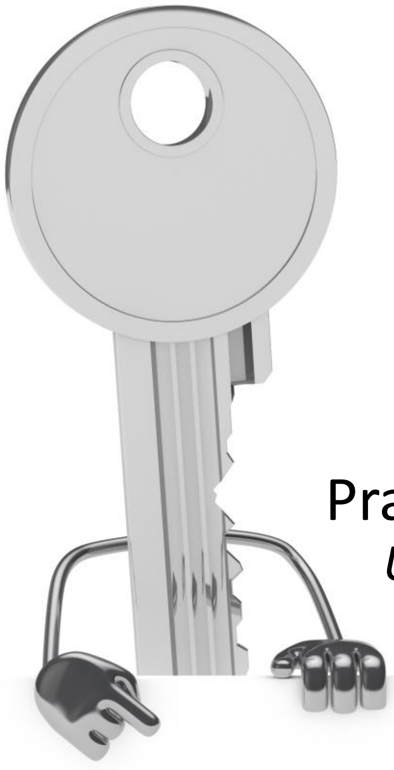
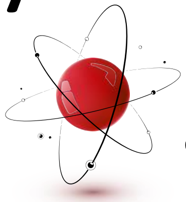


Cryptography from Pseudorandom  States

Prabhanjan Ananth
UC Santa Barbara

Luowen Qian
Boston University

Henry Yuen
Columbia University

ia.cr/2021/1663

Root of classical crypto: one-way functions

- Functions that are easy to compute but hard to invert
- Sufficient for: a lot of crypto (secret-key encryption, signature, commitment, ZK, (weak) coin flipping, pseudorandomness…)
- Necessary for: almost all crypto! (encryption, signature, commitment, *key exchange*, *MPC*, pseudorandomness…)
- Holy grail for theory of crypto: minimize assumptions

One-way functions in a quantum world

Post-quantum crypto: Crypto against quantum adversaries

- Functions that are easy to compute but hard to invert
- Sufficient for: a lot of crypto (secret-key encryption, signature, commitment, ZK, (weak) coin flipping, pseudorandomness…)
- Necessary for: almost all crypto! (encryption, signature, commitment, *key exchange*, *MPC*, pseudorandomness…)
- Holy grail for theory of crypto: minimize assumptions

Power of quantum for crypto

OWFs might not be minimal

- Key exchange unconditionally, aka quantum key distribution [Bennett, Brassard'84]
- MPC from OWF [Bennett, Brassard, Crépeau, Skubiszewska'91; Bartusek, Coladangelo, Khurana, Ma'21; Grilo, Lin, Song, Vaikuntanathan'21]
- "Impossible" crypto: unclonable crypto, position verification, everlasting security… [Wiesner'83; Kent'02; Unruh'12; …]
- (Crypto of quantum tasks: quantum encryption/authentication/MPC, quantum delegation, ZK for QMA…)

One-way functions in a quantum world

Post-quantum crypto:
Crypto against
quantum adversaries

- Functions that are easy to compute but hard to invert

Quantum crypto: Crypto with quantum parties

- Su… ture, commitment, ZK, (weak) coin flipping, pseudorandomness…)
- Necessary for: almost all crypto! (encryption, signature, commitment, *key exchange*, *MPC*, pseudorandomness…)
- Holy grail for theory of crypto: minimize assumptions

Still true?

What are the minimal assumptions for quantum crypto?

Classical vs Quantum Pseudorandomness

One-Way Function

- Pseudorandom Generator (PRG)
  - $G(\{0,1\}^\lambda) \in \{0,1\}^n$
  - Random $\{0,1\}^n, n > \lambda$
- Pseudorandom Functions (PRF)
  - $f_{\{0,1\}^\lambda}$: $\{0,1\}^d \to \{0,1\}^n$
  - Random F: $\{0,1\}^d \to \{0,1\}^n$ (query access)
- Pseudorandom Permutations (PRP)

JLS19

[Ji, Liu, Song'19]

- Pseudorandom States (PRS)
  - $G(\{0,1\}^\lambda) \to n$ qubits
  - Haar random pure state

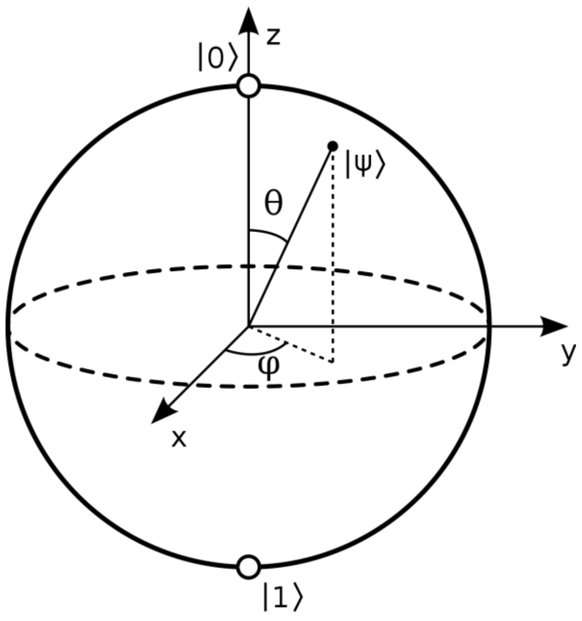
Kretschmer'20: Might be hard

- Pseudorandom Unitaries (PRU)
  - $U_{\{0,1\}^\lambda}$: a unitary
  - Haar random unitary (query access)

?

Quantum states and Haar random states

- Qubit (quantum bit) $|\psi\rangle$: unit vector in $\mathbb{C}^2$
- n qubits $|\psi\rangle$: unit vector in $(\mathbb{C}^2)^{\otimes n} = \mathbb{C}^{2^n}$
- Haar random states:
  the uniform distribution μ over unit sphere of $\mathbb{C}^{2^n} \cong \mathbb{R}^{2 \cdot 2^n}$
  (Requires $\exp(n)$ bits to describe an approximation)
- Unitary invariance: $\forall U: U \cdot \mathrm{Haar} \equiv \mathrm{Haar}$



Pseudorandom States (PRS) [JLS19]

A quantum algorithm G is an n-qubit PRS generator if:

- Efficient generation
  - Takes as input $k \in \{0,1\}^\lambda$
  - Runs in $\mathrm{poly}(\lambda)$ time
  - Outputs a pure state $|\psi_k\rangle\langle\psi_k|$ of $n(\lambda)$ qubits
- Pseudorandomness:
  - $|\psi_k\rangle$ "looks" Haar random even with many copies, i.e.
  - $\forall \mathrm{poly}\ t(\cdot)\ \forall \mathrm{QPT}_\lambda\ A,$

$$\left| \Pr_{k \leftarrow \{0,1\}^\lambda}\left[A\left(|\psi_k\rangle^{\otimes t(\lambda)}\right) = 1\right] - \Pr_{|\phi\rangle \leftarrow \mathrm{Haar}_{n(\lambda)}}\left[A\left(|\phi\rangle^{\otimes t(\lambda)}\right) = 1\right] \right| \leq \mathrm{negl}(\lambda)$$

No cloning

Similar to t-designs but does not fix t

OWF vs PRS

- JLS19: OWF $\rightarrow$ $\omega(\log\lambda)$-qubit PRS
  $\rightarrow$ (private-key query-secure) quantum money
- Kretschmer'20: In a relativized world, $\mathrm{BQP} = \mathrm{QMA}$ but PRS exists (PRS does not imply OWF in a black-box way)
- PRS could be a weaker (quantum) assumption!

What classical crypto task can we achieve just with PRS?

