Existentially Unforgeable Quantum Physical Unclonable Functions

Soham Ghosh[†]

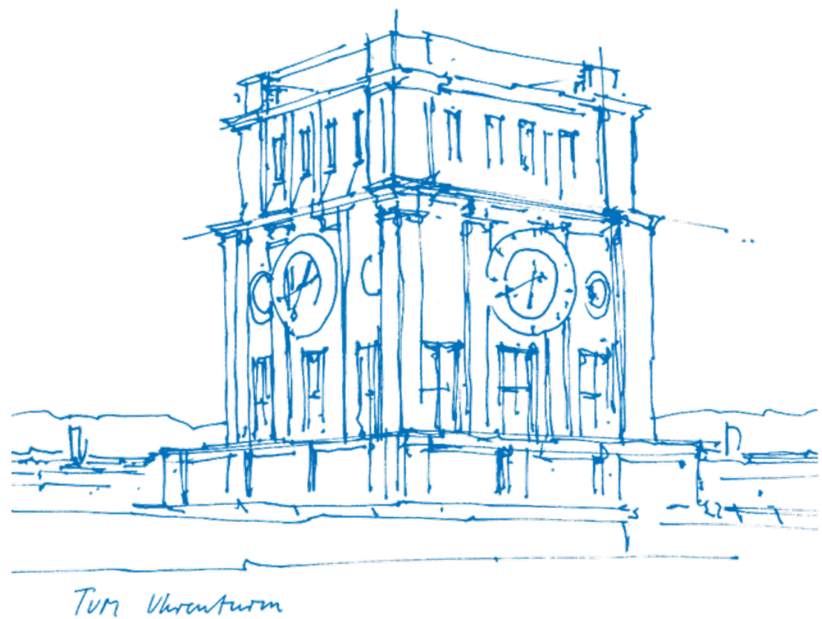
soham.ghosh@tum.de

Joint work with

Vladlen Galetsky[†], Pol Julià Farré[‡],
Christian Deppe[‡], Roberto Ferrara[†] and Holger Boche[†]

[†] School of Computation, Information and Technology,
Technical University of Munich, Germany

[‡] Institute for Communications Technology,
Technical University of Braunschweig, Germany



Physical Unclonable Functions (PUFs)

