Quantum Fingerprints that Keep Secrets

Dmitry Gavinsky[*] Tsuyoshi Ito[†]

Abstract

We introduce a new type of cryptographic primitive that we call a *hiding fingerprinting scheme*. A (quantum) fingerprinting scheme maps a binary string of length n to d (qu)bits, typically $d \ll n$, such that given any string y and a fingerprint of x, one can decide with high accuracy whether $x = y$. It is easy to see that a classical fingerprint of x that guarantees error $\leq \varepsilon$ necessarily reveals $\Omega\left(\log \frac{1}{\varepsilon + 2^{-n}}\right)$ bits of information about x. We call a scheme *hiding* if it reveals $o\big(\min\left\{n, \log \frac{1}{\varepsilon}\right\}\big)$ bits; accordingly, no classical scheme is hiding.

We demonstrate that a hiding fingerprinting scheme exists in the quantum world. We construct two types of hiding fingerprinting schemes, both of them map $x \in \{0,1\}^n$ to $O(\log n)$ qubits and guarantee one-sided error probability at most $1/n^c$, for any fixed c. The first type uses pure states and "leaks" at most $O(1)$ bits; the second kind uses mixed states and "leaks" at most $1/n^c$ bits – here "leakage" is defined as accessible information about the string x contained in its fingerprint.

Both our schemes are computationally efficient. In terms of hiding properties, the mixed-state scheme is optimal, as shown via a generic strategy that extracts $1/\operatorname{poly}(n)$ bits from any fingerprinting scheme on $O(\log n)$ qubits.

In the context of communication complexity our constructions can be viewed as quantum protocols for the equality problem in the models of one-way communication and simultaneous message passing that have communication cost $O(\log n)$ and offer *hiding guarantees* that cannot be matched by classical protocols of any cost.

1 Introduction

Cryptography is probably the area that benefits most from replacing classical computers by quantum ones. Many cryptographic goals that can be achieved classically only if unproven computational assumptions are made have unconditionally secure quantum realizations.

The famous *quantum key distribution* protocol by Bennett and Brassard [BB84] is one example where assuming that *quantum mechanics is valid* is enough to guarantee unconditional security of a construction. It is a natural and interesting research problem to find more examples of quantum crypto-protocols with unconditional security guarantees: Besides pleasing those of us who prefer to keep their secrets for themselves, such examples might shed more light on the nature of differences between quantum and classical information.

Informally speaking, the possibility to use quantum mechanics in order to achieve unconditional cryptographic security comes from the fact that, in general, quantum states are not "cloneable" (cf. [WZ82]). Sometimes it can be very challenging to use this property alone (not making any computational assumptions) in order to build a cryptographic primitive; moreover, some very tempting

[*] NEC Laboratories America, Inc., Princeton, NJ, U.S.A.

[†] NEC Laboratories America, Inc., Princeton, NJ, U.S.A. Part of this work was done while at the Institute for Quantum Computing and David R. Cheriton School of Computer Science, University of Waterloo, Waterloo, Ontario, Canada.

goals are already known to be beyond the reach (cf. [May97]). It is the quest of quantum cryptography to understand which goals can be achieved in a universe where the laws of quantum mechanics are valid.

1.1 Fingerprints and their hiding properties

In this paper we give a new example of a quantum crypto-primitive that is not reproducible classically. We call it *hiding fingerprints*. Noticeably, hiding fingerprints are impossible classically even modulo arbitrarily strong consistent assumptions.

In the context of this work the meaning of (classical) *fingerprints* is as follows. Given a binary string x of length n, we want to efficiently produce its "partial description" by d bits, typically with $d \ll n$, such that given only the description of x and any $y \in \{0,1\}^n$ one can test, with high accuracy, whether $x = y$. This can be achieved classically, for example by using a randomized mapping $x \longrightarrow (s, h_s(x))$, where h_s is chosen at random from a 2-universal family of hash functions (s identifies h_s inside the family).

Quantum fingerprints have been introduced by Buhrman, Cleve, Watrous and de Wolf in [BCWdW01]. An *n bits to d qubits quantum fingerprinting scheme* is a mapping from n-bit binary strings to density matrices in 2^d-dimensional complex Hilbert space, such that when ρ_x is the fingerprint of x then, given ρ_x and y, one can decide with high confidence whether $x = y$. Moreover, the construction of [BCWdW01] allowed testing whether $x = y$ given only the fingerprints ρ_x and ρ_y, which was the most important advantage of the quantum scheme over any possible classical solution.

In this work we view quantum fingerprints as cryptographic primitives. Let $\mathcal{E}$ be a quantum fingerprinting scheme, we are asking the following question: Given ρ_x, how much classical information about x can be "extracted" from it? Formally, for any quantum measurement P, how large can be the mutual information between a random variable $X = x$ that is uniformly distributed over $\{0,1\}^n$ and the outcome of P applied to ρ_x? The supremum of that value is called *the accessible information of $\mathcal{E}$*. In the special case when $\mathcal{E}$ is a classical scheme, its accessible information equals the mutual information between X and a fingerprint of X that $\mathcal{E}$ produces.

We will say that a fingerprinting scheme is *hiding* if its accessible information is $o\big(\min\left\{n, \log\frac{1}{\varepsilon}\right\}\big)$, where ε is the error probability of the scheme. This is the "cryptographic ingredient" that we add to the otherwise known notion of fingerprints. *No classical fingerprinting scheme can be hiding*, as we see next.

Let a *collision* be the event when a fingerprint of x leads its holder to the conclusion that "$x = y$", even though the two strings are different. Denote by ε_+ the maximum collision probability, taken over all pairs $x \neq y$. Let ε_- be the maximum probability over all x's that the fingerprint holder declares "$x \neq y$", conditional upon $y = x$. Denote $\varepsilon \overset{\text{def}}{=} \max\{\varepsilon_+, \varepsilon_-\}$, this is the worst case error probability of the fingerprinting scheme.

Let $\mathcal{E}_{cla}$ be a classical scheme that guarantees error at most ε. Let us fix x and its fingerprint[1], and consider the situation when the holder of the fingerprint loops through all 2^n possible values of y and makes his best (binary) guesses whether $x = y$. Let A contain those y's where the guess was "$x = y$". On the one hand, the expectation of $|A|$ is at most $(2^n - 1)\varepsilon_+ + 1$; on the other hand, $x \in A$ with probability at least $1 - \varepsilon_-$. Therefore, at least

$$\Omega\left((1-\varepsilon_-)\log\left(\frac{2^n}{2^n\varepsilon_+ + 1}\right)\right) \subseteq \Omega\left(\log\frac{1}{\varepsilon + 2^{-n}}\right)$$

[1] Note that according to our definition any nontrivial classical fingerprinting scheme must be randomized.

bits are leaked about x by its fingerprint in $\mathcal{E}_{cla}$. Accordingly, $\mathcal{E}_{cla}$ is not hiding.

The same reasoning does not apply to the case of *quantum fingerprinting schemes*, where a binary string $x \in \{0,1\}^n$ is mapped to a quantum state ρ_x, such that given any $y \in \{0,1\}^n$ one can measure ρ_x, in order to decide with high accuracy whether $x = y$. The argument fails because to make a guess whether $x = y$ one may be required to perform a quantum measurement, and such measurements can, in general, change the state of a quantum fingerprint in an irreversible way. Alternatively, one can say that the "looping trick" cannot be used because ρ_x is not necessarily cloneable.

From the practical point of view, hiding fingerprints shall be used when there is a need to allow a "semi-trusted" agent to recognize a string, but not to share with others the ability to recognize the target. Putting it differently, hiding fingerprints allow to issue an "authorization" to perform certain pattern recognition limited number of times.

1.2 Our results

We construct new quantum fingerprinting schemes that hide information about x in a way that cannot be achieved classically. For any constant c, we construct two different schemes, both mapping $x \in \{0,1\}^n$ to $O(\log n)$ qubits and guaranteeing error probability at most $1/n^c$ when $x \neq y$ and no error when $x = y$. The first scheme uses pure states and guarantees leaking of at most $O(1)$ bits; the second scheme uses mixed states and guarantees leaking of at most $1/n^c$ bits. As follows from the previous argument, these results introduce a new type of cryptographic primitives that cannot be achieved classically.

Similarly to [BCWdW01], our pure-state scheme additionally allows testing whether $x = y$, given only the fingerprints of x and y.

Our schemes are computationally efficient. Constructions themselves are probabilistic: A description of a scheme includes polynomial number of random bits, and using uniformly chosen bits results in a good construction with all but exponentially small probability. This random string is part of the definition of the scheme; in particular, it does not have to be kept in secret (e.g., the same random string may be used by everybody without compromising security). This is conceptually different from the role of randomness in every nontrivial classical fingerprinting scheme that inevitably depends on the assumption that the random seed used to build a fingerprint is not known to the adversary who chooses the strings x and y.

The "hiding guarantees" of our mixed-state schemes are optimal.[2] To demonstrate that, we construct a generic strategy for extracting information from arbitrary quantum fingerprints. This "no-go" result remains valid for several weaker notions of fingerprinting schemes than what we construct (e.g., for schemes with two-sided error; see Section 4 for more).

More formally, our main results are (cf. Theorems 3.13 and 4.5):

Theorem 1.1. *For any constant c there exist quantum fingerprinting schemes that*

- *map n-bit strings to mixed states of $O(\log n)$ qubits and whose error probability and accessible information are both bounded by $1/n^c$;*
- *map n-bit strings to pure states of $O(\log n)$ qubits, whose error probability is bounded by $1/n^c$ and accessible information is $O(1)$.*

[2] Our optimality argument can probably be tuned to show that our pure-state construction is also optimal, we have not pursued that direction.

The schemes are computationally efficient and have one-sided error with $\varepsilon_- = 0$ (answers "$x \neq y$" are always true).

Any quantum fingerprinting scheme that uses d qubits and guarantees error below $1/2 - \Omega(1)$ has accessible information $2^{-O(d)}$.

1.2.1 Our approach

Similarly to [BCWdW01], we base our fingerprinting schemes on classical error-correcting codes and use their minimal distance guarantees to argue correctness. However, for our schemes to be also *hiding* we need to require more from the underlying classical code. Namely, we want the codewords to be distributed "almost uniformly" in certain geometrical sense (cf. Lemma 3.9). To guarantee this we define *quasi-linear codes*, which can be viewed as a generalization of random linear codes (cf. Section 3.1).

It is very likely that some explicit classical code might have the desired properties; even if that is the case, we find it more convenient to use polynomial amount of randomness in order to keep our construction simpler.[3]

1.2.2 Communication complexity perspective

The notion of quantum fingerprints has been introduced in [BCWdW01] mainly in the context of *communication complexity*. The main conceptual contribution of the present work is to view quantum fingerprints as a cryptographic primitive. Nevertheless, our results can be interpreted in the language of communication complexity, as follows.

The most common communication complexity scenario is the one where two players, Alice and Bob, receive two parts of input, x and y, respectively. The players communicate in order to compute the value of certain function $f(x, y)$, trying to minimize the amount of communication. Various models exist that define the constraints that Alice and Bob have to obey when they compute $f(x, y)$. Relevant to us are the following two:

- *One-way communication* is a model where Alice sends a single message to Bob, who has to give an answer based on that message and his input y.
- *Simultaneous Message Passing (SMP)* is a model involving a third participant, *a referee*. Here both Alice and Bob send one message each to the referee, who has to give an answer based on the received messages.[4]

In both the cases the players are computationally unlimited, and the *cost* of a communication protocol equals the total number of sent bits. Quantum analogues of the models can be defined, where players send qubits and locally perform arbitrary unitary transformations.

One of the most basic communication problems corresponds to the *equality* predicate, where the goal of the players is to decide whether $x = y$. In general, fingerprinting schemes can be naturally viewed as solutions to the equality problem, as follows.

[3] It is natural to view the error-correcting properties of classical codes as a sort of "pseudorandomness". Then in order to guarantee hiding properties of our schemes we require the underlying classical code to be pseudorandom in a much stronger sense than just having large minimum distance, as captured in the statement of Lemma 3.9. The question whether those pseudorandom properties can be granted by an explicit classical code might be of independent interest.

[4] We consider the version of SMP without shared randomness.

In the model of SMP, Alice and Bob both send the fingerprints of, respectively, x and y to the referee. Then the referee performs the swap test that would always return “equal” if $x = y$ and would have positive constant probability of returning “not equal” if $x \neq y$. Thus, he can answer whether $x = y$ with one-sided constant error.

This idea was used in [BCWdW01] to get a quantum protocol of cost $O(\log n)$, which implied exponential separation between the quantum and the classical versions of the SMP model (it had been shown by Newman and Szegedy [NS96] that the classical complexity is $\Omega(\sqrt{n})$). Our pure-state scheme can be used instead, to get a quantum protocol of similar cost. The benefit would be that hiding properties of the scheme would make the protocol secure, in the sense that an “eavesdropper” can learn *at most $O(1)$ bits* of information about the input (x, y). Prior to our work this was not known to be possible (unless shared randomness was available, which turned the equality problem into trivial even classically). Note that the argument of [NS96] can be modified to show that any classical SMP protocol (even a very long one) for equality leaks at least $\Omega(\sqrt{n})$ bits about the input.

In the model of one-way communication, our mixed-state hiding fingerprinting scheme translates trivially to a protocol of cost $O(\log n)$ that solves the equality problem with error at most $1/\operatorname{poly}$ and leaks at most $1/\operatorname{poly}$ bits about the input. On the other hand, our classical impossibility argument implies that any classical protocol that solves the equality problem with error ε necessarily leaks $\Omega(\log(1/\varepsilon))$ bits about the input, and this is true for protocols of any cost.

1.2.3 Subsequent work

Soon after a preprint of this work had been circulated, Fawzi, Hayden and Sen [FHS11] came up with an alternate construction of a mixed-state hiding fingerprinting scheme that has both advantages and disadvantages in comparison to our constructions.[5]

2 Preliminaries and more

Here we state only those technical lemmas that are relevant for the first part of the paper (construction and analysis of the new fingerprinting schemes). Lemmas that will be used only in the second part of the paper (showing optimality of our schemes) will be stated is Section 4.1.

We write $\exp(x)$ and $\operatorname{sg}(x)$ to denote e^x and $(-1)^x$, respectively. We write $\log$ to denote the natural logarithm and $\log_2$ for the logarithm to the base 2. We denote $\mathrm{i} = \sqrt{-1}$ (to be distinguished from the variable i).