Difficulties of using PRS

(will expand more later)

- Output is highly entangled [JLS19]
- We do not know: [Brakerski, Shmueli'20]

  n-qubit PRS $\rightarrow$ n'-qubit PRS for any nontrivial $n \neq n'$
  - Even shrinking naïvely causes the state to be mixed
- Output might not be expanding $n \leq \lambda$

$\boxed{\text{Our solution: state analogue of PRF}}$

Pseudorandom Function-like States (PRFS)

As useful as PRF
(SKE, MAC, …)

A quantum algorithm G is a PRFS generator if:

- Efficient generation
  - Takes as input $k \in \{0,1\}^\lambda$, $x \in \{0,1\}^d$
  - Runs in $\mathrm{poly}(\lambda)$ time
  - Outputs a state $|\psi_{k,x}\rangle$ of n qubits
- Pseudorandomness
  - $\forall$poly t, $\forall$poly # of (distinct) indices $x_{1\ldots s}$ (known to distinguisher),
    $\left(|\psi_{k,x_1}\rangle \cdots |\psi_{k,x_s}\rangle\right)^{\otimes t}$ for random k is computationally indistinguishable from
    $(|\phi_1\rangle \cdots |\phi_s\rangle)^{\otimes t}$ for n-qubit Haar random states $\{|\phi_i\rangle\}$

Our results

Using PRFS as an intermediate step, we show

1. One-time encryption of messages of any length exists assuming $\omega(\log \lambda)$-qubit PRS
2. Statistically binding commitments exists assuming $2\log\lambda + \omega(\log\log\lambda)$-qubit PRS (Corollary: MPC via [BCKM21])

$\exists O(\log \lambda)$-qubit statistical PRS [BS20]

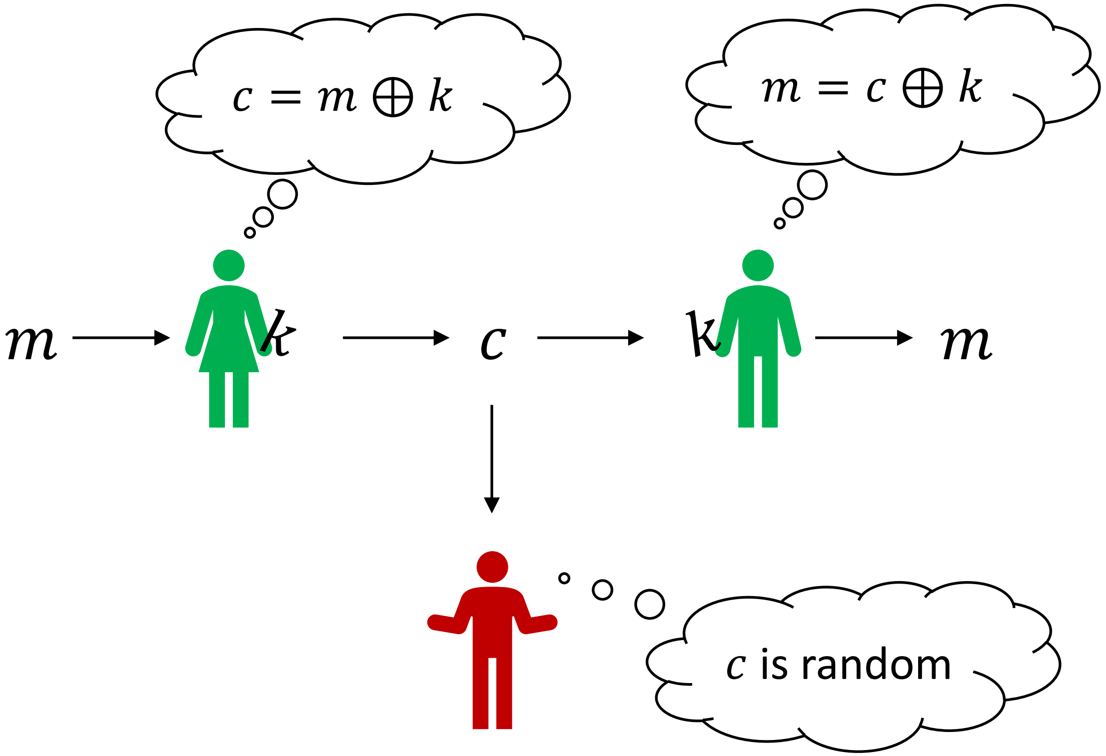
[Morimae, Yamakawa'21]: commitments and one-time signatures assuming $c\lambda$-qubit PRS for $c > 1$

