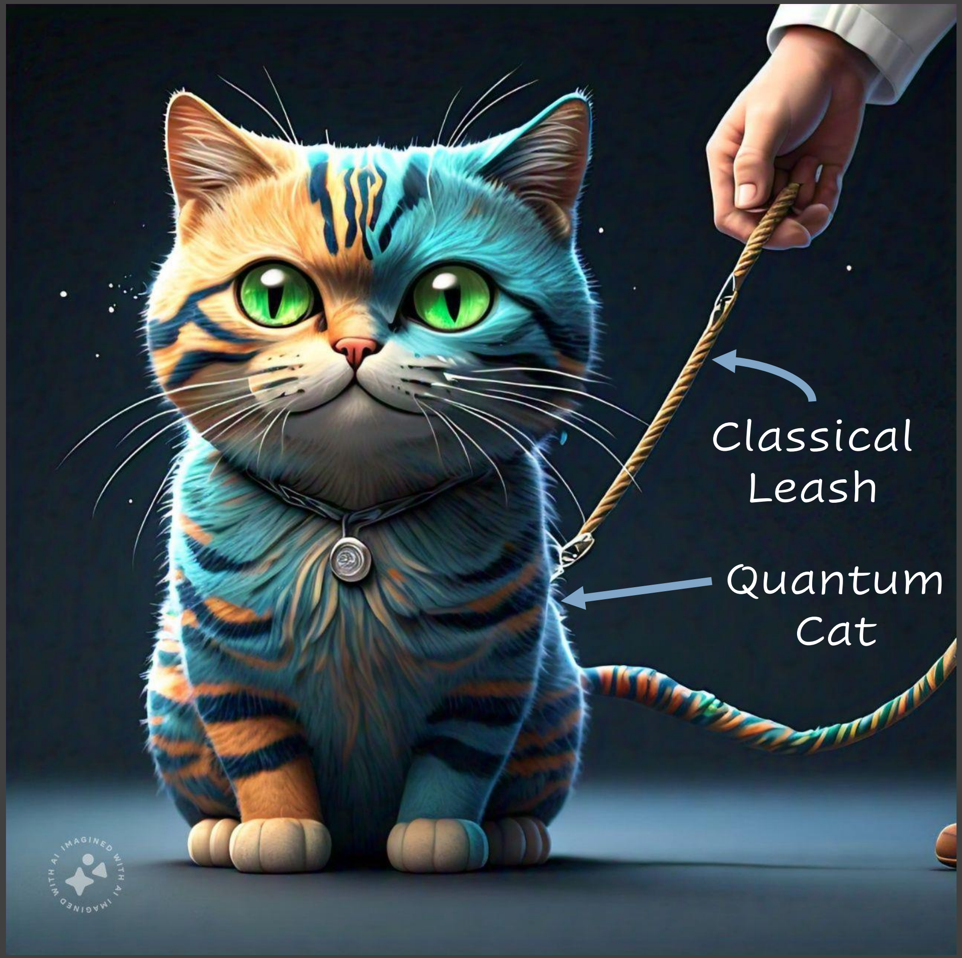


CLASSICAL VERIFICATION OF QUANTUM COMPUTATIONS

COL872: Lattices in CS

Anish Banerjee

Shankh Gupta

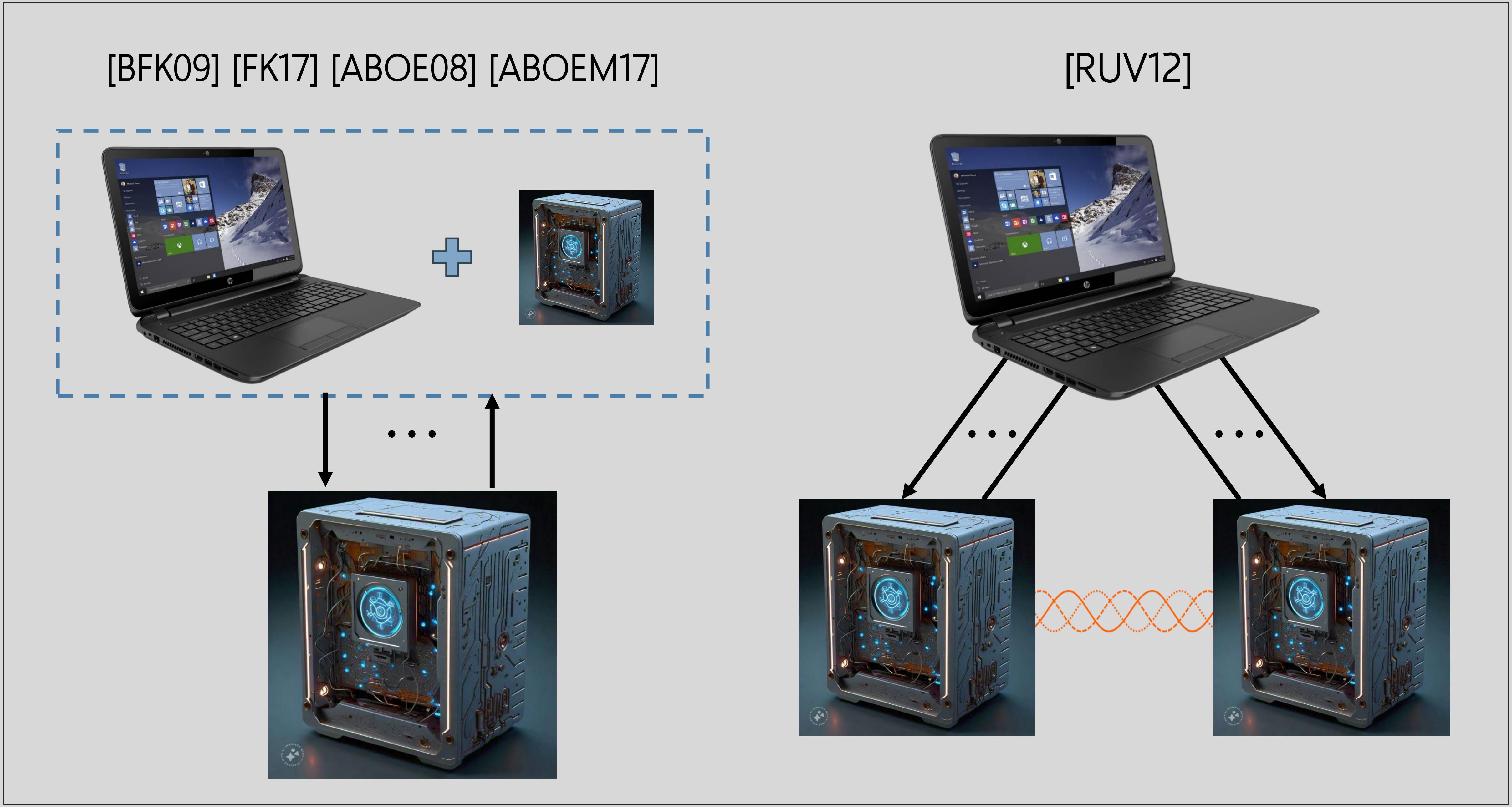
Based on the [Mah23] of the same name

HISTORY

[Got04] : Is it possible for an **efficient classical verifier** to verify the output of an **efficient quantum prover**?

IP=PSPACE and BQP $\subseteq$ PSPACE
$\Rightarrow$ BQP $\subseteq$ IP

But prover in IP is all powerful!
Can we work with an **efficient quantum** prover?


