Tutorial XII

08 January 2021 17:06

QUANTUM CRYPTOGRAPHY – Quantum key distribution

→ Shared keys are important

→ encryption (OTP)

→ authentication (Orthogonal arrays)

→ Complexity solutions:

→ Diffie-Hellman protocol

→ EC-DH protocol

→ Vulnerable to quantum computers

→ Post-quantum cryptography

→ QKD – possible solution

Quantum mechanics – the very basics

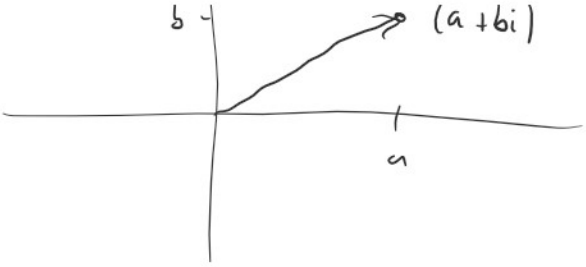
Mathematical description of a (pure) qubit

Qubit – basic information unit

Qubits are normalized vectors in $\mathbb{C}^2$ ($\mathbb{C}$ are complex numbers)

$$\left.\begin{aligned} |0\rangle &= \begin{pmatrix} 1 \\ 0 \end{pmatrix} \\ |1\rangle &= \begin{pmatrix} 0 \\ 1 \end{pmatrix} \end{aligned}\right\}$$ these form orthonormal basis

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}, \quad \alpha, \beta \in \mathbb{C}, \quad |\alpha|^2 + |\beta|^2 = 1$$



$$|a+bi| = \sqrt{a^2+b^2}$$

$\{|0\rangle, |1\rangle\}$ = cannonical (computational)

There are infinitely many orthonormal bases of $\mathbb{C}^2$

$$|+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} = \begin{pmatrix} 1/\sqrt{2} \\ 1/\sqrt{2} \end{pmatrix}$$

$$|-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}} = \begin{pmatrix} 1/\sqrt{2} \\ -1/\sqrt{2} \end{pmatrix}$$

$$(a,b)\circ(c,d) = a\cdot c + b\cdot d = 0 \iff$$ (a,b) and (c,d) are orthogonal

$$\begin{pmatrix} a \\ b \end{pmatrix}^T \cdot \begin{pmatrix} c \\ d \end{pmatrix} = (a,b)\cdot\begin{pmatrix} c \\ d \end{pmatrix} = ac+bd =$$ scalar product

$$\langle a|b\rangle = (\alpha^*, \beta^*)\cdot\begin{pmatrix} \gamma \\ \delta \end{pmatrix} = \alpha^*\cdot\gamma + \beta^*\cdot\delta$$

$\alpha = a+bi$

$\alpha^* = a-bi$

$|a\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$

$\langle a| = (\alpha^*, \beta^*)$

$|b\rangle = \begin{pmatrix} \gamma \\ \delta \end{pmatrix}$

$$\langle a|a\rangle = (\alpha^* \beta^*)\cdot\begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \alpha^*\cdot\alpha + \beta^*\cdot\beta = |\alpha|^2 + |\beta|^2 = 1$$

$$(a-ib)\cdot(a+ib) = a^2 - (ib)^2 = a^2+b^2 = |\alpha|^2$$

$$\langle a|a\rangle = 1$$

$\boxed{|+\rangle \text{ and } |-\rangle \text{ are an orthonormal basis}}$

$$\langle + | + \rangle = \frac{1}{\sqrt{2}} \Big(\langle 0| + \langle 1| \Big) \cdot \frac{1}{\sqrt{2}} \Big(|0\rangle + |1\rangle \Big)$$

$$= \frac{1}{2} \Big(\langle 0|0\rangle + \langle 1|0\rangle + \langle 0|1\rangle + \langle 1|1\rangle \Big)$$

$$\langle 0|0\rangle \quad (1\ 0) \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix} = 1$$

$$= \frac{1}{2} \Big(1 + 0 + 0 + 1 \Big)$$

$$\langle 1|0\rangle = (0\ 1) \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix} = 0$$

$$= 1$$

→ normalization

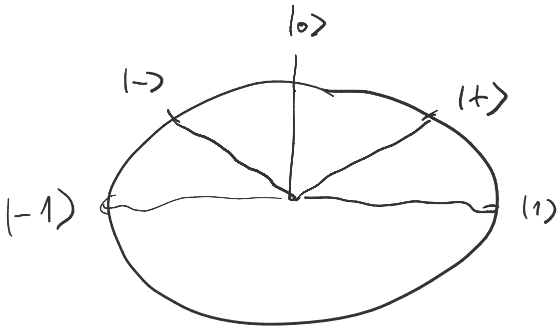
$\langle - | - \rangle = 1$ → both are normalized

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

$$\langle - | + \rangle = \left(\frac{1}{\sqrt{2}},\ -\frac{1}{\sqrt{2}}\right) \cdot \begin{pmatrix} 1/\sqrt{2} \\ 1/\sqrt{2} \end{pmatrix} = \frac{1}{2} - \frac{1}{2} = 0$$

$$\langle + | - \rangle = 0$$

→ orthogonality



Any state $|\psi\rangle$ can be written in any basis

$$\boxed{|\psi\rangle = \alpha|0\rangle + \beta|1\rangle}$$

⇝ $|\psi\rangle$ is a superposition of $|0\rangle$ and $|1\rangle$

α and β are called amplitudes

$$|0\rangle = \frac{|+\rangle + |-\rangle}{\sqrt{2}} = \begin{pmatrix} 1/2 \\ 1/2 \end{pmatrix} + \begin{pmatrix} 1/2 \\ -1/2 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

