# Pseudorandom Isometries

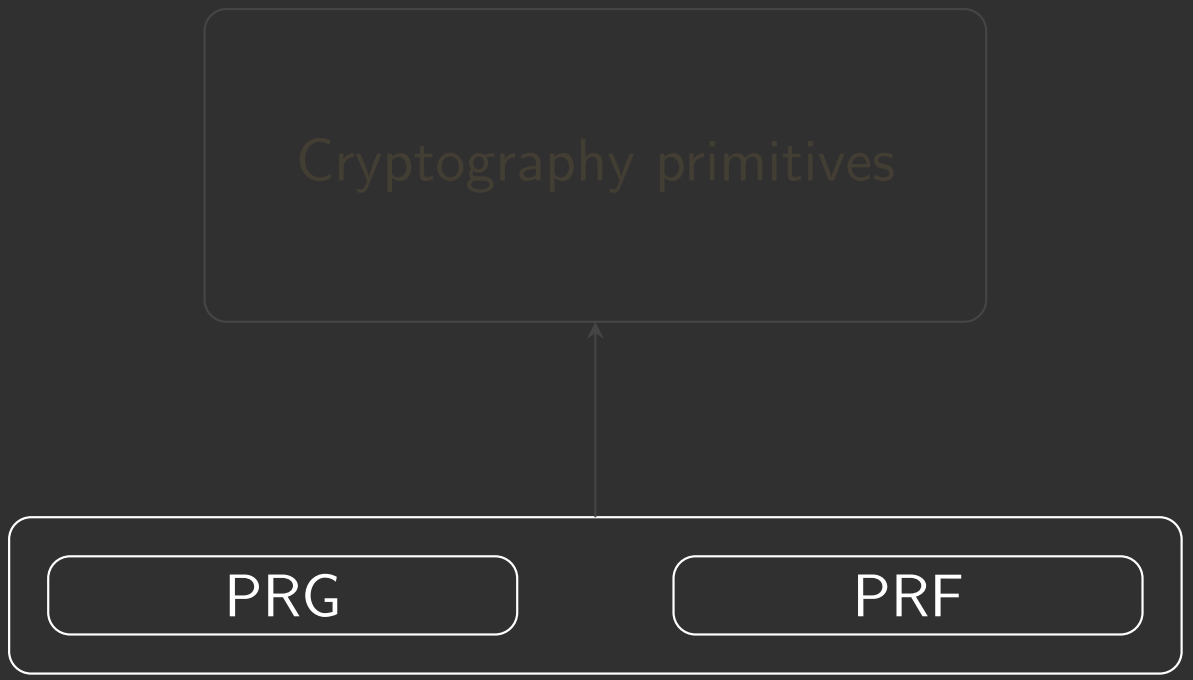
Prabhanjan Ananth (UCSB),
Aditya Gulati (UCSB),
Fatih Kaleoglu (UCSB),
Yao-Ting Lin (UCSB)

Eurocrypt 2024

May 27, 2024

# Pseudorandomness

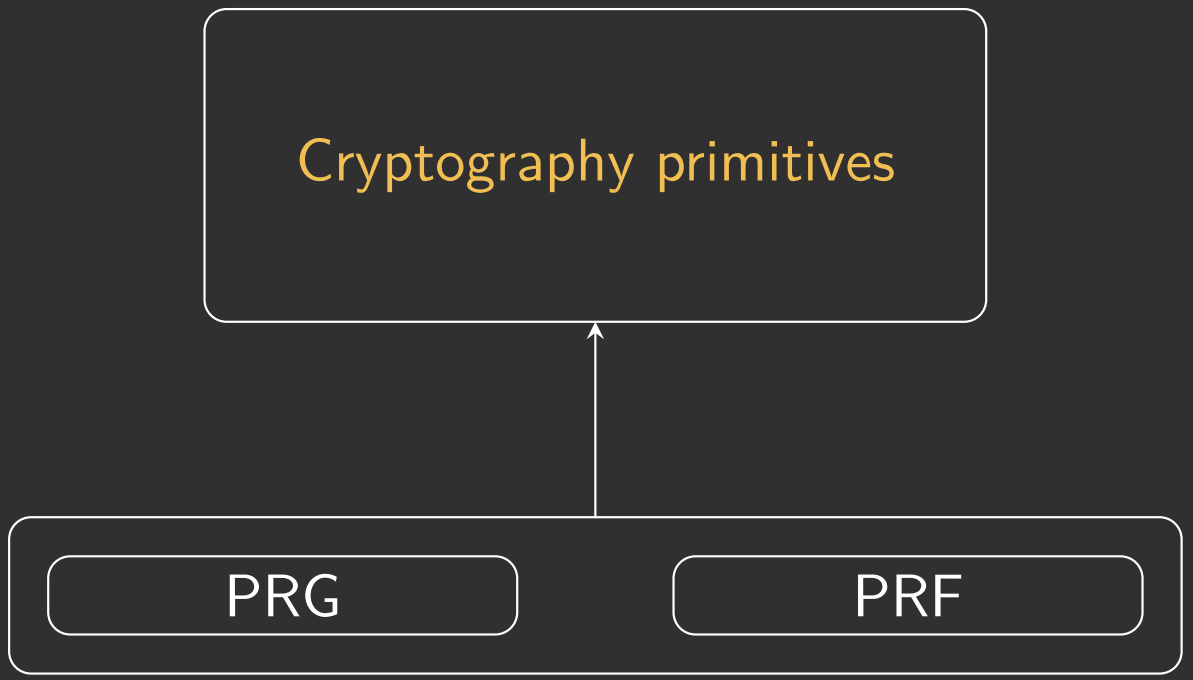
## Classical




## Quantum ?

# Pseudorandomness

## Classical

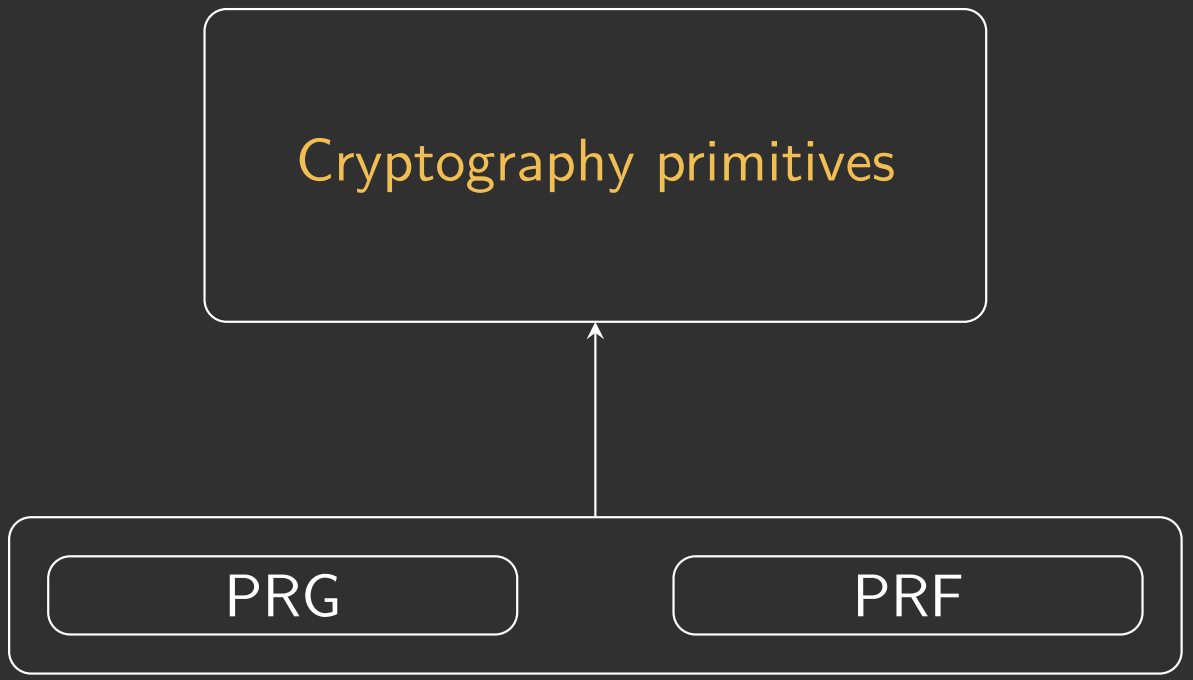



## Quantum

?

