Quantum Key Distribution (QKD) 量子密钥分发

△ Key Distribution

usually
key: One-time pad technique — Data is encrypted using a truly random key of the same length as the data being encrypted.

plain text —encryption→ cipher text

甲方 —key1→ 信息(明文) → 密文 —公开信道→ 乙方 —key2→ 明文

if key1 == key2: 对称密码/私密密码 (symmetric Cryptography)
else: 非对称密码/公开密码.

△ Current key distribution methods:

usually use public key ciphers { RSA, Diffie-Hellman, EEC

These ciphers are based on upon mathematical calculations that are simple to compute, but require an infeasible amount of processing power to invert.

比如: 求2个质数的乘法很简单,但做大数质因式分解就比较麻烦.

△ { BB84 (Charles H.B, Gilles B., 1984): the first quantum cryptography protocol.
E91 (Artur E., 1991)

1. BB84 protocol: communicating a private key in one-time pad encryption.

⇓

Make the right information publicly know at the right times. and keep the secret information secret.

一次性密码本 OTP {
- 用以加密的文本,也就是一次性密码本,必须是随机产生的.
- 它至少需和被加密文件等长
- 用以加密的文本只能用一次.而且必须对非关系人非常保密.不再使用时应销毁密码本,以防重复使用.

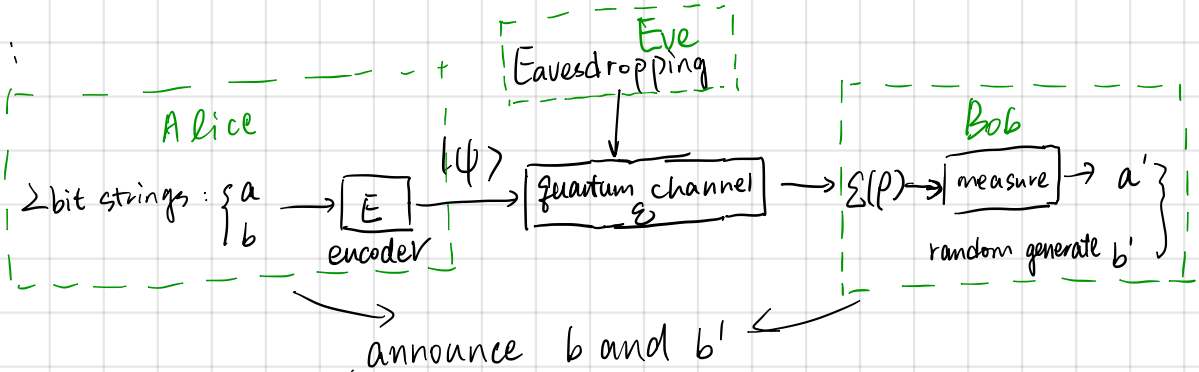
如果密码比加密信息短, We will be forced to use parts of the key more than once.

加密算法举例: 加密 "This is an example".

可以用加密而一次性密码本: MASKL NSFLD FKJPQ

This is an example ⇒	19	7	8	18	8	18	0	13	4	23	0	12	15	11	4
MASKL NSFLD FKJPQ ⇒	12	0	18	10	11	13	18	5	11	3	5	10	9	15	16
相加后得:	31	7	26	28	19	31	18	18	15	26	5	32	24	26	20
因为一共26个字母⇒模26:	5	7	0	2	19	5	18	18	15	0	5	22	24	0	20
得到b加密后的:	F	H	A	C	T	F	S	S	P	A	F	W	Y	A	U

BB84:



both Alice and Bob discard the qubits in a and a' where b and b' don't match
(用概率来看,平均下来b和b'应有一半是一致的)

以下是对过程图的具体解释:

1.1 Encoder:

$|\psi\rangle = \bigotimes_{i=1}^{n} |\psi_{a_i b_i}\rangle \Rightarrow a_i, b_i$: i-th bits of a, b; and a_i, b_i follows:

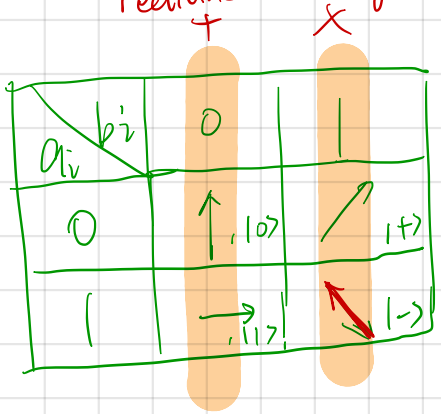
对称编码

- 0 ↑ $|\psi_{00}\rangle = |0\rangle$
- 1 → $|\psi_{10}\rangle = |1\rangle$
- 0 ↗ $|\psi_{01}\rangle = |+\rangle = \frac{\sqrt{2}|0\rangle + \sqrt{2}|1\rangle}{2}$
- 1 ↖ $|\psi_{11}\rangle = |-\rangle = \frac{\sqrt{2}|0\rangle - \sqrt{2}|1\rangle}{2}$

→ BB84用2 pairs of states. each pair conjugate to the other.
two states within a pair orthogonal with each other.
↓ called "basis"

→ wiki给的方向是对的. 应为45°, 而非-45°.

