Pseudorandom Quantum States

constructions, applications, and open problems

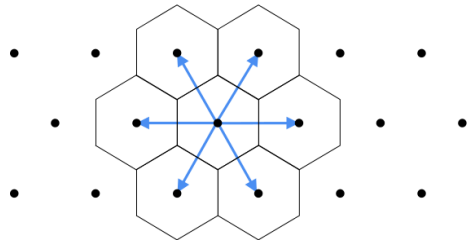
Henry Yuen
Columbia

Cryptography in a quantum world

Post-Quantum Crypto

NIST
National Institute of Standards and Technology

Classical crypto primitives secure against quantum computers



Information-Theoretic Fully Quantum Crypto

BB84 protocol: unconditionally-secure key distribution, using quantum communication.

Device-independent protocols

Computationally-Secure Fully Quantum Crypto

Public-key Quantum Money

Quantum Copy Protection

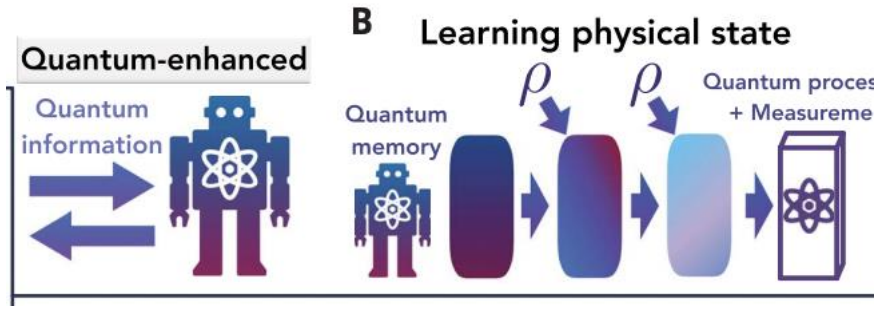
Pseudorandom States/Unitaries

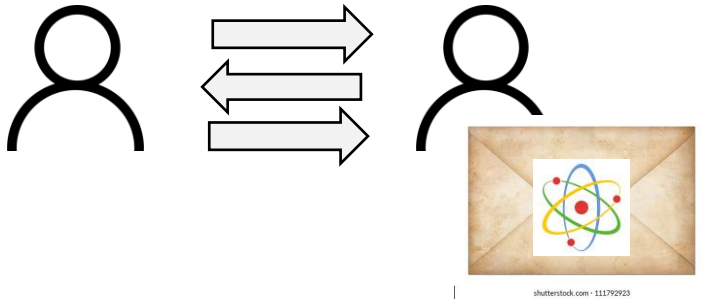
Certified Deletion

Pseudorandom quantum states (PRS)

- Efficiently-computable quantum states that look Haar-random to an outside observer. [Ji, Liu, Song 2018]

- Applications:
  - Quantum cryptography
  - Quantum machine learning
  - Quantum complexity theory
  - Quantum gravity





This tutorial

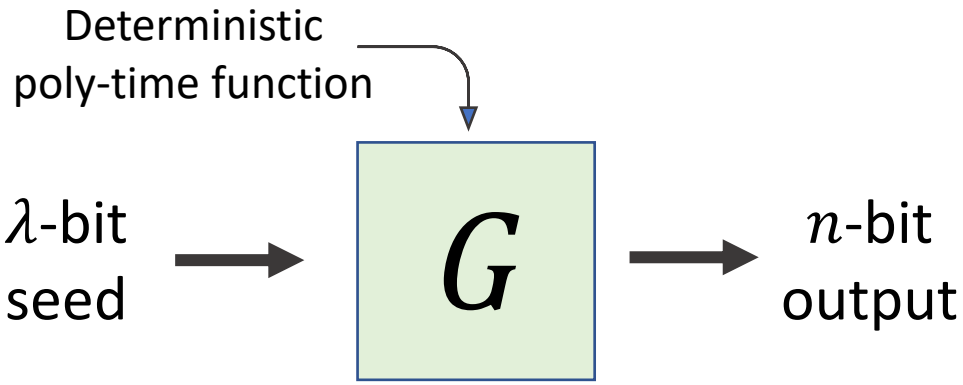
- Definition of pseudorandom states (PRS)
- Constructions
- Properties
- Applications
- Open questions

This tutorial

- Definition of pseudorandom states (PRS)
- Constructions
- Properties
- Applications
- Open questions