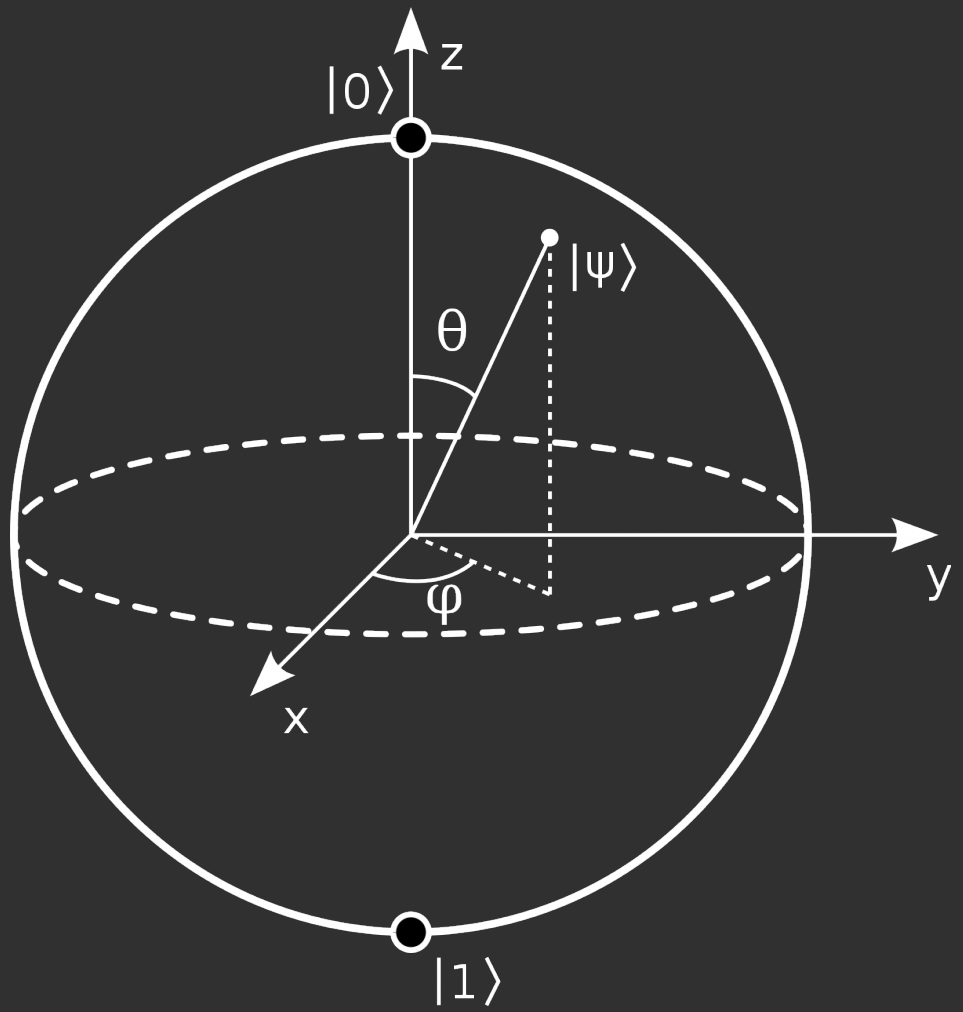
# Pseudorandomness

## Classical



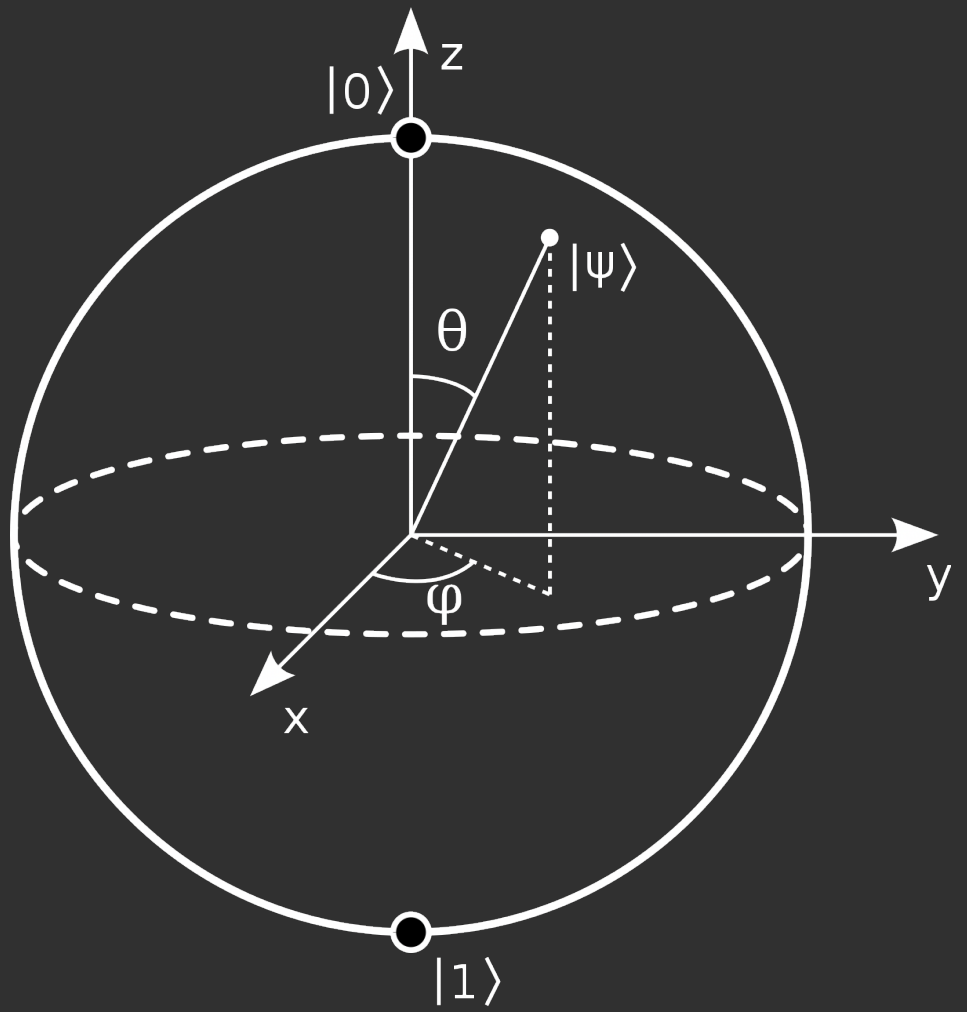

## Quantum ?

# Haar Random State




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

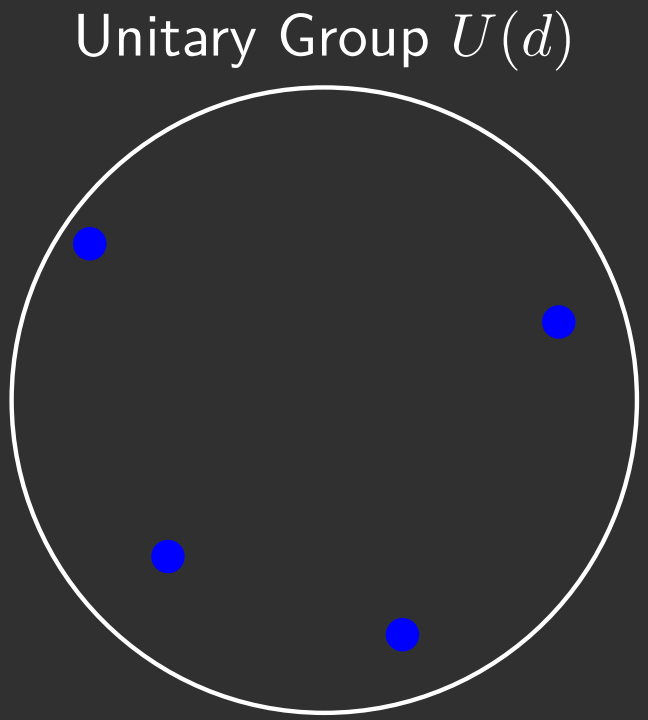
# Haar Random State




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

# Haar Random Unitaries

## Haar Random Unitaries



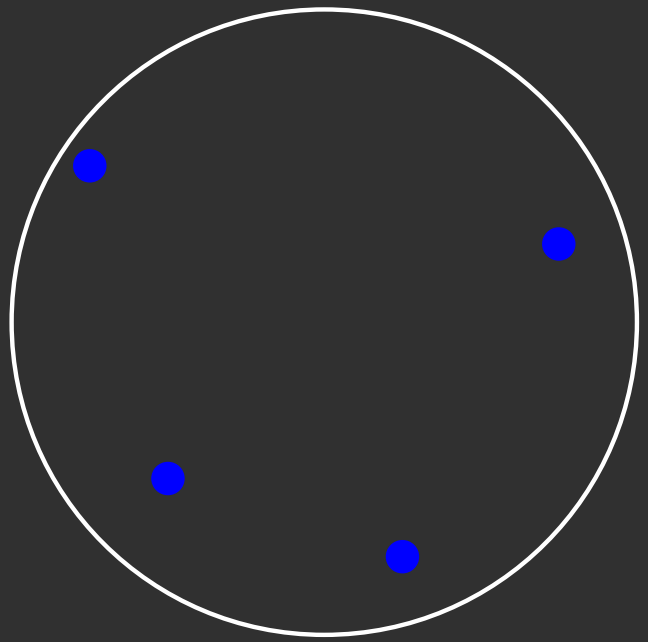

**Haar Random Unitary** "looks like" it is picked uniformly from the unitary group $U(d)$.

Figure: Haar measure on $U(d)$

# Haar Random Unitaries

## Haar Random Unitaries

Unitary Group $U(d)$



Uniform Distribution

**Property: Invariance**

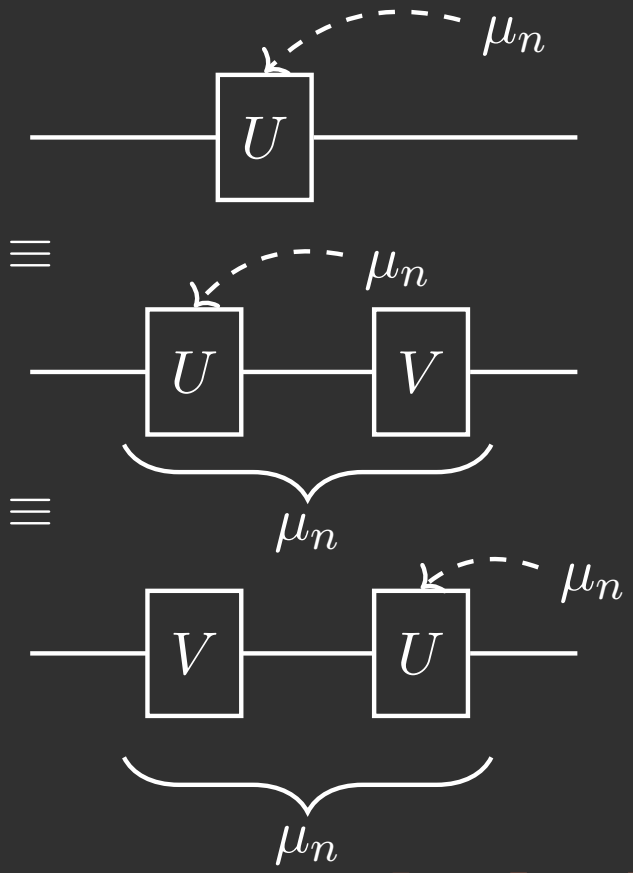



Figure: Haar measure on $U(d)$

# Quantum Pseudorandomness

## States

Pseudorandom States (PRS)

(JLS18,BS19,BS20,...)

Pseudorandom Function-like States (PRFS)

(AQY22,AGQY22,BBSS23,...)

## Operations

Pseudorandom Unitaries (PRU)

(JLS18,HBK23,MPSY24,...)

Pseudorandom State Scramblers (PRSS)

(LQS+23,...)

# Quantum Pseudorandomness

## States

Pseudorandom States (PRS)

(JLS18,BS19,BS20,...)

Pseudorandom Function-like States (PRFS)

(AQY22,AGQY22,BBSS23,...)

## Operations

Pseudorandom Unitaries (PRU)

(JLS18,HBK23,MPSY24,...)

Pseudorandom State Scramblers (PRSS)

(LQS+23,...)

# Quantum Pseudorandomness

## States

Pseudorandom States (PRS)

(JLS18,BS19,BS20,...)

Pseudorandom Function-like States (PRFS)

(AQY22,AGQY22,BBSS23,...)

## Operations

Pseudorandom Unitaries (PRU)

(JLS18,HBK23,MPSY24,...)

Pseudorandom State Scramblers (PRSS)

(LQS+23,...)

# Quantum Pseudorandomness

**Pseudorandom States (PRS)**

(JLS18,BS19,BS20,...)

**Pseudorandom Unitaries (PRU)**

(JLS18,HBK23,MPSY24,...)

**Applications:**

- Crypto from Minimal Assumptions

  (Kre20,...)
- QML (HBC+21,...)
- AdS/CFT

  (BFV19,...)

**Pseudorandom Function-like States (PRFS)**

(AQY22,AGQY22,BBSS23,...)

**Pseudorandom State Scramblers (PRSS)**

(LQS+23,...)

# Quantum Pseudorandomness

Pseudorandom States (PRS)

(JLS18,BS19,BS20,...)

Pseudorandom Unitaries (PRU)

(JLS18,HBK23,MPSY24,...)

Applications:

- Crypto from Minimal Assumptions (Kre20,...)
- QML (HBC+21,...)
- AdS/CFT (BFV19,...)

Pseudorandom Function-like States (PRFS)

(AQY22,AGQY22,BBSS23,...)

Pseudorandom State Scramblers (PRSS)

(LQS+23,...)

# Quantum Pseudorandomness

Pseudorandom States (PRS)

(JLS18,BS19,BS20,...)

Applications:

- Crypto from Minimal Assumptions

  (Kre20,...)
- QML (HBC+21,...)
- AdS/CFT

  (BFV19,...)

Pseudorandom Unitaries (PRU)

(JLS18,HBK23,MPSY24,...)

Pseudorandom Function-like States (PRFS)

(AQY22,AGQY22,BBSS23,...)

Pseudorandom State Scramblers (PRSS)

(LQS+23,...)

# Quantum Pseudorandomness

Pseudorandom States (PRS)

(JLS18,BS19,BS20,...)

Pseudorandom Unitaries (PRU)

(JLS18,HBK23,MPSY24,...)

Can we find a systematic method to analyse these primitives?

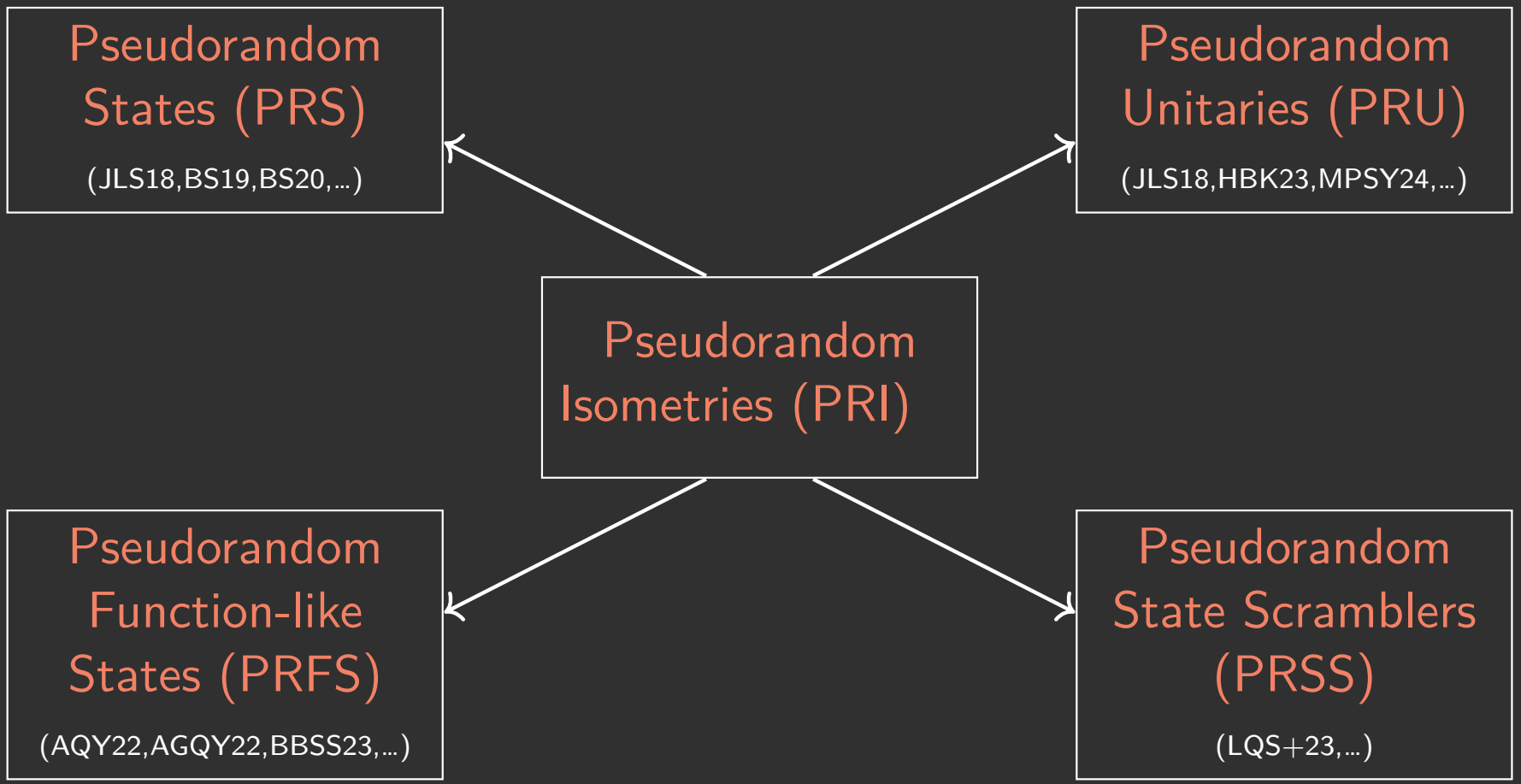
Pseudorandom Function-like States (PRFS)

(AQY22,AGQY22,BBSS23,...)

Pseudorandom State Scramblers (PRSS)

(LQS+23,...)

