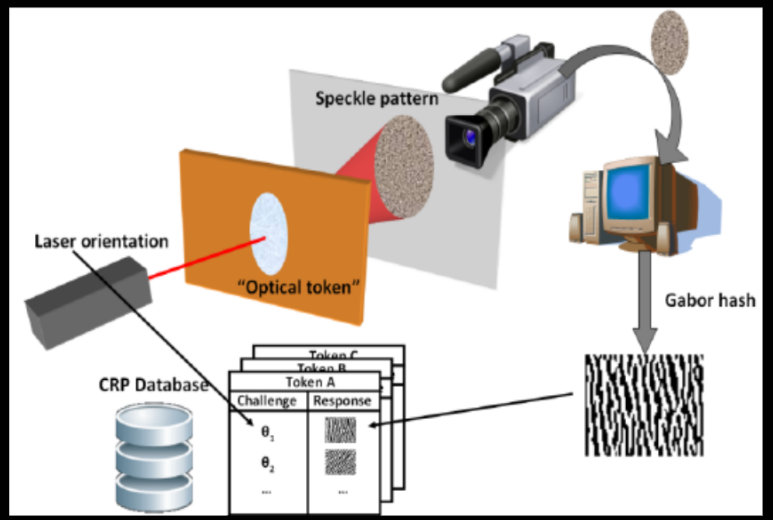
Existentially-Unforgeable Quantum Physically-Unclonable Functions (QPUF) based on Quantum Phase Estimation

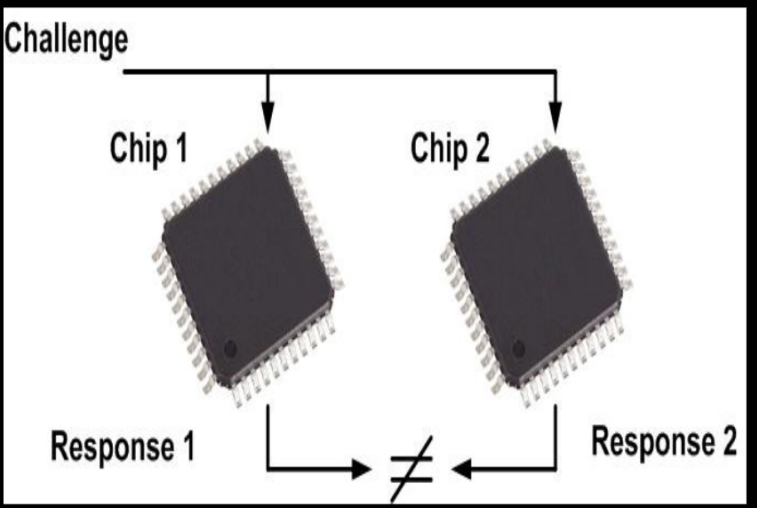
Soham Ghosh, Vladlen Gabetsky, Pol Julià Farré, Christian Deppe, Roberto Ferrara

Technical University Of Munich

Physical Unclonable Functions (PUF)

"A device with the assumption of being almost impossible to clone", even for the manufacturer!! Information can only be obtained by "querying it" (using it).





Optical PUF: EXYNOS 9820 CHIP, SAMSUNG GALAXY S10

Ring Oscillator based PUF:- Xilinix FPGA (Y. Xin, J.P. Kaps, K. Guj)

Hardware Requirements for PUF

1. Uniqueness:

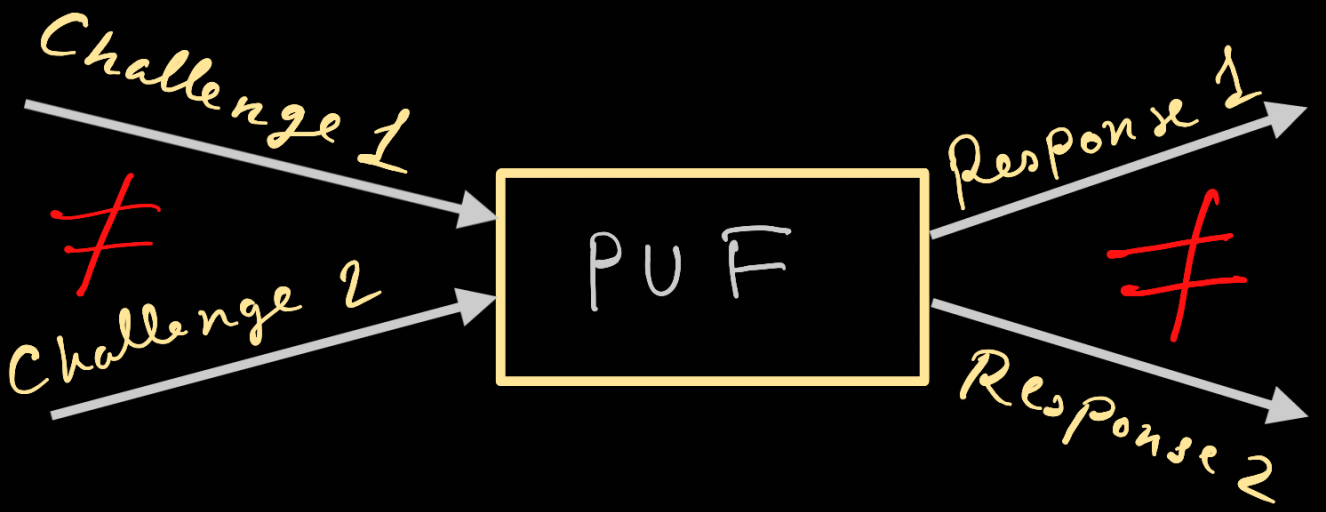
$PUF_1 : \{0,1\}^n \rightarrow \{0,1\}^m$

$\neq$

$PUF_2 : \{0,1\}^n \rightarrow \{0,1\}^m$

Different PUFs should have different evaluation algorithms.

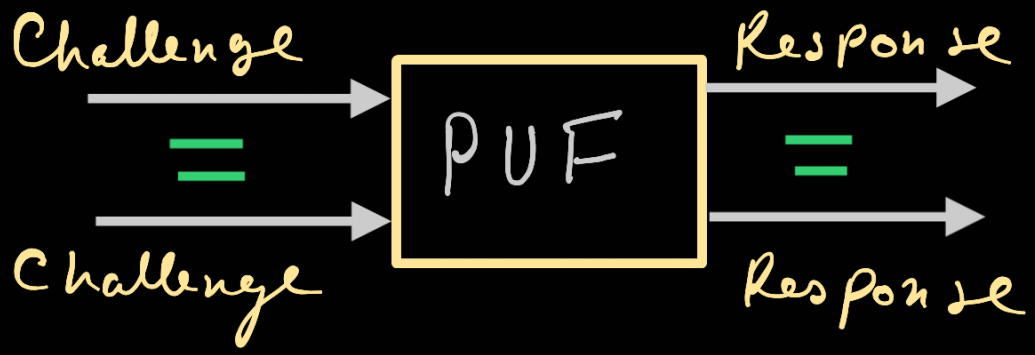
2. Collision-resistance :-



For a fixed PUF:

Different challenges ⟺ Different responses

3. Robustness:

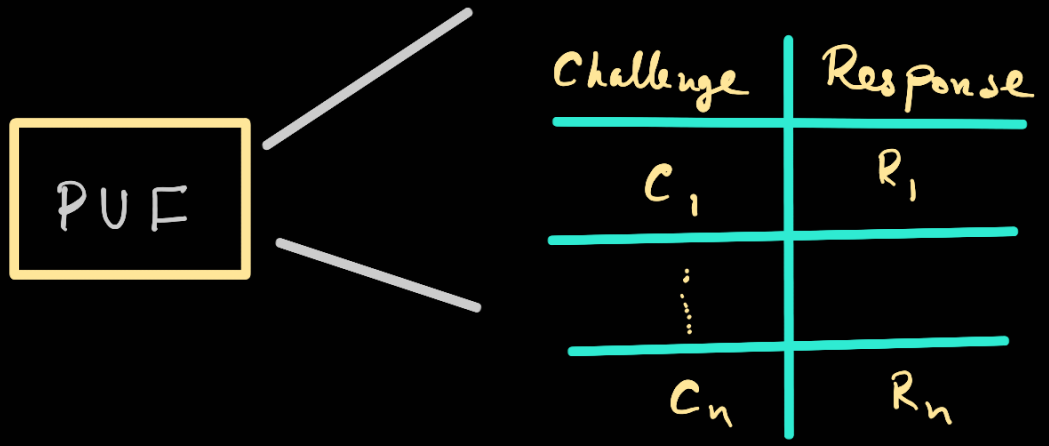


For a fixed PUF:

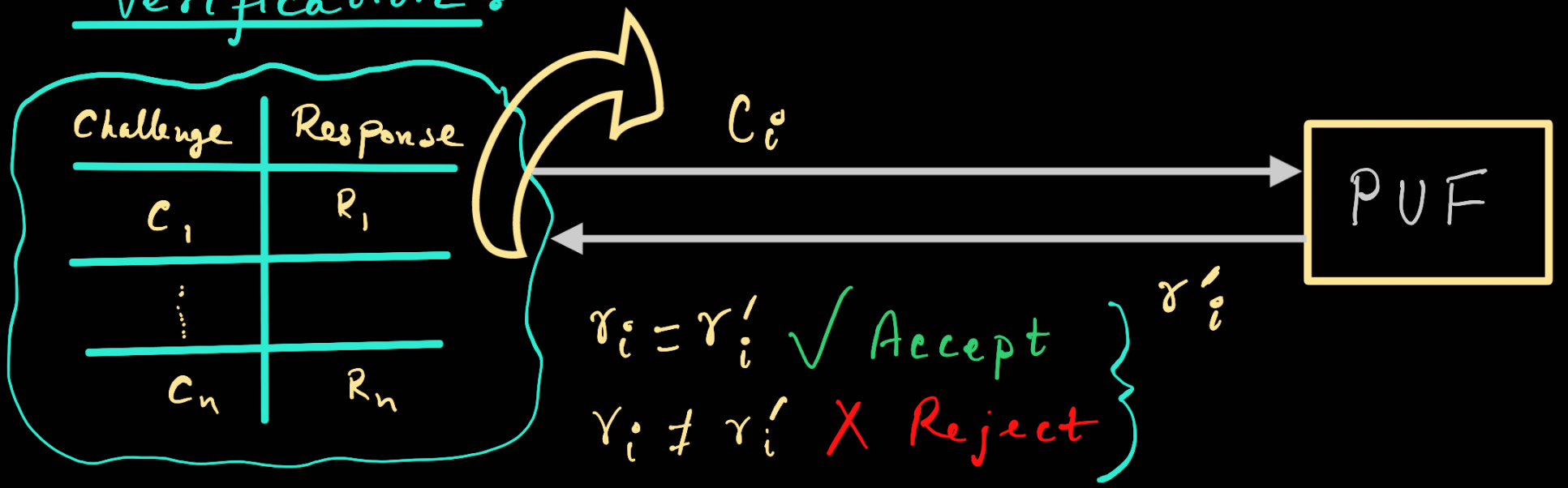
Same Challenges $\Longleftrightarrow$ Same Responses

Standard Authentication Protocol

Enrollment :-



Verification :-



Quantum Advantage

In classical :

Challenges cannot be used more than once.

In Quantum :

NO CLONING!

Quantum State Tomography also cannot be done with few copies.

Quantum Physical Unclonable Functions (QPUF)

Any "Completely Positive Trace Preserving" quantum process (Λ) can be a candidate for QPUF.

$$\Lambda : \mathcal{B}(\mathcal{H}) \longrightarrow \mathcal{B}(\mathcal{H})$$
$$\rho \longmapsto \Lambda(\rho) \; ; \; \mathrm{Tr}(\Lambda(\rho)) = 1$$

$\mathcal{B}(\mathcal{H})$ = Space of Bounded operators from $\mathcal{H} \to \mathcal{H}$.

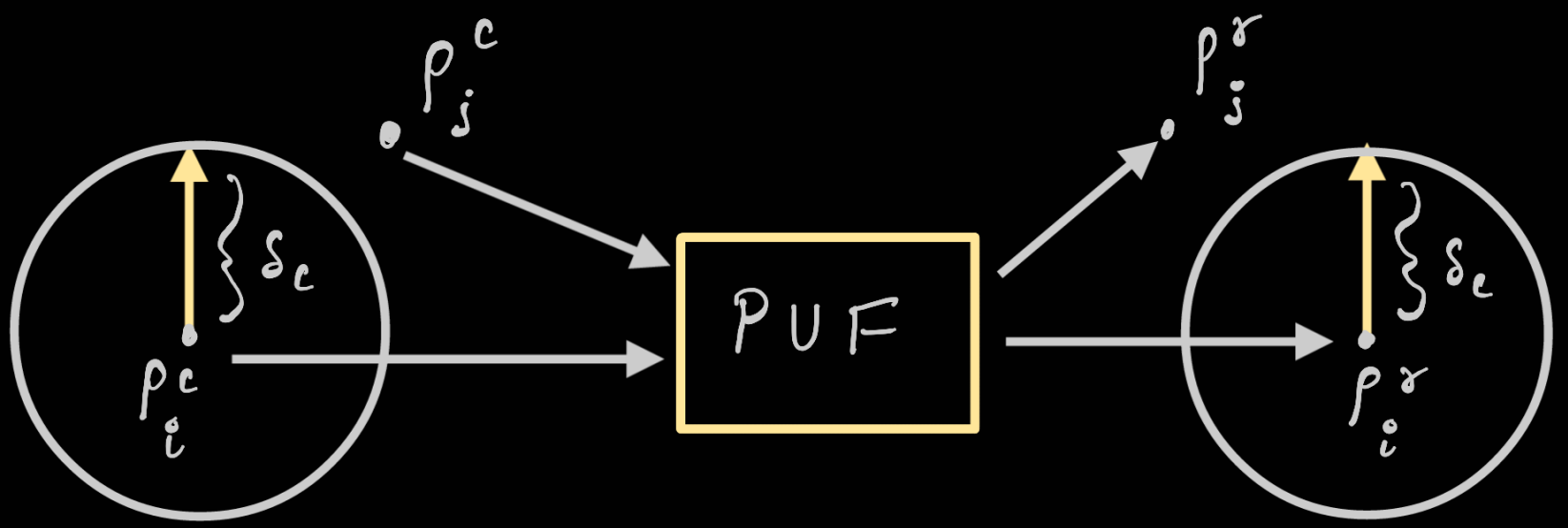
Hardware Requirements for QPUF [Arapins et. al.]

1. δ_u - Uniqueness :-

$$\| \Lambda - \Lambda' \|_\diamond \geq \delta_u$$

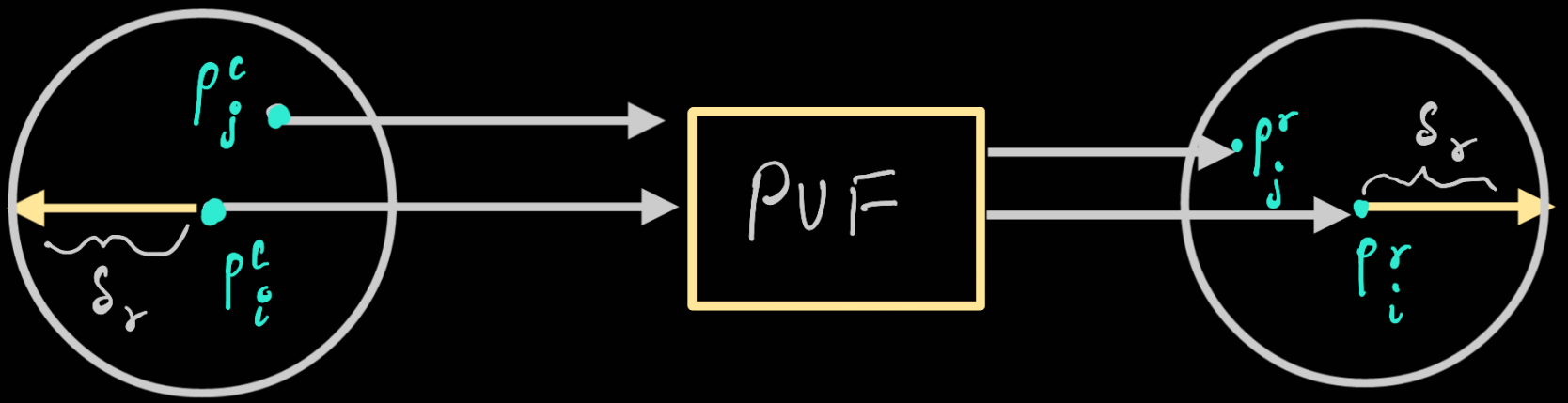
CPTP maps of two different QPUFs should have atleast "δ_u" distance in diamond norm.

