Pseudorandom Quantum States

Zhengfeng Ji[1], Yi-Kai Liu[2], and Fang Song[3]

[1] Centre for Quantum Software and Information, School of Software,
Faculty of Engineering and Information Technology,
University of Technology Sydney, NSW, Australia
Zhengfeng.Ji@uts.edu.au
[2] Joint Center for Quantum Information and Computer Science (QuICS),
National Institute of Standards and Technology (NIST), Gaithersburg, MD, USA,
and University of Maryland, College Park, MD, USA
yi-kai.liu@nist.gov
[3] Computer Science Department, Portland State University, Portland, OR, USA
fang.song@pdx.edu

Abstract. We propose the concept of pseudorandom quantum states, which appear random to any quantum polynomial-time adversary. It offers a *computational* approximation to perfectly random quantum states analogous in spirit to cryptographic pseudorandom generators, as opposed to *statistical* notions of quantum pseudorandomness that have been studied previously, such as quantum t-designs analogous to t-wise independent distributions.

Under the assumption that quantum-secure one-way functions exist, we present efficient constructions of pseudorandom states, showing that our definition is achievable. We then prove several basic properties of pseudorandom states, which show the utility of our definition. First, we show a cryptographic no-cloning theorem: no efficient quantum algorithm can create additional copies of a pseudorandom state, when given polynomially-many copies as input. Second, as expected for random quantum states, we show that pseudorandom quantum states are highly entangled on average. Finally, as a main application, we prove that any family of pseudorandom states naturally gives rise to a private-key quantum money scheme.

1 Introduction

Pseudorandomness is a foundational concept in modern cryptography and theoretical computer science. A distribution $\mathcal{D}$, e.g., over a set of strings or functions, is called *pseudorandom* if no computationally-efficient observer can distinguish between an object sampled from $\mathcal{D}$, and a truly random object sampled from the uniform distribution [57,64,10]. Pseudorandom objects, such as pseudorandom generators (PRGs), pseudorandom functions (PRFs) and pseudorandom permutations (PRPs) are fundamental cryptographic building blocks, such as in the design of stream ciphers, block ciphers and message authentication codes [25,38,24,54,28]. Pseudorandomness is also essential in algorithm design and complexity theory such as derandomization [48,33].

The law of quantum physics asserts that truly random bits can be generated easily even with untrusted quantum devices [15,42]. Is pseudorandomness, a seemingly weaker notion of randomness, still relevant in the context of quantum information processing? The answer is yes. By a simple counting argument, one needs exponentially many bits even to specify a truly random function on n-bit strings. Hence, in the *computational* realm, pseudorandom objects that offer efficiency as well as other unique characteristics and strengths are indispensable.

A fruitful line of work on pseudorandomness in the context of quantum information science has been about quantum t-designs and unitary t-designs [4,17,27,12,16,34,60,70,46,45,44,11,41]. However, while these objects are often called "pseudorandom" in the mathematical physics literature, they are actually analogous to t-wise independent random variables in theoretical computer science. Our focus in this work is a notion of *computational* pseudorandomness, and in particular suits (complexity-theoretical) cryptography.

The major difference between t-wise independence and cryptographic pseudorandomness is the following. In the case of t-wise independence, the observer who receives the random-looking object may be computationally unbounded, but only *a priori* (when the random-looking object is constructed) fixed number t samples are given. Thus, quantum t-designs satisfy an "information-theoretic" or "statistical" notion of security. In contrast, in the case of cryptographic pseudorandomness, the observer who receives the random-looking object is assumed to be computationally efficient, in that it runs in probabilistic polynomial time for an arbitrary polynomial that is chosen by the observer, *after* the random-looking object has been constructed. This leads to a "computational" notion of security, which typically relies on some complexity-theoretic assumption, such as the existence of one-way functions).

In general, these two notions, t-wise independence and cryptographic pseudorandomness, are incomparable. In some ways, the setting of cryptographic pseudorandomness imposes stronger restrictions on the observer, since it assumes a bound on the observer's total computational effort (say, running in probabilistic polynomial time). In other ways, the setting of t-wise independence imposes stronger restrictions on the observer, since it forces the observer to make a limited number of non-adaptive "queries," specified by the parameter t, which is usually a constant or a fixed polynomial. In addition, different distance measures are often used, e.g., trace distance or diamond norm, versus computational distinguishability.

Cryptographic pseudorandomness in quantum information, which has received relatively less study, mostly connects with quantum money and post-quantum cryptography. Pseudorandomness is used more-or-less implicitly in quantum money, to construct quantum states that look complicated to a dishonest party, but have some hidden structure that allows them to be verified by the bank [1,40,2,3,69]. In post-quantum cryptography, one natural question is whether the classical constructions such as PRFs and PRPs remain secure against quantum attacks. This is a challenging task as, for example, a quantum adversary may query the underlying function or permutation in *superposition*. Fortunately, people have

so far restored several positive results. Assuming a one-way function that is hard to invert for polynomial-time quantum algorithms, we can attain quantum-secure PRGs as well as PRFs [28,66]. Furthermore, one can construct quantum-secure PRPs from quantum-secure PRFs using various *shuffling* constructions [68,58].

In this work, we study pseudorandom *quantum* objects such as quantum states and unitary operators. Quantum states (in analogy to strings) and unitary operations (in analogy to functions) form continuous spaces, and the Haar measure is considered the perfect randomness on the spaces of quantum states and unitary operators. A basic question is:

How to define and construct computational pseudorandom *approximations of Haar randomness, and what are their applications?*

Our contributions. We propose definitions of pseudorandom quantum states (PRS's) and pseudorandom unitary operators (PRUs), present efficient constructions of PRS's, demonstrate basic properties such as no-cloning and high entanglement of pseudorandom states, and showcase the construction of private-key quantum money schemes as one of the applications.

1. We propose a suitable definition of *quantum pseudorandom states*.
   We employ the notion of quantum *computational indistinguishability* to define quantum pseudorandom states. Loosely speaking, we consider a collection of quantum states $\{|\phi_k\rangle\}$ indexed by $k \in \mathcal{K}$, and require that no efficient quantum algorithm can distinguish between $|\phi_k\rangle$ for a random k and a state drawn according to the Haar measure. However, as a unique consideration in the quantum setting, we need to be cautious about *how many copies* of the input state are available to an adversary.
   Classically, this is a vacuous concern for defining a pseudorandom distribution on strings, since one can freely produce many copies of the input string. The quantum no-cloning theorem, however, forbids copying an unknown quantum state in general. Pseudorandom states in terms of *single-copy* indistinguishability have been discussed in the literature (see for example [13] and a recent study [14]). Though this single-copy definition may be suitable for certain cryptographic applications, it also loses many properties of Haar random states as a purely classical distributions already satisfies the definition [4].
   Therefore we require that no adversary can tell a difference even given any *polynomially many* copies of the state. This subsumes the single-copy version and is strictly stronger. We gain from it many interesting properties, such as the no-cloning property and entanglement property for pseudorandom states as discussed later in the paper.
2. We present concrete efficient constructions of PRS's with the minimal assumption that quantum-secure one-way functions exist.

[4] For example, a uniform distribution over the computational basis state $\{|k\rangle\}$ has an identical density matrix as a Haar random state and satisfy the single-shot definition of PRS. But distinguishing them becomes easy as soon as we have more than one copies. These states also do not appear to be hard to clone or possess entanglement.

Our construction uses any quantum-secure $\mathsf{PRF} = \{\mathsf{PRF}_k\}_{k\in\mathcal{K}}$ and computes it into the phases of a uniform superposition state (see equation (8)). We call such family of PRS the *random phase states*. This family of states can be efficiently generated using the quantum Fourier transform and a phase kick-back trick. We prove that this family of state is pseudorandom by a hybrid argument. By the quantum security of PRF, the family is computationally indistinguishable from a similar state family defined by truly random functions. We then prove that, this state family corresponding to truly random functions is statistically indistinguishable from Haar random states. Finally, by the fact that PRF exists assuming quantum-secure one-way functions, we can base our PRS construction on quantum-secure one-way functions.
We note that Aaronson [1, Theorem 3] has described a similar family of states, which uses some polynomial function instead of a PRF in the phases. In that construction, however, the size of the state family depends on (i.e., has to grow with) the adversary's number of queries that the family wants to tolerate. It therefore fails to satisfy our definition, in which any polynomial number queries independent of the family are permitted.

3. We prove *cryptographic no-cloning theorems* for PRS's, and they give a simple and generic construction of private-key quantum money schemes based on any PRS.
   We prove that a PRS remains pseudorandom, even if we additionally give the distinguisher an oracle that reflects about the given state (i.e., $O_\phi := \mathbb{1} - 2|\phi\rangle\langle\phi|$). This establishes the equivalence between the standard and a strong definition of PRS's. Technically, this is proved using the fact that with polynomially many copies of the state, one can approximately simulate the reflection oracle O_ϕ.
   We obtain general *cryptographic no-cloning theorems* of PRS's both with and without the reflection oracle. The theorems roughly state that given any polynomially many copies of pseudorandom states, no polynomial-time quantum algorithm can produce even one more copy of the state. We call them cryptographic no-cloning theorems due to the computational nature of our PRS. The proofs of these theorems use SWAP tests in the reduction from a hypothetical cloning algorithm to an efficient distinguishing algorithm violating the definition of PRS's.
   Using the strong pseudorandomness and the cryptographic no-cloning theorem with reflection oracle, we show that any PRS immediately gives a *private-key quantum money scheme*. While much attention has been focused on public-key quantum money [1,40,2,3,69], we emphasize that private-key quantum money is already non-trivial. Early schemes for private-key quantum money due to Wiesner and others were not *query secure*, and could be broken by online attacks [62,9,39,20]. Aaronson and Christiano finally showed a query-secure scheme in 2012, which achieves information-theoretic security in the random oracle model, and computational security in the standard model [2]. They used a specific construction based on hidden subspace states, whereas our construction (which is also query-secure) is more generic and can be based on any PRS. The freedom to choose and tweak the underlying

pseudorandom functions or permutations in the PRS may motivate and facilitate the construction of public-key quantum money schemes in future work.

4. We show that pseudorandom states are highly entangled.
   It is known that a Haar random state is entangled with high probability. We establish a similar result for any family of pseudorandom states. Namely, the states in any PRS family are entangled on average. It is shown that the expected Schmidt rank for any PRS is superpolynomial in κ and that the expected min entropy and von Neumann entropy are of the order $\omega(\log \kappa)$ where κ is the security parameter. This is yet another evidence of the suitability of our definition.
   The proof again rests critically on that our definition grants multiple copies to the distinguisher—if the expected entanglement is low, then SWAP test with respect to the corresponding subsystems of two copies of the state will serve as a distinguisher that violates the definition.
5. We propose a definition of *quantum pseudorandom unitary operators* (PRUs). We also present candidate constructions of PRUs (without a proof of security), by extending our techniques for constructing PRS's.
   Loosely speaking, these candidate PRUs resemble unitary t-designs that are constructed by interleaving random permutations with the quantum Fourier transform [27], or by interleaving random diagonal unitaries with the Hadamard transform [45,44], and iterating this construction several times. We conjecture that a PRU can be obtained in this way, using only a constant number of iterations. This is in contrast to unitary t-designs, where a parameter counting argument suggests that the number of iterations must grow with t. This conjecture is motivated by examples such as the Luby-Rackoff construction of a pseudorandom permutation using multi-round Feistel network built using a PRF.

