Tutorial XII

05 December 2019 10:00

Quantum Key Distribution

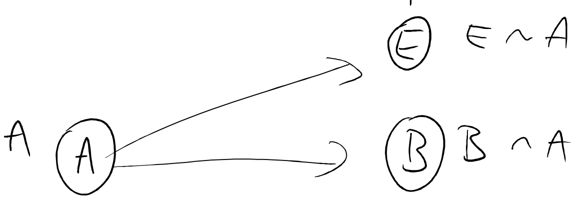
1.) Shared keys are important

→ encryption (OTP)

→ authentication (Orthogonal arrays)

OTP → size of key is enormous

| Shared key distribution over distance is impossible without additional assumption.



$\boxed{\text{Not secure because of quantum computers}}$

Complexity solution → Diffie-Hellman

$\boxed{\text{Quantum mechanics solution} \to \text{QKD}}$

Quantum mechanics - very basics

Qubit - basic information unit

Qubit is described as a normalized vector in $\mathbb{C}^2$

($\mathbb{C}$ - complex numbers)

ket

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

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

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

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

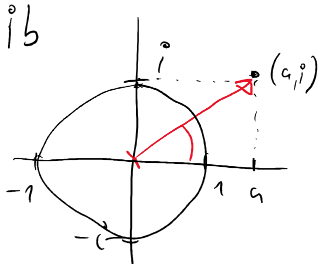
$|-\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle = \begin{pmatrix}\frac{1}{\sqrt{2}}\\-\frac{1}{\sqrt{2}}\end{pmatrix}$

$\left|\frac{1}{\sqrt{2}}\right|^2 + \left|\frac{1}{\sqrt{2}}\right|^2 = \frac{1}{2} + \frac{1}{2} = 1$ ✓

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

$(a,b)\cdot(c,d) = a.c + b.d = 0 \iff (a,b)$, (c,d) are perpendicular

$a + ib$



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

$\shortparallel$

$(a+ib)(a-ib)$

$\shortparallel$

$|c| = c \cdot c^*$

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

are perpendicular

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

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle = \begin{pmatrix}\alpha \\ \beta\end{pmatrix}$$

$$\langle\psi| = \alpha^*\langle 0| + \beta^*\langle 1| = (\alpha^*, \beta^*)$$

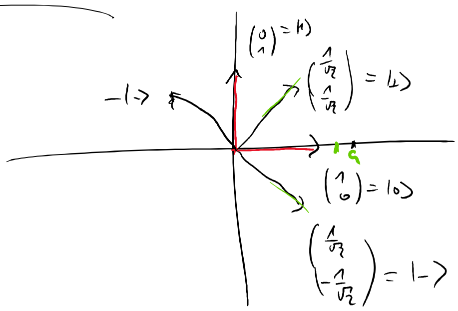
$$\langle +|-\rangle = \left(\frac{1}{\sqrt2}^*, \frac{1}{\sqrt2}^*\right) \cdot \begin{pmatrix}\frac{1}{\sqrt2} \\ -\frac{1}{\sqrt2}\end{pmatrix} = \frac12 - \frac12 = 0$$

$|+\rangle, |-\rangle$ are normalized and perpendicular, they form a basis

$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ can be expressed in $|+\rangle, |-\rangle$ basis b – • $\begin{pmatrix}a \\ b\end{pmatrix}$

$$|0\rangle = \frac{|+\rangle + |-\rangle}{\sqrt2}$$

$$|1\rangle = \frac{|+\rangle - |-\rangle}{\sqrt2}$$



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

$$= \alpha\left(\frac{|+\rangle + |-\rangle}{\sqrt2}\right) + \beta\left(\frac{|+\rangle - |-\rangle}{\sqrt2}\right)$$

$$= \boxed{\frac{\alpha+\beta}{\sqrt2}} |+\rangle + \boxed{\frac{\alpha-\beta}{\sqrt2}} |-\rangle$$

$$\left(\frac{\alpha+\beta}{\sqrt2}\right)^2 + \left(\frac{\alpha-\beta}{\sqrt2}\right)^2$$

$$\frac{\alpha^2 + 2\alpha\beta + \beta^2}{2} + \frac{\alpha^2 - 2\alpha\beta + \beta^2}{2}$$

$$= \frac{2\alpha^2 + 2\beta^2}{2} = \alpha^2 + \beta^2 = 1$$

There are infinitely many orthonormal bases

Quantum (Projective) Measurements

To each projective measurement we associate an orthonormal basis. $\{|0\rangle, |1\rangle\}$, $\{|+\rangle, |-\rangle\}$ generally $\{|a\rangle, |b\rangle\}$

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

→ answer is random (truly unpredictable) and probabilities depend on expression of $|\psi\rangle$ in basis $\{|a\rangle, |b\rangle\}$

→ answer is random (truly unpredictable) and probabilities depend on expression of $|\psi\rangle$ in basis $\{|a\rangle, |b\rangle\}$

→ if $|\psi\rangle = \alpha|a\rangle + \beta|b\rangle$

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

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

→ Post-measurement state is $|a\rangle$ or $|b\rangle$ (depending on the outcome)

$|\psi\rangle$ measurement in $\{|0\rangle, |1\rangle\}$ and the answer is $|1\rangle$, measuring again in $\{|0\rangle, |1\rangle\}$ the answer is $|1\rangle$ w.p. 1.