[BFK09] [FK17] [ABOE08] [ABOEM17]
[RUV12]

Main Results (Informal)

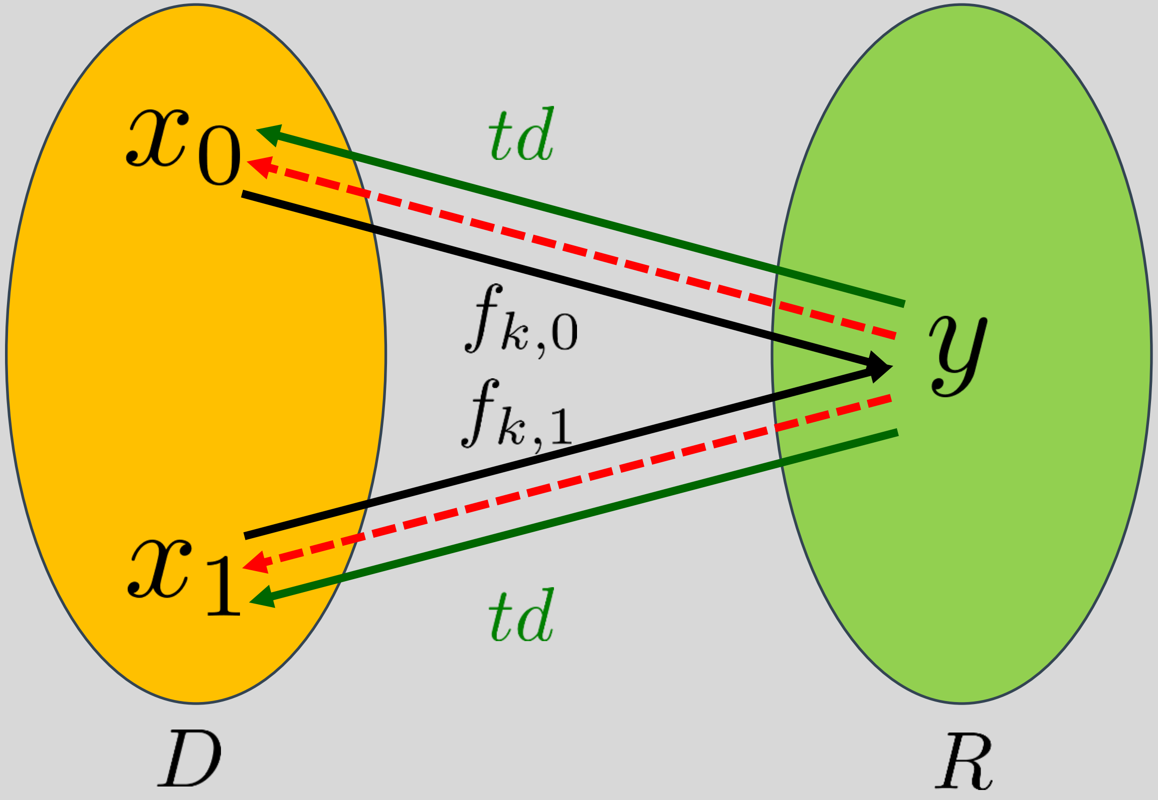
LWE is hard for a BQP machine

There exists an **extended trapdoor claw-free family**.

All decision problems in BQP can be verified by an efficient classical machine through interaction.