We let $\mathbb{N} = \{1, 2, \ldots, \}$ and $[i] = \{1, 2, \ldots, i\}$. We often implicitly assume the natural correspondence between the elements of $[2^n]$ and those of $\{0,1\}^n$. For any finite set A we let $\mathcal{U}_A$ denote the uniform probability distribution over the elements of A.

We use $\circ$ to denote concatenation of strings. For any set A and $x \in A^n$ we will write x_i to address the i'th position of x; more generally, $x_{i_1,\ldots,i_k} \stackrel{\text{def}}{=} x_{i_1} \circ \cdots \circ x_{i_k}$ for $(i_1, \ldots, i_k) \in [n]^k$. For two strings x and y of the same length, we will let $d_H(x, y) \stackrel{\text{def}}{=} |\{i \,|\, x_i \neq y_i\}|$ stand for the Hamming distance.

For $D \in \mathbb{N}$, we write I_D to denote the identity operator over $\mathbb{C}^D$. For a $D \times D$ matrix X, we denote the trace norm of X by $\|X\|_1 = \operatorname{tr}\left(\sqrt{X^* X}\right)$, and the operator norm of X by $\|X\| =$

[5] The construction in [FHS11] has a stronger guarantee about leaked information than would be possible via accessible information, but requires mixed states, as opposed to our both mixed- and pure-state constructions. The proof technique of [FHS11] does not seem to apply to pure-state schemes, which are required for certain applications (e.g., in the context of SMP communication).

$\max\{|Xv| \mid |v|=1\}$.

We will mostly use Dirac's "bra-ket" notation for pure quantum states, but sometimes we will find it convenient to switch to the standard notation (e.g., both v and $|v\rangle$ will be used to denote the same unit vector in a Hilbert space). We will be addressing mixed states via their density matrices, and for $D \in \mathbb{N}$ denote by $\mathbf{Den}[D]$ the subset of $\mathbb{C}^{D\times D}$ corresponding to density matrices.

2.1 Random variables and their concentration

The Hoeffding bound will be one of our basic tools, we will use it in the following form (Theorem 2.5 in [McD98]):

Lemma 2.1. (Hoeffding bound) *Let the random variables $X_1, \ldots, X_n$ be mutually independent, satisfying $\mathbf{E}[X]_i = \mu_i$ and $a_i \le X_i \le b_i$ for some constants a_i and b_i for all i. Then for any $t > 0$,*

$$\mathbf{Pr}\left[\left|\sum X_i - \sum \mu_i\right| \ge t\right] \le 2\exp\left(\frac{-2t^2}{\sum (b_i - a_i)^2}\right).$$

The following lemma can be viewed as a generalization of the Hoeffding bound to the case of random variables taking values in $\mathbb{C}$.[6]

Lemma 2.2. *Let the random variables $X_1, \ldots, X_n$ take values in $\mathbb{C}$ and be mutually independent, satisfying $\mathbf{E}[X]_i = 0$ and $|X_i| \le c_i$ for some constants c_i for all i. Then for any $t > 0$,*

$$\mathbf{Pr}\left[\left|\sum X_i\right| \ge t\right] \le 4\exp\left(\frac{-t^2}{4\sum |c_i|^2}\right).$$

Proof. By the Hoeffding bound (Lemma 2.1), for any $u > 0$

$$\mathbf{Pr}\left[\Re\left(\sum X_i\right) \ge u\right],\ \mathbf{Pr}\left[\Im\left(\sum X_i\right) \ge u\right] \le 2\exp\left(\frac{-u^2}{2\sum |c_i|^2}\right).$$

As $|\sum X_i| \ge t$ implies that either $\Re(\sum X_i) \ge \sqrt{t^2/2}$ or $\Im(\sum X_i) \ge \sqrt{t^2/2}$, the result follows. ■

The next statement will be very convenient for proving upper bounds on expected values of random variables.

Lemma 2.3. *Let f be a monotone non-decreasing function taking non-negative values, and let Y and $\tilde{Y}$ be random variables satisfying $\mathbf{Pr}\left[\tilde{Y} \ge y\right] \ge \mathbf{Pr}[Y \ge y]$ for every y such that $f(y) > 0$. If $\mathbf{E}\left[f(\tilde{Y})\right] < \infty$ then $\mathbf{E}\left[f(\tilde{Y})\right] \ge \mathbf{E}[f(Y)]$.*

Proof. Let $Z \overset{\text{def}}{=} f(Y)$ and $\tilde{Z} \overset{\text{def}}{=} f(\tilde{Y})$. Then $Z \ge 0$ and for every $z \ge 0$ it holds that

$$\mathbf{Pr}\left[\tilde{Z} \ge z\right] \ge \mathbf{Pr}[Z \ge z].$$

Therefore,

$$\mathbf{E}[Z] = \int_0^\infty \mathbf{Pr}[Z \ge z]dz \le \int_0^\infty \mathbf{Pr}\left[\tilde{Z} \ge z\right]dz = \mathbf{E}\left[\tilde{Z}\right],$$

as required. ■

[6] We view $\mathbb{C}$ as a vector space isometric to $\mathbb{R}^2$. For the general case of random variables taking values in an Euclidean space there are known "dimension-independent" bounds. We do not use one of those, instead we state Lemma 2.2 whose proof is "dimension-dependent" but the final expression is more convenient for our purposes.

Our next goal is to prove yet another generalization of the Hoeffding bound. We will use a modification of the standard method for proving such bounds, namely the "Bernstein's trick". The next lemma is the main technical ingredient for that.

Lemma 2.4. *Let Y be a random variable satisfying $\mathbf{E}\left[Y\right] = 0, Y \geq a$ and $\mathbf{Pr}\left[Y \geq y\right] \leq \beta \exp(-\alpha(y-a))$ for all $y \geq a$ and some constants $a \leq 0$, $\beta \geq 1$ and $\alpha > 0$. Then for every $h \in (0, \alpha/2]$ and $c \in (0, 2]$,*

$$\mathbf{E}\left[\exp(hY)\right] \leq c + \exp\left(\frac{\left(\log\frac{2\beta}{c}\right)^2}{2\alpha^2}h^2\right) \leq \exp\left(c + \frac{\left(\log\frac{2\beta}{c}\right)^2}{2\alpha^2}h^2\right).$$

Proof. Denote by E_b the event that $\langle Y \leq b\rangle$, were $b \geq a + \frac{\log\beta}{\alpha}$ is a constant, and let I_b be the Boolean indicator of E_b. Then

$$\mathbf{E}\left[\exp(hY)\right] = \mathbf{E}\left[I_b \cdot \exp(hY)\right] + \mathbf{E}\left[(1 - I_b)\cdot\exp(hY)\right]. \tag{1}$$

Let Y_1 be a random variable distributed as Y modulo E_b. Then $\mathbf{E}\left[I_b \cdot \exp(hY)\right] \leq \mathbf{E}\left[\exp(hY_1)\right]$, $\mathbf{E}\left[Y_1\right] \leq \mathbf{E}\left[Y\right] = 0$, and $a \leq Y_1 \leq b$. A standard result from the theory of concentration bounds (e.g., see Lemma 2.6 in [McD98]) implies that

$$\mathbf{E}\left[\exp(hY_1)\right] \leq \exp\left(\frac{(b-a)^2}{8}h^2\right).$$

Let Y_2 be a random variable satisfying $\mathbf{Pr}\left[Y_2 \geq y\right] = \beta\exp(-\alpha(y-a))$ for all $y \geq b$. Then Lemma 2.3 implies that

$$\begin{aligned}\mathbf{E}\left[(1-I_b)\cdot\exp(hY)\right] \leq \mathbf{E}\left[(1-I_b)\exp(hY_2)\right] &= \int_b^\infty \exp(hy)\cdot\beta\alpha\exp(-\alpha(y-a))\,dy \\ &\leq \beta\alpha\int_b^\infty \exp((h-\alpha)(y-a))\,dy \leq \beta\alpha\int_b^\infty \exp(-\frac{\alpha}{2}(y-a))\,dy.\end{aligned}$$

From (1),

$$\begin{aligned}\mathbf{E}\left[\exp(hY)\right] &\leq \exp\left(\frac{(b-a)^2}{8}h^2\right) + \beta\alpha\int_b^\infty \exp(-\frac{\alpha}{2}(y-a))\,dy \\ &= \exp\left(\frac{(b-a)^2}{8}h^2\right) + 2\beta\exp(-\frac{\alpha}{2}(b-a)).\end{aligned}$$

This holds for every $b \geq a + \frac{\log\beta}{\alpha}$, therefore

$$\mathbf{E}\left[\exp(hY)\right] \leq \min\left\{\exp\left(\frac{b'^2}{8}h^2\right) + 2\beta\exp(-\frac{\alpha}{2}b')) \,\middle|\, b' \geq \frac{\log\beta}{\alpha}\right\}.$$

Let $c \in (0, 2]$ be any, and choose $b' = \frac{2}{\alpha}\log\frac{2\beta}{c}$. Then $2\beta\exp(-\frac{\alpha}{2}b') = c$ and

$$\mathbf{E}\left[\exp(hY)\right] \leq \exp\left(\frac{b'^2}{8}h^2\right) + c = \exp\left(\frac{\left(\log\frac{2\beta}{c}\right)^2}{2\alpha^2}h^2\right) + c,$$

which is the first inequality stated in the lemma. Finally,

$$c + \exp\left(\frac{\left(\log\frac{2\beta}{c}\right)^2}{2\alpha^2}h^2\right) \le (1+c)\exp\left(\frac{\left(\log\frac{2\beta}{c}\right)^2}{2\alpha^2}h^2\right) \le \exp\left(c + \frac{\left(\log\frac{2\beta}{c}\right)^2}{2\alpha^2}h^2\right),$$

as $\log(1+c) < c$ for $c > 0$. ■

We are ready to prove a new concentration bound that can be viewed as a "less demanding" analogue of the Hoeffding bound.

Theorem 2.5. *Let the random variables $X_1, \ldots, X_n$ be mutually independent, satisfying $\mathbf{E}\left[X\right]_i = \mu$, $X_i \ge a$ and $\mathbf{Pr}\left[X_i \ge x\right] \le \beta\exp(-\alpha(x-a))$ for all $x \ge a$, $i \in [n]$ and some constants $a \le 0$, $\alpha > 0$ and $\beta \ge 1$. Let $S_n \overset{def}{=} \sum X_i$ for $i \in [n]$. Then for every $t \in (0, \frac{1}{7\alpha}]$,*

$$\mathbf{Pr}\left[\frac{1}{n}S_n \ge \mu + t\right] \le \exp\left(-\frac{nt^2\alpha^2}{244\left(\log\frac{\beta}{t\alpha}\right)^2}\right).$$

Proof. By Lemma 2.4, for any $h \in (0, \alpha/2]$ and $c \in (0, 2]$

$$\mathbf{E}\left[\exp\left(h(S_n - n\mu)\right)\right] = \prod \mathbf{E}\left[\exp\left(h(X_i - \mu)\right)\right] \le \exp\left(nc + \frac{n\left(\log\frac{2\beta}{c}\right)^2}{2\alpha^2}h^2\right).$$

By Markov's inequality,

$$\mathbf{Pr}\left[S_n \ge n\mu + nt\right] \le \exp(-hnt)\,\mathbf{E}\left[\exp\left(h(S_n - n\mu)\right)\right] \le \exp\left(nc + \frac{n\left(\log\frac{2\beta}{c}\right)^2}{2\alpha^2}h^2 - hnt\right).$$

Let

$$c_0 \overset{\text{def}}{=} \frac{t^2\alpha^2}{122\left(\log\frac{\beta}{t\alpha}\right)^2} \text{ and } h_0 \overset{\text{def}}{=} \frac{t\alpha^2}{\left(\log\frac{2\beta}{c_0}\right)^2}.$$

From $t\alpha \le \frac{1}{7}$, it holds that $0 < c_0 < 1$ and $0 < h_0 < \alpha/2$. Thus we may substitute $h = h_0$ and $c = c_0$, still satisfying the requirements of Lemma 2.4. So,

$$\mathbf{Pr}\left[\frac{1}{n}S_n \ge \mu + t\right] \le \exp\left(nc_0 - \frac{nt^2\alpha^2}{2\left(\log\frac{2\beta}{c_0}\right)^2}\right).$$

It can be seen[7] that $t\alpha \le \frac{1}{7}$ and $\beta \ge 1$ imply $c_0 < t^2\alpha^2 \Big/ 4\left(\log\frac{2\beta}{c_0}\right)^2$, and therefore

$$\mathbf{Pr}\left[\frac{1}{n}S_n \ge \mu + t\right] \le \exp\left(-\frac{nc_0}{2}\right) = \exp\left(-\frac{nt^2\alpha^2}{244\left(\log\frac{\beta}{t\alpha}\right)^2}\right),$$

[7] Let $x \overset{\text{def}}{=} t\alpha$ and $f(x,\beta) \overset{\text{def}}{=} c_0 \Big/ \frac{t^2\alpha^2}{4\left(\log\frac{2\beta}{c_0}\right)^2}$, then modulo $x \in (0, \frac{1}{7}]$ and $\beta \ge 1$ it is always true that $\frac{df}{d\beta} < 0$. Let $f'(x) \overset{\text{def}}{=} f(x,1)$, then $\frac{df'}{dx} > 0$ and therefore $f(x,\beta) \le f(\frac{1}{7}, 1) < 1$.

as required. ■

2.2 ε-nets for pure states

In our proof we will need a "continuous analogue" of the union bound: Namely, for every $D \in \mathbb{N}$ we want to have some sufficiently large T, such that if certain event $E(v)$ holds with probability at most δ for any fixed vector $v \in \mathbb{C}^D$, then with probability at least $1 - T\delta$ there is no $v' \in \mathbb{C}^D$ such that $E(v')$ holds. Of course, in general that is not possible for infinite domains like $\mathbb{C}^D$; however, the situation can be helped if there exists a "relaxed" version of E that we denote by E', such that if $E(v)$ holds and $d(v, w) \leq \varepsilon$, where $d(\cdot, \cdot)$ is a measure of distance between vectors in $\mathbb{C}^D$ and ε is sufficiently small, then $E'(w)$ must also hold.

Fix ε and let $W_\varepsilon = \{w_1, \dots, w_T\}$ be a finite set of vectors from $\mathbb{C}^D$, such that for every $v \in \mathbb{C}^D$ there exists some $w_i \in W_\varepsilon$ satisfying $d(v, w_i) \leq \varepsilon$ (such sets are commonly called *ε-nets*). Assume that for any fixed $v \in \mathbb{C}^D$ the probability that $E'(v)$ holds is at most δ. Then, by the union bound, the probability that $E'(w)$ holds for some $w \in W_\varepsilon$ is at most $T\delta$. Now, if $E(v)$ holds for some $v \in \mathbb{C}^D$, then $E'(w)$ holds for at least one $w \in W_\varepsilon$, as the set contains an element at distance at most ε from v. Therefore, the probability that $E(v)$ holds for some $v \in \mathbb{C}^D$ is at most $T\delta$.

