CS6846 – Quantum Algorithms and Cryptography

Quantum PKE and FHE

Instructor: Shweta Agrawal, IIT Madras
Email: shweta@cse.iitm.ac.in

Quantum Public Key Enc

Recollect QOTP (a, b, ρ):

$X^a Z^b \rho (X^a Z^b)^\dagger$ where $a, b \leftarrow \{0,1\}$.

Let Π be a classical, Q-secure PKE

QKeyGen(1^λ): ① Π. Keygen $(1^\lambda) \to$ PK, SK

② Output (PK, SK).

QEnc$(\rho$, PK$)$:

① Pick $a, b \leftarrow \{0,1\}$

② Perform QOTP$(a, b, \rho) = \rho'$

③ Enc (a, b) using Q-secure PKE $= \Pi.ct$

④ O/P

Dec (SK, CT):

① Dec Π. ct using Π. SK $\Rightarrow a, b$

② Recover ρ using QOTP dec.

Correctness follows from that of QOTP & Π.

Security: $CT(\rho_0) \approx CT(\rho_1)$.

$QOTP(\rho_0), \Pi.ct_{(a,b)}$

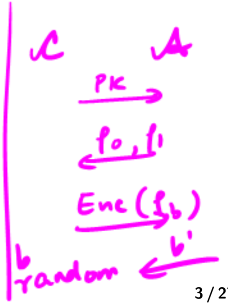
Hyb 0: Adv sees PK, $CT(\rho_0) = \rho', \Pi.ct_{a,b}$

Hyb 1: Change Π ct to enc $(0,0)$ instead of (a,b). $\rho' = QOTP(\rho_0), \Pi.ct(0,0)$

Hyb 2: Replace QOTP with ρ_1

Replace Π ct w/ (a,b)

Hyb 3: Adv sees PK, $CT(\rho_1)$



Hyb 0 & Hyb 1 are indist if Π is secure (Classical)

PKE Chal.	PKE Adv / QPKE Ch $\underline{\underline{\mathcal{B}}}$	Q PKE Adv. $\underline{\underline{\mathcal{A}}}$

$\xrightarrow{\Pi.PK}$ $\qquad$ $\xrightarrow{\text{QPKE PK}}$

$\xleftarrow[(a,b)\,,\,(0,0)]{m_0 \qquad m_1}$ $\qquad$ compute QOTP of ρ_0 as ρ' $\qquad$ $\xleftarrow{\rho_0,\ \rho_1}$

$\xrightarrow{\Pi.ct(m_b)}$ $\qquad$ $\xrightarrow{\text{Return } \rho',\ \Pi.ct(m_b)}$

$\xleftarrow{b'}$ $\qquad$ $\xleftarrow{b'}$

$\underset{\sim\sim\sim}{\text{Q-FHE}}$

$$\mathrm{Enc}\left(\frac{|0\rangle + |1\rangle}{\cancel{\sqrt{2}}}\right) \stackrel{?}{=} \mathrm{Enc}(|0\rangle) + \mathrm{Enc}(|1\rangle)\ ?$$

$$\underline{\alpha}|0\rangle + \underline{\beta}|1\rangle$$

$$H(|0\rangle) = |+\rangle. \qquad H\left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right) = |0\rangle.$$

$$\frac{1}{2}\left(|0\rangle + \cancel{|1\rangle} + |0\rangle - \cancel{|1\rangle}\right) = |0\rangle.$$

$$\mathrm{Enc}\,|0\rangle + \underbrace{\cancel{\mathrm{Enc}\,|1\rangle}} + \mathrm{Enc}\,|0\rangle - \underbrace{\cancel{\mathrm{Enc}\,|1\rangle}}$$

$$|0\rangle = \begin{pmatrix}1\\0\end{pmatrix} \qquad |1\rangle = \begin{pmatrix}0\\1\end{pmatrix}$$

Evaluate Quantum Ckts:

- QOTP (a, b, ρ)
- Classical FHE. (a, b)

Z gate:

have $CT = \underbrace{X^a Z^b \rho (X^a Z^b)^\dagger}_{\rho'}$, $enc(a, b)$.

$\longrightarrow enc(a, b \oplus 1)$

Say I want CT for $\underline{\underline{Z \rho Z^\dagger}}$.

$$\rho' = X^a Z^b \rho (X^a Z^b)^\dagger$$

$$= X^a Z^{b \oplus 1} \underline{\underline{Z \rho Z^\dagger}} Z^{\dagger(b \oplus 1)} X^{\dagger a}$$

Similar idea works for (say) X.

Universal Gates

"Clifford Group" + Toffoli.

