Tutorial XII group 2

05 December 2019 16:03

Quantum Cryptography

Quantum Key Distribution

→ Shared secret keys are important
- → encryption (OTP)
- → authentication (Orthogonal arrays)
- → . . .

→ complexity solutions: Diffie Hellman
Elliptic Diffie Hellman
Post-quantum complexity solutions

→ quantum mechanics solution: QKD

Quantum mechanics - the very basic

Qubit - basic information unit

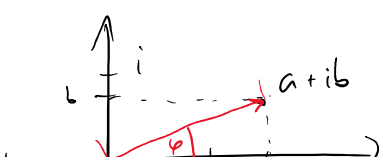
Mathematical description

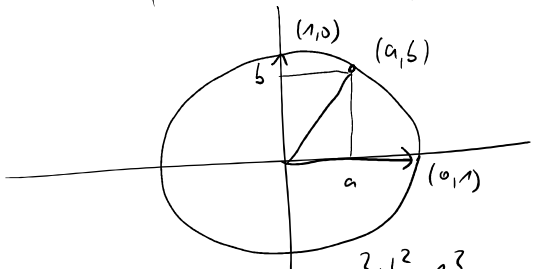
Qubits are normalized vectors in $\mathbb{C}^2$ ($\mathbb{C}$ complex numbers)

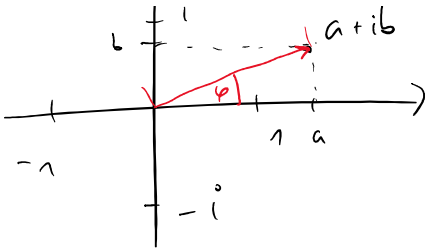
kets

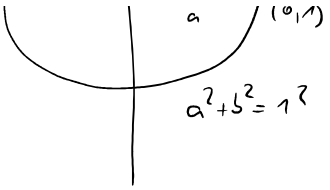
$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \quad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$ these form an orthonormal basis

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



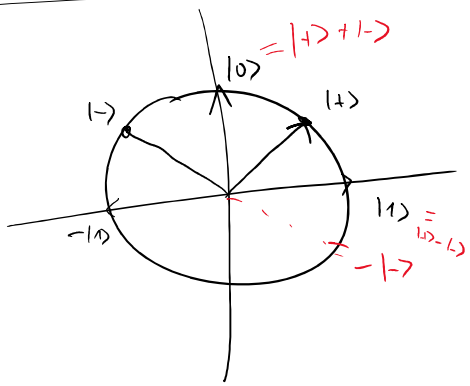






$$|a+ib| = \sqrt{a^2+b^2}$$

There are different qubit bases



$$|+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}$$

$$|-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

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

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

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

$$|\alpha|^2 = \alpha^*\alpha$$

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

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

$$\langle b| = (\lambda^*, \beta^*)$$

$|+\rangle$ and $|-\rangle$ are a basis

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

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

→ Normalized

$$\langle -|+\rangle = \left(\frac{1}{\sqrt{2}}^*, -\frac{1}{\sqrt{2}}^*\right)\begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix} = \frac{1}{2} - \frac{1}{2} = 0 \rightarrow \text{orthogonal}$$

$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ α and β are amplitudes

and ψ is in a superposition of $|0\rangle$ and $|1\rangle$

$$|0\rangle = \frac{|+\rangle + |-\rangle}{\sqrt{2}}$$

$$|1\rangle = \frac{|+\rangle - |-\rangle}{\sqrt{2}}$$

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

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

$|\psi\rangle$ is also in a superposition of $|+\rangle$ and $|-\rangle$

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

Measurements

To (projective) measurements we associate a basis

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

you get answer to the following question:

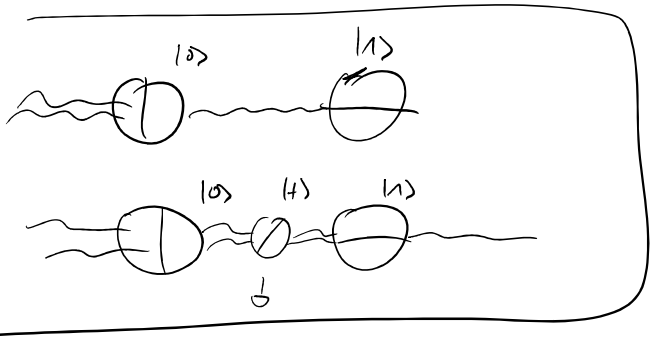
is qubit $|\psi\rangle$ in state $|a\rangle$ or $|b\rangle$?

