Quantum Pseudorandomness from a Single Haar Random State

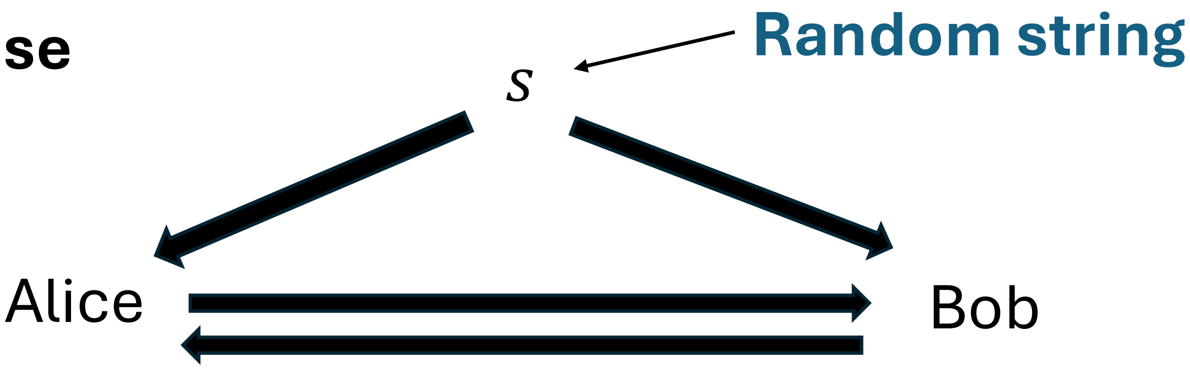
Boyang Chen (Tsinghua University)

Andrea Coladangelo (University of Washington)

Or Sattath (Ben-Gurion University)

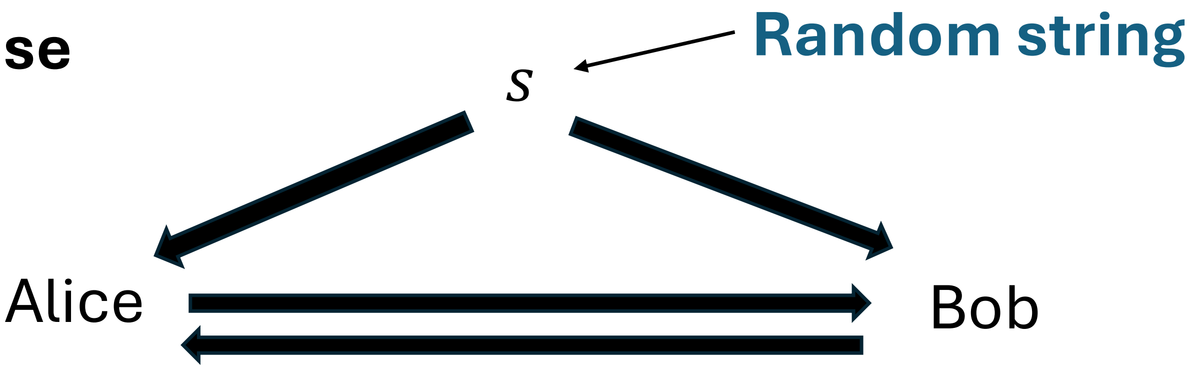
Cryptography with common randomness

- **Classical case**



Cryptography with common randomness

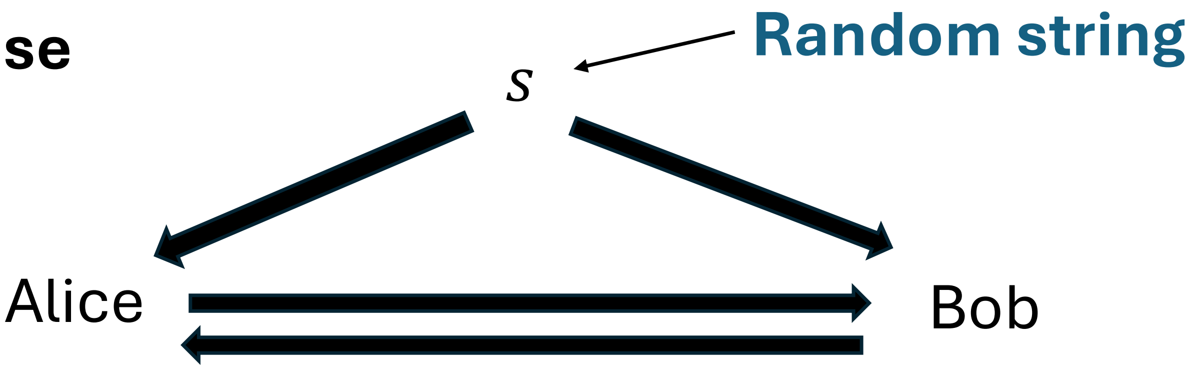
- **Classical case**



No unconditional cryptography in the common random string model

Cryptography with common randomness

- **Classical case**

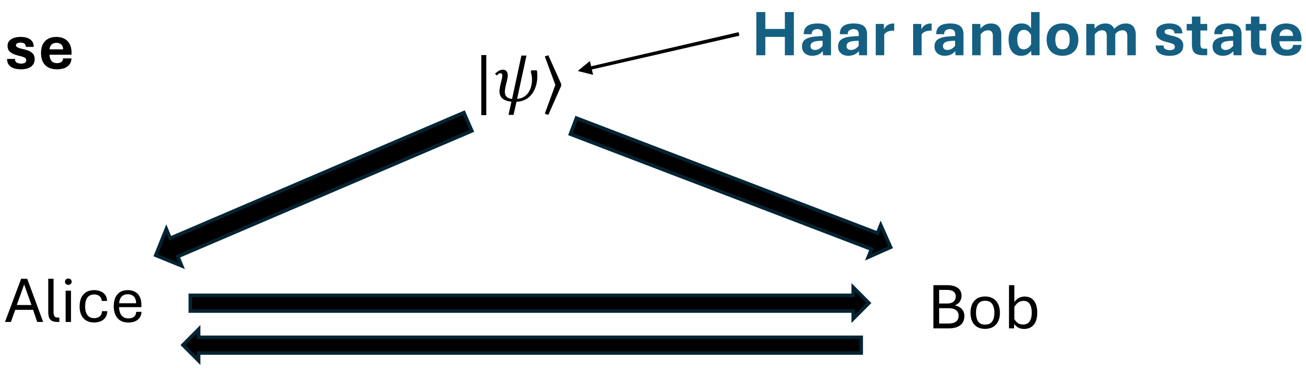


No unconditional cryptography in the common random string model

What about the quantum setting?