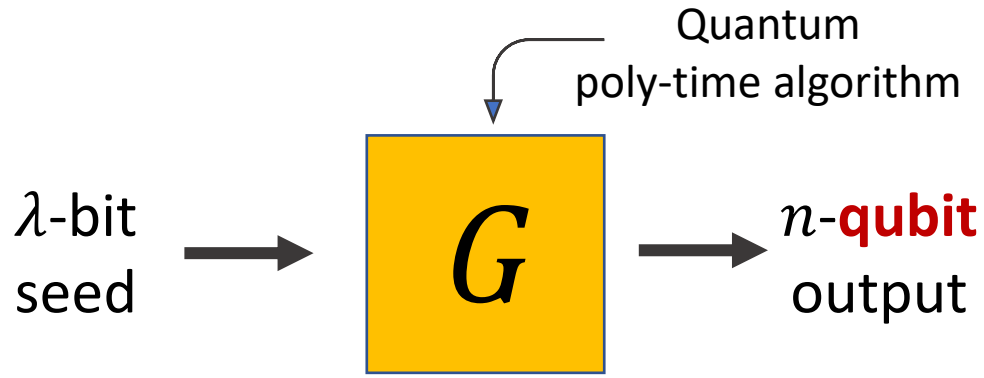
A quantum analogue of pseudorandom generators

Pseudorandom Generator



No poly-time algorithm can distinguish output of G from n uniformly random bits (even though $n > \lambda$).

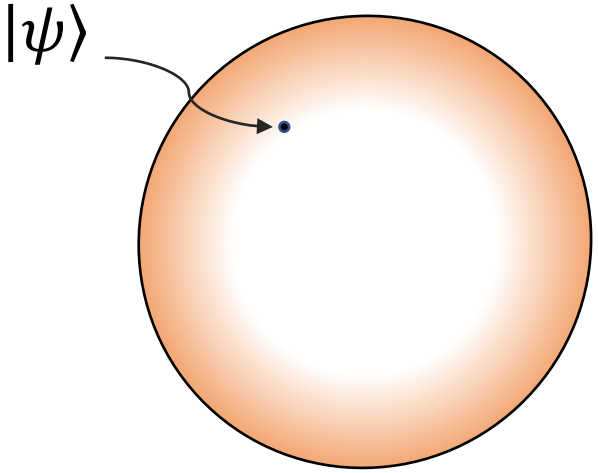
Pseudorandom *State* Generator



No poly-time algorithm can distinguish (copies of) output of G from (copies of) an n-qubit state sampled from the ***Haar distribution***.

Haar-random quantum states

n-qubit (pure) state is unit vector $|\psi\rangle \in \mathbb{C}^{2^n}$.



Intuitively, Haar distribution is **uniform distribution** over quantum states.

A random n-bit string can be sampled efficiently.
A *Haar-random* n-qubit state **cannot**.

Haar distribution is **unitarily invariant**: If $|\psi\rangle$ is Haar-random, then for any n-qubit unitary matrix U so is $U|\psi\rangle$.

Pseudorandom quantum states

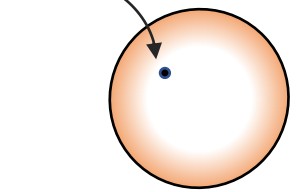
A quantum poly-time algorithm G is a **pseudorandom state (PRS) generator** if

- given key $k \in \{0,1\}^\lambda$, $G(k)$ outputs n-qubit state $|\psi_k\rangle$
- for all t, for all poly(λ)-time algorithms D (called a **distinguisher**),

$|\psi_k\rangle = G(k)$ for random $k \in \{0,1\}^\lambda$

$$D\left(|\psi_k\rangle^{\otimes t}\right) \approx D\left(|\vartheta\rangle^{\otimes t}\right)$$

$|\vartheta\rangle$ is Haar-random



Pseudorandom quantum states

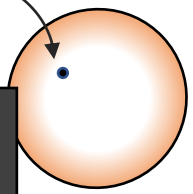
A quantum poly-time algorithm G is a **pseudorandom state (PRS) generator** if

- given key $k \in \{0,1\}^\lambda$, $G(k)$ outputs n-qubit state $|\psi_k\rangle$
- for all t, for all poly(λ)-time algorithms D (called a **distinguisher**),

$|\psi_k\rangle = G(k)$ for random $k \in \{0,1\}^\lambda$

$$D\left(|\psi_k\rangle^{\otimes t}\right) \approx D\left(|\vartheta\rangle^{\otimes t}\right)$$

$|\vartheta\rangle$ is Haar-random



Quantum states cannot be **copied** (no-cloning theorem).
So having $t+1$ copies is **different** from having t copies.