The notion of distance between vectors can be formalized in many different ways, depending on the nature of E and E'. The following definition serves our future goals.

Definition 1. *For $\varepsilon > 0$, we call a set $M \subseteq \mathbb{C}^D$ of unit vectors an* ε-net for the set of pure states in $\mathbb{C}^D$ with respect to the trace distance*, if for every unit vector $|u\rangle \in \mathbb{C}^D$ there exists $|v\rangle \in M$, such that $\left\| |u\rangle\langle u| - |v\rangle\langle v| \right\|_1 \leq \varepsilon$.*

The following lemma is a slight improvement over Lemma II.4 of [HLSW04] and Lemma 4 of [BHL$^+$05], where the upper bound on the size of the ε-net was $(5/\varepsilon)^{2D}$.

Lemma 2.6. *For every $0 < \varepsilon \leq 2$, there exists an ε-net for the set of pure states in $\mathbb{C}^D$ with respect to the trace distance whose size is at most $(4/\varepsilon)^{2(D-1)}$.*

The proof of the lemma is given in the appendix.

3 New quantum fingerprinting schemes and their properties

We will use the standard way to construct a (pure-state) quantum fingerprinting scheme based on a classical error-correcting code. Namely, given a code C from n to 2^d bits, we will define, for every $a \in \{0,1\}^n$, its fingerprint on d qubits via $|u_a\rangle = \frac{1}{2^{d/2}} \sum_{i \in [2^d]} \mathrm{sg}(b_i) |i\rangle$, where $b = (b_1, \dots, b_{2^d}) = C(a)$.

It would be very convenient for us to use a purely random code C; however we cannot afford that as we want our construction to be computationally efficient. On the other hand, we can get an efficient construction by using a random linear C, however it turns out that such code would not be "random enough" for our needs (we need more randomness to guarantee that a scheme is hiding). So, we define a new type of classical codes that still admit efficient encoding but contain more randomness than random linear codes.[8]

[8] Note that in the context of quantum fingerprinting there is no need to ever decode the underlying classical code, in particular using a random linear code would be computationally feasible, despite the fact that no efficient decoding is known for such codes.

3.1 Random quasi-linear codes

In the following definition we use 2^d to denote the codewords' length in order to make the notation more consistent throughout the paper.

One of the core ingredients of our constructions will be *quasi-linear codes* that can be viewed, informally, as the bit-wise xor of an *arbitrary code* applied to the first r bits of an input with a *linear code* applied to the last $(n-r)$ bits, for some parameter r.

Definition 2. *Let $r, n, d \in \mathbb{N}$, $r < n < 2^d$. An $(n, r, 2^d)$-*quasi-linear code *C is represented by an 2^d-tuple of $(n-r)$-bit vectors $(c_1, \ldots, c_{2^d})$ and a 2^r-tuple of 2^d-bit vectors $(d_1, \ldots, d_{2^r})$. For every $a \in \{0,1\}^n$ we denote $a^{(1)} \overset{\text{def}}{=} a|_{1,\ldots,r}$, $a^{(2)} \overset{\text{def}}{=} a|_{r+1,\ldots,n}$, and define*

$$C(a) \overset{\text{def}}{=} d_{a^{(1)}} \oplus \left(\left\langle c_i, a^{(2)} \right\rangle \right)_{i=1}^{2^d},$$

where $\oplus$ denotes bit-wise xor.

For the rest of the paper we will write $x^{(1)}$ and $x^{(2)}$ to address, respectively, $x|_{1,\ldots,r}$ and $x|_{r+1,\ldots,n}$, when n, r and $x \in \{0,1\}^n$ are clear from the context.

Obviously, $C(a)$ can be computed efficiently when $r \in O(\log n)$ and $d \in O(\log(n))$. We call a quasi-linear code (uniformly) random if both $(c_1, \ldots, c_{2^d})$ and $(d_1, \ldots, d_{2^r})$ are selected uniformly at random. We will denote this distribution by $\mathcal{U}_C$ and write $C \sim \mathcal{U}_C$ to say that C is chosen uniformly at random (the values of the parameters n, r and d will be clear from the context). Note that efficient description of such code is possible as long as $r \in O(\log n)$ and $d \in O(\log(n))$.

As random objects, quasi-linear codes have higher entropy that linear ones, and this will be one of the main reasons for using them in our constructions: In order to guarantee hiding properties of our schemes we will need "more randomness" than linear codes contain.

Denote $\gamma_C \overset{\text{def}}{=} \max\left\{ \left| d_H\left(C(a_1), C(a_2)\right) - 2^{d-1} \right| \,\middle|\, a_1 \neq a_2 \right\}$. The following property of random quasi-linear codes can be viewed as a generalization of the notion of minimal distance.

Lemma 3.1. *For every $t > 0$, $\mathbf{Pr}_{C \sim \mathcal{U}_C}\left[\gamma_C \geq t\right] < 2\exp\left(n + r - \frac{2t^2}{2^d}\right)$.*

Proof. Define $A_C \overset{\text{def}}{=} \{C(a_1) \oplus C(a_2) \,|\, a_1 \neq a_2\}$. Observe that $A_C = B_1 \oplus B_2 \cup B_1 \cup B_2$, where $\oplus$ is element-wise, $B_1 = \{d_{a_1} \oplus d_{a_2} \,|\, a_1, a_2 \in \{0,1\}^r; a_1 \neq a_2\}$ and

$$B_2 = \left\{ \left(\langle c_i, a_1 \oplus a_2 \rangle\right)_{i=1}^{n-r} \,\middle|\, a_1, a_2 \in \{0,1\}^{n-r}; a_1 \neq a_2 \right\} = \left\{ \left(\langle c_i, a \rangle\right)_{i=1}^{n-r} \,\middle|\, 0 \neq a \in \{0,1\}^{n-r} \right\}.$$

Direct counting reveals that $|A_C| \leq 2^{n+r}$.

It is easy to see that for every $a_1 \neq a_2$ the string $C(a_1) \oplus C(a_2)$ is chosen uniformly at random from $\{0,1\}^{2^d}$ when $C \sim \mathcal{U}_C$. By the Hoeffding bound (Lemma 2.1), for every $t > 0$

$$\mathop{\mathbf{Pr}}_{C \sim \mathcal{U}_C}\left[\left| d_H\left(C(a_1), C(a_2)\right) - 2^{d-1} \right| \geq t \right] \leq 2\exp\left(\frac{-2t^2}{2^d} \right),$$

and the union bound implies the statement of the lemma. ∎

3.2 Pure-state scheme

For the rest of the paper we assume that $d \in O(\log n)$ and that $r \in O(\log n)$.

First, we define and analyze our fingerprinting scheme that uses pure states. Afterwords (Section 3.3) we will consider a mixed-state scheme that can be viewed as a generalization.

Definition 3. *Let C be an $(n, r, 2^d)$-quasi-linear code, we denote by $\mathcal{E}^C_{pure}$ the following fingerprinting scheme. Every $a \in \{0,1\}^n$ is mapped to*

$$|u_a\rangle = \frac{1}{2^{d/2}} \sum_{i \in [2^d]} \mathrm{sg}(b_i) \, |i\rangle \, ,$$

where $b = (b_1, \ldots, b_{2^d}) = C(a)$. We call $|u_a\rangle$ the fingerprint *of a.*

Given $|u_{a_1}\rangle$ and any $a_2 \in \{0,1\}^n$, in order to check whether $a_1 = a_2$ one should measure $|u_{a_1}\rangle$ w.r.t. the projective measurement $\{P_{a_2}, I_{2^d} - P_{a_2}\}$, where $P_{a_2} = |u_{a_2}\rangle\langle u_{a_2}|$. If the outcome corresponds to P_{a_2} then "$a_1 = a_2$" shall be returned, otherwise the guess should be "$a_1 \neq a_2$".

Note that the transformation $a \rightarrow |u_a\rangle$ can be computed efficiently as long as $C(a)$ is easy to compute for every a, and that the required projective measurement can be performed efficiently because $d \in O(\log(n))$ and $|u_{a_2}\rangle$ is known.

It can be seen that our construction closely resembles that of [BCWdW01], but uses random quasi-linear codes. A random linear code was enough to get a valid fingerprinting scheme; however, it turned out that in order to argue hiding properties we needed something that could be viewed as a "more global uniformity" than just the minimal distance requirement, as formalized in the statement of Lemma 3.9. We had to put more entropy into the definition of our codes in order to be able to show that the desired property is likely to hold.

Intuitively, the fingerprints corresponding to different pre-images should be nearly orthogonal. This is formalized by the following lemma.

Lemma 3.2. *For $\{|u_a\rangle \,|\, a \in \{0,1\}^n\}$ defined over a randomly chosen $(n, r, 2^d)$-quasi-linear code C, for any $\delta > 0$ it holds that $\max\{|\langle u_{a_1}|u_{a_2}\rangle| \,|\, a_1 \neq a_2\} < \delta$ with probability at least $1 - 2\exp(n + r - \delta^2 2^{d-1})$.*

Proof.

$$|\langle u_{a_1}|u_{a_2}\rangle| = \frac{1}{2^d} \left| \sum_{i \in [2^d]} \mathrm{sg}\left(b_{1i} + b_{2i}\right) \right| = \left| 2\frac{d_H\left(b_1, b_2\right)}{2^d} - 1 \right| \leq \frac{2\gamma_C}{2^d},$$

where $b_1 = C(a_1)$ and $b_2 = C(a_2)$. By Lemma 3.1,

$$\mathop{\mathbf{Pr}}_{C \sim \mathcal{U}_C} \left[\frac{2\gamma_C}{2^d} \geq \delta \right] < 2\exp\left(n + r - \delta^2 2^{d-1}\right),$$

as required. ■

Now let us see that $\mathcal{E}^C_{pure}$ is likely to be a valid fingerprinting scheme.

Lemma 3.3. *For $\mathcal{E}^C_{pure}$ defined over a randomly chosen $(n, r, 2^d)$-quasi-linear code C, it holds that $\varepsilon_- = 0$ always and that $\varepsilon_+ < \delta$ with probability at least $1 - 2\exp\left(n + r - 2^{d-1}\delta\right)$, for any $\delta > 0$.*

Proof. Clearly, when $a_1 = a_2$ the answer is always correct, i.e., $\varepsilon_- = 0$. When, on the other hand, $a_1 \neq a_2$ the probability of the wrong answer is $|\langle u_{a_1}|u_{a_2}\rangle|^2$, and therefore by Lemma 3.2, $\varepsilon_+ < \delta$ with probability at least $1 - 2\exp(n + r - 2^{d-1}\delta)$, as required. ■

Our next goal is to show that $\mathcal{E}_{pure}^C$ defined over a randomly chosen quasi-linear code C is hiding with high probability. This will be done in stages.

Let us denote for every $a \in \{0,1\}^n$: $\rho_a \stackrel{\text{def}}{=} |u_a\rangle\langle u_a|$, $\rho'_a \stackrel{\text{def}}{=} 2^{d-n}\rho_a$, and for arbitrary $v \in \mathbb{C}^{2^d}$, $\mu_v(a) \stackrel{\text{def}}{=} \langle v|\,\rho'_a\,|v\rangle$.

We will see later (Lemma 3.8) that for almost all choices of C we have $\sum_a \rho'_a = I_{2^d}$, and therefore $\mu_v(a)$ is a probability distribution over $a \in \{0,1\}^n$ for every fixed unit vector v. Intuitively, this distribution corresponds to the "view about a" of a holder of ρ_a who has measured it and got the outcome $|v\rangle\langle v|$. Therefore, if originally a was chosen uniformly then some sort of distance between μ_v and $\mathcal{U}_{\{0,1\}^n}$ should tell us how much has been learnt about a as a result of the measurement.

The following technical statement is the key part of our upper bound on the accessible information for $\mathcal{E}_{pure}^C$.

Lemma 3.4. *Let $v \in \mathbb{C}^{2^d}$ be a unit vector and $a_0 \in \{0,1\}^n$ be fixed, and assume that $\mathcal{E}_{pure}^C$ is defined over an $(n, r, 2^d)$-quasi-linear code C, then*

$$\mathop{\mathbf{E}}_{C\sim\mathcal{U}_C}\left[\max\left\{0, \mu_v(a_0)\log\left(2^n\mu_v(a_0)\right)\right\}\right] < \frac{23}{2^n}.$$

In the view of the intuition expressed above, it shouldn't be surprising that we want to prove this kind of statement. Indeed, if μ_v is a probability distribution then $\sum_a \mu_v(a)\log\left(2^n\mu_v(a_0)\right)$ is the relative entropy between μ_v and $\mathcal{U}_{\{0,1\}^n}$.

Proof. Let

$$\omega_v^a \stackrel{\text{def}}{=} \left|\sum_{i\in[2^d]} \operatorname{sg}\left(\left\langle a^{(2)}, c_i\right\rangle \oplus d_{a^{(1)}i}\right) v_i\right|^2,$$

then $\mu_v(a_0) = \frac{\omega_v^{a_0}}{2^n}$ and for every $t \geq 0$,

$$\Pr_C\left[\mu_v(a_0) \geq \frac{t}{2^n}\right] = \mathbf{Pr}\left[\omega_v^{a_0} \geq t\right] = \mathop{\mathbf{Pr}}_{\beta_1,\ldots,\beta_{2^d}\sim\mathcal{U}_{\{-1,1\}}}\left[\left|\sum \beta_i v_i\right| \geq \sqrt{t}\right] \leq 4\exp\left(\frac{-t}{4}\right), \qquad (2)$$

where the inequality follows from Lemma 2.2 and the fact that $\|v\| = 1$.

Define $g(x) \stackrel{\text{def}}{=} \max\{0, x\log(x)\}$ and let $\tilde{\mu}$ be a random variable whose distribution satisfies $\mathbf{Pr}\left[\tilde{\mu} \geq t\right] = 4\exp(-t/4) \stackrel{\text{def}}{=} f(t)$ for $t \geq 8\log 2$. Then

$$\mathbf{E}\left[\max\left\{0, \mu_v(a_0)\log\left(2^n\mu_v(a_0)\right)\right\}\right] \leq \frac{1}{2^n}\mathbf{E}\left[g(2^n\mu_v(a_0))\right] \leq \frac{1}{2^n}\mathbf{E}\left[g(\tilde{\mu})\right],$$

where the first inequality follows from the definition of $g(\cdot)$ and the second one is by Lemma 2.3 (whose requirements are implied by (2) and g's definition).