Cryptography with common randomness

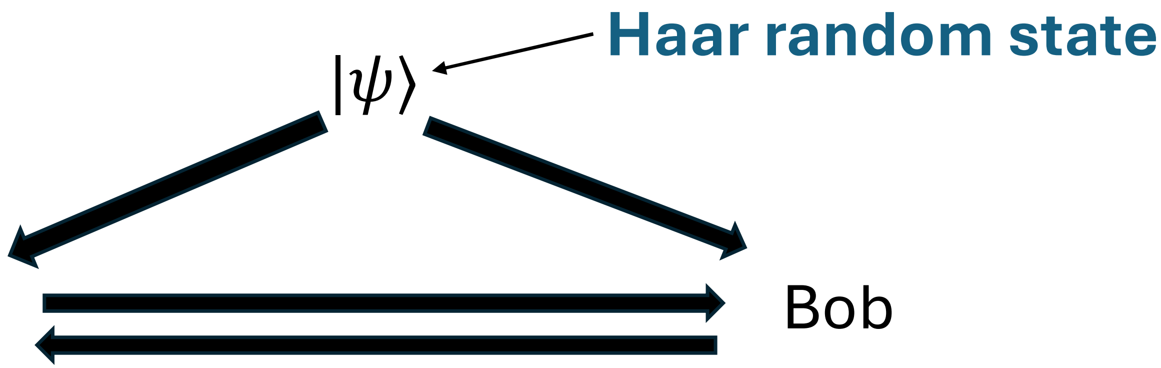
- **Quantum case**



~~No~~ **unconditional cryptography** in the common random state model **exists!!**

Cryptography with common randomness

- **Quantum case**



~~**No**~~ **unconditional cryptography** in the common random state model **exists!!**

This model is called the common Haar random state model (abbreviated as the CHRS model).

Pseudorandom states

Definition(Adapted from [Ji-Liu-Song 17])

An m-qubit state family $|\phi_k\rangle$ is ℓ**-pseudorandom state family (PRS)** if:

- $|\phi_k\rangle$ can be efficiently prepared given $k \in \{0,1\}^n$
- For any adversary $\mathcal{A}$

$$\Pr_{k\sim\{0,1\}^n}\left[\mathcal{A}\left(|\phi_k\rangle^{\otimes \ell}\right) = 1\right] - \Pr_{|\phi\rangle\leftarrow Haar}\left[\mathcal{A}\left(|\phi\rangle^{\otimes \ell}\right) = 1\right] \le negl(n)$$

Pseudorandom states

Definition(Adapted from [Ji-Liu-Song 17])

An m-qubit state family $|\phi_k\rangle$ is ℓ**-pseudorandom state family (PRS)** if:

- $|\phi_k\rangle$ can be efficiently prepared given $k \in \{0,1\}^n$
- For any adversary $\mathcal{A}$

$$\Pr_{k\sim\{0,1\}^n}\left[\mathcal{A}\left(|\phi_k\rangle^{\otimes\ell}\right) = 1\right] - \Pr_{|\phi\rangle\leftarrow Haar}\left[\mathcal{A}\left(|\phi\rangle^{\otimes\ell}\right) = 1\right] \leq negl(n)$$

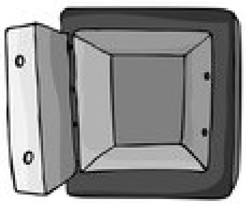
- As a special case, a **1PRS** family is such that:
  a single copy of the state is **computationally indistinguishable** from **a totally mixed state**.
- Stretch: A 1-copy pseudorandom state family is nontrivial only if $\boldsymbol{m > n}$.