# Quantum Pseudorandomness



# Results

- **Pseudorandom Isometries (PRI):** Definition and framework to study other primitives.
- **Almost Invariance:** A technique to prove psuedorandomness.
- **Construction:** Using OWF to achieve PRI.
- **Applications:**
  - Length Extension Theorem
  - Quantum Message Authentication Codes (MACs)
  - Multi-copy secure encryption schemes
  - Succinct quantum commitments

# Results

- **Pseudorandom Isometries (PRI):** Definition and framework to study other primitives.
- **Almost Invariance:** A technique to prove psuedorandomness.
- **Construction:** Using OWF to achieve PRI.
- **Applications:**
  - Length Extension Theorem
  - Quantum Message Authentication Codes (MACs)
  - Multi-copy secure encryption schemes
  - Succinct quantum commitments

# Results

- **Pseudorandom Isometries (PRI):** Definition and framework to study other primitives.
- **Almost Invariance:** A technique to prove psuedorandomness.
- **Construction:** Using OWF to achieve PRI.
- **Applications:**
  - Length Extension Theorem
  - Quantum Message Authentication Codes (MACs)
  - Multi-copy secure encryption schemes
  - Succinct quantum commitments

# Results

- **Pseudorandom Isometries (PRI):** Definition and framework to study other primitives.
- **Almost Invariance:** A technique to prove psuedorandomness.
- **Construction:** Using OWF to achieve PRI.
- **Applications:**
  - Length Extension Theorem
  - Quantum Message Authentication Codes (MACs)
  - Multi-copy secure encryption schemes
  - Succinct quantum commitments

# Pseudorandom Isometries

## What are Pseudorandom Isometries?

# Haar Random Isometries

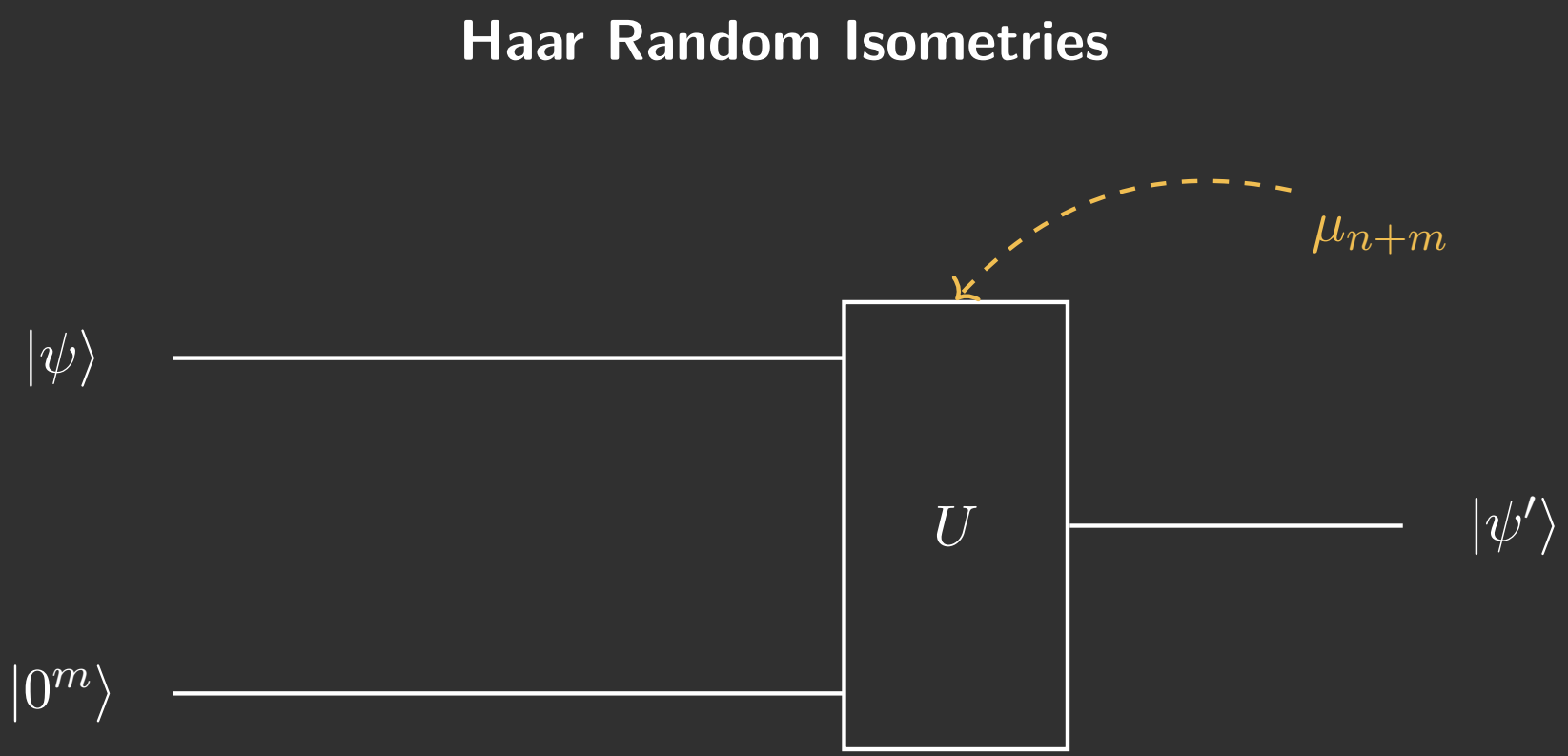


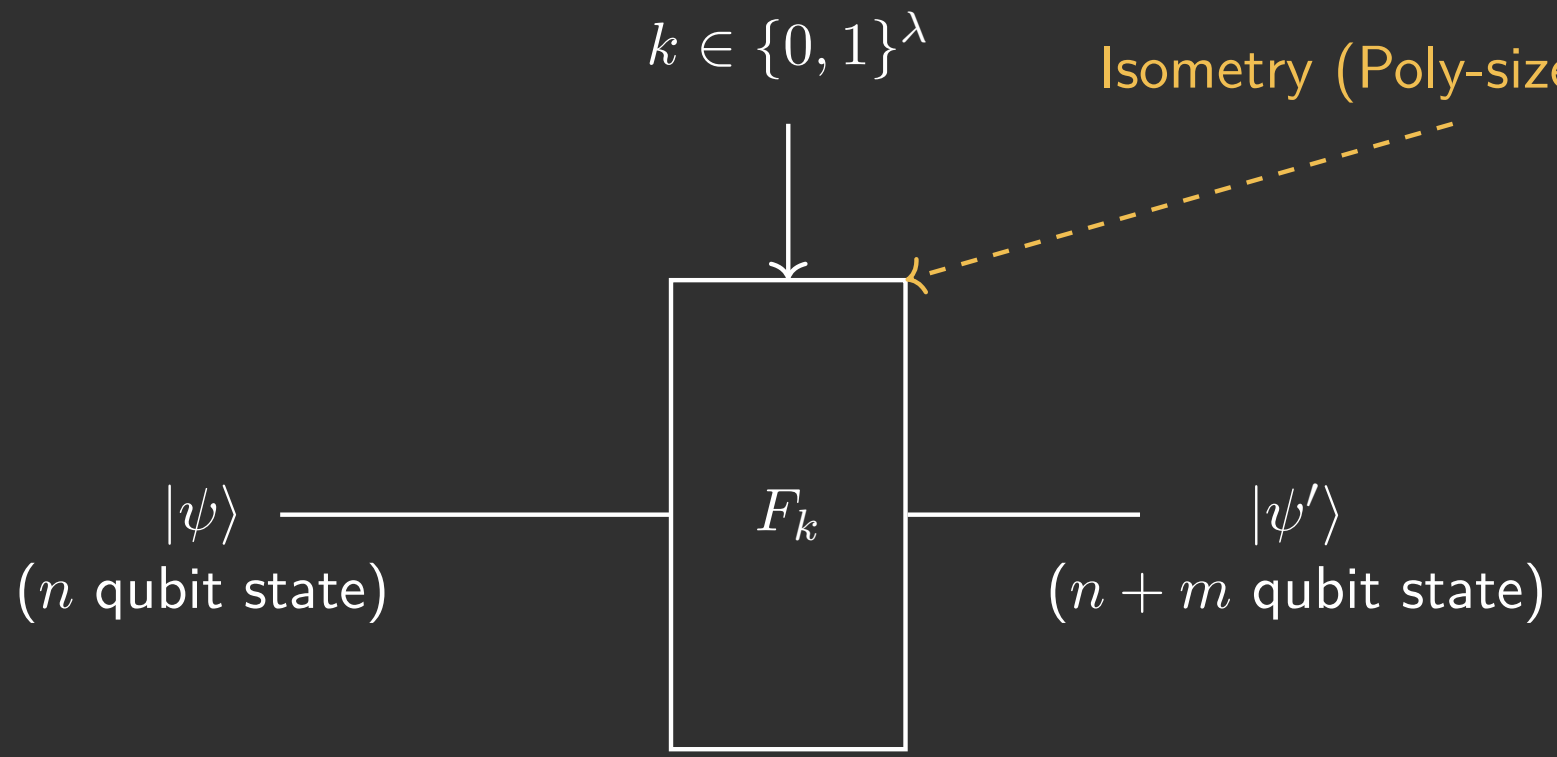

Figure: Quantum circuit representation of Haar isometries

# Pseudorandom Isometries (PRI)

Efficiently implementable circuits that "behave like" Haar random isometries.

# Pseudorandom Isometries (PRI)

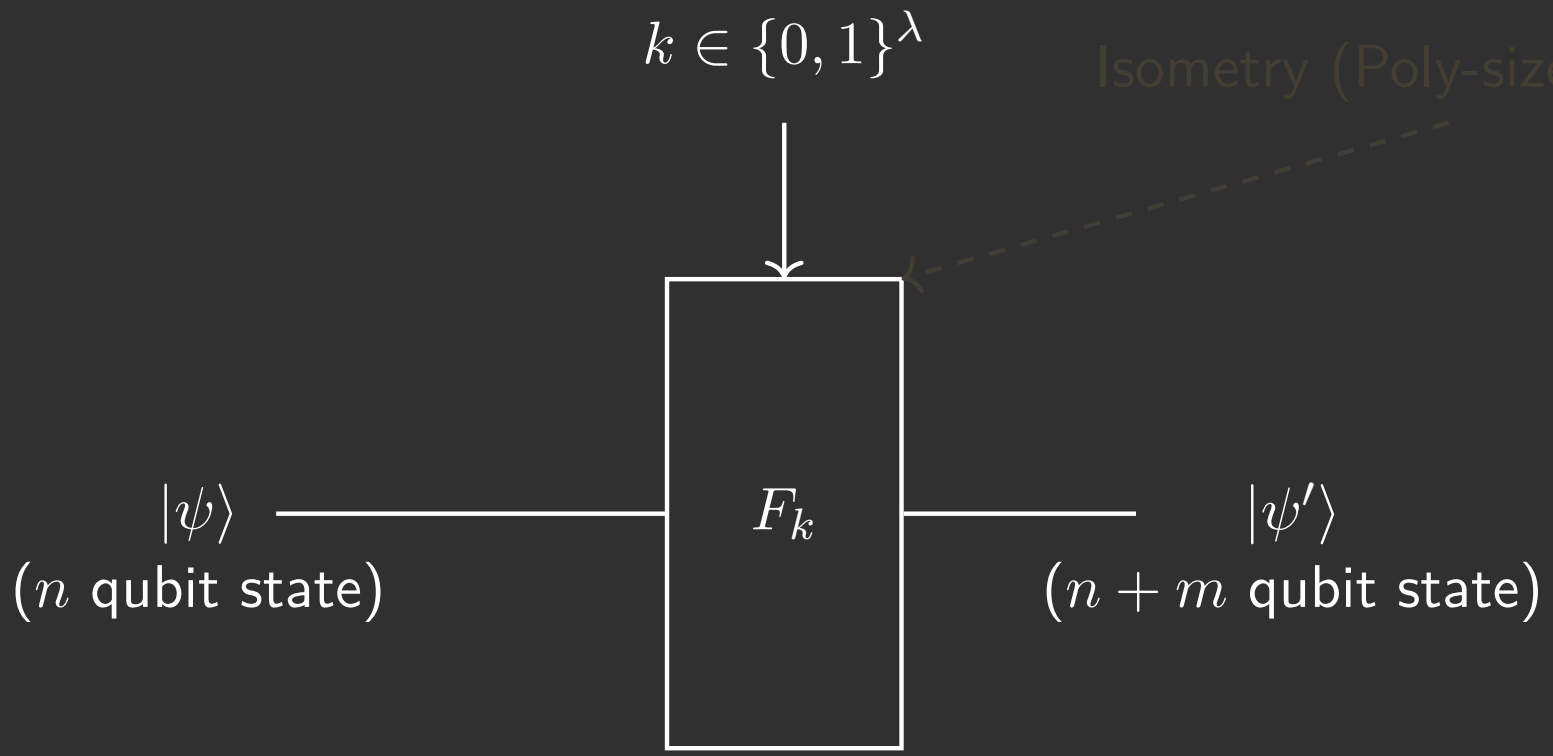
1. Efficient implementation:




Notation: $(n, n+m)$-$PRI$

# Pseudorandom Isometries (PRI)

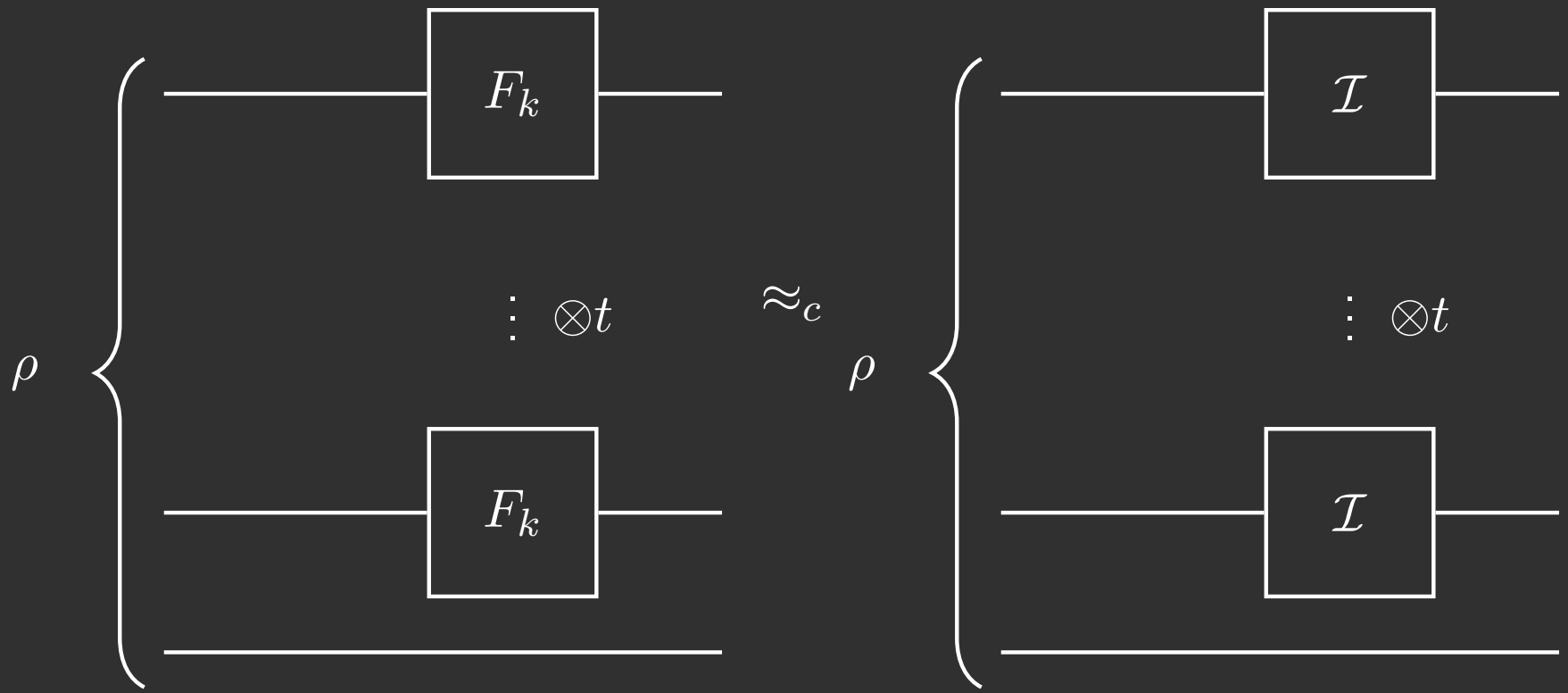
1. Efficient implementation:




Notation: $(n, n+m)$-$PRI$

# Pseudorandom Isometries (PRI)

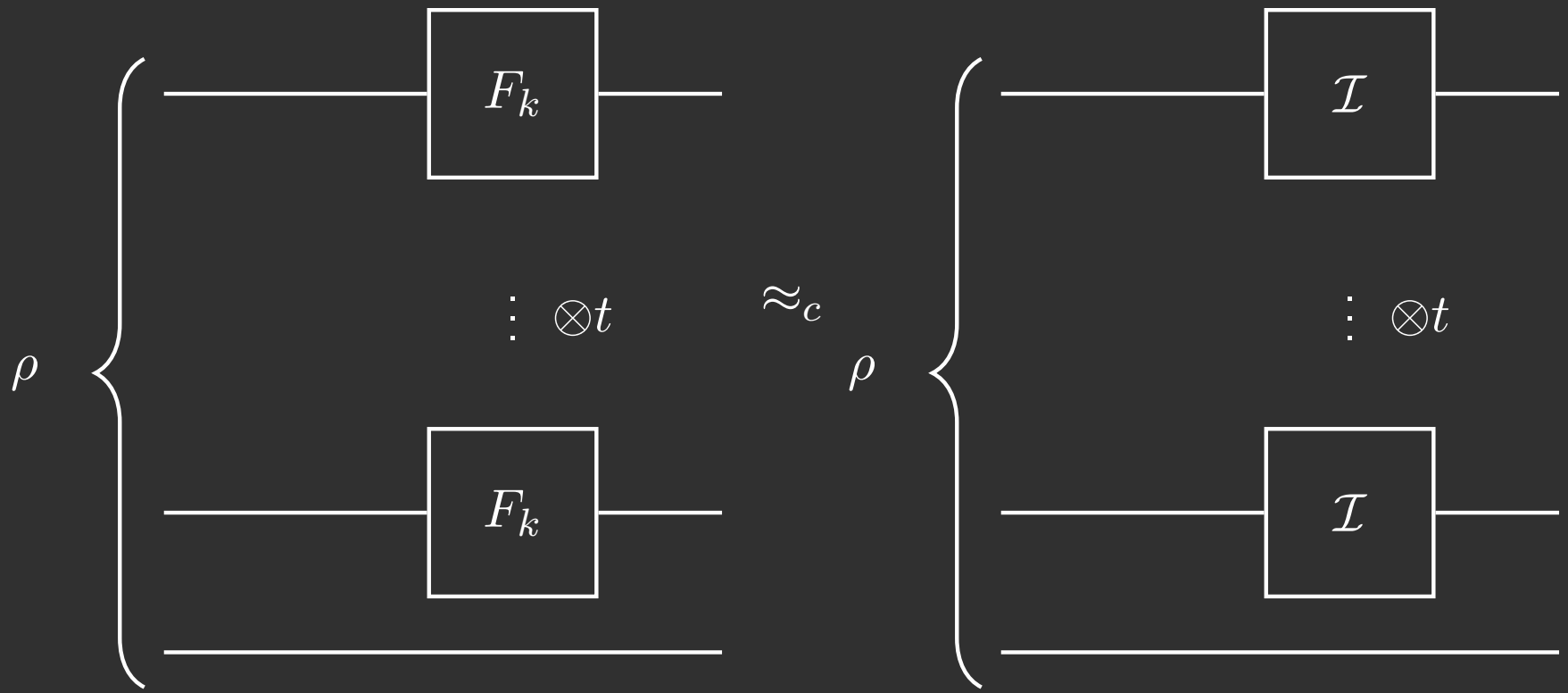
2. $\mathcal{Q}$-security: $\rho \in \mathcal{Q}$




Notation: $(n, n+m)$-$\mathcal{Q}$-secure-$PRI$

# Pseudorandom Isometries (PRI)

2. $\mathcal{Q}$-security: $\rho \in \mathcal{Q}$




Notation: $(n, n+m)$-$\mathcal{Q}$-secure-$PRI$

# PRI as a Framework to Analyze Other Primitives

How are Pseudorandom Isometries related to other primitives?

# Relationship with Other Primitives

## Relationship with Other Primitives

- **Pseudorandom States:**
  PRI secure on $|0^n\rangle$ is a PRS.

$$\mathcal{Q} = \{|0^n\rangle^{\otimes t}\}$$

- **Pseudorandom State Scrambler:**
  PRI on $t$-tensor same state is a PRSS.

$$\mathcal{Q} = \{|\psi\rangle^{\otimes t} : |\psi\rangle \text{ is an } n\text{-qubit state}\}$$

- **Pseudorandom Function-like States:**
  PRI secure on computation basis states is a PRFS.

$$\mathcal{Q} = \{\otimes_{i=1}^{t} |x_i\rangle : x_i \in \{0,1\}^n\}.$$

- **PRU:**
  - $(n, n)$-PRI is a PRU.
  - PRU implies PRI.

# Relationship with Other Primitives

## Relationship with Other Primitives

- **Pseudorandom States:**
  PRI secure on $|0^n\rangle$ is a PRS.

$$\mathcal{Q} = \{|0^n\rangle^{\otimes t}\}$$

- **Pseudorandom State Scrambler:**
  PRI on $t$-tensor same state is a PRSS.

$$\mathcal{Q} = \{|\psi\rangle^{\otimes t} : |\psi\rangle \text{ is an } n\text{-qubit state}\}$$

- **Pseudorandom Function-like States:**
  PRI secure on computation basis states is a PRFS.

$$\mathcal{Q} = \{\otimes_{i=1}^{t} |x_i\rangle : x_i \in \{0,1\}^n\}.$$

- **PRU:**
  - $(n, n)$-PRI is a PRU.
  - PRU implies PRI.

# Relationship with Other Primitives

## Relationship with Other Primitives

- **Pseudorandom States:**
  PRI secure on $|0^n\rangle$ is a PRS.

$$\mathcal{Q} = \{|0^n\rangle^{\otimes t}\}$$

- **Pseudorandom State Scrambler:**
  PRI on $t$-tensor same state is a PRSS.

$$\mathcal{Q} = \{|\psi\rangle^{\otimes t} : |\psi\rangle \text{ is an } n\text{-qubit state}\}$$

- **Pseudorandom Function-like States:**
  PRI secure on computation basis states is a PRFS.

$$\mathcal{Q} = \{\otimes_{i=1}^{t} |x_i\rangle : x_i \in \{0,1\}^n\}.$$

- **PRU:**
  - $(n, n)$-PRI is a PRU.
  - PRU implies PRI.

# Relationship with Other Primitives

## Relationship with Other Primitives

- **Pseudorandom States:**
  PRI secure on $|0^n\rangle$ is a PRS.

$$\mathcal{Q} = \{|0^n\rangle^{\otimes t}\}$$

- **Pseudorandom State Scrambler:**
  PRI on $t$-tensor same state is a PRSS.

$$\mathcal{Q} = \{|\psi\rangle^{\otimes t} : |\psi\rangle \text{ is an } n\text{-qubit state}\}$$

- **Pseudorandom Function-like States:**
  PRI secure on computation basis states is a PRFS.

$$\mathcal{Q} = \{\otimes_{i=1}^{t} |x_i\rangle : x_i \in \{0,1\}^n\}.$$

- **PRU:**
  - $(n, n)$-PRI is a PRU.
  - PRU implies PRI.

# Almost Invariance Implies Security

How do we analyse Pseudorandomness of PRIs (and other primitives)?

# Almost Invariance Implies Security

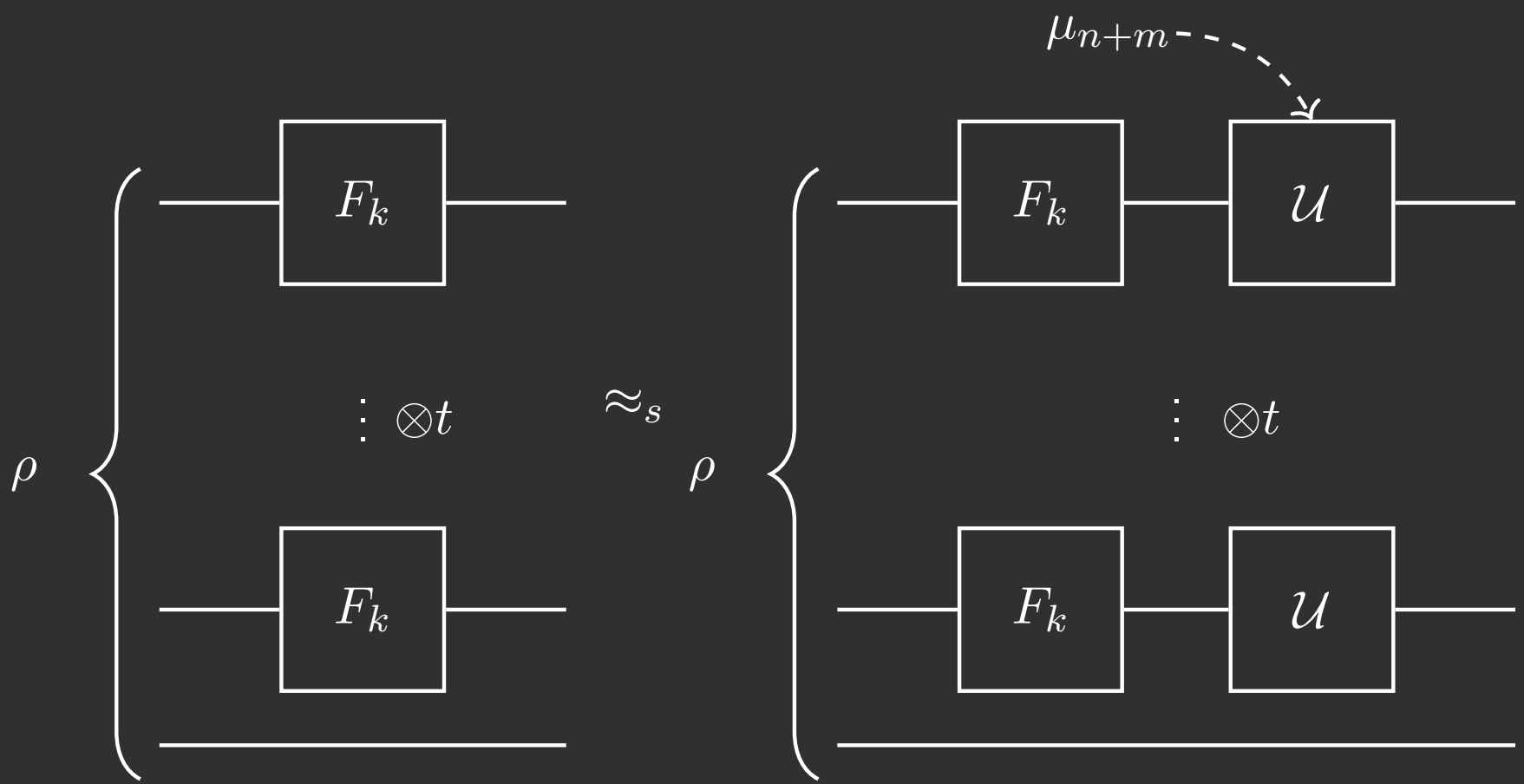
**Intuition: The output of Pseudorandom primitives are "maximally scrambled", hence applying $t$-fold Haar shouldn't change it much.**

# Almost Invariance Implies Security

**Almost Invariance implies security: If the output of a Pseudorandom primitive is invariant under $t$-fold Haar Unitary, then the Pseudorandom primitive is secure.**

