Pseudorandom (Function-Like) Quantum State Generators

New Definitions And Applications

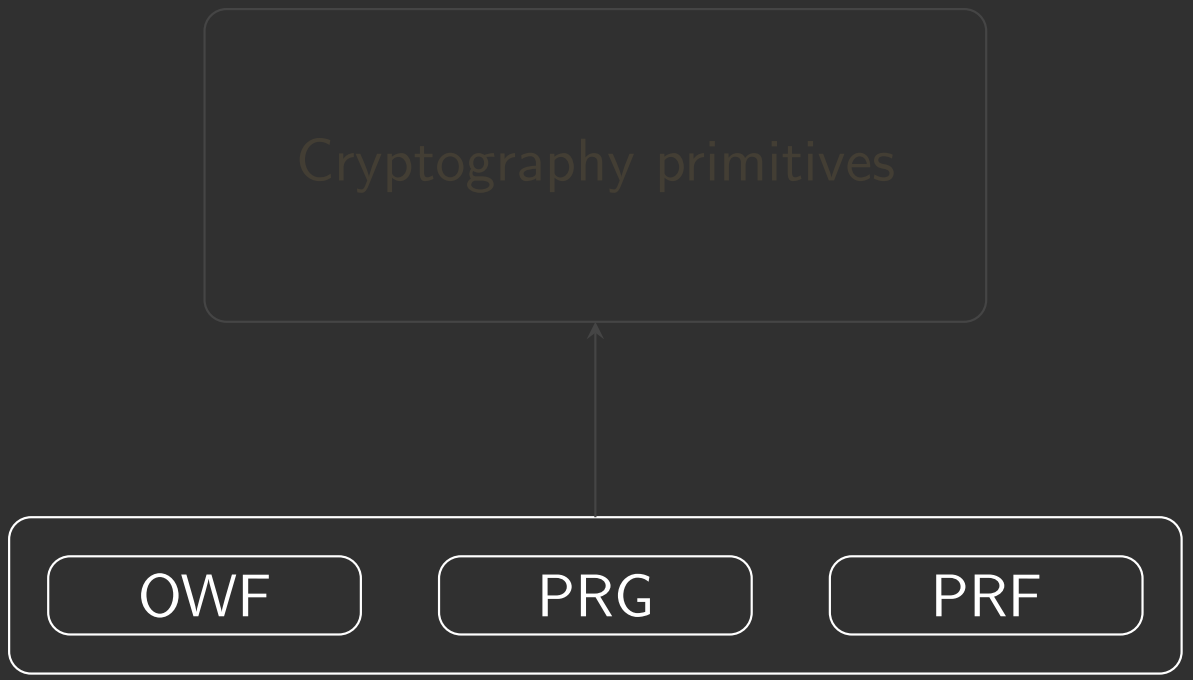
Prabhanjan Ananth (UCSB),
Aditya Gulati (UCSB),
Luowen Qian (Boston University),
Henry Yuen (Columbia University)

Theoretical Cryptography Conference 2022

November 7, 2022

Pseudorandomness

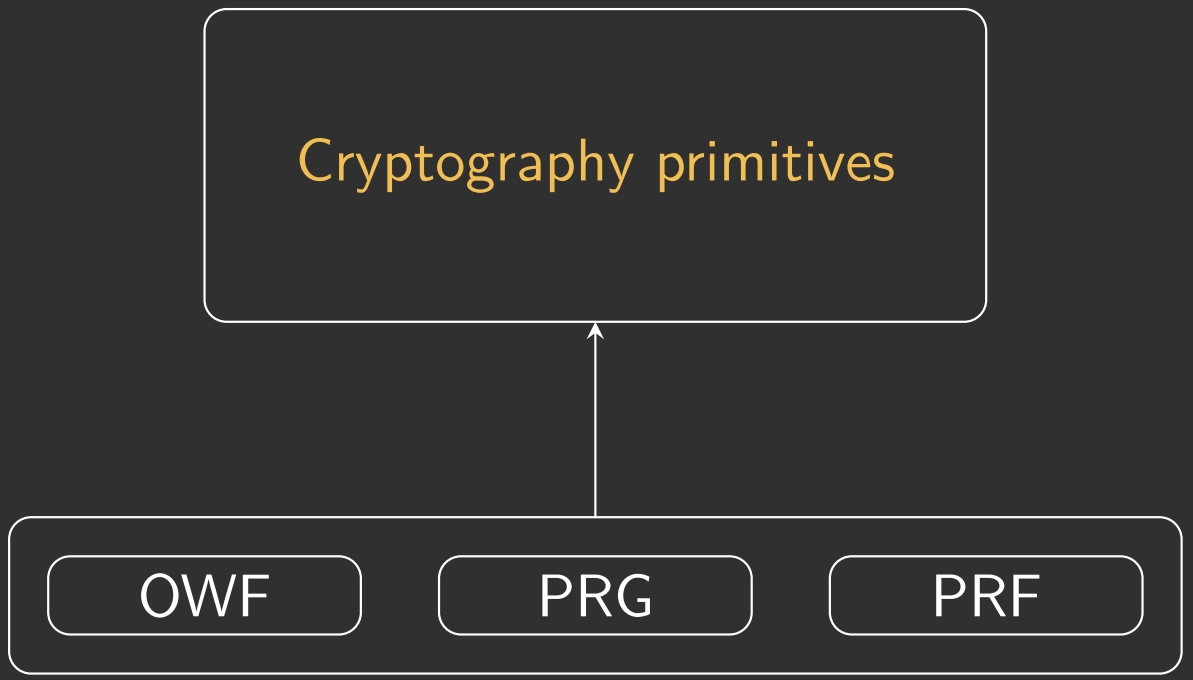
Classical



Quantum ?

Pseudorandomness

Classical

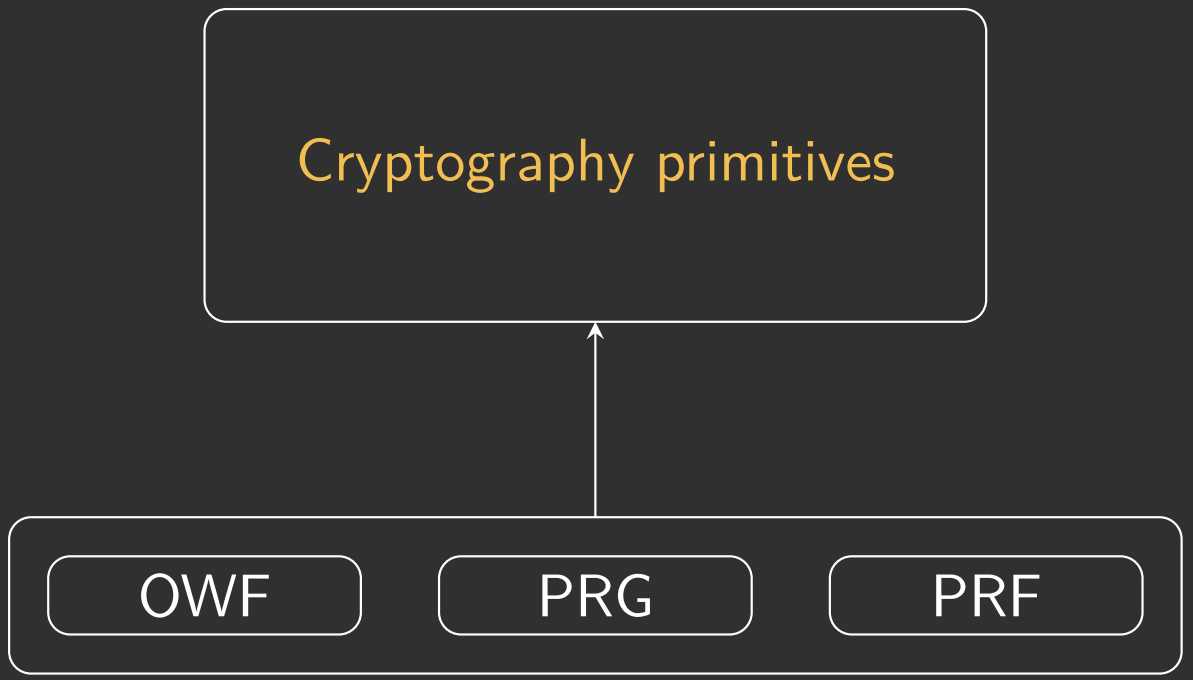


Quantum

?