This procedure encodes a in the basis "+" or "X", as determined by b.



a_i: random bit created by Alice

b_i: for each a_i, Alice randomly chooses one of the two bases according to b_i and transmit a_i in.
↓
根据左边的表

The qubits are now in states that aren't mutually orthogonal, so it's impossible to distinguish all of them with certainty without knowing b.

→ 2个 vectors orthogonal: 它们相互垂直,点积得0.
↘ a set of vectors $\{\vec{v}_1, \vec{v}_2, \vec{v}_3, \ldots \vec{v}_n\}$ mutually orthogonal: every pair of vectors is orthogonal

1.2 $\mathcal{E}(\rho)$: quantum channel后Bob收到的state.

$\mathcal{E}(\rho) = \mathcal{E}(|\psi\rangle\langle\psi|)$ // $\mathcal{E}$ represents both the noise and eavesdropping by a 3rd party, Eve //
// $|\psi\rangle$ is what Alice sent over a public and authenticated quantum channel //

注: $|\psi\rangle$ (ket)是 $\langle\psi|$ (bra)的共轭转置

inner product of ket and bra: $\langle\phi|\psi\rangle = (\langle\phi|)(|\psi\rangle)$

outer product: $|\phi\rangle\langle\psi|$, $(|\phi\rangle\langle\psi|)(|\pi\rangle) = \langle\psi|\pi\rangle|\phi\rangle$

For a finite-dimensional vector space, the outer product can be understood as simple matrix multiplication:

$$|\phi\rangle\langle\psi| \doteq \begin{pmatrix} \phi_1 \\ \phi_2 \\ \vdots \\ \phi_N \end{pmatrix} \begin{pmatrix} \psi_1^* & \psi_2^* & \cdots & \psi_N^* \end{pmatrix} = \begin{pmatrix} \phi_1\psi_1^* & \phi_1\psi_2^* & \cdots & \phi_1\psi_N^* \\ \phi_2\psi_1^* & \phi_2\psi_2^* & \cdots & \phi_2\psi_N^* \\ \vdots & \vdots & \ddots & \vdots \\ \phi_N\psi_1^* & \phi_N\psi_2^* & \cdots & \phi_N\psi_N^* \end{pmatrix}$$

The outer product is an $N \times N$ matrix, as expected for a linear operator.

在Bob收到他的states后，Alice、Bob、Eve都有他们的states. 但只有Alice知道b(bi decides which basis ai is encoded in)，所以Bob和Eve不可能distinguish the states of qubits.

而且，根据不可克隆原理(no-cloning theorem)，除非Eve做出measurement，否则她不能拥有一个发到Bob那里的qubits的copy. 做measurement有一定可能性得到wrong answer.

no-cloning theorem: it is impossible to create an identical copy of an arbitrary unknown quantum state.

↓

Quantum Information和Quantum Cryptography的基石之一.

即不可能构造一个能够完全复制任意量子比特，却不对原始量子态产生干扰的系统.

原理：量子力学的线性特征

量子信息在信道中传输，不可能被第三方复制而窃取信息，却不对量子信息产生干扰.

1.3 Bob proceeds to generate a string of random bits b' of the same length as b and then measures the string he has received from Alice, a'. At this point, Bob announces publicly that he has received Alice's transmission. Alice then knows she can now safely announce b. Bob communicates over a public channel with Alice to determine which b_i and b'_i are not equal. Both Alice and Bob now discard the qubits in a and a' where b and b' do not match, which is half on average, leaving half the bits as a shared key.

1.4

From the remaining k bits where both Alice and Bob measured in the same basis, Alice randomly chooses $k/2$ bits and discloses her choices over the public channel. Both Alice and Bob announce these bits publicly and run a check to see whether more than a certain number of them agree. If this check passes, Alice and Bob proceed to use information reconciliation and privacy amplification techniques to create some number of shared secret keys. Otherwise, they cancel and start over.

透露.

信息协调和隐私放大

整个过程举个例子：

a ⇒	Alice's random bit	0	1	1	0	1	0	0	1
b ⇒	Alice's random sending basis	+	+	×	+	×	×	×	+
a'/a根据b编码后 ⇒	Photon polarization Alice sends	↑	→	↘	↑	↘	↗	↗	→
b' ⇒	Bob's random measuring basis	+	×	×	×	+	×	+	+
根据b'观测a'后. ⇒	Photon polarization Bob measures	↑	↗	↘	↗	→	↗	→	→
	PUBLIC DISCUSSION OF BASIS								
	Shared secret key	0		1			0		1

发送给Bob的光.

相当于：

⇒ 有"×"的地方正做一次Hadamard变换，"+"时不变

⇒ 有"×"的地方反做一次Hadamard变换，有"+"时不变

下一页会对这个过程详细说明.

