

Quantum hashing is maximally secure against classical leakage

Cupjin Huang and Yaoyun Shi

Department of Electrical Engineering and Computer Science
University of Michigan, Ann Arbor, MI 48109, USA
cupjinh, shiyy@umich.edu

Abstract

Cryptographic hash functions are fundamental primitives widely used in practice. For such a function $f : \{0, 1\}^n \rightarrow \{0, 1\}^m$, it is nearly impossible for an adversary to produce the hash $f(x)$ without knowing the secret message $x \in \{0, 1\}^n$. Unfortunately, all hash functions are vulnerable under the side-channel attack, which is a grave concern for information security in practice. This is because typically $m \ll n$ and an adversary needs only m bits of information to pass the verification test.

In sharp contrast, we show that when quantum states are used, the leakage allowed can be almost the entire secret. More precisely, we call a function that maps n bits to m qubits a quantum cryptographic function if the maximum fidelity between two distinct hashes is negligible in n . We show that for any $k = n - \omega(\log n)$, all quantum cryptographic hash functions remain cryptographically secure when leaking k bits of information. By the quantum fingerprinting constructions of Buhrman et al. (*Phys. Rev. Lett.* 87, 167902), for all $m = \omega(\log n)$, there exist such quantum cryptographic hash functions. We also show that one only needs $\omega(\log^2 n)$ qubits to verify a quantum cryptographic hash, rather than the whole classical information needed to generate one.

Our result also shows that to approximately produce a small amount of quantum side information on a classical secret, it may require almost the full information of the secret. This large gap represents a significant barrier for proving quantum security of classical-proof extractors.

1 Introduction

1.1 The problem and the motivation

Cryptographic hash functions are a fundamental primitive used widely in today’s cryptographic systems. They are considered “workhorses of modern cryptography”¹ For simplicity, we focus our discussions on *keyless* (cryptographic) hash functions, each of which is an efficiently computable function h from some message space \mathcal{M} to some *digest space* \mathcal{T} [6, 22, 23]. Ideally, we want the hash function to have the following properties. First, the digest should be much shorter than the message. Depending on applications, the following security properties are desirable [23]. (1) *Collision resistant*: It is computationally infeasible to find a “collision”, i.e., two distinct messages x and x' , such that $h(x) = h(x')$. (2) *Preimage Resistance*: It is computationally infeasible to invert h . (3) *Second Preimage Resistance*: Given a message x , it should be computational infeasible to $x' \neq x$ with $h(x') = h(x)$.

Prominent examples of widely used cryptographic hash functions include SHA-256 and SHA-512, part of the SHA-2 algorithms that were designed by NSA and are US Federal Standards. These algorithms are used in UNIX and LINUX for secure password hashing, in Bitcoin for proof-of-work. As a motivating example, we consider how proof-of-work can be carried out through hash. Suppose that Alice receives a trove of valuable documents $x \in \{0, 1\}^n$, and Bob claims that he was the person producing and sending it. To prove his claim, he sends Alice a tag $t \in \{0, 1\}^m$, which supposedly is the result of applying a cryptographic hash function $h : \{0, 1\}^n \rightarrow \{0, 1\}^m$ on x . Alice simply checks if $t = h(x)$. Accept if yes, reject otherwise. By the collision resistance property, it is nearly impossible that Bob can produce $h(x)$ without knowing x .

In practice, there may be information leakage of the message over time due to information transmission, adversarial attacks, etc. Therefore, it is rather desirable if the hash function is resilient against information leakage. We ask: how many bits ℓ about the message x can be leaked before the adversary is able to forge the tag $h(x)$ easily?

Clearly, $\ell \leq m$, since if the tag $h(x)$ itself is known to the adversary, he does not need to know more about x to pass the verification. This is rather disappointing, since m is typically much smaller than n . We then ask: what if a quantum tag is used instead? If the leakage is quantum, by the same reasoning, m remains a trivial and rather lower upper-bound on ℓ . This leads us to our central question: *Can a quantum hash function be much more resilient to classical leakage?*

1.2 Quantum cryptographic hash functions

By a “quantum hash function,” we simply mean a classical-to-quantum encoding $\phi : \{0, 1\}^n \rightarrow \mathbb{C}^{2^m}$ that maps $x \in \{0, 1\}^n$ to a pure m -qubit state $|\phi_x\rangle$. In a seminal paper, Buhrman et al. [8] introduced the notion of *quantum fingerprinting*. In their most general form, a quantum fingerprinting is the following.

Definition 1 (Generalized Quantum Fingerprinting (Buhrman et al. [8])). *A function $\phi : \{0, 1\}^n \rightarrow \mathbb{C}^{2^m}$ is a (n, m, δ) (generalized) quantum fingerprinting where $\delta := \max_{x, x': x \neq x'} |\langle \phi_x | \phi_{x'} \rangle|$.*

We use the convention that $\phi := |\phi\rangle\langle\phi|$ represent the projector for the pure state $|\phi\rangle$. If one replaces the predicate $h(x) = h(x')$ by the fidelity $F(\phi_x, \phi_{x'}) = |\langle \phi_x | \phi_{x'} \rangle|$, one sees that δ precisely quantify the extent of collision resistance. For concreteness, we define what we mean by quantum cryptographic hash function as follows. For a function $\delta_n \in (0, 1)$, we say δ_n is negligible in n if $\delta_n \leq 1/n^c$ for all $c > 0$ and all sufficiently large n .

¹Bob Schneier, https://www.schneier.com/essays/archives/2004/08/cryptanalysis_of_md5.html.

Definition 2. A (n, m, δ) quantum fingerprinting ϕ is a quantum cryptographic hash function if $\delta = \text{negl}(n)$.

We note that while classical cryptographic hash functions necessarily rely on computational assumptions for security, their quantum counterparts can achieve the three security properties (1-3) information-theoretically. We now proceed to formulate our leakage problem precisely. We consider average case security and model classical side-channel information using a classical-classical (c-c) state, called the *side information state*, $\eta_{XY} := \sum_{x,y} p_{x,y} |x\rangle\langle x| \otimes |y\rangle\langle y|$ on $\{0, 1\}^n \times \{0, 1\}^{n'}$. Here X is uniformly distributed and Y represents the side information. The largest probability of correctly guessing X conditioned on Y is $p_g := p_g(X|Y)_\eta := \sum_y \max_x p_{x,y}$. The *conditional min-entropy* is $H_{\min}(X|Y)_\eta := -\log p_g(X|Y)_\eta$. We quantify the amount of leakage by $k := n - H_{\min}(X|Y)_\eta$.

The adversary is given the Y sub-system and creates a classical-quantum (cq) state ρ_{XE} , called the *forgery state*, through local quantum operations on Y . The *verification scheme* for ϕ is the following measurement on XE : $V := \sum_x |x\rangle\langle x| \otimes \phi_x$. The probability of the forgery state to pass the verification scheme is $e_s := \text{Tr}(V\rho)$. Given the leakage ℓ , the optimal passing probability of a forgery state is denoted by $e_s^* := e_s^*(\ell)$. We can now define security precisely.

Definition 3 (Resilience against classical leakage). A (n, m, δ) quantum cryptographic hash function ϕ is said to be σ -resilient against ℓ bits of classical leakage if for all forgery state ρ obtained from ℓ bits of side information, the probability of passing the verification scheme $e_s^*(\ell) \leq \sigma$. If no σ is specified, it is assumed that $\sigma = \text{negl}(n)$.

1.3 Main Result

We show that quantum cryptographic hash functions can be extremely resilient to classical leakage. Our main theorem is informally stated below.

Theorem 1.1 (Main Theorem). For all n and $k = n - \omega(\log n)$, all quantum cryptographic hash functions are resilient against k bits of classical leakage.

Buhrman et al. [8] showed that for all n and $\delta \in (0, 1)$, there exists a (n, m, δ) quantum fingerprinting for $m = \log n + O(\log 1/\delta)$ for which explicit constructions can be derived from [17]. We thus have the following corollary.

Corollary 1.2. For all n , $k = n - \omega(\log n)$, and $m = \omega(\log n)$, there exist efficient quantum cryptographic hash functions resilient to leaking k bits of information.