Pseudorandomness

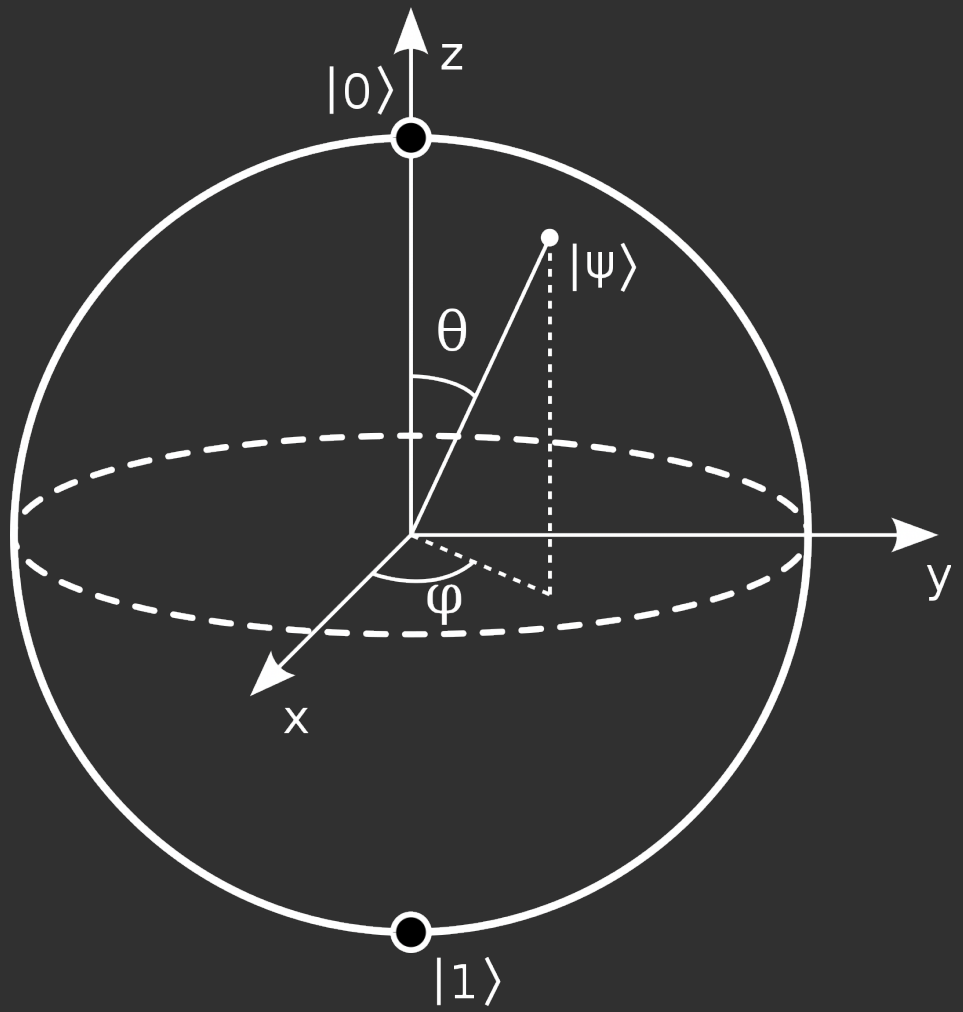
Classical



Quantum

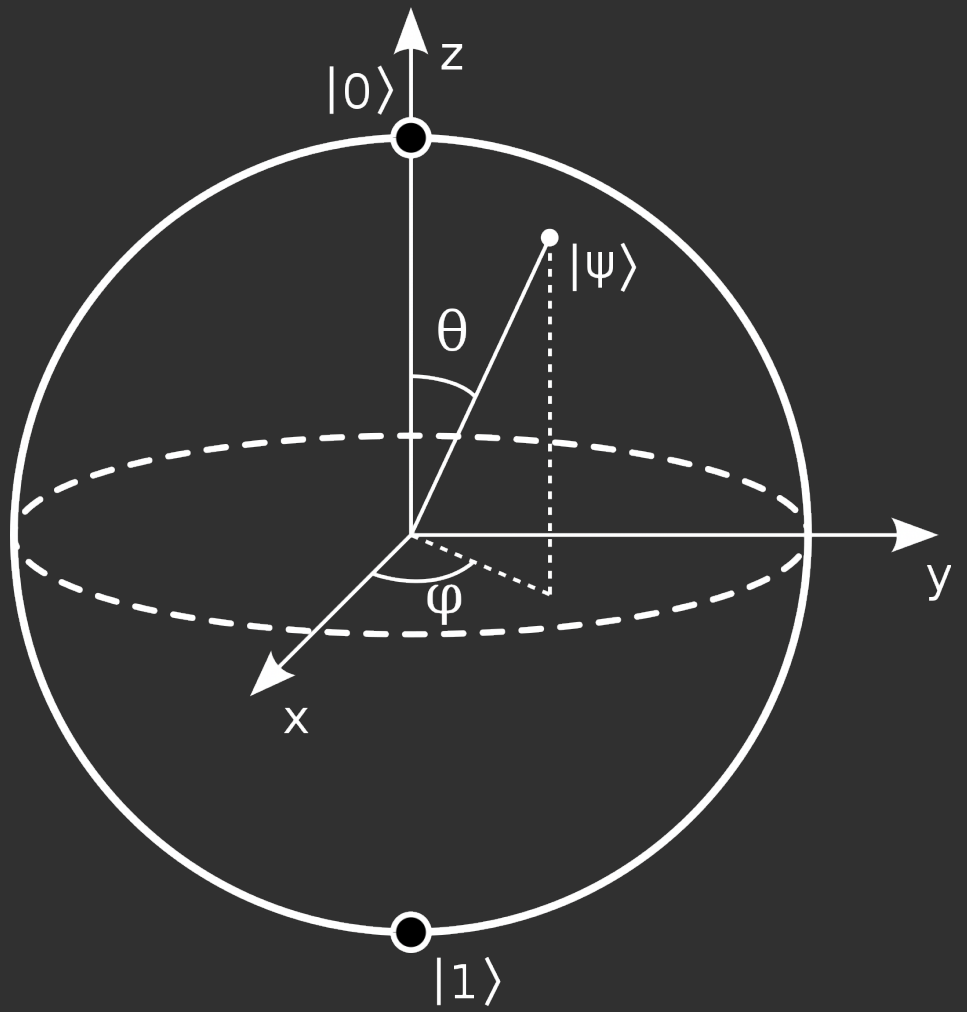
?

Haar-Random State



Haar random state looks like picking a random point on the bloch sphere.

Haar-Random State



Haar random state looks like picking a random point on the bloch sphere.

Pseudorandom Quantum State (PRS)

Efficiently computable states that “look like” Haar random states.

Pseudorandom Quantum State (PRS)

1. Efficient generation:

PRS generator (Poly-sized circuit)

Notation: n-PRS

Pseudorandom Quantum State (PRS)

1. Efficient generation:

PRS generator (Poly-sized circuit)

Notation: n-PRS

Pseudorandom Quantum State (PRS)

$\forall q(\lambda) = \mathrm{poly}(\lambda)$

2. Psuedorandomness

$$\{G(k)^{\otimes q(\lambda)}\} \approx_c \left\{|\psi\rangle^{\otimes q(\lambda)}\right\}$$

$|\psi\rangle$: Haar random state on n qubits

Can't copy quantum states!

Pseudorandom Quantum State (PRS)

$\forall q(\lambda) = \mathrm{poly}(\lambda)$

2. Psuedorandomness

$$\{G(k)^{\otimes q(\lambda)}\} \approx_c \left\{|\psi\rangle^{\otimes q(\lambda)}\right\}$$

$|\psi\rangle$: Haar random state on n qubits

Can't copy quantum states!