Encryption

From $\omega(\log \lambda)$-qubit PRS

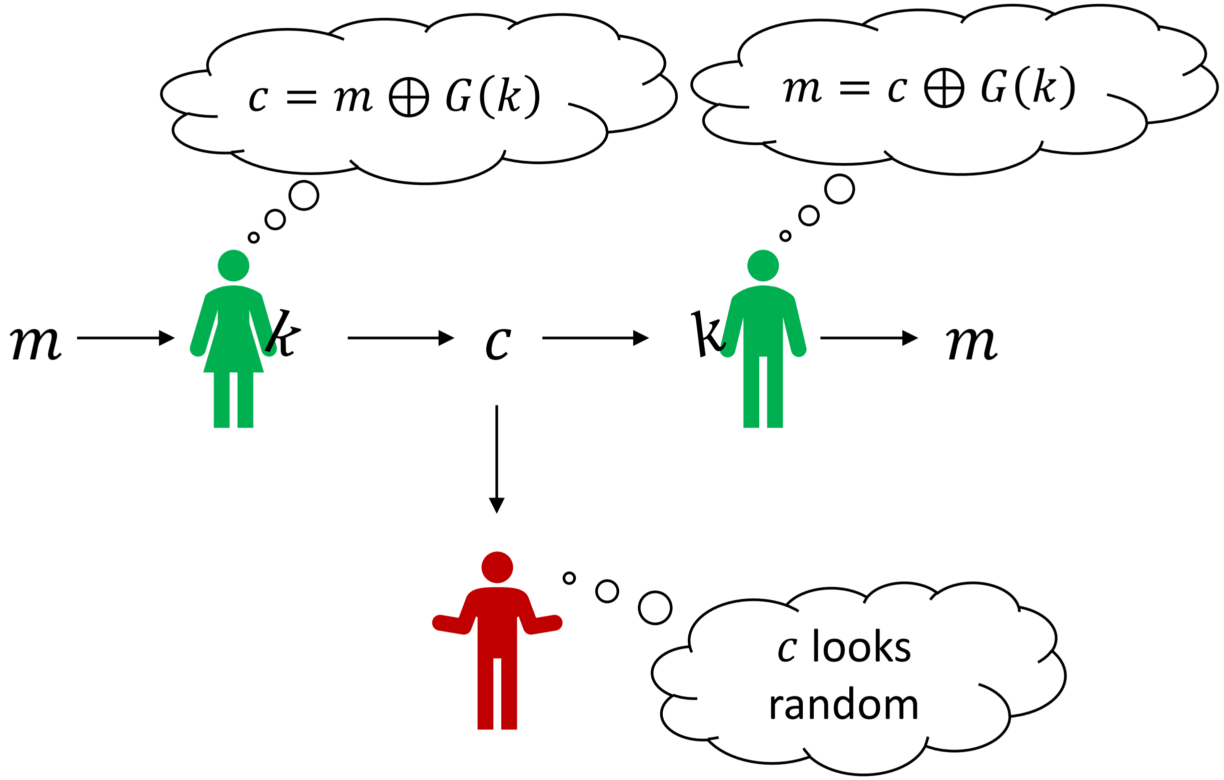
One-Time Pad

$|k| \geq |m|$



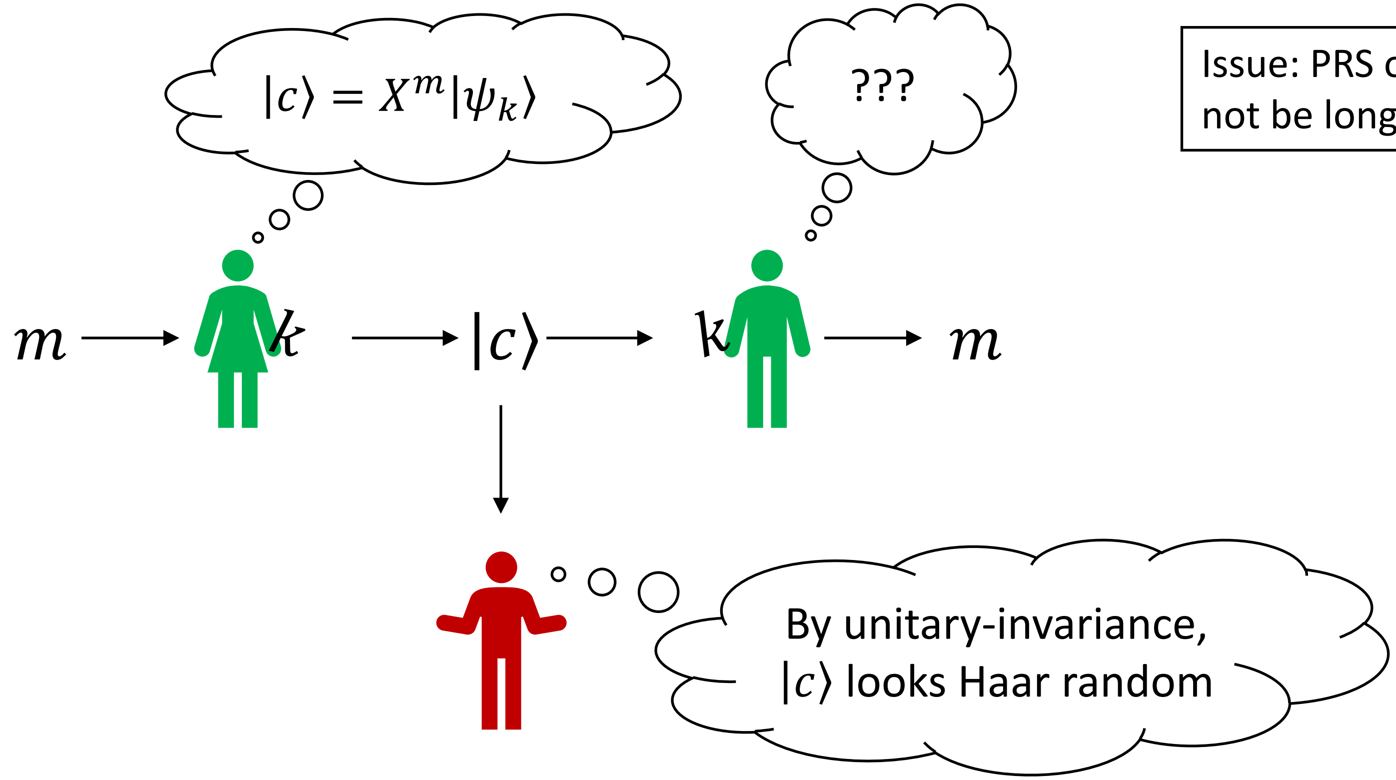
Pseudo OTP from PRG

$G: \{0,1\}^{|k|} \to \{0,1\}^{|m|}$ is a PRG



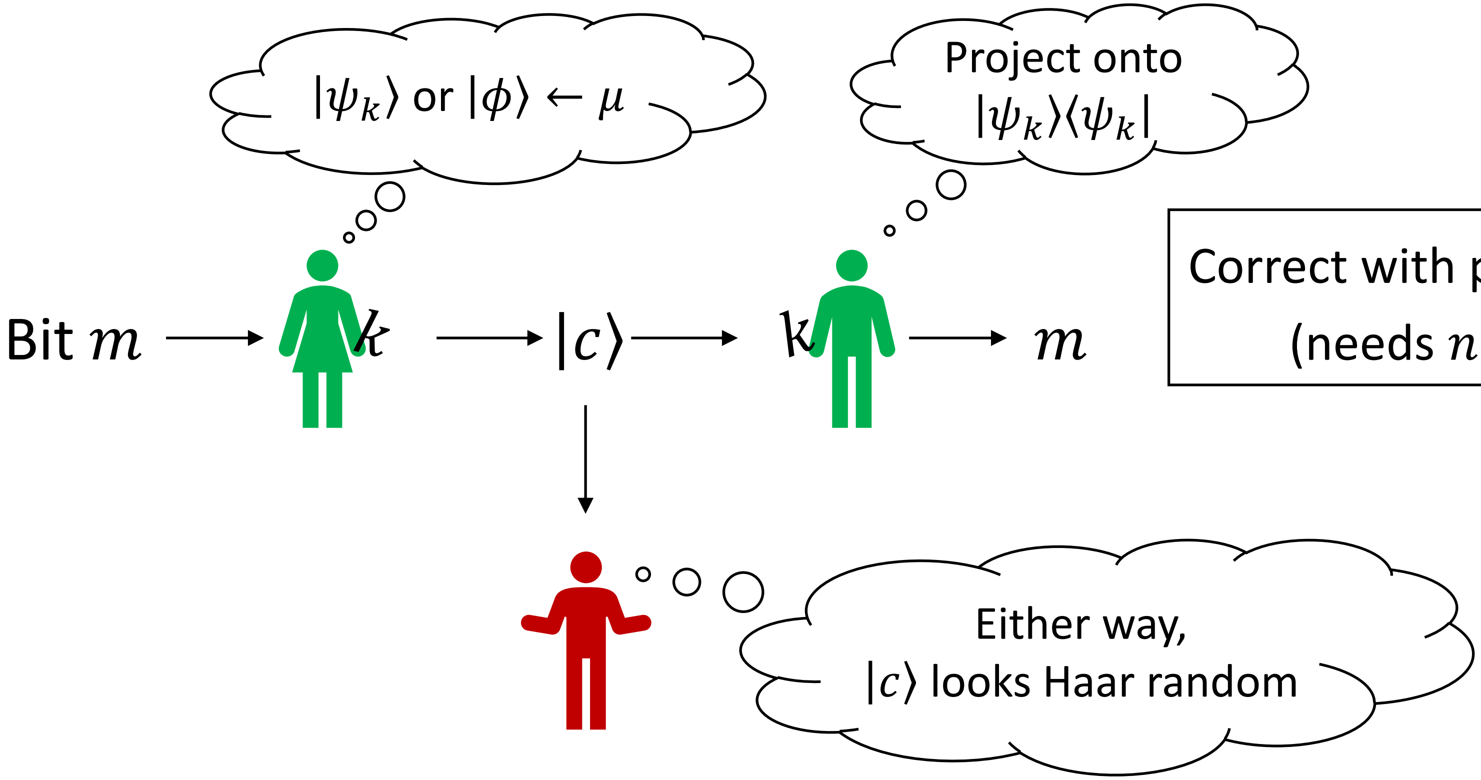
If PRS is like PRG, can we extend this for PRS?