2. δ_c - Collision Resistance :-



$$0 \leq F(p_i^c, p_j^c) \leq 1-\delta_c \iff 0 \leq F(p_i^r, p_j^r) \leq 1-\delta_c$$

3. δ_r - Robustness :-



$$\delta_r \leq F(P_i^c, P_j^c) \leq 1 \iff \delta_r \leq F(P_i^r, P_j^r) \leq 1$$

Theorem [Arapins et. al.]

If domain = range for CPTP map of QPUF, then it is "almost" unitary.

$$\Lambda(\rho) = (1-\varepsilon) U \rho U^{+} + \varepsilon \Lambda'(\rho)$$

where $\varepsilon = negl(\lambda)$; λ = security parameter

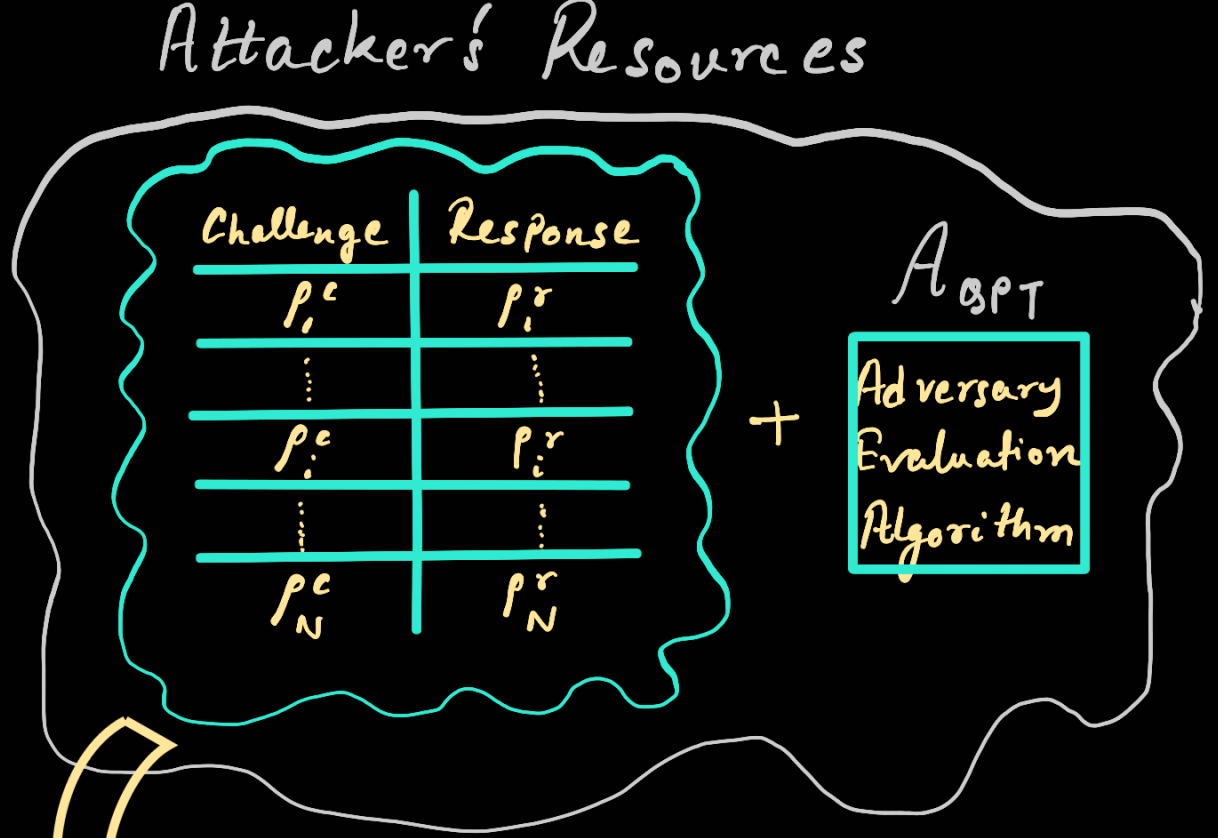
U = Unitary map.

Hardware Assumption for QPUF [Arapins et. al.]

The unitary quantum process for QPUF is an uniform (Haar) random matrix.

(Simplest and Strongest Assumption!)

Existential Unforgeability



$N = poly(\lambda)$

λ = security parameter

If $\nexists A_{QPT}$, s.t.

$\forall p \notin$ C | R

$A_{QPT}^{(p)} \neq \Lambda_{QPUF}^{(p)}$

Then QPUF is existentially unforgeable!

Theorem [Arapins et. al.]

No Haar Random Unitary QPUF can have existential unforgeability!

Hence, we develop a model to achieve this level of security!

Quantum Phase Estimation

Motivation :-

Any $D \times D$ Unitary matrix can be written as :-

$$U = \sum_{j \in \mathbb{Z}_D} e^{i 2\pi \frac{\phi_j}{d}} |\phi_j\rangle\langle\phi_j| \quad ; \quad \{|\phi_j\rangle\} \rightarrow \text{Complete set of eigen basis}$$

where $\phi_j \in [0, d[$.

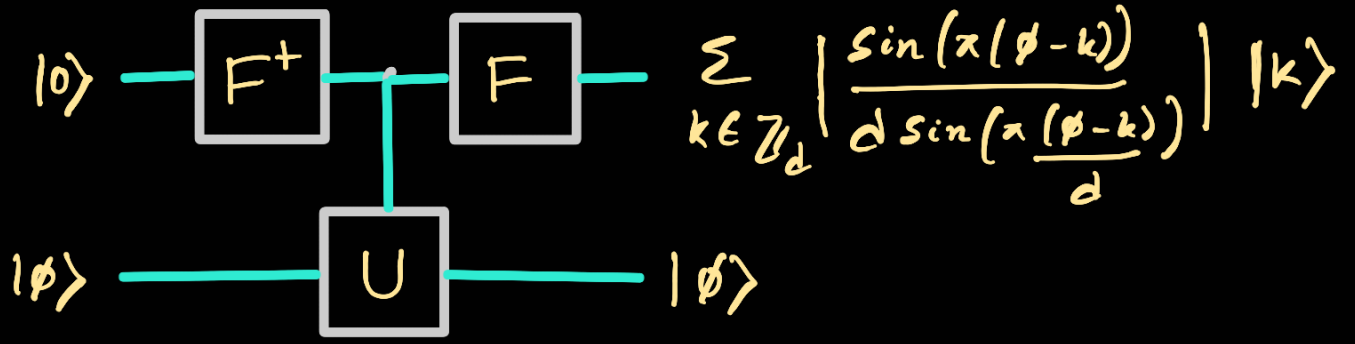
Goal :- Given $\{|\phi_i\rangle\}$, find $\phi_i \ \forall \ i$.

Notice :- We use "d" and not "D" to define $\{\phi_j\}$ as "d" represents Precision of our estimation.