Finally,

$$\mathbf{E}\left[g(\tilde{\mu})\right] = \int_{8\log 2}^{\infty} x\log(x)\left(-\frac{df}{dx}\right)dx = \int_{8\log 2}^{\infty} \exp(\log x + \log\log x - x/4)\,dx < 23,$$

as required. ■

At this point we suspend our analysis of $\mathcal{E}^C_{pure}$ and turn to a mixed-state scheme $\mathcal{E}^C_{mix}$. Analysis of $\mathcal{E}^C_{pure}$ will be resumed and merged with that of $\mathcal{E}^C_{mix}$ in Section 3.4.

3.3 Mixed-state scheme

To define our mixed-state scheme we introduce another parameter $k \in \mathbb{N} \cup \{0\}$, such that 2^k is the rank of every fingerprint (i.e., $k = 0$ corresponds to a pure-state scheme). It will always be assumed, often implicitly, that $d \geq k$ and $r \geq k$ (the second assumption is probably less obvious, we need it for technical reasons). Recall that $\circ$ denotes concatenation of strings.

Definition 4. *Let C be an $(n + k, r, 2^d)$-quasi-linear code, where $d \geq k$ and $r \geq k$. We denote by $\mathcal{E}^C_{mix}$ the following fingerprinting scheme. For every $x \in \{0, 1\}^{n+k}$ we let*

$$|u_x\rangle = \frac{1}{2^{d/2}} \sum_{i\in[2^d]} \mathrm{sg}(b_i)\, |i\rangle\,,$$

where $b = (b_1, \ldots, b_{2^d}) = C(x)$. Every $a \in \{0, 1\}^n$ is mapped to

$$\rho_a = \frac{1}{2^k} \sum_{i\in\{0,1\}^k} |u_{i\circ a}\rangle\!\langle u_{i\circ a}|\,.$$

We call ρ_a the fingerprint *of a.*

Given ρ_{a_1} and any $a_2 \in \{0, 1\}^n$, in order to check whether $a_1 = a_2$ one should measure ρ_{a_1} w.r.t. the POVM measurement $\{P_{a_2}, I_{2^d} - P_{a_2}\}$, where P_{a_2} is the projection to the subspace of $\mathbb{R}^{2^d}$ that is spanned by $\left\{u_{i\circ a_2} \;\middle|\; i \in \{0, 1\}^k\right\}$. If the outcome corresponds to P_{a_2} then "$a_1 = a_2$" shall be returned, otherwise the guess should be "$a_1 \neq a_2$".

Note that when $k = 0$ the above definition gives $\mathcal{E}^C_{pure}$, and the notions of $|u_a\rangle$ and ρ_a coincide with those considered in Section 3.2. To construct ρ_a, the holder of a tosses $i \sim \mathcal{U}_{\{0,1\}^k}$, produces $|u_{i\circ a}\rangle\!\langle u_{i\circ a}|$ and then erases i. The measurement $\{P_a, I_{2^d} - P_a\}$ can also be performed efficiently (as any explicit measurement on $O(\log n)$ qubits), the simplest way to do so is to represent the measurement as a projection in $\mathbb{C}^{2^{d+1}}$ (recall that $d \in O(\log(n))$) and perform that, using an auxiliary space of dimension 2^d.

To see that $\mathcal{E}^C_{mix}$ is a valid fingerprinting scheme with high probability, we will use Lemma 3.2 together with the following technical lemma.

Lemma 3.5. *For $0 \leq i < 2^r$, let M be any mapping from an i-tuple of unit vectors in $\mathbb{R}^{2^d}$ to a unit vector in $\mathbb{R}^{2^d}$. Then for any $s \in \{0, 1\}^{n-r}$, $\delta > 0$, and $\{|u_a\rangle \,|\, a \in \{0, 1\}^n\}$ defined over a randomly chosen $(n, r, 2^d)$-quasi-linear code C, it holds that $\left|\langle M(u_{0\circ s}, \ldots, u_{(i-1)\circ s}) | u_{i\circ s}\rangle\right| < \delta$ with probability at least $1 - 2\exp(-\delta^2 2^{d-1})$.*

Proof. Note that by the construction of quasi-linear codes, $|u_{i\circ s}\rangle$ is a uniformly random element of $\left\{2^{-d/2} \sum_k \beta_k |k\rangle \;\middle|\; \beta_1, \ldots, \beta_{2^d} \in \{-1, 1\}\right\}$, even if conditioned upon $v \overset{\text{def}}{=} M(u_{0\circ s}, \ldots, u_{(i-1)\circ s})$. So,

$$\Pr_C\left[\left|\langle M(u_{0\circ s}, \ldots, u_{(i-1)\circ s}) | u_{i\circ s}\rangle\right| < \delta\right] = \Pr_C\left[\left|\sum_{k\in[2^d]} \beta_k v_k\right| < 2^{d/2}\delta\right] \geq 1 - 2\exp(-2^{d-1}\delta^2),$$

where the inequality follows from the Hoeffding bound (Lemma 2.1) and the fact that $\|v\| = 1$. ■

Let us see that $\mathcal{E}^C_{mix}$ is likely to be a valid fingerprinting scheme.

Lemma 3.6. *For $\mathcal{E}^C_{mix}$ defined over a randomly chosen $(n+k, r, 2^d)$-quasi-linear code C, it holds that $\varepsilon_- = 0$ with certainty and $\varepsilon_+ < \delta$ with probability higher than $1 - 3\exp(n+r+k-\delta^2 2^{d-4k-7})$, for any $\delta > 0$.*

Proof. Clearly, when $a_1 = a_2$ the answer is always correct, i.e., $\varepsilon_- = 0$.

When, on the other hand, $a_1 \neq a_2$, the probability of the wrong answer is $\mathrm{tr}(P_{a_2}\rho_{a_1})$. Let $P'_{a_2} \overset{\text{def}}{=} \sum_{i\in\{0,1\}^k} u_{i\circ a_2} u^*_{i\circ a_2}$; we will see that, with high probability over $C \sim \mathcal{U}_C$, both $\mathrm{tr}(P'_{a_2}\rho_{a_1})$ and $\left|\mathrm{tr}((P_{a_2} - P'_{a_2})\rho_{a_1})\right|$ are small.

$$\mathrm{tr}\left(P'_{a_2}\rho_{a_1}\right) = \sum_{i\in\{0,1\}^k} \mathrm{tr}\left(u_{i\circ a_2} u^*_{i\circ a_2}\rho_{a_1}\right) \le 2^k \delta_C^2, \tag{3}$$

where $\delta_C \overset{\text{def}}{=} \max\left\{\left|u^*_{x_1} u_{x_2}\right| \;\middle|\; x_1 \neq x_2\right\}$.

Observe that $P_{a_2} = \sum_{i\in\{0,1\}^k} v_i v_i^*$, where v_i's are "orthonormalized $u_{i\circ a_2}$'s", as follows

$$v'_0 = v_0 \overset{\text{def}}{=} u_{0\circ a_2}; \quad v'_i \overset{\text{def}}{=} u_{i\circ a_2} - \sum_{j<i} v_j v_j^* u_{i\circ a_2}; \quad v_i \overset{\text{def}}{=} v'_i / \left|v'_i\right|.$$

Let $\Delta_i \overset{\text{def}}{=} v_i - u_{i\circ a_2}$, then

$$|\Delta_i| \le \left|u_{i\circ a_2} - v'_i\right| + \left|v_i - v'_i\right| \le 2\sum_{j=0}^{i-1}\left|v_j^* u_{i\circ a_2}\right| \le 2^k \max_j\left\{\left|v_j^* u_{i\circ a_2}\right|\right\},$$

and

$$\begin{aligned}\left|\mathrm{tr}((P_{a_2} - P'_{a_2})\rho_{a_1})\right| &\le \left\|P_{a_2} - P'_{a_2}\right\| \\ &\le \sum_{i\in\{0,1\}^k} \left\|(u_{i\circ a_2} + \Delta_i)(u^*_{i\circ a_2} + \Delta_i^*) - (u_{i\circ a_2}u^*_{i\circ a_2})\right\| \\ &\le 3\cdot 2^k \max_i\{|\Delta_i|\} \le 3\cdot 2^{2k} \max_{0\le j<i<2^k}\left\{\left|v_j^* u_{i\circ a_2}\right|\right\}.\end{aligned} \tag{4}$$

Now we apply Lemma 3.5, where M is the mapping that, according to our orthonormalization process, maps $(u_{k\circ a_2})_{k=0}^{j}$ to v_j. For fixed a_2 and $j < i$, the lemma guarantees that $3\cdot 2^{2k}\left|v_j^* u_{i\circ a_2}\right|$ is less than $\delta/2$ with probability at least $1 - 2\exp(-\delta^2 2^{d-4k-3}/9)$. By the union bound, the right-hand side of (4) is less than $\delta/2$ with probability at least $1 - 2^{2k}\exp(-\delta^2 2^{d-4k-3}/9) > 1 - \exp(2k - \delta^2 2^{d-4k-7})$. Another application of the union bound implies that the same holds for every a_2 with probability higher than $1 - \exp(n + 2k - \delta^2 2^{d-4k-7})$.

By Lemma 3.2, it holds that the right-hand side of (3) is less than $\delta/2$ (i.e., $2^k\delta_C^2 < \delta/2$) with probability at least $1 - 2\exp(n + r + k - \delta 2^{d-k})$. Therefore, $\mathrm{tr}(P_{a_2}\rho_{a_1}) < \delta$ for every $a_1 \neq a_2$ with probability higher than $1 - 3\exp(n + r + k - \delta^2 2^{d-4k-7})$, as required. ■

Our next step is a statement analogous to Lemma 3.4 that would apply to $\mathcal{E}^C_{mix}$. As before, we let $\rho'_a = 2^{d-n}\rho_a$ and $\mu_v(a) = \langle v|\,\rho'_a\,|v\rangle$ for arbitrary $v \in \mathbb{C}^{2^d}$.

Lemma 3.7. *Let $v \in \mathbb{C}^{2^d}$ be a unit vector and $a_0 \in \{0,1\}^n$ be fixed, and assume that $\mathcal{E}_{mix}^{C}$ is defined over an $(n+k, r, 2^d)$-quasi-linear code C, where $2^k \in \omega(\log n)$ and $d \in O(\log(n))$. Then*

$$\mathop{\mathbf{E}}_{C \sim \mathcal{U}_C}\left[\max\left\{0, \mu_v(a_0)\log\left(2^n \mu_v(a_0)\right)\right\}\right] \in O\left(\frac{1}{2^{n+k\left(\frac{1}{2}-\lambda\right)}}\right)$$

for every $\lambda > 0$.

We will follow in the footsteps of our proof of Lemma 3.4, however we will have to use somewhat "heavier" concentration tools.

Proof. For every $j \in \{0,1\}^k$, let

$$\omega_v^a(j) \overset{\text{def}}{=} \left|\sum_{i \in [2^d]} sg\left(\left\langle x^{(2)}, c_i\right\rangle \oplus d_{{x^{(1)}}_i}\right) v_i\right|^2,$$

where $x = j \circ a$. Then $\mu_v(a_0) = \frac{1}{2^{n+k}} \sum_{j \in \{0,1\}^k} \omega_v^{a_0}(j)$.

For every j,

$$\mathop{\mathbf{E}}_{C \sim \mathcal{U}_C}\left[\omega_v^{a_0}(j)\right] = \mathop{\mathbf{E}}_{\beta_1,\ldots,\beta_{2^d} \sim \mathcal{U}_{\{-1,1\}}}\left[\sum_{i,j} \beta_i \beta_j v_i v_j\right] = \|v\|^2 = 1$$

and $\mathbf{E}\left[\mu_v(a_0)\right] = 1/2^n$. Moreover, as we've seen in the proof of Lemma 3.4, from Lemma 2.2 and from $\|v\| = 1$ it follows that that for every $t \geq 0$, $\mathbf{Pr}\left[\omega_v^{a_0}(j) \geq t\right] \leq 4\exp(-t/4)$. Therefore, by Theorem 2.5 it holds that

$$\mathop{\mathbf{Pr}}_{C}\left[\mu_v(a_0) \geq \frac{1+t}{2^n}\right] \leq \exp\left(\frac{-2^k t^2}{3904\left(\log\frac{16}{t}\right)^2}\right) \overset{\text{def}}{=} f(t)$$

for $0 < t \leq 4/7$. Besides, it holds that $0 \leq \omega_v^{a_0}(j) \leq 2^d$.

As before, we define $g(x) \overset{\text{def}}{=} \max\{0, x\log(x)\}$ and let $\tilde{\mu}$ be a new random variable that will replace $\mu_v(a_0)$ in further analysis. We define the distribution of $\tilde{\mu}$ by demanding that $\mathbf{Pr}\left[\tilde{\mu} \geq 1+t\right] = f(t)$ for $0 < t \leq 4/7$ and $\mathbf{Pr}\left[\tilde{\mu} = 2^d\right] = f(4/7)$. The requirements of Lemma 2.3 are satisfied by $g(\cdot)$, μ and $\tilde{\mu}$, and therefore

$$\mathbf{E}\left[\max\left\{0, \mu_v(a_0)\log\left(2^n \mu_v(a_0)\right)\right\}\right] \leq \frac{1}{2^n}\,\mathbf{E}\left[g(\tilde{\mu})\right].$$

By the definition,

$$\mathbf{E}\left[g(\tilde{\mu})\right] = \int_0^{4/7} (1+x)\log(1+x)\left(-\frac{df}{dx}\right)dx + 2^d d \cdot f(4/7).$$

Clearly, $f(4/7) \in \exp\left(-\Omega\left(2^k\right)\right)$ and $(1+x)\log(1+x)\left(-\frac{df}{dx}\right) \leq 2^k x^2 f(x)$. For every $\lambda > 0$ there exists $A_\lambda > 0$, such that $f(x) \leq \exp\left(-A_\lambda 2^k x^{2+\lambda}\right)$ for $0 < x \leq 4/7$. So,

$$\begin{aligned}\mathbf{E}\left[g(\tilde{\mu})\right] &< \int_0^{\infty} 2^k x^2 \exp\left(-A_\lambda 2^k x^{2+\lambda}\right)dx + \exp\left(d + \log d - \Omega\left(2^k\right)\right)\\ &\leq \frac{2^k}{(2+\lambda)\left(A_\lambda 2^k\right)^{\frac{3}{2+\lambda}}} \cdot \Gamma\left(\frac{3}{2+\lambda}\right) + \exp(d - \Omega\left(2^k\right)),\end{aligned}$$

where $\Gamma(a) \overset{\text{def}}{=} \int_0^\infty x^{a-1} \exp(-x)\, dx$ is the Gamma-function. Therefore for $2^k \in \omega(\log n)$ and every $\lambda > 0$,

$$\mathbf{E}\left[g(\tilde{\mu})\right] \leq O\left(\frac{1}{2^{k\left(\frac{1}{2}-\lambda\right)}}\right),$$

as required. ■

3.4 Further security analysis of $\mathcal{E}_{pure}^{C}$ and $\mathcal{E}_{mix}^{C}$

Based on Lemmas 3.4 and 3.7, we continue our analysis of $\mathcal{E}_{pure}^{C}$ and $\mathcal{E}_{mix}^{C}$. From this point on and unless stated otherwise, we view the former as a special case of the latter, corresponding to $k = 0$.

