Tutorial 12

08 December 2021 13:58

QUANTUM CRYPTOGRAPHY – Quantum Key Distribution

→ Shared Secret Keys are important

→ encryption (one-time-pad)

→ authentication (Orthogonal arrays)

→ Complexity solutions:

→ Diffie-Hellman

→ EC-DH protocol

Vulnerable to quantum computers

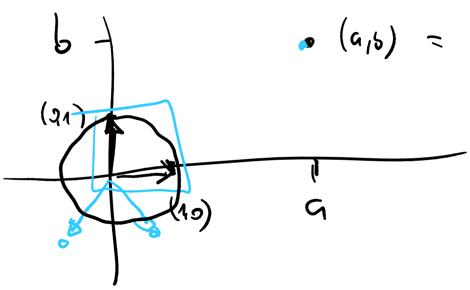
→ Post-quantum cryptography

→ Quantum Key Distribution

Quantum mechanics – the very basics

Qubit – basic information unit

Mathematical description of a (pure) qubits is a $\boxed{\text{unit}}$ vector in $\mathbb{C}^2$ ($\mathbb{C}$ are complex numbers).

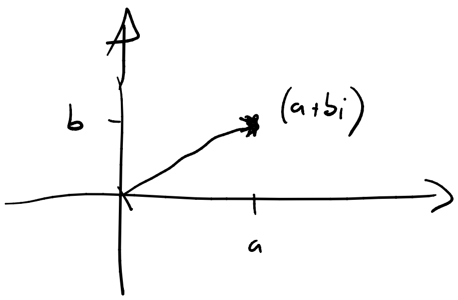


$(a,b) = a\cdot(1,0) + b\cdot(0,1)$

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

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

$a^2+b^2=c^2$

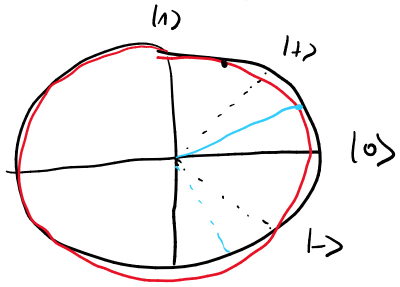


$$|a+bi| = \sqrt{a^2+b^2}$$

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

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

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



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

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

scalar product for complex spaces

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

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

$\alpha = a+bi$

$\alpha^* = a-bi$

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

$(a+ib)\cdot(a-ib)$ $\qquad |\beta^2|$

$=$

$a^2-(ib)^2$

$=$

$a^2+b^2 = |\alpha|^2$

$\langle +|$

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

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

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

$$\langle -|-\rangle = 1$$

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

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

Any $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ can be written in any other orthonormal basis.

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

α and β are called amplitudes

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

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

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

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

$|\psi\rangle$ is a $\boxed{\text{superposition}}$ 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 an orthonormal basis

if you measure $|\psi\rangle$ in basis $\{|0\rangle, |1\rangle\}$

you get an answer to a question

is qubit $|\psi\rangle$ in state $|0\rangle$ or $|1\rangle$?

$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ $\qquad$ $|\psi\rangle$ is in a superposition of $|0\rangle$ and $|1\rangle$ with amplitudes α and β

answer: $\left.\begin{array}{ll} |0\rangle & \text{w.p. } |\alpha|^2 \\ |1\rangle & \text{w.p. } |\beta|^2 \end{array}\right\} \quad |\alpha|^2 + |\beta|^2 = 1$

$(|+\rangle, |-\rangle) \rightarrow$ is $|\psi\rangle$ in state $|+\rangle$ or $|-\rangle$?

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

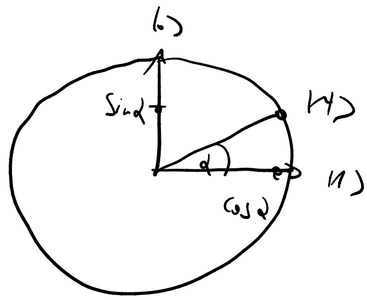
$|+\rangle$ w.p. $\left|\frac{\alpha+\beta}{\sqrt{2}}\right|^2$

$|-\rangle$ w.p. $\left|\frac{\alpha-\beta}{\sqrt{2}}\right|^2$

after measuring $|\psi\rangle$ in a basis $\{|a\rangle, |b\rangle\}$

$$\boxed{\begin{array}{ll} |a\rangle \text{ w.p. } & |\langle a|\psi\rangle|^2 \\ |b\rangle \text{ w.p. } & |\langle b|\psi\rangle|^2 \end{array}}$$

$$\boxed{|\psi\rangle = \langle a|\psi\rangle |a\rangle + \langle b|\psi\rangle |b\rangle}$$



after measuring $|\psi\rangle$ in basis $\{|a\rangle, |b\rangle\}$ and getting an answer $|a\rangle$ all subsequent measurements in $\{|a\rangle, |b\rangle\}$ basis will give result $|a\rangle$.