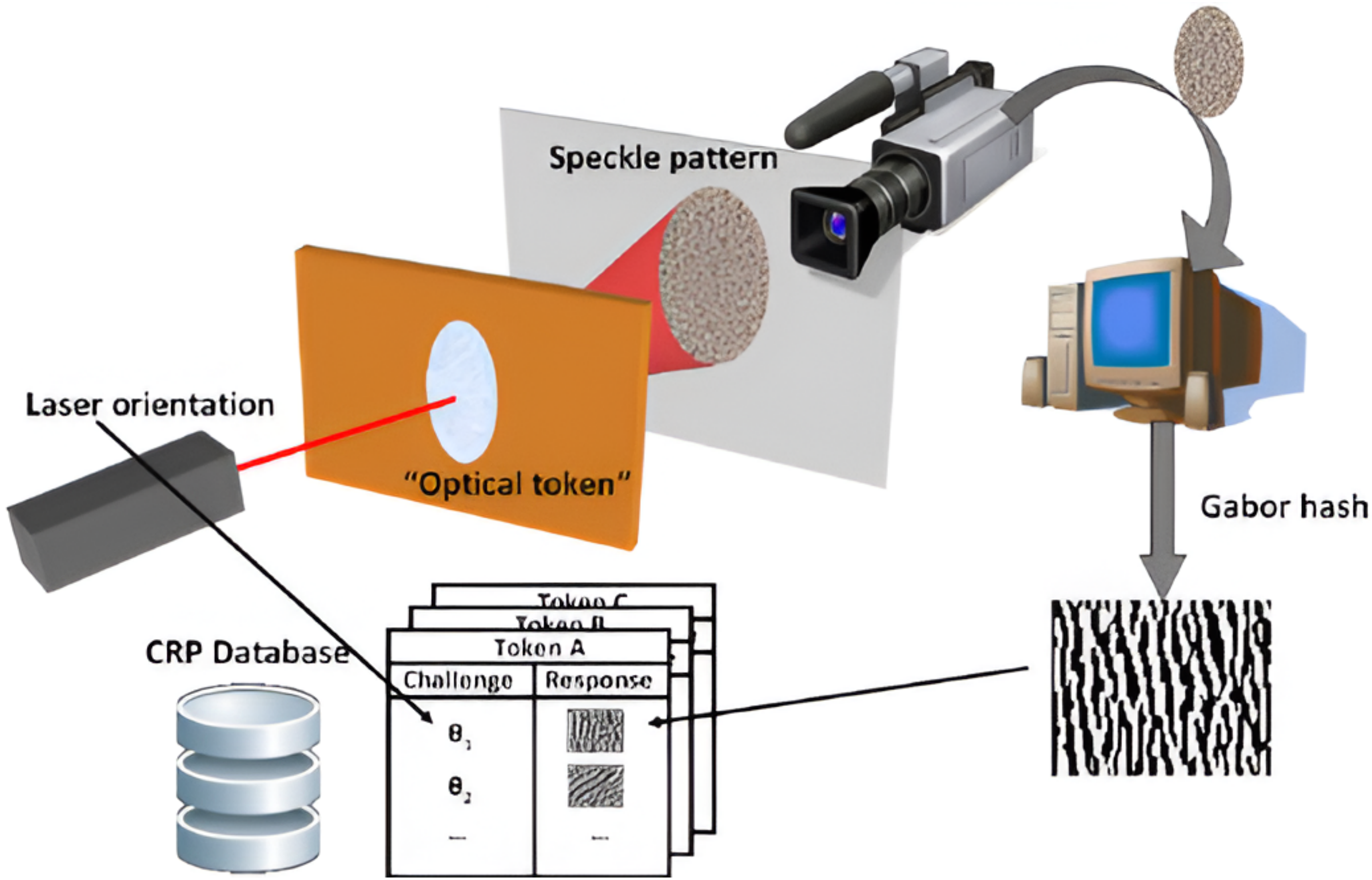
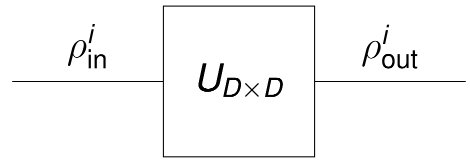


Figure: Optical PUF [Maes, Verbauwhede 2010]

Quantum Physical Unclonable Functions (QPUFs)

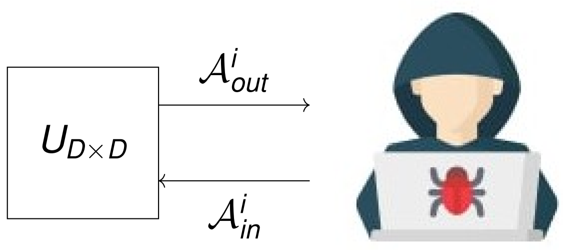
[Arapinis,Delavar,Doosti,Kashefi 2021]



$U \sim \mu(D),\ \text{where } \mu(D) \equiv$ Haar measure defined on the D-dimensional Unitary group.

Challenge-Response Database: $\{(\rho^i_{in}, \rho^i_{out})\}$.

Existential Unforgeability

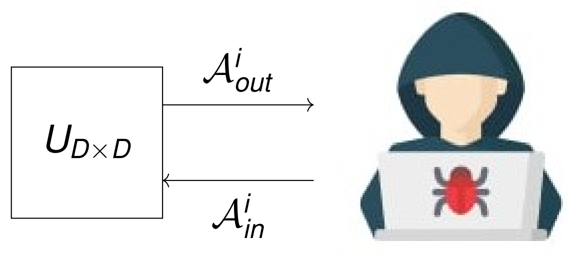


$$Q_{\mathcal{A}} := \{\mathcal{A}^i_{in}, \mathcal{A}^i_{out}\}$$

Definition (Existential Unforgeability)

U is existentially unforgeable if $\forall$ possible input state $\rho \notin Q_{\mathcal{A}}$, the probability of predicting the correct response state $U\rho U^\dagger$ by the Adversary $\mathcal{A}$ is negligible.