First, as promised earlier, we prove that for almost all quasi-linear codes C, we have $\sum_a \rho'_a = I_{2^d}$.

Lemma 3.8. *If C is an $(n+k, r, 2^d)$-quasi-linear code such that the vectors $c_1, \ldots, c_{2^d}$ are all distinct, then $\sum_a \rho'_a = I_{2^d}$. In particular, if an $(n+k, r, 2^d)$-quasi-linear code C is chosen uniformly at random, then $\sum_a \rho'_a = I_{2^d}$ with probability at least $1 - 2^{2d+r-n-k}$.*

Proof. If $c_1, \ldots, c_{2^d}$ are all distinct, then

$$\sum_a \rho'_a = 2^{d-n-k} \sum_{x \in \{0,1\}^{n+k}} |u_x\rangle\langle u_x|$$

$$= 2^{-n-k} \sum_{x^{(1)}} \sum_{i,j} \mathrm{sg}\left((d_{x^{(1)}})_i \oplus (d_{x^{(1)}})_j\right) \left(\sum_{x^{(2)}} \mathrm{sg}\langle c_i \oplus c_j, x^{(2)}\rangle\right) |i\rangle\langle j| = I_{2^d},$$

where $x^{(1)} \in \{0,1\}^r$, $x^{(2)} \in \{0,1\}^{n+k-r}$, and $i, j \in [2^d]$.

Now let $C \sim \mathcal{U}_C$. For any fixed distinct i and j, c_i equals c_j with probability 2^{r-n-k}. By the union bound, the probability that all c_i's are distinct is at least

$$1 - \binom{2^d}{2} \cdot 2^{r-n-k} < 2^{2d+r-n-k},$$

as desired. ■

Next we will argue that $\sum_{a \in \{0,1\}^n} \mu_v(a) \log\left(2^n \mu_v(a)\right)$ is unlikely to be large when $C \sim \mathcal{U}_C$. Technically, the following statement is the reason why we need all the randomness present in quasi-linear codes in order to argue hiding properties of our schemes.

Lemma 3.9. *Let $v \in \mathbb{C}^{2^d}$ be a unit vector and assume that C is a uniformly random $(n+k, r, 2^d)$-quasi-linear code, then for every $\delta > 0$*

$$\Pr_C\left[\sum_{a \in \{0,1\}^n} \mu_v(a) \log\left(2^n \mu_v(a)\right) > \alpha_k + \delta\right] < \exp\left(n - 2^{r-k-2d}\left(\frac{\delta}{d}\right)^2\right),$$

where $\alpha_0 < 23$, and $\alpha_k \in O\left(1/2^{k(1/2-\lambda)}\right)$ for $2^k \in \omega(\log n)$ and any $\lambda > 0$.

Proof. We will use concentration bounds in conjunction with the mean guarantees of Lemmas 3.4 and 3.7.

Define new random variables

$$\tilde{\mu}(a) \stackrel{\text{def}}{=} \max\left\{0, \mu_v(a)\log\left(2^n\mu_v(a)\right)\right\},$$

then $0 \le \tilde{\mu}(a) \le 2^{d-n}d$. From Lemmas 3.4 and 3.7 we know that $\mathbf{E}_C\left[\tilde{\mu}(a)\right] < 23/2^n$ for $k = 0$ and every $\lambda > 0$, and $\mathbf{E}_C\left[\tilde{\mu}(a)\right] \in O\big(1/2^{n+k(1/2-\lambda)}\big)$ for $2^k \in \omega(\log n)$.

We want to bound the probability that $\sum_a \tilde{\mu}(a) > \delta$. Let $t \stackrel{\text{def}}{=} r - k$, assume w.l.g. that $t > 0$ and define

$$A_i \stackrel{\text{def}}{=} \left\{j \circ i \;\middle|\; j \in \{0,1\}^t\right\}$$

for every $i \in \{0,1\}^{n-t}$. Observe that for every $i_0 \in \{0,1\}^n$ the random values $\Big(C(a)\Big)_{a\in A_{i_0}}$ are distributed identically and independently when $C \sim \mathcal{U}_C$, and the same is true for $\Big(\tilde{\mu}(a)\Big)_{a\in A_{i_0}}$. Therefore the Hoeffding bound (Lemma 2.1) can be applied, resulting in

$$\mathop{\mathbf{Pr}}_U\left[\sum_{a\in A_{i_0}}\tilde{\mu}(a) > \frac{2^n\mu_0+\delta}{2^{n-t}}\right] < 2\exp\left(\frac{-2^{t+1}\delta^2}{2^{2d}d^2}\right),$$

where $\mu_0 \stackrel{\text{def}}{=} \mathbf{E}_C\left[\tilde{\mu}(a)\right]$. Therefore, from the union bound:

$$\mathop{\mathbf{Pr}}_U\left[\sum_{a\in\{0,1\}^n}\tilde{\mu}(a) > \alpha_k + \delta\right] < 2^{n-t+1}\exp\left(-2^{r-k-2d}\left(\frac{\delta}{d}\right)^2\right),$$

as required. ∎

As we discussed before, if $\sum_{a\in\{0,1\}^n}\mu_v(a)\log\left(2^n\mu_v(a)\right)$ is small for a fixed v, which means that, informally, a holder of ρ_a who has measured it and got the outcome $|v\rangle\langle v|$ has not learnt much about a.

Our next step will be to argue that, with high probability, $\sum_{a\in\{0,1\}^n}\mu_v(a)\log\left(2^n\mu_v(a)\right)$ is small for every pure state $|v\rangle \in \mathbb{C}^{2^d}$. According to the same intuition (which will be formalized soon), that would imply that no outcome of a measurement of ρ_a exists that can "tell much about a".

First we claim that the function $|v\rangle\langle v| \mapsto \sum_{a\in\{0,1\}^n}\mu_v(a)\log\left(2^n\mu_v(a)\right)$ has a good continuity property (called the "almost Lipschitz continuity") in order to discretize "every pure state $|v\rangle \in \mathbb{C}^{2^d}$" in the above argument.

Lemma 3.10. *Let C be an $(n+k, r, 2^d)$-quasi-linear code, such that $\sum_a \rho'_a = I_{2^d}$. Let $0 < \varepsilon \le 2/e$ and $|v\rangle$ and $|w\rangle$ be unit vectors in $\mathbb{C}^{2^d}$ such that $\left\||v\rangle\langle v| - |w\rangle\langle w|\right\|_1 \le \varepsilon$. Then,*

$$\left|\sum_a \mu_v(a)\log(2^n\mu_v(a)) - \sum_a \mu_w(a)\log(2^n\mu_w(a))\right| \le 2^{d-1}\varepsilon\log\frac{2}{\varepsilon}.$$

Proof. Fix any a and we will prove $|\mu_v(a)\log(2^{n-d}\mu_v(a)) - \mu_w(a)\log(2^{n-d}\mu_w(a))| \le 2^{d-n-1}\varepsilon\log(2/\varepsilon)$. Without loss of generality, we can assume that $\mu_v(a) \le \mu_w(a)$. Then,

$$\mu_w(a) - \mu_v(a) = 2^{d-n}\operatorname{tr}\left(\rho_a(|w\rangle\langle w| - |v\rangle\langle v|)\right) \le 2^{d-n-1}\left\||v\rangle\langle v| - |w\rangle\langle w|\right\|_1 \le 2^{d-n-1}\varepsilon.$$

Therefore,

$$\begin{aligned}
&\mu_w(a)\log(2^{n-d}\mu_w(a)) - \mu_v(a)\log(2^{n-d}\mu_v(a)) \\
&= \mu_w(a)\log(2^{n-d}\mu_w(a)) - \mu_v(a)\log(2^{n-d}\mu_w(a)) + \mu_v(a)\log(2^{n-d}\mu_w(a)) - \mu_v(a)\log(2^{n-d}\mu_v(a)) \\
&= (\mu_w(a) - \mu_v(a))\log(2^{n-d}\mu_w(a)) + \mu_v(a)\log\left(1 + \frac{\mu_w(a) - \mu_v(a)}{\mu_v(a)}\right).
\end{aligned}$$

Note that $(\mu_w(a) - \mu_v(a))\log(2^{n-d}\mu_w(a)) \leq 0$ and $\mu_v(a)\log(1 + (\mu_w(a) - \mu_v(a))/\mu_v(a)) \geq 0$. Therefore,

$$\begin{aligned}
&|\mu_v(a)\log(2^{n-d}\mu_v(a)) - \mu_w(a)\log(2^{n-d}\mu_w(a))| \\
&= \left|(\mu_w(a) - \mu_v(a))\log(2^{n-d}\mu_w(a)) + \mu_v(a)\log\left(1 + \frac{\mu_w(a) - \mu_v(a)}{\mu_v(a)}\right)\right| \\
&\leq \max\left\{-(\mu_w(a) - \mu_v(a))\log(2^{n-d}\mu_w(a)), \mu_v(a)\log\left(1 + \frac{\mu_w(a) - \mu_v(a)}{\mu_v(a)}\right)\right\} \\
&\leq \max\left\{-(\mu_w(a) - \mu_v(a))\log(2^{n-d}(\mu_w(a) - \mu_v(a))), \mu_v(a)\cdot\frac{\mu_w(a) - \mu_v(a)}{\mu_v(a)}\right\} \\
&\leq \max\left\{2^{d-n-1}\varepsilon\log\frac{2}{\varepsilon}, 2^{d-n-1}\varepsilon\right\} \\
&= 2^{d-n-1}\varepsilon\log\frac{2}{\varepsilon}.
\end{aligned}$$

By the triangle inequality, we have

$$\left|\sum_a \mu_v(a)\log(2^{n-d}\mu_v(a)) - \sum_a \mu_w(a)\log(2^{n-d}\mu_w(a))\right| \leq 2^{d-1}\varepsilon\log\frac{2}{\varepsilon}.$$

The left-hand side can be rewritten as

$$\begin{aligned}
&\left|\sum_a \mu_v(a)\log(2^{n-d}\mu_v(a)) - \sum_a \mu_w(a)\log(2^{n-d}\mu_w(a))\right| \\
&= \left|\sum_a \mu_v(a)\log(2^{n}\mu_v(a)) - \sum_a \mu_w(a)\log(2^{n}\mu_w(a)) + \left(\sum_a \mu_v(a) - \sum_a \mu_w(a)\right)\log 2^{-d}\right| \\
&= \left|\sum_a \mu_v(a)\log(2^{n}\mu_v(a)) - \sum_a \mu_w(a)\log(2^{n}\mu_w(a))\right|,
\end{aligned}$$

which completes the proof. ■

We are ready to see that with high probability, $\sum \mu_v(a)\log(2^n\mu_v(a))$ is small for every $|v\rangle$.

Lemma 3.11. *Let C be a uniformly random $(n+k, r, 2^d)$-quasi-linear code. Let $\delta > 0$ satisfy that $e^{3/2}\delta/4 \leq 2^d$. Then,*

$$\Pr_C\left[\exists\,|v\rangle : \sum_{a\in\{0,1\}^n} \mu_v(a)\log(2^n\mu_v(a)) > \alpha_k + \delta\right] < \exp\left(2^{d+1}\log\frac{2^{2d+5}}{e^2\delta^2} + n - 2^{r-k-2d}\left(\frac{\delta}{2d}\right)^2\right),$$

where α_k is as in Lemma 3.9.

Proof. Let $\varepsilon = 2^{-2d-3}e^2\delta^2$. By the assumption, we have $\varepsilon \le 2/e$. Then we have

$$2^{d-1}\varepsilon \log \frac{2}{\varepsilon} = \frac{e\delta}{2} \cdot \frac{e\delta}{2^{d+2}} \log \frac{2^{d+2}}{e\delta} \le \frac{e\delta}{2} \cdot \frac{1}{e} = \frac{\delta}{2},$$

where the inequality follows from $x\log(1/x) \le 1/e$. By Lemma 2.6, there exists an ε-net M for the set of 2^d-dimensional states with respect to the trace distance with size

$$|M| \le \left(\frac{4}{\varepsilon}\right)^{2^{d+1}} = \left(\frac{2^{2d+5}}{e^2\delta^2}\right)^{2^{d+1}}.$$

Suppose that the quasi-linear code C is such that there exists a unit vector v such that

$$\sum_{a\in\{0,1\}^n} \mu_v(a)\log\left(2^n\mu_v(a)\right) > \alpha_k + \delta.$$

Let $w \in M$ be a unit vector satisfying $\||v\rangle\langle v| - |w\rangle\langle w|\|_1 \le \varepsilon$. By Lemma 3.10,

$$\sum_{a\in\{0,1\}^n} \mu_w(a)\log(2^n\mu_w(a)) \ge \sum_{a\in\{0,1\}^n} \mu_v(a)\log(2^n\mu_v(a)) - 2^{d-1}\varepsilon\log\frac{2}{\varepsilon} > \alpha_k + \frac{\delta}{2}.$$

This implies that

$$\begin{aligned}&\mathop{\mathbf{Pr}}_{C}\left[\exists\,|v\rangle : \sum_{a\in\{0,1\}^n} \mu_v(a)\log\left(2^n\mu_v(a)\right) > \alpha_k + \delta\right]\\ &\qquad\qquad \le \mathop{\mathbf{Pr}}_{C}\left[\exists\,|w\rangle \in M\colon \sum_{a\in\{0,1\}^n} \mu_w(a)\log\left(2^n\mu_w(a)\right) > \alpha_k + \frac{\delta}{2}\right].\end{aligned}$$

By Lemma 3.9 and union bound, the right-hand side is at most

$$|M|\cdot\exp\left(n - 2^{r-k-2d}\left(\frac{\delta}{2d}\right)^2\right) \le \exp\left(2^{d+1}\log\frac{2^{2d+5}}{e^2\delta^2} + n - 2^{r-k-2d}\left(\frac{\delta}{2d}\right)^2\right),$$

as required. ■

It remains to be seen that small values of $\sum \mu_v(a)\log\left(2^n\mu_v(a)\right)$ for all $|v\rangle \in \mathbb{C}^{2^d}$ indeed imply good hiding properties of the corresponding fingerprinting scheme.