Bit commitment

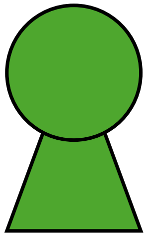
Commit phase

Hiding

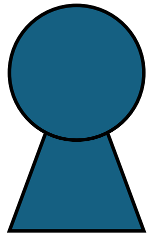
Input: b



Sender



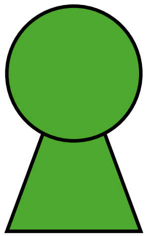
Receiver



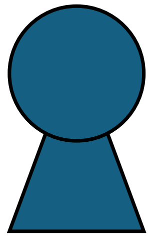
Reveal phase

Binding

Sender



Receiver



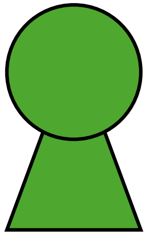
Bit commitment

Commit phase

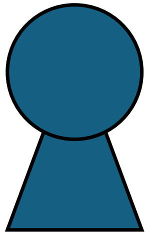
Hiding

Input: b

Sender



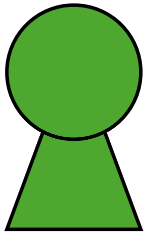
Receiver



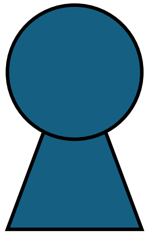
Reveal phase

Binding

Sender



Receiver

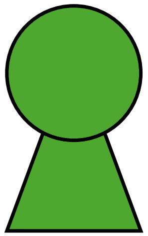


Bit commitment

Commit phase

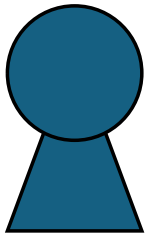
Input: b

Sender



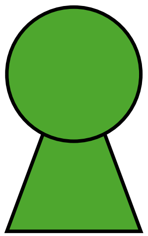
Hiding

Receiver



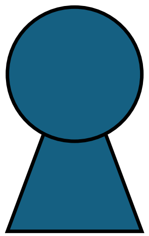
Reveal phase

Sender



Binding

Receiver

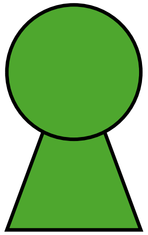


Bit commitment

Commit phase

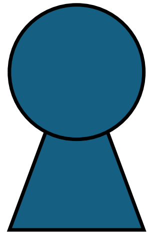
Input: b

Sender



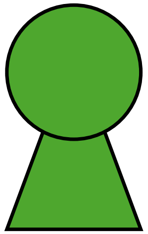
Hiding

Receiver



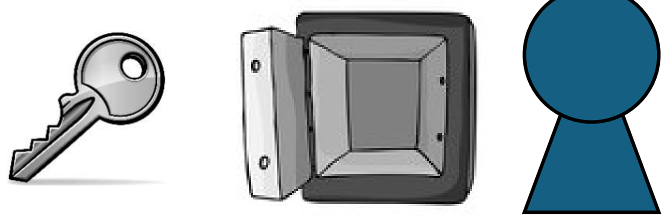
Reveal phase

Sender



Binding

Receiver



Commitment from 1PRS

Theorem [Morimae-Yamakawa'22, Morimae-Nehoran-Yamakawa'24]

1PRS implies quantum bit commitment.

Pseudorandom states

Definition

An m-qubit state family $|\phi_k\rangle$ is **ℓ-pseudorandom state family (PRS)** if:

- $|\phi_k\rangle$ can be efficiently prepared given $k \in \{0,1\}^n$
- For any adversary $\mathcal{A}$

$$\Pr_{k\sim\{0,1\}^n}[\mathcal{A}(|\phi_k\rangle^{\otimes\ell}) = 1] - \Pr_{|\phi\rangle\leftarrow Haar}[\mathcal{A}(|\phi\rangle^{\otimes\ell}) = 1] \leq \text{negl}(n)$$

- As a special case, a **1PRS** family is such that: a single copy of the state is **computationally indistinguishable** from **a totally mixed state**.
- Stretch: A 1-copy pseudorandom state family is nontrivial only if $\boldsymbol{m > n}$.

Pseudorandom states in the CHRS model

Definition

An m-qubit state family $|\phi_k\rangle$ is **ℓ-pseudorandom state family (PRS)** if:

- $|\phi_k\rangle$ can be efficiently prepared given $k \in \{0,1\}^n$ **and $|\psi\rangle^{\otimes poly}$**
- For any adversary $\mathcal{A}$

$$\Pr_{k\sim\{0,1\}^n}[\mathcal{A}(|\phi_k\rangle^{\otimes \ell}, |\psi\rangle^{\otimes poly}) = 1] - \Pr_{|\phi\rangle\leftarrow Haar}\left[\mathcal{A}(|\phi\rangle^{\otimes \ell}, |\psi\rangle^{\otimes poly}) = 1\right] \leq \mathrm{negl}(n)$$

- As a special case, a **1PRS** family is such that:
  a single copy of the state is **computationally indistinguishable** from **a totally mixed state**.
- Stretch: A 1-copy pseudorandom state family is nontrivial only if $\boldsymbol{m > n}$.

Cryptography from 1PRS

Main theorem (informal)
1PRS exist unconditionally in the CHRS model

As a corollary, quantum bit commitment exists unconditionally in the CHRS model.

Construction of PRS

Construction of PRS

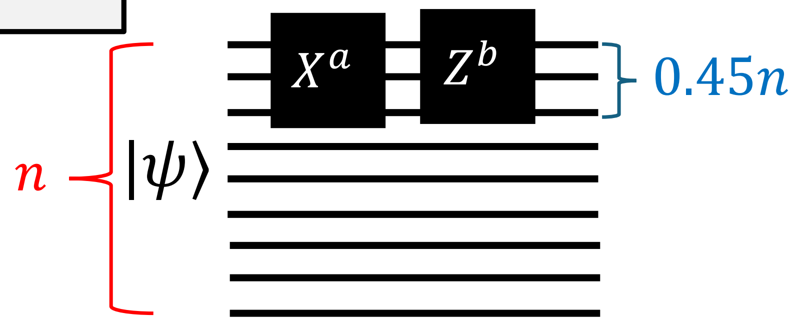
Construction:

Apply random Pauli on the first $0.45n$ qubits of the common random state $|\psi\rangle$:

$$|\phi_k\rangle := X^a Z^b \otimes I|\psi\rangle$$

where $k \in \{0,1\}^{0.9n}$, $k = a||b$

$X^a := \otimes_{i=1}^{a} X^{a_i}, Z^b := \otimes_{i=1}^{b} Z^{b_i}$



Construction of PRS

Construction:

Apply random Pauli on the first $0.45n$ qubits of the common random state $|\psi\rangle$:

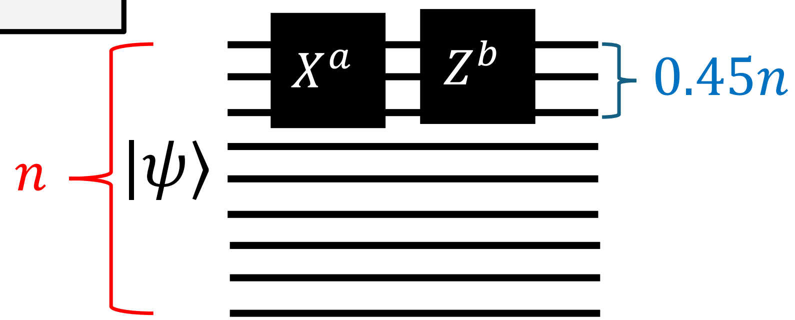
$$|\phi_k\rangle := X^a Z^b \otimes I|\psi\rangle$$

where $k \in \{0,1\}^{0.9n}$, $k = a||b$

$X^a := \otimes_{i=1}^{a} X^{a_i}, Z^b := \otimes_{i=1}^{b} Z^{b_i}$

☑ **Efficient Generation**

☑ **Stretch**

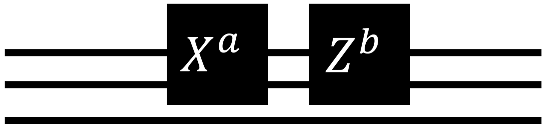


Proof sketch

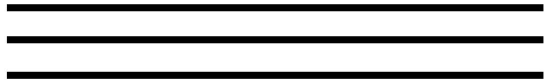
Statistical 1-copy Security

- What does 1-copy security mean?

$\ell = 1$ $|\psi\rangle$



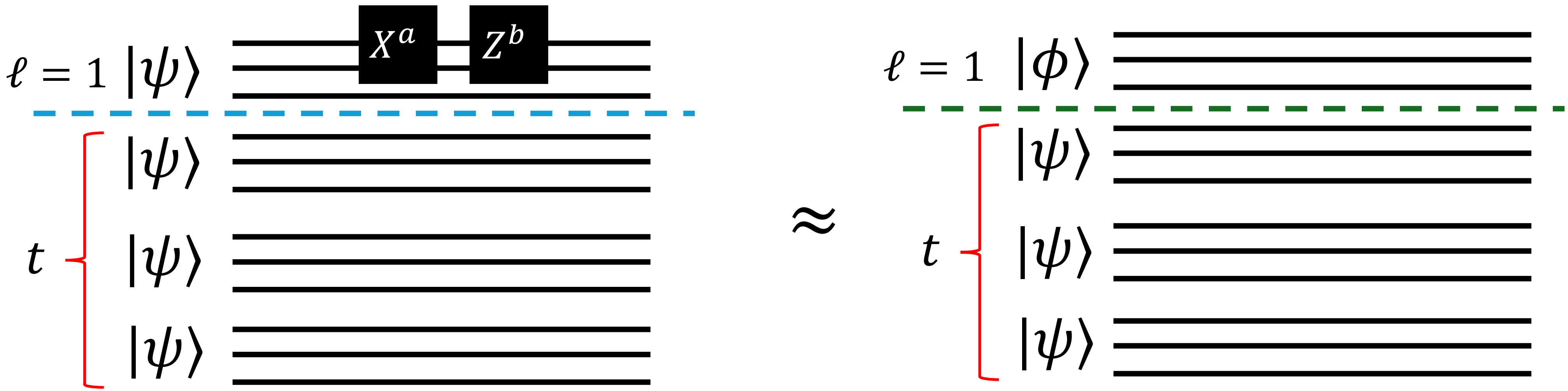
$\ell = 1$ $|\phi\rangle$



- $X^a Z^b |\psi\rangle$ is indistinguishable from a fresh Haar random state $|\phi\rangle$

Statistical 1-copy Security

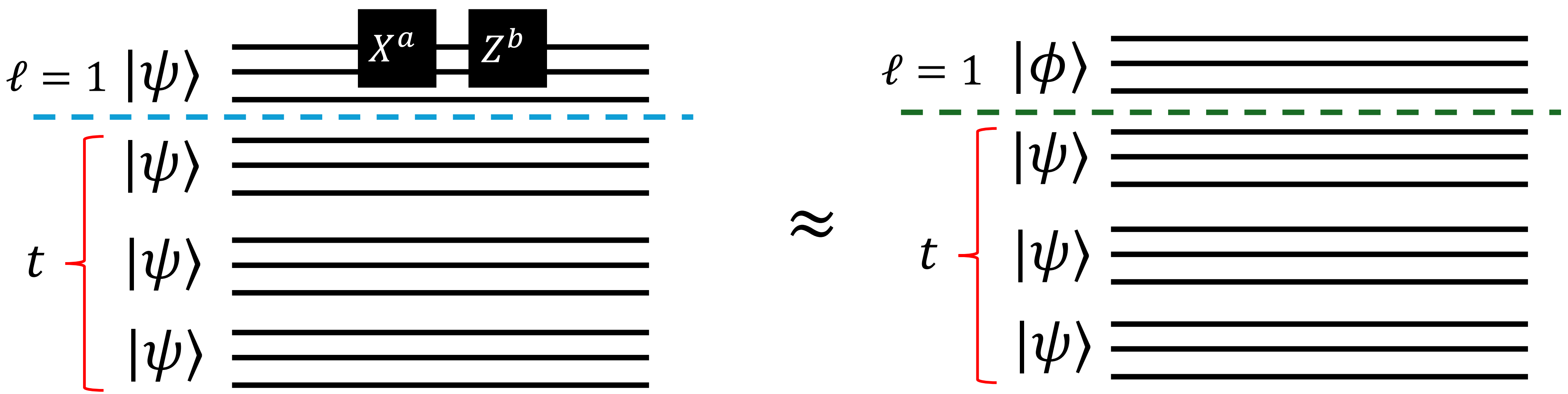
- What does 1-copy security mean *in the CHRS model*?