Pseudorandom quantum states

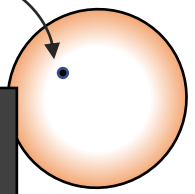
A quantum poly-time algorithm G is a **pseudorandom state (PRS) generator** if

- given key $k \in \{0,1\}^\lambda$, $G(k)$ outputs n-qubit state $|\psi_k\rangle$
- for all t, for all poly(λ)-time algorithms D (called a **distinguisher**),

$$D\left(|\psi_k\rangle^{\otimes t}\right) \approx D\left(|\vartheta\rangle^{\otimes t}\right)$$

$|\psi_k\rangle = G(k)$ for random $k \in \{0,1\}^\lambda$

$|\vartheta\rangle$ is Haar-random



A PRS generator is different from a **state t-design**, where indistinguishability only holds for some *fixed* t.

This tutorial

- Definition of pseudorandom states (PRS)
- Constructions
- Properties
- Applications
- Open questions

Pseudorandom states from pseudorandom functions

Let $\{F_k : \{0,1\}^n \to \{0,1\}\}_k$ be a **(post-quantum) pseudorandom function** (PRF) family.

This means for all poly-time (quantum) distinguishers D

$$D^{F_k} \approx D^H$$

where k is uniformly random and $H : \{0,1\}^n \to \{0,1\}$ is a random function.

Theorem [**Zhandry '12**]: Post-quantum PRFs exist iff post-quantum one-way functions (OWFs) exist.

Pseudorandom states from pseudorandom functions

Fix post-quantum PRF family $\{F_k : \{0,1\}^n \to \{0,1\}\}_k$.

Ji, Liu and Song proposed* the ***binary phase PRS***:

$$|\psi_k\rangle = 2^{-n/2} \sum_{x \in \{0,1\}^n} (-1)^{F_k(x)} \quad |x\rangle$$

Clearly efficiently computable! What about pseudorandomness?

*Binary phase PRS analyzed by [Brakerski, Shmueli '21] [Ananth, Gulati, Qian, Y. '22]

Pseudorandom states from pseudorandom functions

Analysis:

By pseudorandomness of PRF $\{F_k\}_k$, we have

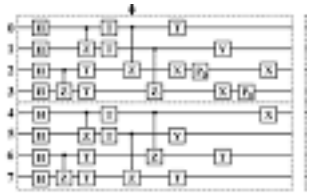
$$|\psi_k\rangle^{\otimes t} \approx_c 2^{-nt/2} \sum_{x_1,\dots,x_t \in \{0,1\}^n} \alpha_{x_1} \cdots \alpha_{x_t} \quad |x_1, \dots, x_t\rangle$$

where for each $x \in \{0,1\}^n$, the constant α_x is a uniformly random ± 1 value, and "$\approx_c$" means "computationally indistinguishable".

Then, show that random binary phase states are **statistically indistinguishable** from Haar-random states.

A candidate PRS generator

The generator G interprets key k as description of quantum circuit C_k, and outputs the state $C_k|0\cdots 0\rangle$.

$k =$  $\rightarrow$ G $\rightarrow$ $C_k|0\cdots 0\rangle$

The output of G is output of a random poly-sized quantum circuit.

It is conjectured in physics and quantum information that random quantum circuits are ***chaotic***, ***structureless***, and ***hard to predict***…(related to quantum supremacy and black holes). Reasonable to conjecture it gives rise to PRS.

This tutorial

- Definition of pseudorandom states (PRS)
- Constructions
- Properties
- Applications
- Open questions

PRS are *computational*

- Given exponential time it is possible to distinguish between PRS and Haar distribution:
  - The span of $|\psi_k\rangle^{\otimes t}$ has dimension 2^λ
  - The span of $|\vartheta\rangle^{\otimes t}$ for all $|\vartheta\rangle$ has dimension $\binom{2^n+t-1}{t}$
  - For sufficiently large $t = poly(n, \lambda)$, $\binom{2^n+t-1}{t} \gg 2^\lambda$

- By measuring the projection onto P, can distinguish between Haar random and output of PRS with high probability.

- Thus we need *some* computational assumptions on the distinguisher!