Existential Unforgeability



$$Q_{\mathcal{A}} := \{\mathcal{A}^i_{in}, \mathcal{A}^i_{out}\}$$

Definition (Existential Unforgeability)

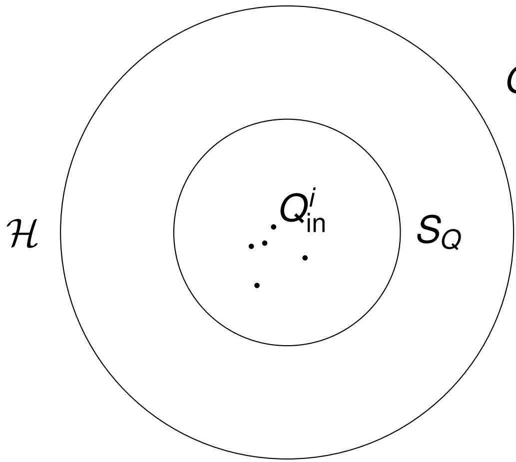
U is existentially unforgeable if $\forall$ possible input state $\rho \notin Q_{\mathcal{A}}$, the probability of predicting the correct response state $U\rho U^\dagger$ by the Adversary $\mathcal{A}$ is negligible.

Theorem (Arapinis,Delavar,Doosti,Kashefi 2021)

No Unitary QPUF is Existentially Unforgeable!

Failure of Unitary QPUFs

Universal Quantum Emulator [Marvian, Llyod 2016]

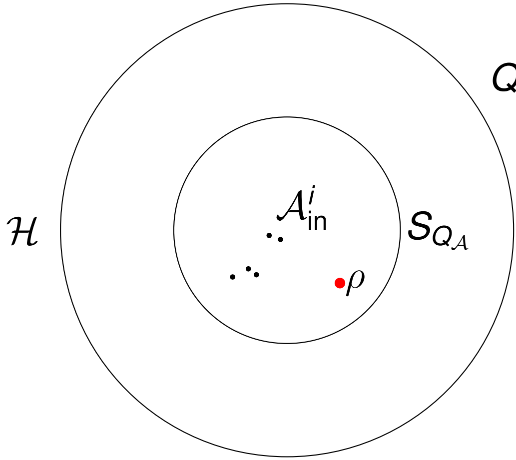


$$Q := \{Q^i_{in}, UQ^i_{in}U^\dagger\}$$

$UQE : Q \mapsto E^Q_U$ such that $\forall \sigma \in S_Q \subseteq \mathcal{H}$,

$$U\rho U^\dagger \approx E^Q_U \rho E^{Q\dagger}_U.$$

Failure of Unitary QPUFs



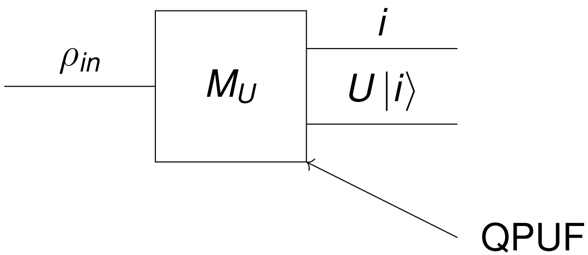
$$Q_\mathcal{A} := \{\mathcal{A}^i_{in}, U\mathcal{A}^i_{in}U^\dagger\}$$

Since $Q_\mathcal{A} \subseteq S_{Q_\mathcal{A}}$, $\exists \rho \notin Q_\mathcal{A}$ such that

$$E_U^{Q_\mathcal{A}} \rho E_U^{Q_\mathcal{A}\dagger} \approx U\rho U^\dagger$$

No Existential Unforgeability!