- $X^a Z^b |\psi\rangle$ is indistinguishable from a fresh Haar random state $|\phi\rangle$ **even given polynomially many copies of $|\psi\rangle$**

Statistical 1-copy Security

$\sigma = \mathbf{E}_{k,|\psi\rangle}[(X^a Z^b \otimes I)|\psi\rangle\langle\psi|(X^a Z^b \otimes I) \otimes |\psi\rangle\langle\psi|^{\otimes t}]$ $\quad$ $\boldsymbol{\rho} = \mathbf{E}[|\phi\rangle\langle\phi|] \otimes \mathbf{E}[|\psi\rangle\langle\psi|^{\otimes t}]$



- **We show:** Trace distance (quantum analog of TVD of distributions) between σ and ρ is $O(t^2/1.01^n)$
- **Approach:** Approximate σ and ρ with maximally entangled state

Approximating ρ

- t copies of an m-qubit Haar random state:

$$\mathbf{E}_{|\psi\rangle\leftarrow\mathrm{Haar}(2^n)}[|\psi\rangle\langle\psi|^{\otimes t}]$$

- t copies of random maximally entangled state :

$$\mathbf{E}_{U\leftarrow\mathrm{Haar}(2^{n/2})}[|\Phi_U\rangle\langle\Phi_U|^{\otimes t}]$$

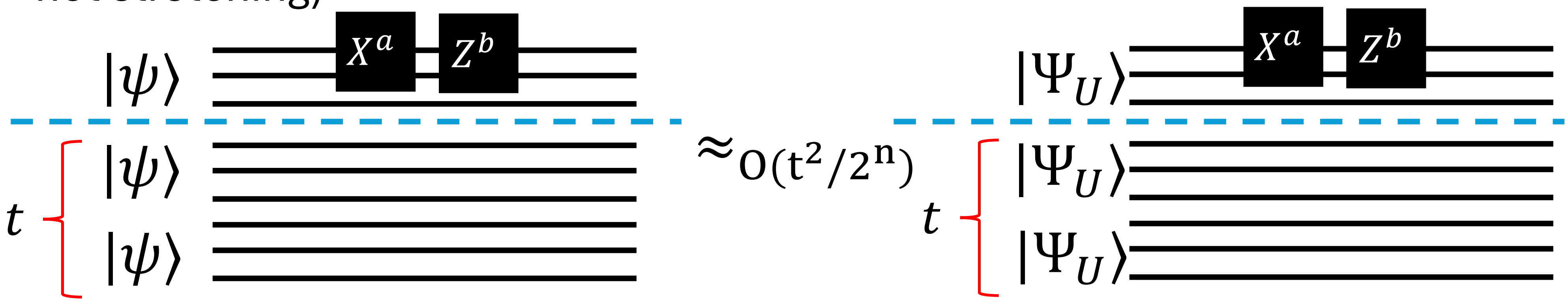
where $|\Phi_U\rangle = \frac{1}{\sqrt{2^{n/2}}}\sum_{i=0}^{2^{n/2}-1}(U\otimes I)|ii\rangle$

Lemma [Harrow 24]:

$$\mathbf{E}_{|\psi\rangle\leftarrow\mathrm{Haar}(2^m)}\left[|\psi\rangle\langle\psi|^{\otimes t}\right] \approx_{O(t^2/2^{n/2})} \mathbf{E}_{U\leftarrow\mathrm{Haar}(2^{n/2})}[|\Phi_U\rangle\langle\Phi_U|^{\otimes t}]$$

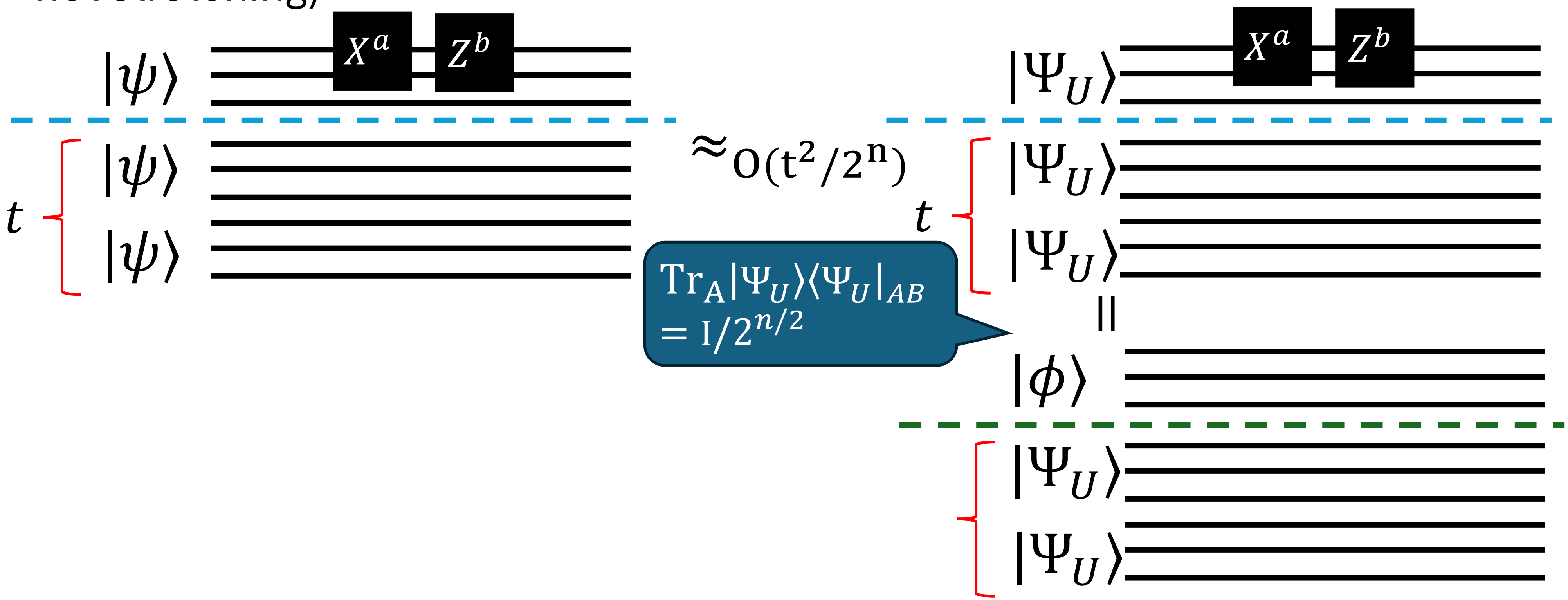
Secure 1PRS without stretching

- Firstly, we show that random Pauli on first $0.5n$ qubits is secure (although not stretching)