The Algorithm :-

Dimension of ancilla = d

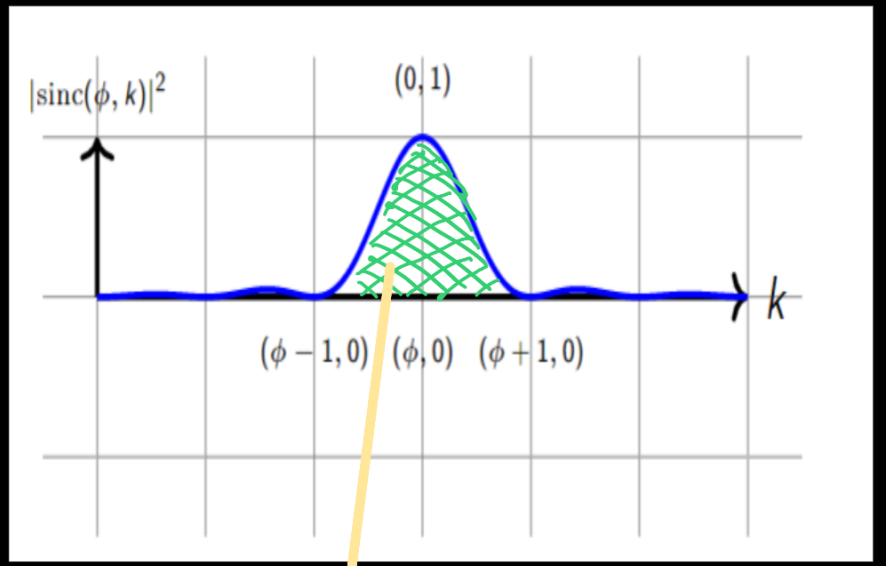
Dimension of target = D



Probability of getting measurement outcome "k" in ancilla when d is large :

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

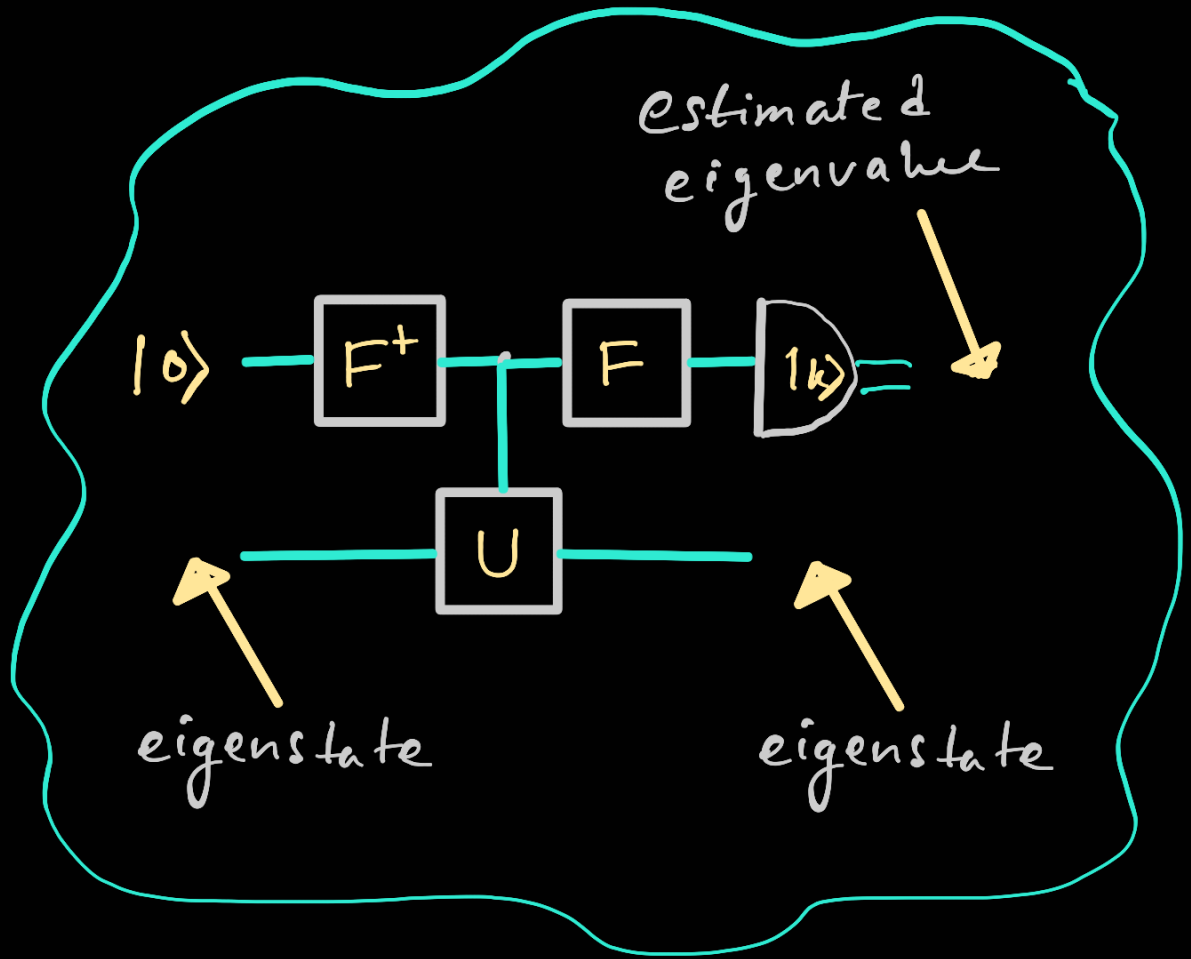
$$|\mathrm{sinc}(\phi,k)^2| = \left|\frac{\sin(\pi(\phi-k))}{\pi(\phi-k)}\right|^2$$



more probable values of "k".

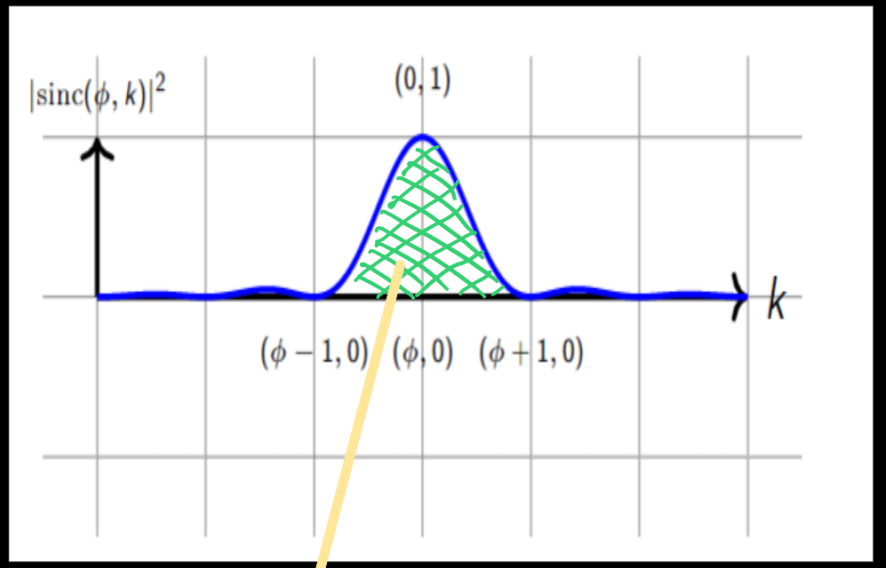
If $\phi \in \mathbb{Z}_d$, then $P_r[\phi = k] = 1$.