One drawback of the verification scheme is that the verifier has to get access to full information about the original message X in order to perform the verification. In some cases this would be a heavy burden on the verifier. One natural question to ask is that if it is possible to develop a lightweighted verification scheme where the verifier does not need to read the whole message. More formally, let the verifier now receive k qubits of *advice state* and m bits of the *forgery state* provided by the adversary. An (n, k, m) verification scheme V would then be a joint measurement on the advice state together with the forgery state. This generalizes the original verification where $k = n$ and $V = \sum_x |x\rangle\langle x| \otimes \phi_x$.

Our next result shows that, by increasing the hash a little bit we can dramatically reduce the size of system needed by the verifier:

Theorem 1.3. For all n , fix $k = m = \omega(\log^2 n)$, $\ell \leq n - \omega(\log n)$. There exists a verification scheme V acting on $k + m$ qubits, together with an ensemble of k -qubit states $\{\rho_x\}$ such that

$$\sup_{Y: H_{\min}(X|Y) \leq \ell} \sup_{\{\sigma_Y\}} \mathbb{E}_{XY} \text{Tr}[V(\rho_X \otimes \sigma_Y)] \leq \text{negl}(n).$$

Arunachalam et al. [3] showed that $\Omega(n)$ copies of a quantum cryptographic hash based on linear codes is necessary to recover the original n -bit classical message, regardless of the length of the hash itself. Our result shows the complimentary aspect that only $\omega(\log n)$ copies are sufficient to ensure that the prover holds the classical message.

Our central technical result is the following. Recall that $p_g := 2^{\ell-n}$ is the optimal guessing probability of the message conditioned on the ℓ -bit side information.

Lemma 1.4 (Lemma 4.1, informally stated). *For any (n, m, δ) quantum fingerprinting ϕ and any leakage of ℓ classical bits, the probability of the forgery state passing the verification scheme satisfies*

$$e_s \leq p_g + \delta.$$

This implies that

$$O(p_g + \delta^2) \leq e_s^* \leq p_g + \delta, \tag{1.1}$$

by considering the two cheating strategies of guessing X first (then applying ϕ) and using a fixed fingerprint state. Consequently, when $\delta = \text{negl}(n)$, the above inequality means that e_s^* is negligible if and only if p_g is negligible.

Since $\ell = n - O(\log n)$ is the threshold for $p_g(\ell)$ to be non-negligible, the bounds (1.1) show for quantum cryptographic hash functions, the leakage resilience can approach the *maximum* of $n - O(\log n)$ bits.

One counterpart of this result is shown in [3], saying that $\Omega(n)$ copies of quantum fingerprints would be necessary for an adversary to recover the original message with non-negligible probability. Thus, the quantum cryptographic hash functions based on fingerprinting have the following property: The hash itself is efficiently computable, but it is information-theoretically resilient to recovery of the message from the hash (which requires $\Omega(n)$ copies of the hash) and to recovery of the hash from partial information of the message.

1.4 Implications on quantum-proof randomness extraction

Our result reveals some stark contrast between quantum and classical side information. This difference shows the difficulty for establishing the quantum security of classical-proof extractors. Roughly speaking, a randomness extractor is a randomized algorithm which turns a weakly random source into near uniform [20, 21, 26]. These are fundamental objects with a wide range of applications in computational complexity, cryptography, and other areas [5, 10, 12, 25, 16]. In particular, they accomplish the important tasks of privacy amplification [4, 5, 15], by decoupling the correlation between the output and the side information.

A major open problem in randomness extraction is whether every classical-proof randomness extractor for k min-entropy sources is secure against quantum adversaries with comparable amount but quantum side information. Loss of parameter is already shown to be inevitable in [11], but possibilities still remain in the case where the ranges of parameters are relevant to most typical applications.

If all quantum side information can be constructed from a comparable amount of classical side information, we would have resolved this major problem positively. Our result shows that this approach would necessarily fail. For details, see Section 6.

Theorem 1.5 (Theorem 6.2, informally stated). *There exists a family of classical-quantum states with arbitrarily small amount of quantum side information, yet these quantum states cannot be approximately constructed from classical side information that is almost a perfect copy of the classical message.*

1.5 Sketch of Proofs

To prove Separation Lemma 1.4, we first answered the following question (see Section 3): *Given a c - q state, how much classical side information is needed to approximate it up to a given error ϵ ?* It turns out that this quantity, denoted by the *conversion parameter*, can be simplified to a fairly nice expression. An important step is to show (in Lemma 3.2) that classical information can without loss of generality be identifying a subset of the messages, and conditioned on this information, the messages are uniformly distributed on that subset. At the end, the proof reduces to estimating the operator norm of $\sum_i T_i$, where T_i 's are projections to the fingerprint states, thus pairwise almost orthogonal. Cotlar-Stein Lemma gives us the desired bound.

1.6 Related works.

As mentioned above, Buhrman et al. [8] introduced the notion and provide the constructions of quantum fingerprinting. The application they focused on is for message identification. For our cryptographic applications, we are primarily interested in instances of a negligible fidelity. They did not discuss properties of quantum fingerprinting in an adversarial context like ours. That quantum fingerprinting satisfies the security properties of cryptographic hash functions was observed and explored by [1, 27].

Side-channel attack is a major paradigm studied in the classical information security and cryptography community due to its high level of threat in practice [24, 18, 2, 9, 7, 13]. Side-channel key recovery attack has in particular drawn much attention [24]. However, these classical works address problems that necessarily require computational assumptions and many other works focus on the hardware aspects. To the best of our knowledge, this work appears to be the first studying information theoretical security of quantum cryptography against classical side-channel attack.

2 Preliminaries

In the subsequent subsections, we summarize the necessary background on quantum information, probability theory and operator theory. We assume that readers are familiar with linear algebra. We refer to [19] for more detailed knowledge on quantum information and quantum computation.

2.1 Quantum Information

Quantum States. The state space of a k -qubit system can be characterized as a 2^k -dimensional Hilbert space $\mathcal{H} \cong \mathbb{C}^{2^k}$. A k -qubit quantum state is described by a density operator ρ on \mathcal{H} , i.e. a positive semidefinite operator with unit trace. We often use $\rho \succcurlyeq 0$ to denote that ρ is positive semidefinite. The set of all density matrices on \mathcal{H} is then denoted by $\mathcal{S}_=(\mathcal{H}) := \{\rho \succcurlyeq 0 | \text{Tr}[\rho] = 1\}$. Sometimes we are also interested in the set of subnormalized states $\mathcal{S}_\leq(\mathcal{H}) := \{\rho \succcurlyeq 0 | \text{Tr}[\rho] \leq 1\}$.

Let $L(\mathcal{H})$ denote the set of all linear operators on \mathcal{H} onto itself. For two operators $A, B \in L(\mathcal{H})$, one can define the inner product $\langle A, B \rangle$ to be $\text{Tr}[A^\dagger B]$, A^\dagger being the adjoint conjugate of A . Also we denote the identity operator by I .

The state space for a multipartite system is the tensor of the state space of each individual system, i.e. a general multipartite state ρ_{ABC} can be described by a density operator in $\mathcal{S}_=(\mathcal{A} \otimes \mathcal{B} \otimes \mathcal{C})$. For such a state ρ , the marginal state on a subsystem, say ρ_A , is the partial trace over the other subsystems, namely $\rho_A = \text{Tr}_{BC}[\rho_{ABC}]$.

A *classical-quantum*-, or cq-state is a state of the form

$$\rho_{XE} = \sum_x |x\rangle\langle x| \otimes \rho_x,$$

where $\{|x\rangle\}$ are orthonormal and ρ_x 's are subnormalized states which sum up to a density matrix. This is to say, the bipartite state ρ_{XE} is classical on the X side while quantum on the E side. Furthermore, if the E side is also classical, then the state is of the form

$$\rho_{XE} = \sum_{x,y} p(x,y) |x\rangle\langle x| \otimes |y\rangle\langle y|.$$

Such a state is called a *classical-classical*- or cc-state. Note that cc-states can be identified as classical joint distributions.