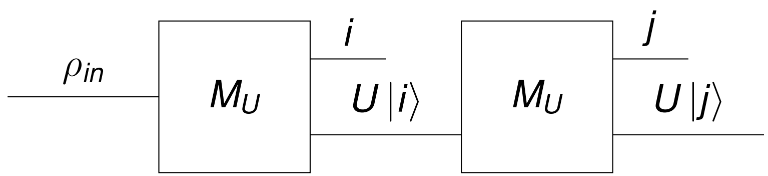
Non-unitary construction



$$M_U(\rho) = \sum_{i \in \mathbb{Z}_D} |i\rangle\langle i| \otimes \Pi_i^U \rho \Pi_i^U$$

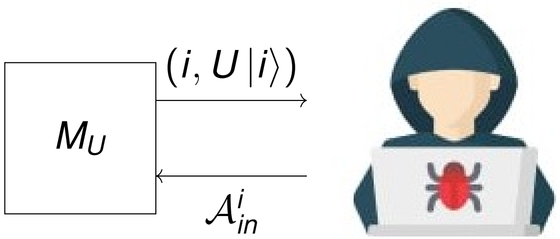
$$\{\Pi_i^U\}_{i \in \mathbb{Z}_D} = \{U|i\rangle\langle i| U^\dagger\}_{i \in \mathbb{Z}_D}$$

Authentication Protocol:



- Verifier creates state $U|i\rangle$ and sends to prover and stores the public classical value i.
- Prover sends back the received state upon verification and verifier makes QPUF measurement.
- Pass if $i = j$, fail otherwise.

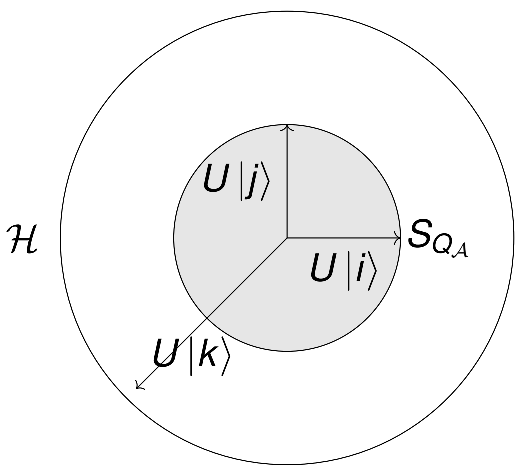
New Existential Unforgeability



$Q_{\mathcal{A}} := \{\mathcal{A}_{in}^i, i, U|i\rangle\}$

Definition (New Existential Unforgeability)

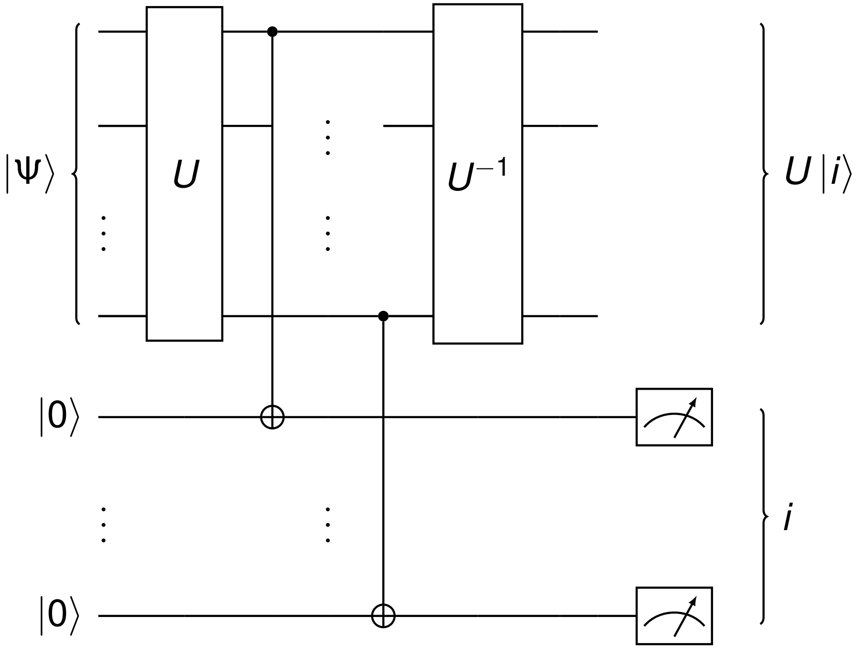
M_U is existentially unforgeable if $\forall$ possible classical values $i \notin Q_{\mathcal{A}}$, the probability of predicting the correct response state $U|i\rangle$ by the Adversary is negligible.