Generated by

(H, S, CNOT). Includes Pauli Gates.

S ↓ Phase shift

Useful Property of Clifford Gates:

$\forall (x, z) \ \exists \ (x', z')$ s.t. $\forall \ |\psi\rangle$

$$C X^{x} Z^{z} |\psi\rangle = X^{x'} Z^{z'} C|\psi\rangle$$

where C is a Clifford Gate.

Have $\rho' = \text{QOTP}(x, z, \rho)$, $\Pi.\text{ct}(x, z)$

Compute $C\rho' C^\dagger = C X^x Z^z \rho (X^x Z^z)^\dagger C^\dagger$

$= X^{x'} Z^{z'} \underbrace{C \rho C^\dagger}_{\text{what I wanted}} (X^{x'} Z^{z'})^\dagger$

Update $\Pi.\text{ct}(x, z)$ to $\Pi.\text{ct}(x', z')$.

Handling Toffoli Gates:

Mahadev '20

Trapdoor Claw-Free function Pairs:

A TCF function pair is a pair of functions (f_0, f_1) s.t.:

1) Both are injective & have the same image.

2). It is hard to find a "claw" i.e. x_0, x_1 s.t. $f_0(x_0) = f_1(x_1)$.

3). Can find it using "trapdoor" given any y in image

Obtain superposition over a claw:

Given f_0, f_1, want to compute

$$\frac{1}{\sqrt{2}}\left(|0, x_0\rangle + |1, x_1\rangle\right) \text{ s.t. } f(x_0) = f(x_1).$$

How?

1). Prepare uniform superposition

$$|\psi\rangle = \sum_{\substack{b \in \{0,1\} \\ x \in \{0,1\}^\lambda}} |b\rangle |x\rangle |0\rangle.$$

2). $(b, x, y) \to (b, x, f_b(x) \oplus y)$.

So we get

$$\sum_{b,x} |b\rangle\, |x\rangle\, |f_b(x)\rangle$$

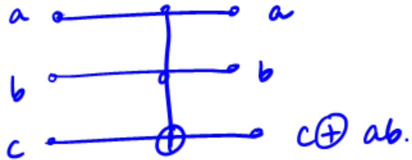
3). Measure last register.

$$\sum_{x : f_b(x) = y} |b\rangle\, |x_b\rangle\, \cancel{|y\rangle}.$$

$$\Rightarrow \quad |0\rangle\, |x_0\rangle + |1\rangle\, |x\rangle \quad \text{where} \quad f_0(x_0) = f_1(x_1).$$

QFHE.

Want to support Clifford, Toffoli



Say we start with

$$|\psi'\rangle = X^{x'} Z^{z'} \underline{T} |\psi\rangle.$$

$$T\, |\psi'\rangle = \underbrace{\left(T\, X^{x}\, Z^{z}\, T^{\dagger}\right)}_{X^{x'} Z^{z'}} T\, |\psi\rangle$$

Need to convert our state to this form!

Recall: QPKE is QOTP & CPKE

quantum, classical

FACT

$$\underbrace{T}X^{x}Z^{z}T^{\dagger} = T\left(X^{x_1}Z^{z_1}\otimes X^{x_2}Z^{z_2}\otimes X^{x_3}Z^{z_3}\right)T^{\dagger}$$

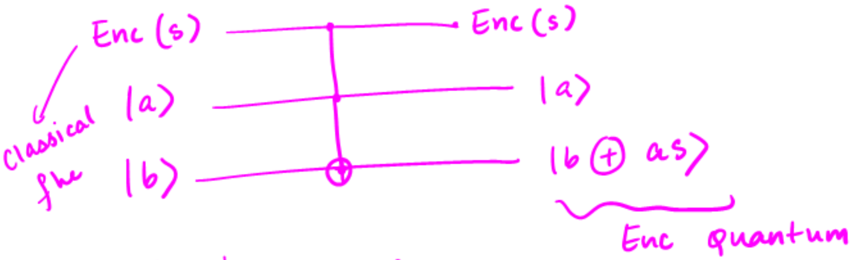
$$= \mathrm{CNOT}^{x_2}_{1,3}\,\mathrm{CNOT}^{x_1}_{2,3}\,\hat{Z}^{3}_{1,2}\left(X\;Z^{z_1+x_2z_3}\otimes X^{x_2}\;Z^{z_2+x_1z_3}\otimes X^{x_1x_2+x_3}\;Z^{z_3}\right)$$

where

$$\hat{Z} = (I\otimes H)\,\mathrm{CNOT}^{z_3}_{1,2}\,(I\otimes H).$$

Here CNOT^{y}_{ij} means $\mathrm{CNOT}(i,j)$ is performed if $y=1$

Observe: control bits are classically encrypted.