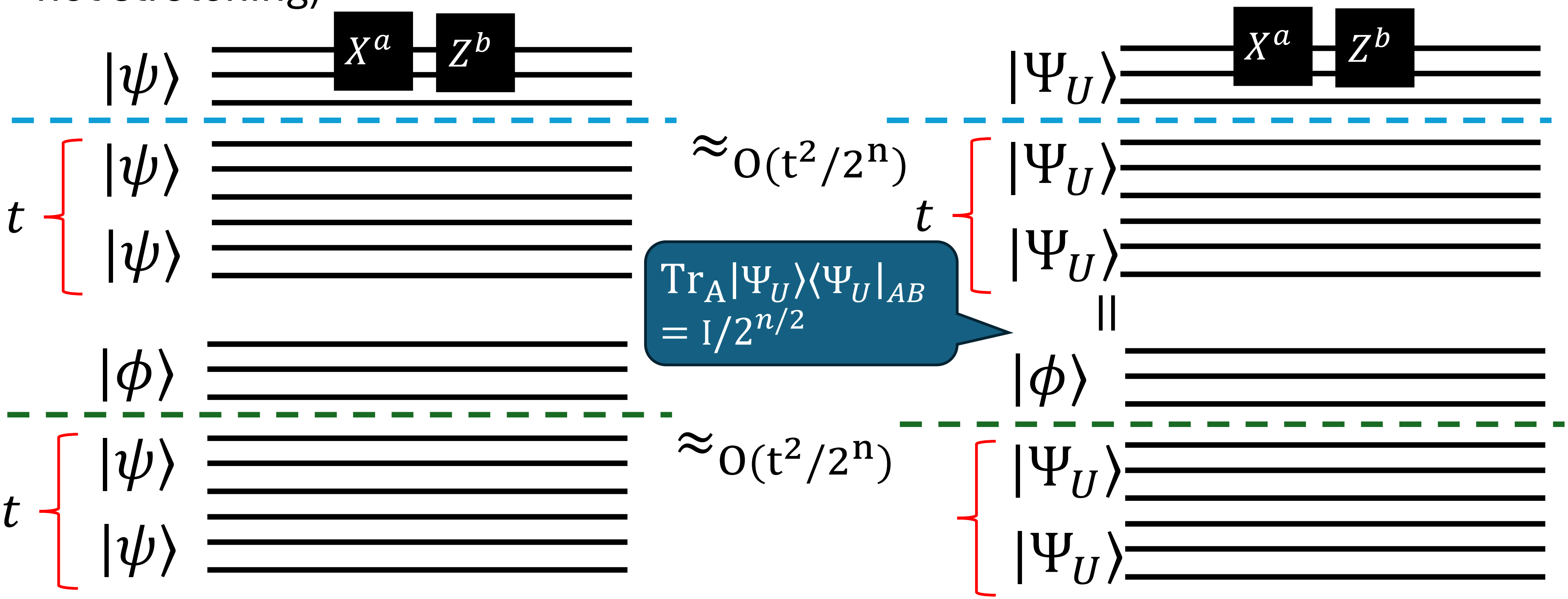
Secure 1PRS without stretching

- Firstly, we show that random Pauli on first $0.5n$ qubits is secure (although not stretching)



Secure 1PRS without stretching

- Firstly, we show that random Pauli on first $0.5n$ qubits is secure (although not stretching)



Reducing the key size

- Decompose common Haar random states according to the first qubit

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle|\psi_0\rangle + |1\rangle|\psi_1\rangle)$$

- Then, typically, $|\psi_0\rangle$ and $|\psi_1\rangle$ are close to two independent $(n-1)$-qubit Haar random states.

Reducing the key size

- Decompose common Haar random states according to the first qubit

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle|\psi_0\rangle + |1\rangle|\psi_1\rangle)$$