span$\{U|k\rangle\}$ is a measure zero set $\implies$ Existential Unforgeability!

$$E[P_{hack}] \leq \frac{1}{D - \dim(Q_{\mathcal{A}})}$$

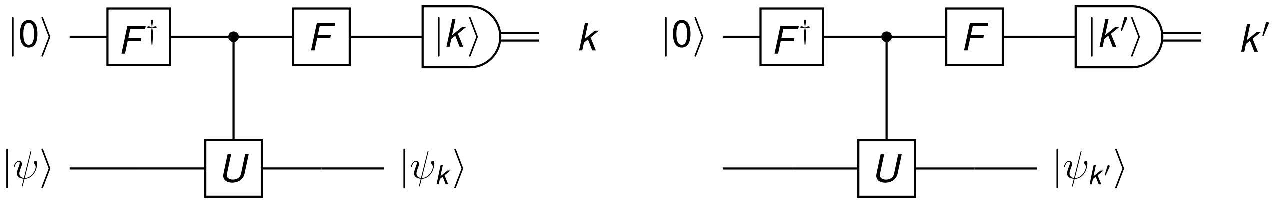
Implementations



How to invert an unknown unitary?

Known methods have exponential complexity [Quintino et. al. 2019].

Implementation based on Quantum Phase Estimation

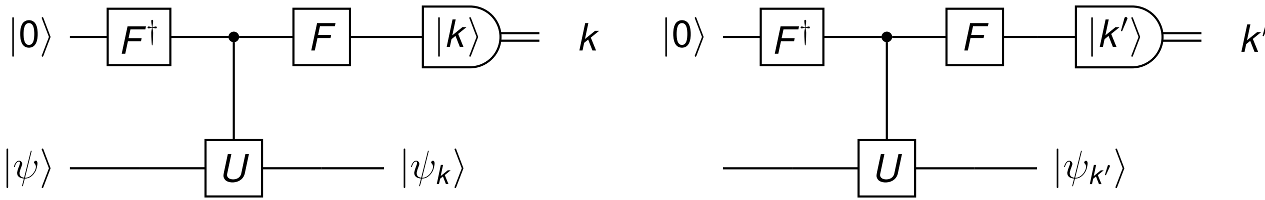


Check $|k - k'| \leq \Delta$?

Δ- is a chosen decision boundary and

$$CU \equiv \sum_{i \in \mathbb{Z}_D} |i\rangle \langle i| \otimes U^i.$$

Implementation based on Quantum Phase Estimation



Check $|k - k'| \leq \Delta$?

Δ- is a chosen decision boundary and

$$CU \equiv \sum_{i \in \mathbb{Z}_D} |i\rangle \langle i| \otimes U^i .$$

Probability of getting $|k - k'| \leq \Delta$ for honest prover:

$$\Pr[|k - k'| \leq \Delta] > \left(1 - \sqrt{1 - f(\Delta)}\right)^2 \quad , \tag{1}$$

where

$$f(\Delta) = \left(1 - \frac{2}{\pi^2 \left(\sqrt{\Delta} + \frac{1}{2}\right)}\right) \cdot \left(1 - \frac{2}{\pi^2 (\Delta - \frac{1}{2})}\right) .$$