Naïve Pseudo OTP from PRS



Issue: PRS output might not be longer than $|k|$

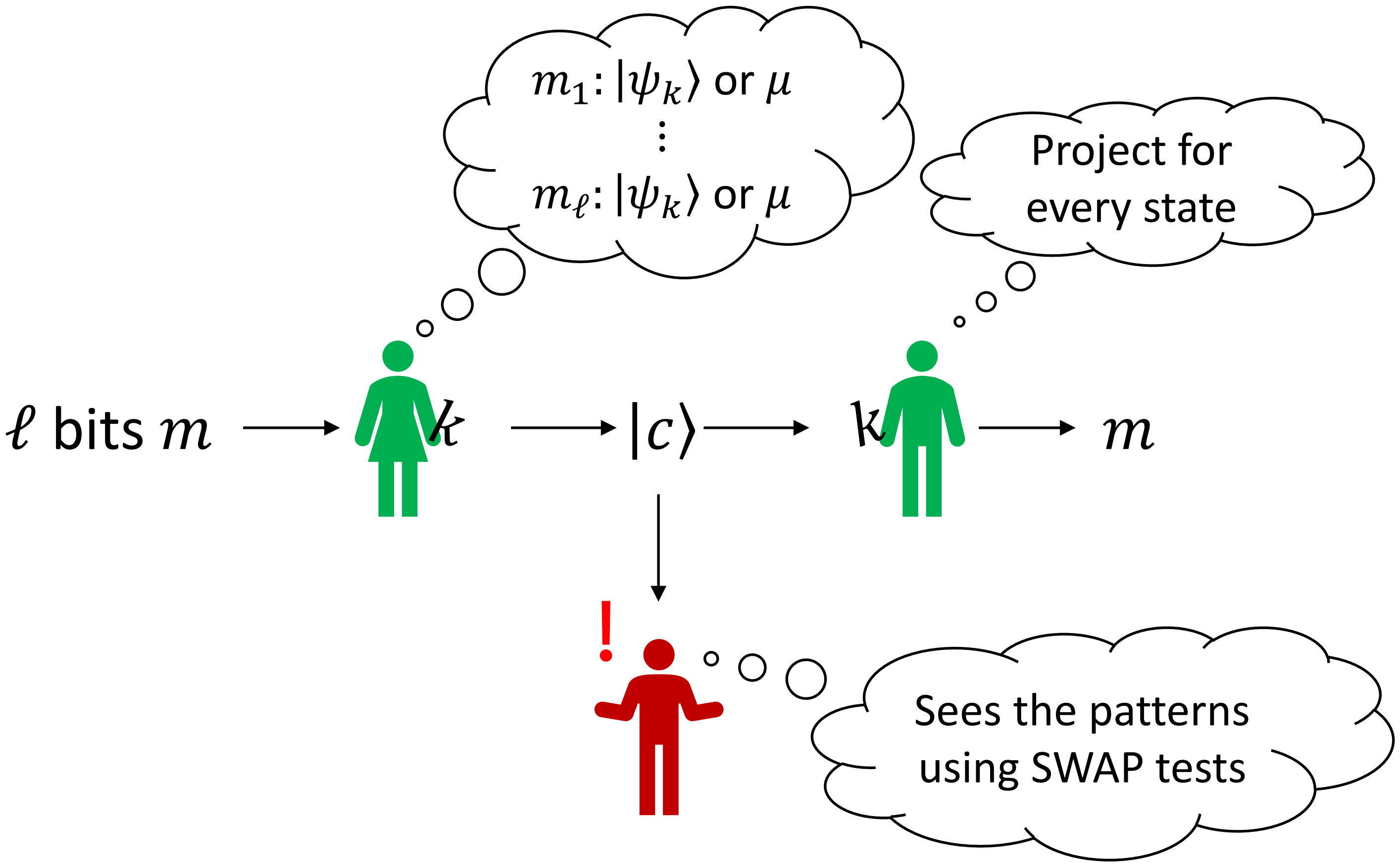
One-time encryption of a single bit



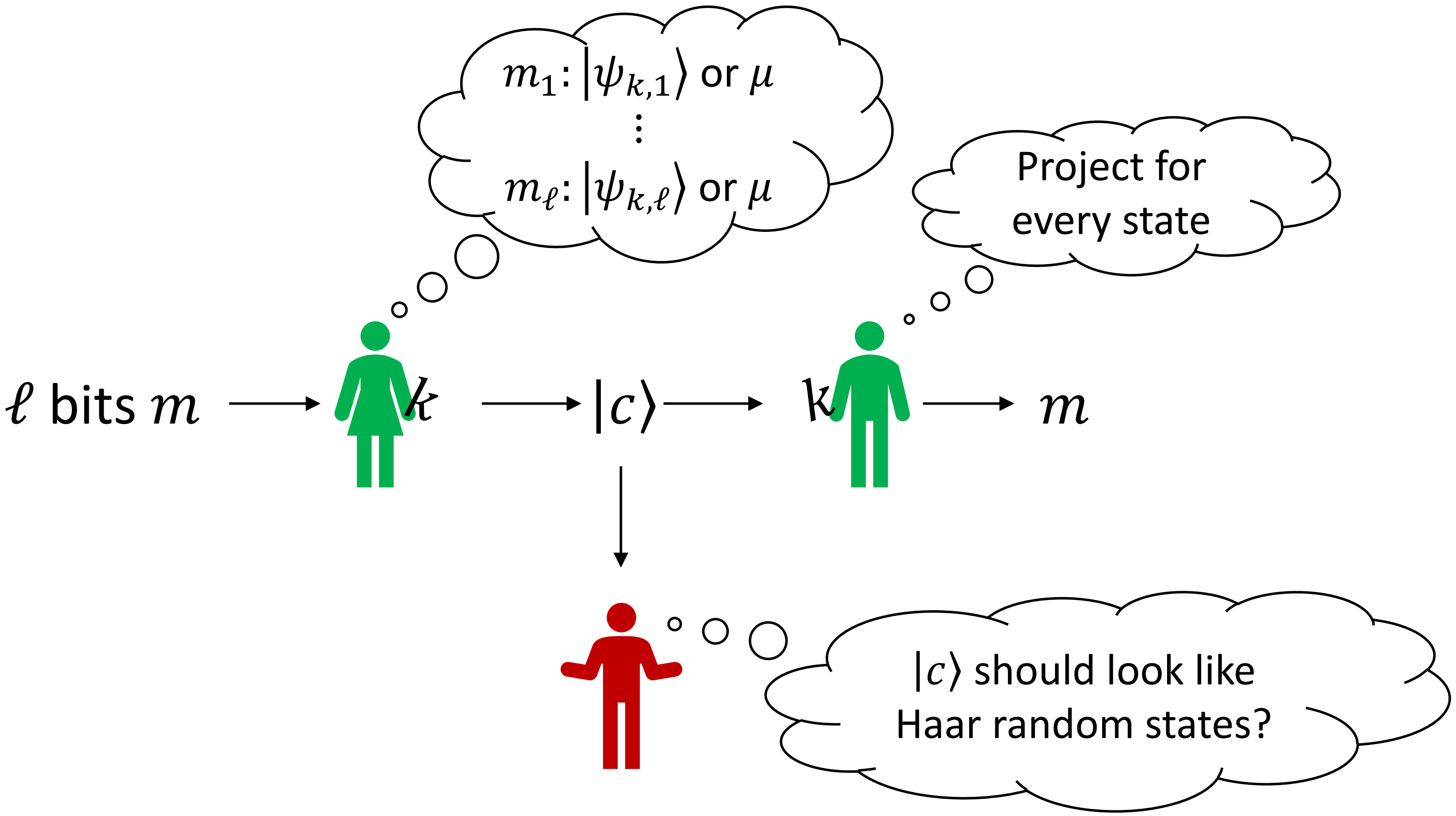
Correct with probability $1 - \frac{1}{2^n}$
(needs $n = \omega(\log \lambda)$)

How to encrypt many bits?