Trapdoor Claw-free functions

$f_{k,0}, f_{k,1} : D \to R$
Injective, same range



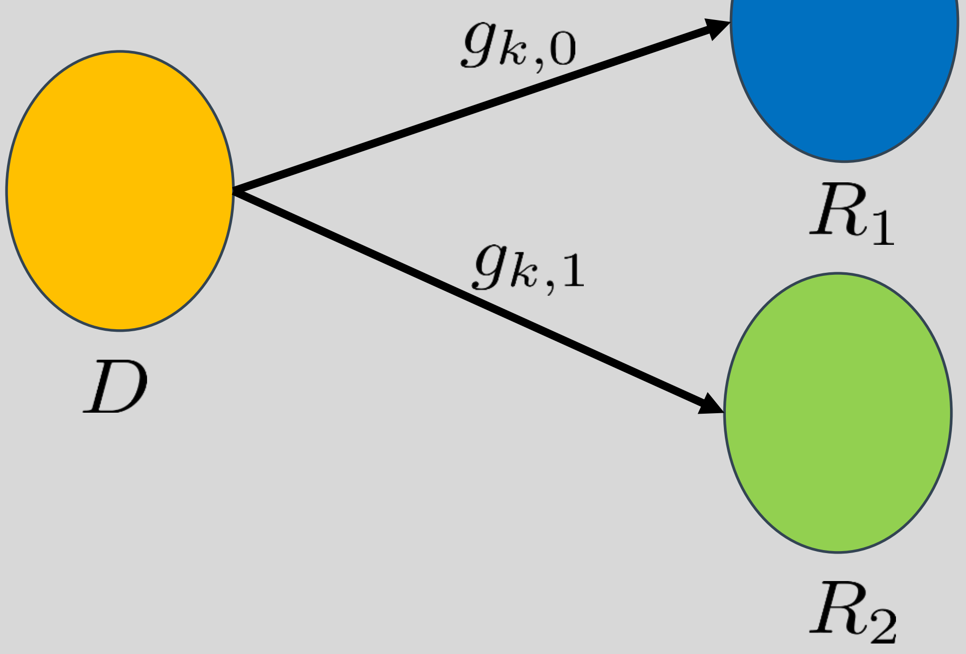
Hard to find a **claw** (x_0, x_1) such that $f_{k,0}(x_0) = f_{k,1}(x_1)$ without td.

Also satisfies two other **hardcore bit** properties

Trapdoor Injective Functions

$g_{k,0}, g_{k,1} : D \to R$

Injective, disjoint range



Given $y=g_{k,b}(x)$, hard to find (b,x) without td.

ETCF=TCF+TIF+Injective Invariance

Hard to distinguish between (f_0,f_1) and (g_0,g_1)

Relation to this course

- ETCFs are built using LWE.
- Extensively used in the construction of several verification protocols.
- However, we only have **approximate constructions.**
- We want to study these constructions and understand why we don't have exact.

Hadamard & Standard Basis Measurements

$$|\psi\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle = \alpha_0 \begin{pmatrix} 1 \\ 0 \end{pmatrix} + \alpha_1 \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} \alpha_0 \\ \alpha_1 \end{pmatrix}$$

Standard Basis

Obtain b with probability $|\alpha_b^2|$

Hadamard Basis

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

$$H|\psi\rangle = \frac{1}{\sqrt{2}}(\alpha_0 + \alpha_1)|0\rangle + \frac{1}{\sqrt{2}}(\alpha_0 - \alpha_1)|1\rangle$$

Obtain b with probability $\frac{1}{2}\left|\alpha_0 + (-1)^b \alpha_1\right|^2$

Classical Notion of Verification

Verifier

Reduce the problem into a 3-SAT instance ϕ

Asks for a satisfying assignment

Assignment τ

Verify that τ satisfies the instance ϕ

Prover (unbounded)

Quantum Analogue of NP

Verifier

Reduce the problem to a Local Hamiltonian H.

Asks for a ground state

Sends n-qubit quantum state ρ

Verify that ρ has low energy w.r.t. H

Prover

- [BL08] H, S measurements are sufficient to estimate energy.
- [MF16] Using H,S measurements, we can verify results of any BQP computation