Pseudorandom Quantum State (PRS)

$\forall q(\lambda) = \mathsf{poly}(\lambda)$

2. Psuedorandomness

$$\left\{G(k)^{\otimes q(\lambda)}\right\} \approx_c \left\{|\psi\rangle^{\otimes q(\lambda)}\right\}$$

$|\psi\rangle$: Haar random state on n qubits

Can't copy quantum states!

Pseudorandom Quantum State (PRS)

Constructions

PRS from one-way functions.

- Ji-Liu-Song'18
- Brakerski-Shmueli'19,20

PRF

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

Binary phase PRS

Pseudorandom Quantum State (PRS)

Constructions

PRS from one-way functions.

- Ji-Liu-Song'18
- Brakerski-Shmueli'19,20

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

PRF

Binary phase PRS

PRS vs OWF

[Kretshmer'TQC'20]

There is an oracle with respect to which:

- OWF doesn't exist
- PRS exists

Pseudorandom Quantum State (PRS)

Q1. For what parameters does information-theoretic PRS exist?

Classically, 1 bit stretch requires computational assumptions.

Pseudorandom Quantum State (PRS)

Q1. For what parameters does information-theoretic PRS exist?

Classically, 1 bit stretch requires computational assumptions.

Feasibilty of PRS (Contribution)

[Brakerski, Shmueli'20] $\exists c \in \mathbb{R}, n = c \cdot \log(\lambda)$: information theoretic PRS.

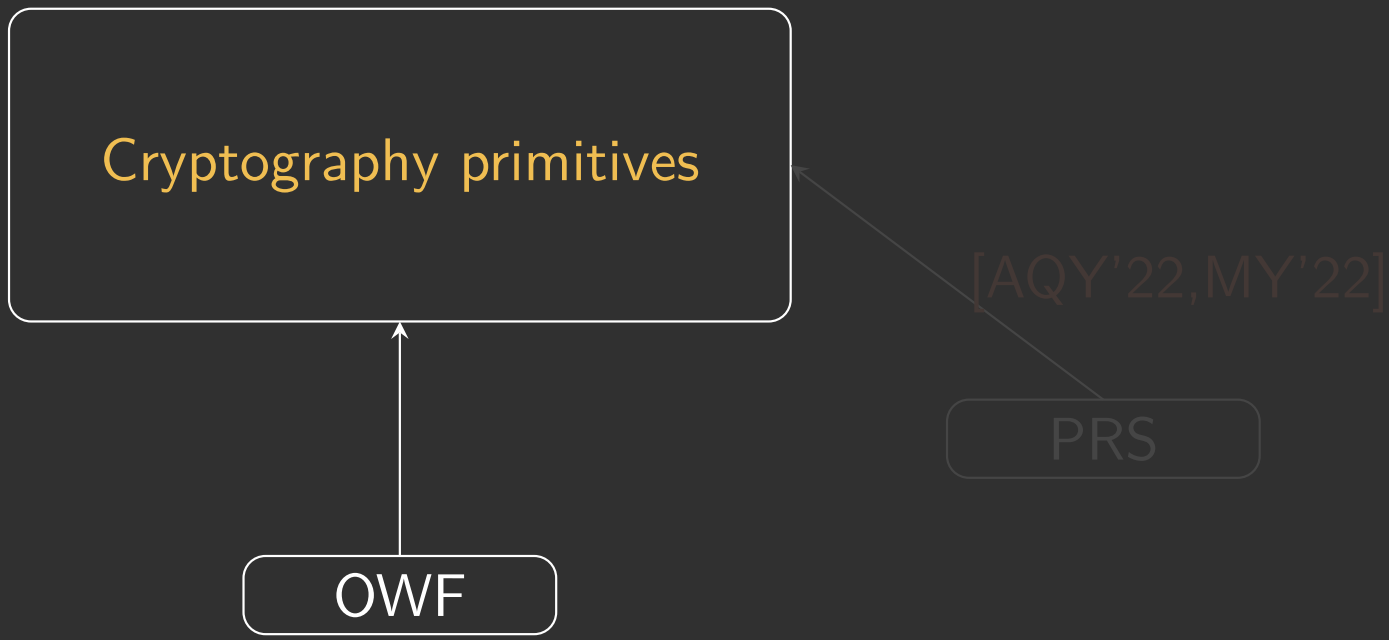
$n \geq \log(\lambda)$: needs computational assumptions.

Feasibilty of PRS (Contribution)

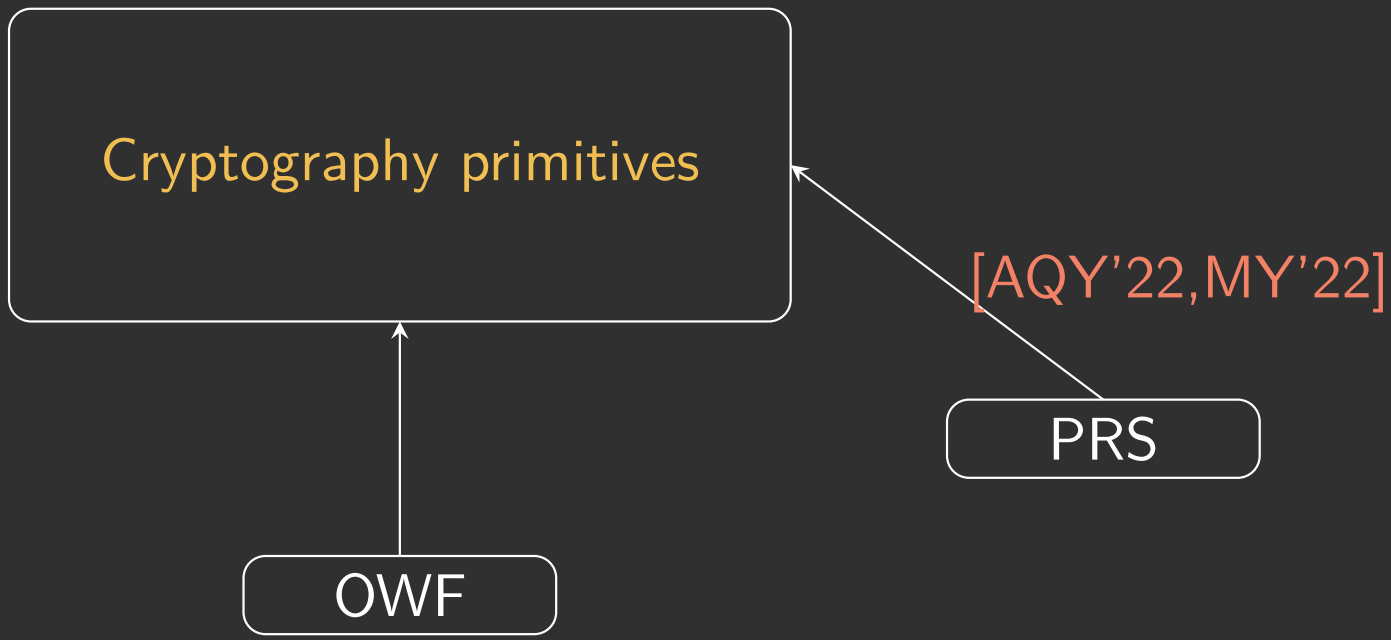
[Brakerski, Shmueli'20] $\exists c \in \mathbb{R}, n = c \cdot \log(\lambda)$: information theoretic PRS.

$n \geq \log(\lambda)$: needs computational assumptions.

PRS vs OWF



PRS vs OWF



Psuedorandom Function-Like State (PRFS)

Pseudorandom Function-Like State (PRFS)

1. Efficient generation:

Notation: (n, d)-$PRFS$

Pseudorandom Function-Like State (PRFS)

$\forall q(\lambda) = \mathsf{poly}(\lambda), x_1, \ldots, x_q,$

2. Selective Security:[AQY'22]

$$\{F(k,x_1)^{\otimes q}, \ldots, F(k,x_q)^{\otimes q}\} \approx_c \left\{|\psi_{x_1}\rangle^{\otimes q}, \ldots, |\psi_{x_q}\rangle^{\otimes q}\right\}$$

$|\psi_{x_1}\rangle, \ldots, |\psi_{x_q}\rangle$: Haar random states on n qubits.