Quantum Measurement. The most general type of quantum measurement is *Positive-operator-valued measurement (POVM)*. A POVM is a set of measurements $\mathcal{M} = \{M_o\}_{o \in O}$, where O is the set of all outcomes, M_o is positive semidefinite for all o and $\sum_{o \in O} M_o = I$. For a state ρ , the probability that the outcome is o under the measurement \mathcal{M} is $\text{Tr}[M_o \rho]$.

Quantum Channel. A physically realizable quantum channel $\mathcal{C}_{A \rightarrow B}$ is a completely positive, trace preserving linear map from $L(\mathcal{A})$ to $L(\mathcal{B})$.

Sometimes we may consider more restrictive quantum channels, such as classical-to-quantum channels and classical-to-classical channels (note that quantum-to-classical channels can be identified as measurements). A classical-to-quantum channel $\mathcal{C}_{A \rightarrow B}$ can be written as

$$\mathcal{C}(\cdot) = \sum_a \langle a | \cdot | a \rangle \cdot \rho_a,$$

where $\rho_a \in \mathcal{S}_=(\mathcal{B})$. When B is also classical, the channel coincides with the standard definition of a channel in classical information theory, specified by the conditional distribution $p_{B|A}$.

2.2 Probability Theory

Random Source. A distribution X over a finite set \mathcal{X} is also called a random source in this work. Specifically, denote $U_{\mathcal{X}}$ the uniform distribution over the set \mathcal{X} . For a random source X , we can define *support set*

$$\text{Supp}(X) := \{x \in \mathcal{X} \mid \Pr[X = x] > 0\},$$

and *guessing probability*

$$p_g(X) = \max_x \Pr[X = x].$$

The operational definition of guessing probability is as follows: if one is asked to guess the value generated by the random source X without any side information, the optimal strategy is to guess the most probable one, and the winning probability would be $p_g(X)$.

Statistical Distance. For two distributions X_1, X_2 over a finite set \mathcal{X} , the statistical distance is defined to be

$$\Delta(X_1, X_2) := \frac{1}{2} \sum_x |\Pr[X_1 = x] - \Pr[X_2 = x]| = \max_{S \subseteq \mathcal{X}} \Pr[X_1 \in S] - \Pr[X_2 \in S].$$

The operational definition of statistical distance is as follows: if one is asked to tell whether a given message x is generated from source X_1 or X_2 , the success probability under optimal strategy is $\frac{1 + \Delta(X_1, X_2)}{2}$.

Random Source with Classical Side Information. For a joint distribution XY over a set $\mathcal{X} \otimes \mathcal{Y}$, the *guessing probability* of X conditioned on Y is given by

$$p_g(X|Y) := \mathbb{E}_{y \sim Y} p_g(X|Y = y) = \sum_y \max_x \Pr[X = x, Y = y].$$

This is to say, upon possessing classical side information y of the random source X , the optimal strategy to guess the value of X is simply guessing the most probable one conditioned on $Y = y$. The overall winning probability would then be $p_g(X|Y)$.

Quantum Random Source. Now suppose that the side information can be quantum, i.e. the random source X together with the quantum side information ρ_E form a classical-quantum (cq) state

$$\rho_{XE} = \sum_x |x\rangle\langle x| \otimes \rho_x,$$

where the X part is still classical while the E part can be quantum. Note that ρ_x 's are subnormalized and they sum up to a normalized state ρ_E . Then the guessing probability of X conditioned on E is defined as the guessing probability under an optimal POVM:

$$p_g(X|E)_\rho := \max_{\mathcal{M}_{E \rightarrow Y}} p_g(X|Y)_{(\mathcal{I} \otimes \mathcal{M})(\rho)}.$$

It can be shown using SDP duality that

$$p_g(X|E)_\rho = \min_{\sigma: \forall x, \sigma \succ \rho_x} \text{Tr}[\sigma].$$

When the number of qubits in the quantum side information is a small number k , we have the following bound for the guessing probability:

$$p_g(X|E) \leq p_g(X) \cdot 2^k.$$

2.3 Operator Theory

For an operator $K \in L(\mathcal{A})$, define the p -Schatten norm to be

$$\|K\|_p = \text{Tr} \left[(K^\dagger K)^{p/2} \right]^{1/p},$$

for all $1 \leq p < \infty$. Some concrete examples are as follows:

- $p = 1$, then

$$\|K\|_{tr} = \|K\|_1 = \text{Tr}[\sqrt{K^\dagger K}]$$

is called the *trace norm* of K . For two quantum states $\rho, \sigma \in \mathcal{S}_=(\mathcal{A})$, the *trace distance* $\|\rho - \sigma\|_{tr}$ is the maximum l_1 -distance of distributions obtained via any quantum measurement.

- $p = \infty$, then the ∞ -Schatten norm is defined to be

$$\|K\|_\infty = \lim_{p \rightarrow \infty} \|K\|_p.$$

This is also called the *operator norm*

$$\|K\|_{op} := \sup_{v \neq 0} \|Kv\| / \|v\|.$$

In the case that K is positive semidefinite, $\|K\|_\infty$ is the largest eigenvalue of K .

3 Characterizing the Smooth Conversion Parameter

Given a cq state ρ_{XE} , we are now interested in determining the least amount of classical correlation, measured by the *conversion parameter*, that one needs in order to generate ρ by applying a quantum channel on the side information.

Definition 4 (Conversion Parameter). *Let $\rho_{XE} \in \mathcal{S}_\leq(\mathcal{X} \otimes \mathcal{E})$ be a cq state. The conversion parameter of X conditioned on E is defined as*

$$p_\downarrow(X|E)_\rho := \min_{\substack{\eta_{XY}, \mathcal{C} \\ \mathcal{I} \otimes \mathcal{C}(\eta) = \rho}} p_g(X|Y)_\eta.$$

By monotonicity of guessing probability under quantum channels acting on the side information, we have $p_\downarrow(X|E)_\rho \geq p_g(X|E)_\rho$.

The definitions above would be less interesting if we do not allow the existence of an extra error term ϵ for the following reason. For a state ρ with the form

$$\rho_{XE} = \sum_x q_x |x\rangle\langle x| \otimes |\psi_x\rangle\langle \psi_x|,$$

where $|\psi_x\rangle$ for each x are distinct, the only classical side information to generate ρ losslessly would be the classical message itself; but if we allow that the generated state be ϵ -close to the desired state ρ , we may be able to approximate ρ using classical information with significantly lower guessing probability.

Definition 5 (Smooth Conversion Parameter). *Let $\epsilon \geq 0$ and $\rho_{XE} \in \mathcal{S}_=(\mathcal{X} \otimes \mathcal{E})$. Then the ϵ -smooth conversion parameter of X conditioned on E is defined as*

$$p_\downarrow^\epsilon(X|E)_\rho := \min_{\substack{\eta_{XY}, \mathcal{C} \\ \|\mathcal{I} \otimes \mathcal{C}(\eta) - \rho\|_{tr} \leq \epsilon}} p_g(X|Y)_\eta.$$

One may wonder if we can derive a good estimate of $p_{\downarrow}^{\epsilon}(X|E)_{\rho}$ for given parameter ϵ . Recall that for guessing probability $p_g(X|E)_{\rho}$, we have

$$p_g(X|E)_{\rho} = \min_{\sigma: \forall x, \sigma \succ \rho_x} \text{Tr}[\sigma]$$

by SDP duality of quantum guessing probability. Similarly, we can prove the following lemma for smooth conversion parameter:

Lemma 3.1. *Let $\epsilon \geq 0$ and $\rho_{XE} = \sum_x |x\rangle\langle x| \otimes \rho_x \in \mathcal{S}_{=}(\mathcal{X} \otimes \mathcal{E})$, then*

$$p_{\downarrow}^{\epsilon}(X|E)_{\rho} = \min_{\substack{p_S, \hat{\rho}_S \\ \sum_x \|\sum_{x \in S} p_S \hat{\rho}_S - \rho_x\|_{tr} \leq \epsilon}} \sum_S p_S,$$

where S ranges over all nonempty subsets of \mathcal{X} .