PRG vs PRS

Pseudorandom Generator

Extremely useful in classical cryptography.

Equivalent to OWFs.

PRG that stretches $\lambda \to \lambda + 1$ bits implies PRG that stretches $\lambda \to n$ bits for any $n = \mathrm{poly}(\lambda)$.

Truncating output of PRG still yields PRG.

Can copy outputs of PRG.

Pseudorandom State Generator

Not obvious how to use PRS for crypto.

PRS do not generically imply OWFs.

Unclear how to stretch output length of PRS generator.

PRS are highly entangled, so cannot be truncated.

Cannot copy PRS.

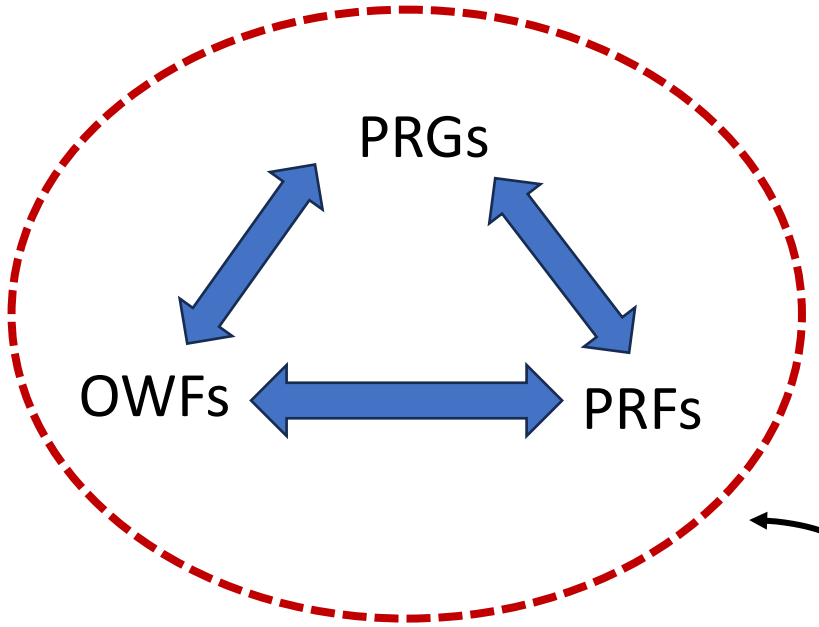
Pseudorandom states are brittle!

This tutorial

- Definition of pseudorandom states (PRS)
- Constructions
- Properties
- Applications
- Open questions

Applications of classical PRGs

Classical crypto 101: PRGs are *equivalent* to many fundamental primitives.



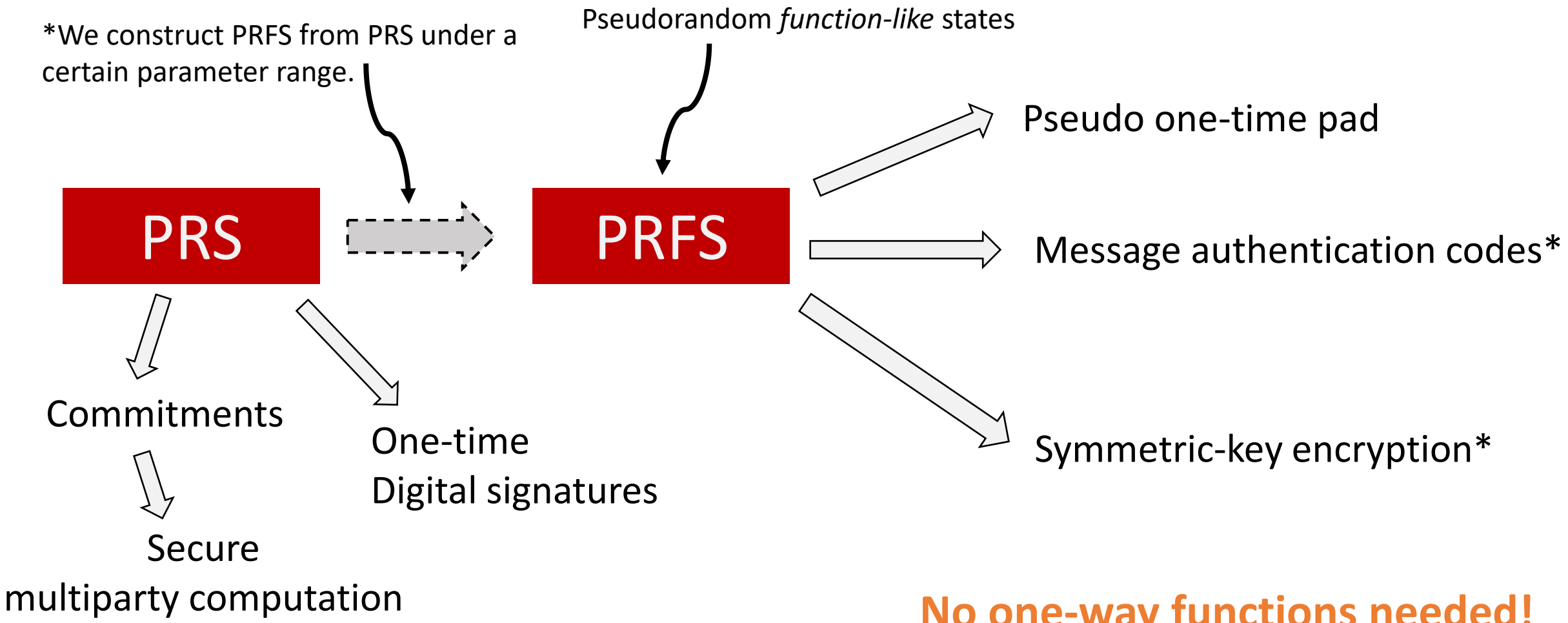
MiniCrypt Primitives:

- Private-key encryption
- Commitments
- Digital signatures
- Zero knowledge proofs

Equivalences hold in *classical world*.

Question: What cryptographic primitives can be constructed ***directly*** from PRS?

Applications of PRS



No one-way functions needed!

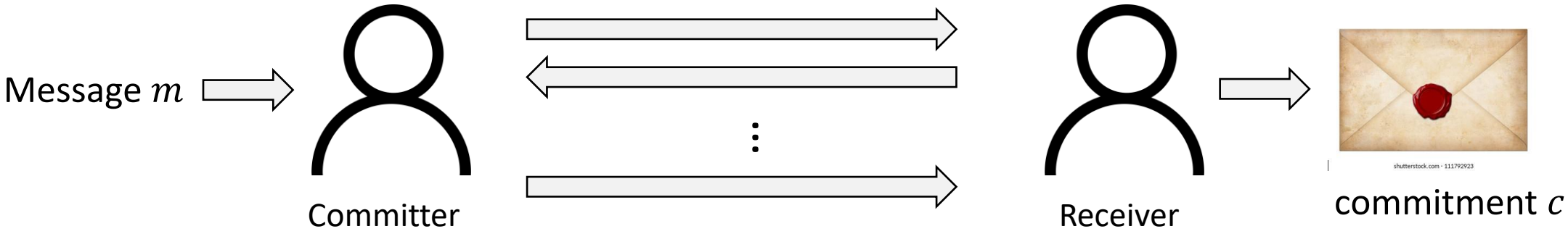
Commitments from PRS

Commitment schemes

Protocol executed between two mistrustful parties (**committer, receiver**).
Cryptographic equivalent of putting a message in sealed envelope that is opened later.

Commitment Phase: committer (having m) interacts with receiver, who obtains a ***commitment*** c.

Hiding Property: The commitment c does not reveal m to receiver.