Simulations

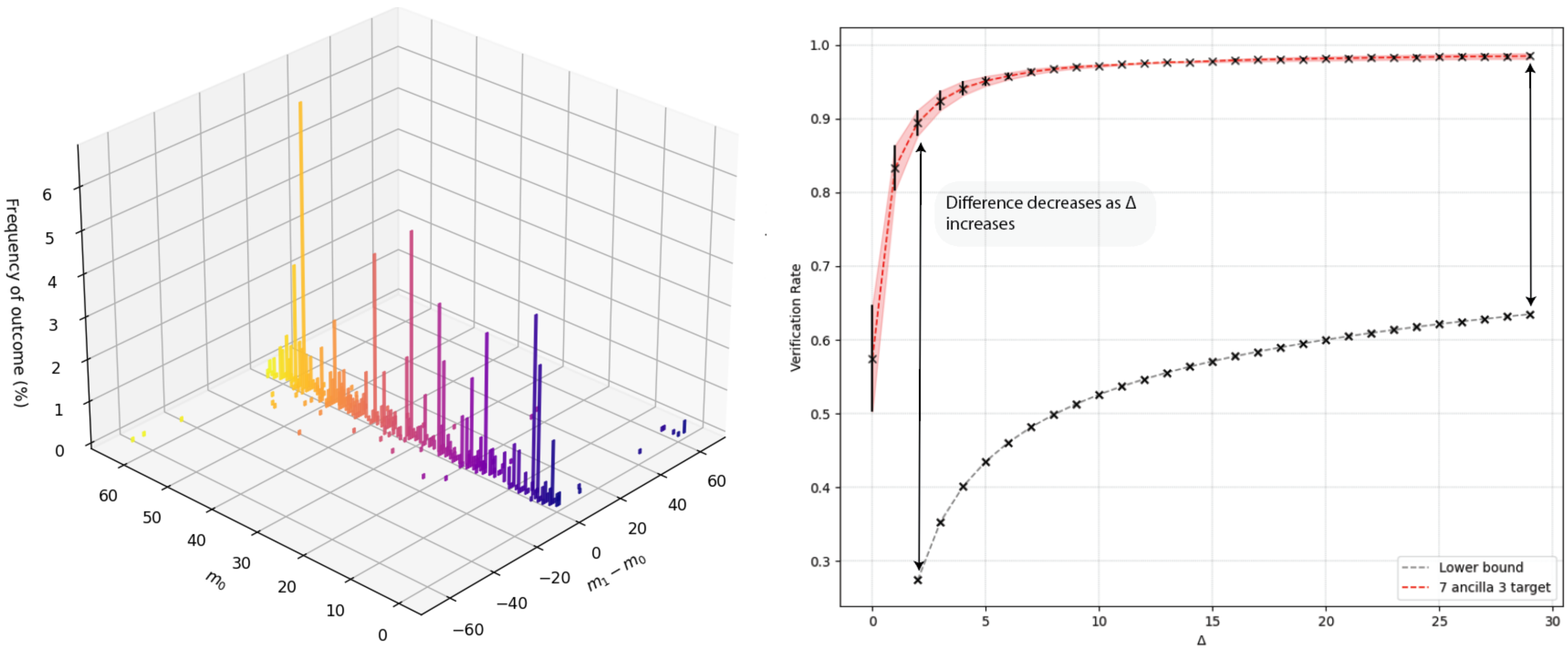


Figure: (Left) m_0 and m_1 represent measurement outcomes at generation and verification respectively. 6 ancilla, 6 target, 10^3 shots on IBM aer-simulator backend. (Right) Simulation results (above) compared with analytical bound (below).