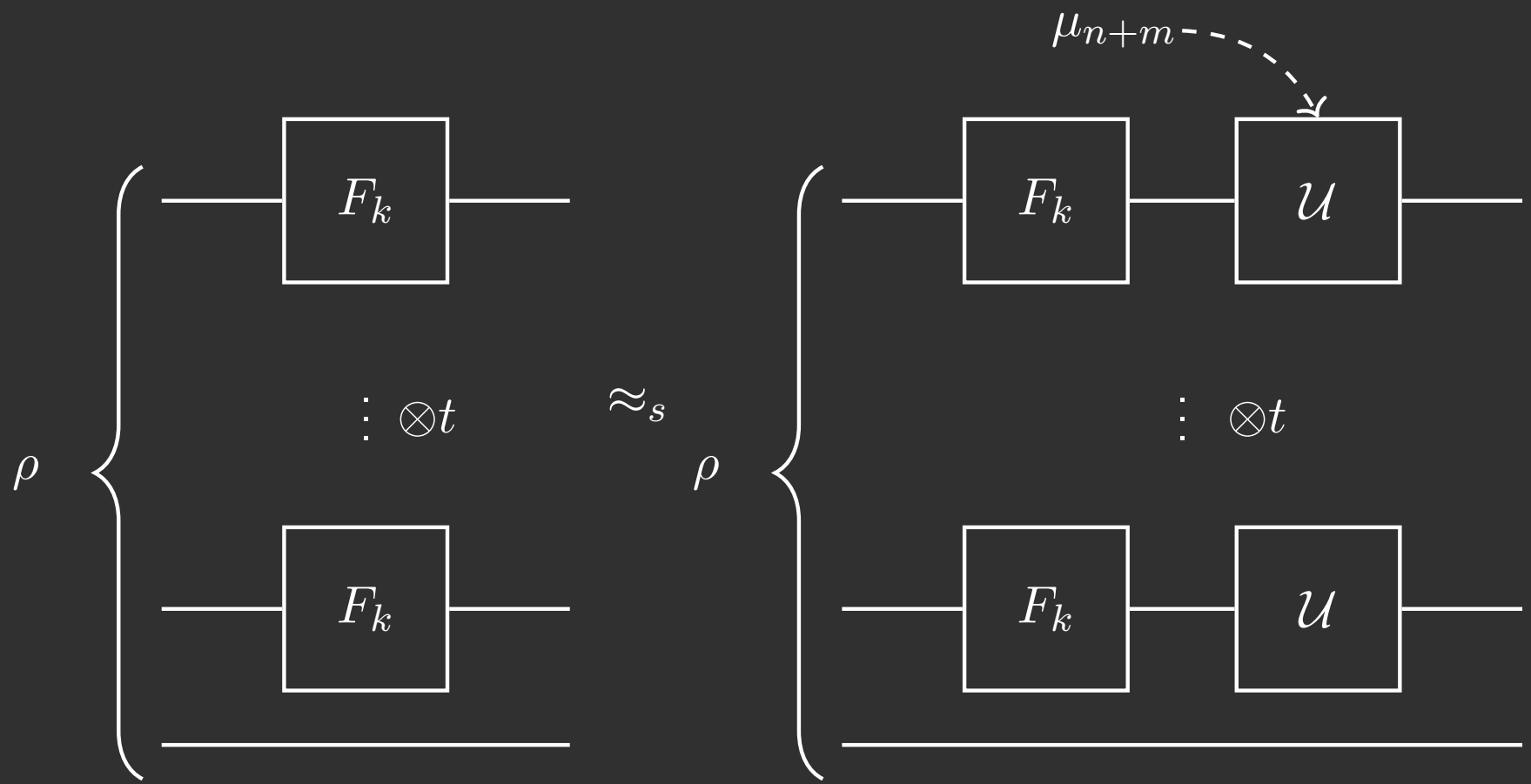
# Almost Invariance Implies Security

PRI is $\mathcal{Q}$-secure iff $\rho \in \mathcal{Q}$



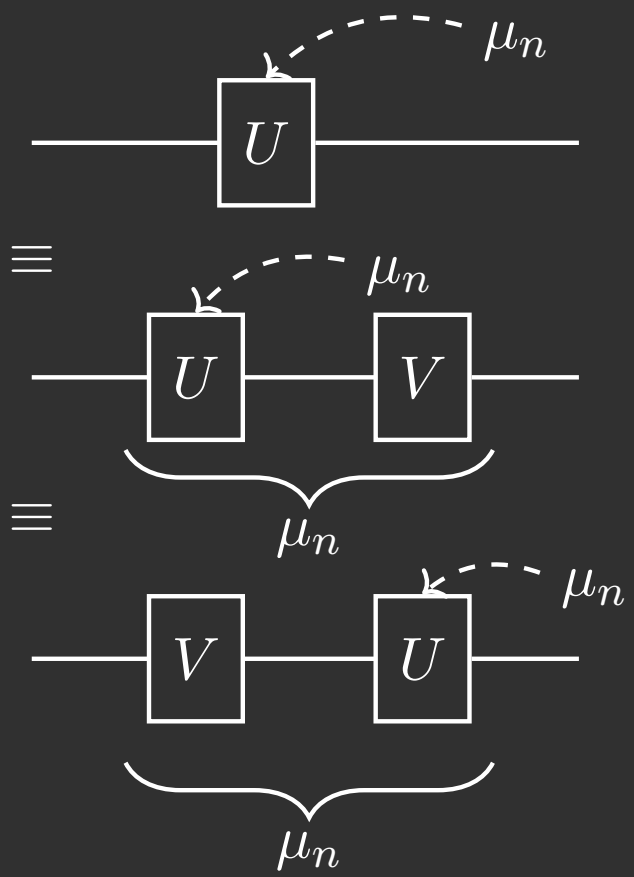
# Almost Invariance Implies Security

PRI is $\mathcal{Q}$-secure iff $\rho \in \mathcal{Q}$ (Used by BM'24 (subsequent work) to prove pseudorandomness of PRU's.)

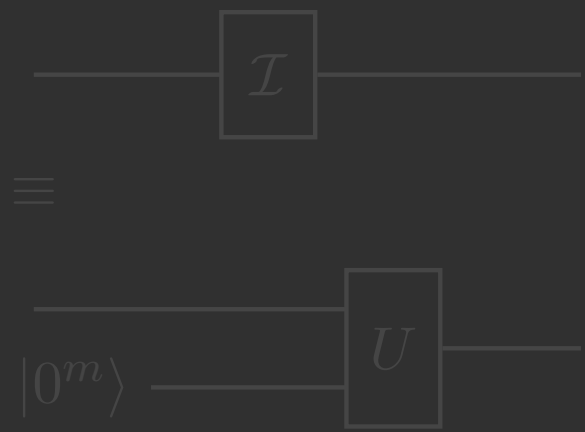


# Proof of Almost Invariance Implies Security

## Recall: Haar Invariance

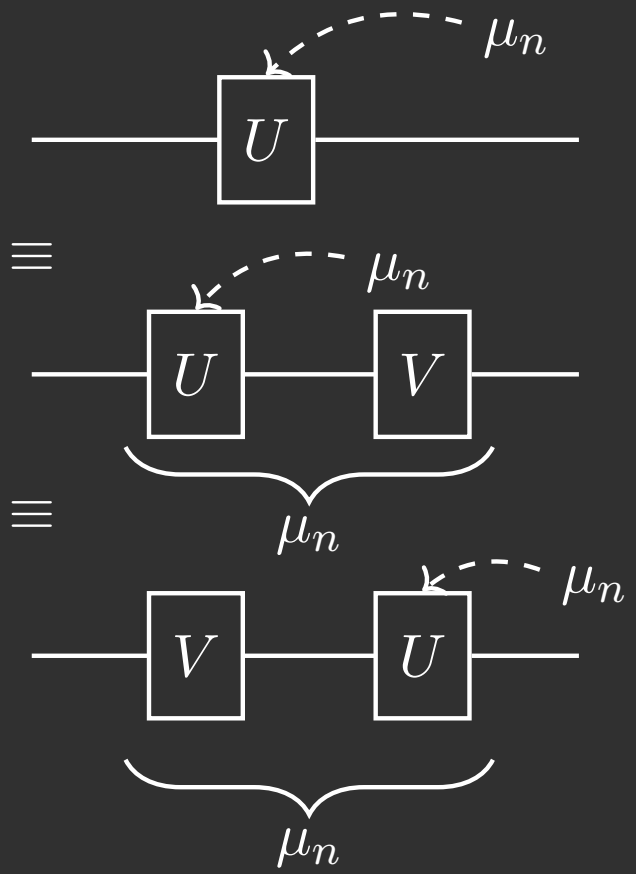



## Isometry definition

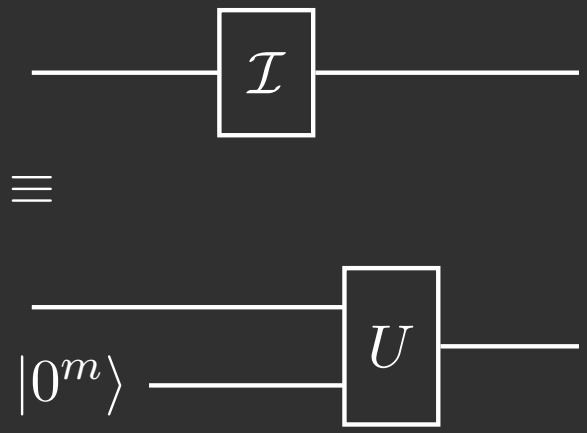


# Proof of Almost Invariance Implies Security

**Recall: Haar Invariance**

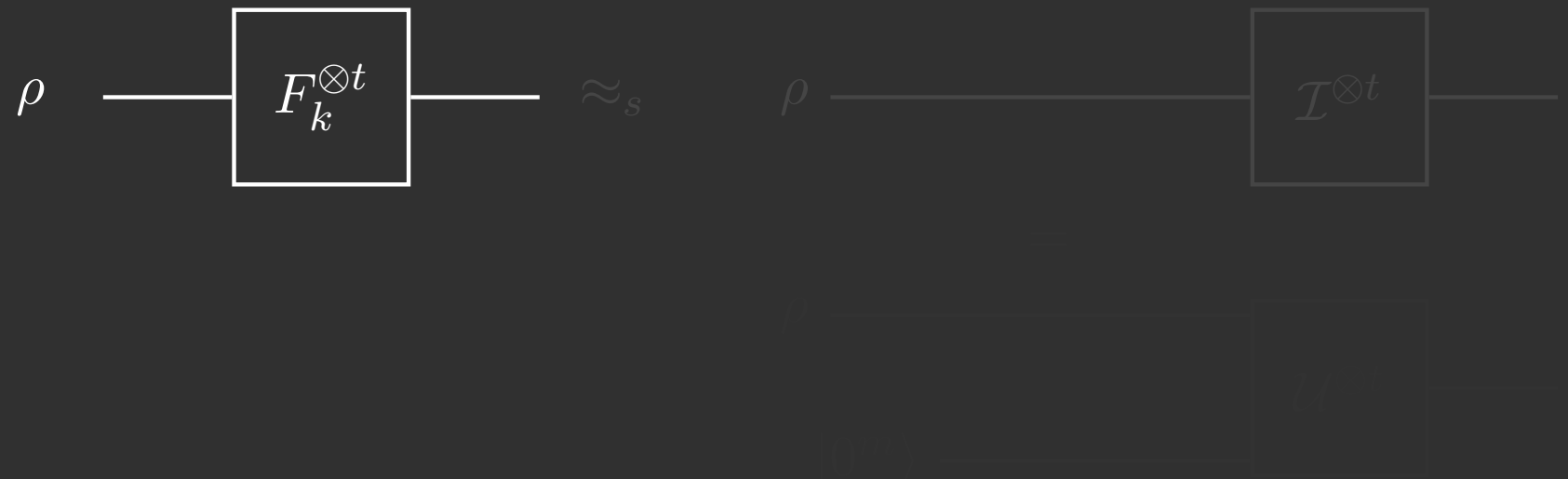



**Isometry definition**



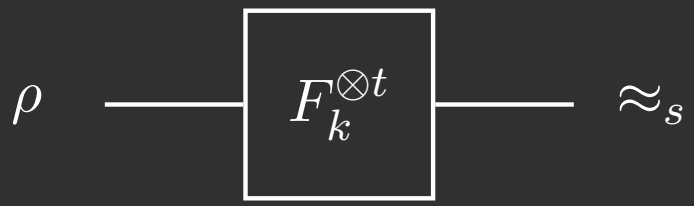
# Proof of Almost Invariance Implies Security

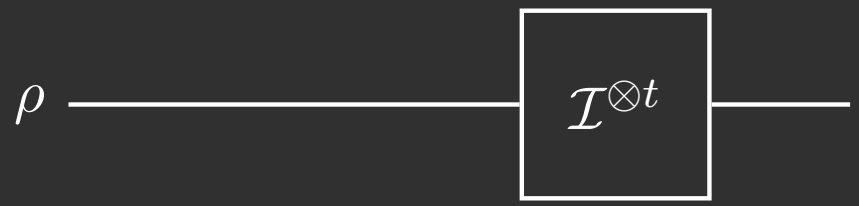
PRI is $\mathcal{Q}$-secure iff $\rho \in \mathcal{Q}$