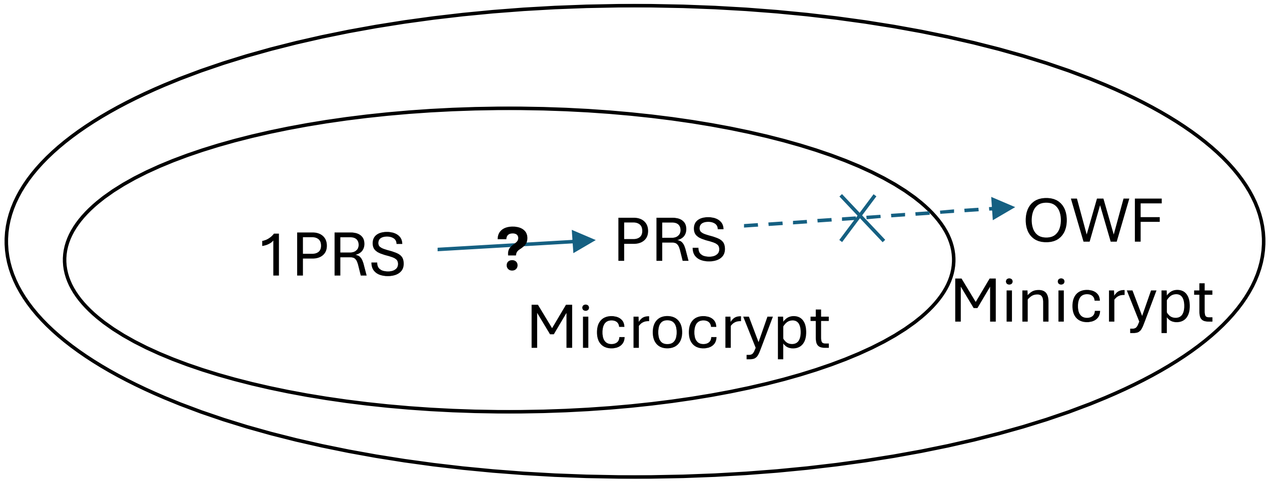
- Then, typically, $|\psi_0\rangle$ and $|\psi_1\rangle$ are close to two independent $(n-1)$-qubit Haar random states.
- **Key observation**: If $X^a Z^b$ maps $|\psi_0\rangle$ and $|\psi_1\rangle$, $|\psi_0\rangle \pm |\psi_1\rangle$, $|\psi_0\rangle \pm i|\psi_1\rangle$ to the maximally mixed state (approximately on average), then it must also map $|\psi\rangle$ to the maximally mixed state.

CHRS model and quantum crypto primitives

What we know: PRS do not imply OWF in a black-box way [Kretschmer 21, KQST 23], PRS imply quantum cryptography [AQY21, MY 21]

What we don't know: how 1-copy PRS and multi-copy PRS are related

The CHRS model helps answer this question

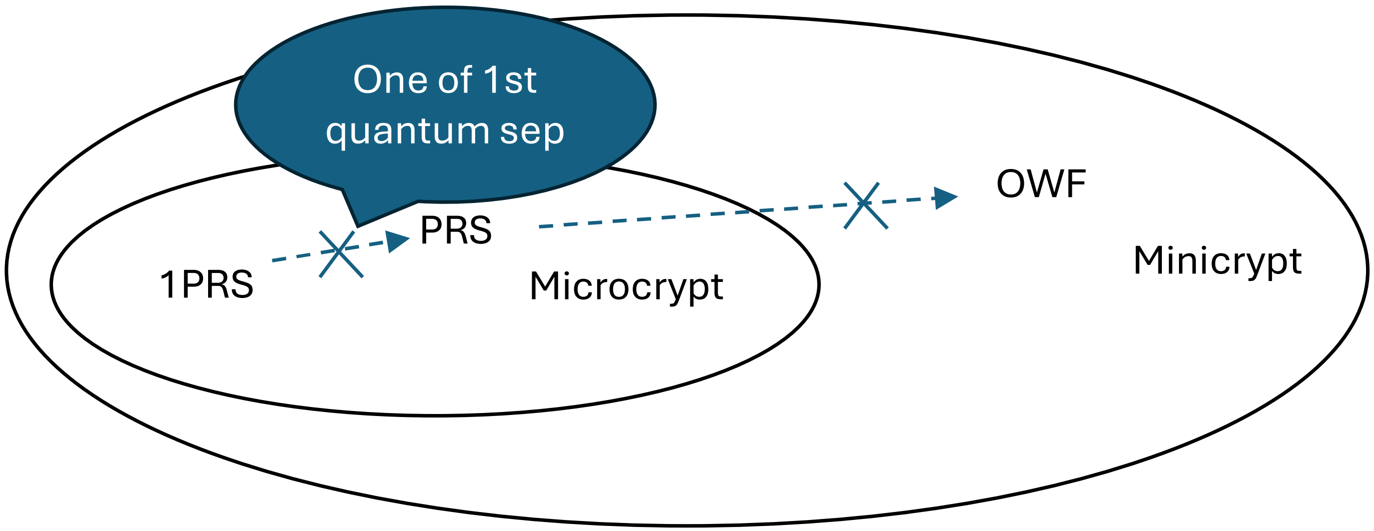


Black-box separation of 1PRS and PRS

Theorem

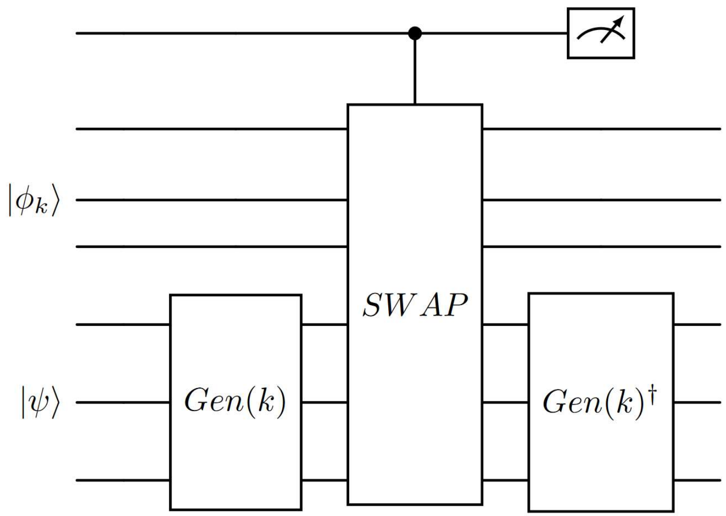
Relative to the following oracle, 1PRS exists while PRS does not:

- A family of common Haar random state $\{|\psi_n\rangle\}$
- A QPSPACE-complete oracle