Table 1. Summary of various notions that approximate true randomness

	Classical	**Quantum**
True randomness	Uniform distribution	Haar measure
t-wise independence	t-wise independent random variables	Quantum t-designs
Pseudorandomness	PRGs PRFs, PRPs	(*this work*) PRS's PRUs

Discussion. We summarize the mentioned variants of randomness in Table 1. The focus of this work is mostly about PRS's and we briefly touch upon PRUs. We view our work as an initial step and anticipate further fundamental investigation inspired by our notion of pseudorandom states and unitary operators.

We mention some immediate open problems. First, can we prove the security of our candidate PRU constructions? The techniques developed in quantum unitary designs [27,12] seem helpful. Second, are quantum-secure one-way functions necessary for the construction of PRS's? Third, can we establish security proofs for more candidate constructions of PRS's? Different constructions may have their own special properties that may be useful in different settings. It is also interesting to explore whether our quantum money construction may be adapted to a public-key money scheme under reasonable cryptographic assumptions. Finally, the entanglement property we prove here refers to the standard definitions of entanglement. If we approach the concept of pseudo-entanglement as a quantum analogue of pseudo-entropy for a distribution [7], can we improve the quantitative bounds?

We point out a possible application in physics. PRS's may be used in place of high-order quantum t-designs, giving a performance improvement in certain applications. For example, pseudorandom states can be used to construct toy models of quantum *thermalization*, where one is interested in quantum states that can be prepared efficiently via some dynamical process, yet have "generic" or "typical" properties as exemplified by Haar-random pure states, for instance [52]. Using t-designs with polynomially large t, one can construct states that are "generic" in a information-theoretic sense [36]. Using PRS, one can construct states that satisfy a weaker property: they are computationally indistinguishable from "generic" states, for a polynomial-time observer.

In these applications, PRS states may be more physically plausible than high-order quantum t-designs, because PRS states can be prepared in a shorter time, e.g., using a polylogarithmic-depth quantum circuit, based on known constructions for low-depth PRFs [6,47].

2 Preliminaries

2.1 Notions

For a finite set $\mathcal{X}$, $|\mathcal{X}|$ denotes the number of elements in $\mathcal{X}$. We use the notion $\mathcal{Y}^{\mathcal{X}}$ to denote the set of all functions $f : \mathcal{X} \to \mathcal{Y}$. For finite set $\mathcal{X}$, we use $x \leftarrow \mathcal{X}$ to mean that x is drawn uniformly at random from $\mathcal{X}$. The permutation group over elements in $\mathcal{X}$ is denoted as $S_{\mathcal{X}}$. We use $\mathrm{poly}(\kappa)$ to denote the collection of polynomially bounded functions of the security parameter κ, and use $\mathrm{negl}(\kappa)$ to denote negligible functions in κ. A function $\epsilon(\kappa)$ is *negligible* if for all constant $c > 0$, $\epsilon(\kappa) < \kappa^{-c}$ for large enough κ.

In this paper, we use a *quantum register* to name a collection of qubits that we view as a single unit. Register names are represented by capital letters in a *sans serif* font. We use $\mathrm{S}(\mathcal{H})$, $\mathrm{D}(\mathcal{H})$, $\mathrm{U}(\mathcal{H})$ and $\mathrm{L}(\mathcal{H})$ to denote the set of pure quantum states, density operators, unitary operators and bounded linear operators on space $\mathcal{H}$ respectively. An ensemble of states $\{(p_i, \rho_i)\}$ represents a system prepared in ρ_i with probability p_i. If the distribution is uniform, we write the ensemble as $\{\rho_i\}$. The adjoint of matrix M is denoted as M^*. For matrix

M, $|M|$ is defined to be $\sqrt{M^*M}$. The operator norm $\|M\|$ of matrix M is the largest eigenvalue of $|M|$. The trace norm $\|M\|_1$ of M is the trace of $|M|$. For two operators $M, N \in \mathrm{L}(\mathcal{H})$, the Hilbert-Schmidt inner product is defined as

$$\langle M, N\rangle = \mathrm{tr}(M^*N).$$

A quantum channel is a physically admissible transformation of quantum states. Mathematically, a quantum channel

$$\mathcal{E} : \mathrm{L}(\mathcal{H}) \to \mathrm{L}(\mathcal{K})$$

is a completely positive, trace-preserving linear map.

The trace distance of two quantum states $\rho_0, \rho_1 \in \mathrm{D}(\mathcal{H})$ is

$$\mathrm{TD}(\rho_0, \rho_1) \stackrel{\mathrm{def}}{=} \frac{1}{2} \|\rho_0 - \rho_1\|_1 . \tag{1}$$

It is known (Holevo-Helstrom theorem [30,31]) that for a state drawn uniformly at random from the set $\{\rho_0, \rho_1\}$, the optimal distinguish probability is given by

$$\frac{1 + \mathrm{TD}(\rho_0, \rho_1)}{2}.$$

Define number $N = 2^n$ and set $\mathcal{X} = \{0, 1, \ldots, N-1\}$. The quantum Fourier transform on n qubits is defined as

$$F = \frac{1}{\sqrt{N}} \sum_{x,y \in \mathcal{X}} \omega_N^{xy} |x\rangle\langle y|. \tag{2}$$

It is a well-known fact in quantum computing that F can be implemented in time $\mathrm{poly}(n)$.

For Hilbert space $\mathcal{H}$ and integer m, we use $\vee^m \mathcal{H}$ to denote the symmetric subspace of $\mathcal{H}^{\otimes m}$, the subspace of states that are invariant under permutations of the subsystems. Let N be the dimension of $\mathcal{H}$ and let $\mathcal{X}$ be the set $\{0, 1, \ldots, N-1\}$ such that $\mathcal{H}$ is the span of $\{|x\rangle\}_{x \in \mathcal{X}}$. For any $\mathbf{x} = (x_1, x_2, \ldots, x_m) \in \mathcal{X}^m$, let m_j be the number of j in $\mathbf{x}$ for $j \in \mathcal{X}$. Define state

$$\big|\mathbf{x}; \mathrm{Sym}\big\rangle = \sqrt{\frac{\prod_{j \in \mathcal{X}} m_j!}{m!}} \sum_{\sigma} \Big| x_{\sigma(1)}, x_{\sigma(2)}, \ldots, x_{\sigma(m)} \Big\rangle. \tag{3}$$

The summation runs over all possible permutations σ that give different tuples $(x_{\sigma(1)}, x_{\sigma(2)}, \ldots, x_{\sigma(m)})$. Equivalently, we have

$$\big|\mathbf{x}; \mathrm{Sym}\big\rangle = \frac{1}{\sqrt{m! \prod_{j \in \mathcal{X}} m_j!}} \sum_{\sigma \in S_m} \Big| x_{\sigma(1)}, x_{\sigma(2)}, \ldots, x_{\sigma(m)} \Big\rangle. \tag{4}$$

The coefficients in the front of the above two equations are normalization constants. The set of states

$$\big\{ \big|\mathbf{x}; \mathrm{Sym}\big\rangle \big\}_{\mathbf{x} \in \mathcal{X}^m} \tag{5}$$

forms an orthonormal basis of the symmetric subspace $\vee^m \mathcal{H}$ [59, Prop.7.2]. This implies that the dimension of the symmetric subspace is

$$\binom{N+m-1}{m}.$$

Let Π_m^{Sym} be the projection onto the symmetric subspace $\vee^m \mathcal{H}$. For a permutation $\sigma \in S_m$, define operator

$$W_\sigma = \sum_{x_1,x_2,\ldots,x_m \in \mathcal{X}} \left|x_{\sigma^{-1}(1)}, x_{\sigma^{-1}(2)}, \ldots, x_{\sigma^{-1}(m)}\right\rangle\!\left\langle x_1, x_2, \ldots, x_m\right|.$$

The following identity will be useful [59, Prop.7.1]

$$\Pi_m^{\mathrm{Sym}} = \frac{1}{m!} \sum_{\sigma \in S_m} W_\sigma. \tag{6}$$

Let μ be the Haar measure on $\mathrm{S}(\mathcal{H})$, it is known that [26, Prop.6]

$$\int \left(|\psi\rangle\langle\psi|\right)^{\otimes m} \mathrm{d}\mu(\psi) = \binom{N+m-1}{m}^{-1} \Pi_m^{\mathrm{Sym}}. \tag{7}$$

2.2 Cryptography

In this section, we recall several definitions and results from cryptography that is necessary for this work.

Pseudorandom functions (PRF) and pseudorandom permutations (PRP) are important constructions in classical cryptography. Intuitively, they are families of functions or permutations that looks like truly random functions or permutations to polynomial-time machines. In the quantum case, we need a strong requirement that they still look random even to polynomial-time quantum algorithms.

Definition 1 (Quantum-Secure Pseudorandom Functions and Permutations). *Let $\mathcal{K}$, $\mathcal{X}$, $\mathcal{Y}$ be the key space, the domain and range, all implicitly depending on the security parameter κ. A keyed family of functions $\left\{\mathsf{PRF}_k : \mathcal{X} \to \mathcal{Y}\right\}_{k\in\mathcal{K}}$ is a quantum-secure pseudorandom function (QPRF) if for any polynomial-time quantum oracle algorithm $\mathcal{A}$, PRF_k with a random $k \leftarrow \mathcal{K}$ is indistinguishable from a truly random function $f \leftarrow \mathcal{Y}^{\mathcal{X}}$ in the sense that:*

$$\left|\Pr_{k\leftarrow\mathcal{K}}\left[\mathcal{A}^{\mathsf{PRF}_k}(1^\kappa) = 1\right] - \Pr_{f\leftarrow\mathcal{Y}^{\mathcal{X}}}\left[\mathcal{A}^{f}(1^\kappa) = 1\right]\right| = \mathrm{negl}(\kappa).$$

Similarly, a keyed family of permutations $\left\{\mathsf{PRP}_k \in S_{\mathcal{X}}\right\}_{k\in\mathcal{K}}$ is a quantum-secure pseudorandom permutation (QPRP) if for any quantum algorithm $\mathcal{A}$ making at most polynomially many queries, PRP_k with a random $k \leftarrow \mathcal{K}$ is indistinguishable from a truly random permutation in the sense that:

$$\left|\Pr_{k\leftarrow\mathcal{K}}\left[\mathcal{A}^{\mathsf{PRP}_k}(1^\kappa) = 1\right] - \Pr_{P\leftarrow S_{\mathcal{X}}}\left[\mathcal{A}^{P}(1^\kappa) = 1\right]\right| = \mathrm{negl}(\kappa).$$

In addition, both PRF_k and PRP_k are polynomial-time computable (on a classical computer).