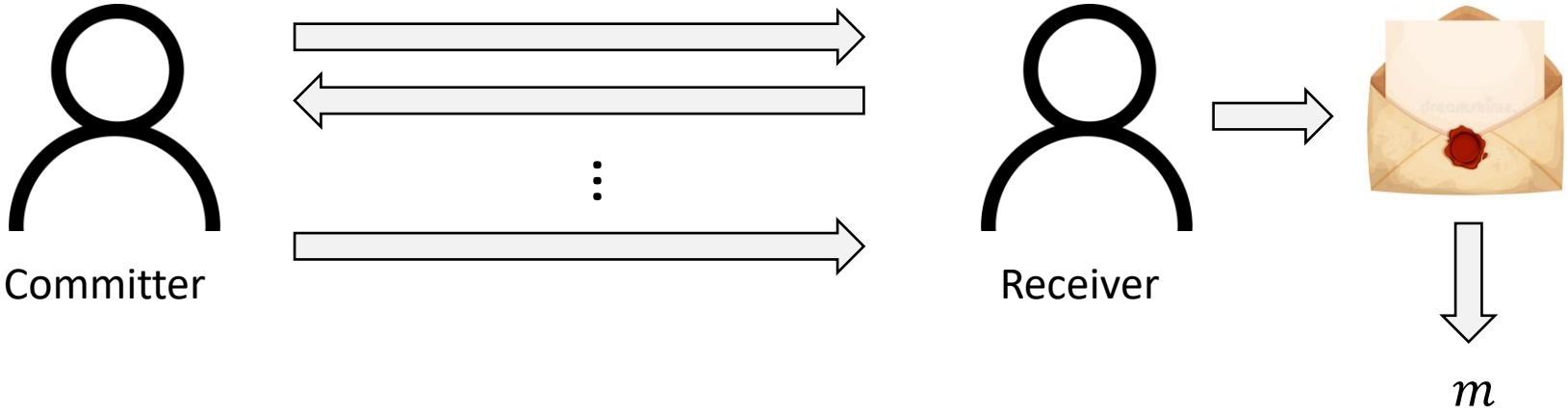


Commitment schemes

Protocol executed between two mistrustful parties (**committer, receiver**).
Cryptographic equivalent of putting a message in sealed envelope that is opened later.

Opening Phase: committer ***opens*** commitment and reveals message m. Receiver rejects if opening is inconsistent with commitment, and accepts otherwise.

Binding Property: The committer cannot open to a different $m' \neq m$ to receiver.



Quantum commitments from PRS

[Morimae, Yamakawa '22] Let $\{|\psi_k\rangle\}_k$ be PRS with output length $\geq 3\lambda$.
Given bit b, committer generates

$$|\phi_b\rangle := \sum_{k,x,z} |k,x,z\rangle_R \otimes P_{x,z}^b \, |\psi_k\rangle_C$$

where k = PRS key, and $P_{x,z}$ = quantum one-time pad with keys $x, z \in \{0,1\}^n$.

Commit(b): committer sends register C to receiver.

Reveal: committer sends remaining register R to receiver, who then checks if global state is $|\phi_0\rangle$ or $|\phi_1\rangle$.

Quantum commitments from PRS

[Morimae, Yamakawa '22] Let $\{|\psi_k\rangle\}_k$ be PRS with output length $\geq 3\lambda$.
Given bit b, committer generates

$$|\phi_b\rangle := \sum_{k,x,z} |k,x,z\rangle_R \otimes P_{x,z}^b \, |\psi_k\rangle_C$$

Receiver can verify the commitment: $|\phi_0\rangle$ is almost orthogonal to $|\phi_1\rangle$. This uses 1-design property of one-time pad.

Computational Hiding property: Receiver cannot efficiently distinguish between $b = 0$ vs $b = 1$. Otherwise could distinguish between $\mathbb{E}|\psi_k\rangle\langle\psi_k|$ and maximally mixed state, which violates pseudorandomness property.

Quantum commitments from PRS

[Morimae, Yamakawa '22] Let $\{|\psi_k\rangle\}_k$ be PRS with output length $\geq 3\lambda$.
Given bit b, committer generates

$$|\phi_b\rangle := \sum_{k,x,z} |k,x,z\rangle_R \otimes P_{x,z}^b \, |\psi_k\rangle_C$$

Statistical binding property: Reduced density matrices of $|\phi_b\rangle$ on register C are far apart. There is no way for the committer to change $|\phi_0\rangle$ to $|\phi_1\rangle$ by acting on R only.

Pseudorandom *function-like* states

Pseudorandom *function-like* states

[Ananth, Qian, Y. '22] introduced **pseudorandom *function-like* states (PRFS).**

Designed to be more flexible and less brittle than PRS.

PRFS is quantum analogue of a **pseudorandom function (PRF)** in classical cryptography -- hence the name *function-like*.

Pseudorandom *function-like* states

A quantum poly-time algorithm G is a **PRFS generator** if

- given **key** $k \in \{0,1\}^\lambda$ and **input** $x \in \{0,1\}^d$, $G(k,x)$ outputs n-qubit state $|\psi_{k,x}\rangle$
- for all t, for all distinct inputs $x_1, \dots, x_s$, for all poly-time distinguishers D

$$D\left(|\psi_1\rangle^{\otimes t}, \dots, |\psi_s\rangle^{\otimes t}\right) \quad \approx \quad D\left(|\vartheta_1\rangle^{\otimes t}, \dots, |\vartheta_s\rangle^{\otimes t}\right)$$

$|\psi_i\rangle$'s sampled by:
- sampling random $k \in \{0,1\}^\lambda$
- setting $|\psi_i\rangle = G(k, x_i)$ for $i = 1, \dots, s$

$|\vartheta_i\rangle$'s sampled by:
- Independently sampling Haar-random $|\vartheta_i\rangle$ for $i = 1, \dots, s$

Important: the distinguisher D is allowed to depend on $x_1, \dots, x_s$!