Schematics of Algorithm



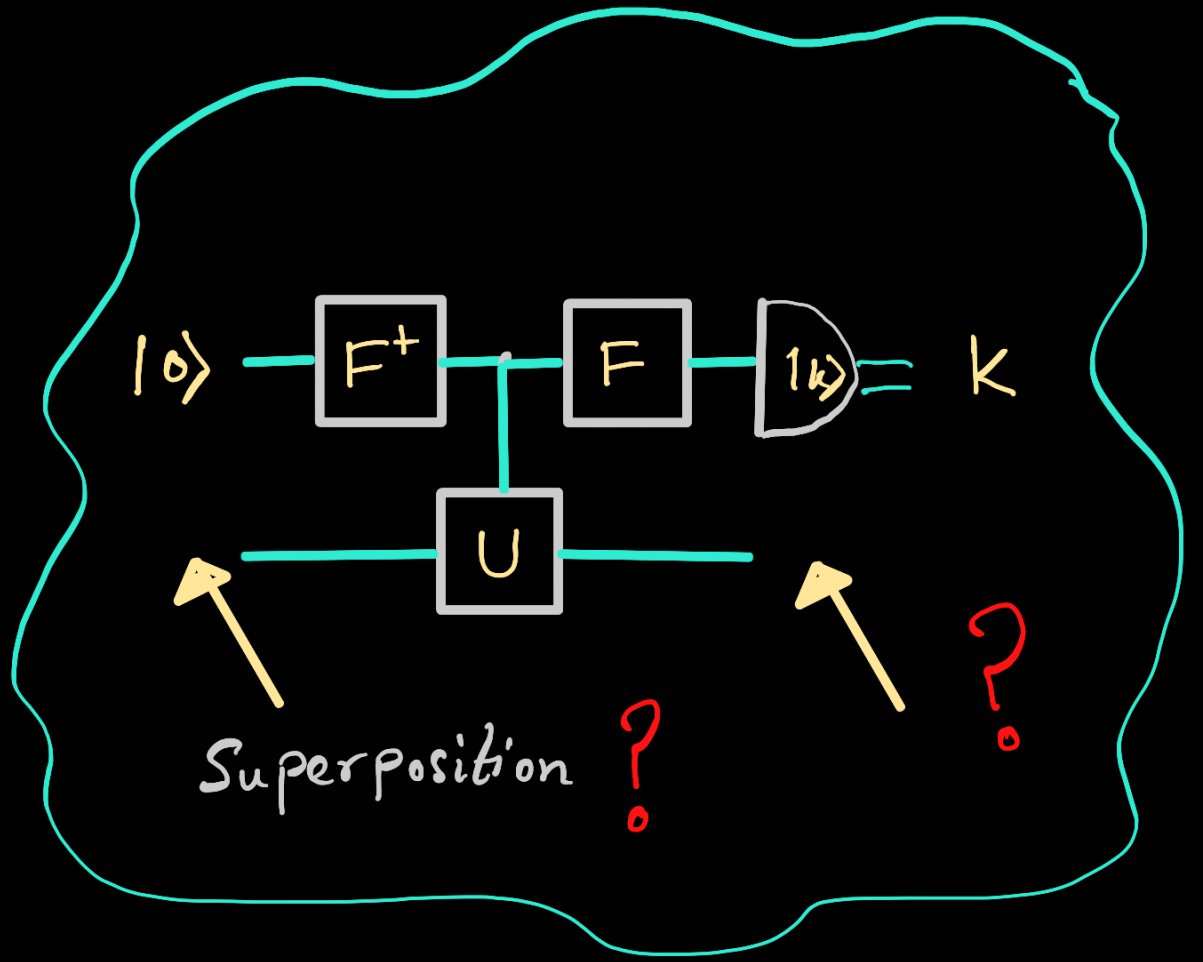
$$\left|\mathrm{sinc}(\phi,k)^2\right| = \left|\frac{\sin(\pi(\phi-k))}{\pi(\phi-k)}\right|^2$$

Schematics of Algorithm



more probable values of "k".

If $\phi \in \mathbb{Z}_d$, then $Pr[\phi=k]=1$.



Superposition

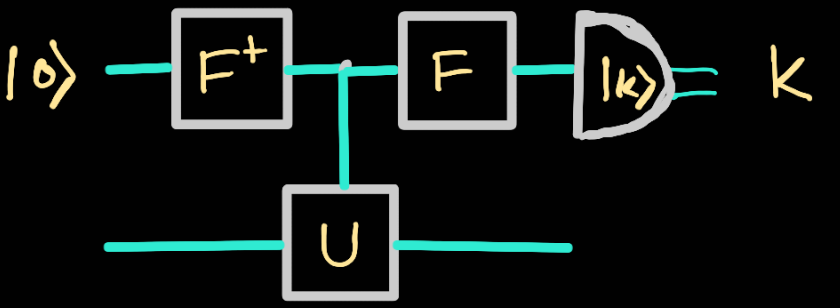
Consider the Quantum instrument :

$$\Lambda(\rho) = \sum_{k \in \mathbb{Z}_d} |k\rangle\langle k| \otimes U_k \rho U_k^+$$

Tracing Quantum Part,

Measurement channel, with POVM $\{M_k\}$.

$U_k =$

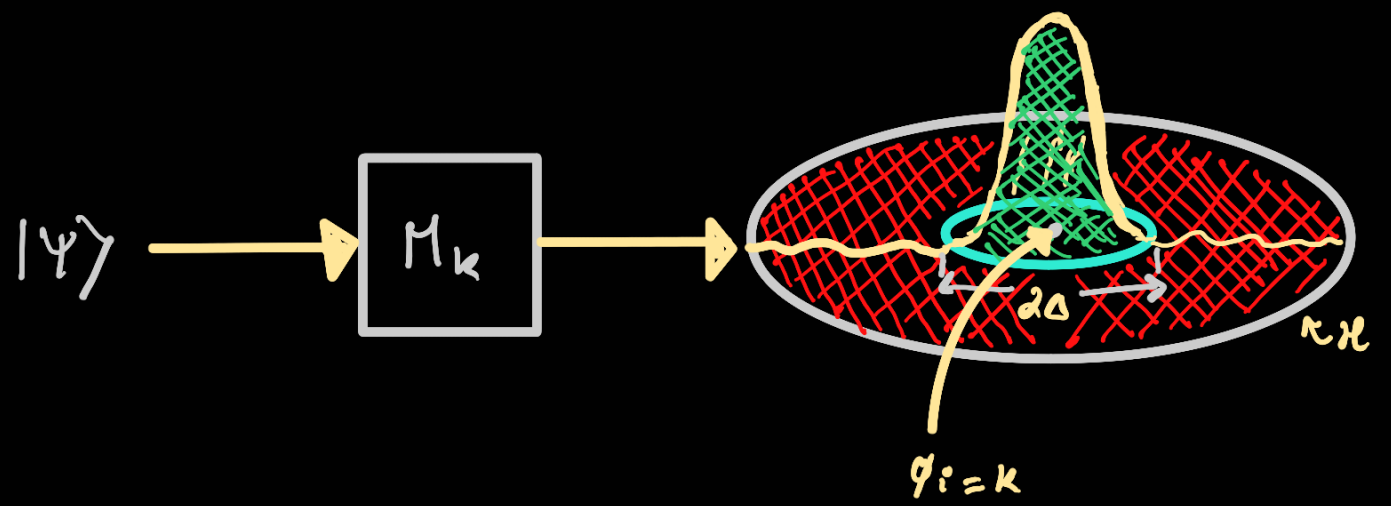


$$M_k := U_k^+ U_k = \sum_{i \in \mathbb{Z}_D} \mathrm{sinc}^2(\pi(\phi_i - k)) \, |\phi_i\rangle\langle\phi_i|$$

POVM as Projectors

$$M_k = \sum_{i \in \mathbb{Z}_D} \operatorname{sinc}^2(\pi(\phi_i - k)) \, |\phi_i\rangle\langle\phi_i|$$

$$\approx \sum_i \mathbb{1}_{-\Delta,\Delta}(\phi_i - k) \, |\phi_i\rangle\langle\phi_i| \quad ; \quad \mathbb{1}_{-\Delta,\Delta}(x) = \begin{cases} 1, & |x| \le \Delta \\ 0, & \text{o.w.} \end{cases}$$