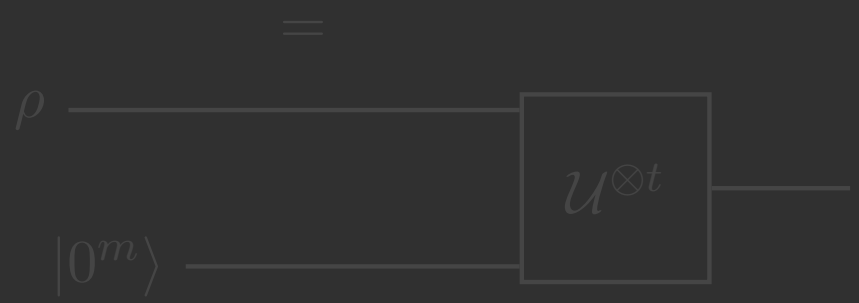


# Proof of Almost Invariance Implies Security

PRI is $\mathcal{Q}$-secure iff $\rho \in \mathcal{Q}$

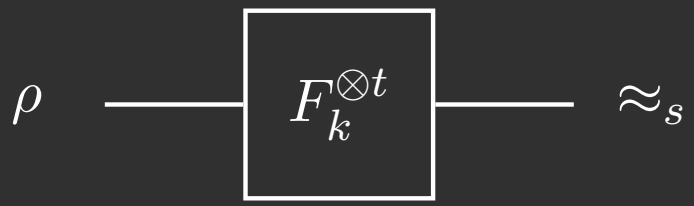


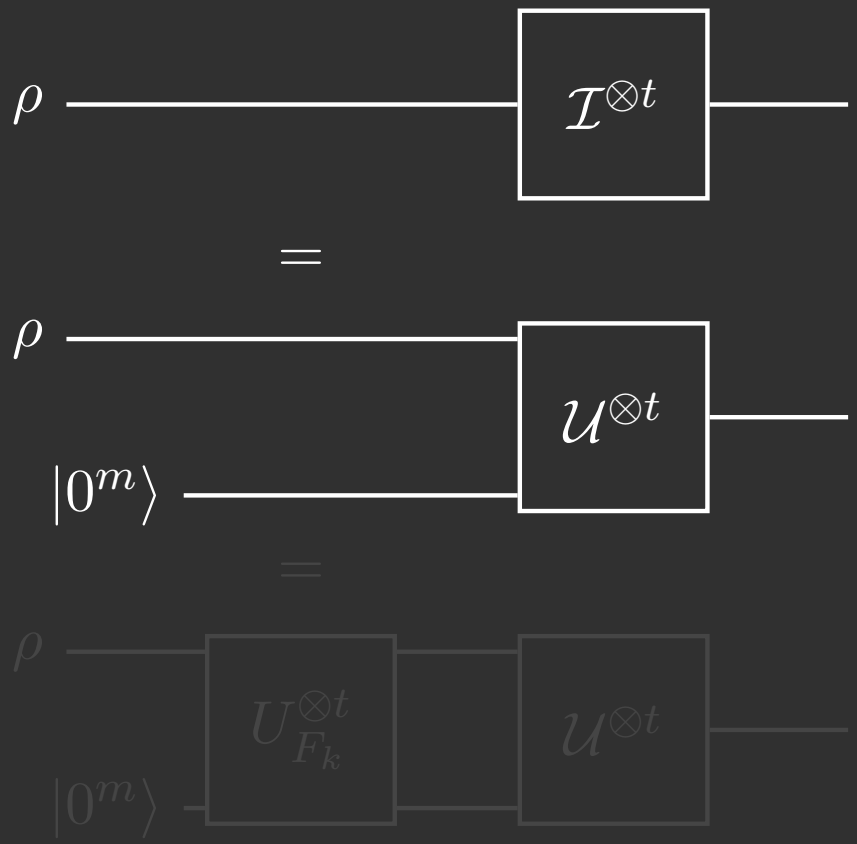



# Proof of Almost Invariance Implies Security

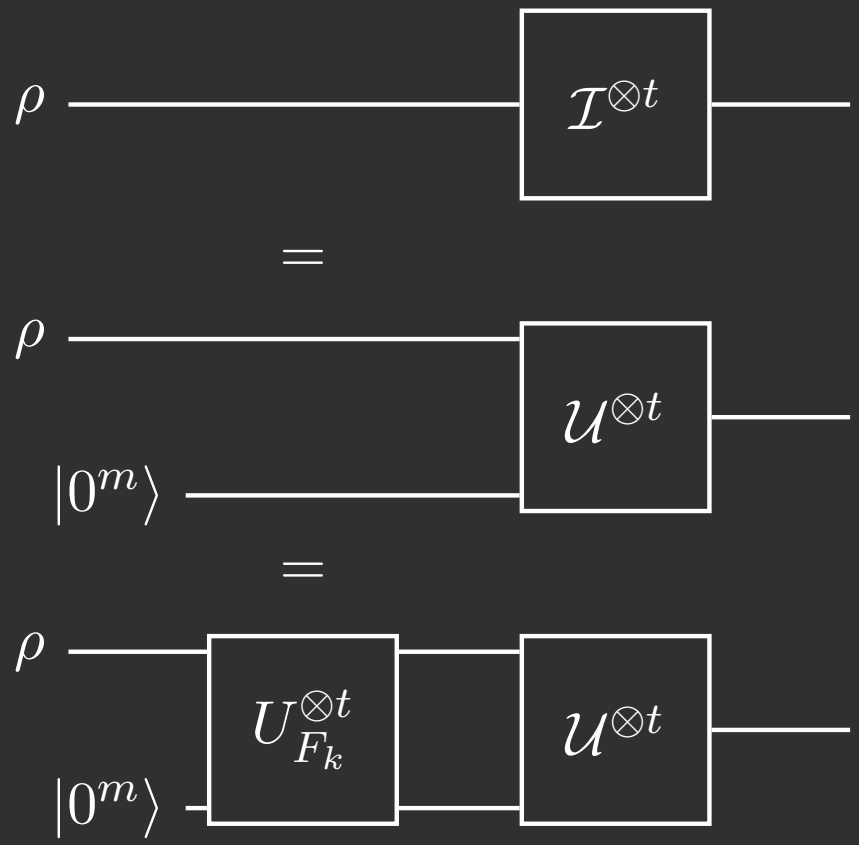
PRI is $\mathcal{Q}$-secure iff $\rho \in \mathcal{Q}$



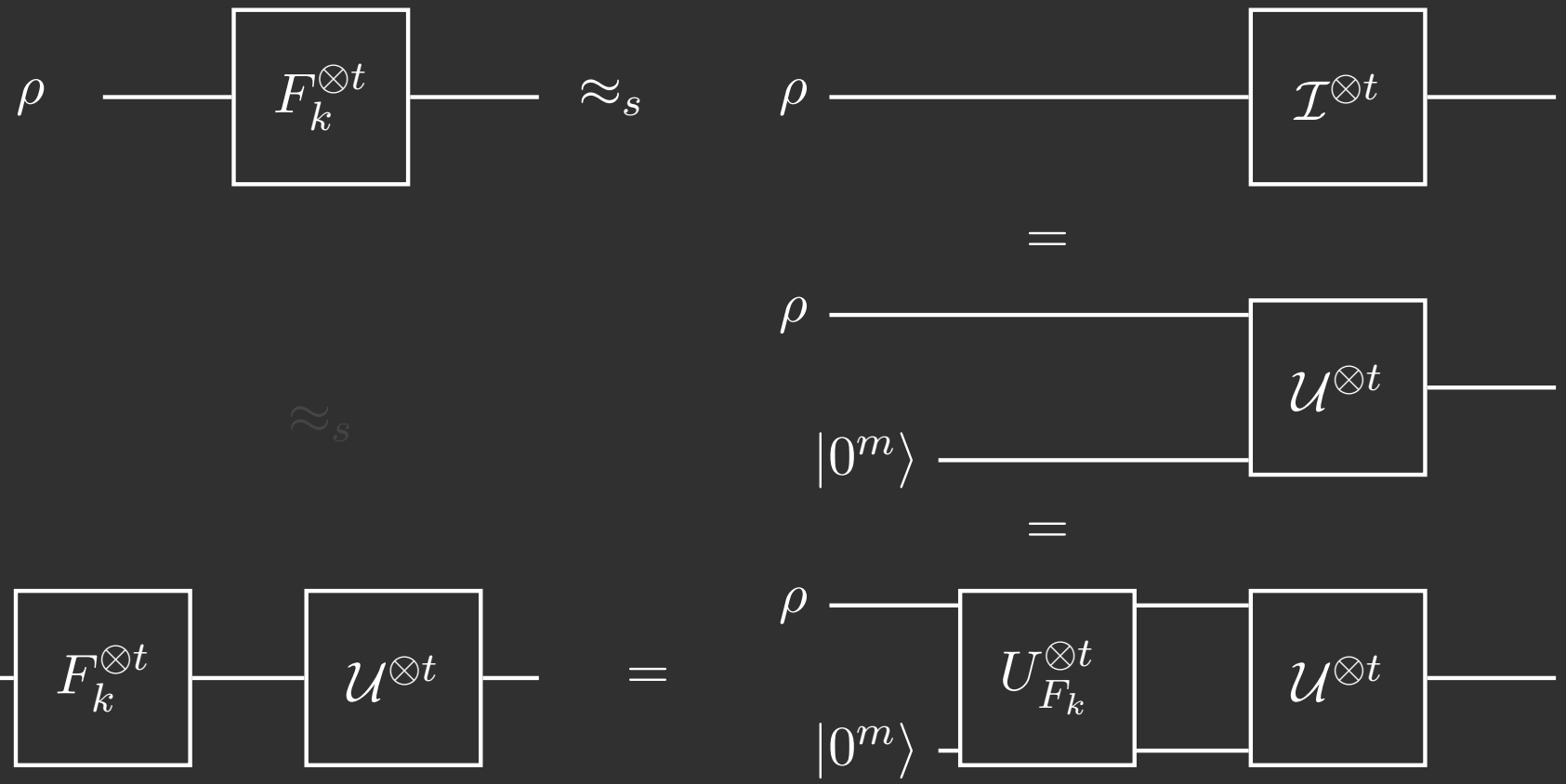
# Proof of Almost Invariance Implies Security

PRI is $\mathcal{Q}$-secure iff $\rho \in \mathcal{Q}$

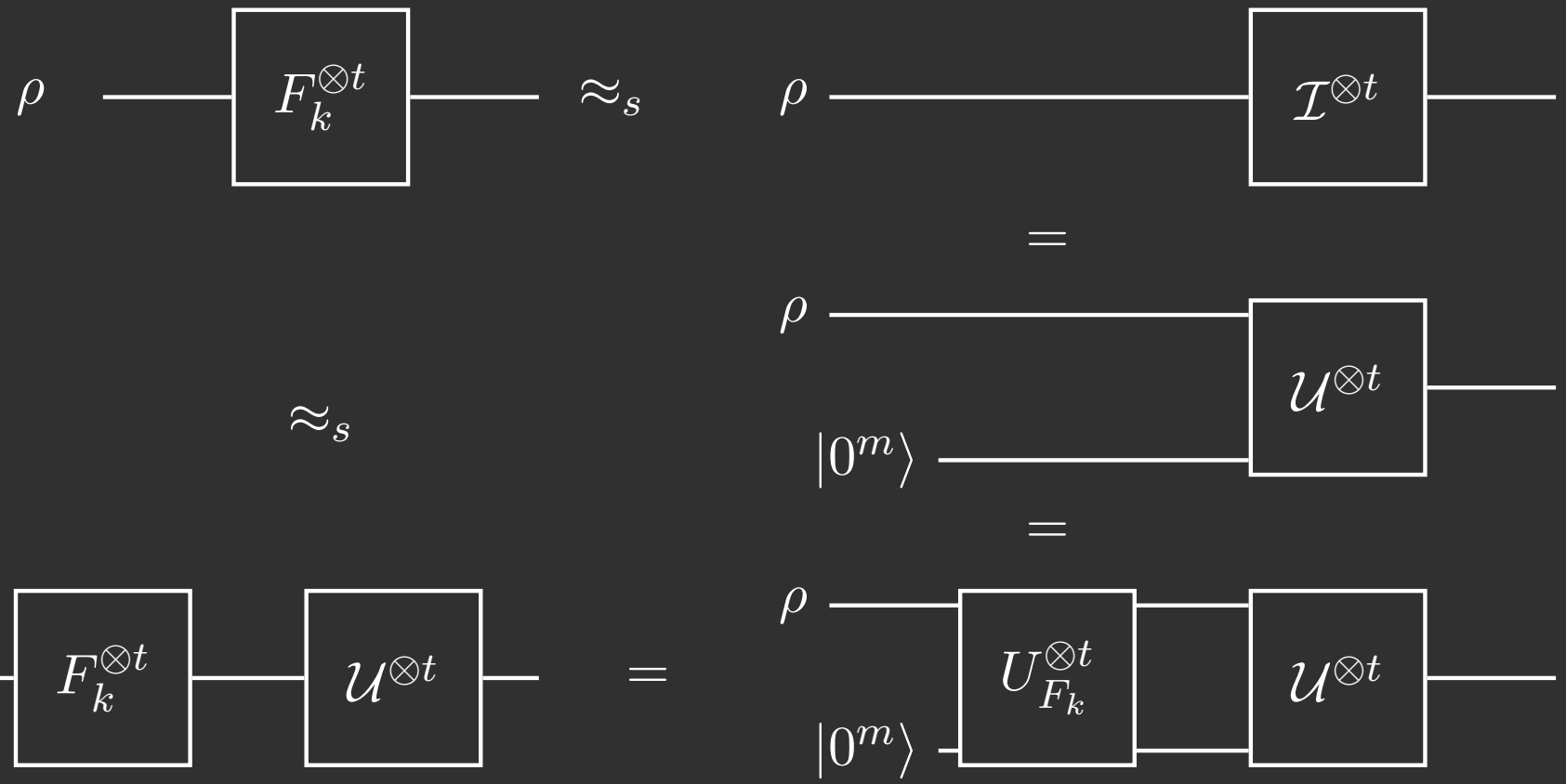

# Proof of Almost Invariance Implies Security

PRI is $\mathcal{Q}$-secure iff $\rho \in \mathcal{Q}$



# Proof of Almost Invariance Implies Security

PRI is $\mathcal{Q}$-secure iff $\rho \in \mathcal{Q}$

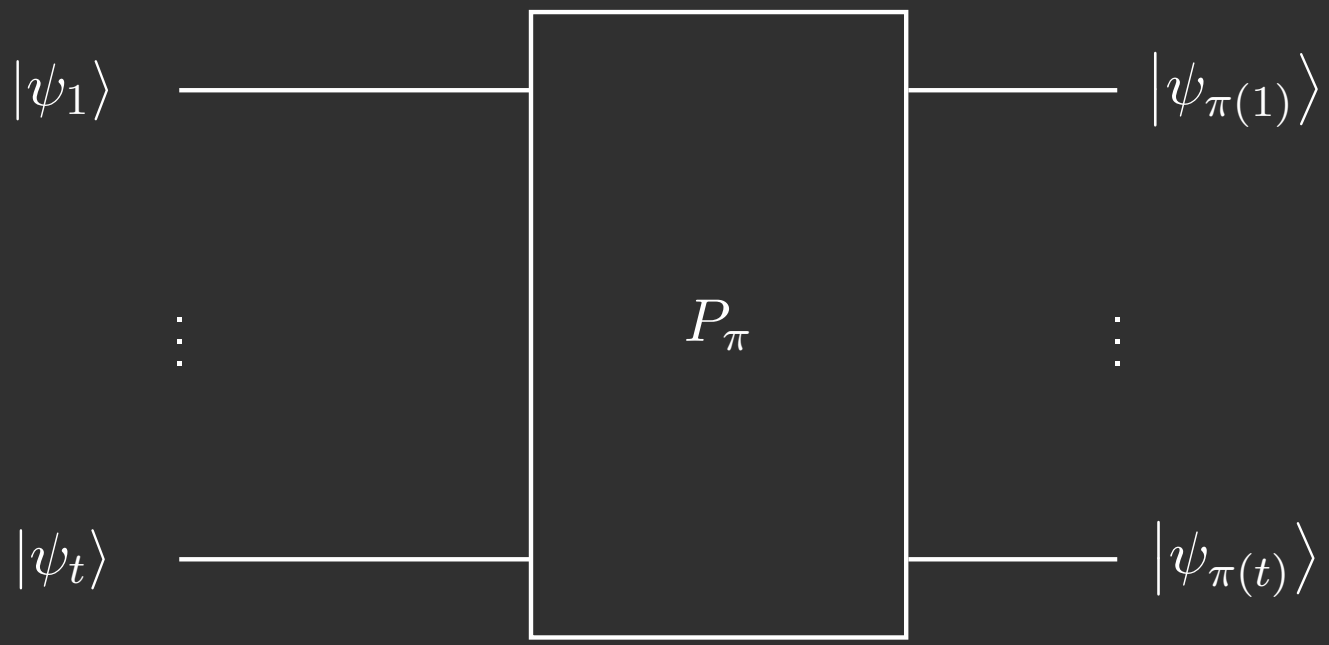


# Characterisation of Almost invariance

Can we characterise these "almost invariant" states?