Fact 1 *QPRFs and QPRPs exist if quantum-secure one-way functions exist.*

Zhandry proved the existence of QPRFs assuming the existence of one-way functions that are hard to invert even for quantum algorithms [66]. Assuming QPRF, one can construct QPRP using various *shuffling* constructions [68,58]. Since a random permutation and a random function is indistinguishable by efficient quantum algorithms [65,67], existence of QPRP is hence equivalent to existence of QPRF.

3 Pseudorandom Quantum States

In this section, we will discuss the definition and constructions of pseudorandom quantum states.

3.1 Definition of Pseudorandom States

Intuitively speaking, a family pseudorandom quantum states are a set of random states $\left\{|\phi_k\rangle\right\}_{k\in\mathcal{K}}$ that is indistinguishable from Haar random quantum states.

The first idea on defining pseudorandom states can be the following. Without loss of generality, we consider states in $\mathrm{S}(\mathcal{H})$ where $\mathcal{H} = (\mathbb{C}^2)^{\otimes n}$ is the Hilbert space for n-qubit systems. We are given either a state randomly sampled from the set $\left\{|\phi_k\rangle \in \mathcal{H}\right\}_{k\in\mathcal{K}}$ or a state sampled according to the Haar measure on $\mathrm{S}(\mathcal{H})$, and we require that no efficient quantum algorithm will be able to tell the difference between the two cases.

However, this definition does not seem to grasp the quantum nature of the problem. First, the state family where each $|\phi_k\rangle$ is a uniform random bit string will satisfy the definition—in both cases, the mixed states representing the ensemble are $\mathbb{1}/2^n$. Second, many of the applications that we can find for PRS's will not hold for this definition.

Instead, we require that the family of states looks random even if polynomially many copies of the state are given to the distinguishing algorithm. We argue that this is the more natural way to define pseudorandom states. One can see that this definition also naturally generalizes the definition of pseudorandomness in the classical case to the quantum setting. In the classical case, asking for more copies of a string is always possible and one does not bother making this explicit in the definition. This of course also rules out the example of classical random bit strings we discussed before. Moreover, this strong definition, once established, is rather flexible to use when studying the properties and applications of pseudorandom states.

Definition 2 (Pseudorandom Quantum States (PRS's)). *Let κ be the security parameter. Let $\mathcal{H}$ be a Hilbert space and $\mathcal{K}$ the key space, both parameterized by κ. A keyed family of quantum states $\left\{|\phi_k\rangle \in \mathrm{S}(\mathcal{H})\right\}_{k\in\mathcal{K}}$ is **pseudorandom**, if the following two conditions hold:*

1. (***Efficient generation***). *There is a polynomial-time quantum algorithm G that generates state $|\phi_k\rangle$ on input k. That is, for all $k \in \mathcal{K}$, $G(k) = |\phi_k\rangle$.*
2. (***Pseudorandomness***). *Any polynomially many copies of $|\phi_k\rangle$ with the same random $k \in \mathcal{K}$ is* ***computationally indistinguishable*** *from the same number of copies of a Haar random state. More precisely, for any efficient quantum algorithm $\mathcal{A}$ and any $m \in \mathrm{poly}(\kappa)$,*

$$\left| \Pr_{k \leftarrow \mathcal{K}} \left[\mathcal{A}(|\phi_k\rangle^{\otimes m}) = 1 \right] - \Pr_{|\psi\rangle \leftarrow \mu} \left[\mathcal{A}(|\psi\rangle^{\otimes m}) = 1 \right] \right| = \mathrm{negl}(\kappa),$$

where μ is the Haar measure on $\mathrm{S}(\mathcal{H})$.

3.2 Constructions and Analysis

In this section, we give an efficient construction of pseudorandom states which we call random phase states. We will prove that this family of states satisfies our definition of PRS's. There are other interesting and simpler candidate constructions, but the family of random phase states is the easiest to analyze.

Let $\mathsf{PRF} : \mathcal{K} \times \mathcal{X} \to \mathcal{X}$ be a quantum-secure pseudorandom function with key space $\mathcal{K}$, $\mathcal{X} = \{0, 1, 2, \ldots, N-1\}$ and $N = 2^n$. $\mathcal{K}$ and N are implicitly functions of the security parameter κ. The family of pseudorandom states of n qubits is defined

$$|\phi_k\rangle = \frac{1}{\sqrt{N}} \sum_{x \in \mathcal{X}} \omega_N^{\mathsf{PRF}_k(x)} |x\rangle, \tag{8}$$

for $k \in \mathcal{K}$ and $\omega_N = \exp(2\pi i/N)$.

Theorem 1. *For any QPRF $\mathsf{PRF} : \mathcal{K} \times \mathcal{X} \to \mathcal{X}$, the family of states $\{|\phi_k\rangle\}_{k \in \mathcal{K}}$ defined in Eq. (8) is a PRS.*

Proof. First, we prove that the state can be efficiently prepared with a single query to PRF_k. As PRF_k is efficient, this proves the efficient generation property.

The state generation algorithm works as follows. First, it prepares a state

$$\frac{1}{N} \sum_{x \in \mathcal{X}} |x\rangle \sum_{y \in \mathcal{X}} \omega_N^y |y\rangle.$$

This can be done by applying $H^{\otimes n}$ to the first register initialized in $|0\rangle$ and the quantum Fourier transform to the second register in state $|1\rangle$.

Then the algorithm calls PRF_k on the first register and subtract the result from the second register, giving state

$$\frac{1}{N} \sum_{x \in \mathcal{X}} |x\rangle \sum_{y \in \mathcal{X}} \omega_N^y |y - \mathsf{PRF}_k(x)\rangle.$$

The state can be rewritten as

$$\frac{1}{N} \sum_{x \in \mathcal{X}} \omega_N^{\mathsf{PRF}_k(x)} |x\rangle \sum_{y \in \mathcal{X}} \omega_N^y |y\rangle.$$

Therefore, the effect of this step is to transform the first register to the required form and leaving the second register intact.

Next, we prove the pseudorandomness property of the family. For this purpose, we consider three hybrids. In the first hybrid H_1, the state will be $|\phi_k\rangle^{\otimes m}$ for a uniform random $k \in \mathcal{K}$. In the second hybrid H_2, the state is $|f\rangle^{\otimes m}$ for truly random functions $f \in \mathcal{X}^{\mathcal{X}}$ where

$$|f\rangle = \frac{1}{\sqrt{N}} \sum_{x \in \mathcal{X}} \omega_N^{f(x)} |x\rangle.$$

In the third hybrid H_3, the state is $|\psi\rangle^{\otimes m}$ for $|\psi\rangle$ chosen according to the Haar measure.

By the definition of the quantum-secure pseudorandom functions for PRF, we have for any polynomial-time quantum algorithm $\mathcal{A}$ and any $m \in \mathrm{poly}(\kappa)$,

$$\big|\Pr\big[\mathcal{A}(H_1) = 1\big] - \Pr\big[\mathcal{A}(H_2) = 1\big]\big| = \mathrm{negl}(\kappa).$$

By Lemma 1, we have for any algorithm $\mathcal{A}$ and $m \in \mathrm{poly}(\kappa)$,

$$\big|\Pr\big[\mathcal{A}(H_2) = 1\big] - \Pr\big[\mathcal{A}(H_3) = 1\big]\big| = \mathrm{negl}(\kappa).$$

This completes the proof by triangle inequality.

Lemma 1. *For function $f : \mathcal{X} \to \mathcal{X}$, define quantum state*

$$|f\rangle = \frac{1}{\sqrt{N}} \sum_{x \in \mathcal{X}} \omega_N^{f(x)} |x\rangle.$$

For $m \in \mathrm{poly}(\kappa)$, the state ensemble $\big\{|f\rangle^{\otimes m}\big\}$ is statistically indistinguishable from $\big\{|\psi\rangle^{\otimes m}\big\}$ for Haar random $|\psi\rangle$.

Proof. Let $m \in \mathrm{poly}(\kappa)$ be the number of copies of the state. We have

$$\mathop{\mathbb{E}}_f\Big[\big(|f\rangle\langle f|\big)^{\otimes m}\Big] = \frac{1}{N^m} \sum_{\mathbf{x} \in \mathcal{X}^m, \mathbf{y} \in \mathcal{X}^m} \mathop{\mathbb{E}}_f \omega_N^{f(x_1)+\cdots+f(x_m)-[f(y_1)+\cdots+f(y_m)]} \big|\mathbf{x}\big\rangle\big\langle\mathbf{y}\big|,$$

where $\mathbf{x} = (x_1, x_2, \ldots, x_m)$ and $\mathbf{y} = (y_1, y_2, \ldots, y_m)$. For later convenience, define density matrix

$$\rho^m = \mathop{\mathbb{E}}_f\Big[\big(|f\rangle\langle f|\big)^{\otimes m}\Big].$$

We will compute the entries of ρ^m explicitly.

For $\mathbf{x} = (x_1, x_2, \ldots, x_m) \in \mathcal{X}^m$, let m_j be the number of j in $\mathbf{x}$ for $j \in \mathcal{X}$. Obviously, one has $\sum_{j \in \mathcal{X}} m_j = m$. Note that we have omitted the dependence of m_j on $\mathbf{x}$ for simplicity. Recall the basis states defined in Eq. (4)

$$\big|\mathbf{x}; \mathrm{Sym}\big\rangle = \frac{1}{\sqrt{\Big(\prod_{j \in \mathcal{X}} m_j!\Big) m!}} \sum_{\sigma \in S_m} \Big|x_{\sigma(1)}, x_{\sigma(2)}, \ldots, x_{\sigma(m)}\Big\rangle.$$

For $\mathbf{x}, \mathbf{y} \in \mathcal{X}^m$, let m_j be the number of j in $\mathbf{x}$ and m'_j be the number of j in $\mathbf{y}$.