Pseudorandom Function-Like State (PRFS)

$\forall q(\lambda) = \mathsf{poly}(\lambda), x_1, \ldots, x_q,$

2. Selective Security:[AQY'22]

$$\{F(k,x_1)^{\otimes q}, \ldots, F(k,x_q)^{\otimes q}\} \approx_c \left\{|\psi_{x_1}\rangle^{\otimes q}, \ldots, |\psi_{x_q}\rangle^{\otimes q}\right\}$$

Might not be sufficient for many applications.

2. Adaptive Security:

- Adversary can choose $x_1, \ldots, x_q$ adaptively.
- Quantum access: query $\sum_{x,y} \alpha_{x,y}|x,y\rangle$ and receive $\sum_{x,y} \alpha_{x,y}|x,y \oplus F(k,x)\rangle$.

Pseudorandom Function-Like State (PRFS)

$\forall q(\lambda) = \mathsf{poly}(\lambda), x_1, \ldots, x_q,$

2. Selective Security:[AQY'22]

$$\{F(k,x_1)^{\otimes q}, \ldots, F(k,x_q)^{\otimes q}\} \approx_c \left\{|\psi_{x_1}\rangle^{\otimes q}, \ldots, |\psi_{x_q}\rangle^{\otimes q}\right\}$$

Might not be sufficient for many applications.

2. Adaptive Security:

- Adversary can choose $x_1, \ldots, x_q$ adaptively.
- Quantum access: query $\sum \alpha_x |x\rangle$ and receive $\sum \alpha_x |x\rangle |\psi_x\rangle$.

Pseudorandom Function-Like State (PRFS)

$\forall q(\lambda) = \mathsf{poly}(\lambda), x_1, \ldots, x_q,$

2. Selective Security:[AQY'22]

$$\{F(k,x_1)^{\otimes q}, \ldots, F(k,x_q)^{\otimes q}\} \approx_c \left\{|\psi_{x_1}\rangle^{\otimes q}, \ldots, |\psi_{x_q}\rangle^{\otimes q}\right\}$$

Might not be sufficient for many applications.

2. Adaptive Security:

- Adversary can choose $x_1, \ldots, x_q$ adaptively.
- Quantum access: query $\sum \alpha_x |x\rangle$ and receive $\sum \alpha_x |x\rangle |\psi_x\rangle$.

Pseudorandom Function-Like State (PRFS)

Q2. Does PRFS with these stronger notions exist?

Stronger security notion (Contribution)

- Construct Adaptive PRFS from post-quantum one-way functions.
- Construct Quantum Access Adaptive PRFS from post-quantum one-way functions.
- Simpler proof of Binary Phase PRS by getting a better representation of Haar random states
  [Brakerski, Shmueli'19]: involved proof!

Stronger security notion (Contribution)

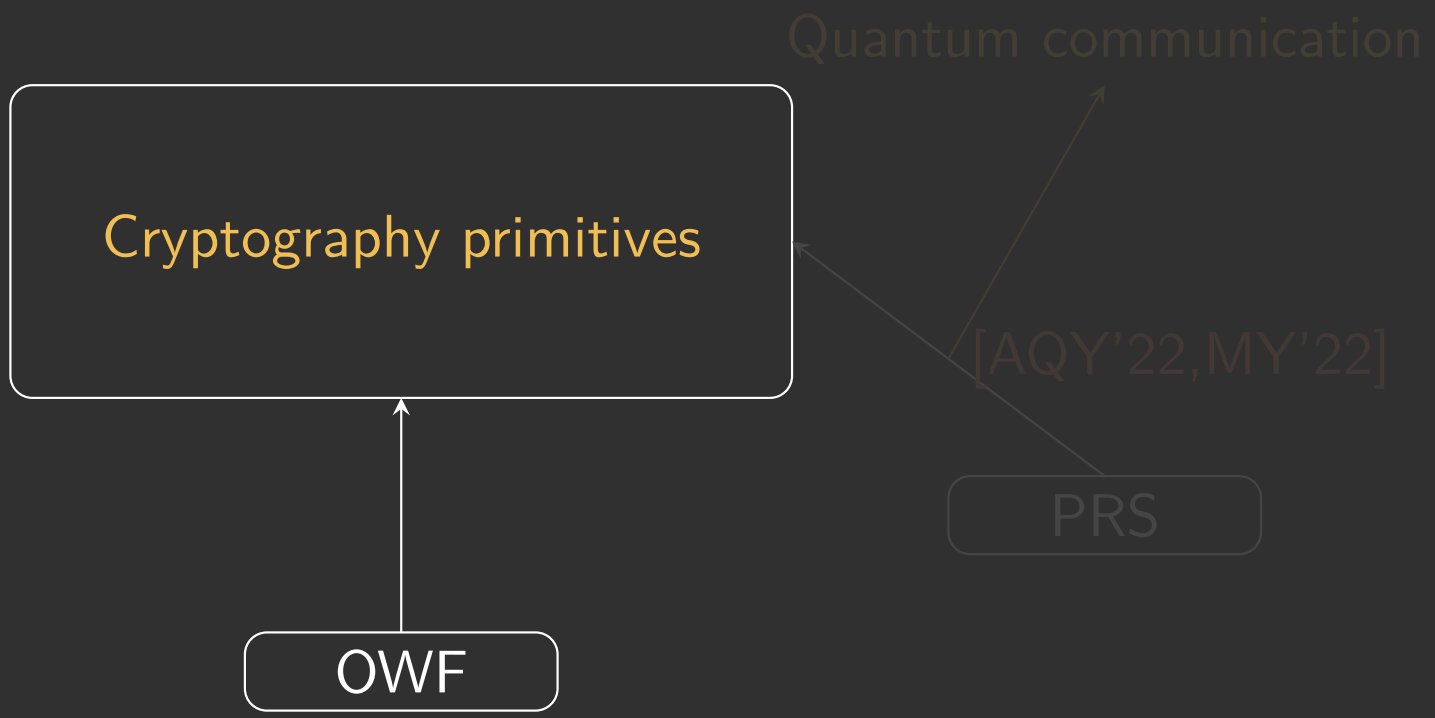
- Construct Adaptive PRFS from post-quantum one-way functions.
- Construct Quantum Access Adaptive PRFS from post-quantum one-way functions.
- Simpler proof of Binary Phase PRS by getting a better representation of Haar random states
  [Brakerski, Shmueli'19]: involved proof!

Stronger security notion (Contribution)

