A$, and $\sigma^{\perp}_{Y'_A Y_A XE'}$, corresponding to conditioning on $Y'_A \neq Y_A$.

Conditioned on $Y'_A = Y_A$, by definition of a MAC the probability that $(Y'_B, W') \neq (Y_B, W)$ and Alice reaches the KeyConfirmed state is at most ϵ_{MAC}. If $(Y'_B, W') = (Y_B, W)$ then $R_A = R_B$, so that in this case robustness holds with error at most ϵ_{MAC}.

Now suppose $Y'_A \neq Y_A$. Consider a modified adversary Adv' that keeps a copy of Y_A, applies the map T_1, and if $Y'_A = Y_A$ replaces Y'_A with a uniformly random string that is distinct from Y_A. This adversary implements a CPTP map T'_1 that has no fixed point. By the assumption that nmExt is a quantum-proof non-malleable extractor,

$$\sigma'_{\mathrm{nmExt}(X,Y_A)\mathrm{nmExt}(X,Y'_A)Y_A Y'_A E'} \approx_{\epsilon_{\mathrm{nmExt}}} U_m \otimes \sigma'_{\mathrm{nmExt}(X,Y'_A)Y_A Y'_A E'}, \tag{A.1}$$

where here $Y'_A E'$ is defined as the output system of the map T'_1 implemented by Adv'. Conditioned on $Y_A \neq Y'_A$ the maps T_1 and T'_1 are identical, thus it follows from (A.1) and the definition of $\rho^{\perp}$ that

$$\sigma^{\perp}_{\mathrm{nmExt}(X,Y_A)\mathrm{nmExt}(X,Y'_A)Y_A Y'_A E'} \approx_{\epsilon_{\mathrm{nmExt}}} U_m \otimes \sigma^{\perp}_{\mathrm{nmExt}(X,Y'_A)Y_A Y'_A E'},$$

where now the states are sub-normalized. Since $Z' = \mathrm{nmExt}(X, Y'_A)$ this means that the key used by Alice to verify the signature in Step 3. of Protocol DW is (up to statistical distance $\epsilon_{\mathrm{nmExt}}$) uniform and independent of the key used by Bob to make the MAC. By the security of MAC, the probability for Alice to reach the KeyConfirmed state in this case is at most $\epsilon_{\mathrm{nmExt}} + \epsilon_{\mathrm{MAC}}$. Adding both parts together, $\Pr(R_A \notin \{R_B, \perp\}) \leq \epsilon_{\mathrm{nmExt}} + 2\epsilon_{\mathrm{MAC}}$. Since R_B is never $\perp$, this implies the robustness property.

For the extraction property, it is sufficient to show that $(R_B, V, E) \approx_{\epsilon} (U_m, V, E)$ since then key extraction property follows from the robustness and the fact that R_B is never $\perp$. We have that $R_B = \mathrm{Ext}(X, Y_B)$ is close to uniform given $V = Y_A Y_B W$ and E', and we need to establish two properties: first, independence between X and Y_B given $Y_A Z' E'$ and second, that the source has enough entropy conditioned on $Y_A Z' E'$. Regarding the first property, observe that conditioned on $Y_A Z'$, X and Y_B are independent given E'. Regarding the source entropy, by the chain rule for the (smooth) min-entropy [37], it follows that $H_{\min}^{\epsilon_{\mathrm{Ext}}}(X|Y_A Z' E') \geq k - \log d_Z - c \log(1/\epsilon_{\mathrm{Ext}})$ for some constant $c > 0$. Note that

$$\left\|(R_B, V, E')_{\sigma} - (U_m, V, E')_{\sigma}\right\|_1 \leq \left\|(R_B, Y_A, Y_B, Z', E')_{\sigma} - (U_m, Y_A, Y_B, Z', E')_{\sigma}\right\|_1,$$

which follows since W is a deterministic function Y_B and Z'. Using that Ext is a strong quantum-proof extractor, we conclude that $(R_B, V, E) \approx_{\epsilon} (U_m, V, E)$, as long as ϵ is such that $\epsilon > \epsilon_{\mathrm{Ext}}$.

□