Measurement Protocol

Goal: Force the prover to behave as the verifier's trusted measurement device

Ideal Functionality

Constructs an n-qubit state **ρ**

Chooses either H/S
basis measurement for each qubit

Outputs measurement result of **ρ**
in the chosen basis

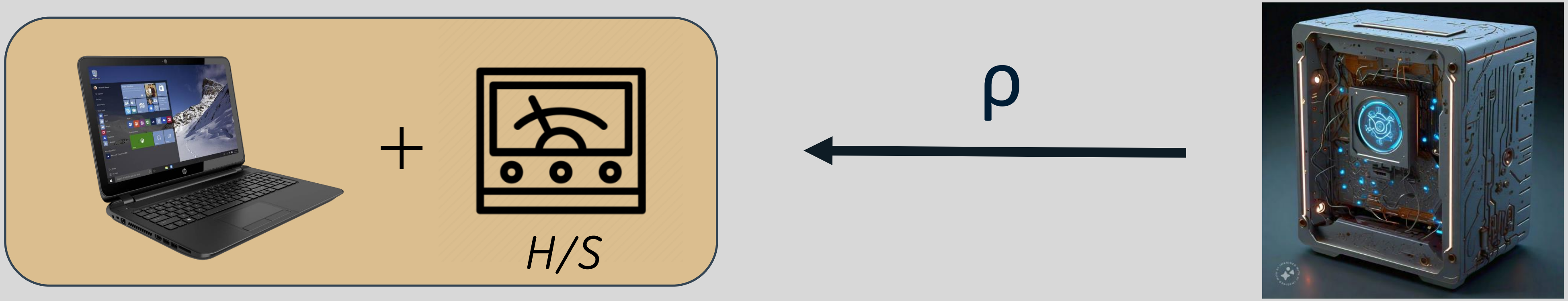
Verifier

Prover

Soundness:
If the verifier accepts, there exists ***a quantum state independent of the verifier's measurement choice*** underlying the measurement results

Using Measurement Protocol for Verification

- The measurement protocol implements the following model :



- Prover sends n-qubit state **ρ** and verifier measures the state.

- We can show that quantum computations can be verified in the above model.

Measurement Protocol Outline

Verifier chooses either H/S basis for each qubit

Verifier

Sends (f_0, f_1) or (g_0, g_1) for each qubit

Sends measurement results $\{y_i\}_{i\in[n]}$

Requests a H/S basis measurement

Response

Prover

Hadamard Basis Measurement

Sample $(f_0, f_1, td) \leftarrow$ TCF.Setup()

f_0, f_1 →

← $y \leftarrow f_b(x)$

Computes $x_{0,y}$ & $x_{1,y}$ using td

Chooses $|\psi\rangle = \alpha_0 |0\rangle + \alpha_1 |1\rangle$

Apply f_0, f_1 (in superposition) on state $|\psi\rangle$

$$|\psi_1\rangle = \sum_{b\in\{0,1\}} \sum_{x\in\mathcal{X}} \alpha_b |b\rangle |x\rangle |f_b(x)\rangle$$

Measure the final register, obtaining $y \in \mathcal{Y}$

$$|\psi_2\rangle = \alpha_0 |0\rangle |x_{0,y}\rangle + \alpha_1 |1\rangle |x_{1,y}\rangle$$

Hadamard Basis Measurement (cont.)

$$m \leftarrow b' \oplus d.(x_{0,y} \oplus x_{1,y})$$

d, b'

Applies Hadamard Transform and measures the pre-image register obtaining d

$$X^{d.(x_{0,y} \oplus x_{1,y})} H|\psi\rangle$$

Finally, perform measurement in the Standard basis to obtain b'

Standard Basis Measurement

Sample $(g_0, g_1, td) \leftarrow$ TIF.Setup()

g_0, g_1

$y \leftarrow g_b(x)$

Computes b & $x_{b,y}$ using td

Chooses $|\psi\rangle = \alpha_0 |0\rangle + \alpha_1 |1\rangle$

Apply g_0, g_1 (in superposition) on state $|\psi\rangle$

$$|\psi_1\rangle = \sum_{b\in\{0,1\}} \sum_{x\in\mathcal{X}} \alpha_b |b\rangle|x\rangle|g_b(x)\rangle$$

Measure the final register, obtaining $y \in \mathcal{Y}$

$$|b\rangle|x_{b,y}\rangle$$

Conclusion

- Verifiable, secure delegation of quantum computations is possible with a classical machine
- Rely on quantum secure Trapdoor claw-free functions (from Learning with Errors).

THANK YOU