We can compute the entries of ρ^m as

$$\begin{aligned}&\big\langle \mathbf{x}; \mathrm{Sym} \big| \rho^m \big| \mathbf{y}; \mathrm{Sym} \big\rangle \\ =&\frac{m!}{N^m \sqrt{\Big(\prod_{j\in\mathcal{X}} m_j!\Big)\Big(\prod_{j\in\mathcal{X}} m'_j!\Big)}} \mathop{\mathbb{E}}_{f} \Big[\exp\Big(\frac{2\pi i}{N} \sum_{l=1}^{m} \big(f(x_l) - f(y_l) \big) \Big) \Big].\end{aligned}$$

When $\mathbf{x}$ is not a permutation of $\mathbf{y}$, the summation $\sum_{l=1}^{m} \big(f(x_l) - f(y_l) \big)$ is a summation of terms $\pm f(z_j)$ for distinct values z_j. As f is a truly random function, $f(z_j)$ is uniformly random and independent of $f(z_{j'})$ for $z_j \neq z_{j'}$. So it is not hard to verify that the entry is nonzero only if $\mathbf{x}$ is a permutation of $\mathbf{y}$. These nonzero entries are on the diagonal of ρ^m in the basis of $\big\{ \big| \mathbf{x}; \mathrm{Sym} \big\rangle \big\}$. These diagonal entries are

$$\big\langle \mathbf{x}; \mathrm{Sym} \big| \rho^m \big| \mathbf{x}; \mathrm{Sym} \big\rangle = \frac{m!}{N^m \prod_{j\in\mathcal{X}} m_j!} \,.$$

Let ρ_μ^m be the density matrix of a random state $|\psi\rangle^{\otimes m}$, for $|\psi\rangle$ chosen from the Haar measure μ. From Eqs. (5) and (7), we have that

$$\rho_\mu^m = \binom{N+m-1}{m}^{-1} \sum_{\mathbf{x};\mathrm{Sym}} \big| \mathbf{x}; \mathrm{Sym} \big\rangle \big\langle \mathbf{x}; \mathrm{Sym} \big| .$$

We need to prove

$$\mathrm{TD}\big(\rho^m, \rho_\mu^m \big) = \mathrm{negl}(\kappa).$$

Define

$$\delta_{\mathbf{x};\mathrm{Sym}} = \frac{m!}{N^m \prod_{j\in\mathcal{X}} m_j!} - \binom{N+m-1}{m}^{-1}.$$

Then

$$\mathrm{TD}(\rho^m, \rho_\mu^m) = \frac{1}{2} \sum_{\mathbf{x};\mathrm{Sym}} \big| \delta_{\mathbf{x};\mathrm{Sym}} \big| \,.$$

The ratio of the two terms in $\delta_{\mathbf{x};\mathrm{Sym}}$ is

$$\frac{m! \binom{N+m-1}{m}}{N^m \prod_{j\in\mathcal{X}} m_j!} = \frac{\prod_{l=0}^{m-1} \Big(1 + \frac{l}{N} \Big)}{\prod_{j\in\mathcal{X}} m_j!}.$$

For sufficient large security parameter κ, the ratio is larger than 1 only if $\prod_{j\in\mathcal{X}} m_j! = 1$, which corresponds to $\mathbf{x}$'s whose entries are all distinct. As there are $\binom{N}{m}$ such $\mathbf{x}$'s, we can calculate the trace distance as

$$\begin{aligned}\mathrm{TD}\big(\rho^m, \rho_\mu^m \big) &= \binom{N}{m} \left[\frac{m!}{N^m} - \binom{N+m-1}{m}^{-1} \right] \\ &= \frac{N(N-1)\cdots(N-m+1)}{N^m} - \frac{N(N-1)\cdots(N-m+1)}{(N+m-1)\cdots N}.\end{aligned}$$

As first term is less than 1 and is at least

$$(1-\frac{1}{N})\cdots(1-\frac{m-1}{N}) \geq 1-\frac{1+2+\cdots+(m-1)}{N}$$

For our choices of $m \in \mathrm{poly}(\kappa)$ and $N \in 2^{\mathrm{poly}(\kappa)}$, this term is $1-\mathrm{negl}(\kappa)$ for sufficiently large security parameter κ. Similar analysis applies to the second term and this completes the proof.

3.3 Comparison with Related Work

We remark that a similar family of states was considered in [1] (Theorem 3). However, the size of the state family there depends on a parameter d which should be larger than the sum of the number of state copies and the number of queries. In our construction, the key space is fixed for a given security parameter, which may be advantageous for various applications.

We mention several other candidate constructions of PRS's and leave detailed analysis of them to future work. A construction closely related to the random phase states in Eq. (8) uses random ± 1 phases,

$$|\phi_k\rangle = \frac{1}{\sqrt{N}}\sum_{x\in\mathcal{X}}(-1)^{\mathsf{PRF}_k(x)}|x\rangle.$$

Intuitively, this family is less random than the random phase states in Eq. (8) and the corresponding density matrix ρ^m has small off-diagonal entries, making the proof more challenging. The other family of candidate states on $2n$ qubits takes the form

$$|\phi_k\rangle = \frac{1}{\sqrt{N}}\mathsf{PRP}_k\left[\sum_{x\in\mathcal{X}}|x\rangle\otimes|0^n\rangle\right].$$

In this construction, the state is an equal superposition of a random subset of size 2^n of $\{0,1\}^{2n}$ and PRP is any pseudorandom permutation over the set $\{0,1\}^{2n}$. We call this the *random subset states* construction.

Finally, we remark that under plausible cryptographic assumptions our PRS constructions can be implemented using shallow quantum circuits of polylogarithmic depth. To see this, note that there exist PRFs that can be computed in polylogarithmic depth [6], which are based on lattice problems such as "learning with errors" (LWE) [53], and are believed to be secure against quantum computers. These PRFs can be used directly in our PRS construction. (Alternatively, one can use low-depth PRFs that are constructed from more general assumptions, such as the existence of trapdoor one-way permutations [47].)

This shows that PRS states can be prepared in surprisingly small depth, compared to quantum state t-designs, which generally require at least linear depth when t is a constant greater than 2, or polynomial depth when t grows polynomially with the number of qubits [4,12,44,41]. (Note, however, that for $t = 2$, quantum state 2-designs can be generated in logarithmic depth [16].) Moreover, PRS states are sufficient for many applications where high-order t-designs are used [52,36], provided that one only requires states to be *computationally* (not statistically) indistinguishable from Haar-random.

4 Cryptographic No-cloning Theorem and Quantum Money

A fundamental fact in quantum information theory is that unknown or random quantum states cannot be cloned [63,18,61,49,51]. The main topic of this section is to investigate the cloning problem for pseudorandom states. As we will see, even though pseudorandom states can be efficiently generated, they do share the no-cloning property of generic quantum states.

Let $\mathcal{H}$ be the Hilbert space of dimension N and $m < m'$ be two integers. The numbers N, m, m' depend implicitly on a security parameter κ. We will assume that N is exponential in κ and $m \in \mathrm{poly}(\kappa)$ in the following discussion.

We first recall the fact that for Haar random state $|\psi\rangle \in \mathrm{S}(\mathcal{H})$, the success probability of producing m' copies of the state given m copies is negligibly small. Let $\mathcal{C}$ be a cloning channel that on input $(|\psi\rangle\langle\psi|)^{\otimes m}$ tries to output a state that is close to $(|\psi\rangle\langle\psi|)^{\otimes m'}$ for $m' > m$. The expected success probability of $\mathcal{C}$ is measured by

$$\int \Big\langle \big(|\psi\rangle\langle\psi|\big)^{\otimes m'}, \mathcal{C}\big(\big(|\psi\rangle\langle\psi|\big)^{\otimes m}\big) \Big\rangle \, \mathrm{d}\mu(\psi).$$

It is known that [61], for all cloning channel $\mathcal{C}$, this success probability is bounded by

$$\binom{N+m-1}{m} \Big/ \binom{N+m'-1}{m'},$$

which is $\mathrm{negl}(\kappa)$ for our choices of N, m, m'.

We establish a no-cloning theorem for PRS's which says that no efficient quantum cloning procedure exists for a general PRS. The theorem is called the cryptographic no-cloning theorem because of its deep roots in pseudorandomness in cryptography.

Theorem 2 (Cryptographic No-cloning Theorem). *For any PRS family $\{|\phi_k\rangle\}_{k\in\mathcal{K}}$, $m \in \mathrm{poly}(\kappa)$, $m < m'$ and any polynomial-time quantum algorithm $\mathcal{C}$, the success cloning probability*

$$\mathop{\mathbb{E}}_{k\in\mathcal{K}} \Big\langle \big(|\phi_k\rangle\langle\phi_k|\big)^{\otimes m'}, \mathcal{C}\big(\big(|\phi_k\rangle\langle\phi_k|\big)^{\otimes m}\big) \Big\rangle = \mathrm{negl}(\kappa).$$

Proof. Assume on the contrary that there is a polynomial-time quantum cloning algorithm $\mathcal{C}$ such that the success cloning probability of producing $m+1$ from m copies is κ^{-c} for some constant $c > 0$. We will construct a polynomial-time distinguisher $\mathcal{D}$ that violates the definition of PRS's. Distinguisher $\mathcal{D}$ will draw $2m+1$ copies of the state, call $\mathcal{C}$ on the first m copies, and perform the SWAP test on the output of $\mathcal{C}$ and the remaining $m+1$ copies. It is easy to see that $\mathcal{D}$ outputs 1 with probability $(1+\kappa^{-c})/2$ if the input is from PRS, while if the input is Haar random, it outputs 1 with probability $(1+\mathrm{negl}(\kappa))/2$. Since $\mathcal{C}$ is polynomial-time, it follows that $\mathcal{D}$ is also polynomial-time. This is a contradiction with the definition of PRS's and completes the proof.

4.1 A Strong Notion of PRS and Equivalence to PRS

In this section, we show that, somewhat surprisingly, PRS in fact implies a seemingly stronger notion, where indistinguishability needs to hold even if a distinguisher additionally has access to an oracle that reflects about the given state. There are at least a couple of motivations to consider an augmented notion. Firstly, unlike a classical string, a quantum state is inherently *hidden*. Give a quantum register prepared in some state (i.e., a physical system), we can only choose some observable to measure which just reveals partial information and will collapse the state in general. Therefore, it is meaningful to consider offering a distinguishing algorithm more information *describing* the given state, and the reflection oracle comes naturally. Secondly, this stronger notion is extremely useful in our application of quantum money schemes, and could be interesting elsewhere too.

More formally, for any state $|\phi\rangle \in \mathcal{H}$, define an oracle $O_\phi := \mathbb{1} - 2|\phi\rangle\langle\phi|$ that reflects about $|\phi\rangle$.

Definition 3 (Strongly Pseudorandom Quantum States). *Let $\mathcal{H}$ be a Hilbert space and $\mathcal{K}$ be the key space. $\mathcal{H}$ and $\mathcal{K}$ depend on the security parameter κ. A keyed family of quantum states $\left\{|\phi_k\rangle \in \mathrm{S}(\mathcal{H})\right\}_{k\in\mathcal{K}}$ is **strongly pseudorandom**, if the following two conditions hold:*

1. *(**Efficient generation**). There is a polynomial-time quantum algorithm G that generates state $|\phi_k\rangle$ on input k. That is, for all $k \in \mathcal{K}$, $G(k) = |\phi_k\rangle$.*
2. *(**Strong Pseudorandomness**). Any polynomially many copies of $|\phi_k\rangle$ with the same random $k \in \mathcal{K}$ is **computationally indistinguishable** from the same number of copies of a Haar random state. More precisely, for any efficient quantum oracle algorithm $\mathcal{A}$ and any $m \in \mathrm{poly}(\kappa)$,*

$$\left|\Pr_{k\leftarrow\mathcal{K}}\left[\mathcal{A}^{O_{\phi_k}}(|\phi_k\rangle^{\otimes m}) = 1\right] - \Pr_{|\psi\rangle\leftarrow\mu}\left[\mathcal{A}^{O_\psi}(|\psi\rangle^{\otimes m}) = 1\right]\right| = \mathrm{negl}(\kappa),$$

where μ is the Haar measure on $\mathrm{S}(\mathcal{H})$.