# Characterisation of Almost Invariant states

Define $P_\pi$:



# Characterisation of Almost Invariant states

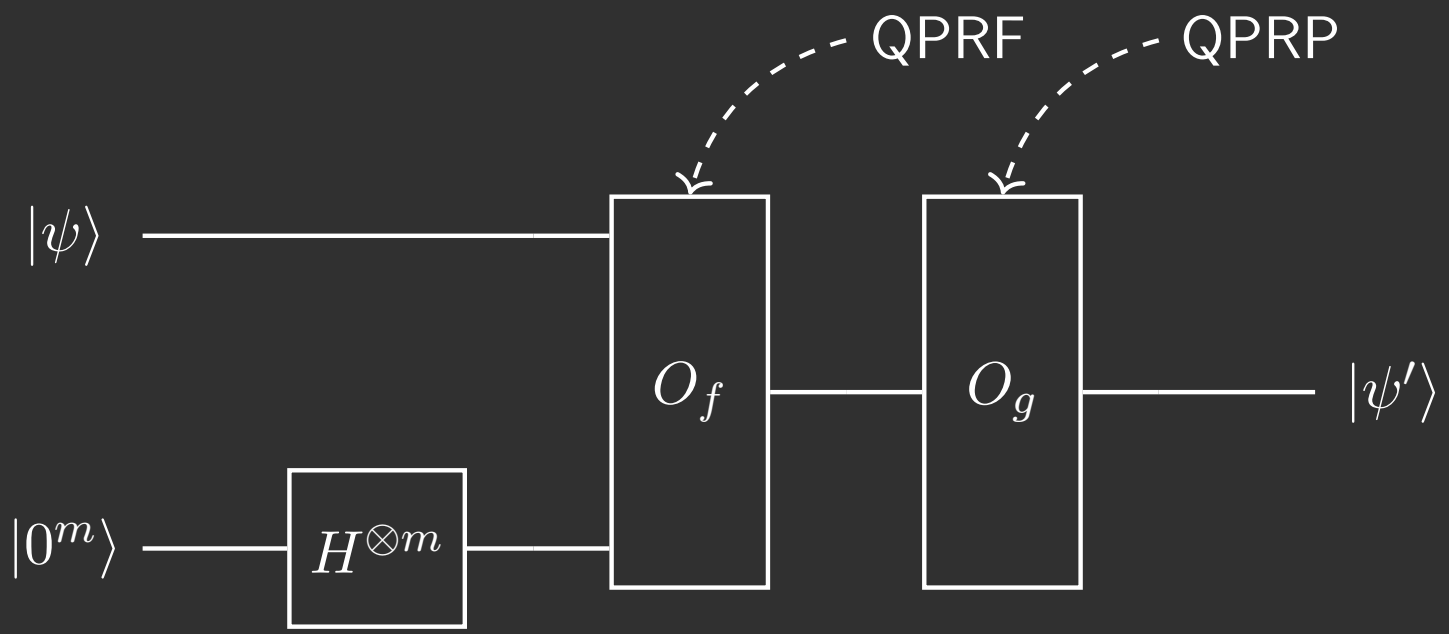
**Theorem**

*A state $\rho$ is almost invariant under $t$-fold Haar if and only if $\rho \approx_s \sum_\pi \alpha_\pi P_\pi$ for some $\pi \in S_t$.*

# Construction

Do we have a PRI from OWF?

# Implementation



# Security of the Construction

**Theorem**

*Assuming the existence of post-quantum one-way functions, the given construction is $\mathcal{Q}$-secure for $\mathcal{Q} \in \{\mathcal{Q}_{PRFS}, \mathcal{Q}_{PRSS}, \mathcal{Q}_{Haar}\}$.*

**Theorem (Conjecture)**

*Assuming the existence of post-quantum one-way functions, the given construction is $\mathcal{Q}$-secure for $\mathcal{Q} = \mathcal{D}(H)$.*

# Security of the Construction

## Theorem

*Assuming the existence of post-quantum one-way functions, the given construction is $\mathcal{Q}$-secure for $\mathcal{Q} \in \{\mathcal{Q}_{PRFS}, \mathcal{Q}_{PRSS}, \mathcal{Q}_{Haar}\}$.*

## Theorem (Conjecture)

*Assuming the existence of post-quantum one-way functions, the given construction is $\mathcal{Q}$-secure for $\mathcal{Q} = \mathcal{D}(H)$.*

# Security of the Construction

**Theorem**

*Assuming the existence of post-quantum one-way functions, the given construction is $\mathcal{Q}$-secure for $\mathcal{Q} \in \{\mathcal{Q}_{PRFS}, \mathcal{Q}_{PRSS}, \mathcal{Q}_{Haar}\}$.*

**Theorem (MPSY'24 (subsequent work))**

*Assuming the existence of post-quantum one-way functions, the given construction is $\mathcal{Q}$-secure for $\mathcal{Q} = \mathcal{D}(H)$.*

# Applications

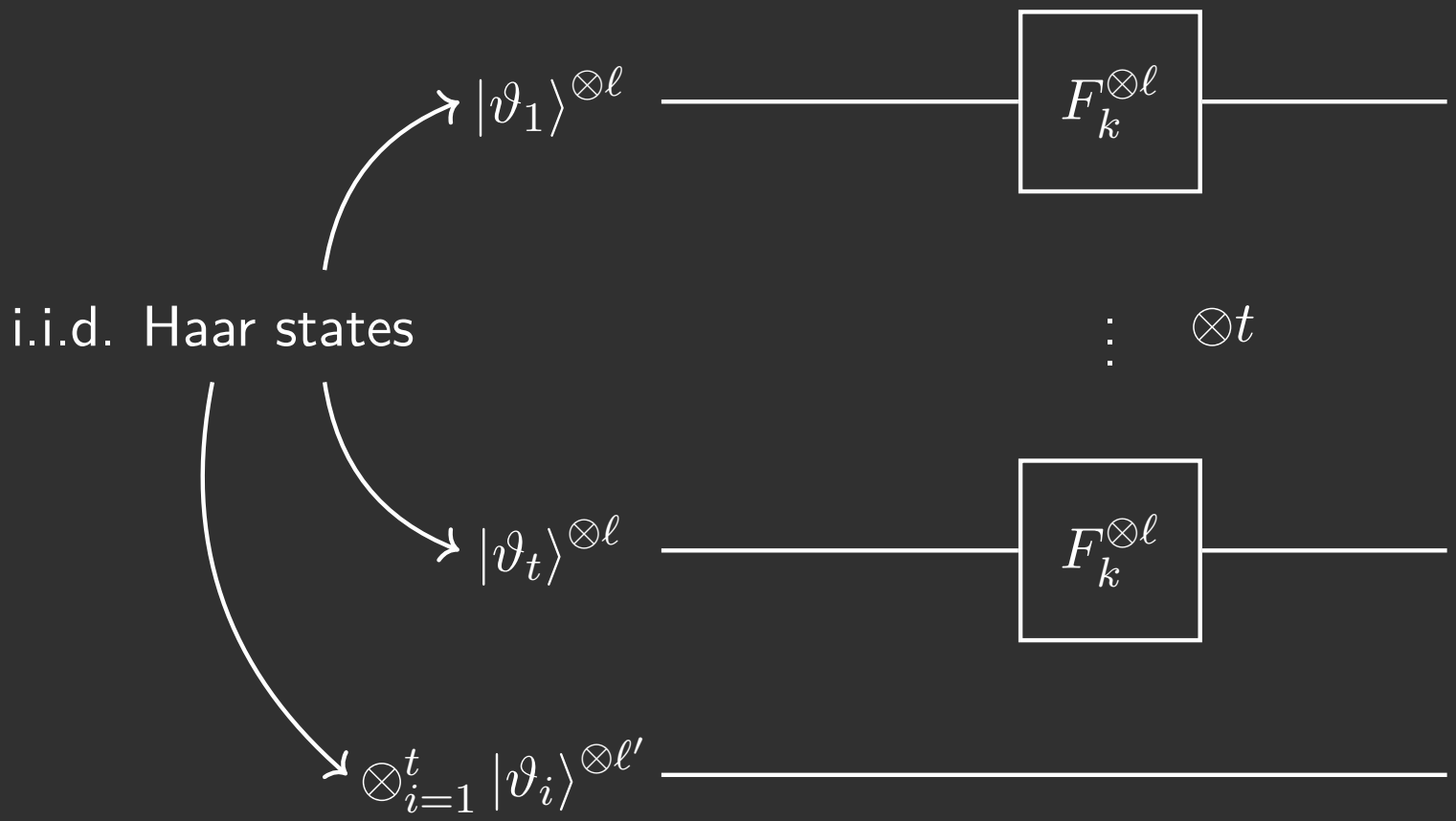
## Applications

# Length Extension

## Length Extension

# Security against Haar-queries

$\mathcal{Q}_{\mathsf{Haar}}$-security:



# Length Extension Theorem: Formal Statement

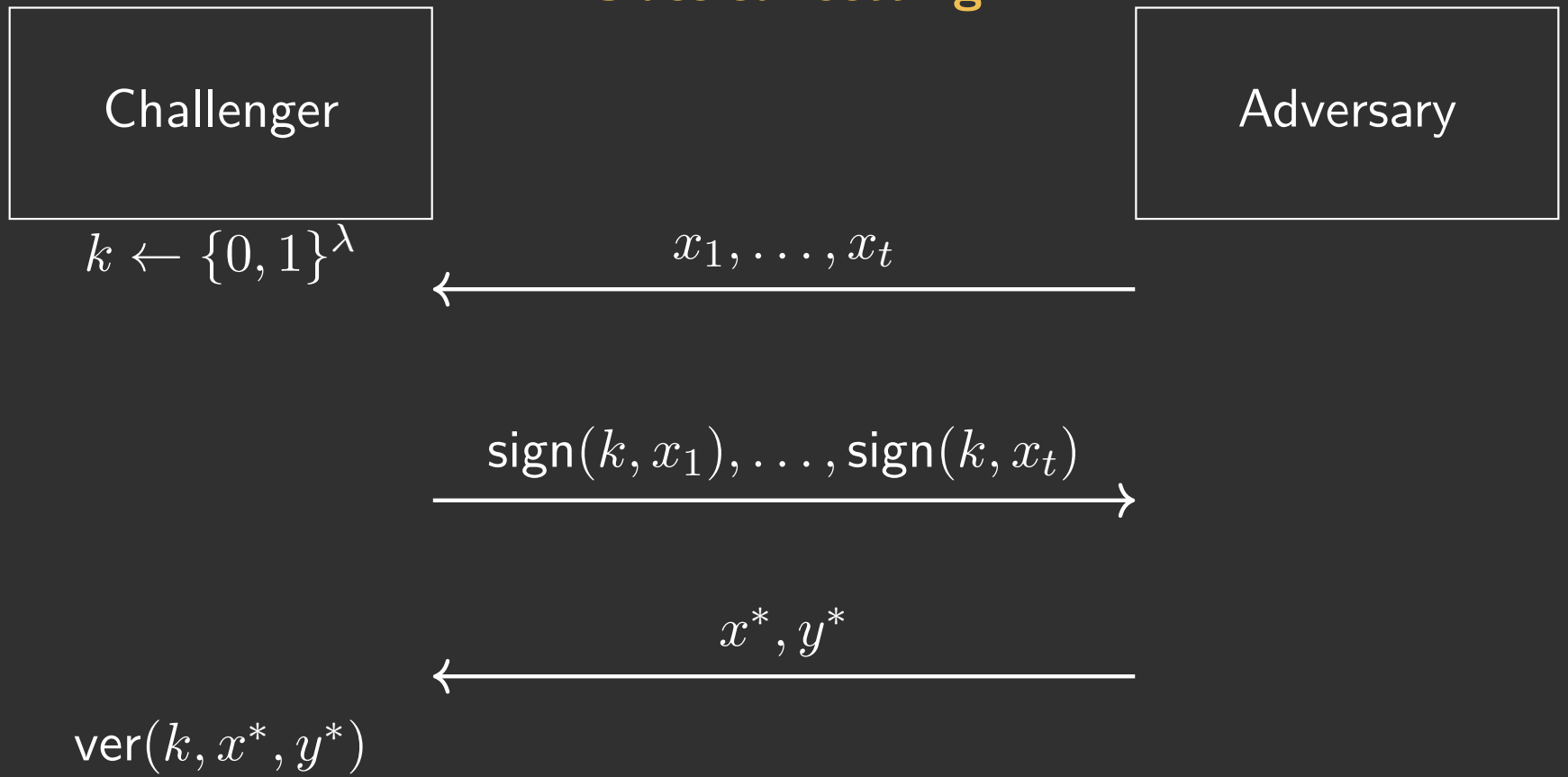
- Assuming the existence a $\mathcal{Q}_{\mathsf{Haar}}$-secure $(n, n+m)$-pseudorandom isometry, then given an $n$-qubit PRSG, there exists an $n+m$-qubit PRSG.
- Assuming the existence a $\mathcal{Q}_{\mathsf{Haar}}$-secure $(n, n+m)$-pseudorandom isometry, then given an $n$-qubit PRFSG, there exists an $n+m$-qubit PRFSG.

# Other Applications of PRI

- Quantum Message Authentication Codes (MACs).
- Multi-copy secure encryption schemes.
- Succinct quantum commitments.