Mechanics of Quantum Phase Estimation

Spectral decomposition of U

$$U = \sum_{i \in \mathbb{Z}_D} e^{i2\pi \frac{\phi_i}{d}} \left|\phi_i\right\rangle \left\langle\phi_i\right|, \quad \phi_i \in [0, d[\, .$$

Mechanics of Quantum Phase Estimation

Spectral decomposition of U

$$U = \sum_{i \in \mathbb{Z}_D} e^{i2\pi \frac{\phi_i}{d}} \left|\phi_i\right\rangle \left\langle\phi_i\right|, \quad \phi_i \in [0, d[\ .$$

QPE quantum instrument:

$$\Lambda_U^{QPE}(\rho) \equiv \sum_{k \in \mathbb{Z}_d} \left|k\right\rangle \left\langle k\right| \otimes U_k \rho U_k^\dagger.$$

Mechanics of Quantum Phase Estimation

Spectral decomposition of U

$$U = \sum_{i \in \mathbb{Z}_D} e^{i2\pi \frac{\phi_i}{d}} |\phi_i\rangle \langle\phi_i| , \quad \phi_i \in [0, d[\ .$$

QPE quantum instrument:

$$\Lambda_U^{QPE}(\rho) \equiv \sum_{k \in \mathbb{Z}_d} |k\rangle \langle k| \otimes U_k \rho U_k^\dagger .$$

The explicit form of the Kraus operators can be calculated as:

$$U_k = \sum_{j \in \mathbb{Z}_D} \frac{e^{i\pi(\phi_j - k)}}{e^{i\frac{\pi}{d}(\phi_j - k)}} \frac{\sin(\pi(\phi_j - k))}{d \sin\left(\frac{\pi(\phi_j - k)}{d}\right)} |\phi_j\rangle \langle\phi_j| ,$$

Mechanics of Quantum Phase Estimation

Spectral decomposition of U

$$U = \sum_{i \in \mathbb{Z}_D} e^{i2\pi \frac{\phi_i}{d}} \left|\phi_i\right\rangle \left\langle\phi_i\right|, \quad \phi_i \in [0, d[\ .$$

QPE quantum instrument:

$$\Lambda_U^{QPE}(\rho) \equiv \sum_{k \in \mathbb{Z}_d} \left|k\right\rangle \left\langle k\right| \otimes U_k \rho U_k^{\dagger}.$$

The explicit form of the Kraus operators can be calculated as:

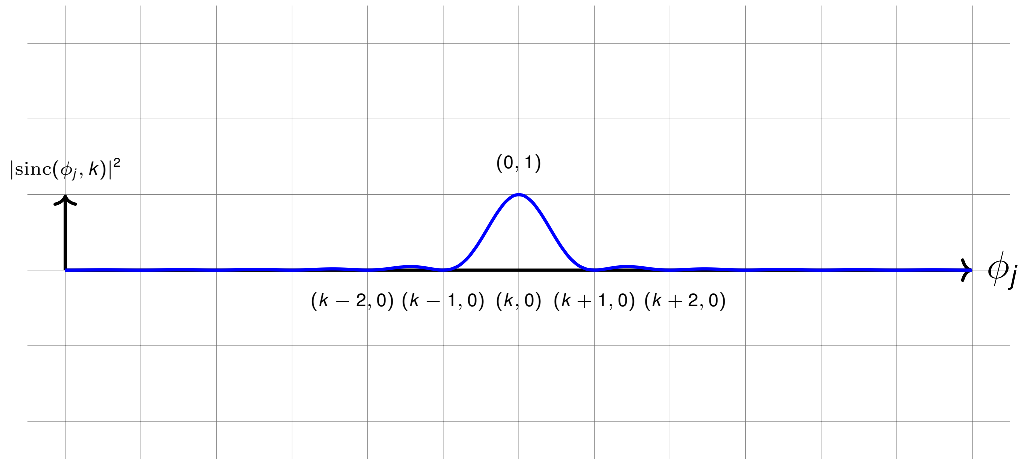
$$U_k = \sum_{j \in \mathbb{Z}_D} \frac{e^{i\pi(\phi_j - k)}}{e^{i\frac{\pi}{d}(\phi_j - k)}} \frac{\sin(\pi(\phi_j - k))}{d \sin\left(\frac{\pi(\phi_j - k)}{d}\right)} \left|\phi_j\right\rangle \left\langle\phi_j\right|,$$

with POVM elements,

$$M_k := U_k^{\dagger} U_k = |U_k| = \sum_{j \in \mathbb{Z}_D} \frac{\sin^2(\pi(\phi_j - k))}{d^2 \sin^2(\frac{\pi(\phi_j - k)}{d})} \left|\phi_j\right\rangle \left\langle\phi_j\right|.$$