Pseudorandom *function-like* states

Easy direction: PRFS generators implies the existence of PRS generators.

Constructions: Using OWFs, can build PRFS generators using Ji, Liu, Song's construction.

Not obvious how to construct PRFS using PRS as a black box.

The famous Goldreich-Goldwasser-Micali construction that builds pseudorandom functions (PRF) from PRGs requires **copying** outputs.

GGM seems incompatible with PRS!

PRFS from PRS

Open question: construct PRFS from PRS in a black box way.

Theorem: Let $d = O(\log \lambda)$. Assuming the existence of PRS generators with $(n + d)$-qubit outputs, there exist PRFS generators with d-bit inputs and n-qubit outputs.

Idea: Write $|\psi_k\rangle = \sum \alpha_{k,x} |x\rangle \otimes |\psi_{k,x}\rangle$ and use post-selection.

Corollary: This Theorem is enough to build the PRFS needed for the previous applications (pseudo one-time pad, encryption).

(Private-key)

Encryption from PRFS

Pseudo one-time pad

In 1948 Shannon showed that the one-time pad achieves perfect secrecy. However, it requires a random key as long as the message.

Pseudo one-time pad: use a *pseudorandom* key instead from a PRG.

Can we build pseudo one-time pads from pseudorandom states?

It is not obvious! Let's use PRFS…

Quantum pseudo one-time pad

Suppose we want to encrypt r-bit messages m.

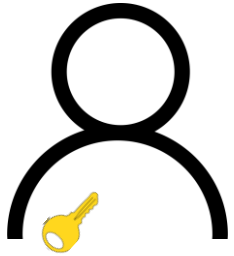
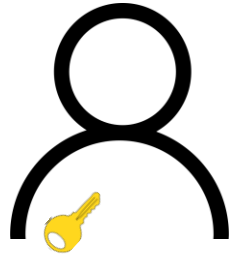
$G(k, x)$: PRFS generator with input (the "x" part) length $O(\log r)$.

Quantum Pseudo One-time Pad

poly-time adversary

Looks completely random to me…

= shared random key $k \in \{0,1\}^\lambda$

$m \in \{0,1\}^r$ ⇒  ⇒ $|\psi_1\rangle, \dots, |\psi_r\rangle$ ⇒  ⇒ m

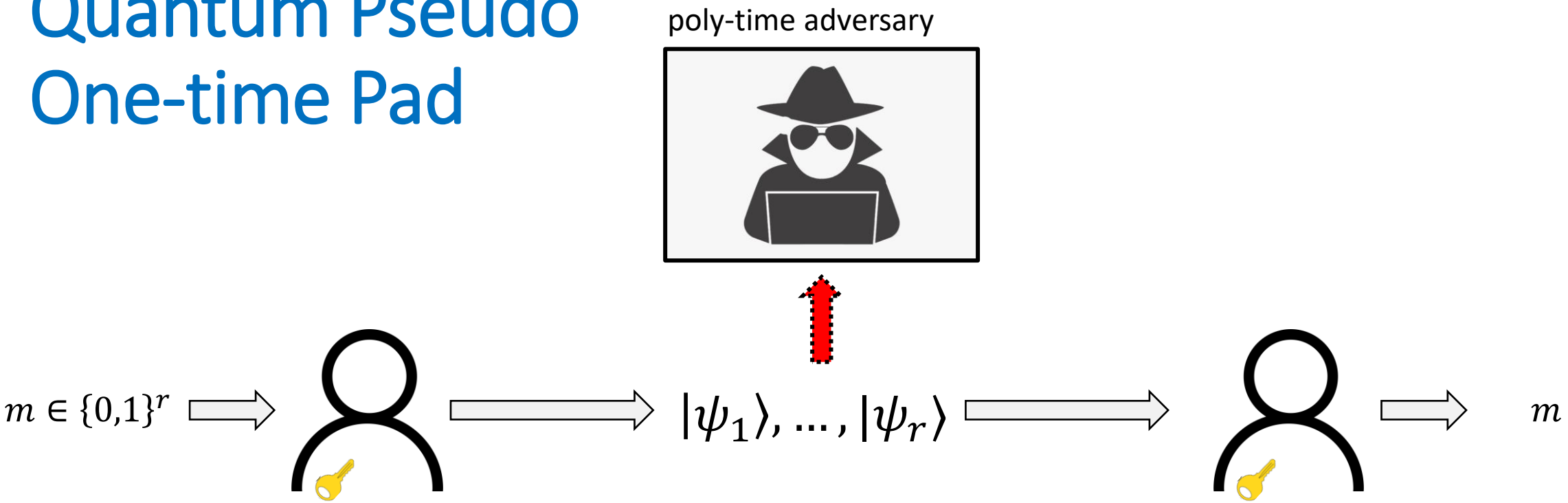
Encoding: Encode i^{th} bit of m as $|\psi_i\rangle = G(k, i \circ m_i)$.