Encrypting many bits via repetition



One-time encryption of many bits

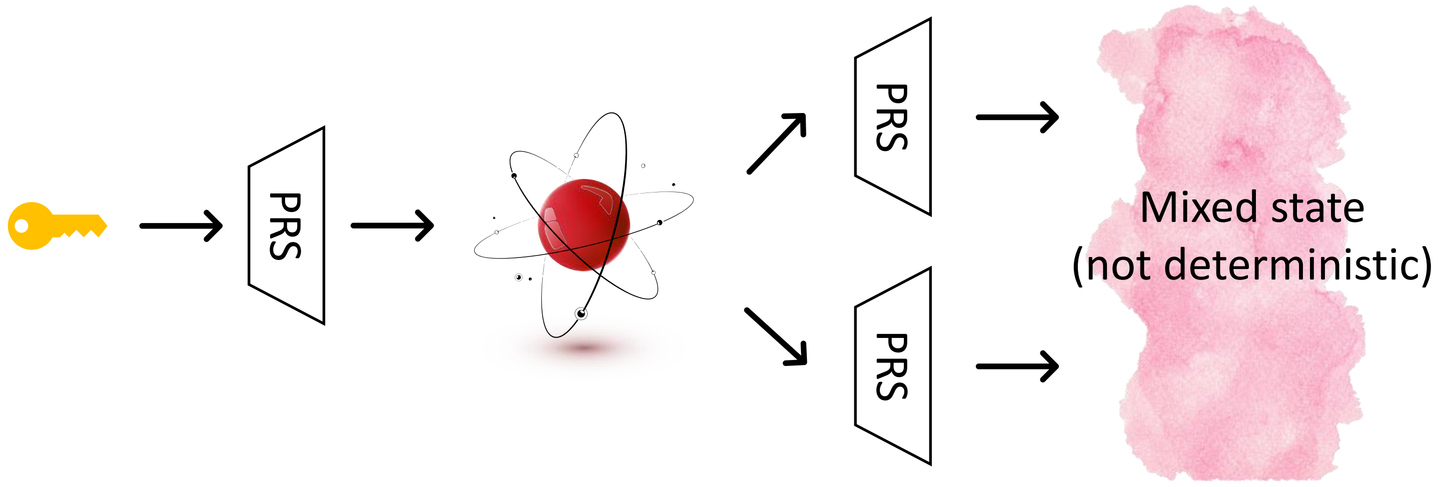


Only need to construct PRFS with input domain $2^d \geq \ell$

Construct PRFS from PRS?

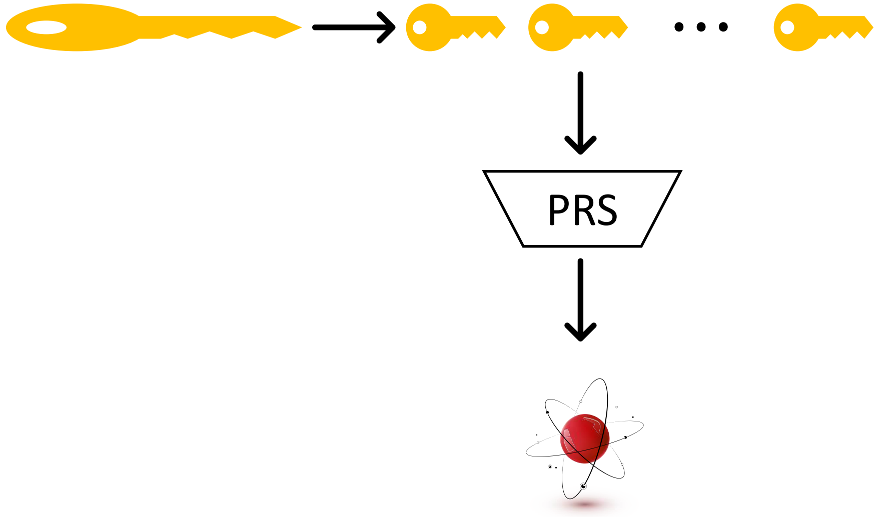
PRFS: $d = O(\log \lambda)$
PRS: $n = \omega(\log \lambda)$

PRFS via GGM [Goldreich, Goldwasser, Micali’84]



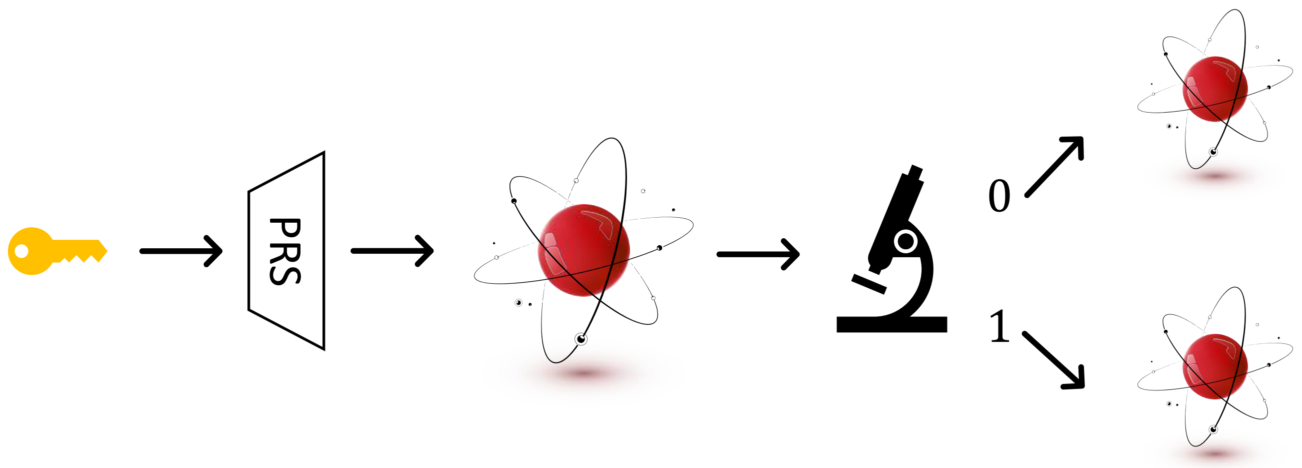
PRFS via splitting key

- Split key $k = k_1||k_2||\cdots||k_\ell$ and invoke PRS on k_i



- Only gives encryption of ℓ bits

PRFS via splitting Haar: post-selection



- Given $|\psi_k\rangle$, measure the first d qubits and conditioned on getting x, output the post-measurement state on the $n-d$ qubits
- Post-selection success probability for Haar is exponentially concentrated around $\frac{1}{2^d}$ → post-selection is efficient if $d = O(\log \lambda)$

Recap: from PRS to one-time encryption

Putting things together: to encrypt message of length $\ell = \lambda^{O(1)}$

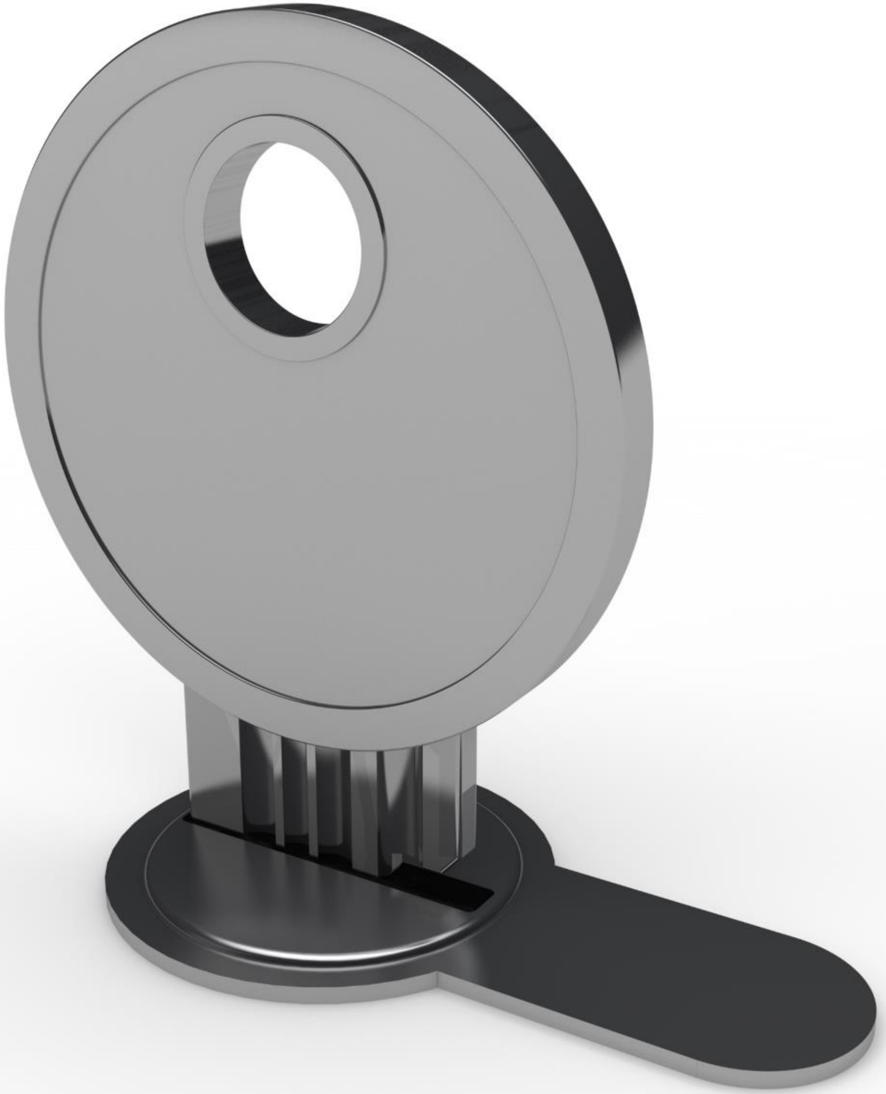
n-qubit PRS with $n = \omega(\log \lambda)$-qubit output