Note that since the distinguisher $\mathcal{A}$ is polynomial-time, the number of queries to the reflection oracle (O_{ϕ_k} or O_ψ) is also polynomially bounded.

We prove the advantage that a reflection oracle may give to a distinguisher is limited. In fact, standard PRS implies strong PRS, and hence they are equivalent.

Theorem 3. *A family of states $\left\{|\phi_k\rangle\right\}_{k\in\mathcal{K}}$ is strongly pseudorandom if and only if it is (standard) pseudorandom.*

Proof. Clearly a strong PRS is also a standard PRS by definition. It suffice to prove that any PRS is also strongly pseudorandom.

Suppose for contradiction that there is a distinguishing algorithm $\mathcal{A}$ that breaks the strongly pseudorandom condition. Namely, there exists $m \in \mathrm{poly}(\kappa)$ and constant $c > 0$ such that for sufficiently large κ,

$$\left|\Pr_{k\leftarrow\mathcal{K}}\left[\mathcal{A}^{O_{\phi_k}}(|\phi_k\rangle^{\otimes m}) = 1\right] - \Pr_{|\psi\rangle\leftarrow\mu}\left[\mathcal{A}^{O_\psi}(|\psi\rangle^{\otimes m}) = 1\right]\right| = \varepsilon(\kappa) \geq \kappa^{-c}.$$

We assume $\mathcal{A}$ makes $q \in \text{poly}(\kappa)$ queries to the reflection oracle. Then, by Theorem 4, there is an algorithm $\mathcal{B}$ such that for any l

$$\left| \Pr_{k \leftarrow \mathcal{K}} \left[\mathcal{A}^{O_{\phi_k}}(|\phi_k\rangle^{\otimes m}) \right] - \Pr_{k \leftarrow \mathcal{K}} \left[\mathcal{B}(|\phi_k\rangle^{\otimes (m+l)}) \right] \right| \leq \frac{2q}{\sqrt{l+1}},$$

and

$$\left| \Pr_{|\psi\rangle \leftarrow \mu} \left[\mathcal{A}^{O_{\psi}}(|\psi\rangle^{\otimes m}) \right] - \Pr_{|\psi\rangle \leftarrow \mu} \left[\mathcal{B}(|\psi\rangle^{\otimes (m+l)}) \right] \right| \leq \frac{2q}{\sqrt{l+1}}.$$

By triangle inequality, we have

$$\left| \Pr_{k \leftarrow \mathcal{K}} \left[\mathcal{B}(|\phi_k\rangle^{\otimes (m+l)}) \right] - \Pr_{|\psi\rangle \leftarrow \mu} \left[\mathcal{B}(|\psi\rangle^{\otimes (m+l)}) \right] \right| \geq \kappa^{-c} - \frac{4q}{\sqrt{l+1}}.$$

Choosing $l = 64q^2\kappa^{2c} \in \text{poly}(\kappa)$, we have

$$\left| \Pr_{k \leftarrow \mathcal{K}} \left[\mathcal{B}(|\phi_k\rangle^{\otimes (m+l)}) \right] - \Pr_{|\psi\rangle \leftarrow \mu} \left[\mathcal{B}(|\psi\rangle^{\otimes (m+l)}) \right] \right| \geq \kappa^{-c}/2,$$

which is a contradiction with the definition of PRS for $\{|\phi_k\rangle\}$. Therefore, we conclude that PRS and strong PRS are equivalent.

We now show a technical ingredient that allows us to simulate the reflection oracle about a state by using multiple copies of the given state. This result is inspired by a similar theorem proved by Ambainis et al. [5, Lemma 42]. Our simulation applies the reflection about the standard symmetric subspace, as opposed to a reflection operation about a particular subspace in [5], on the multiple copies of the given state, which we know how to implement efficiently.

Theorem 4. *Let $|\psi\rangle \in \mathcal{H}$ be a quantum state. Define oracle $O_\psi = \mathbb{1} - 2|\psi\rangle\langle\psi|$ to be the reflection about $|\psi\rangle$. Let $|\xi\rangle$ be a state not necessarily independent of $|\psi\rangle$. Let $\mathcal{A}^{O_\psi}$ be an oracle algorithm that makes q queries to O_ψ. For any integer $l > 0$, there is a quantum algorithm $\mathcal{B}$ that makes no queries to O_ψ such that*

$$\text{TD}\big(\mathcal{A}^{O_\psi}(|\xi\rangle), \mathcal{B}(|\psi\rangle^{\otimes l} \otimes |\xi\rangle)\big) \leq \frac{q\sqrt{2}}{\sqrt{l+1}}\,.$$

Moreover, the running time of $\mathcal{B}$ is polynomial in that of $\mathcal{A}$ and l.

Proof. Consider a quantum register T, initialized in the state $|\Theta\rangle_{\mathsf{T}} = |\psi\rangle^{\otimes l} \in \mathcal{H}^{\otimes l}$. Let Π be the projection onto the symmetric subspace $\vee^{l+1}\mathcal{H} \subset \mathcal{H}^{\otimes (l+1)}$, and let $R = \mathbb{1} - 2\Pi$ be the reflection about the symmetric subspace.

Assume without loss of generality that algorithm $\mathcal{A}$ is unitary and only performs measurements at the end. We define algorithm $\mathcal{B}$ to be the same as $\mathcal{A}$, except that when $\mathcal{A}$ queries O_ψ on register D, $\mathcal{B}$ applies the reflection R on the collection of quantum registers D and T. We first analyze the corresponding states after the first oracle call to O_ψ in algorithms $\mathcal{A}$ and $\mathcal{B}$,

$$|\Psi_A\rangle = O_\psi\big(|\phi\rangle_{\mathsf{D}}\big) \otimes |\Theta\rangle_{\mathsf{T}}, \quad |\Psi_B\rangle = R\big(|\phi\rangle_{\mathsf{D}} \otimes |\Theta\rangle_{\mathsf{T}}\big).$$

For any two states $|x\rangle, |y\rangle \in \mathcal{H}$, we have

$$\begin{aligned}\big(\langle x| \otimes \langle\Theta|\big) R\big(|y\rangle \otimes |\Theta\rangle\big) &= \langle x|y\rangle - 2 \mathop{\mathbb{E}}_{\pi \in S_{l+1}} \big(\langle x| \otimes \langle\Theta|\big) W_\pi \big(|y\rangle \otimes |\Theta\rangle\big) \\ &= \langle x|y\rangle - \frac{2}{l+1} \langle x|y\rangle - \frac{2l}{l+1} \langle x|\psi\rangle \langle\psi|y\rangle \\ &= \frac{l-1}{l+1} \langle x|y\rangle - \frac{2l}{l+1} \langle x|\psi\rangle \langle\psi|y\rangle ,\end{aligned}$$

where the first step uses the identity in Eq. (6) and the second step follows by observing that the probability of a random $\pi \in S_{l+1}$ mapping 1 to 1 is $1/(l+1)$. These calculations imply that,

$$\big(\mathbb{1} \otimes \langle\Theta|\big) R\big(\mathbb{1} \otimes |\Theta\rangle\big) = \frac{l-1}{l+1}\mathbb{1} - \frac{2l}{l+1}|\psi\rangle\langle\psi|.$$

We can compute the inner product of the two states $|\Psi_A\rangle$ and $|\Psi_B\rangle$ as

$$\begin{aligned}\langle\Psi_A|\Psi_B\rangle &= \mathrm{tr}\Big(\big(|\phi\rangle \otimes |\Theta\rangle\big) \big(\langle\phi| \otimes \langle\Theta|\big) \left(O_\psi \otimes \mathbb{1}\right) R\Big) \\ &= \mathrm{tr}\Big(|\phi\rangle\langle\phi|\, O_\psi \left(\mathbb{1} \otimes \langle\Theta|\right) R \left(\mathbb{1} \otimes |\Theta\rangle\right)\Big) \\ &= \mathrm{tr}\left(|\phi\rangle\langle\phi|\big(\mathbb{1} - 2|\psi\rangle\langle\psi|\big) \left(\frac{l-1}{l+1}\mathbb{1} - \frac{2l}{l+1}|\psi\rangle\langle\psi|\right)\right) \\ &= \frac{l-1}{l+1} + \frac{2l}{l+1} |\langle\phi|\psi\rangle|^2 - \frac{2(l-1)}{l+1} |\langle\phi|\psi\rangle|^2 \\ &= \frac{l-1}{l+1} + \frac{2}{l+1} |\langle\phi|\psi\rangle|^2 \\ &\geq 1 - \frac{2}{l+1}.\end{aligned}$$

This implies that

$$\big\||\Psi_A\rangle - |\Psi_B\rangle\big\| \leq \frac{2}{\sqrt{l+1}}.$$

Let $|\Psi_A^q\rangle$ and $|\Psi_B^q\rangle$ be the final states of algorithm $\mathcal{A}$ and $\mathcal{B}$ before measurement respectively. Then by induction on the number of queries, we have

$$\big\||\Psi_A^q\rangle - |\Psi_B^q\rangle\big\| \leq \frac{2q}{\sqrt{l+1}}\,.$$

This concludes the proof by noticing that

$$\mathrm{TD}\big(|\Psi_A^q\rangle, |\Psi_B^q\rangle\big) \leq \big\||\Psi_A^q\rangle - |\Psi_B^q\rangle\big\|\,.$$

Finally, we show that if $\mathcal{A}$ is polynomial-time, then so is $\mathcal{B}$. Based on the construction of $\mathcal{B}$, it suffices to show that the reflection R is efficiently implementable for any polynomially large l. Here we use a result by Barenco et al. [8] which provides an efficient implementation for the projection Π onto $\vee^{l+1}\mathcal{H}$. More

precisely, they design a quantum circuit of size $O(\mathrm{poly}(l, \log \dim \mathcal{H}))$ that implements a unitary U such that $U|\phi\rangle = \sum_j |\xi_j\rangle|j\rangle$ on $\mathcal{H}^{\otimes(l+1)} \otimes \mathcal{H}'$ for an auxiliary space $\mathcal{H}'$ of dimension $O(l!)$. Here $|\xi_0\rangle = \Pi|\phi\rangle$ corresponds to the projection of $|\phi\rangle$ on the symmetric subspace. With U, we can implement the reflection R as $U^* S U$ where S is the unitary that introduces a minus sign conditioned on the second register being 0.

$$S|\Psi\rangle|j\rangle = \begin{cases} -|\Psi\rangle|j\rangle & \text{if } j = 0, \\ |\Psi\rangle|j\rangle & \text{otherwise.} \end{cases}$$

4.2 Quantum Money from PRS

Using Theorem 3, we can improve Theorem 2 to the following version. The proof is omitted as it is very similar to that for Theorem 2 and uses the complexity-theoretic no-cloning theorem [1,2] for Haar random states.