$a=1,\ b=0 \Rightarrow s.$

$$\boxed{\text{Enc CNOT}}$$

Formally, given a quantum state

$$|\psi\rangle = \sum_{a,b} \alpha_{ab} |a,b\rangle$$

Denote

$$\mathrm{CNOT}^{s}(|\psi\rangle) \to \sum_{a,b} \alpha_{ab} |a, b \oplus as\rangle$$

<u>Want</u>: $\mathrm{CNOT}^{\text{fhe Enc}(s)}(|\psi\rangle) \to \mathrm{QEnc}\left(\sum_{a,b} \alpha_{ab} |a, b \oplus as\rangle\right)$

We don't know how to do this directly

Break it into 2 steps:

① Convert fhe enc (s) → "special" enc
TCF enc.

② Use TCF enc to <u>compute enc CNOT</u>.

TCF enc:

Define TCF enc of a bit s as

a TCF function pair $f_0, f_1 : X \to Y$

(Break $X = \{0,1\} \times R$) s.t.

$\forall$ claws $\underbrace{(\mu_0, r_0)}_{x_0}$ $\underbrace{(\mu_1, r_1)}_{x_1}$ it holds that

$$\mu_0 \oplus \mu_1 = s.$$

Using TCF enc to perform enc CNOT:

Have $|\psi\rangle = \sum_{a,b} \alpha_{ab} \, |a,b\rangle \,\&\, Enc(s)$

<u>Want</u> $QEnc\left(\sum_{a,b} \alpha_{ab} |a, b \oplus as\rangle\right)$

Given f_0, f_1 , sample random y in image & entangle $|\psi\rangle$ with the corresponding claw.

$$|\psi\rangle \to \sum_b \alpha_{0b} |0\, b\, x_0\rangle + \alpha_{1b} |1\, b\, x_1\rangle$$

where x_0, x_1 is a claw.

This is done as before:

$$\sum_x |\psi\rangle |x\rangle |0\rangle = \sum_{x,a,b} \alpha_{ab} |a, b, x, 0\rangle$$

$$\rightarrow \sum_{a,b,x} \alpha_{ab} \, |a, b, x, f_a(x)\rangle$$

Measure last reg $\rightarrow$ $\sum_b \alpha_{0b} |0\ b\ x_0\rangle + \alpha_{1b} |1, b, x_1\rangle.$

For simplicity let $b = 0$.

$$\sum_{a \in \{0,1\}} \alpha_a \, |a\rangle \, |x_a\rangle = \sum_a \alpha_a |a\rangle \, |\underline{\underline{\mu_a}}\ r_a\rangle$$

$$= \sum_a \alpha_a |a\rangle \, \underline{|\mu_0 \oplus as, \ r_a\rangle}.$$

<u>Wanted</u> $\approx$ $\underline{\left(\sum_a \alpha_a |a\rangle \, |as\rangle \right)}$

Extra: $\underline{\mu_0 \; , \; r_0 \; , r_1}$

Missing: OTP padding $X^x Z^z$

$$\sum_a \alpha_a |a\rangle \,|\, \mu_0 \oplus as \,,\; r_a\rangle$$

$$= (I \otimes X^{\mu_0} \otimes I) \sum_a \alpha_a \,|a\rangle\, |as, r_a\rangle$$

Turns out that if we perform Hadamard & measure register containing r_a, (get o/p d) the resultant state is:

$$Z^{d \cdot (r_0 \oplus r_1)} \otimes X^{\mu_0} \left(\sum_a \alpha_a |a\rangle\, |as\rangle \right)$$

STEP 1: fhe enc $\rightarrow$ TCF enc.

$f_0(\mu_0, r_0)$: fhe enc of bit μ_0 w/ rand r_0.

$f_1(\mu_1, r_1)$: $f_0(\mu_1, r_1) \oplus \text{Enc}(s)$.

$= \text{Enc}(\mu_1) \oplus \text{Enc}(s)$

$= \text{Enc}(\mu_1 \oplus s)$

Check TCF enc properties:

① If $f_0(\mu_0, r_0) = f_1(\mu_1, r_1)$

$\text{Enc}(\mu_0) = \text{Enc}(\mu_1 \oplus s)$.

$\Rightarrow \mu_0 = \mu_1 \oplus s$. ✓

② claw free by security of fhe.

③ Injective ✓ Image same (can be arranged). ✓

④ Trapdoor: some the schemes from lattices support trapdoor allows for randomness recovery.

Quantum Capable the.