Pseudorandom States, No-Cloning Theorems and Quantum Money

Zhengfeng Ji (UTS:QSI)

QCrypt 2018, Shanghai

A Joint Work With

Yi-Kai Liu
(NIST and UMD)

Fang Song
(PSU -> TAMU)

Pseudorandomness

One of the foundations of modern cryptography

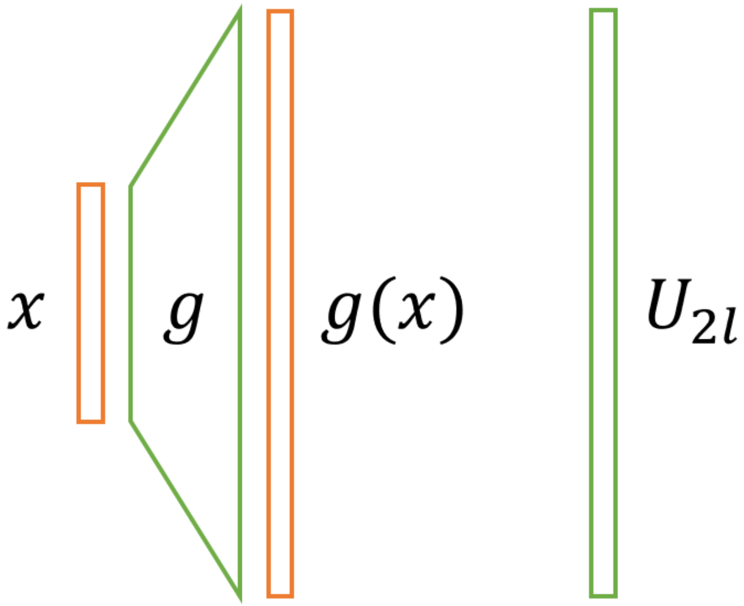
Pseudorandomness in Modern Cryptography

- Pseudorandom objects look random to computationally bounded adversaries
- Computational indistinguishability
- Pseudorandom generators (PRGs)

$$g : \{0,1\}^l \to \{0,1\}^{2l}$$

- PRGs exist if one-way functions (OWFs) exist

[Håstad, Impagliazzo, Levin, and Luby 1999]



Pseudorandom Functions and Permutations

- A random function $f : \mathcal{X} \rightarrow \mathcal{Y}$ assigns a random value from the range $\mathcal{Y}$ to each input from domain $\mathcal{X}$.
- Pseudorandom functions (PRFs)

> A function $\mathsf{PRF} : \mathcal{K} \times \mathcal{X} \rightarrow \mathcal{Y}$ is pseudorandom if for any polynomial-time randomized algorithm $\mathcal{A}$
>
> $$\left| \Pr_{k \leftarrow \mathcal{K}} \left[\mathcal{A}^{\mathsf{PRF}_k}(1^\kappa) = 1 \right] - \Pr_{f \leftarrow \mathcal{Y}^{\mathcal{X}}} \left[\mathcal{A}^{f}(1^\kappa) = 1 \right] \right| = \mathrm{negl}(\kappa).$$

- Pseudorandom permutations (PRPs)
- Stream ciphers, block ciphers, message authentication, …

Pseudorandomness in the Quantum Era

- True randomness from quantum mechanics

  Prepare state $|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$ and measure in the computational basis

  Device-independent randomness expansion and amplification

  Why do we need to care about pseudorandomness in quantum computing?

- The problem of efficiency

  The number of random functions with n-bit input/output is 2^{n2^n} and we need exponentially many bits simply to specify a truly random function

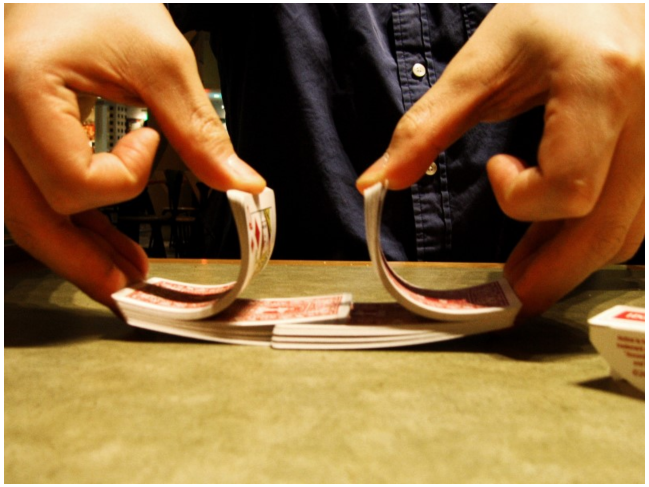
  Similar argument applies to the space of quantum states of n qubits

- Pseudorandomness is not a weaker form randomness; it is a different variant of randomness, a combinatorial construction

Pseudorandomness Against Quantum Attacks

- Stronger assumption: quantum OWFs, functions that are easy to compute classically, but hard to invert even quantumly
- Security proofs
  - Quantum-secure PRGs exist assuming quantum OWFs
  - Quantum-secure PRFs exist assuming quantum OWFs

[Zhandry 2012]



  - Quantum-secure PRPs exist assuming quantum OWFs

[Zhandry 2016], [Song 2017, Blog post at http://qcc.fangsong.info/2017-06-quantumprp/]

Pseudorandom Quantum Objects

From classical objects to quantum objects

Pseudorandom Quantum States (PRS's)

- Truly random quantum states and Haar measure on state space
- How to define PRS?