$\rightarrow$ PRFS with $\log \ell = O(\log \lambda)$-bit input domain
and $n - \log \ell = \omega(\log \lambda)$-qubit output

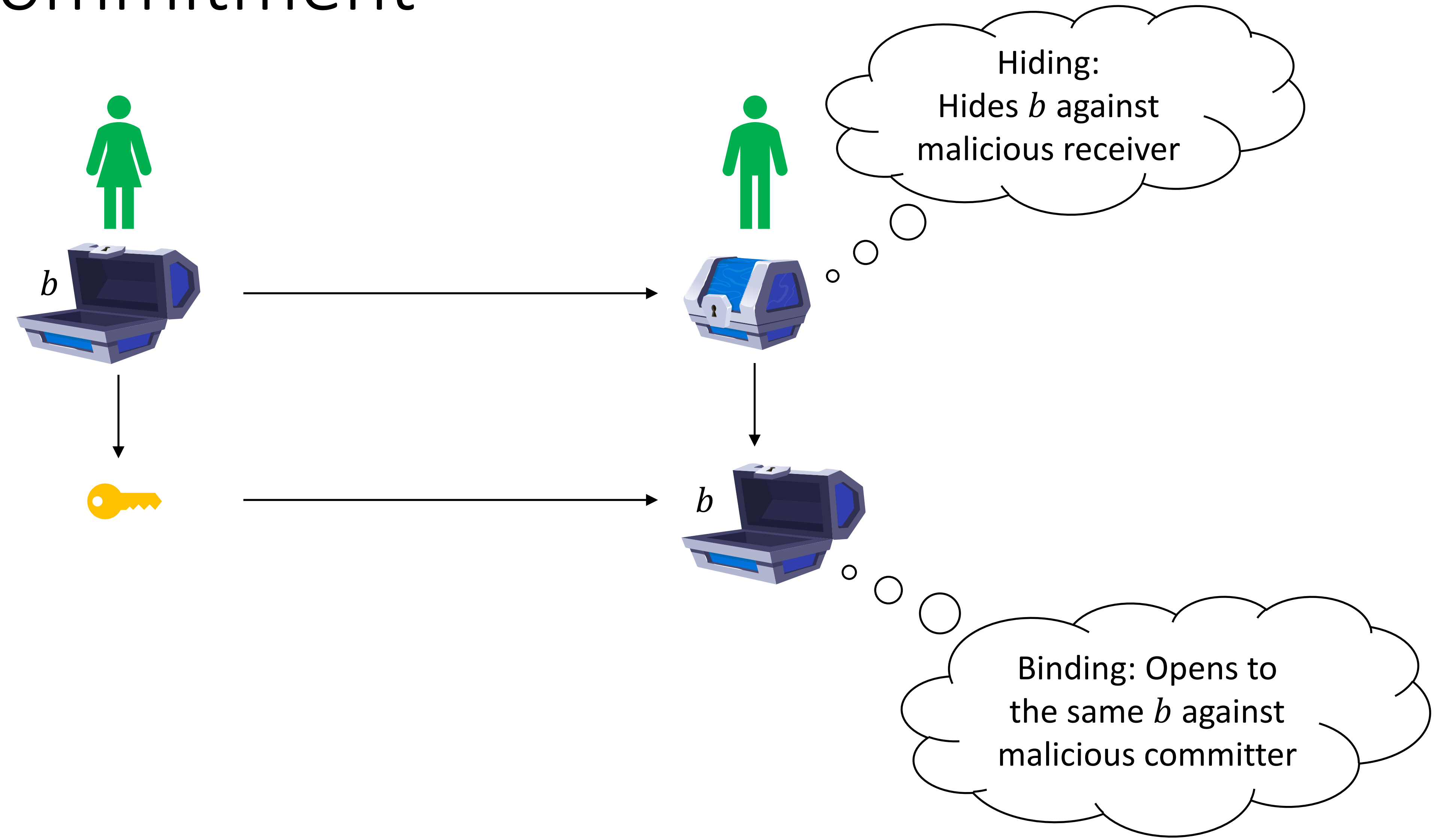
$\rightarrow$ ℓ-bit encryption

Commitment

From $\omega(\log \lambda)$-qubit PRS

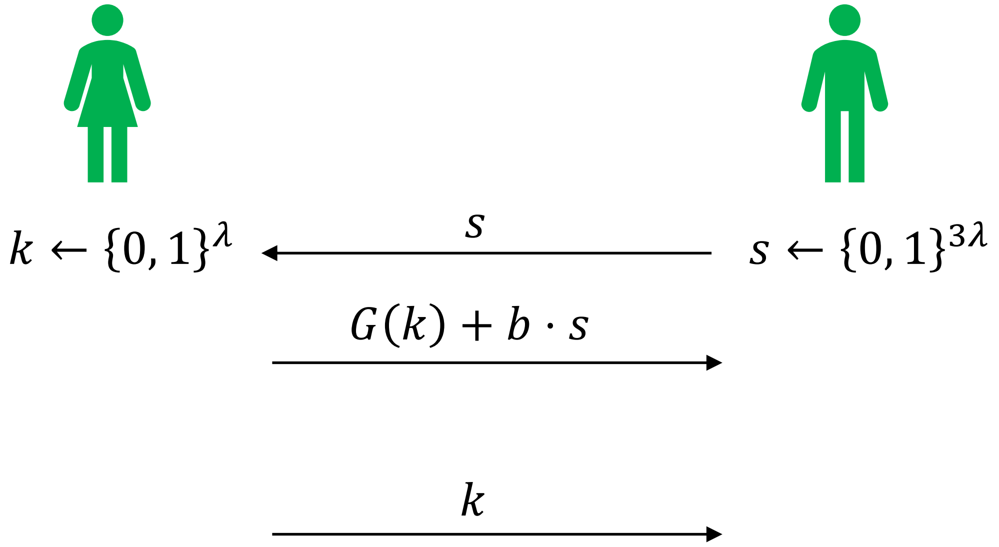


Bit commitment



Naor commitment from PRG [Naor’91]

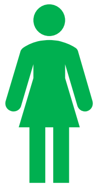
G is a PRG mapping λ bits to 3λ bits

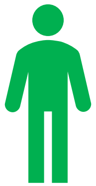


- Hiding: $G(k) + b \cdot s$ looks random as $G(k)$ looks random
- Binding: b is uniquely determined with high probability over s

Naor commitment from PRS

G is a PRS mapping λ bits to 3λ qubits





$k \leftarrow \{0,1\}^{\lambda}$ $\xleftarrow{\quad P \quad}$ $P \leftarrow \{0,1\}^{6\lambda}$ (interpret as a Pauli)

$\xrightarrow{\quad P^b|\psi_k\rangle \quad}$

$\xrightarrow{\quad k \quad}$

Only need the distribution to be Pauli invariant

- Hiding: $P^b|\psi_k\rangle$ looks Haar random as Haar random is unitary invariant