但这一行会有出入.

BB84 算法过程详解（依据的是Qiskit的教程，可能与上页最后来自wiki的表格不一致）

—：Alice随机产生的 bit string　　—：Bob随机产生的 bit string

initial key a	0	1	1	0	1	0	0	1
⇓转换成qubit								
initial key a (qubit)	$\|0\rangle$	$\|1\rangle$	$\|1\rangle$	$\|0\rangle$	$\|1\rangle$	$\|0\rangle$	$\|0\rangle$	$\|1\rangle$
randomly Hadamard变换	Hadmard transform on a if basis is "x". do nothing for "+"							
random rotation string b	0	0	1	0	1	1	1	0
⇓ 0 stands for "+", 1 stands for "×"								
对应的rotation basis	+	+	×	+	×	×	×	+
待传输的key 数学表达	$\|0\rangle$	$\|1\rangle$	$\frac{\|0\rangle-\|1\rangle}{\sqrt{2}}$	$\|0\rangle$	$\frac{\|0\rangle-\|1\rangle}{\sqrt{2}}$	$\frac{\|0\rangle+\|1\rangle}{\sqrt{2}}$	$\frac{\|0\rangle+\|1\rangle}{\sqrt{2}}$	$\|1\rangle$
待传输的key 方向表达	↑(90°)	→(0°)	↖(135°)	↑(90°)	↖(135°)	↗(45°)	↗(45°)	→(0°)
Quantum Channel								
传输后的key	$\|0\rangle$	$\|1\rangle$	$\frac{\|0\rangle-\|1\rangle}{\sqrt{2}}$	$\|0\rangle$	$\frac{\|0\rangle-\|1\rangle}{\sqrt{2}}$	$\frac{\|0\rangle+\|1\rangle}{\sqrt{2}}$	$\frac{\|0\rangle+\|1\rangle}{\sqrt{2}}$	$\|1\rangle$
randomly inverse Hadamard变换	Inverse Hadmard transform on a if basis is "x". do nothing for "+"							
random rotation string b'	0	1	1	1	0	1	0	0
⇓ 0 stands for "+", 1 stands for "×"								
对应的rotation basis	+	×	×	×	+	×	+	+
最终的qubit key	$\|0\rangle$	$\frac{\|0\rangle-\|1\rangle}{\sqrt{2}}$	$\|1\rangle$	$\frac{\|0\rangle+\|1\rangle}{\sqrt{2}}$	$\frac{\|0\rangle-\|1\rangle}{\sqrt{2}}$	$\|0\rangle$	$\frac{\|0\rangle+\|1\rangle}{\sqrt{2}}$	$\|1\rangle$
⇓measure a'	0	0或1	1	0或1	0或1	0	0或1	1

b和b'相同位上的a和a'也一定相同，它们组成新的key

Shared secret key 〖以秘钥字符其ASCII平均值为a/a'/b/b'长度的一半〗

注：1. randomly选择"+"或"-" basis的过程就相当于randomly作Hadamard变换

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

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

Hadamard gate 的矩阵表示：$H=\frac{1}{\sqrt{2}}\begin{bmatrix}1&1\\1&-1\end{bmatrix}$

$\frac{1}{\sqrt{2}}\begin{bmatrix}1&1\\1&-1\end{bmatrix}\begin{bmatrix}1\\0\end{bmatrix}=\frac{1}{\sqrt{2}}\begin{bmatrix}1\\1\end{bmatrix}=\frac{1}{\sqrt{2}}\begin{bmatrix}1\\0\end{bmatrix}+\frac{1}{\sqrt{2}}\begin{bmatrix}0\\1\end{bmatrix}$

$\frac{1}{\sqrt{2}}\begin{bmatrix}1&1\\1&-1\end{bmatrix}\begin{bmatrix}0\\1\end{bmatrix}=\frac{1}{\sqrt{2}}\begin{bmatrix}1\\-1\end{bmatrix}=\frac{1}{\sqrt{2}}\begin{bmatrix}1\\0\end{bmatrix}-\frac{1}{\sqrt{2}}\begin{bmatrix}0\\1\end{bmatrix}$

2. Inverse transform of Hadamard gate:

$H=\frac{1}{\sqrt{2}}\begin{bmatrix}1&1\\1&-1\end{bmatrix}=\begin{bmatrix}\frac{1}{\sqrt{2}}&\frac{1}{\sqrt{2}}\\\frac{1}{\sqrt{2}}&-\frac{1}{\sqrt{2}}\end{bmatrix}$.

$H^{-1}=\frac{1}{-\frac{1}{2}-\frac{1}{2}}\begin{bmatrix}-\frac{1}{\sqrt{2}}&-\frac{1}{\sqrt{2}}\\-\frac{1}{\sqrt{2}}&\frac{1}{\sqrt{2}}\end{bmatrix}=\frac{1}{\sqrt{2}}\begin{bmatrix}1&1\\1&-1\end{bmatrix}$

∴ Hadamard逆变换 = Hadamard变换