Lemma 3.12. *Let C be an $(n+k, r, 2^d)$-quasi-linear code such that $c_1, \ldots, c_{2^d}$ are all distinct. If $a \in \{0,1\}^n$ is chosen uniformly at random, then the accessible information of the ensemble (ρ_a) is at most*

$$\max_{|v\rangle} \sum_{a\in\{0,1\}^n} \mu_v(a)\log\left(2^n\mu_v(a)\right).$$

Proof. We follow a similar path to that used in a proof in Section 2.2 of Leung [Leu09]. Since the accessible information can be always achieved by a rank-one POVM, let $M = \{\alpha_j |v_j\rangle\langle v_j|\}_j$ be a rank-one POVM achieving the accessible information, where $|v_j\rangle$ is a pure state, $\alpha_j > 0$ and $\sum_j \alpha_j = 2^d$. If A is the random variable representing the choice of a and J is the random variable representing the measurement result of the state under M, then

$$\begin{aligned}
I_{\text{acc}} &= H(J) - H(J \mid A) \\
&= -\sum_j \alpha_j \langle v_j| \frac{I_{2^d}}{2^d} |v_j\rangle \log(\alpha_j \langle v_j| \frac{I_{2^d}}{2^d} |v_j\rangle) + \frac{1}{2^n} \sum_{a,j} \alpha_j \langle v_j| \rho_a |v_j\rangle \log(\alpha_j \langle v_j| \rho_a |v_j\rangle) \\
&= -\sum_j \frac{\alpha_j}{2^d} \log \frac{\alpha_j}{2^d} + \frac{1}{2^n} \sum_{a,j} \alpha_j \langle v_j| \rho_a |v_j\rangle \log \alpha_j + \frac{1}{2^n} \sum_{a,j} \alpha_j \langle v_j| \rho_a |v_j\rangle \log \langle v_j| \rho_a |v_j\rangle \\
&= -\sum_j \frac{\alpha_j}{2^d} \log \frac{\alpha_j}{2^d} + \sum_j \frac{\alpha_j}{2^d} \log \alpha_j + \frac{1}{2^n} \sum_{a,j} \alpha_j \langle v_j| \rho_a |v_j\rangle \log \langle v_j| \rho_a |v_j\rangle \\
&= d \log 2 + \frac{1}{2^n} \sum_{a,j} \alpha_j \langle v_j| \rho_a |v_j\rangle \log \langle v_j| \rho_a |v_j\rangle \\
&= d \log 2 + \frac{1}{2^n} \sum_{a,j} \alpha_j 2^{n-d} \langle v_j| \rho'_a |v_j\rangle \log(2^{n-d} \langle v_j| \rho'_a |v_j\rangle) \\
&= \sum_{a,j} \frac{\alpha_j}{2^d} \mu_{v_j}(a) \log(2^n \mu_{v_j}(a)) \\
&\leq \max_{|v\rangle} \sum_a \mu_v(a) \log(2^n \mu_v(a)),
\end{aligned}$$

where the inequality follows from the convexity argument (the convex combination is at most the maximum). ■

Lemmas 3.3, 3.6, 3.8, 3.11 and 3.12 imply the following theorem:

Theorem 3.13. *For any constant c there exist quantum fingerprinting schemes that*

- *map n-bit strings to mixed states over $O(\log n)$ qubits and whose error probability and accessible information are both bounded by $1/n^c$;*
- *map n-bit strings to pure states over $O(\log n)$ qubits, whose error probability is bounded by $1/n^c$ and accessible information is $O(1)$.*

The schemes are computationally efficient and have one-sided error with $\varepsilon_- = 0$ (answers "$x \neq y$" are always true).

Proof. Let $k = \lceil 4c \lg n \rceil$, $d = \lceil (18c + 1) \lg n \rceil$ and $r = \lceil (60c + 3) \lg n \rceil$, and let $\mathcal{E}^C_{mix}$ be the mixed-state fingerprinting scheme defined over a randomly chosen $(n + k, r, 2^d)$-quasi-linear code C. By Lemma 3.6, the probability that $\varepsilon_+ \geq 1/n^c$ vanishes as $n \to \infty$.

The probability that C violates the condition of Lemma 3.8 is negligible, so we assume the opposite, and that allows us to use Lemma 3.12. Applying Lemma 3.11 with $\delta = 1/(2n^c)$ to Lemma 3.12 and noting that $\alpha_k \in O\big(1/2^{k/3}\big) \subseteq o(1/n^c)$, we obtain that the accessible information is at most $1/n^c$.

Choosing $k = 0$ and adjusting d and r accordingly gives the desired result for $\mathcal{E}^C_{pure}$. ■

Note that only polynomial amount of randomness is required in order to describe any of our fingerprinting schemes. Moreover, a random string may be published openly without compromising the hiding guarantees of the schemes.

Mixed-state schemes can be viewed as a natural generalization of pure-state ones. Our mixed-state construction achieves much better hiding guarantees (in the following section we argue its optimality), but even the pure-state one already reaches beyond the limitations of classical schemes, where we've seen (cf. Section 1.1) that $\Omega(\log(1/\varepsilon))$ bits are leaked by any scheme with error at most ε.

4 Optimality of our schemes

In this part we construct a generic strategy for extracting information from arbitrary quantum fingerprints. For any $D \in \mathbb{N}$ we give a strategy that retrieves at least $1/\operatorname{poly}(D)$ bits of information about x from a (w.l.g., mixed-state) fingerprint of x over $\log D$ qubits.

We note that the following "no-go" argument remains valid for some weaker versions of fingerprinting than what is guaranteed by Theorem 3.13, namely:

- schemes with two-sided error;
- schemes that only work in average w.r.t. "balanced uniform" input distribution (i.e., $(x, y) \sim (\mathcal{U}_A + \mathcal{U}_B)/2$, where $A = \{(x, x)\}$ and $B = \{(x, y) \mid x \neq y\}$).

To extract classical information about unknown $x \sim \mathcal{U}_{\{0,1\}^n}$ from its fingerprint $\rho(x) \in \mathbb{C}^{D \times D}$, we apply to $\rho(x)$ a complete projective measurement

$$P_V \stackrel{\text{def}}{=} \{|v\rangle\langle v| \mid v \in V\},$$

where V is a uniformly chosen random orthonormal basis for $\mathbb{C}^D$.[9] We will see that the mutual information between the outcome of P_V and x is at least $1/\operatorname{poly}(D)$.

4.1 Technical preliminaries

Optimality of our scheme from Section 3 will follow from several technical lemmas that we state next.

It is well known that the "distinguishability" of two arbitrary quantum states σ_1 and σ_2 is determined by their trace distance $\|\sigma_1 - \sigma_2\|_1$. Informally speaking, we will show that *a randomly chosen complete projective measurement distinguishes between σ_1 and σ_2 only $\operatorname{poly}(D)$ times less efficiently than a best distinguishing measurement*.

Let $\mathcal{U}_1^D$ denote the uniform distribution of unit vectors in $\mathbb{C}^D$. The following is a well-known fact about $\mathcal{U}_1^D$.

Claim 4.1. *Sampling $v \sim \mathcal{U}_1^D$ can be realized via the following algorithm:*

1 Independently sample $u_r^1, \ldots, u_r^D$ and $u_i^1, \ldots, u_i^D$ from the standard normal distribution $N(0, 1)$.

2 Let $v \stackrel{\text{def}}{=} u/\|u\|$ where $u \stackrel{\text{def}}{=} \left(u_r^j + u_i^j \cdot \mathrm{i}\right)_{j=1}^D$.

[9] The idea of using randomly chosen projective measurements in order to prove a lower bound on accessible information has appeared in [JRW94]. However, our setting and the analysis are different.

Proof. The density function of u is spherically symmetric. ∎

We need several technical lemmas. First, let us see that the length of the projection of a randomly chosen vector $v \sim \mathcal{U}_1^D$ to any subspace cannot be "too concentrated":

Lemma 4.2. *Let $A \subset [D]$, $1 \le |A| < D$. Then for some $\eta_1 \in \Omega\left(\frac{1}{D^2 \log D}\right)$ and $\eta_2 \in \Omega\left(\frac{1}{D^2 (\log D)^4}\right)$,*

$$\mathop{\mathbf{Pr}}_{v \sim \mathcal{U}_1^D}\left[\sum_{i \in A} \left|v^i\right|^2 \ge \frac{|A|}{D} + \eta_1\right] \ge \eta_2.$$

It is easy to see (by linearity of expectation and the fact that $|v| = 1$) that $\mathbf{E}_v\left[\sum_A \left|v^i\right|^2\right] = |A|/D$, and therefore the above statement can be viewed as complementary to concentration bounds.

Proof. In the notation of Claim 4.1,

$$\begin{aligned}
\mathop{\mathbf{Pr}}_{v \sim \mathcal{U}_1^D}\left[\sum_{i \in A} \left|v^i\right|^2 \ge \frac{|A|}{D} + \varepsilon\right] &= \mathbf{Pr}\left[\sum_{i \notin A} \left|v^i\right|^2 \le 1 - \frac{|A|}{D} - \varepsilon\right] \\
&= \mathbf{Pr}\left[\frac{\sum_{i \in A} \left|v^i\right|^2}{\sum_{i \notin A} \left|v^i\right|^2} \ge \frac{|A| + D\varepsilon}{D - |A| - D\varepsilon}\right] \\
&= \mathbf{Pr}\left[\frac{\sum_{i \in A}((u_r^j)^2 + (u_i^j)^2)}{\sum_{i \notin A}((u_r^j)^2 + (u_i^j)^2)} \ge \frac{|A| + D\varepsilon}{D - |A| - D\varepsilon}\right] \\
&\ge \mathbf{Pr}\left[Y^+ \ge 2|A| + 2D\varepsilon\right] \cdot \mathbf{Pr}\left[Y^- \le 2D - 2|A| - 2D\varepsilon\right],
\end{aligned} \tag{5}$$

where $Y^+ \overset{\text{def}}{=} \sum_{i \in A}((u_r^j)^2 + (u_i^j)^2)$, $Y^- \overset{\text{def}}{=} \sum_{i \notin A}((u_r^j)^2 + (u_i^j)^2)$, and the inequality follows from Y^+ and Y^- being mutually independent.

We analyze the behavior of Y^+ and Y^-. Let "$\odot$" stand for either "$+$" or "$-$". The distribution of $Y^\odot$ is known as $\chi^2_{k^\odot}$, where $k^+ \overset{\text{def}}{=} 2|A|$ and $k^- \overset{\text{def}}{=} 2D - 2|A|$; its density function is

$$\psi^\odot(x) = \frac{1}{2^{k^\odot/2}\Gamma(k^\odot/2)} \exp\left(-\frac{x}{2}\right) x^{k^\odot/2-1}$$

(cf. [JKB94]). One can see that $\mathbf{E}\left[Y^\odot\right] = k^\odot$ and $\mathbf{E}\left[(Y^\odot)^2\right] = {k^\odot}^2 + 2k^\odot$ (thus, $\mathbf{Var}\left[Y^\odot\right] = 2k^\odot$).

For $\gamma^\odot \overset{\text{def}}{=} 5k^\odot \log(k^\odot) + 20$, let $Y^\odot_{\gamma^\odot}$ be distributed as $Y^\odot$ modulo $Y^\odot \le \gamma^\odot$. The density function of $Y^\odot_{\gamma^\odot}$ is

$$\psi^\odot_{\gamma^\odot}(x) = \begin{cases} \alpha_{\gamma^\odot}\psi(x) & \text{if } x \le \gamma^\odot \\ 0 & \text{else} \end{cases},$$

for $\alpha_{\gamma^\odot} \overset{\text{def}}{=} 1/\mathbf{Pr}\left[Y^\odot \le \gamma^\odot\right]$. Then

$$k^\odot \ge \mathbf{E}\left[Y^\odot_{\gamma^\odot}\right] = \alpha_{\gamma^\odot}\left(k^\odot - \int_{\gamma^\odot}^\infty x\psi^\odot(x)\,dx\right) \ge k^\odot - \zeta^\odot$$

and

$$\mathbf{E}\left[\left(Y^{\odot}_{\gamma^{\odot}}\right)^{2}\right] = \alpha_{\gamma^{\odot}}\left(k^{\odot 2} + 2k^{\odot} - \int_{\gamma^{\odot}}^{\infty} x^{2}\psi^{\odot}(x)\,dx\right) \geq k^{\odot 2} + 2k^{\odot} - \zeta^{\odot},$$

where

$$\zeta^{\odot} \overset{\text{def}}{=} \int_{\gamma}^{\infty} x^{2}\psi^{\odot}(x)\,dx \leq \frac{1}{2^{k^{\odot}/2}\Gamma(k^{\odot}/2)} \int_{\gamma^{\odot}}^{\infty} \exp\left(-\frac{x}{4}\right) dx \tag{6}$$

(the inequality follows from $x^{2} \cdot \exp(-x/2)x^{k^{\odot}/2-1} \leq \exp(-x/4)$, as guaranteed by our choice of $\gamma^{\odot}$). In particular, $\zeta^{\odot} < 1$ and $\mathbf{Var}\left[Y^{\odot}_{\gamma}\right] \geq 2k^{\odot} - \zeta^{\odot} > k^{\odot}$ and

$$\mathbf{E}\left[\left|Y^{\odot}_{\gamma^{\odot}} - \mathbf{E}\left[Y^{\odot}_{\gamma^{\odot}}\right]\right|\right] \geq \mathbf{Var}\left[Y^{\odot}_{\gamma^{\odot}}\right]/\gamma^{\odot} > k^{\odot}/\gamma^{\odot}. \tag{7}$$