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

Measuring $|0\rangle$ and $|1\rangle$ in $\{|+\rangle, |-\rangle\}$ basis gives a random outcome

$|+\rangle$ and $|-\rangle$ in $\{|0\rangle, |1\rangle\}$ basis gives a random outcome

---

BB84 protocol

1.) Repeat 2N times (rounds)

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

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

0	$\|0\rangle$	$\{\|0\rangle, \|1\rangle\}$	0	$\|\langle 0\|0\rangle\|^2 = 1$
1	$\|1\rangle$	$\{\|0\rangle, \|1\rangle\}$	1	
0	$\|+\rangle$	$\{\|+\rangle, \|-\rangle\}$	0	
1	$\|-\rangle$	$\{\|+\rangle, \|-\rangle\}$	1	
0	$\|+\rangle$	$\{\|0\rangle, \|1\rangle\}$	0 1	$\|\langle 0\|+\rangle\|^2 = 1/2$ $\|\langle 1\|+\rangle\|^2 = 1/2$

2.) Sifting: Alice publishes her 2N 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 in which their bases match

3.) $\boxed{\text{Parameter estimation}}$

Intercept and resend attack

Alice

0 $|0\rangle$ $\longrightarrow$

Eve

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

p $|0\rangle$ 0

w.p. 1/2 $|0\rangle$ 0

$\longrightarrow$

Bob

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

$|0\rangle$ 0

b

$\longrightarrow$ $\longrightarrow$ $|0\rangle$ 0

w.p. $\frac{1}{2}$ $|0\rangle$ 0

$|0\rangle$

0 $|+\rangle \longrightarrow$ $\longrightarrow$ $\{|+\rangle, |-\rangle\}$ $\boxed{\begin{matrix} \text{w.p. } \frac{1}{2} & |+\rangle \\ \text{w.p. } \frac{1}{2} & |-\rangle \end{matrix}}$

$|1\rangle$

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

Alice and Bob publish some (randomly chosen) part of their strings to estimate the number of errors in each basis

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

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

$\{|0\rangle, |1\rangle\}$ prob. of error = 11%

$\{|+\rangle, |-\rangle\}$ probability of error = 11%

$$\boxed{1 - H(\text{Prob error } |+\rangle, |-\rangle) - H(\text{Prob error } |0\rangle, |1\rangle)}$$

H - Shannon entropy

$$H(p) = -p \cdot \log_2(p) - (1-p) \cdot \log_2(1-p)$$

$$1 - \underbrace{H(0.11)}_{\frac{1}{2}} - \underbrace{H(0.11)}_{\frac{1}{2}} \approx 0$$

3 error correction - errors in their strings need to be corrected

- $\rightarrow$ Assume Bob has ε errors and Eve has $\delta >> \varepsilon$
- $\rightarrow$ Alice creates an error correcting code which can correct

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

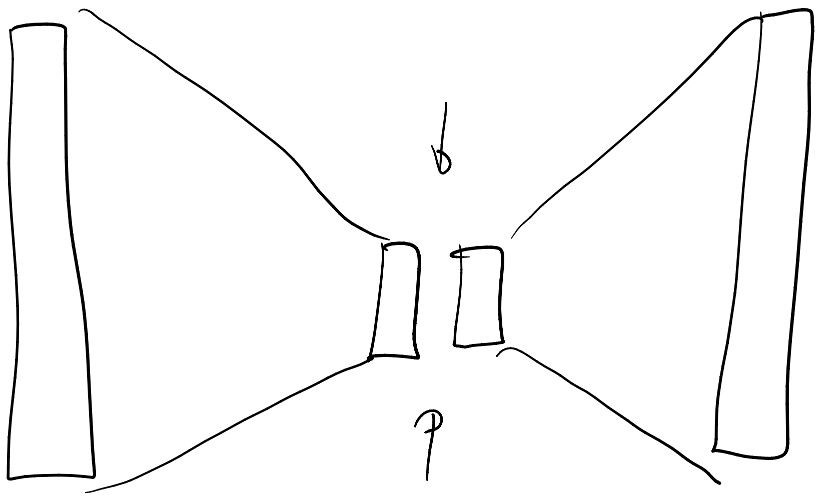
→ Bob corrects his string

→ Eve cannot correct – some secrecy is left

4.) Privacy amplification

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

She and Bob hash their corrected strings



complety secret

shorter string