  A family of states $\{|\phi\rangle_k\}_{k\in\mathcal{K}}$ is pseudorandom if it is computationally indistinguishable from the maximally mixed state?

  [Chen, Chung, Lai, Vadhan and Wu 2017]

- Missing properties: no-cloning, entanglement, …

  How about the random bit strings?

$$\frac{1}{N}\sum_{x\in\{0,1\}^n}|x\rangle\langle x| = \frac{I}{N}$$

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 an efficient quantum algorithm G such that for all $k \in \mathcal{K}$, $G(k) = |\phi_k\rangle$.
2. (Pseudorandomness). For any efficient quantum algorithm $\mathcal{A}$ and any number of copies $m \in \mathrm{poly}(\kappa)$,

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

is negligible.

The number of copies matters quantumly.

Constructions of PRS’s

PRS's from quantum-secure PRFs or PRPs

Random Phase States

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 functions of the security parameter κ. Let $\omega_N = \exp(2\pi i/N)$ be the N-th root of unity. The family of pseudorandom states of n qubits is defined

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

Properties and Applications

Cryptographic No-cloning Theorem

- Pseudorandom states are not efficiently clonable

Theorem. For any PRS $\{|\phi_k\rangle\}_{k\in\mathcal{K}}, m \in \mathrm{poly}(\kappa), m' > m$, and any polynomial-time quantum algorithm $\mathcal{C}$, the success cloning probability

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

- Basic idea

Haar random states are not clonable. So if pseudorandom states are clonable, one can use this property to distinguish it from the Haar random case by SWAP tests.

Quantum Money

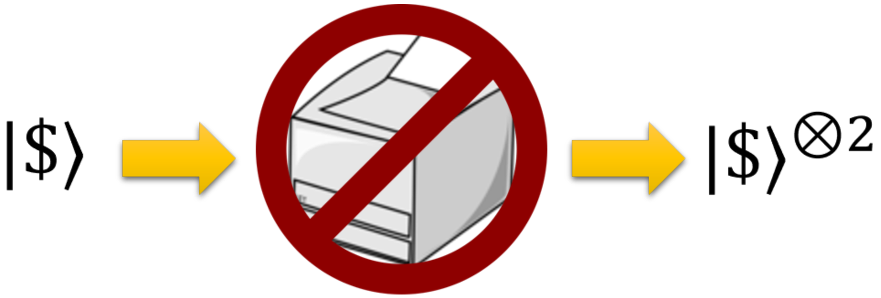
PRS's give rise to quantum money schemes

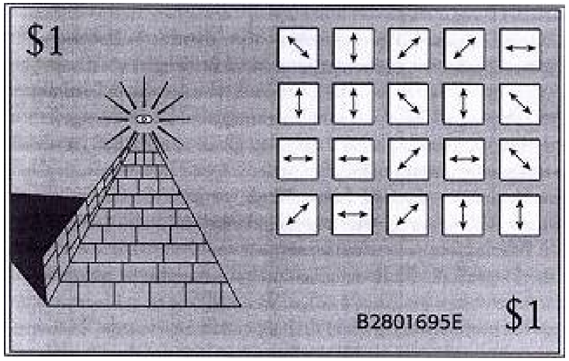
What is Quantum Money

- First proposed by Wiesner that arguably marks the beginning of quantum information

[Wiesner 1969]

- The no-cloning theorem prevents counterfeiting of quantum money





- A money scheme is secure if (1) any valid banknote is accepted with high probability, and (2) any polynomial-time counterfeiter succeeds with negligible probability

Quantum Money from PRS's

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

1. $\mathrm{Bank}(k)$ generates the banknote $|\$\rangle = |\phi_k\rangle$
2. $\mathrm{Ver}(k, \rho)$ applies the projective measurement that accepts ρ with probability $\langle\phi_k|\rho|\phi_k\rangle$

For security proof, we need to strengthen the Cryptographic No-cloning Theorem so that it can handle the oracle call to Ver.

Entanglement in PRS

Let $\{|\phi_k\rangle\}_{k\in\mathcal{K}}$ be a family of PRS with security parameter κ. Consider the partition of the state $|\phi_k\rangle$ into systems A and B each consisting of polynomial number of qubits in the security parameter. We have

1. The expected Schmidt rank of $|\phi_k\rangle \geq \kappa^c$ for all $c > 0$ and sufficiently large κ.
2. The expected entanglement accross the cut A:B is $\mathbb{E}_k E(\phi_k) = \omega(\log \kappa)$.

Conclusions

- The definition of pseudorandom states
- Construction of PRS's
- Cryptographic No-cloning Theorems for PRS's
- Quantum money from PRS's
- Entanglement in PRS
- Open problems
  - How about pseudorandom unitaries?
  - Is quantum-secure OWF necessary?
  - More applications?


Thank You!

Advertisement

Multiple PhD positions available at UTS:QSI

Email: Zhengfeng.Ji@uts.edu.au