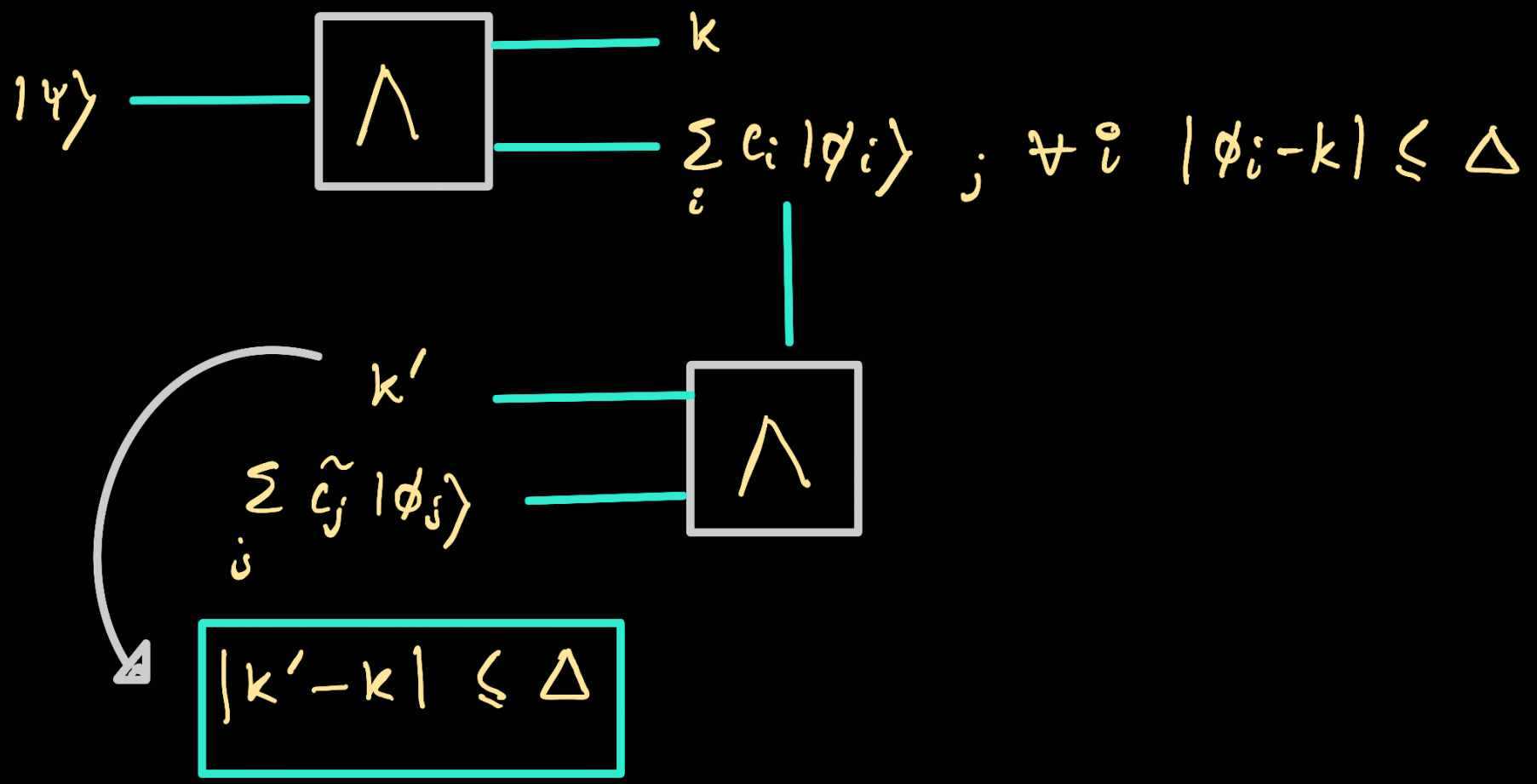


$$\approx \sum_i c_i |\phi_i\rangle$$

$\forall i \; ; \; |\phi_i - k| \le \Delta$

Almost an eigenstate !!

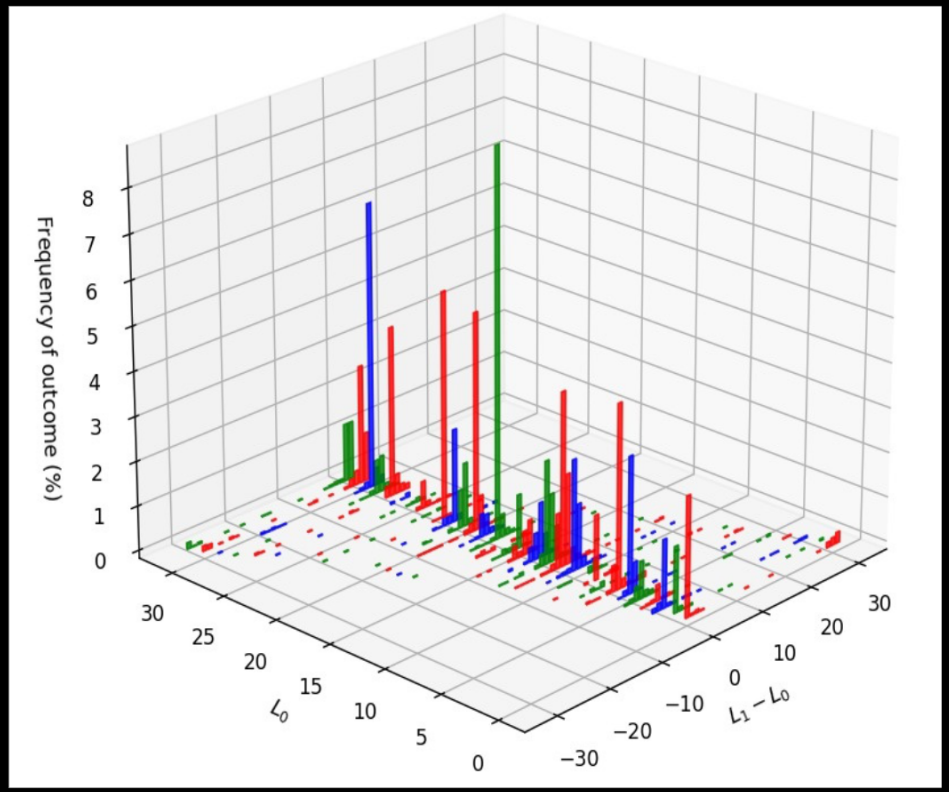
Quantum PUF


$|\psi\rangle$
Λ
k
$\sum_i c_i |\phi_i\rangle$; $\forall i \; |\phi_i - k| \leq \Delta$
k'
$\sum_j \tilde{c}_j |\phi_j\rangle$
Λ
$|k' - k| \leq \Delta$