Theorem 5 (Cryptographic no-cloning Theorem with Oracle). *For any PRS $\{|\phi_k\rangle\}_{k\in\mathcal{K}}$, $m \in \mathrm{poly}(\kappa)$, $m < m'$ and any polynomial-time quantum query algorithm $\mathcal{C}$, the success cloning probability*

$$\mathop{\mathbb{E}}_{k\in\mathcal{K}} \left\langle \left(|\phi_k\rangle\langle\phi_k|\right)^{\otimes m'}, \mathcal{C}^{O_{\phi_k}}\left(\left(|\phi_k\rangle\langle\phi_k|\right)^{\otimes m}\right) \right\rangle = \mathrm{negl}(\kappa).$$

A direct application of this no-cloning theorem is that it gives rise to new constructions for private-key quantum money. As one of the earliest findings in quantum information [62,9], quantum money schemes have received revived interests in the past decade (see e.g. [1,40,43,21,22,3]). First, we recall the definition of quantum money scheme adapted from [2].

Definition 4 (Quantum Money Scheme). *A private-key quantum money scheme $\mathcal{S}$ consists of three algorithms:*

- *KeyGen, which takes as input the security parameter 1^κ and randomly samples a private key k.*
- *Bank, which takes as input the private key k and generates a quantum state $|\$\rangle$ called a **banknote**.*
- *Ver, which takes as input the private key k and an alleged banknote $|\dot{\varsigma}\rangle$, and either accepts or rejects.*

*The money scheme $\mathcal{S}$ has **completeness error** ε if $\mathsf{Ver}(k, |\$\rangle)$ accepts with probability at least $1 - \varepsilon$ for all valid banknote $|\$\rangle$.*

*Let Count be the money counter that output the number of valid banknotes when given a collection of (possibly entangled) alleged banknotes $|\dot{\varsigma}_1, \dot{\varsigma}_2, \ldots, \dot{\varsigma}_r\rangle$. Namely, Count will call Ver on each banknotes and return the number of times that Ver accepts. The money scheme $\mathcal{S}$ has **soundness error** δ if for any polynomial-time counterfeiter C that maps q valid banknotes $|\$_1\rangle, \ldots, |\$_q\rangle$ to r alleged banknotes $|\dot{\varsigma}_1, \ldots, \dot{\varsigma}_r\rangle$ satisfies*

$$\Pr\left[\mathsf{Count}\left(k, C(|\$_1\rangle, \ldots, |\$_q\rangle)\right) > q\right] \leq \delta.$$

*The scheme $\mathcal{S}$ is **secure** if it has completeness error $\leq 1/3$ and negligible soundness error.*

For any $\mathsf{PRS} = \{|\phi_k\rangle\}_{k\in\mathcal{K}}$ with key space $\mathcal{K}$, we can define a private-key quantum money scheme $\mathcal{S}_{\mathsf{PRS}}$ as follows:

- $\mathsf{KeyGen}(1^\kappa)$ randomly outputs $k \in \mathcal{K}$.
- $\mathsf{Bank}(k)$ generates the banknote $|\$\rangle = |\phi_k\rangle$.
- $\mathsf{Ver}(k, \rho)$ applies the projective measurement that accepts ρ with probability $\langle\phi_k|\rho|\phi_k\rangle$.

We remark that usually the money state $|\$\rangle$ takes the form $|\$\rangle = |s, \psi_s\rangle$ where the first register contains a classical serial number. Our scheme, however, does not require the use of the serial numbers. This simplification is brought to us by the strong requirement that any polynomial copies of $|\phi_k\rangle$ are indistinguishable from Haar random states.

Theorem 6. *The private-key quantum money scheme $\mathcal{S}_{\mathsf{PRS}}$ is secure for all PRS.*

Proof. It suffices to prove the soundness of S_{PRS} is negligible. Assume to the contrary that there is a counterfeiter C such that

$$\Pr\big[\mathsf{Count}\big(k, C(|\phi_k\rangle^{\otimes q})\big) > q\big] \geq \kappa^{-c}$$

for some constant $c > 0$ and sufficiently large κ. From the counterfeiter C, we will construct an oracle algorithm $\mathcal{A}^{O_{\phi_k}}$ that maps q copies of $|\phi_k\rangle$ to $q+1$ copies with noticeable probability and this leads to a contradiction with Theorem 5.

The oracle algorithm $\mathcal{A}$ first runs C and implement the measurement

$$\Big\{M^0 = \mathbb{1} - |\phi_k\rangle\langle\phi_k|, M^1 = |\phi_k\rangle\langle\phi_k|\Big\}$$

on each copy of the money state C outputs. This measurement can be implemented by attaching an auxiliary qubit initialized in $(|0\rangle + |1\rangle)/\sqrt{2}$ and call the reflection oracle O_ϕ conditioned on the qubit being at 1 and performs the X measurement on this auxiliary qubit. This gives r-bit of outcome $\mathbf{x} \in \{0,1\}^r$. If $\mathbf{x}$ has Hamming weight at least $q+1$, algorithm $\mathcal{A}$ outputs any $q+1$ registers that corresponds to outcome 1; otherwise, it outputs $|0\rangle^{\otimes(q+1)}$. By the construction of $\mathcal{A}$, it succeeds in cloning $q+1$ money states from q copies with probability at least κ^{-c}.

Our security proof of the quantum money scheme is arguably simpler than that in [2]. In [2], to prove their hidden subspace money scheme is secure, one needs to develop the so called inner-product adversary method to show the worst-case query complexity for the hidden subspace states and use a random self-reducible argument to establish the average-case query complexity. In our case, it follows almost directly from the cryptographic no-cloning theorem with oracles. The quantum money schemes derived from PRS's enjoy many nice features of the hidden subspace scheme. Most importantly, they are also *query-secure* [2],

meaning that the bank can simply return the money state back to the user after verification.

It is also interesting to point out that quantum money states are not necessarily pseudorandom states. The hidden subspace state [2], for example, do not satisfy our definition of PRS as one can measure polynomially many copies of the state in the computational basis and recover a basis for the hidden subspace with high probability.

5 Entanglement of Pseudorandom Quantum States

In this section, we study the entanglement property of pseudorandom quantum states. Our result shows that any PRS consists of states that have high entanglement on average.

The entanglement property of a bipartite pure quantum state is well understood and is completely determined by the Schmidt coefficients of a bipartite state (see e.g. [32]). Any state $|\psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$ on system A and B can be written as

$$|\psi\rangle = \sum_{j=1}^{R} \sqrt{\lambda_j}\, |\psi_A^j\rangle \otimes |\psi_B^j\rangle,$$

where $\lambda_j > 0$ for all $1 \leq j \leq R$ and the states $|\psi_A^j\rangle$ (and $|\psi_B^j\rangle$) form a set of orthonormal states on A (and B respectively). Here, the positive real numbers λ_j's are the Schmidt coefficients and R is the Schmidt rank of state $|\psi\rangle$. Let ρ_A be the reduced density matrix of $|\psi\rangle$ on system A, then λ_j is the nonzero eigenvalues of ρ_A. Entanglement can be measured by the Schmidt rank R or entropy-like quantities derived from the Schmidt coefficients. We consider the quantum α-Rényi entropy of ρ_A

$$S_\alpha(\rho_A) := \frac{1}{1-\alpha} \log\left(\sum_{j=1}^{R} \lambda_j^\alpha\right).$$

When $\alpha \to 1$, S_α coincides with the von Neumann entropy of ρ_A

$$S(\rho_A) = -\sum_{j=1}^{R} \lambda_j \log \lambda_j.$$

When $\alpha \to \infty$, S_α coincides with the quantum min entropy of ρ_A

$$S_{\min}(\rho_A) = -\log \|\rho_A\| = -\log \lambda_{\max},$$

where $\lambda_{\max}$ is the largest eigenvalue of ρ_A. For $\alpha = 2$, the entropy S_2 is the quantum analogue of the collision entropy.

For Haar random state $|\psi\rangle \sim \mu(\mathcal{H}_A \otimes \mathcal{H}_B)$ where the dimensions of $\mathcal{H}_A$ and $\mathcal{H}_B$ are d_A and d_B respectively, the Page conjecture [50] proved in [23,55,56] states that for $d_A \leq d_B$, the average entanglement entropy is explicitly given as

$$\mathbb{E}\, S(\rho_A) = \frac{1}{\ln 2}\left[\left(\sum_{j=d_B+1}^{d_A d_B} \frac{1}{j}\right) - \frac{d_B - 1}{2d_A}\right] > \log d_A - O(1).$$

That is, the Haar random states are highly entangled on average and, in fact, a typical Haar random state is almost maximumly entangled. A more detailed discussion on this phenomena is give in [29,35]. The following theorem and its corollary tell us that pseudorandom states are also entangled on average though the quantitative bound is much weaker.

Theorem 7. *Let $\{|\phi_k\rangle\}_{k\in\mathcal{K}}$ be a family of PRS with security parameter κ. Consider partitions of the state $|\phi_k\rangle$ into systems A and B consisting of n_A and n_B qubits each where both n_A and n_B are polynomial in the security parameter. Let ρ_k be the reduced density matrix on system A. Then,*

$$\mathop{\mathbb{E}}_{k} \operatorname{tr}(\rho_k^2) = \operatorname{negl}(\kappa).$$

Proof. Assume to the contrary that

$$\mathop{\mathbb{E}}_{k} \operatorname{tr}(\rho_k^2) \geq \kappa^{-c}$$

for some constant $c > 0$ and sufficiently large κ. We will construct a distinguisher $\mathcal{A}$ that tells the family of state $\{|\phi_k\rangle\}$ apart from the Haar random states.

