

LECTURE 25.

- * Wrap up local Hamiltonian, story of CVQC
- * Quantum Money
- * Quantum Lightning ... One-shot Signatures

LOCAL HAMILTONIAN

Given a T-gates quantum circuit C , with input x , we define the local Hamiltonian H_C as

$$H_C = - \sum_{i,j} \underbrace{J_{ij}}_{\text{Hermitian matrix}} \underbrace{(\sigma_{x_i} \sigma_{x_j} + \sigma_{z_i} \sigma_{z_j})}_{\text{real coefficients}}$$

$(i \neq j \in \text{poly}(T))$

efficiently computable from C , input x .

I. \exists a state $|\psi\rangle$ such that

$$\Pr[C(x, |\psi\rangle) = 1] \geq \frac{2}{3} \iff \text{smallest eigenvalue}$$

of H_C is \leq some fixed "a".

$$\boxed{\text{I}} \quad \forall \text{ states } |\psi\rangle, \quad \Pr [c(x, |\psi\rangle) = 1] \leq \frac{1}{3}$$

\Leftrightarrow Smallest eigenvalue of $H_c \geq a + \delta$
 $\hookrightarrow \frac{1}{\text{poly}(n)}$

To check if C outputs 1 w.p. $\geq \frac{2}{3}$,

it suffices to check that \exists a quantum state $|\psi\rangle$

(eigenstate of H_c with smallest eigenvalues)

that passes certain statistical tests.

(QMA) :

$$\mathcal{L}_c = \left\{ x \text{ s.t. } \exists |\psi\rangle \text{ s.t. } \Pr [c(x, |\psi\rangle) = 1] \geq \frac{2}{3} \right\}$$

$$|c| = \text{poly}(|x|)$$

NP :

$$\mathcal{L}_c = \left\{ x \text{ s.t. } \exists w \text{ s.t. } c(x, w) = 1 \right\}$$

$$|c| = \text{poly}(|x|)$$

Fitzsimmons - Morimae (Lecture 5 of Notes)

\mathcal{P}

(C, x)

$\exists |\psi\rangle$ s.t. $C(x, |\psi\rangle) = 1$

Compute $H_C, \{J_{ij}\}_{i,j}$

$|\tilde{\psi}\rangle$: eigenstate of H_C with smallest eigenvalue.

(Eigenstate: $\exists \lambda$ s.t. $H_C |\tilde{\psi}\rangle = \lambda |\tilde{\psi}\rangle$)

Send $|\tilde{\psi}\rangle$ to V qubit-by-qubit

Capabilities:

1) Hold one qubit in memory;

2) Measure qubit in X or Z basis

(C, x)

Compute $H_C, \{J_{ij}\}_{i,j}$

Measures each qubit in basis $W, W \leftarrow \{X, Z\}$

write down the outcome.

Statistical classical test

$(\{J_{ij}, \text{measurement outcomes}\})$
or

QUANTUM MONEY

Wiesner $\{ |0\rangle, |1\rangle, |+\rangle, |-\rangle \}$.

Notes that cannot be counterfeited

Bank. : outputs quantum states (bills).

Each bill has :

1) A classical serial number s .

2) A quantum state $|\Psi_{f(s)}\rangle$ (n qubits)

Each qubit in $|\Psi\rangle$:

$$\begin{cases} |\Psi_{00}\rangle = |0\rangle \\ |\Psi_{01}\rangle = |1\rangle \\ |\Psi_{10}\rangle = |+\rangle \\ |\Psi_{11}\rangle = |-\rangle \end{cases}$$

- First compute $y = f_k(s)$.
- Set first qubit in $|\Psi\rangle$ to be $|\Psi_{y_1 y_2}\rangle$,
second y " $|\Psi_{y_3 y_4}\rangle$...

Verification: Given bill, test if it is authentic.

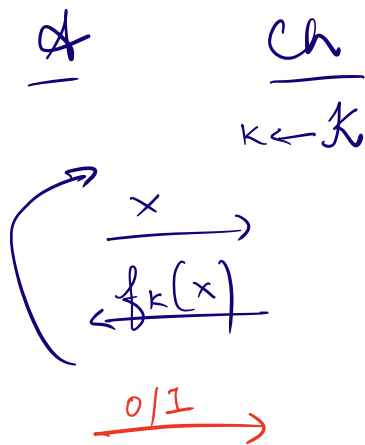
$(s, |\psi\rangle)$

Compute $y = f_k(s)$, check if

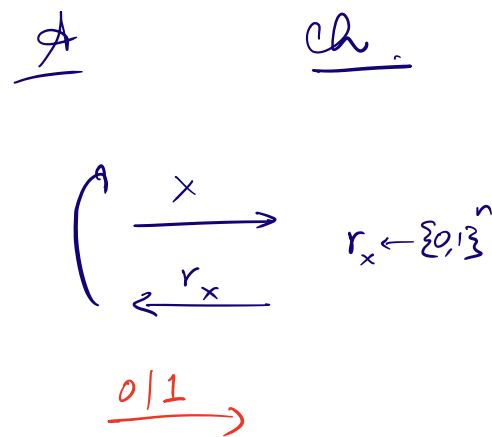
- first qubit in $|\psi\rangle$ is $|\psi_{y_1 y_2}\rangle$,
- second " " " $|\psi_{y_3 y_4}\rangle$...

Security relies on the fact that $f_k(\cdot)$ is a pseudo-random function (PRF).

Expt₀



Expt₁



\forall QPPT A ,

$$\left| \Pr [\text{Expt}_0 = 1] - \Pr [\text{Expt}_1 = 1] \right| \leq \text{negl}(n).$$

where $|\mathcal{K}| = n$.

$|0\rangle$ basis: computational $|0\rangle$

basis: Hadamard $|+\rangle$ w.p. $\frac{1}{2}$

$|-\rangle$ w.p. $\frac{1}{2}$
 $|+\rangle$ or $|-\rangle$.

OPEN:

Public - Key Quantum Money from LWE

KNOWN:

n n from obfuscation.

A

Bank.

$\leftarrow s, |\psi_{(s)}\rangle$

$\dots \rightarrow (|1\rangle, \dots)$

$S, |\psi\rangle = |0\rangle \otimes \dots \otimes |1\rangle$ (last $n-1$ qubits)

Yes, return $|\psi\rangle$

Elitzur - Vaidman Bomb

MPC

CCA security

signing keys

FE

Malicious FHE

iD.

U U

erase info
computationally.