Denote:

$$\begin{aligned}
\mu^{\odot} &\overset{\text{def}}{=} \mathbf{E}\left[Y^{\odot}_{\gamma^{\odot}}\right] & \Delta^{\odot} &\overset{\text{def}}{=} \mathbf{E}\left[\left|Y^{\odot}_{\gamma^{\odot}} - \mu^{\odot}\right|\right] \\
\mu^{\odot}_{+} &\overset{\text{def}}{=} \mathbf{E}\left[Y^{\odot}_{\gamma^{\odot}} \middle| Y^{\odot}_{\gamma^{\odot}} \geq \mu^{\odot}\right] & q^{\odot}_{+} &\overset{\text{def}}{=} \mathbf{Pr}\left[Y^{\odot}_{\gamma^{\odot}} \geq \mu^{\odot}\right] \\
\mu^{\odot}_{-} &\overset{\text{def}}{=} \mathbf{E}\left[Y^{\odot}_{\gamma^{\odot}} \middle| Y^{\odot}_{\gamma^{\odot}} < \mu^{\odot}\right] & q^{\odot}_{-} &\overset{\text{def}}{=} \mathbf{Pr}\left[Y^{\odot}_{\gamma^{\odot}} < \mu^{\odot}\right]
\end{aligned}$$

Then

$$\begin{aligned}
&q^{\odot}_{+}\mu^{\odot}_{+} + q^{\odot}_{-}\mu^{\odot}_{-} = \mu^{\odot}, \\
&q^{\odot}_{+}\left(\mu^{\odot}_{+} - \mu^{\odot}\right) + q^{\odot}_{-}\left(\mu^{\odot} - \mu^{\odot}_{-}\right) = \Delta^{\odot}, \\
&q^{\odot}_{+} + q^{\odot}_{-} = 1,
\end{aligned}$$

which implies

$$q^{\odot}_{+}\left(\mu^{\odot}_{+} - \mu^{\odot}\right) = q^{\odot}_{-}\left(\mu^{\odot} - \mu^{\odot}_{-}\right) = \Delta^{\odot}/2. \tag{8}$$

Clearly, $0 \leq Y^{\odot}_{\gamma^{\odot}} \leq \gamma^{\odot}$ implies that

$$\mathbf{Pr}\left[Y^{\odot}_{\gamma^{\odot}} \geq \mu^{\odot}_{+} - \beta\right] > \frac{q^{\odot}_{+}\beta}{\gamma^{\odot}} \quad \text{and} \quad \mathbf{Pr}\left[Y^{\odot}_{\gamma^{\odot}} \leq \mu^{\odot}_{-} + \beta\right] > \frac{q^{\odot}_{-}\beta}{\gamma^{\odot}}$$

for every $\beta > 0$. Choosing $\beta = (\mu^{+}_{+} - \mu^{+})/2$ gives

$$\mathbf{Pr}\left[Y^{+}_{\gamma^{+}} \geq \left(\mu^{+} + \mu^{+}_{+}\right)/2\right] \geq \frac{q^{+}_{+}\left(\mu^{+}_{+} - \mu^{+}\right)}{2\gamma^{+}} = \frac{\Delta^{+}}{4\gamma^{+}},$$

and similarly, via $\beta = (\mu^{-} - \mu^{-}_{-})/2$ one obtains

$$\mathbf{Pr}\left[Y^{-}_{\gamma^{+}} \leq \left(\mu^{-} + \mu^{-}_{-}\right)/2\right] \geq \frac{\Delta^{-}}{4\gamma^{-}}.$$

On the other hand, (8) implies that $\mu^{+}_{+} - \mu^{+} \geq \Delta^{+}/2$ and $\mu^{-} - \mu^{-}_{-} \geq \Delta^{-}/2$. Therefore, from (7):

$$\mathbf{Pr}\left[Y^{+}_{\gamma} \geq k^{+} - \zeta^{+} + \frac{k^{+}}{2\gamma^{+}}\right] \geq \mathbf{Pr}\left[Y^{+}_{\gamma^{+}} \geq \mu^{+} + \Delta^{+}/2\right] \geq \frac{\Delta^{+}}{4\gamma^{+}} \geq \frac{k^{+}}{4{\gamma^{+}}^{2}},$$

and similarly,

$$\mathbf{Pr}\left[Y^{-}_{\gamma} \leq k^{-} - \frac{k^{-}}{2\gamma^{-}}\right] \geq \frac{k^{-}}{4{\gamma^{-}}^{2}}.$$

From (6) it is obvious that $\zeta^{+} < \frac{1}{4\gamma^{+}}$, and therefore, by the definition of $Y^{+}_{\gamma^{+}}$,

$$\mathbf{Pr}\left[Y^{+} \geq 2\left|A\right| + \frac{1}{4\gamma^{+}}\right] \geq \mathbf{Pr}\left[Y^{+}_{\gamma^{+}} \geq k^{+} + \frac{1}{4\gamma^{+}}\right] \geq \frac{k^{+}}{4{\gamma^{+}}^{2}}.$$

By the definition of $Y^{-}_{\gamma^{-}}$ and the obvious fact that $\mathbf{Pr}\left[Y^{-} \leq \gamma^{-}\right] > 1/2$,

$$\mathbf{Pr}\left[Y^{-} \leq 2D - 2\left|A\right| - \frac{1}{2\gamma^{-}}\right] \geq \mathbf{Pr}\left[Y^{-} \leq \gamma^{-}\right] \cdot \mathbf{Pr}\left[Y^{-}_{\gamma^{-}} \leq k^{-} - \frac{k^{-}}{2\gamma^{-}}\right] > \frac{k^{-}}{8{\gamma^{-}}^{2}}.$$

Observe that $\frac{k^{\odot}}{{\gamma^{\odot}}^{2}} \geq \frac{1}{51D(\log D)^{2}}$ and $\frac{1}{\gamma^{\odot}} \geq \frac{1}{11D\log D}$ for large enough D. Together with (5) this implies

$$\mathop{\mathbf{Pr}}_{v\sim\mathcal{U}_1^D}\left[\sum_{i\in A}\left|v^{i}\right|^{2} \geq \frac{|A|}{D} + \frac{1}{88D^{2}\log D}\right] \geq \frac{1}{83232\cdot D^{2}(\log D)^{4}},$$

as required. ■

Denote by $\mathcal{U}_{\text{bas}}$ the uniform distribution of orthonormal bases of $\mathbb{C}^{D}$ (i.e., the Haar measure). For $\rho \in \mathbf{Den}[D]$, we will write $P_{V\sim\mathcal{U}_{\text{bas}}}(\rho)$ to denote the distribution of the outcome of $P_{V}(\rho)$ when $V \sim \mathcal{U}_{\text{bas}}$. We will implicitly identify an outcome of $P_{V\sim\mathcal{U}_{\text{bas}}}(\rho)$ with the corresponding unit vector in $\mathbb{C}^{D}$.

We need yet another "anti-concentration" statement, this time to say that the outcomes of $P_{V\sim\mathcal{U}_{\text{bas}}}(\rho)$ cannot be too concentrated for any fixed ρ:

Lemma 4.3. *Let B be a subset of unit vectors in $\mathbb{C}^{D}$, such that $\mathcal{U}_1^D(B) \geq \varepsilon$. Then for any $\rho \in$ $\mathbf{Den}[D]$,*

$$\mathop{\mathbf{Pr}}_{v\sim P_{V\sim\mathcal{U}_{bas}}(\rho)}\left[v \in B\right] > \frac{\varepsilon^{4}}{256}.$$

Intuitively, by choosing ρ adversarially one can selectively "hide" some unit vectors in $\mathbb{C}^{D}$ from $P_{V\sim\mathcal{U}_{\text{bas}}}(\rho)$. However, only those v's are hidden well that are almost orthogonal to all spectral components of ρ, and that cannot happen to too many v's simultaneously; in particular, if B is sufficiently large then it is impossible to efficiently avoid all its elements.

Proof. Observe that the distribution $\mathcal{U}_1^D$ is the same as $P_{V\sim\mathcal{U}_{\text{bas}}}(I_D/D)$, and its density function is constant on the support (unit vectors in $\mathbb{C}^{D}$) – denote it by ϕ_0. Then by linearity, for any ρ the density function of $P_{V\sim\mathcal{U}_{\text{bas}}}(\rho)$ is

$$\phi_\rho(v) \overset{\text{def}}{=} \phi_0 \cdot D \cdot \langle v|\rho|v\rangle\ .$$

For $\delta \overset{\text{def}}{=} \varepsilon^{3}/64$, let us bound from above the value of

$$\mathop{\mathbf{Pr}}_{v\sim\mathcal{U}_1^D}\left[\phi_\rho(v) < \delta\cdot\phi_0\right] = \mathop{\mathbf{Pr}}_{\mathcal{U}_1^D}\left[\langle v|\rho|v\rangle < \delta/D\right]. \tag{9}$$

The expectation of $\langle v|\rho|v\rangle$ is $1/D$, and therefore the value is maximized when ρ has rank one (if ρ is a mixture that makes the value of $\langle v|\rho|v\rangle$ more concentrated). On the other hand, for every fixed u_0 and $v \sim \mathcal{U}_1^D$, the distribution of $|\langle u_0|v\rangle|$ only depends on $|u_0|$ (and not on the "direction" of u_0).

Therefore, in order to bound (9), we can assume w.l.g. that $\rho = |u_0\rangle\langle u_0|$, where $u_0 = (1, 0, \ldots, 0)$. That is,

$$\mathop{\mathbf{Pr}}_{v\sim\mathcal{U}_1^D}\left[\phi_\rho(v) < \delta\cdot\phi_0\right] \le \mathop{\mathbf{Pr}}_{\mathcal{U}_1^D}\left[\left|v^1\right| < \sqrt{\delta/D}\right],$$

where v^1 is the first coordinate of v.

By Claim 4.1 we have:

$$\mathop{\mathbf{Pr}}_{v\sim\mathcal{U}_1^D}\left[\left|v^1\right| < \sqrt{\delta/D}\right] = \mathbf{Pr}\left[\left|u^1\right|/\|u\| < \sqrt{\delta/D}\right] \le \mathbf{Pr}\left[\left|u^1\right| < 2\sqrt{\delta/\varepsilon}\right] + \mathbf{Pr}\left[\|u\|^2 > \frac{4D}{\varepsilon}\right].$$

We know that $\|u\|^2 \sim \chi^2_{2D}$, and therefore its expectation is $2D$ and $\mathbf{Pr}\left[\|u\|^2 > 4D/\varepsilon\right] < \varepsilon/2$ by Markov inequality. We also know that $\Re(u^1) \sim N(0,1)$, and therefore $\mathbf{Pr}\left[\left|u^1\right| < 2\sqrt{\delta/\varepsilon}\right] < 2\sqrt{\delta/\varepsilon} = \varepsilon/4$. We conclude that $\mathbf{Pr}_{v\sim\mathcal{U}_1^D}\left[\phi_\rho(v) < \delta\cdot\phi_0\right] < 3\varepsilon/4$.

Let $B' \overset{\text{def}}{=} \{v \in B \,|\, \phi_\rho(v) \ge \delta\cdot\phi_0\}$, then it necessarily holds that $\mathcal{U}_1^D(B') > \varepsilon/4$. By the definition of B',

$$\mathop{\mathbf{Pr}}_{v\sim P_{V\sim\mathcal{U}_{\text{bas}}}(\rho)}\left[v \in B'\right] \ge \delta\cdot\mathcal{U}_1^D(B') > \frac{\delta\varepsilon}{4} = \frac{\varepsilon^4}{256},$$

and the result follows. ■

The next lemma will be the core of our optimality argument.

Lemma 4.4. *Let* $\sigma_1, \sigma_2, \rho \in \mathbf{Den}[D]$, *satisfying* $\|\sigma_1 - \sigma_2\|_1 = \delta > 0$. *Then for some* $\xi \in \Omega\Big(\frac{\delta}{D^3\log D}\Big)$,

$$\mathop{\mathbf{Pr}}_{v\sim P_{V\sim\mathcal{U}_{bas}}(\rho)}\left[\langle v|\sigma_1|v\rangle \ge (1+\xi)\,\langle v|\sigma_2|v\rangle\right] \in \Omega\big((D\log D)^{-20}\big).$$

Proof. To prove the statement, we will first consider the simpler case when $v \sim \mathcal{U}_1^D$, then see what happens when $v \sim P_{V\sim\mathcal{U}_{\text{bas}}}(\rho)$.

Let $\sigma' \overset{\text{def}}{=} \sigma_1 - \sigma_2$, then

$$\mathop{\mathbf{Pr}}_{v\sim\mathcal{U}_1^D}\left[\langle v|\sigma_1|v\rangle \ge (1+\xi)\,\langle v|\sigma_2|v\rangle\right] = \mathbf{Pr}\left[\langle v|\sigma'|v\rangle \ge \xi\,\langle v|\sigma_2|v\rangle\right] \ge \mathbf{Pr}\left[\langle v|\sigma'|v\rangle \ge \xi\right].$$

Let $\sigma' = \sum_{i=1}^D e_i\,|u_i\rangle\langle u_i|$ be a spectral decomposition, $A^+ \overset{\text{def}}{=} \{i\,|\,e_i > 0\}$ and $A^- \overset{\text{def}}{=} \{i\,|\,e_i < 0\}$, then for every ξ

$$\begin{aligned}\mathop{\mathbf{Pr}}_{v\sim\mathcal{U}_1^D}\left[\langle v|\sigma'|v\rangle \ge \xi\right] &= \mathbf{Pr}\left[\sum_i e_i\,|\langle u_i|v\rangle|^2 \ge \xi\right]\\ &= \mathbf{Pr}\left[\sum_{i\in A^+} e_i\,|\langle u_i|v\rangle|^2 \ge \xi + \sum_{i\in A^-} -e_i\,|\langle u_i|v\rangle|^2\right] \qquad (10)\\ &\ge \mathbf{Pr}\left[\sum_{i\in A^+} e_i\,|\langle u_i|v\rangle|^2 \ge \xi + \mathop{\mathbf{E}}_{v\sim\mathcal{U}_1^D}\left[\sum_{i\in A^+} e_i\,|\langle u_i|v\rangle|^2\right]\right],\end{aligned}$$

where the inequality follows from $\sum e_i = 0$ and the fact that the random values $\sum_{A^+} e_i \left|\langle u_i|v\rangle\right|^2$ and $\sum_{A^-} -e_i \left|\langle u_i|v\rangle\right|^2$ are anti-correlated when $v \sim \mathcal{U}_1^D$.