Mechanics of Quantum Phase Estimation

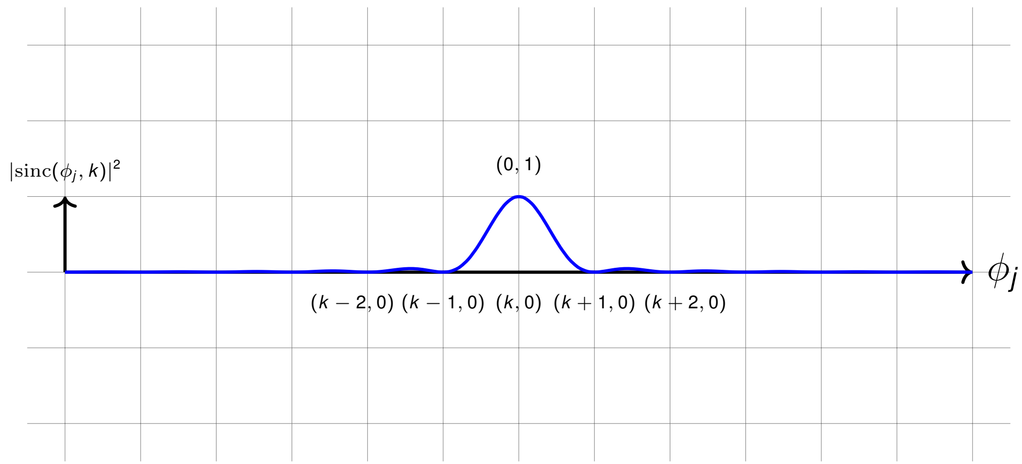
$$\lim_{d\to\inf} \left| \frac{\sin(\pi(\phi_j - k))}{d\sin\left(\pi(\frac{\phi_j - k}{d})\right)} \right|^2 = \left| \frac{sin(\pi(\phi_j - k))}{\pi(\phi_j - k)} \right|^2$$



$M_k \approx \sum_j |\phi_j\rangle\langle\phi_j|$, such that $\forall j, \exists\Delta$ such that $|\phi_j - k| \leq \Delta$.
The POVMs M_k approximate a von-Neumann Measurement on the eigenbasis of U.

Mechanics of Quantum Phase Estimation

$$\lim_{d \to \inf} \left| \frac{\sin(\pi(\phi_j - k))}{d \sin\left(\pi(\frac{\phi_j - k}{d})\right)} \right|^2 = \left| \frac{sin(\pi(\phi_j - k))}{\pi(\phi_j - k)} \right|^2$$



$M_k \approx \sum_j |\phi_j\rangle \langle\phi_j|$, such that $\forall j, \exists \Delta$ such that $|\phi_j - k| \leq \Delta$.
The POVMs M_k approximate a von-Neumann Measurement on the eigenbasis of U.

Problem: Implementation of $CU^{2^{n-1}}$ has exponential gate cost complexity.

Summary

- Defined PUFs and motivated quantum advantage for studying QPUFs.

Summary

- Defined PUFs and motivated quantum advantage for studying QPUFs.
- Defined Existential Unforgeability, explained failure of Unitary QPUFs and motivated the search for non-unitary constructions.

Summary

- Defined PUFs and motivated quantum advantage for studying QPUFs.
- Defined Existential Unforgeability, explained failure of Unitary QPUFs and motivated the search for non-unitary constructions.
- Provided explicit non-unitary constructions.

Summary

- Defined PUFs and motivated quantum advantage for studying QPUFs.
- Defined Existential Unforgeability, explained failure of Unitary QPUFs and motivated the search for non-unitary constructions.
- Provided explicit non-unitary constructions.
- Explained the short-comings of the constructions and defined some open problems.

The End

Thank you.