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

Hermitian matrix

$$H_C = -\sum_{i,j} \frac{J_{ij}}{2} \left(\sigma_{x_i} \sigma_{x_j} + \sigma_{z_i} \sigma_{z_j} \right)$$

$(i \neq j \in poly(T))$

real coefficients

efficiently computable from C, input x.

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

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

of H_C is $\leq$ some fixed "a".

II. $\forall$ states $|\psi\rangle$, $\Pr\left[C(x,|\psi\rangle)=1\right] \leq \frac{1}{3}$

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

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):

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

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)

Capabilities:
1) Hold one qubit in memory
2) Measure qubit in X or Z basis

$\mathcal{P}$

(C, x)

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

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

$|\tilde{\psi}\rangle$: 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

(C, x)

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

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

write down the outcome.

Statistical classical test (J_{ij}, measurement outcomes) on

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 " " $|\psi_{y_3 y_4}\rangle$ ....

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).

Expmt$_0$

$\mathcal{A}$ | Ch

$k \leftarrow \mathcal{K}$

$\mathcal{A} \xrightarrow{x}$

$\mathcal{A} \xleftarrow{f_k(x)}$

$\mathcal{A} \xrightarrow{0/1}$

Expmt$_1$

$\mathcal{A}$ | Ch

$\mathcal{A} \xrightarrow{x}$

$r_x \leftarrow \{0,1\}^n$

$\mathcal{A} \xleftarrow{r_x}$

$\mathcal{A} \xrightarrow{0/1}$

$\forall$ QPPT $\mathcal{A}$,

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

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

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

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

"−" w.p. $\frac{1}{2}$

$|+\rangle$ or $|-\rangle$.

OPEN:

Public-Key Quantum Money from LWE

KNOWN:

" " from obfuscation.

A Bank.

$s, |\psi_{f(s)}\rangle$ ←

$\ldots \to |s\rangle(|\psi_{\ldots}\rangle)$

S, $|\psi'\rangle = |0\rangle(|\psi_{fix}\rangle$ / last n-1 qubits

2 ← Yes, return $|\psi'\rangle$

Elitzur- Vaidman Bomb

MPC

CCA security | Signing keys

FE

Malicious FHE

iO.

V U

erase info computationally.