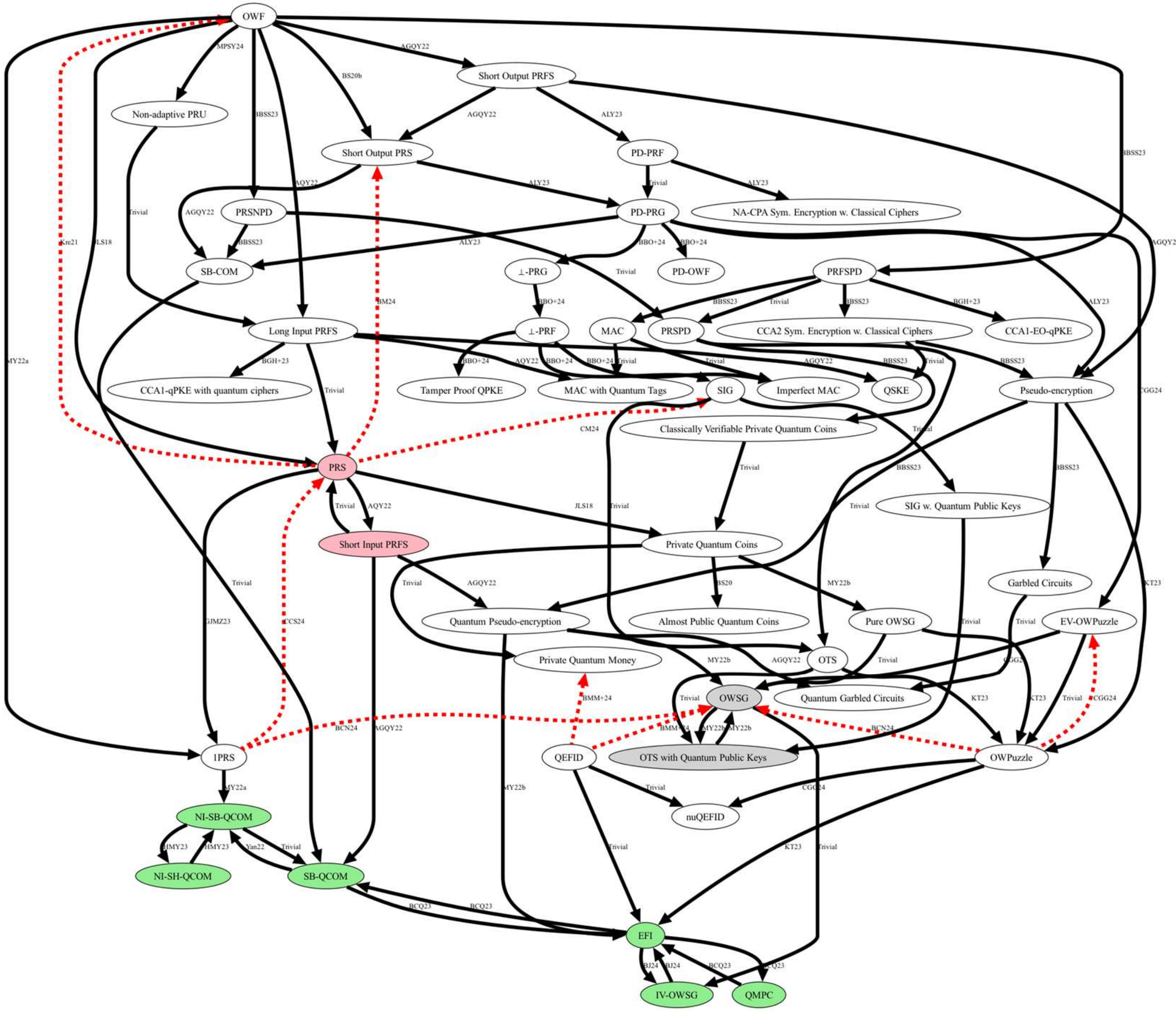
Generic attack on multi-copy PRS in the CHRS model

- Suppose $|\phi_k\rangle = Gen(k)|\psi\rangle$, consider the projector
$$\Lambda_k = (I \otimes Gen(k)^\dagger)SWAP(I \otimes Gen(k))$$
- $|\phi_k\rangle \otimes |\psi\rangle$ passes the test w.p. 1. A fresh random state $|\phi\rangle \otimes |\psi\rangle$ passes the test w.p. ~1/2. Thus $\Lambda_k^{\otimes 10n}$ provides an exponential gap between PRS and fresh Haar.
- Then use the quantum OR lemma $\Lambda_k^{\otimes 10n}$ for all k, we can distinguish PRS and Haar.



Concluding remarks

- Unlike classical settings, unconditional crypto exists in the presence of a common Haar random state.
- Follow-up work ([AGL24, BCN25, BMM+25, GZ25]): OWSG, classical communication commitment do not exist in the CHRS model, while EFID and one-way puzzles exist. The oracle can be lifted to a unitary oracle.
- Many other open questions.


OWF
Non-adaptive PRU
Short Output PRFS
Short Output PRS
PD-PRF
PRSNPD
PD-PRG
NA-CPA Sym. Encryption w. Classical Ciphers
SB-COM
⊥-PRG
PD-OWF
PRFSPD
Long Input PRFS
⊥-PRF
MAC
PRSPD
CCA2 Sym. Encryption w. Classical Ciphers
CCA1-EO-qPKE
CCA1-qPKE with quantum ciphers
Tamper Proof QPKE
MAC with Quantum Tags
SIG
Imperfect MAC
QSKE
Pseudo-encryption
Classically Verifiable Private Quantum Coins
PRS
SIG w. Quantum Public Keys
Short Input PRFS
Private Quantum Coins
Garbled Circuits
Quantum Pseudo-encryption
Almost Public Quantum Coins
Pure OWSG
EV-OWPuzzle
Private Quantum Money
OTS
OWSG
Quantum Garbled Circuits
1PRS
QEFID
OTS with Quantum Public Keys
OWPuzzle
NI-SB-QCOM
nuQEFID
NI-SH-QCOM
SB-QCOM
EFI
IV-OWSG
QMPC