Before proceeding to the proof of the lemma, we want to first narrow down the set of classical side information we need to consider.

Lemma 3.2. *Let $\eta_{XY} = \sum_{xy} p_{xy} |x\rangle\langle x| \otimes |y\rangle\langle y|$ be a cc state. Then there exists a cc state $\eta'_{XS} \in \mathcal{S}_{=}(\mathcal{X} \otimes 2^{\mathcal{X}})$ with the following three properties:*

1. $p_g(X|Y)_{\eta} = p_g(X|S)_{\eta'}$;
2. There exists a classical channel $C_{S \rightarrow Y}$ such that $(I \otimes C)(\eta') = \eta$;
3. η' is of the form

$$\eta' = \sum_{S \subseteq \mathcal{X}} p_S \left(\sum_{x \in S} |x\rangle\langle x| \otimes |S\rangle\langle S| \right).$$

This lemma implies that, for our purposes, the set of all joint distributions we need to consider is of the form where the side information only indicates in which set the classical information is uniformly distributed.

Proof. We provide a constructive proof. For sake of simplicity we will use classical probability notations, i.e. η_{XY} will be identified as the classical joint distribution p_{XY} .

All subset of \mathcal{X} form a directed acyclic graph under containment relations, therefore we can recursively define

$$p_S(y) = \min_{x \in S} p(x, y) - \sum_{S' \subsetneq S} p_{S'}(y)$$

for all nonempty $S \subseteq \mathcal{X}$. Let $\hat{p}_S = \sum_y p_S(y)$ and $C_S = \text{Supp}(p_S(y))$. We claim that the distribution

$$p'(x, S) = \hat{p}_S \delta_{x \in S},$$

together with the channel

$$C(y|S) = p_S(y) / \hat{p}_S$$

satisfies our requirements for η' .

First we need to show that p'_{XS} is indeed a distribution, and C is indeed a classical channel. It suffices to show that $p_S(y) \geq 0$ for all S and y .

To prove this, we apply induction on size of the set to prove two things:

- $p_S(y) \geq 0$ for all S and y ;

- For all S_1 and S_2 where no one contains the other, we have $C_{S_1} \cap C_{S_2} = \emptyset$.

The base case is when $|S|, |S_1|, |S_2| \geq |\mathcal{X}|$. Apparently we have $S = S_1 = S_2 = \mathcal{X}$, so the second statement is true. For the first one, we have by construction

$$p_{\mathcal{X}}(y) = \min_x p(x, y) \geq 0.$$

Let's move on to the induction step. Assume now that for all S_1, S_2 where

- $|S_1|, |S_2| > k$
- $S_1, S_2 \subsetneq S_1 \cup S_2$

we have $p_S(y) \geq 0$ for all y and $C_{S_1} \cap C_{S_2} = \emptyset$. Then for a given y and a subset S with $|S| = k$, the collection of subsets

$$\{S' | y \in \text{Supp}(S'), S \subsetneq S'\}$$

must form a chain $S'_1 \subsetneq S'_2 \subsetneq \dots \subsetneq S'_m$ under containment relations. Then

$$\begin{aligned} p_S(y) &= \min_{x \in S} p(x, y) - \sum_{S \subsetneq S'} p_{S'}(y) \\ &= \min_{x \in S} p(x, y) - \sum_{i=1}^m p_{S'_i}(y) \\ &= \min_{x \in S} p(x, y) - \left(\min_{x \in S'_1} p(x, y) - \sum_{i=2}^m p_{S'_i}(y) \right) - \sum_{i=2}^m p_{S'_i}(y) \\ &= \min_{x \in S} p(x, y) - \min_{x \in S'_1} p(x, y) \\ &\geq 0. \end{aligned}$$

Also, for S_1, S_2 not contained in each other and with size $\geq k$, we have

$$\begin{aligned} p_{S_1}(y) &= \min_{x \in S_1} p(x, y) - \sum_{S_1 \subsetneq S'} p_{S'}(x, y) \\ &= \left(\min_{x \in S_1} p(x, y) - \min_{x \in S_1 \cup S_2} p(x, y) \right) - \sum_{S_1 \subseteq S', S_2 \not\subseteq S'} p_{S'}(y) \\ &\leq \min_{x \in S_1} p(x, y) - \min_{x \in S_1 \cup S_2} p(x, y) \end{aligned}$$

and similarly

$$p_{S_2}(y) \leq \min_{x \in S_2} p(x, y) - \min_{x \in S_1 \cup S_2} p(x, y)$$

using the induction hypothesis $p_S(y) \geq 0$ for all $|S| \geq k$. As

$$\min_{x \in S_1 \cup S_2} p(x, y) = \min\left\{ \min_{x \in S_1} p(x, y), \min_{x \in S_2} p(x, y) \right\},$$

we know that either $p_{S_1}(y) = 0$ or $p_{S_2}(y) = 0$, which results in that $y \notin C_{S_1} \cap C_{S_2}$. As this holds for an arbitrary y , we must have $C_{S_1} \cap C_{S_2} = \emptyset$. This completes the induction step.

We then proceed to prove that p' and C satisfies the three properties listed in Lemma 3.2. Note that property 3 is automatically satisfied by the form of p' , so it suffices to show just the first two properties.

1. To see property 1 of Lemma 3.2, note that the guessing probability of p and p' are respectively $p_g(X|Y)_p = \sum_y \max_x p(x, y)$ and $p_g(X|S)_{p'} = \sum_S \hat{p}_S = \sum_y \sum_S p_S(y)$. It then suffices to prove that $\sum_S p_S(y) = \max_x p(x, y)$ holds for all y .

One direction is easier to prove: for all x we have

$$\begin{aligned} \sum_S p_S(y) &\geq \sum_{\{x\} \subseteq S} p_S(y) \\ &= p(x, y) - \sum_{\{x\} \subsetneq S} p_S(y) + \sum_{\{x\} \subsetneq S} p_S(y) \\ &= p(x, y), \end{aligned}$$

thus $\sum_S p_S(y) \geq \max_x p(x, y)$. To prove the other direction, let's look more in detail into what we have proved so far. For every subset S , we have shown that the sum $\sum_{S \subsetneq S'} p_{S'}(y)$ can be reduced to summation on a chain. Without loss of generality, this chain can be completed to maximal length such that the difference of cardinalities of adjacent terms on this chain is 1, as additional terms would not change the final result. As

$$\sum_S p_S(y) = \sum_{\emptyset \subsetneq S} p_S(y),$$

there exists a chain $\emptyset \subsetneq S_1 \subsetneq \dots \subsetneq S_{|\mathcal{X}|} = \mathcal{X}$ such that $|S_i| = i$ and

$$\sum_S p_S(y) = \sum_{i=1}^{|\mathcal{X}|} p_{S_i}(y).$$

As $|S_1| = 1$, there must exist x^* such that $S_1 = \{x^*\}$. Then

$$\sum_S p_S(y) = \sum_{i=1}^{|\mathcal{X}|} p_{S_i}(y) = p(x^*, y) \leq \max_x p(x, y),$$

which proves the opposite direction of property 1.

2. For property 2, denote p''_{XY} the joint distribution we get from applying C onto p' . We have

$$\begin{aligned} p''(x, y) &= \sum_S p'(x, S) C(y|S) \\ &= \sum_S \delta_{x \in S} \hat{p}_S \cdot p_S(y) / \hat{p}_S \\ &= \sum_{x \in S} p_S(y) \\ &= p_{\{x\}}(y) + \sum_{\{x\} \subsetneq S} p_S(y) \\ &= p(x, y) - \sum_{\{x\} \subsetneq S} p_S(y) + \sum_{\{x\} \subsetneq S} p_S(y) \\ &= p(x, y). \end{aligned}$$

This proves property 2, which finishes the entire proof of Lemma 3.2.

□

With Lemma 3.2, we are now ready to prove Lemma 3.1.