Simulation Results

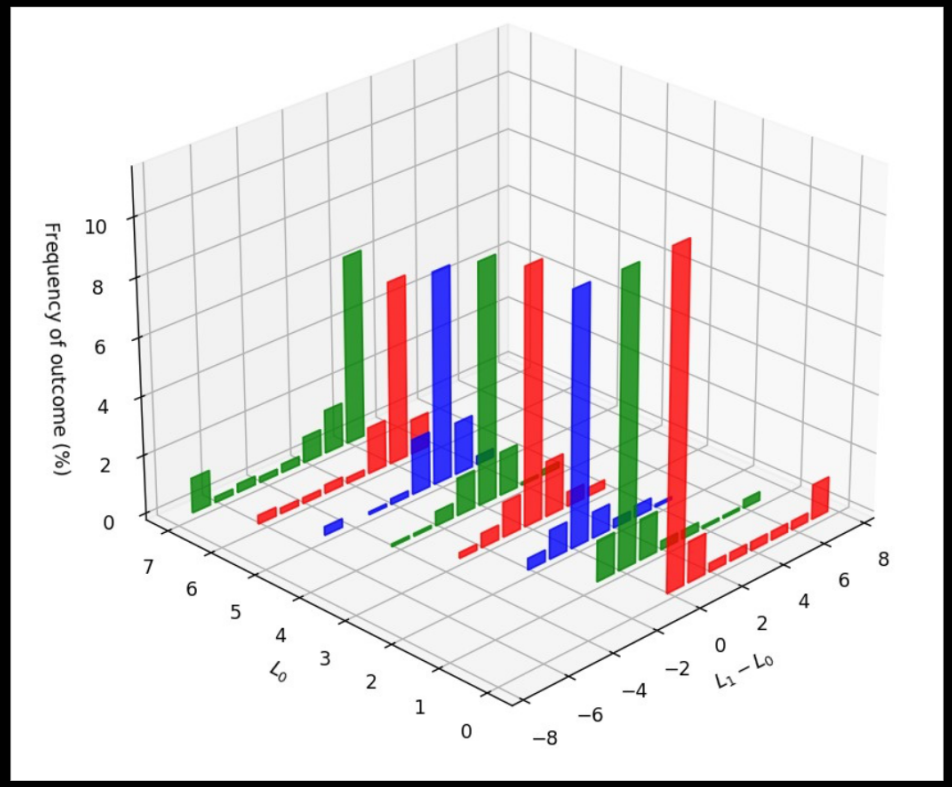
L_0 = Measurement outcome at generation

L_1 = Measurement outcome at verification



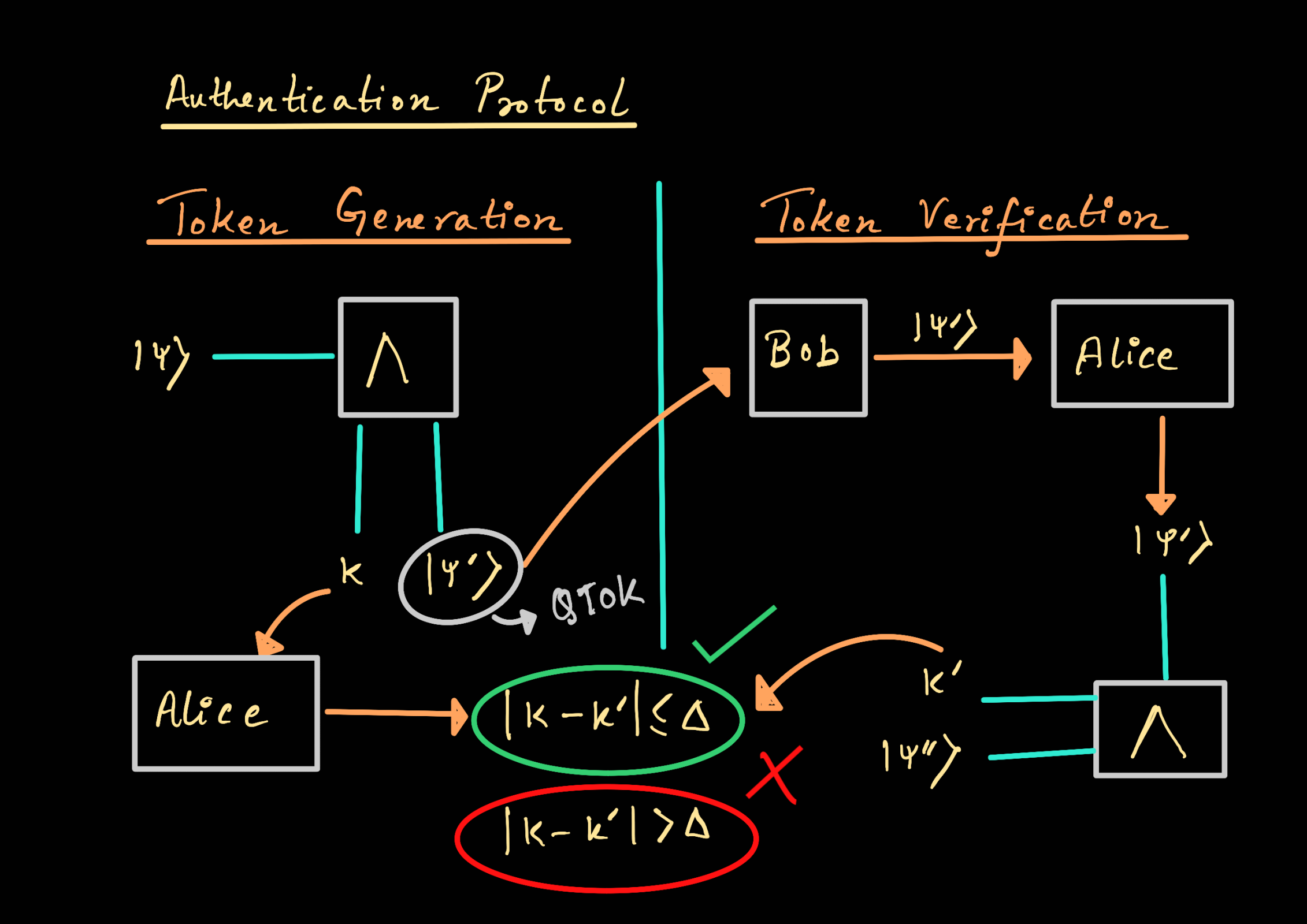
94.6% of total frequency observed for $|L_0 - L_1| \leq 4$.

Ancilla = Target dim = 2^5



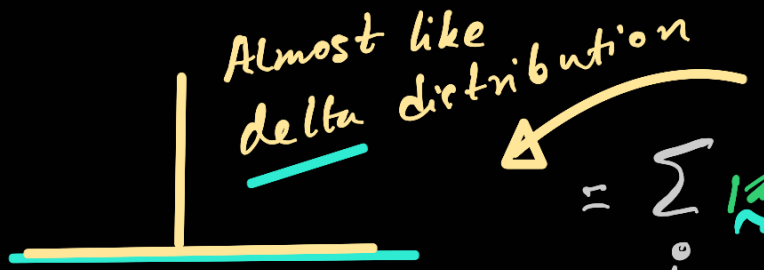
95.3% of total frequency observed for $|L_0 - L_1| \leq 4$.

Ancilla = 2^3, Target = 2^8

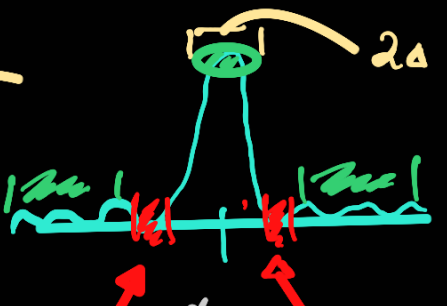

Authentication Protocol
Token Generation
Token Verification
|ψ⟩
Λ
k
|ψ'⟩
QTok
Alice
Bob
|ψ'⟩
Alice
|ψ'⟩
k'
|ψ''⟩
Λ
Alice
|k-k'|≤Δ
|k-k'|>Δ

Security

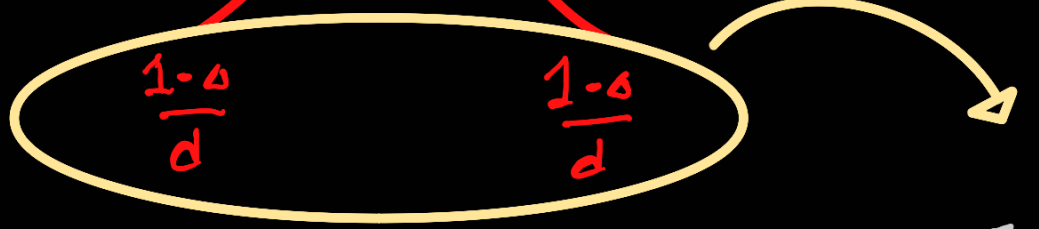
Recall :- $M_k = \sum_i \text{sinc}^2(\phi_i - k)\,|\phi_i\rangle\langle\phi_i|$



$= \sum_i$



$|\phi_i\rangle\langle\phi_i|$



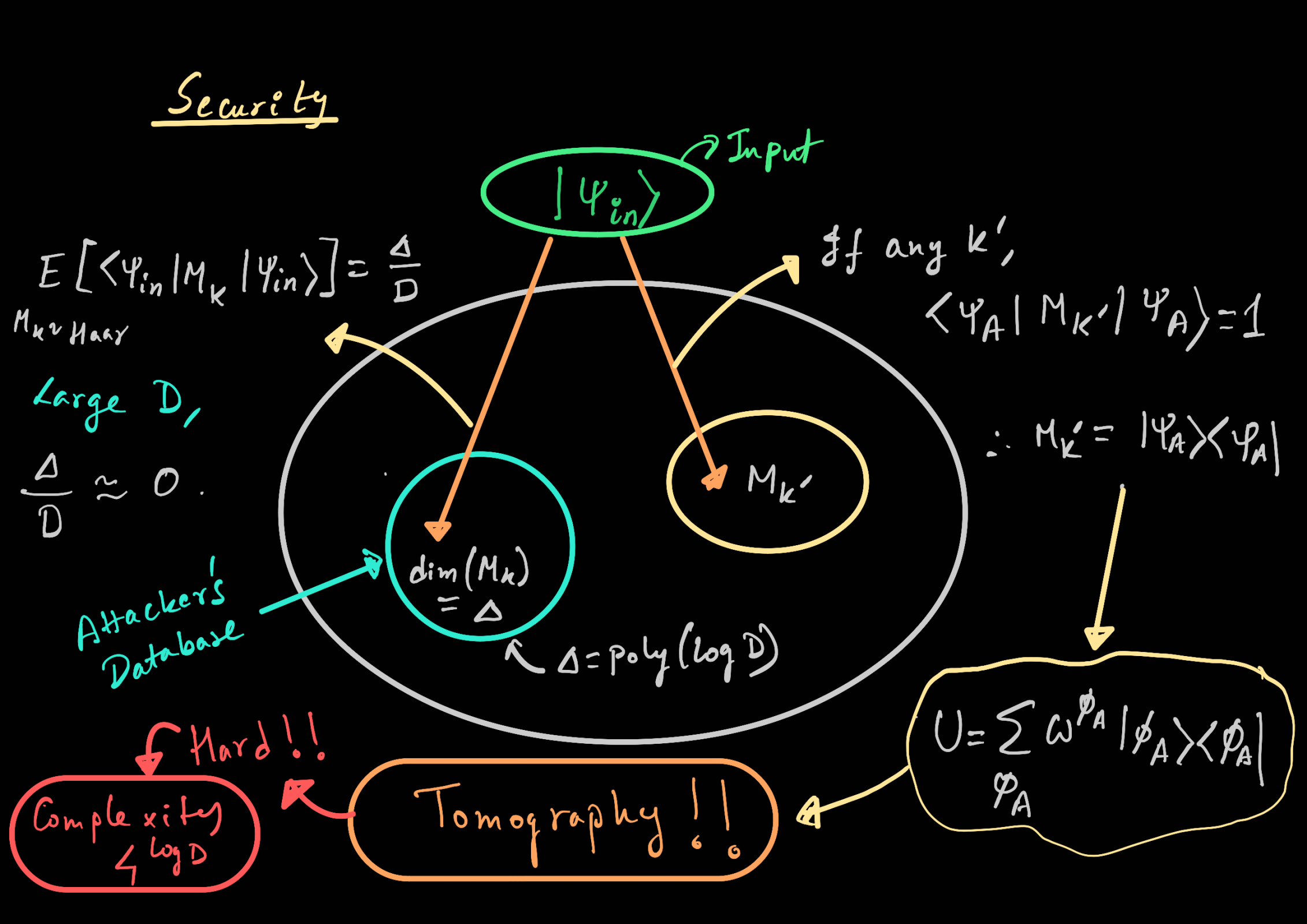
$\therefore \Pr[\phi_i \in \Gamma] = 2\left(\frac{1-\Delta}{d}\right)$