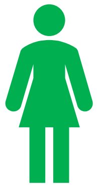
Pauli invariant distributions:

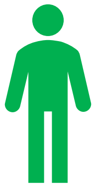
- Haar random states (special case of unitary-invariant)
- A string of Haar random qubits
- A string of Haar random states → PRFS

MY21: can be made non-interactive generically

Naor commitment from PRFS

G is a PRFS with $2^d \cdot n \geq 7\lambda$





$k \leftarrow \{0,1\}^\lambda$ $\xleftarrow{\quad P \quad}$ $P \leftarrow \{0,1\}^{7\lambda}$ (interpret as a Pauli)

$\xrightarrow{P^b\left(|\psi_{k,1}\rangle \cdots |\psi_{k,2^d}\rangle\right)}$

$\xrightarrow{\quad k \quad}$

- Hiding: commitment looks like 2^d many Haar random states
- Binding: b is "uniquely determined" with high probability over P

Recap: from PRS to MPC

Putting things together:

n-qubit PRS with $n = \omega(\log \lambda)$-qubit output

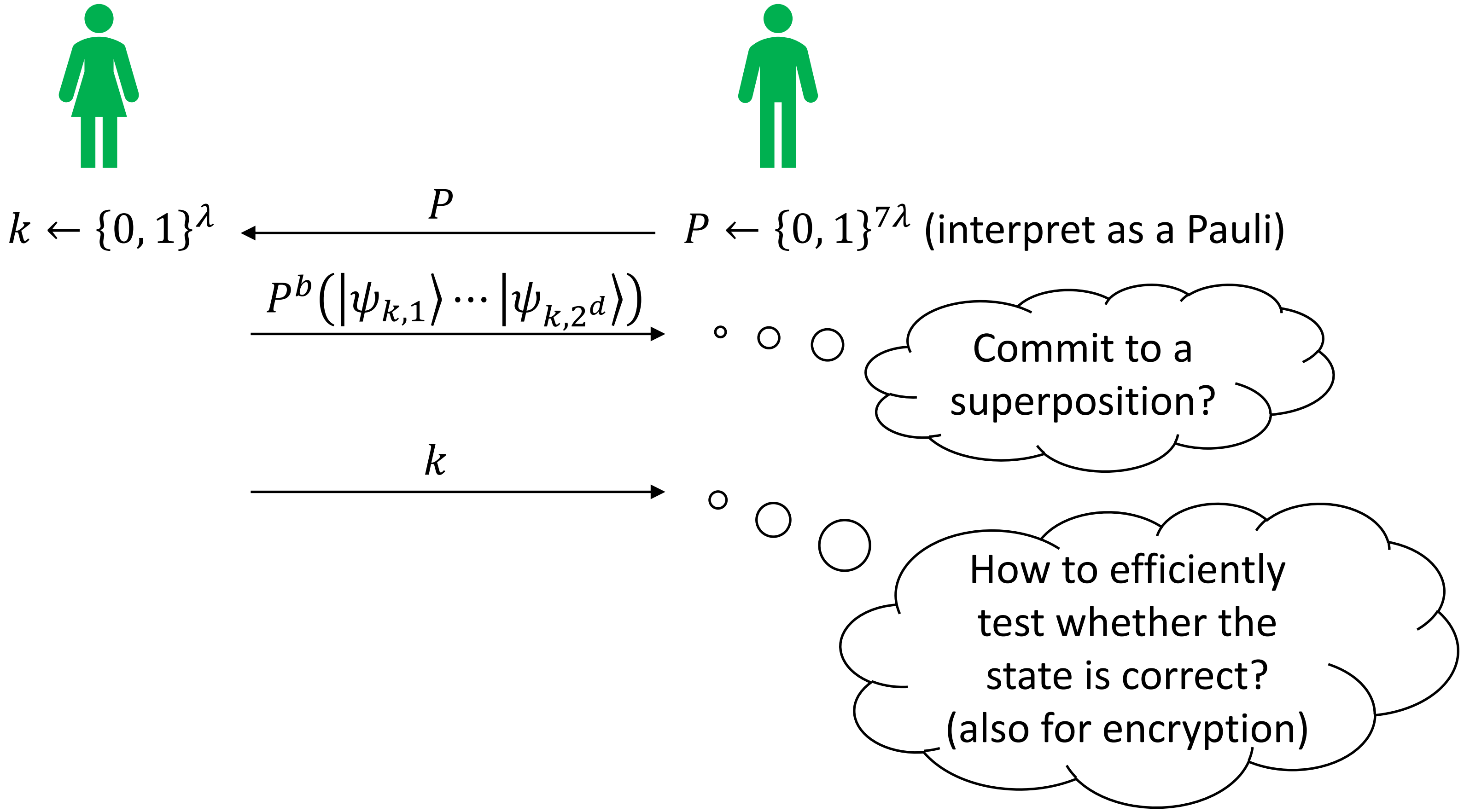
$\rightarrow$ PRFS with $\log \lambda$-bit input domain
and $n - \log \lambda = \omega(\log \lambda)$-qubit output
$(2^d(n - \log \lambda) = \omega(\lambda))$

$\rightarrow$ Quantum analogue of Naor commitment

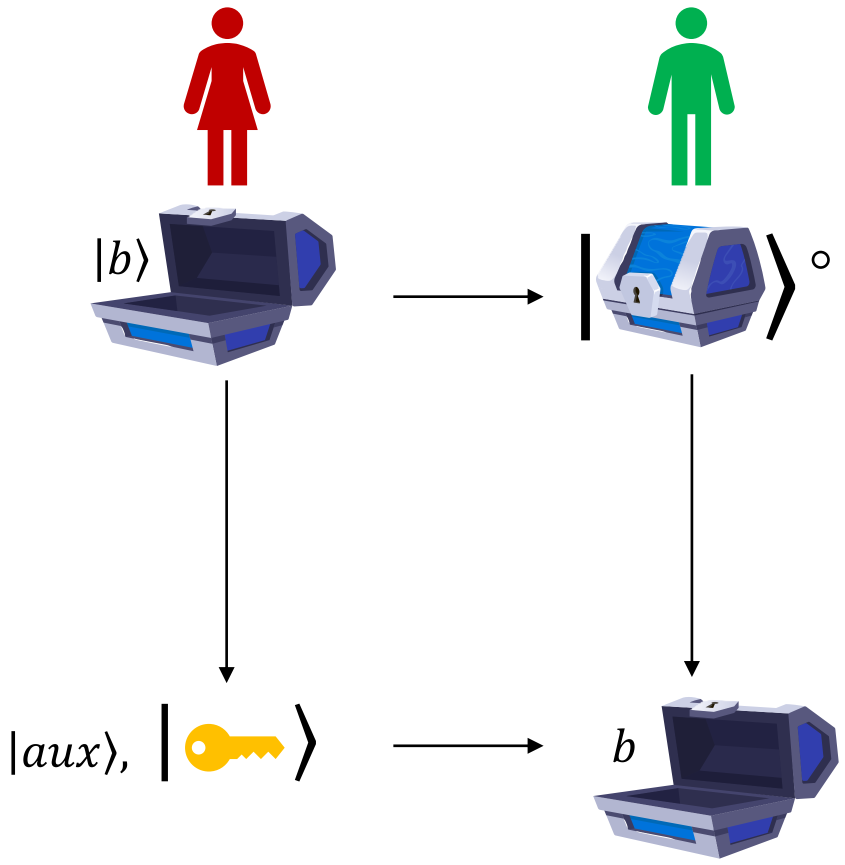
$\rightarrow$ Malicious MPC [BCKM21]