$|\psi\rangle = \alpha|a\rangle + \beta|b\rangle$ ⇝ is in superposition of $|a\rangle$ and $|b\rangle$

answer is $|a\rangle$ w.p. $|\alpha|^2$ } truly random

and answer $|b\rangle$ w.p. $|\beta|^2$ }

after measuring $|\psi\rangle$ and getting answer $|a\rangle$ state continues its existance in state $|a\rangle$. E.g. if you measure it again in $\{|a\rangle, |b\rangle\}$ the answer is $|a\rangle$ w.p 1.



Measuring $|\psi\rangle$ in $\{|a\rangle, |b\rangle\}$

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

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

Quantum Key Distribution (BB84 protocol)

1.) Repeat $2N$ times (rounds)

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

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

$2N$

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

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

They keep only rounds where their basis match

A: $|0\rangle$ (0), $|1\rangle$ (1), $|+\rangle$ (0), $|-\rangle$ (1)

B: $\{|0\rangle, |1\rangle\}$ 0 ; $\{|0\rangle, |1\rangle\}$ 1 ; $\{|+\rangle, |-\rangle\}$ 0 ; $\{|+\rangle, |-\rangle\}$ 1

$= 1$ $= 0$

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

E ↓ $|0\rangle$ $|1\rangle$ ↗ intercept resend attack

A $|0\rangle$ ——— $\{|a\rangle, |b\rangle\}$ $\xrightarrow{|a\rangle/|b\rangle}$ $\{|0\rangle, |1\rangle\}$ 0

0 % 1 % 1

Probability of Eve measuring $|a\rangle$

$|0\rangle$ w.p. $|\langle a|0\rangle|^2 \overline{|\langle 0|a\rangle|^2} = |\langle 0|a\rangle|^4$

$|\langle b|0\rangle|^2 |\langle 0|b\rangle|^2 = |\langle 0|b\rangle|^4$ } if $\{|a\rangle, |b\rangle\} \neq \{|0\rangle, |1\rangle\}$

$|1\rangle$ w.p. $|\langle a|1\rangle|^4 + |\langle b|1\rangle|^4$

Eves dropping introduces errors to Bob's string!

Classical postprocessing

1.) Parameter estimation

How many errors are there in Bob's string

They reveal a small (representative) sample to estimate error in the rest of their strings

if too many errors → Abort

11% error is critical

2.) Error correction

→ Assume Bob has ξ errors and Eve has $\delta >> \xi$

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

→ Bob correct his string

→ Eve can't do this so there is some secret left

3.) Privacy amplification

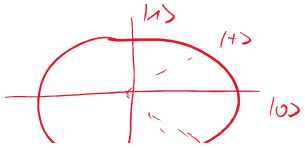
→ Hashing (Universal hashing)

They hash long and partially secret strings to short but perfectly secret strings.

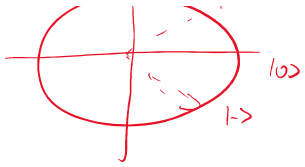
= they share a key!

Very simple attack

↓ EVE in each round



Eve $\{|0\rangle, |1\rangle\}$ in each round



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

$|1\rangle \to \{|0\rangle,|1\rangle\} \xrightarrow{k0+1\rangle|^2\ k-1+\rangle|^2} \{|0\rangle,|1\rangle\}$

$|+\rangle \to \{|0\rangle,|1\rangle\} \xrightarrow{|0\rangle/|1\rangle} \{|+\rangle,|-\rangle\}$

$|-\rangle \to \{|0\rangle,|1\rangle\} \longrightarrow \{|+\rangle,|-\rangle\}$

A	B	E
0	0	0
1	1	1
0	0 w.p. 1/2, 1 w.p. 1/2	0 w.p. 1/2, 1 w.p. 1/2
1	0 w.p. 1/2, 1 w.p. 1/2	0 w.p. 1/2, 1 w.p. 1/2

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

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

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

$$= \frac{1}{2}$$

$$|\langle 1|+\rangle|^2 = 1/2$$

$$\frac{1}{2}|\langle +|0\rangle|^2 + \frac{1}{2}|\langle +|1\rangle|^2 = \frac{1}{2}\cdot\frac{1}{2} + \frac{1}{2}\cdot\frac{1}{2} = \frac{1}{2}$$

Overall Bob knows 75% of Alice's string

Eve knows 75% of Alice's string

Eve measures $|0\rangle/|1\rangle$ w.p p and does nothing w.p $(1-p)$

How much Error she introduces to Bob?

$0.25p + (1-p)\cdot 1 = 1 - 0.25p$

Assume Bob and Alice observe only 20% error.

$$1 - 0.25\,p = 0.8 \iff 0{,}25\,p = 0{,}2 \iff p = \frac{4}{5} = 0{,}8$$

How much Eve learns?

$$p\cdot(0.75) + (1-p)\frac{1}{2} = \frac{1}{2} + \frac{1}{4}p \quad \text{if } p=0.8 \Rightarrow \frac{1}{2} + \frac{1}{5} = 0{,}7$$