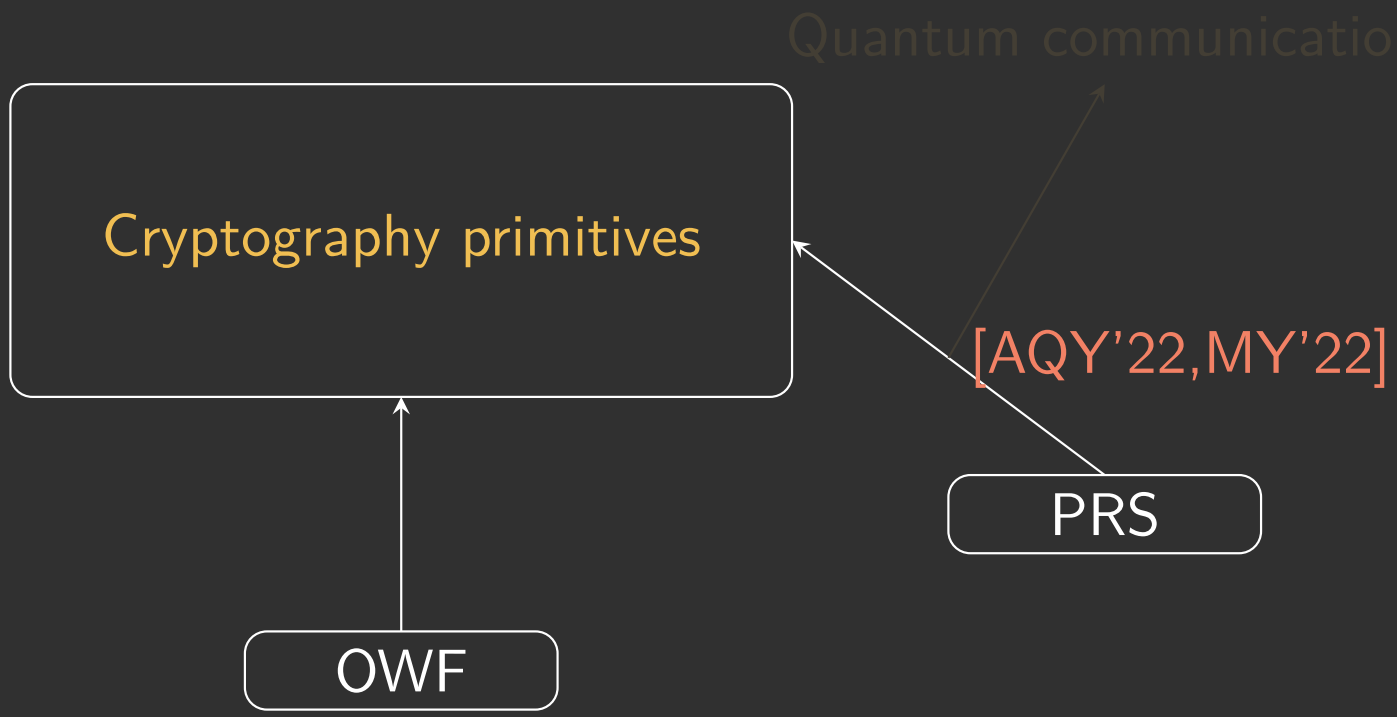
- Construct Adaptive PRFS from post-quantum one-way functions.
- Construct Quantum Access Adaptive PRFS from post-quantum one-way functions.
- Simpler proof of Binary Phase PRS by getting a better representation of Haar random states
  [Brakerski, Shmueli'19]: involved proof!

Applications to cryptography

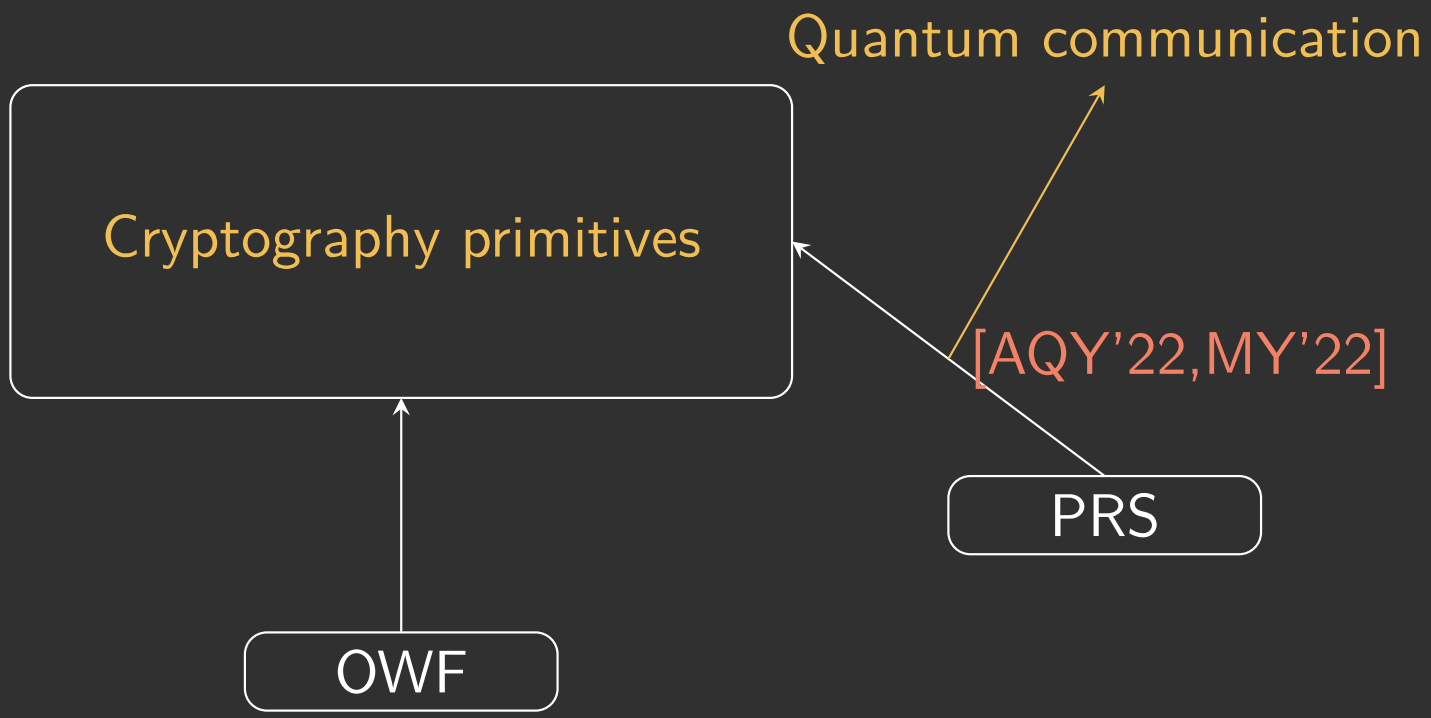
Cryptography from PRS



Cryptography from PRS



Cryptography from PRS



Applications to cryptography

Q3. Is quantum communication necessary in PRS-based primitives?

PRS-based crypto with classical communication (Contribution)

- PRS-based commitment scheme with computational binding and statistical hiding with only classical communication.
- PRS-based QOTP with only classical communication.

PRS-based crypto with classical communication (Contribution)

- PRS-based commitment scheme with computational binding and statistical hiding with only classical communication.
- PRS-based QOTP with only classical communication.

Techniques
Need for computational assumption

Computational assumptions

Inefficient

G is a $\log(\lambda)$-PRS, then $\exists A_\lambda$,

$$\left|\Pr\left[A_\lambda\left(G(k)^{\otimes t}\right)=1\right]-\Pr\left[A_\lambda\left(|\psi\rangle^{\otimes t}\right)=1\right]\right|\geq\frac{1}{3}$$

Haar random

Computational assumptions

$G(k)$ is almost pure.

If $G(k)$ is not pure, A_λ can distinguish using the SWAP test.

Computational assumptions

$G(k)$ is almost pure.
If $G(k)$ is not pure, A_λ can distinguish using the SWAP test.

Computational assumptions

Distinguish by projecting here

PRS

$$\dim\left(\text{Span}\left\{|\psi_k\rangle\langle\psi_k|^{\otimes t}\right\}\right) \leq 2^{\lambda}$$

Haar

$$\dim\left(\text{Span}\left\{|\psi\rangle\langle\psi|^{\otimes t}\right\}\right) = \binom{2^n + t - 1}{t}$$

$$\dim\left(\text{Span}\left\{|\psi\rangle\langle\psi|^{\otimes t}\right\}\right) \geq 6 \cdot 2^{\lambda}$$

$$t = \lambda + 1$$

Computational assumptions

Distinguish by projecting here

PRS

$$\dim\left(\text{Span}\left\{|\psi_k\rangle\langle\psi_k|^{\otimes t}\right\}\right) \leq 2^{\lambda}$$

Haar

$$\dim\left(\text{Span}\left\{|\psi\rangle\langle\psi|^{\otimes t}\right\}\right) = \binom{2^n + t - 1}{t}$$

$$\dim\left(\text{Span}\left\{|\psi\rangle\langle\psi|^{\otimes t}\right\}\right) \geq 6 \cdot 2^{\lambda}$$

$$t = \lambda + 1$$

Computational assumptions

Distinguish by projecting here

PRS

$$\dim\left(\mathsf{Span}\left\{|\psi_k\rangle\langle\psi_k|^{\otimes t}\right\}\right) \leq 2^{\lambda}$$

Haar

$$\dim\left(\mathsf{Span}\left\{|\psi\rangle\langle\psi|^{\otimes t}\right\}\right) = \binom{2^n + t - 1}{t}$$

$$\dim\left(\mathsf{Span}\left\{|\psi\rangle\langle\psi|^{\otimes t}\right\}\right) \geq 6 \cdot 2^{\lambda}$$