Consider the SWAP test performed on the system A of two copies of $|\phi_k\rangle$. The test accepts with probability

$$\frac{1+\operatorname{tr}(\rho_k^2)}{2}.$$

Let distinguisher $\mathcal{A}$ be the above SWAP test, we have

$$\begin{aligned}&\left|\Pr_{k\leftarrow\mathcal{K}}\left[\mathcal{A}(|\phi_k\rangle^{\otimes 2})=1\right] - \Pr_{|\psi\rangle\leftarrow\mu}\left[\mathcal{A}(|\psi\rangle^{\otimes 2})=1\right]\right| \\ =&\frac{1}{2}\left|\mathop{\mathbb{E}}_{k}\operatorname{tr}(\rho_k^2) - \mathop{\mathbb{E}}_{\mu}\operatorname{tr}(\rho_\psi^2)\right| \geq \kappa^{-c}/4,\end{aligned}$$

for sufficiently large κ. The last step follows by a formula of Lubkin [37]

$$\mathop{\mathbb{E}}_{|\psi\rangle\leftarrow\mu}\operatorname{tr}(\rho_\psi^2) = \frac{d_A+d_B}{d_Ad_B+1} = \frac{2^{n_A}+2^{n_B}}{2^{n_A+n_B}+1} = \operatorname{negl}(\kappa).$$

Corollary 1. *Let $\{|\phi_k\rangle\}_{k\in\mathcal{K}}$ be a family of PRS with security parameter κ. Consider partitions of the state $|\phi_k\rangle$ into systems A and B consisting of n_A and n_B qubits each where both n_A and n_B are polynomial in the security parameter. We have*

1. *Let R_k be the Schmidt rank of state $|\phi_k\rangle$ under the A, B partition, then $\mathbb{E}_k R_k \geq \kappa^c$ for all constant $c > 0$ and sufficiently large κ.*
2. *$\mathbb{E}_k S_{\min}(\rho_k) = \omega(\log\kappa)$ and $\mathbb{E}_k S(\rho_k) = \omega(\log\kappa)$.*

Proof. The first item follows from the fact that

$$\mathrm{tr}(\rho_k^2) \geq \frac{1}{R_k}.$$

where R_k is the Schmidt rank of state $|\phi_k\rangle$. The second item for the min entropy follows by Jensen's inequality and

$$\mathrm{tr}(\rho_k^2) \geq \lambda_{\max}^2.$$

Finally, the bound on the expected entanglement entropy follows by the fact that min entropy is the smallest α-Rényi entropy for all $\alpha > 0$.

6 Pseudorandom Unitary Operators (PRUs)

6.1 Definitions

Our notion of pseudorandom states readily extends to distributions over unitary operators. Let $\mathcal{H}$ be a Hilbert space and let $\mathcal{K}$ a key space, both of which depend on a security parameter κ. Let μ be the Haar measure on the unitary group $\mathrm{U}(\mathcal{H})$.

Definition 5. *A family of unitary operators $\{U_k \in \mathrm{U}(\mathcal{H})\}_{k\in\mathcal{K}}$ is **pseudorandom**, if two conditions hold:*

1. *(**Efficient computation**) There is an efficient quantum algorithm Q, such that for all k and any $|\psi\rangle \in \mathrm{S}(\mathcal{H})$, $Q(k, |\psi\rangle) = U_k|\psi\rangle$.*
2. *(**Pseudorandomness**) U_k with a random key k is **computationally indistinguishable** from a Haar random unitary operator. More precisely, for any efficient quantum algorithm $\mathcal{A}$ that makes at most polynomially many queries to the oracle,*

$$\left| \Pr_{k\leftarrow\mathcal{K}}\left[\mathcal{A}^{U_k}(1^\kappa) = 1\right] - \Pr_{U\leftarrow\mu}\left[\mathcal{A}^{U}(1^\kappa) = 1\right] \right| = \mathrm{negl}(\kappa).$$

The extensive literature on approximation of Haar randomness on unitary groups concerns with unitary *designs* [19,12], which are statistical approximations to the Haar random distribution up to a fixed t-th moment. Our notion of pseudorandom unitary operators in terms of computational indistinguishability, in addition to independent interest, supplements and could substitute for unitary designs in various applications.

6.2 Candidate constructions

Clearly, given a pseudorandom unitary family $\{U_k\}$, it immediately gives pseudorandom states as well (e.g., $\{U_k|0\rangle\}$). On the other hand, our techniques for constructing pseudorandom states can be extended to give candidate constructions for pseudorandom unitary operators (PRUs) in the following way. Let

$\mathcal{H} = (\mathbb{C}^2)^{\otimes n}$. Assume we have a pseudorandom function $\mathsf{PRF} : \mathcal{K} \times \mathcal{X} \to \mathcal{X}$, with domain $\mathcal{X} = \{0, 1, 2, \ldots, N-1\}$ and $N = 2^n$. Using the phase kick-back technique, we can implement the unitary transformation $T_k \in \mathrm{U}(\mathcal{H})$ that maps

$$T_k : |x\rangle \mapsto \omega_N^{\mathsf{PRF}_k(x)}|x\rangle, \quad \omega_N = \exp(2\pi i/N). \tag{9}$$

Our pseudorandom states were given by $|\phi_k\rangle = T_k H^{\otimes n}|0\rangle$, where $H^{\otimes n}$ denotes the n-qubit Hadamard transform. We conjecture that by repeating the operation $T_k H^{\otimes n}$ a constant number of times (with different keys k), we get a PRU. This is resembles the construction of unitary t-designs in [45,44].

Alternatively, one can give a candidate construction for PRUs based on pseudorandom permutations (PRPs) as follows. First, let PRP_k be a pseudorandom permutation (with key $k \in \mathcal{K}$) acting on $\{0,1\}^n$, and suppose we have efficient quantum circuits that compute the permutation $P_k : |x\rangle|y\rangle \mapsto |x\rangle|y \oplus \mathsf{PRP}_k(x)\rangle$ as well as its inverse $R_k : |x\rangle|y\rangle \mapsto |x\rangle|y \oplus \mathsf{PRP}_k^{-1}(x)\rangle$ (where $\oplus$ denotes the bitwise xor operation). Then we can compute the permutation in-place by applying the following sequence of operations:

$$\begin{aligned} |x\rangle|0\rangle &\xrightarrow{P_k} |x\rangle|\mathsf{PRP}_k(x)\rangle \\ &\xrightarrow{SWAP} |\mathsf{PRP}_k(x)\rangle|x\rangle \\ &\xrightarrow{R_k} |\mathsf{PRP}_k(x)\rangle|0\rangle. \end{aligned} \tag{10}$$

For simplicity, let us denote this operation by $S_k : |x\rangle \mapsto |\mathsf{PRP}_k(x)\rangle$ (ignoring the second register, which stays in the state $|0\rangle$). Now we can consider repeating the operation $S_k H^{\otimes n}$ several times (with different keys k), as a candidate for a PRU. Note that this resembles the construction of unitary t-designs in [27].

It is an interesting challenge to prove that these constructions actually yield PRUs. For the special case of non-adaptive adversaries, one could try to use the proof techniques of [27,45,44] for unitary t-designs. For the general case, where the adversary can make adaptive queries to the pseudorandom unitary, new proof techniques seem to be needed. Finally, we can consider combining all of these ingredients (the pseudorandom operations S_k and T_k, and the Hadamard transform) to try to obtain more efficient constructions of PRUs.

References

1. Aaronson, S.: Quantum copy-protection and quantum money. In: Proceedings of the Twenty-Fourth Annual IEEE Conference on Computational Complexity (CCC'09). pp. 229–242. IEEE Computer Society (2009), http://dx.doi.org/10.1109/CCC.2009.42
2. Aaronson, S., Christiano, P.: Quantum money from hidden subspaces. In: Proceedings of the Forty-fourth Annual ACM Symposium on Theory of Computing. pp. 41–60. STOC '12, ACM, New York, NY, USA (2012), http://doi.acm.org/10.1145/2213977.2213983
3. Aaronson, S., Farhi, E., Gosset, D., Hassidim, A., Kelner, J., Lutomirski, A.: Quantum money. Commun. ACM 55(8), 84–92 (Aug 2012), http://doi.acm.org/10.1145/2240236.2240258
4. Ambainis, A., Emerson, J.: Quantum t-designs: t-wise Independence in the Quantum World. In: Proceedings of the Twenty-Second Annual IEEE Conference on Computational Complexity (CCC'07). pp. 129–140 (June 2007)
5. Ambainis, A., Rosmanis, A., Unruh, D.: Quantum attacks on classical proof systems: The hardness of quantum rewinding. In: Proceedings of the 2014 IEEE 55th Annual Symposium on Foundations of Computer Science. pp. 474–483. IEEE Computer Society (2014), http://dx.doi.org/10.1109/FOCS.2014.57, full version at https://arxiv.org/abs/1404.6898
6. Banerjee, A., Peikert, C., Rosen, A.: Pseudorandom functions and lattices. In: Advances in Cryptology–Eurocrypt 2012. pp. 719–737. Springer-Verlag (2012), http://dx.doi.org/10.1007/978-3-642-29011-4_42
7. Barak, B., Shaltiel, R., Wigderson, A.: Computational analogues of entropy. In: Arora, S., Jansen, K., Rolim, J.D.P., Sahai, A. (eds.) Approximation, Randomization, and Combinatorial Optimization.. Algorithms and Techniques. pp. 200–215. Springer Berlin Heidelberg, Berlin, Heidelberg (2003)
8. Barenco, A., Berthiaume, A., Deutsch, D., Ekert, A., Jozsa, R., Macchiavello, C.: Stabilization of quantum computations by symmetrization. SIAM Journal on Computing 26(5), 1541–1557 (1997), https://doi.org/10.1137/S0097539796302452
9. Bennett, C.H., Brassard, G., Breidbart, S., Wiesner, S.: Quantum Cryptography, or Unforgeable Subway Tokens, pp. 267–275. Springer, Boston, MA (1983)
10. Blum, M., Micali, S.: How to Generate Cryptographically Strong Sequences of Pseudorandom Bits. SIAM Journal on Computing 13(4), 850–864 (1984), https://doi.org/10.1137/0213053
11. Brandão, F.G.S.L., Harrow, A.W., Horodecki, M.: Efficient quantum pseudorandomness. Phys. Rev. Lett. 116, 170502 (Apr 2016), https://link.aps.org/doi/10.1103/PhysRevLett.116.170502
12. Brandão, F.G.S.L., Harrow, A.W., Horodecki, M.: Local random quantum circuits are approximate polynomial-designs. Communications in Mathematical Physics 346(2), 397–434 (Sep 2016), https://doi.org/10.1007/s00220-016-2706-8
13. Bremner, M.J., Mora, C., Winter, A.: Are random pure states useful for quantum computation? Phys. Rev. Lett. 102, 190502 (May 2009), https://link.aps.org/doi/10.1103/PhysRevLett.102.190502
14. Chen, Y.H., Chung, K.M., Lai, C.Y., Vadhan, S.P., Wu, X.: Computational notions of quantum min-entropy. arXiv:1704.07309 (2017)
15. Chung, K.M., Shi, Y., Wu, X.: Physical randomness extractors: generating random numbers with minimal assumptions. arXiv preprint arXiv:1402.4797 (2014)