Quantum Key Distribution (BB84)

1.) Repeat 2N times (round)

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

$\quad 0 \quad 1 \quad 0 \quad 1$

b.) Bob chooses (at random) a measurement $\{|0\rangle, |1\rangle\}$ or $\{|+\rangle, |-\rangle\}$ and measures recieved qubit in the chosen basis

2.) Sifting – Both Alice and Bob reveal their basis. (Alice does not reveal the state only basis). They keep only pairs in which their basis match

Meaning

A	measur B		
1 $\|1\rangle$	$\{\|0\rangle, \|1\rangle\}$	$\|1\rangle$	1
0 $\|0\rangle$	$\{\|0\rangle, \|1\rangle\}$	$\|0\rangle$	0
0 $\|+\rangle$	$\{\|+\rangle, \|-\rangle\}$	$\|+\rangle$	0
1 $\|-\rangle$	$\{\|+\rangle, \|-\rangle\}$	$\|-\rangle$	1

→ raw key

this is ideal (errorless situation)

How do errors happen?

$|0\rangle$ | $\quad |+\rangle$ /

1.) Channel noise $\qquad |1\rangle$ — $\quad |-\rangle$ \

$\boxed{\text{2.) Evesdropping}}$

Intercept resend attack

A $\qquad$ E $\{|a\rangle, |b\rangle\}$

$|0\rangle \longrightarrow \quad \xrightarrow{|a\rangle/|b\rangle} \{|0\rangle, |1\rangle\}$

to get measurement probabilities of measuring $|a\rangle$ in $\{|0\rangle, |1\rangle\}$ basis, we need to calculate:

$$|a\rangle = (\langle 0|a\rangle)|0\rangle + (\langle 1|a\rangle)|1\rangle$$

With probability $|\langle 0|a\rangle|^2$ result is $|0\rangle$

and $\qquad |\langle 1|a\rangle|^2$ result is $|1\rangle$

Classical post processing

1.) Parameter estimation

- → how many errors are in their strings?
- → they reveal a small portion of their keys to estimate the number of errors

if there are too many errors they abort

2.) Error correction

- → There are ε errors between Alice's and Bob's string, eve has $\gg \varepsilon$ errors in her estimate
- → Alice designs an error correcting code, which can correct ε error, which contains her string as a code word.
- → She sends the code to Bob
- → Bob corrects his string using the code
- → Eve has more errors, she cannot correct.

3.) Privacy amplification

- → hashing (Universal hashing)

→ Shortening strings decreases Eves knowledge

→ Outcome is the final key

Easiest attack, Eve measures each qubit in $\{|0\rangle, |1\rangle\}$ basis

$$A \longrightarrow \underset{\downarrow}{\overset{\text{Eve}}{\{|0\rangle,|1\rangle\}}} \longrightarrow B$$

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

		A	B	E
$|0\rangle \to \{|0\rangle,|1\rangle\}$	Eve learns everything Bob has no errors	0	0	0
$|1\rangle \to \{|0\rangle,|1\rangle\}$	——— h ———	1	1	1

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

		A	B	E	
$|+\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$	$\underline{|0\rangle/|1\rangle}$	0	0/1 w.p. 1/2	0/1	w.p. 1/2

$$\begin{aligned}
|\langle +|0\rangle|^2 &= \left|\left(\tfrac{1}{\sqrt{2}}\langle 0| + \tfrac{1}{\sqrt{2}}\langle 1|\right)|0\rangle\right|^2 \\
&= \left|\left(\tfrac{1}{\sqrt{2}}\langle 0|0\rangle + \tfrac{1}{\sqrt{2}}\langle 1|0\rangle\right)\right|^2 \\
&= \left|\left(\tfrac{1}{\sqrt{2}} + 0\right)\right|^2 = 1/2 \\
|\langle -|0\rangle|^2 &= \left|\left(\tfrac{1}{\sqrt{2}}\langle 0| - \tfrac{1}{\sqrt{2}}\langle 1|\right)|0\rangle\right|^2 \\
&= \left|\left(\tfrac{1}{\sqrt{2}}\langle 0|0\rangle - \tfrac{1}{\sqrt{2}}\langle 1|0\rangle\right)\right|^2 \\
&= \frac{1}{2}
\end{aligned}$$

$|-\rangle \rightarrow$ $\{|0\rangle, |1\rangle\}$ $\xrightarrow{|0\rangle/|1\rangle}$ $\{|+\rangle, |-\rangle\}$ 1 $0/1$ w.p. $1/2$ $0/1$ w.p. $1/2$

Bob knows 75% of Alices string $\left(\frac{1}{2} \cdot 1 + \frac{1}{2} \cdot \frac{1}{2}\right) = 0{,}75$

Eve knows 75% of Alices string

What if there is only 20% of errors Between A and B?

Assume Eve looks with probability p and doesn't look with probability (1-p)

How much Bob knows? $p \cdot 0{,}75 + (1-p) \cdot 1 = 1 - 0{,}25p$

How much Eve knows? $p \cdot 0{,}75 + (1-p)\frac{1}{2} = \frac{1}{2} + 0{,}25p$

$1 - 0{,}25p = 0{,}8 \Rightarrow 0{,}2 = 0{,}25p \Rightarrow p = \frac{0{,}2}{0{,}25} = \frac{4}{5} = \boxed{0{,}8}$

$\Rightarrow 0{,}8 \cdot 0{,}75 + 0{,}2 \cdot 0{,}5 = 0{,}6 + 0{,}1 = \boxed{0{,}7}$