...plitudes

$$|0\rangle = \frac{|+\rangle + |-\rangle}{\sqrt{2}} = \begin{pmatrix} 1/2 \\ 1/2 \end{pmatrix} + \begin{pmatrix} 1/2 \\ -1/2 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

$$|1\rangle = \frac{|+\rangle - |-\rangle}{\sqrt{2}} = \begin{pmatrix} 1/2 \\ 1/2 \end{pmatrix} - \begin{pmatrix} 1/2 \\ -1/2 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

$$|\psi\rangle = \alpha\left(\frac{|+\rangle + |-\rangle}{\sqrt{2}}\right) + \beta\left(\frac{|+\rangle - |-\rangle}{\sqrt{2}}\right)$$

$$= \frac{\alpha+\beta}{\sqrt{2}}|+\rangle + \frac{\alpha-\beta}{\sqrt{2}}|-\rangle$$

is a superposition of $|+\rangle$ and $|-\rangle$ with amplitudes $\frac{\alpha+\beta}{\sqrt{2}}$ and $\frac{\alpha-\beta}{\sqrt{2}}$

Measurements of qubits

To each (projective) measurement we associate a basis

If you measure $|\psi\rangle$ in basis $\{|a\rangle, |b\rangle\}$

you get an answer to the following question:

is qubit $|\psi\rangle$ is state $|a\rangle$ or $|b\rangle$?

$|\psi\rangle = \alpha|a\rangle + \beta|b\rangle$ ~ $|\psi\rangle$ is in a superposition of $|a\rangle$ and $|b\rangle$ with amplitudes α and β

answer $|a\rangle$ w.p. $|\alpha|^2$
$|b\rangle$ w.p. $|\beta|^2$ $\Big\}$ $|\alpha|^2 + |\beta|^2 = 1$

after measuring $|\psi\rangle$ in $\{|a\rangle, |b\rangle\}$ and geting an answer $|a\rangle$, state $|\psi\rangle$ collapses into state $|a\rangle$. E.g. if you measure it again in state $\{|a\rangle, |b\rangle\}$ you will get an answer $|a\rangle$ w.p. 1

$|\psi\rangle$ and measure it in $\{|a\rangle, |b\rangle\}$

$|\langle a|\psi\rangle|^2 \sim$ probability of answer $|a\rangle$

$|\langle b|\psi\rangle|^2 \sim$ probability of answer $|b\rangle$

$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$

$|\psi\rangle = \langle +|\psi\rangle|+\rangle + \langle -|\psi\rangle|-\rangle$

Quantum Key Distribution (BB 84 protocol)

1.) Repeat 2N times (rounds)

a.) Alice prepares one of 4 possible states $\{\overset{0}{|0\rangle}, \overset{1}{|1\rangle}, \overset{0}{|+\rangle}, \overset{1}{|-\rangle}\}$ at random and sends it to Bob

b.) Bob measures the received qubit in a randomly chosen basis $\{\underset{0}{|0\rangle}, \underset{1}{|1\rangle}\}$ or $\{\underset{0}{|+\rangle}, \underset{1}{|-\rangle}\}$

2.) Sifting Alice publishes her 2N preparation bases $\{|0\rangle, |1\rangle\}$ or $\{|+\rangle, |-\rangle\}$

Bob publishes his 2N measurement choices $\{|0\rangle, |1\rangle\}$ or $\{|+\rangle, |-\rangle\}$

They keep only rounds where their basis matches.

$|\langle 0|0\rangle|^2 = 1$ $|\langle 1|0\rangle|^2 = 0$

$\Rightarrow$ 0 $|0\rangle$ $\{|0\rangle, |1\rangle\}$ 0

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

0 $|+\rangle$ $\{|+\rangle, |-\rangle\}$ 0

0 $|+\rangle$ $\quad \{|+\rangle, |-\rangle\}$ 0

1 $|-\rangle$ $\quad \{|+\rangle, |-\rangle\}$ 1

A $\quad$ E

$|0\rangle$ —— $\quad \not\!\!b\ \{|a\rangle, |b\rangle\}$ $\xrightarrow{|a\rangle/|b\rangle}$ $\{|0\rangle, |1\rangle\}$

intercept-resend attack

w.p. $|\langle a|0\rangle|^2 = P_a$

$|\langle b|0\rangle|^2 = P_b$

$|0\rangle$: $P_a |\langle 0|a\rangle|^2 + P_b |\langle 0|b\rangle|^2 = |\langle a|0\rangle|^4 + |\langle b|0\rangle|^4$

$|1\rangle$: $P_a |\langle 1|a\rangle|^2 + P_b |\langle 1|b\rangle|^2 = |\langle a|1\rangle|^4 + |\langle b|1\rangle|^4$

$\not b$

$\delta = 1$ iff $\{|a\rangle, |b\rangle\} = \{|0\rangle, |1\rangle\}$

Adversary Eve is causing errors in Bob's string!

Classical post-processing

1.) Parameter estimation – How many errors are there in Bob's string?

They reveal a small (representative) portion of their strings to estimate error rate

if too many errors – ABORT

11% error is critical

2.) Error correction

→ Assume Bob has ε errors and Eve has $\delta \gg \varepsilon$

→ Alice creates an error correcting code, which can correct ε errors (but not more), s.t. her string is a codeword

ε errors (but not more), s.t. her string is a codeword.

She publishes the code

→ Bob corrects his string

→ Eve cannot do this some secret left

3.) Privacy amplification

→ Alice chooses a random hash function (2-universal set)

She and Bob hash their corrected string.

Now they share a shorter, but fully secret key