≈ 0 (large d)

$\therefore M_k \approx M_{\phi_i} \approx |\phi_i\rangle\langle\phi_i|$

$\Rightarrow$ $\boxed{U \approx \sum_i \omega^{\phi_i} M_{\phi_i}}$

Security


Input
$|\psi_{in}\rangle$
$E[\langle\psi_{in}|M_K|\psi_{in}\rangle] = \frac{\Delta}{D}$
M_K ~ Haar
Large D,
$\frac{\Delta}{D} \simeq 0$.
If any k',
$\langle\psi_A|M_{K'}|\psi_A\rangle = 1$
$\therefore M_{K'} = |\psi_A\rangle\langle\psi_A|$
$M_{K'}$
$\dim(M_K) = \Delta$
Attacker's Database
$\Delta = \text{poly}(\log D)$
$U = \sum_{\phi_A} \omega^{\phi_A} |\phi_A\rangle\langle\phi_A|$
Tomography !!
Hard !!!
Complexity $\leq \log D$

Thank You For Your Attention.

Chair of Theoretical Information Technology
http://www.ce.cit.tum.de/lti
Technical University of Munich

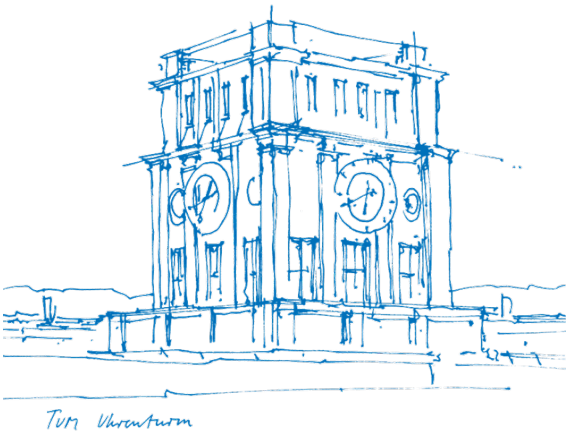
Quantum PUF

An Information Theoretic Perspective

Kumar Nilesh

Chair of Theoretical Information Technology
http://www.ce.cit.tum.de/lti
Technical University of Munich

May 8th, 2023



Secret key generation from cPUF & qPUF

- Classical PUF: DMMS with output RVs X^n and Y^n
- SK Generation: $f : X^n \to K \times M$
- Decoder estimates K: $g : Y^n \times M \to \hat{K}$

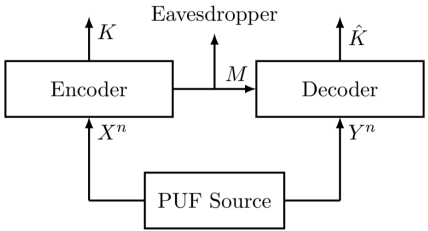


Figure 1

Secret key generation from cPUF & qPUF

- Generalization
  1. $p_X(x) \leftrightarrow \rho \equiv \sum_{x \in \mathcal{X}} p_X(x) |x\rangle\langle x|$
  2. $X \equiv \sum_{x \in \mathcal{X}} x |x\rangle\langle x|$
     - $\mathbb{E}_\rho[X] = \mathrm{Tr}\{X\rho\}$

- A generalization for classical PUF to quantum setting in terms of information theory is also possible.

Secret key generation from cPUF & qPUF

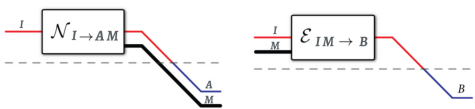
Quantum PUF is assumed to be a quantum channel $\mathcal{N}$

- Encoder: Takes input a pure state ψ^n and outputs a quantum state ρ and a classical state M.
  - This particular channel is known as "Quantum Instrument"

$$|\psi^n\rangle \to \sum_j \mathcal{E}_j(\psi^n) \otimes |j\rangle \langle j|_J$$

- Decoder: Takes input a pure state ϕ^n and a classical state M and outputs a quantum state $\hat{\rho}$.
  - This particular channel is known as "Conditional Quantum Encoder"

$$\mathcal{E}_{IM\to B}(\rho_{IM}) = \mathrm{Tr}_M \left\{ \sum_m p(m)|m\rangle \langle m|_M \otimes \mathcal{E}^m_{I\to B}(\rho^m_A) \right\}$$



Quantum channels are all encompassing

Any physical evaluations, density operators, discarding systems, quantum measurements can be viewed as quantum channels.

- So it is natural to assume any quantum PUF to be some kind of quantum channel.

$$\mathcal{N} = \mathcal{M} \quad \Leftrightarrow \quad (\mathrm{id}_R \otimes \mathcal{N}_{A\to B})(\Phi_{RA}) = (\mathrm{id}_R \otimes \mathcal{M}_{A\to B})(\Phi_{RA})$$

[**?**][Mohseni et. al. 2006]

Requirement for achievable SK generation/privacy

A tuple $(R, L), R, L \geqslant 0$, is an **achievable SK generation/privacy leakage rate pair** if for all $\delta > 0$ there is an $n_0 \in \mathbb{N}$ and a $c > 0$ such that for all $n \geqslant n_0$ there is a SK generation protocol (F, g) such that

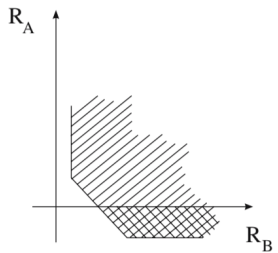
$$\begin{aligned}
&\Pr(K \neq \hat{K}) \leqslant \exp(-nc) \\
&I(K \wedge M) = 0 \\
&H(K) = \log |\mathcal{K}| \\
&\frac{1}{n} \log |\mathcal{K}| \geqslant R - \delta \\
&\frac{1}{n} I\left(M \wedge X^n\right) \leqslant L + \delta.
\end{aligned}$$

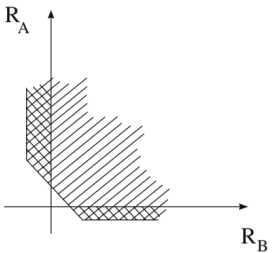
We call the set of all such achievable rate pairs the capacity region $\mathcal{R}_{SK}^{PL}$.

Bounding of Privacy Leakage

- Information content in M about the input state ψ^n.
- $I(A\rangle B) = S(B) - S(AB) \neq 0$
- Intresting case of Quantum Partial Information $S(A|B)$
- Quantum optimality with free classical resource assumption

$$[q \to q] = [qq]$$





Distributed Compression

References

1. Baur, S. J. (2021). Secret Key Generation with Perfect Secrecy; Source Uncertainty and Jamming Attacks (Doctoral dissertation, Technische Universität München).
2. Ignatenko, T., & Willems, F. M. (2012). Biometric security from an information-theoretical perspective. Foundations and Trends® in Communications and Information Theory, 7(2–3), 135-316.
3. Wilde, M. M. (2011). From classical to quantum Shannon theory. arXiv preprint arXiv:1106.1445.
4. Horodecki, M., Oppenheim, J., & Winter, A. (2007). Quantum state merging and negative information. Communications in Mathematical Physics, 269, 107-136.