$t = \lambda + 1$

Computational assumptions

Distinguish by projecting here

PRS

$$\dim\left(\text{Span}\left\{|\psi_k\rangle\langle\psi_k|^{\otimes t}\right\}\right) \leq 2^{\lambda}$$

Haar

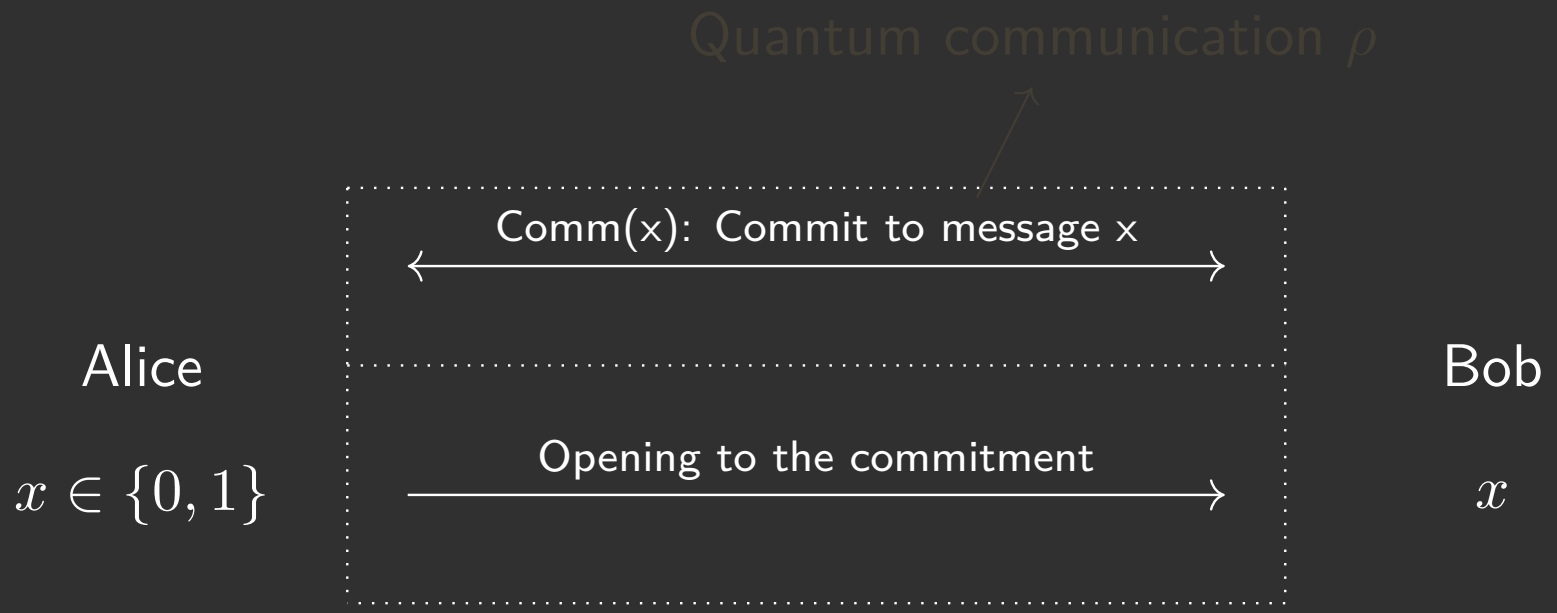
$$\dim\left(\text{Span}\left\{|\psi\rangle\langle\psi|^{\otimes t}\right\}\right) = \binom{2^n + t - 1}{t}$$

$$\dim\left(\text{Span}\left\{|\psi\rangle\langle\psi|^{\otimes t}\right\}\right) \geq 6 \cdot 2^{\lambda}$$

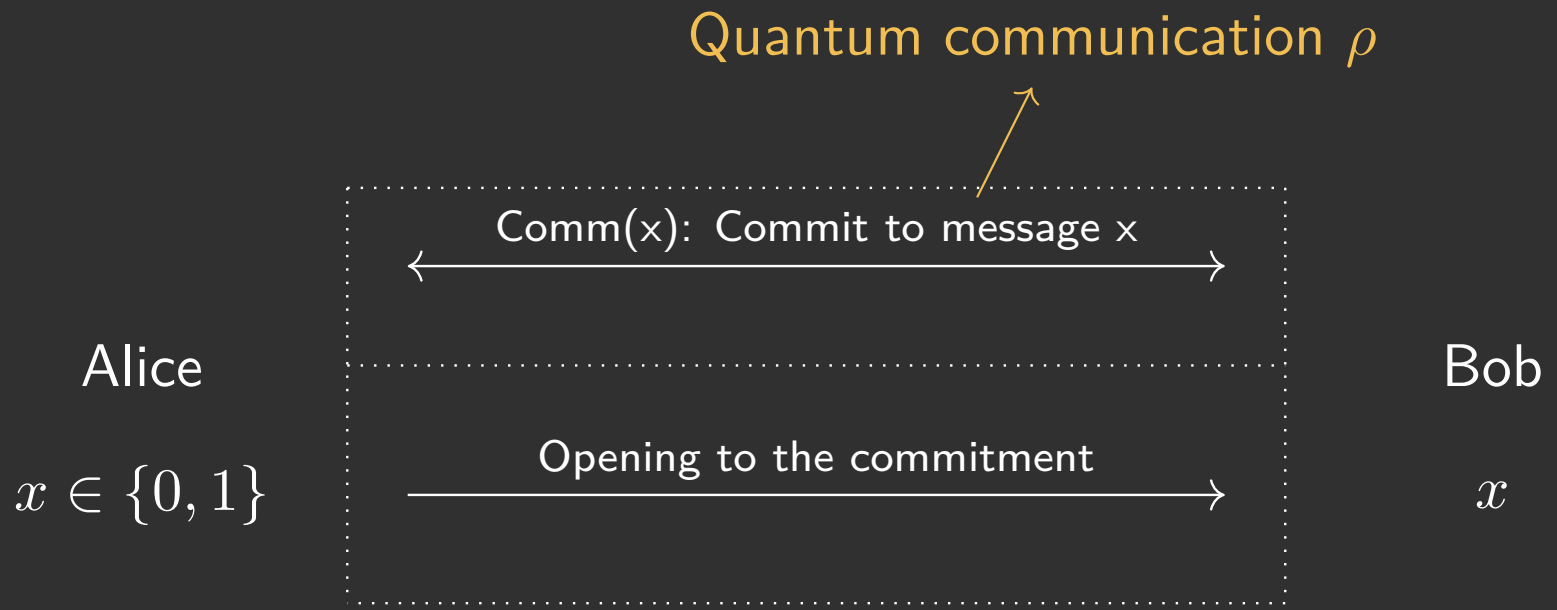
$$t = \lambda + 1$$

Techniques
Commitment scheme

Commitment scheme [AQY'22]



Commitment scheme [AQY'22]



