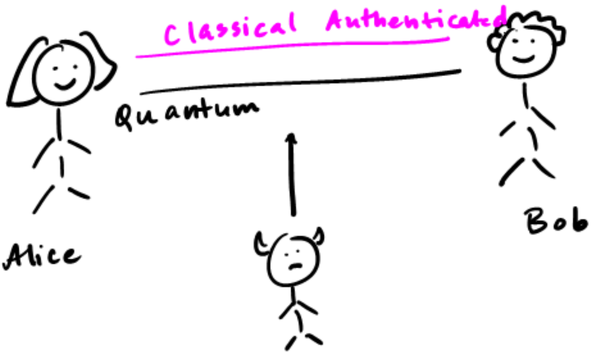
CS6846 – Quantum Algorithms and Cryptography

Quantum Cryptography

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

Quantum Key Distribution

Bennett & Brassard 1984.



Information Theoretic Security.

Protocol:

Main Property: If bit b is encoded in an unknown basis, Eve cannot get info abt b w/o disturbing the state.

1). Alice chooses n random bits $a_1 \dots a_n$, & n random bases, $b_1 \dots b_n$

$b_i \in \{$ Comp, Had $\}$

$\{|0\rangle, |1\rangle\}$ $b=0$

$\{|+\rangle, |-\rangle\}$ $b=1$

Sends a_i in basis b_i.

$a_i = 0$, $b_i = 1$ $\Rightarrow |+\rangle$

2). Bob chooses random bases $b_1' \dots b_n'$ & measures received qubits in these.

Gets $a_1' \dots a_n'$.

3) Bob sends $\{b_i'\}$ to Alice, Alice sends $\{b_i\}$ to Bob.

For "matching" positions $a_i' = a_i$

<u>IF</u> Eve did not tamper.

4) Alice selects $n/4$ locations in shared string & sends Bob a_i & locations.

If fraction of errors is "high", they abort.

5) If not, they get $n/4$ shared bits.

Security Argument:

To transmit bit 0 : $|0\rangle$ w.p $\frac{1}{2}$

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

" " " 1 : $|1\rangle$ w.p. $\frac{1}{2}$

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

Adversary's strategy:

$$|0\rangle = \cos 0 \, |0\rangle + \sin 0 \, |1\rangle$$

$$|+\rangle = \cos \frac{\pi}{4} |0\rangle + \sin \frac{\pi}{4} |1\rangle$$

Eve can measure in the basis

$\cos \frac{\pi}{8} |0\rangle + \sin \frac{\pi}{8} |1\rangle$ } midway bet^n $|0\rangle$ & $|+\rangle$

$-\sin \frac{\pi}{8} |0\rangle + \cos \frac{\pi}{8} |1\rangle$ } midway bet^n $|1\rangle$ & $|-\rangle$

$$\Pr(\text{Eve gets } a_i) = \left(\cos\left(\frac{\pi}{8}\right)^2\right) \approx 0.85$$

Measurement disturbs the state by angle $\geq \frac{\pi}{8}$ so if Bob uses same basis as Alice, then his prob. of recovering incorrect value is $\geq \sin\left(\frac{\pi}{8}\right)^2$ ≈ 0.15.

Quantum One time pad.

Recall: Classical OTP:

Have mesg m, key k. ← Random binary (same length)

CT: $m \oplus k$.

If I know k, $CT \oplus k = m$.

Quantum:

Pauli X Gate: (NOT)

$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

$X|0\rangle = |1\rangle$

$X|1\rangle = |0\rangle$.

$\underline{\underline{m}} \oplus k$

Let $a \leftarrow \{0,1\}$. Then $X^a |\text{bit}\rangle$ is a OTP.

$X|+\rangle = |+\rangle$

$X|-\rangle = -|-\rangle$.

Pauli Z gate $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$

$Z|+\rangle = |-\rangle$

$Z|-\rangle = |+\rangle$

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

Can compute $Z^b |\psi\rangle$ & b random bit.

Let key (a, b), random bits

Let ρ be an arbitrary mixed state.

$$\begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix}.$$

Q-OTP $\quad \mathrm{Enc}(\rho, (a,b)) = \overbrace{X^a Z^b \rho (X^a Z^b)^\dagger}^{CT}$

$$\mathrm{Dec}(CT, (a,b)) : \underbrace{(X^a Z^b)}_{\text{unitary}}{}^\dagger \, CT \, (X^a Z^b)$$

$$\Rightarrow \rho.$$

Security:

$$P = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$$

$$\alpha + \delta = 1.$$

Four combinations of (a, b):

① $P = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$

② $Z P Z^{\dagger} = \begin{pmatrix} \alpha & -\beta \\ -\gamma & \delta \end{pmatrix}$

③ $X P X^{\dagger} = \begin{pmatrix} \delta & \gamma \\ \beta & \alpha \end{pmatrix}$

④ $(XZ) P (XZ)^{\dagger} = \begin{pmatrix} \delta & -\gamma \\ -\beta & \alpha \end{pmatrix}$

Claim:

$$\frac{1}{4} \sum_{a,b \in \{0,1\}} (X^a Z^b) \cdot P \cdot (X^a Z^b)^{\dagger} = \frac{1}{2} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

Maximally mixed

Adding these $\frac{1}{4} \begin{pmatrix} 2\underbrace{(\alpha + \delta)}_{1} & 0 \\ 0 & 2(\alpha+\delta) \end{pmatrix} = \frac{1}{2} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$