Proof of Lemma 3.1. Recall the definition of ϵ -smooth conversion parameter:

$$p_{\downarrow}^{\epsilon}(X|E)_{\rho} = \min_{\substack{\eta_{XY}, \mathcal{C}_{Y \rightarrow \mathcal{E}} \\ \|(\mathcal{I} \otimes \mathcal{C})(\eta) - \rho\| \leq \epsilon}} p_g(X|Y)_{\eta}.$$

For every η , by Lemma 3.2 there exists $\eta'_{XS} = \sum_S p_S (\sum_{x \in S} |x\rangle\langle x|) \otimes |S\rangle\langle S|$ satisfying the three properties. It is easy to see that η' , with the channel $\mathcal{C}' = \mathcal{C} \circ \mathcal{C}$, is also a cc state achieving the same guessing probability and error, and the guessing probability of η' is $\sum_S p_S$. A general quantum channel acting on the side information can be characterized as follows without loss of generality:

$$\mathcal{C}'_{2x \rightarrow \mathcal{E}}(\cdot) = \sum_S \langle S| \cdot |S\rangle \hat{\rho}_S.$$

Then we have

$$(\mathcal{I} \otimes \mathcal{C}')(\eta') = \sum_S \left(\sum_{x \in S} |x\rangle\langle x| \right) \otimes p_S \hat{\rho}_S,$$

which leads to

$$\|(\mathcal{I} \otimes \mathcal{C}')(\eta') - \rho\| = \sum_x \left\| \sum_{x \in S} p_S \hat{\rho}_S - \rho_x \right\|,$$

finishing the proof of Lemma 3.1. □

4 Proof of Separation Lemma

In this section we provide a proof for our main technical result, the Separation Lemma 4.1.

Lemma 4.1 (Separation Lemma). *For all $\delta > 0, \epsilon \geq 0$ and state*

$$\rho_{XE} = \sum q_x |x\rangle\langle x| \otimes |\psi_x\rangle\langle \psi_x|$$

with maximum overlap

$$\delta = \max_{x, y: x \neq y} |\langle \psi_x | \psi_y \rangle|,$$

we have

$$1 - \epsilon/2 \leq (1 - \delta)p_{\downarrow}^{\epsilon}(X|E)_{\rho} + \delta.$$

Regarding the quantum side information as a cryptographic hash function, now let us consider the following scheme. An adversary, upon receiving some classical leakage of a classical message, tries to forge a quantum system which looks like the authentic hash. The adversary then sends this state to a verifier with full knowledge of the classical message, and the verifier, conditioned on classical information x , performs a projection measurement V on the quantum state provided by the adversary. We say that the adversary cheats the verifier if the measurement outcome is accept. Given that the forged state is ϵ -close to the quantum hash, the passing probability e_s is clearly no less than $1 - \epsilon/2$, and the probability p_g that the adversary can guess the classical message X correctly is no more than $p_{\downarrow}^{\epsilon}(X|E)_{\rho}$. It then suffices to prove that in this particular scheme, we have

$$e_s \leq (1 - \delta)p_g + \delta.$$

In the proof of Lemma 4.1 we will make use of Cotlar-Stein Lemma, which gives a good estimate of the operator norm of the sum of near-orthogonal operators. We will attach the proof of the Cotlar-Stein Lemma in Appendix A for completeness.

Lemma 4.2 (Cotlar-Stein Lemma). *For a set of unit vectors $\{|\psi_1\rangle, |\psi_2\rangle, \dots, |\psi_n\rangle\}$ with maximum fidelity $\max_{i,j:i \neq j} |\langle \psi_i | \psi_j \rangle| \leq \delta$, we have*

$$\lambda_{\max} \left(\sum_{i=1}^n |\psi_i\rangle\langle \psi_i| \right) \leq 1 + (n-1)\delta.$$

Proof of Lemma 4.1. By Lemma 3.1, without loss of generality, we can assume that the joint state of the classical message and the side information obtained by the adversary is of the form

$$\rho_{XZ} = \sum_S p_S \left(\sum_{x \in S} |x\rangle\langle x| \otimes |S\rangle\langle S| \right)$$

where $\sum_{x \in S} p_S = q_x$ for all x . It follows then that

$$p_g = \sum_S p_S, \quad \sum_S p_S |S| = 1.$$

The adversary then prepares state $\hat{\rho}_S$ based on the side information S . We have a precise evaluation of e_s :

$$\begin{aligned} e_s &= \sum_x \langle \psi_x | \sum_{x \in S} p_S \hat{\rho}_S | \psi_x \rangle \\ &= \sum_S p_S \text{Tr}[\hat{\rho}_S \sum_{x \in S} |\psi_x\rangle\langle \psi_x|] \\ &\leq \sum_S p_S \lambda_{\max} \left(\sum_{x \in S} |\psi_x\rangle\langle \psi_x| \right). \end{aligned}$$

By the Cotlar-Stein Lemma, we have

$$\lambda_{\max} \left(\sum_{x \in S} |\psi_x\rangle\langle \psi_x| \right) \leq 1 + (|S| - 1)\delta.$$

Since we have $p_g = \sum_S p_S$ and $1 = \sum_S p_S |S|$,

$$\begin{aligned} e_s &\leq \sum_S p_S \lambda_{\max} \left(\sum_{x \in S} |\psi_x\rangle\langle \psi_x| \right) \\ &\leq \sum_S p_S (1 + (|S| - 1)\delta) \\ &= p_g(1 - \delta) + \delta. \end{aligned}$$

□

5 Quantum Hash

5.1 Quantum Fingerprinting is Resilient to Classical Leakage

Now let us consider the setting of quantum hashing. For the sake of simplicity, we assume that the classical message X is uniformly distributed over $\{0, 1\}^n$, and all parties are information theoretic and considered as channels.

Suppose now that a prover A , either adversarial or honest, upon obtaining some side information Y of X , wants to show that he has full access to the classical message X . To show this, he needs to pass a test held by a verifier V who has full access to X . One way to do this is to send V an m -bit hash M , and V will accept or reject based on the classical messages X and M .

If the adversary wants to cheat as best as he can, the optimal strategy would be applying a deterministic mapping on the side information Y ; similarly, if the verifier wants to distinguish adversarial parties from honest ones as best as he can, the optimal strategy would also be a deterministic algorithm. Therefore we can safely assume that both A and V are deterministic mappings.

Definition 6 (Resilience against leakage). *A mapping $h : \{0, 1\}^n \rightarrow \{0, 1\}^m$ is called σ -resilient against k bits of information leakage if for all classical side information Y of X such that $|Y| \leq k$, for all mappings $f : \{0, 1\}^k \rightarrow \{0, 1\}^m$, we have*

$$\Pr_{XY}[f(Y) = h(X)] \leq \sigma.$$

If σ is not specified then it is assumed that $\sigma = \text{negl}(n)$.

Ideally, one would want a hash function which is resilient against much information leakage and short at the same time. Unfortunately these two requirements cannot be achieved at the same time. If an m -bit verification scheme V is resilient against k bits of classical leakage, one must have $m = k + \omega(\log n)$. This can be seen as follows: suppose otherwise that $m = k + O(\log n)$. Then an adversarial prover, upon getting the first k bits of the message an honest party would send to the verifier, guesses the remaining $O(\log n)$ bits uniformly at random. Such a prover would then have an inverse polynomial probability of passing the test.

Now suppose that both the verifier and the prover have access to quantum power, while the information leakage is still classical. Now the prover can send an m -qubit quantum system ρ to the verifier, and the verifier would then perform a joint measurement on both X and ρ to determine whether to accept or not. Denote the state space of X, Y and M respectively by \mathcal{X}, \mathcal{Y} and \mathcal{M} .

Definition 7 (Resilience of quantum fingerprinting against classical information leakage). *An (n, m, δ) quantum fingerprinting ϕ is called σ -resilient against k bits of classical information leakage if for all classical side information Y of X such that $|Y| \leq k$ and any quantum channel $\mathcal{C}_{\mathcal{Y} \rightarrow \mathcal{M}}$, we have*

$$\text{Tr}[V \cdot (\mathcal{I} \otimes \mathcal{C})(\rho_{XY})] = \sigma,$$

where

$$\rho_{XY} = \sum_{x,y} \text{Tr}[X = x, Y = y] |x\rangle\langle x| \otimes |y\rangle\langle y|,$$

and

$$V = \sum_x |x\rangle\langle x| \otimes \phi_x.$$

When σ is not specified, it is assumed that $\sigma = \text{negl}(n)$.