16. Cleve, R., Leung, D., Liu, L., Wang, C.: Near-linear constructions of exact unitary 2-designs. Quantum Information & Computation 16(9&10), 721–756 (2016), http://www.rintonpress.com/xxqic16/qic-16-910/0721-0756.pdf
17. Dankert, C., Cleve, R., Emerson, J., Livine, E.: Exact and approximate unitary 2-designs and their application to fidelity estimation. Phys. Rev. A 80, 012304 (Jul 2009), https://link.aps.org/doi/10.1103/PhysRevA.80.012304
18. Dieks, D.: Communication by EPR devices. Physics Letters A 92(6), 271–272 (1982)
19. Emerson, J., Weinstein, Y.S., Saraceno, M., Lloyd, S., Cory, D.G.: Pseudo-random unitary operators for quantum information processing. science 302(5653), 2098–2100 (2003)
20. Farhi, E., Gosset, D., Hassidim, A., Lutomirski, A., Nagaj, D., Shor, P.: Quantum state restoration and single-copy tomography for ground states of hamiltonians. Phys. Rev. Lett. 105, 190503 (Nov 2010), https://link.aps.org/doi/10.1103/PhysRevLett.105.190503
21. Farhi, E., Gosset, D., Hassidim, A., Lutomirski, A., Nagaj, D., Shor, P.: Quantum State Restoration and Single-Copy Tomography for Ground States of Hamiltonians. Phys. Rev. Lett. 105, 190503 (Nov 2010), https://link.aps.org/doi/10.1103/PhysRevLett.105.190503
22. Farhi, E., Gosset, D., Hassidim, A., Lutomirski, A., Shor, P.: Quantum money from knots. In: Proceedings of the 3rd Innovations in Theoretical Computer Science Conference. pp. 276–289. ITCS '12, ACM, New York, NY, USA (2012), http://doi.acm.org/10.1145/2090236.2090260
23. Foong, S.K., Kanno, S.: Proof of page's conjecture on the average entropy of a subsystem. Phys. Rev. Lett. 72, 1148–1151 (Feb 1994), https://link.aps.org/doi/10.1103/PhysRevLett.72.1148
24. Goldreich, O., Goldwasser, S., Micali, S.: On the cryptographic applications of random functions. In: Advances in Cryptology – CRYPTO 1984. pp. 276–288. Springer-Verlag New York, Inc. (1985)
25. Goldreich, O., Goldwasser, S., Micali, S.: How to Construct Random Functions. J. ACM 33(4), 792–807 (Aug 1986), http://doi.acm.org/10.1145/6490.6503
26. Harrow, A.W.: The church of the symmetric subspace. arXiv:1308.6595 (2013)
27. Harrow, A.W., Low, R.A.: Efficient quantum tensor product expanders and k-designs. In: Approximation, Randomization, and Combinatorial Optimization. Algorithms and Techniques, pp. 548–561. Springer (2009)
28. Håstad, J., Impagliazzo, R., Levin, L.A., Luby, M.: A pseudorandom generator from any one-way function. SIAM Journal on Computing 28(4), 1364–1396 (1999)
29. Hayden, P., Leung, D.W., Winter, A.: Aspects of generic entanglement. Communications in Mathematical Physics 265(1), 95–117 (Jul 2006), https://doi.org/10.1007/s00220-006-1535-6
30. Helstrom, C.W.: Detection theory and quantum mechanics. Information and Control 10(3), 254–291 (1967)
31. Holevo, A.S.: An analogue of statistical decision theory and noncommutative probability theory. Trudy Moskovskogo Matematicheskogo Obshchestva 26, 133–149 (1972)
32. Horodecki, R., Horodecki, P., Horodecki, M., Horodecki, K.: Quantum entanglement. Rev. Mod. Phys. 81, 865–942 (Jun 2009), https://link.aps.org/doi/10.1103/RevModPhys.81.865
33. Impagliazzo, R., Wigderson, A.: P = BPP if E Requires Exponential Circuits: Derandomizing the XOR Lemma. In: Proceedings of the Twenty-ninth Annual ACM Symposium on Theory of Computing. pp. 220–229. STOC '97, ACM, New York, NY, USA (1997), http://doi.acm.org/10.1145/258533.258590

34. Kueng, R., Gross, D.: Qubit stabilizer states are complex projective 3-designs (2015), arXiv:1510.02767
35. Liu, Z.W., Lloyd, S., Zhu, E.Y., Zhu, H.: Entropic scrambling complexities. arXiv:1703.08104 (2017)
36. Low, R.A.: Large deviation bounds for k-designs. Proceedings of the Royal Society of London A: Mathematical, Physical and Engineering Sciences 465(2111), 3289–3308 (2009), http://rspa.royalsocietypublishing.org/content/465/2111/3289
37. Lubkin, E.: Entropy of an n-system from its correlation with ak-reservoir. Journal of Mathematical Physics 19(5), 1028–1031 (1978)
38. Luby, M., Rackoff, C.: How to construct pseudorandom permutations from pseudorandom functions. SIAM Journal on Computing 17(2), 373–386 (1988)
39. Lutomirski, A.: An online attack against wiesner's quantum money (2010), arXiv:1010.0256
40. Lutomirski, A., Aaronson, S., Farhi, E., Gosset, D., Hassidim, A., Kelner, J., Shor, P.: Breaking and making quantum money: toward a new quantum cryptographic protocol. In: Proceedings of the Innovations in Theoretical Computer Science Conference. pp. 20–31. ITCS '10, Tsinghua University Press (2010)
41. Mezher, R., Ghalbouni, J., Dgheim, J., Markham, D.: Efficient quantum pseudorandomness with simple graph states (2017), arXiv:1709.08091
42. Miller, C.A., Shi, Y.: Robust protocols for securely expanding randomness and distributing keys using untrusted quantum devices. Journal of the ACM (JACM) 63(4), 33 (2016)
43. Mosca, M., Stebila, D.: Quantum coins. In: Bruen, A.A., Wehlau, D.L. (eds.) Error-Correcting Codes, Finite Geometries and Cryptography. Contemporary Mathematics, vol. 523, pp. 35–47. American Mathematical Society (2010), http://www.ams.org/bookstore?fn=20&arg1=conmseries&ikey=CONM-523
44. Nakata, Y., Hirche, C., Koashi, M., Winter, A.: Efficient quantum pseudorandomness with nearly time-independent hamiltonian dynamics. Phys. Rev. X 7, 021006 (Apr 2017), https://link.aps.org/doi/10.1103/PhysRevX.7.021006
45. Nakata, Y., Hirche, C., Morgan, C., Winter, A.: Unitary 2-designs from random x- and z-diagonal unitaries. Journal of Mathematical Physics 58(5), 052203 (2017), https://doi.org/10.1063/1.4983266
46. Nakata, Y., Koashi, M., Murao, M.: Generating a state t -design by diagonal quantum circuits. New Journal of Physics 16(5), 053043 (2014), http://stacks.iop.org/1367-2630/16/i=5/a=053043
47. Naor, M., Reingold, O.: Synthesizers and their application to the parallel construction of pseudo-random functions. J. Comput. Syst. Sci. 58(2), 336–375 (Apr 1999), http://dx.doi.org/10.1006/jcss.1998.1618
48. Nisan, N., Wigderson, A.: Hardness vs randomness. J. Comput. Syst. Sci. 49(2), 149–167 (Oct 1994), http://dx.doi.org/10.1016/S0022-0000(05)80043-1
49. Ortigoso, J.: Twelve years before the quantum no-cloning theorem. arXiv:1707.06910 (2017)
50. Page, D.N.: Average entropy of a subsystem. Phys. Rev. Lett. 71, 1291–1294 (Aug 1993), https://link.aps.org/doi/10.1103/PhysRevLett.71.1291
51. Park, J.L.: The concept of transition in quantum mechanics. Found. Phys. 1, 23–33 (1970)
52. Popescu, S., Short, A.J., Winter, A.: Entanglement and the foundations of statistical mechanics. Nature Physics 2(11), 754 (2006)
53. Regev, O.: On lattices, learning with errors, random linear codes, and cryptography. Journal of the ACM (JACM) 56(6), 34 (2009)

54. Rompel, J.: One-way functions are necessary and sufficient for secure signatures. In: Proceedings of the twenty-second annual ACM symposium on Theory of computing. pp. 387–394. ACM (1990)
55. Sánchez-Ruiz, J.: Simple proof of page's conjecture on the average entropy of a subsystem. Phys. Rev. E 52, 5653–5655 (Nov 1995), https://link.aps.org/doi/10.1103/PhysRevE.52.5653
56. Sen, S.: Average entropy of a quantum subsystem. Phys. Rev. Lett. 77, 1–3 (Jul 1996), https://link.aps.org/doi/10.1103/PhysRevLett.77.1
57. Shamir, A.: On the generation of cryptographically strong pseudorandom sequences. ACM Trans. Comput. Syst. 1(1), 38–44 (Feb 1983), http://doi.acm.org/10.1145/357353.357357
58. Song, F.: Quantum-secure pseudorandom permutations (June, 2017), blog post, available at http://qcc.fangsong.info/2017-06-quantumprp/
59. Watrous, J.: The theory of quantum information. To be published by Cambridge University Press (2018), a draft copy is available at https://cs.uwaterloo.ca/~watrous/TQI/
60. Webb, Z.: The clifford group forms a unitary 3-design. Quantum Information & Computation 16(15&16), 1379–1400 (2016), http://www.rintonpress.com/xxqic16/qic-16-1516/1379-1400.pdf
61. Werner, R.F.: Optimal cloning of pure states. Phys. Rev. A 58, 1827–1832 (Sep 1998), https://link.aps.org/doi/10.1103/PhysRevA.58.1827
62. Wiesner, S.: Conjugate Coding. SIGACT News 15(1), 78–88 (1983), original manuscript written circa 1970
63. Wootters, W.K., Zurek, W.H.: A single quantum cannot be cloned. Nature 299, 802–803 (Oct 1982)
64. Yao, A.C.: Theory and application of trapdoor functions. In: 23rd Annual Symposium on Foundations of Computer Science (SFCS 1982). pp. 80–91 (Nov 1982)
65. Yuen, H.: A quantum lower bound for distinguishing random functions from random permutations. Quantum Information & Computation 14(13-14), 1089–1097 (2014), http://dl.acm.org/citation.cfm?id=2685166
66. Zhandry, M.: How to Construct Quantum Random Functions. In: FOCS 2012. pp. 679–687. IEEE (2012), http://eprint.iacr.org/2012/182
67. Zhandry, M.: A Note on the Quantum Collision and Set Equality Problems. Quantum Information and Computation 15(7 & 8) (2015), http://arxiv.org/abs/1312.1027
68. Zhandry, M.: A Note on Quantum-Secure PRPs (2016), available at https://eprint.iacr.org/2016/1076
69. Zhandry, M.: Quantum lightning never strikes the same state twice (2017), iACR eprint 2017/1080
70. Zhu, H.: Multiqubit clifford groups are unitary 3-designs (2015), arXiv:1510.02619