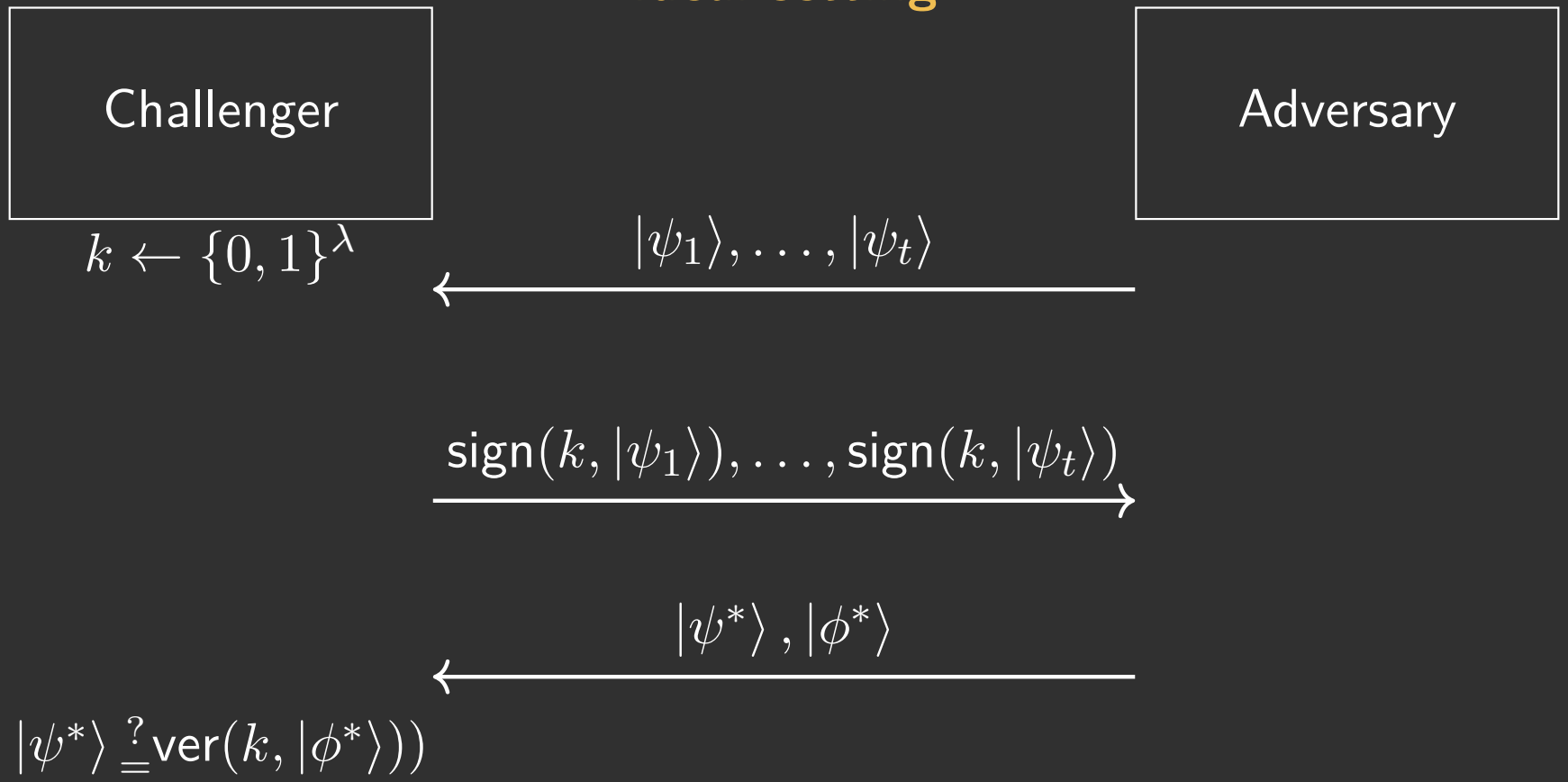
# Quantum Message Authentication Code (MAC)

**Classical setting**



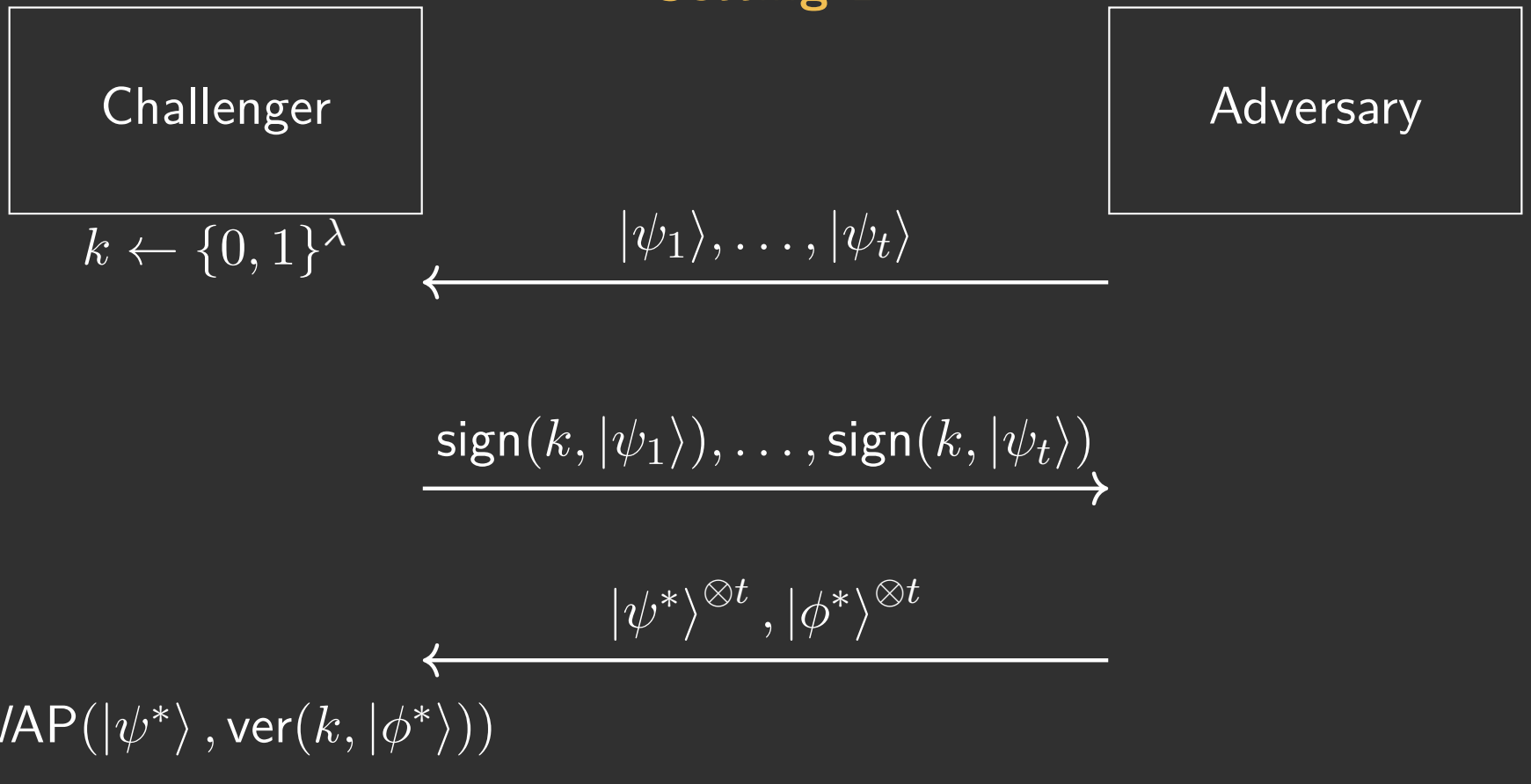
# Quantum Message Authentication Code (MAC)

**Ideal setting**



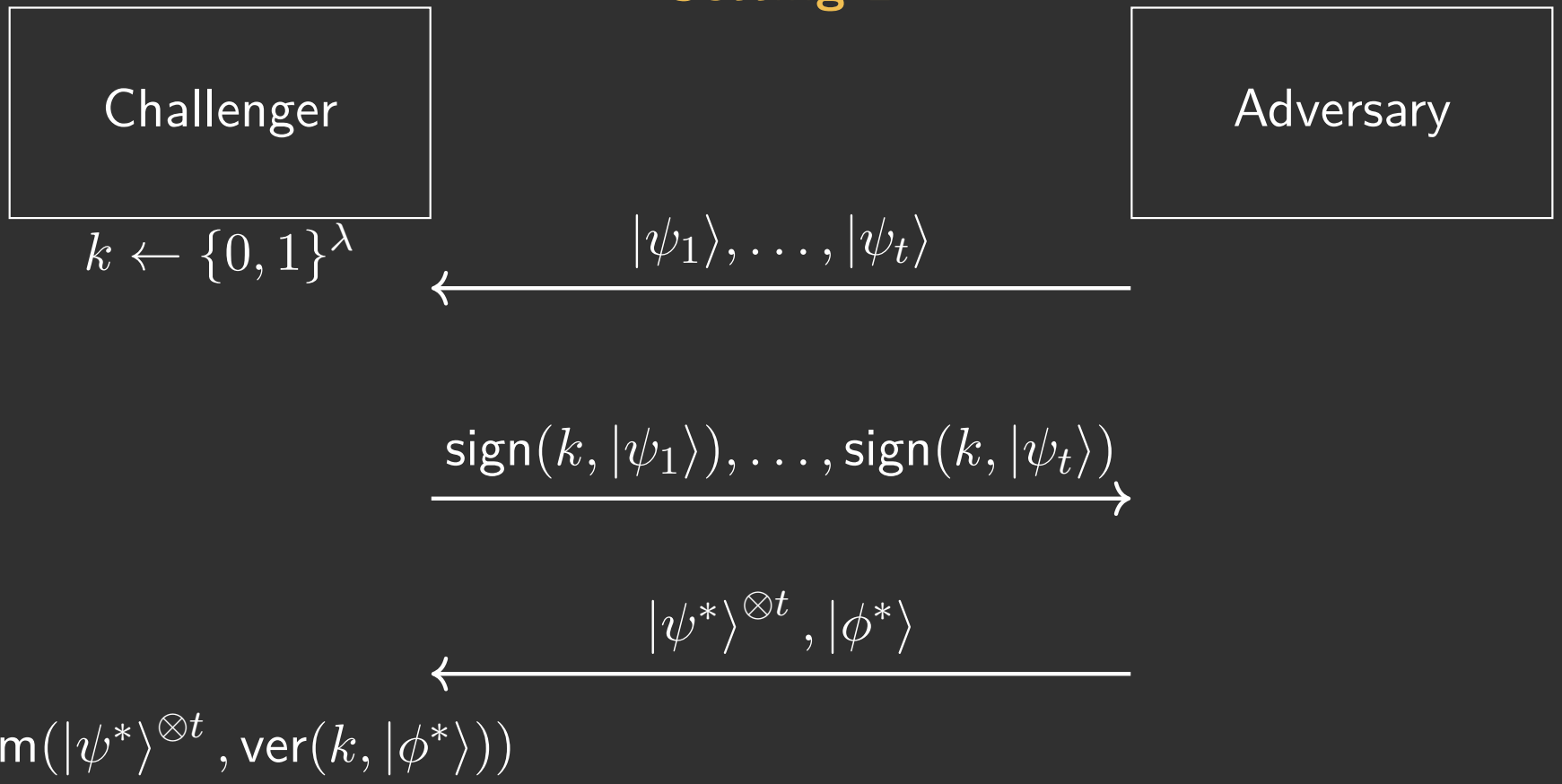
# Quantum Message Authentication Code (MAC)

**Setting 1**



# Quantum Message Authentication Code (MAC)

**Setting 2**



# Multi-Copy Secure Encryption and Succinct Quantum Commitments

## Multi-Copy Secure Encryption

- The security should hold even if the adversary receives polynomially many copies of the ciphertext state.
- $\mathcal{Q}_{\mathsf{single}}$-PRI provides the necessary security for both public-key and private-key encryption schemes. We use techniques similar to those of [LQS + 23].

## Succinct Quantum Commitments

- Achieved using pseudorandom isometries.
- Based on PRI implies one-time secure symmetric encryption schemes. We use techniques similar to those of [GJMZ23].

# Multi-Copy Secure Encryption and Succinct Quantum Commitments

## Multi-Copy Secure Encryption

- The security should hold even if the adversary receives polynomially many copies of the ciphertext state.
- $\mathcal{Q}_{\text{single}}$-PRI provides the necessary security for both public-key and private-key encryption schemes. We use techniques similar to those of [LQS + 23].

## Succinct Quantum Commitments

- Achieved using pseudorandom isometries.
- Based on PRI implies one-time secure symmetric encryption schemes. We use techniques similar to those of [GJMZ23].

# Summary

- **Pseudorandom Isometries (PRI):** Definition and framework to study other primitives.
- **Almost Invariance:** A technique to prove psuedorandomness.
- **Construction:** Using OWF to achieve PRI.
- **Applications:**
  - Length Extension Theorem
  - Quantum Message Authentication Codes (MACs)
  - Multi-copy secure encryption schemes
  - Succinct quantum commitments

# Summary

- **Pseudorandom Isometries (PRI):** Definition and framework to study other primitives.
- **Almost Invariance:** A technique to prove psuedorandomness.
- **Construction:** Using OWF to achieve PRI.
- **Applications:**
  - Length Extension Theorem
  - Quantum Message Authentication Codes (MACs)
  - Multi-copy secure encryption schemes
  - Succinct quantum commitments

# Summary

- **Pseudorandom Isometries (PRI):** Definition and framework to study other primitives.
- **Almost Invariance:** A technique to prove psuedorandomness.
- **Construction:** Using OWF to achieve PRI.
- **Applications:**
  - Length Extension Theorem
  - Quantum Message Authentication Codes (MACs)
  - Multi-copy secure encryption schemes
  - Succinct quantum commitments

# Summary

- **Pseudorandom Isometries (PRI):** Definition and framework to study other primitives.
- **Almost Invariance:** A technique to prove psuedorandomness.
- **Construction:** Using OWF to achieve PRI.
- **Applications:**
  - Length Extension Theorem
  - Quantum Message Authentication Codes (MACs)
  - Multi-copy secure encryption schemes
  - Succinct quantum commitments

# Thank You