In the case where all states we are considering are cq states, it is safe to replace a general channel by mapping each classical information to a state. Therefore, \mathcal{C} can be specified by

$$\mathcal{C}(\cdot) = \sum_y \langle y | \cdot | y \rangle \rho_y.$$

Then the passing probability $\text{Tr}[V \cdot (\mathcal{I} \otimes \mathcal{C})(\rho_{XY})]$ can be written more elegantly as $\mathbb{E}_{XY}[\text{Tr}[\phi_X \rho_Y]]$.

In sharp contrast to the classical case, the Separation Lemma implies that there exists a (n, m, δ) quantum fingerprinting resilient against k bits of classical information leakage, where k is much larger than m . In fact we have the following theorem.

Theorem 5.1. *For all n , $m = \omega(\log n)$ and $k = n - \omega(\log n)$, there exists a quantum (n, m) cryptographic hash which is resilient against k bits of classical information leakage.*

Before proving this theorem, note that this theorem is tight on both sides. If $k = n - O(\log n)$, then an adversary knowing the side information can guess correctly the actual value of X with probability inverse polynomial, thus the success probability would also be non-negligible; on the other hand, if $m = O(\log n)$, we claim that an adversary with zero side information can still pass the test with non-negligible probability.

To see this, let's start from the completeness condition. This is saying that there exist ρ_x 's such that $\mathbb{E}_X[\text{Tr}[M_X \rho_X]] = 1$. This can only happen when each term is 1, which in turn implies that $\text{Tr}[M_x] \geq 1$ for all x . Now suppose the adversary has no side information about the classical message, so the best he can do is to prepare a state ρ . The success probability will then be

$$\mathbb{E}_X \text{Tr}[M_X \rho] \leq \lambda_{\max}(\mathbb{E}_X[M_X]),$$

which can be approached when $\rho_0 = |\psi_0\rangle\langle\psi_0|$, $|\psi_0\rangle$ being the eigenvector corresponding to the largest eigenvalue of $\mathbb{E}_X[M_X]$. The operator norm can be lower bounded from the trace by

$$\lambda_{\max}(\mathbb{E}_X[M_X]) \geq \frac{\text{Tr}[\mathbb{E}_X[M_X]]}{\dim \mathcal{M}} \geq \frac{1}{\text{poly}(n)},$$

resulting in a non-negligible passing probability without any side information.

Now let us proceed to the proof of Theorem 5.1.

Proof of Theorem 5.1. Take an (n, m, δ) quantum fingerprinting ϕ , where δ will be specified later. We know that such a fingerprinting exists for $m = O(\log n + 2 \log \frac{1}{\delta})$, therefore there exists $\delta = \text{negl}(n)$ such that ϕ is a quantum cryptographic hash. The verification scheme associated to this quantum fingerprinting is then

$$V = \sum_x |x\rangle\langle x| \otimes \phi_x.$$

Upon getting $k = n - l$ bits of classical information, the guessing probability of the adversary to the classical message is upper bounded by 2^{-l} . By Separation Lemma, the probability that the adversary pass the test e_s is upper bounded by $2^{-l} + \delta$, which is still a negligible function of n given $l = \omega(\log n)$. \square

5.2 Generalized Verification Scheme Resilient to Classical Leakage

Our verification scheme is maximally resilient to classical leakage of information. However, it is still not good enough because the verifier may need to get full access to the whole message. One

may ask if it is possible that the verifier only use a small amount of information from the message to perform the verification scheme, yet the verification is still resilient to classical leakage.

To formulate this idea, we generalize the definition of a verification scheme $V = (\mathcal{C}, M)$ with three parameters (n, k, m) played by two players A and B as follows:

1. A joint distribution XY , where the marginal distribution of $X \in \{0, 1\}^n$ is uniformly random, is generated by nature.
2. A gets the k -qubit quantum state $\rho_X = \mathcal{C}(|X\rangle\langle X|)$ and B gets the side-information string Y .
3. B generates an m -qubit quantum state μ_Y and sends it to A .
4. A perform a joint measurement M on the state $\rho_X \otimes \mu_Y$. The game is successful if and only if the measurement accepts. The overall success probability is thus

$$e_s^V = \mathbb{E}_{XY}[M(\rho_X \otimes \mu_Y)].$$

For a given ℓ , define the optimal success probability over all classical leakage Y where $H(X|Y) \geq \ell$ to be $e_s^{V^*}(\ell)$. We can then define the resilience formally:

Definition 8. A (n, k, m) -verification scheme $V = (\mathcal{C}, M)$ is called σ -resilient to ℓ bits of classical leakage if we have

$$e_s^{V^*}(\ell) \leq \sigma.$$

In the case where σ is not specified, it is assumed that σ is negligible.

Interestingly, one can use the power of quantum side information to reduce the size of the advice state.

Theorem 5.2. For all n , there exists a (n, k, m) -verification scheme V which is resilient to ℓ bits of classical leakage whenever

$$k = m = \omega(\log^2 n), n - \ell = \omega(\log n).$$

Proof. Proof by construction. Take $t, m' = \sqrt{k} = \omega(n)$. We first fix a (n, m') -quantum cryptographic hash function ϕ . for a given message x , the advice state would just be t -fold tensor product of ϕ_x 's, namely

$$\rho_x := \phi_x^{\otimes t}.$$

Upon receiving the hash μ_Y consisting of t parts of m' -qubit states, the verifier performs SWAP test between all t pairs of ϕ_X and each of the qubit states, accepts if all SWAP tests pass and rejects otherwise. Note that an honest party having full access to X would be able to produce $\phi_X^{\otimes t}$ perfectly, thus successes with probability 1.

To see that this scheme is resilient against classical leakage, assume now that the state received by the verifier is a forgery state μ_Y . Regarding both ρ_X and μ_Y as t -partite states, we use $\rho_X^T, \mu_Y^T, SWAP^T$ to denote the marginal state on subsystems $T \subseteq [t]$ and the swap between the two subsystems respectively. The measurement corresponding to one copy of SWAP test is $\frac{I+SWAP}{2}$,

thus the success probability will be

$$\begin{aligned}
e_s^V &= \mathbb{E}_{XY} \left[\frac{\text{Tr}[(I + \text{SWAP})^{\otimes t}(\rho_X \otimes \mu_Y)]}{2^t} \right] \\
&= \frac{1}{2^t} \sum_{T \in [t]} \mathbb{E}_{XY} \left[\text{Tr}[\bigotimes_{i \in T} \text{SWAP}^i(\rho_X \otimes \mu_Y)] \right] \\
&= \frac{1}{2^t} \sum_{T \in [t]} \mathbb{E}_{XY} [\text{Tr}[\text{SWAP}^T(\rho_X^T \otimes \mu_Y^T)]] \\
&= \frac{1}{2^t} \sum_{T \in [t]} \mathbb{E}_{XY} [\text{Tr}[\rho_X^T \cdot \mu_Y^T]].
\end{aligned}$$

Here the third line comes by tracing out irrelevant states, and the fourth line comes from the identity $\text{Tr}[\text{SWAP}(\rho \otimes \sigma)] = \text{Tr}[\rho\sigma]$. For each term $\text{Tr}[\rho_X^T \cdot \mu_Y^T]$ with nonempty T and any $i \in T$, we have

$$\text{Tr}[(\rho_X^T \cdot \mu_Y^T)] \leq \text{Tr}[(\phi^i \otimes I^{T \setminus \{i\}})\mu_Y^T] = \text{Tr}[\phi_x \rho_Y^i].$$

This gives us

$$e_s^V \leq \frac{1}{2^t} + \max_i \mathbb{E}_{XY} \text{Tr}[\rho_Y^i \phi_X].$$

By Theorem 5.1, for all Y such that $H_{\min}(X|Y) \geq \ell$, $i \in [t]$, $\mathbb{E}_{XY} \text{Tr}[\rho_Y^i \phi_X] = \text{negl}(n)$ given that ϕ is a quantum cryptographic hash function. $e_S^{V*}(\ell) = \text{negl}(n)$ then comes from that $t = \omega(\log n)$. \square

6 Applications of Separation Lemma in Quantum-proof Extractors

Let us now recall the setting of seeded extractor. A seeded extractor $\text{Ext} : \{0, 1\}^n \times \{0, 1\}^d \rightarrow \{0, 1\}^m$ takes a weak random source X as well as a much shorter, uniform and independent seed Y and outputs a nearly uniform distribution. Rigorously we have the following definition.