Tomography

Procedure to get a classical description of a quantum state:

$$\text{Tomography}(\rho^{\otimes \exp(n)}) = M \longrightarrow n = \log(\lambda)$$

such that

$$\|\rho - M\|_F \leq \text{negl}$$

Tomography

Procedure to get a classical description of a quantum state:

$$\text{Tomography}(\rho^{\otimes \exp(n)}) = M \longrightarrow n = \log(\lambda)$$

such that

$$\|\rho - M\|_F \leq \text{negl}$$

Tomography

Procedure to get a classical description of a quantum state:

$$\text{Tomography}(\rho^{\otimes \exp(n)}) = M \qquad n = \log(\lambda)$$

such that

$$\|\rho - M\|_F \leq \text{negl}$$

Tomography

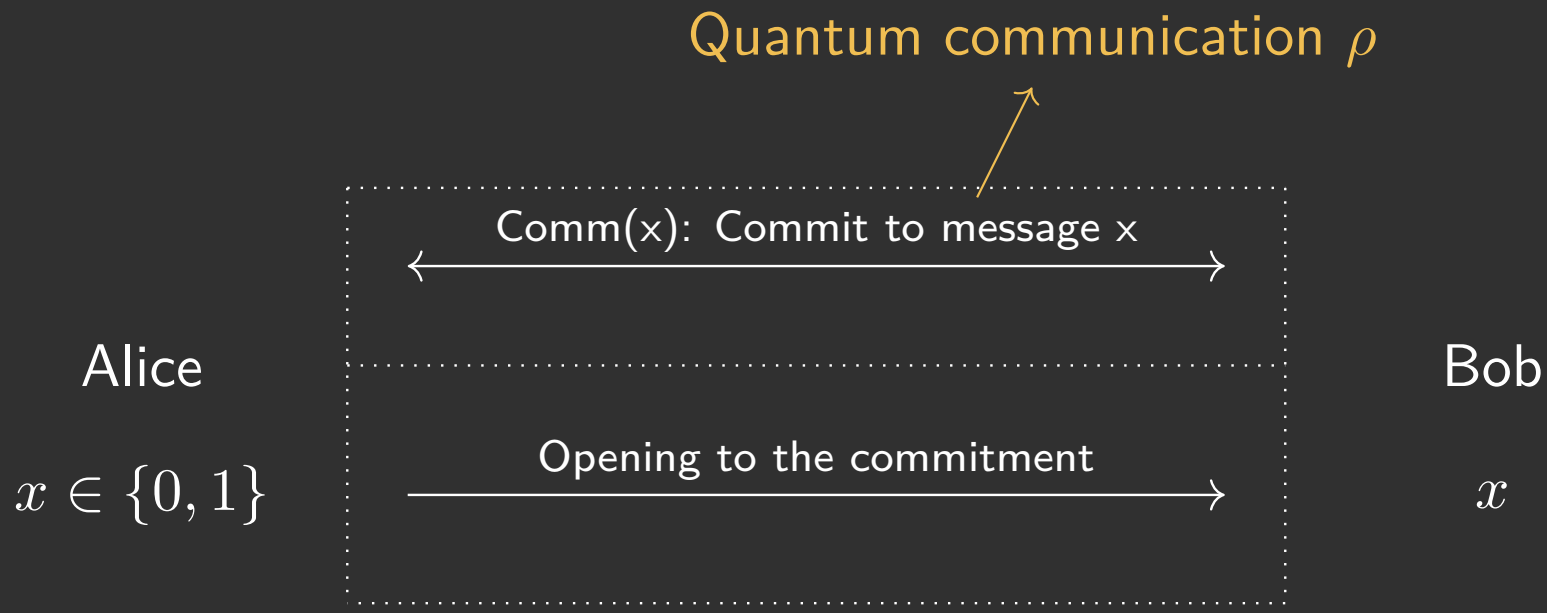
Procedure to get a classical description of a quantum state:

$$\mathsf{Tomography}(\rho^{\otimes \mathsf{exp}(n)}) = M \qquad n = \log(\lambda)$$

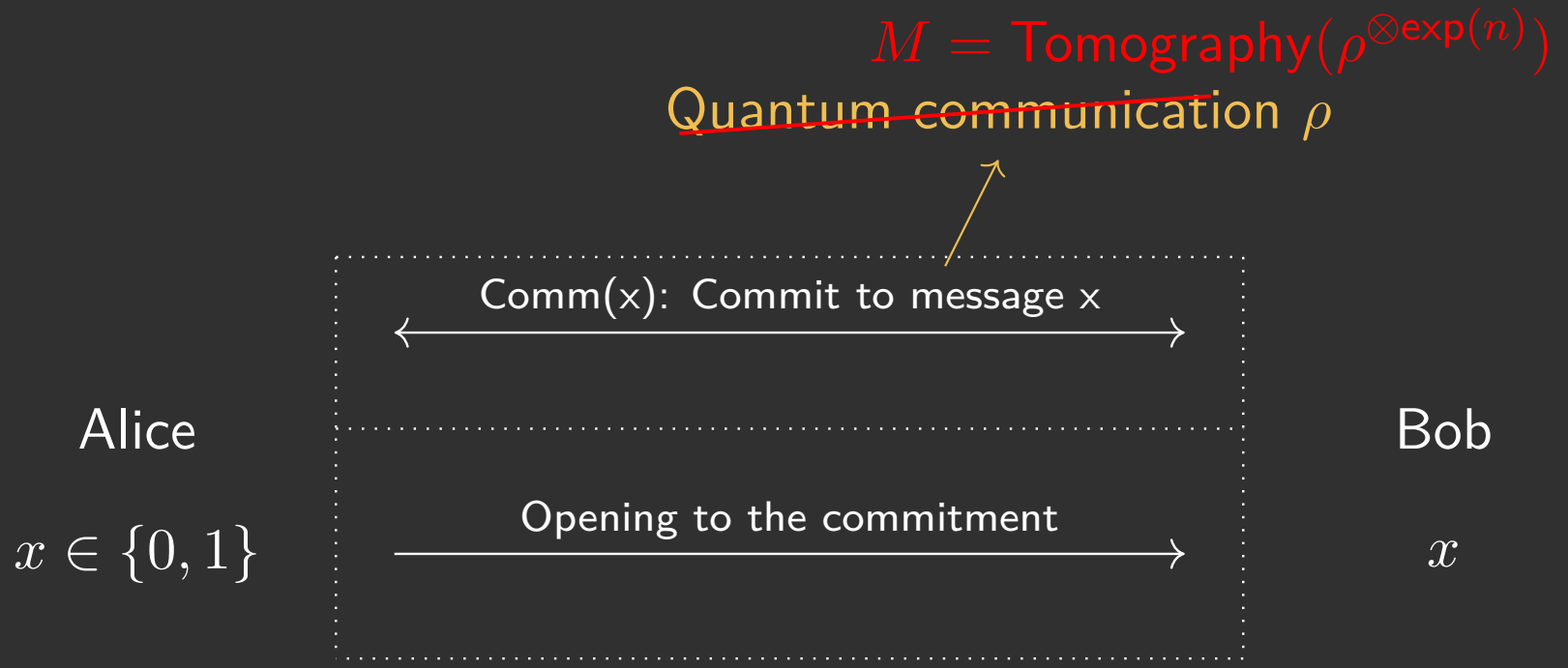
such that

$$\|\rho - M\|_F \leq \mathsf{negl}$$

Commitment scheme



Commitment scheme



Verifiable tomography

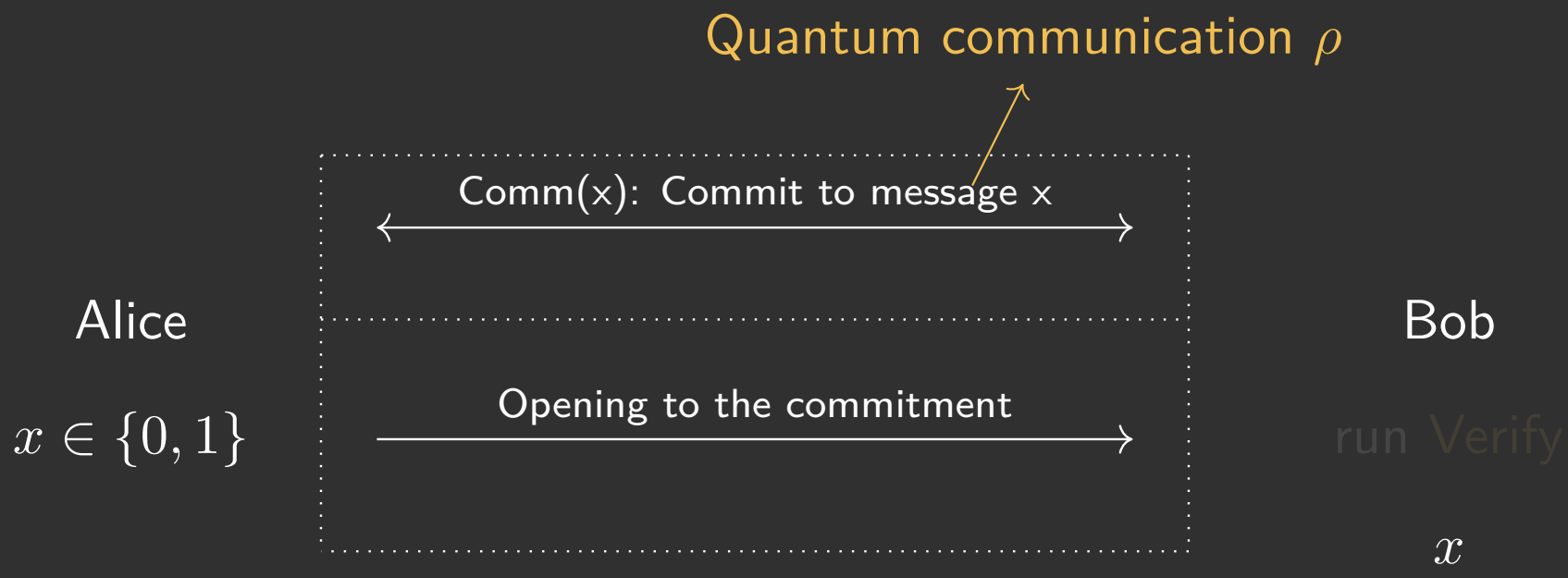
Malicious Adversaries can cheat, hence we need a stronger notion!