Observe that $\sum |e_i| = \delta$, and so $\sum_{A^+} e_i = \delta/2$. As $\mathbf{E}_v \left[\left|\langle u|v\rangle\right|^2\right] = 1/D$ for any unit vector u and the right-hand side of (10) is symmetric w.r.t. any unitary rotation of the vectors $\{u_i\}$,

$$\mathop{\mathbf{Pr}}_{v\sim\mathcal{U}_1^D} \left[\langle v|\sigma'|v\rangle \geq \xi\right] \geq \mathbf{Pr}\left[\sum_{i\in A^+} e_i \cdot \left|v^i\right|^2 \geq \xi + \frac{\delta}{2D}\right]. \tag{11}$$

From Lemma 4.2, for some $\eta_1 \in \Omega\left(\frac{1}{D^2 \log D}\right)$ and $\eta_2 \in \Omega\left(\frac{1}{D^2 (\log D)^4}\right)$

$$\mathop{\mathbf{Pr}}_{v\sim\mathcal{U}_1^D}\left[\sum_{i\in A^+} \left|v^i\right|^2 \geq \frac{|A^+|}{D} + \eta_1\right] \geq \eta_2.$$

By the linearity of expectation,

$$\mathbf{E}\left[\sum_{i\in A^+} e_i \cdot \left|v^i\right|^2 \middle| \sum_{i\in A^+} \left|v^i\right|^2 \geq \frac{|A^+|}{D} + \eta_1\right] \geq \frac{\delta}{2D} \cdot \frac{|A^+| + \eta_1 D}{|A^+|} \geq \frac{\delta}{2D} + \frac{\delta\eta_1}{2D}.$$

Therefore, for some $\xi \in \Omega\left(\frac{\delta}{D^3 \log D}\right)$ and $\eta_3 \in \Omega\left(\frac{1}{(D\log D)^5}\right)$,

$$\begin{aligned}\mathop{\mathbf{Pr}}_{v\sim\mathcal{U}_1^D}\left[\sum_{i\in A^+} e_i \cdot \left|v^i\right|^2 \geq \frac{\delta}{2D} + \xi\right] &= \mathop{\mathbf{Pr}}_{v\sim\mathcal{U}_1^D}\left[\sum_{i\in A^+} e_i \cdot \left|v^i\right|^2 \geq \frac{\delta}{2D} + \frac{\delta\eta_1}{4D}\right] \\ &\geq \mathbf{Pr}\left[\sum_{i\in A^+} \left|v^i\right|^2 \geq \frac{|A^+|}{D} + \eta_1\right] \cdot \\ &\geq \frac{\eta_1\eta_2}{2D} = \eta_3.\end{aligned}$$

From (11), $\mathbf{Pr}_{v\sim\mathcal{U}_1^D}\left[\langle v|\sigma'|v\rangle \geq \xi\right] \geq \eta_3$.

Applying Lemma 4.3 to the set $\left\{v \in \mathbb{C}^D \;\middle|\; \langle v|\sigma'|v\rangle \geq \xi,\ \|v\| = 1\right\}$, we conclude that

$$\mathop{\mathbf{Pr}}_{v\sim P_{V\sim\mathcal{U}_{\text{bas}}}(\rho)}\left[\langle v|\sigma'|v\rangle \geq \xi\right] \geq \frac{(\eta_3)^4}{256} \in \Omega\left(\frac{1}{(D\log D)^{20}}\right),$$

and the result follows. ■

4.2 Optimality statement

The following theorem concludes our optimality argument.

Theorem 4.5. *Let $\Phi = \{\phi(x) \,|\, x \in \{0,1\}^n\} \subset \mathbf{Den}[D]$ be a quantum fingerprinting scheme that guarantees error below $1/2 - \Omega(1)$. Then Φ leaks $\Omega\left(D^{-47}\right)$ bits of information.*

The theorem implies that any quantum fingerprinting scheme that leaks ℓ bits about x requires $\Omega(\log(1/\ell))$ qubits, and therefore our mixed-state construction of Section 3.3 (cf. Theorem 3.13) is optimal. Note that while our constructions of fingerprinting schemes guarantee one-sided error, the above theorem remains valid also for schemes with two-sided error. Moreover, Theorem 4.5 theorem still holds for schemes that only work on average under the balanced uniform input distribution.

Proof. We will show that for any Φ, a measurement P_V chosen at random w.r.t. $V \sim \mathcal{U}_{\text{bas}}$ is likely to have the following property: *The outcome of* $P(\phi(X))$ *has mutual information* $\Omega\big(D^{-47}\big)$ *with the random variable* $X \sim \mathcal{U}_{\{0,1\}^n}$.

Assume $X = x_0$. Let $\rho \overset{\text{def}}{=} \mathbf{E}_{x\in\{0,1\}^n}\left[\phi(x)\right]$. Call a unit vector $v \in \mathbb{C}^D$ x_0-ε-*good* if $\langle v|\phi(x_0)|v\rangle \geq (1+\varepsilon)\langle v|\rho|v\rangle$, where $\varepsilon \geq 0$.

The error guarantee of the theorem implies that $\|\phi(x_0) - \rho\|_1 \in \Omega(1)$ (as long as $n > 0$), and therefore by Lemma 4.4,

$$\mathop{\mathbf{Pr}}_{v\sim P_{V\sim\mathcal{U}_{\text{bas}}}(\rho)}\left[v \text{ is } x_0\text{-}\xi\text{-good}\right] \in \Omega\big((D\log D)^{-20}\big) \tag{12}$$

for some $\xi \in \Omega\big(1/D^3\log D\big)$.

For any unit vector $v \in \mathbb{C}^D$, let A_v be the set of all x's, such that v is x-ξ-good. Let

$$p_0 \overset{\text{def}}{=} \mathop{\mathbf{Pr}}_{\substack{X\sim\mathcal{U}_{\{0,1\}^n}\\ v\sim P_{V\sim\mathcal{U}_{\text{bas}}}(\rho)}}\left[X \in A_v\right] \quad \text{and} \quad p_1 \overset{\text{def}}{=} \mathop{\mathbf{Pr}}_{\substack{X\sim\mathcal{U}_{\{0,1\}^n}\\ v\sim P_{V\sim\mathcal{U}_{\text{bas}}}(\phi(X))}}\left[X \in A_v\right].$$

By the definition of x_0-ε-good we know that $p_1 \geq (1+\xi)\cdot p_0$.

Note that p_1 is the "actual" probability of certain event (namely, $X \in A_v$), and p_0 is what that probability would have been if the outcome of $P_{V\sim\mathcal{U}_{\text{bas}}}(\phi(X))$ did not depend on X. Based on the inequality between the two probabilities, we want to show that the outcome of the measurement is *well-correlated* with the value of X. For that we use a lower bound on p_0, as guaranteed by (12).

Now assume that the underlying distributions are $X \sim \mathcal{U}_{\{0,1\}^n}$ and $v \sim P_{V\sim\mathcal{U}_{\text{bas}}}(\phi(X))$.

$$\mathbf{H}\left[X\middle|v\right] \leq -p_1\cdot\log_2\left(2^{-n}\cdot\frac{p_1}{p_0}\right) - (1-p_1)\cdot\log_2\left(2^{-n}\cdot\frac{1-p_1}{1-p_0}\right),$$

as follows from the fact that the maximum entropy of a discrete distribution over a domain of given size is attained when the distribution is uniform (so, in the right-hand side we consider the situation when X is uniform both modulo "$X \in A_v$" and modulo "$X \notin A_v$"). Then

$$\mathbf{H}\left[X\middle|v\right] \leq n - p_1\log_2\left(\frac{p_1}{p_0}\right) - (1-p_1)\log_2\left(\frac{1-p_1}{1-p_0}\right) = n - d_{KL}\left(D_0||D_1\right),$$

where D_i is the distribution over $\{0,1\}$ that assigns weight p_i to the outcome "0". By the Pinsker's inequality,

$$d_{KL}\left(D_0||D_1\right) \geq \frac{\|D_0 - D_1\|_1^2}{2} = 2(p_1-p_0)^2 \geq 2(\xi p_0)^2 \in \Omega\big(D^{-47}\big),$$

and therefore

$$\mathbf{H}\left[X\right] - \mathbf{H}\left[X\middle|v\right] \in \Omega\big(D^{-47}\big).$$

Since v is the outcome of a measurement performed on a fingerprint of X, the result follows. ■

Acknowledgments

The authors express their appreciation to Debbie Leung, Jérémie Roland, Martin Rötteler and Pranab Sen for valuable discussions. The comments by one of the anonymous reviewers were especially helpful.

References

[BB84] C. H. Bennett and G. Brassard. Quantum Cryptography: Public Key Distribution and Coin Tossing. *Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing*, pages 175–179, 1984.

[BCWdW01] H. Buhrman, R. Cleve, J. Watrous, and R. de Wolf. Quantum Fingerprinting. *Physical Review Letters 87(16)*, 167902, 2001.

[BHL$^+$05] C. H. Bennett, P. Hayden, D. Leung, P. W. Shor, and A. Winter. Remote Preparation of Quantum States. *IEEE Transactions on Information Theory 51(1)*, pages 56–74, 2005.

[FHS11] O. Fawzi, P. Hayden, and P. Sen. From Low-Distortion Norm Embeddings to Explicit Uncertainty Relations and Efficient Information Locking. *Proceedings of the 43st Symposium on Theory of Computing*, 2011.

[HLSW04] P. Hayden, D. Leung, P. W. Shor, and A. Winter. Randomizing Quantum States: Constructions and Applications. *Communications in Mathematical Physics 250(2)*, pages 371–391, 2004.

[JKB94] N. L. Johnson, S. Kotz, and N. Balakrishnan. Continuous Univariate Distributions, Volume 1. *Wiley-Interscience*, 1994.

[JRW94] R. Jozsa, D. Robb, and W. K. Wootters. Lower Bound for Accessible Information in Quantum Mechanics. *Physical Review A 49(2)*, pages 668–677, 1994.

[Leu09] D. Leung. A Survey on Locking of Bipartite Correlations. *Journal of Physics: Conference Series 143*, 012008, 2009.

[May97] D. Mayers. Unconditionally Secure Quantum Bit Commitment is Impossible. *Physical Review Letters 78(17)*, pages 3414–3417, 1997.

[McD98] C. McDiarmid. Concentration. *Probabilistic Methods for Algorithmic Discrete Mathematics*, pages 195–248, 1998.

[NS96] I. Newman and M. Szegedy. Public vs. Private Coin Flips in One Round Communication Games. *Proceedings of the 28th Symposium on Theory of Computing*, pages 561–570, 1996.

[Sýk74] S. Sýkora. Quantum Theory and the Bayesian Inference Problems. *Journal of Statistical Physics 11(1)*, pages 17–27, 1974.

[WZ82] W. K. Wootters and W. H. Zurek. A Single Quantum Cannot be Cloned. *Nature 299*, pages 802–803, 1982.

A Proof of Lemma 2.6

Let us repeat the lemma:

Lemma 2.6: For every $0 < \varepsilon \le 2$, there exists an ε-net for the set of pure states in $\mathbb{C}^D$ with respect to the trace distance whose size is at most $(4/\varepsilon)^{2(D-1)}$.

To prove the lemma we use the following lemma that has been stated in [JRW94], where it was attributed to [Sýk74].

Lemma A.1. ([JRW94]) *Let $\{|e_1\rangle, \dots, |e_D\rangle\}$ be an orthonormal basis of $\mathbb{C}^D$. Let $|u\rangle \in \mathbb{C}^D$ be a random unit vector chosen according to the unitarily invariant probability distribution on the unit sphere in $\mathbb{C}^D$. Let $X_i = |\langle e_i|u\rangle|^2$ for $i = 1, \dots, D$. Then, the range of the D-tuple $\bar{X} = (X_1, \dots, X_D)$ is equal to the probability simplex*

$$\Delta_{D-1} = \left\{ (x_1, \dots, x_D) \colon \sum_{i=1}^{D} x_i = 1,\ x_i \ge 0\ (\forall i) \right\},$$

and the probability distribution of $\bar{X}$ is uniform on Δ_{D-1}.

Corollary A.2. *Let $|w\rangle \in \mathbb{C}^D$ be a fixed unit vector. Choose a unit vector $|u\rangle \in \mathbb{C}^D$ randomly as in Lemma A.1. Then $\mathbf{Pr}\left[|\langle u|w\rangle|^2 \ge x\right] = (1-x)^{D-1}$ for $0 \le x \le 1$.*

Proof of Lemma 2.6. The lemma can be proved by the packing argument in the same way as Lemma II.4 of [HLSW04] and Lemma 4 of [BHL$^+$05]. The difference is that we apply the packing argument directly on the set of pure states by using Corollary A.2, instead of applying the packing argument on the Euclidean space $\mathbb{R}^{2D}$ as an intermediate step.

Let M be a maximal subset of $\{|v\rangle \in \mathbb{C}^D \colon \|v\| = 1\}$ such that every pair of distinct vectors $|u\rangle, |v\rangle \in M$ satisfy $\||u\rangle\langle u| - |v\rangle\langle v|\|_1 \ge \varepsilon$. By the maximality of M, M is an ε-net for the set of pure states in $\mathbb{C}^D$ with respect to the trace distance. For each $|u\rangle \in M$, consider the open ball $B_{\varepsilon/2}(|u\rangle) = \{|w\rangle \in \mathbb{C}^D \colon \|w\| = 1 \wedge \||u\rangle\langle u| - |w\rangle\langle w|\|_1 < \varepsilon/2\}$. First fix $|u\rangle \in M$. Then, if we pick a unit vector $|x\rangle$ uniformly at random, we have

$$\begin{aligned}\mathbf{Pr}\left[|x\rangle \in B_{\varepsilon/2}(|u\rangle)\right] &= \mathbf{Pr}\left[\||u\rangle\langle u| - |x\rangle\langle x|\| < \frac{\varepsilon}{2}\right] \\ &= \mathbf{Pr}\left[|\langle u|x\rangle|^2 > 1 - \left(\frac{\varepsilon}{4}\right)^2\right] = \left(\frac{\varepsilon}{4}\right)^{2(D-1)},\end{aligned}$$

by Corollary A.2. By the condition of M, the $|M|$ open balls $B_{\varepsilon/2}(|u\rangle)$ ($|u\rangle \in M$) are disjoint. Therefore,

$$1 \ge \Pr\left[x \in \bigcup_{|u\rangle \in M} B_{\varepsilon/2}(|u\rangle)\right] = \sum_{|u\rangle \in M} \Pr[|x\rangle \in B_{\varepsilon/2}(|u\rangle)] = |M| \left(\frac{\varepsilon}{4}\right)^{2(D-1)},$$

which implies $|M| \le (4/\varepsilon)^{2(D-1)}$. ■*Lemma 2.6*