Definition 9 (Extractor). *A function $\text{Ext} : \{0, 1\}^n \times \{0, 1\}^d \rightarrow \{0, 1\}^m$ is called an (k, ϵ) -extractor if for all random source X such that $-\log p_g(X) \geq k$, we have*

$$\|U_m - \text{Ext}(X \otimes U_d)\| \leq \epsilon.$$

When used in the setting of privacy amplification, one would consider the case where there is a leakage of the random source. The output of the extractor then need to not only be close to uniform, but also be almost independent of the side information. Depending on whether the leakage is classical or quantum, we have the following definitions for *classical-proof* and *quantum-proof* extractors respectively.

Definition 10 (Classical-proof Extractor). *A function $\text{Ext} : \{0, 1\}^n \times \{0, 1\}^d \rightarrow \{0, 1\}^m$ is called an (k, ϵ) -classical-proof extractor if for all random source X with classical side information Y such that $-\log p_g(X|Y) \geq k$, we have*

$$\|U_m \otimes Y - \text{Ext}(X \otimes U_d)Y\| \leq \epsilon.$$

Definition 11 (Quantum-proof Extractor). *A function $Ext : \{0, 1\}^n \times \{0, 1\}^d \rightarrow \{0, 1\}^m$ is called an (k, ϵ) -quantum-proof extractor if for every cq state ρ_{XE} such that $-\log p_g(X|E) \geq k$, we have*

$$\|U_m \otimes \rho_E - (Ext \otimes \mathcal{I})(\rho_{XE})\|_{tr} \leq \epsilon.$$

Intensive research on all three kinds of extractors has been done over years. Fortunately, the following theorem says that a good extractor is automatically a good classical-proof extractor, up to very little parameter loss:

Theorem 6.1 ([14]). *Any (k, ϵ) -extractor is a $(k + \log 1/\epsilon, 2\epsilon)$ -classical-proof extractor.*

One long-standing open problem, then, is whether a classical-proof extractor is essentially a quantum-proof extractor with roughly the same parameter. Currently the best result is that a (k, ϵ) -classical proof extractor is a $(k + \log 2/\epsilon, O(2^{m/2}\sqrt{\epsilon}))$ -extractor. For nonexponential blow-up of parameters, Gavinsky et al. [11] showed that there exists a $(k - \Theta(n), \epsilon)$ -classical extractor which is not secure against $O(\log n)$ qubits of quantum side information. Proving a result without exponential blowup on the parameter in the practical range, however, is a very challenging problem.

The Separation Lemma here suggests that such a result without a drastic blowing up on the error parameter may not exist. To see this, we need to define some sets first.

Definition 12. *For every k , define the following sets:*

- $C(k)$ is the set of all cq states ρ_{XE} that can be generated from a classical random source XY with

$$-\log \max_y p_g(X|Y = y) \geq k$$

via a channel acting only on the Y part;

- $CC(k)$ is the set of all cq states ρ_{XE} that can be generated from a classical random source XY with

$$-\log p_g(X|Y) \geq k$$

via a channel acting only on the Y part;

- $CQ(k)$ is the set of all cq states ρ_{XE} such that $-\log p_g(X|E)_\rho \geq k$.

Clearly we have $C(k) \subseteq CC(k) \subseteq CQ(k)$. To see the importance of these sets, we can use the alternative, though equivalent definitions of extractors, classical-proof and quantum-proof extractors:

Definition 13 (Alternative definition for extractors). *A function $Ext : \{0, 1\}^n \times \{0, 1\}^d \rightarrow \{0, 1\}^m$ is called a (k, ϵ) -extractor (classical-proof extractor, quantum extractor), if for all cq states $\rho_{XE} \in C(k)(CC(k), CQ(k))$ with $X \in \{0, 1\}^n$ we have*

$$\|U_m \otimes \rho_E - (Ext \otimes \mathcal{I})(\rho_{XE})\|_{tr} \leq \epsilon.$$

The proof of Theorem 6.1 essentially makes use of the fact that every state ρ_{XE} in $CC(k + \log 1/\epsilon)$ is ϵ -close to the set $C(k)$, and thus a (k, ϵ) -extractor, when applied to ρ , would introduce at most 2ϵ error from the state $U_m \otimes \rho_E$ due to monotonicity of trace distance. If one could obtain similar results between $CQ(k)$ and $CC(k)$, then we could easily prove that a classical-proof extractor is secret quantum-proof.

This turns out to not be the case according to Separation Lemma. Recall our definition of ϵ -smooth conversion parameter $p_\downarrow^\epsilon(X|E)_\rho$, which measures the least guessing probability of a classical distribution we need in order to generate the desired state ρ , i.e.

$$d(\rho, CC(k)) \leq \epsilon \Leftrightarrow -\log p_\downarrow^\epsilon(X|E)_\rho \geq k.$$

Theorem 6.2. *For any k , there exists a cq state ρ_{XE} where $X \in \{0, 1\}^{k(1+o(1))}$ such that $\rho \in CQ(k)$ while $d(\rho, CC(2)) \geq 0.98$.*

Proof. Fix $\delta = 0.02$ and $\epsilon = 0.98$. By the Johnson-Lindenstrauss Lemma, we have a cq state

$$\rho_{XE} = 2^{-n} \sum_{x \in \{0,1\}^n} |x\rangle\langle x| \otimes |\psi_x\rangle\langle \psi_x| \in \mathcal{S}_=(\mathcal{X} \otimes \mathcal{E})$$

such that $\log \dim \mathcal{E} = O(\log n)$ and $\max_{x \neq x'} |\langle \psi_x | \psi_{x'} \rangle|$. For given k , there exists $n = k(1 + o(1))$ such that $n - O(\log n) \geq k$. With that n , we have

$$-\log p_g(X|E)_\rho \geq k \Rightarrow \rho \in CQ(k)$$

as well as

$$-\log p_\downarrow^\epsilon(X|E)_\rho \leq 2.$$

By the Separation Lemma, we have

$$p_\downarrow^\epsilon(X|E)_\rho \geq 1 - \delta - \epsilon/2 \Rightarrow d(\rho, CC(2)) \geq 0.98.$$

□

The Separation Lemma suggests that an arbitrary classical extractor may not be quantum-proof, i.e. the sets $CQ(k)$ and $CC(k)$ are spatially separated. Nevertheless, one may still prove that a classical extractor is quantum-proof, but in order to do that, one might need to use additional properties of the extractor, other than that it can extract randomness from all states in $CC(k)$.

Acknowledgements. The authors would like to thank Kai-Min Chung, Ronald de Wolf, Carl Miller, Michael Newman and Fang Zhang for useful discussion on this topic. This research was supported in part by US NSF Award 1216729.