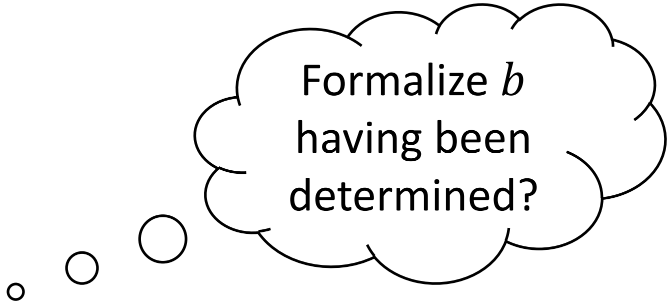
Subtleties

G is a PRFS with $2^d \cdot n \geq 7\lambda$



Generalizing statistical binding for quantum bit commitments





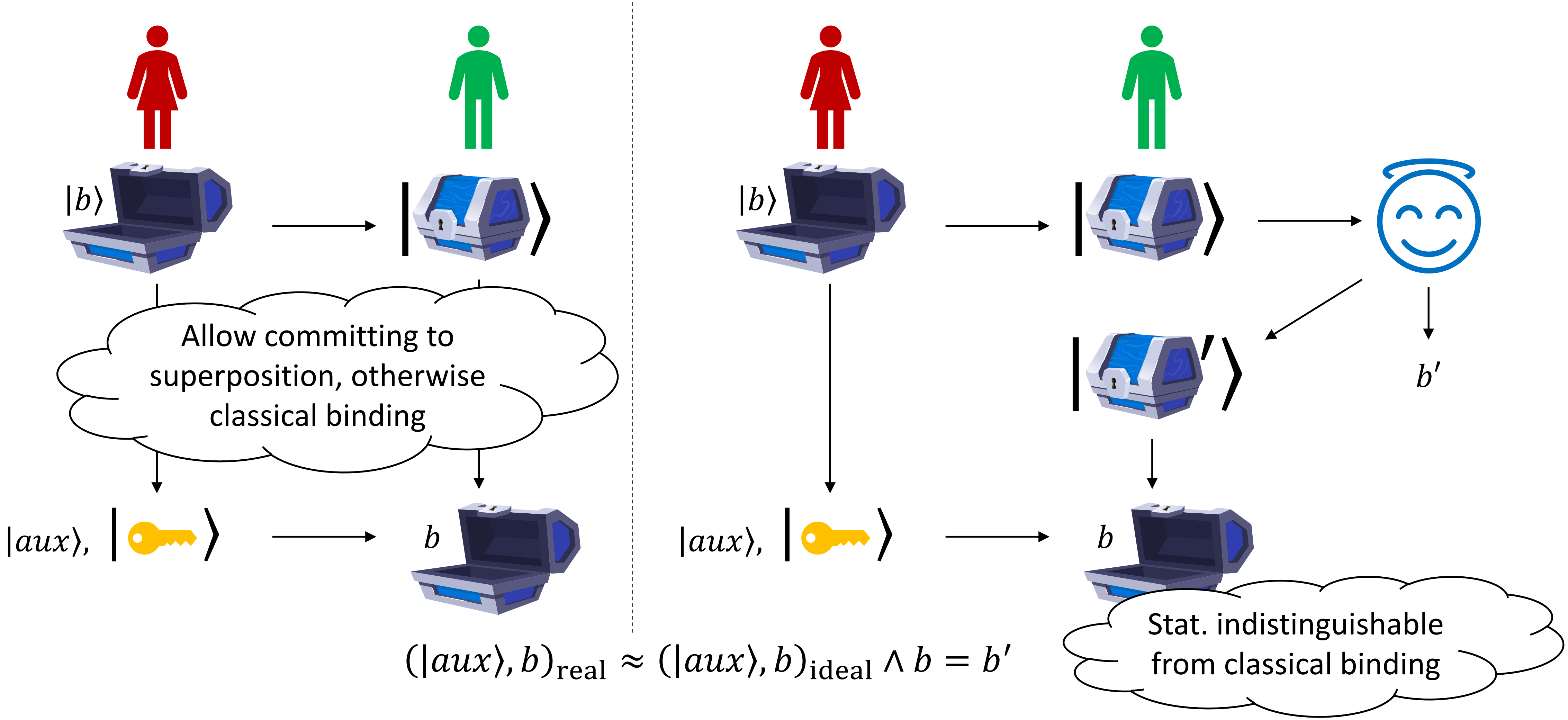
Prior work on defining statistical binding –

- Sum binding: [Yan, Weng, Lin, Quan'15; Unruh'16; Fang, Unruh, Yan, Zhou'20; MY21]

$$\Pr[\text{open } 0] + \Pr[\text{open } 1] \leq 1 + \text{negl}$$

- "Classical" binding: receiver's measurement outcomes statistically determine the bit [Bitansky, Brakerski'21; BCKM21]

Generalizing statistical binding for quantum bit commitments



$$(|aux\rangle, b)_{\text{real}} \approx (|aux\rangle, b)_{\text{ideal}} \wedge b = b'$$

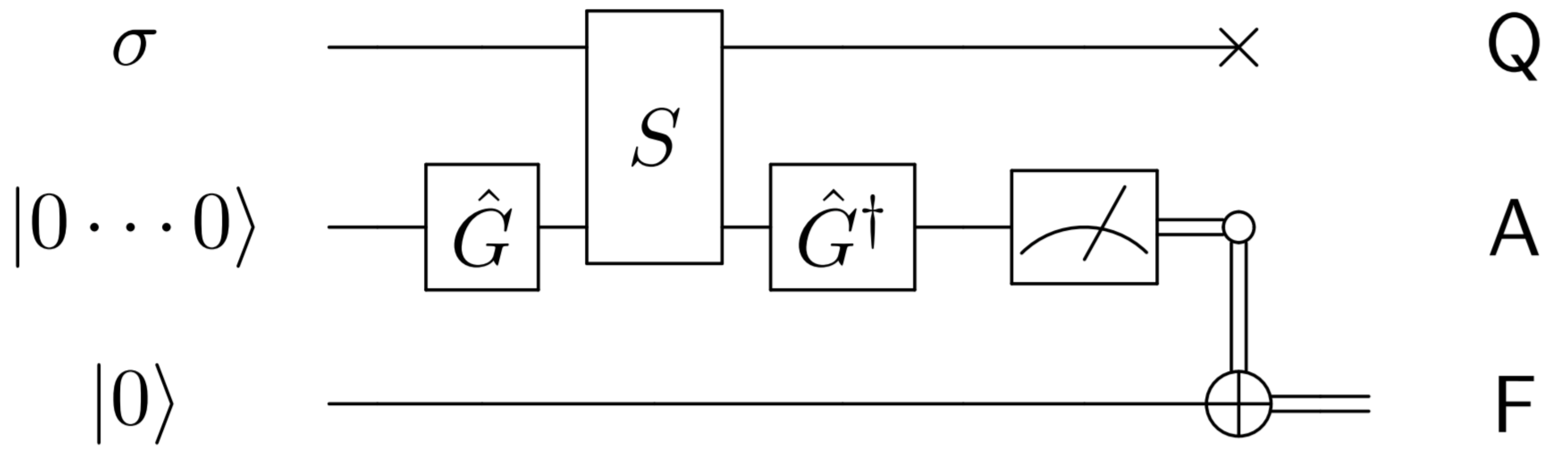
Testing PRS/PRFS: challenges

- SWAP test only gives inverse polynomial guarantee
  (we want negligible security)
- Our PRFS (post-selection) construction does not satisfy standard state generation guarantee
  - runs in expected poly-time
    (or strict poly-time with inverse exponential failure probability)
  - produces garbage auxiliary (also applies to [BS20])
    (auxiliary cannot be generically uncomputed when output is quantum)

Testing PRS/PRFS: solution

We show how to test PRS/PRFS without state generation guarantee (output can even be a mixed state)

See paper for analysis



Open questions

Quantum cryptography from quantum computational assumptions!

- Candidate PRS/PRU without OWF? (Random quantum circuit?)
- Construct crypto from PRS with even smaller output length? (Construct statistical PRS with larger output length?)
- What other interesting quantum hardness lies beyond PRS?

Thank you!