We equip Tomography with Verify to detect this.

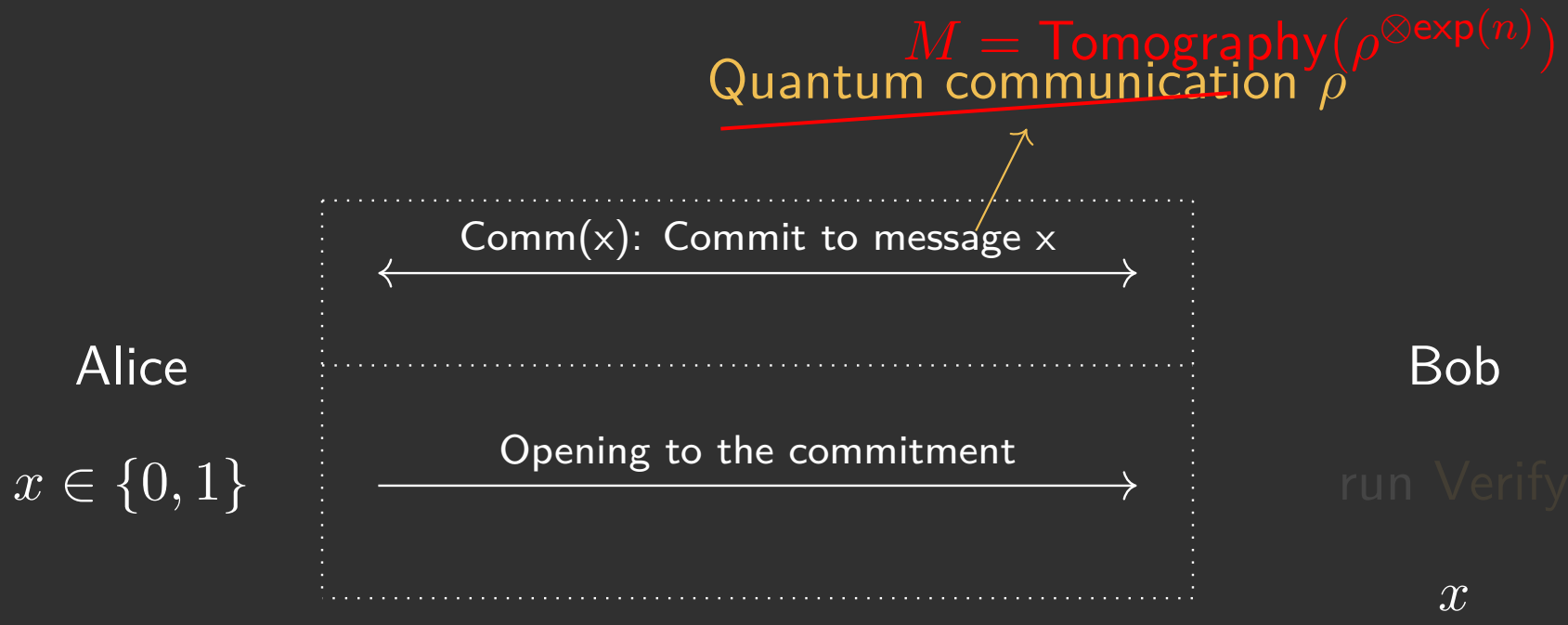
Verifiable tomography

Malicious Adversaries can cheat, hence we need a stronger notion!
We equip Tomography with Verify to detect this.

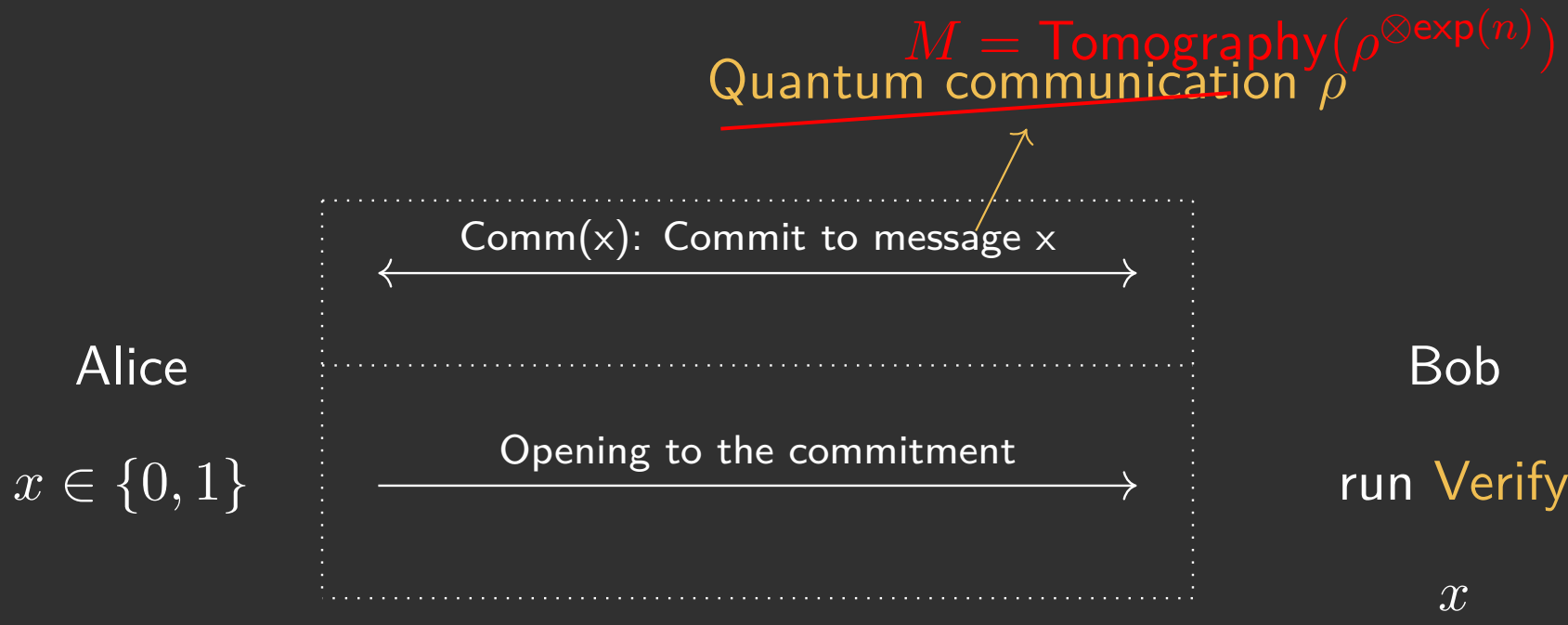
Commitment scheme



Commitment scheme



Commitment scheme



Summary

- PRS with $\omega(\log(\lambda))$-output length requires computational assumptions
- Simpler Proof of Binary Phase PRS
- New variants of PRS and their constructions
- Commitments (and other primitives) from PRFS with classical communication

Thank You