Decoding: Given $|\psi_i\rangle$, test if it equals $G(k, i \circ 0)$. If so, set $m_i = 0$. Otherwise, set $m_i = 1$.

Need to use pseudorandomness of G to argue this works!

G = PRFS generator with $O(\log r)$-bit input

Quantum Pseudo One-time Pad



Theorem: assuming the existence of PRFS generators with $O(\log r)$-bit inputs and $\omega(\log r)$-qubit outputs, there exist secure quantum pseudo one-time pad encryption schemes for r-bit messages.

Other applications of PRS

Other applications of PRS

- **Quantum complexity theory**: PRS can be used to show hardness of fundamental quantum information theory tasks, such as compression of quantum states. [Bostanci, Efron, Metger, Poremba, Qian, Yuen '23]

- **Quantum complexity**: PRS does not imply OWF in a black box way [Kretschmer '21]. In quantum world, OWFs are no longer a ***minimal*** assumption.

- **Quantum crypto**: pseudorandom proofs of destruction [Behera, Brakerski, Sattath, Shmueli '23], quantum public key encryption [Coladangelo '23] [Barooti, Malavolta, Walter '23] [Grilo, Sattath, Vu '23]….

Other applications of PRS

- **Quantum machine learning**: PRS can be used to show hardness of quantum machine learning tasks. [Huang, Broughton, Cotler, et al. ‘23]

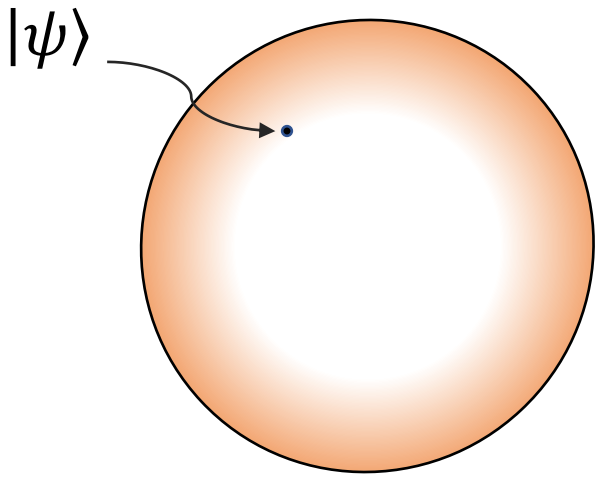
- **Quantum gravity**: Entanglement in PRS can be ”tuned”, leading to “pseudoentanglement”. Has implications for complexity of AdS/CFT correspondence [Bouland, Fefferman, Vazirani ‘22].

- **Quantum pseudorandomness**: PRS inspired a flurry of quantum pseudorandom primitives (EFI, OWSG, pseudorandom unitaries, …)

This tutorial

- Definition of pseudorandom states (PRS)
- Constructions
- Properties
- Applications
- Open questions

Open Questions



1. What can be built directly from PRS in a black box way?
   - PRFS
   - Digital signatures (to sign many messages)
   - Symmetric key encryption (to encrypt many messages)
   - All of cryptomania?

2. Can we separate PRS from some quantum crypto primitives (e.g. quantum money)?

3. What are other candidate constructions of PRS, and can we give evidence for their security?

4. What is the complexity of constructing PRS? Can they be computed by log depth circuits?

5. What are other interesting quantum pseudorandom primitives?

Thank You!