A Proof of the Cotlar-Stein Lemma

Lemma A.1 (Cotlar-Stein Lemma). *For a set of unit vectors $\{|\psi_1\rangle, |\psi_2\rangle, \dots, |\psi_n\rangle\}$ with maximum fidelity $\max_{i,j:i \neq j} |\langle \psi_i | \psi_j \rangle| \leq \delta$, we have*

$$\lambda_{\max} \left(\sum_{i=1}^n |\psi_i\rangle\langle\psi_i| \right) \leq 1 + (n-1)\delta.$$

Proof. We use the fact that the operator norm is upper bounded by all Schatten p norms, i.e.

$$\lambda_{\max}(\rho) = \|\rho\|_{\infty} = \lim_{p \rightarrow \infty} (\text{Tr}[\rho^p])^{1/p}.$$

For an arbitrary positive integer m , let's now bound

$$\left\| \sum_{i=1}^n |\psi_i\rangle\langle\psi_i| \right\|_m^m = \text{Tr} \left[\left(\sum_{i=1}^n |\psi_i\rangle\langle\psi_i| \right)^m \right].$$

We have

$$\begin{aligned} \text{Tr} \left[\left(\sum_{i=1}^n |\psi_i\rangle\langle\psi_i| \right)^m \right] &= \sum_{i_1, \dots, i_m \in [n]} \text{Tr} \left[\prod_{j=1}^m |\psi_{i_j}\rangle\langle\psi_{i_j}| \right] \\ &= \sum_{i_1, \dots, i_m \in [n]} \prod_{j=1}^{m-1} \langle \psi_{i_j} | \psi_{i_{j+1}} \rangle \cdot \langle \psi_{i_m} | \psi_{i_1} \rangle \\ &\leq \sum_{i_1, \dots, i_m \in [n]} \prod_{j=1}^{m-1} |\langle \psi_{i_j} | \psi_{i_{j+1}} \rangle| \cdot |\langle \psi_{i_m} | \psi_{i_1} \rangle|. \end{aligned}$$

Using the fact that both $|\psi_{i_m}\rangle$ and $|\psi_{i_1}\rangle$ are unit vectors, we have $|\langle \psi_{i_m} | \psi_{i_1} \rangle| \leq 1$. Then

$$\begin{aligned} \text{Tr} \left[\left(\sum_{i=1}^n |\psi_i\rangle\langle\psi_i| \right)^m \right] &\leq \sum_{i_1, \dots, i_m \in [n]} \prod_{j=1}^{m-1} |\langle \psi_{i_j} | \psi_{i_{j+1}} \rangle| \\ &\leq \sum_{i_1, \dots, i_{m-1} \in [n]} \prod_{j=1}^{m-2} |\langle \psi_{i_j} | \psi_{i_{j+1}} \rangle| \cdot \sum_{i_m} |\langle \psi_{i_{m-1}} | \psi_{i_m} \rangle| \end{aligned}$$

Note that for every i_{m-1} , the term $\sum_{i_m} |\langle \psi_{i_{m-1}} | \psi_{i_m} \rangle|$ can be upper bounded by $1 + (n-1)\delta$.

Repeatedly applying this argument, we have

$$\begin{aligned}
\mathrm{Tr}[\sum_{i=1}^n |\psi_i\rangle\langle\psi_i|^m] &\leq \sum_{i_1, \dots, i_{m-1} \in [n]} \prod_{j=1}^{m-2} |\langle\psi_{i_j}|\psi_{i_{j+1}}\rangle| \cdot (1 + (n-1)\delta) \\
&\leq \sum_{i_1, \dots, i_{m-2} \in [n]} \prod_{j=1}^{m-3} |\langle\psi_{i_j}|\psi_{i_{j+1}}\rangle| \cdot (1 + (n-1)\delta)^2 \\
&\leq \dots \\
&\leq \sum_{i_1} (1 + (n-1)\delta)^{m-1} \\
&= n \cdot (1 + (n-1)\delta)^{m-1}.
\end{aligned}$$

Therefore, for every m we have

$$\lambda_{\max}(\sum_{i=1}^n |\psi_i\rangle\langle\psi_i|) \leq (1 + (n-1)\delta)^{1-\frac{1}{m}} \cdot n^{1/m}.$$

The result follows by letting $m \rightarrow \infty$. □

References

- [1] F. Ablyayev and A. Vasiliev. Cryptographic quantum hashing. *Laser Physics Letters*, 11(2):025202, 2013.
- [2] A. Akavia, S. Goldwasser, and V. Vaikuntanathan. Simultaneous hardcore bits and cryptography against memory attacks. In *Theory of Cryptography Conference*, pages 474–495. Springer, 2009.
- [3] S. Arunachalam and R. de Wolf. Optimal quantum sample complexity of learning algorithms. *arXiv preprint arXiv:1607.00932*, 2016.
- [4] C. H. Bennett, G. Brassard, C. Crépeau, and U. M. Maurer. Generalized privacy amplification. *IEEE Transactions on Information Theory*, 41(6):1915–1923, 1995.
- [5] C. H. Bennett, G. Brassard, and J.-M. Robert. How to reduce your enemys information. In *Conference on the Theory and Application of Cryptographic Techniques*, pages 468–476. Springer, 1985.
- [6] D. Boneh and V. Shoup. *A Graduate Course in Applied Cryptography*. 2015. Available at https://crypto.stanford.edu/~dabo/cryptobook/draft_0_2.pdf.
- [7] E. Brier and M. Joye. Weierstraß elliptic curves and side-channel attacks. In *International Workshop on Public Key Cryptography*, pages 335–345. Springer, 2002.
- [8] H. Buhrman, R. Cleve, J. Watrous, and R. de Wolf. Quantum fingerprinting. *Physical Review Letters*, 87(16):167902, 2001.
- [9] Y. Dodis, K. Haralambiev, A. López-Alt, and D. Wichs. Efficient public-key cryptography in the presence of key leakage. In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 613–631. Springer, 2010.
- [10] Y. Dodis and D. Wichs. Non-malleable extractors and symmetric key cryptography from weak secrets. In *Proceedings of the forty-first annual ACM symposium on Theory of computing*, pages 601–610. ACM, 2009.
- [11] D. Gavinsky, J. Kempe, I. Kerenidis, R. Raz, and R. 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.
- [12] O. Goldreich, R. Israel, and D. Zuckerman. Another proof that $bpp \subseteq ph$ (and more). In *Electronic Colloquium on Computational Complexity*. Citeseer, 1997.
- [13] M. Joye and J.-J. Quisquater. Hessian elliptic curves and side-channel attacks. In *International Workshop on Cryptographic Hardware and Embedded Systems*, pages 402–410. Springer, 2001.
- [14] R. T. König and B. M. Terhal. The bounded-storage model in the presence of a quantum adversary. *IEEE Transactions on Information Theory*, 54(2):749–762, 2008.
- [15] U. M. Maurer. Secret key agreement by public discussion from common information. *IEEE Transactions on Information Theory*, 39(3):733–742, 1993.
- [16] D. Moshkovitz. Parallel repetition from fortification. In *Foundations of Computer Science (FOCS), 2014 IEEE 55th Annual Symposium on*, pages 414–423. IEEE, 2014.

- [17] J. Naor and M. Naor. Small-bias probability spaces: Efficient constructions and applications. *SIAM journal on computing*, 22(4):838–856, 1993.
- [18] M. Naor and G. Segev. Public-key cryptosystems resilient to key leakage. In *Advances in Cryptology-CRYPTO 2009*, pages 18–35. Springer, 2009.
- [19] M. A. Nielsen and I. L. Chuang. *Quantum computation and quantum information*. Cambridge university press, 2010.
- [20] N. Nisan. Pseudorandom generators for space-bounded computation. *Combinatorica*, 12(4):449–461, 1992.
- [21] N. Nisan and D. Zuckerman. Randomness is linear in space. *Journal of Computer and System Sciences*, 52(1):43–52, 1996.
- [22] B. Preneel. Cryptographic hash functions. *European Transactions on Telecommunications*, 5(4):431–448, 1994.
- [23] P. Rogaway and T. Shrimpton. Cryptographic hash-function basics: Definitions, implications, and separations for preimage resistance, second-preimage resistance, and collision resistance. In *International Workshop on Fast Software Encryption*, pages 371–388. Springer, 2004.
- [24] F.-X. Standaert, T. Malkin, and M. Yung. A unified framework for the analysis of side-channel key recovery attacks. In A. Joux, editor, *EUROCRYPT*, volume 5479 of *Lecture Notes in Computer Science*, pages 443–461. Springer, 2009.
- [25] M. Sudan, L. Trevisan, and S. Vadhan. Pseudorandom generators without the xor lemma. In *Proceedings of the thirty-first annual ACM symposium on Theory of computing*, pages 537–546. ACM, 1999.
- [26] L. Trevisan. Extractors and pseudorandom generators. *Journal of the ACM*, 48(4):860–879, 2001.
- [27] A. Vasiliev and F. Ablyayev. Cryptographic quantum hashing. 2014.