

Quantum Key Distribution (QKD) 密钥分发

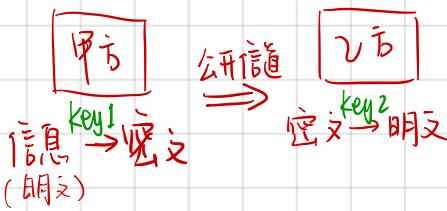
△ Key Distribution

usually

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

encryption

plain text → ciphertext



if $\text{key}_1 = \text{key}_2$: 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
Ell

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

例: 2⁵⁰⁰ 位质数的乘法很简单, 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 (Arthur E., 1991)

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

↓
Make the right information publicly known at the right times, and keep the secret information secret.

一次性密钥 { 用以加密的文本, 也就是一次性密钥串, 必须是随机产生的.

OTP { 它必须和被加密文件等长
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钥串, 以防重复使用.

如果密钥不能比加密信息短, 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".

可以用加密的一次性密钥: MASKL NSFLD FKJPQ

This is an example $\Rightarrow 19\ 7\ 8\ 18\ | 8\ 18\ | 0\ 13\ | 4\ 23\ 0\ 12\ 15\ 11\ 4$

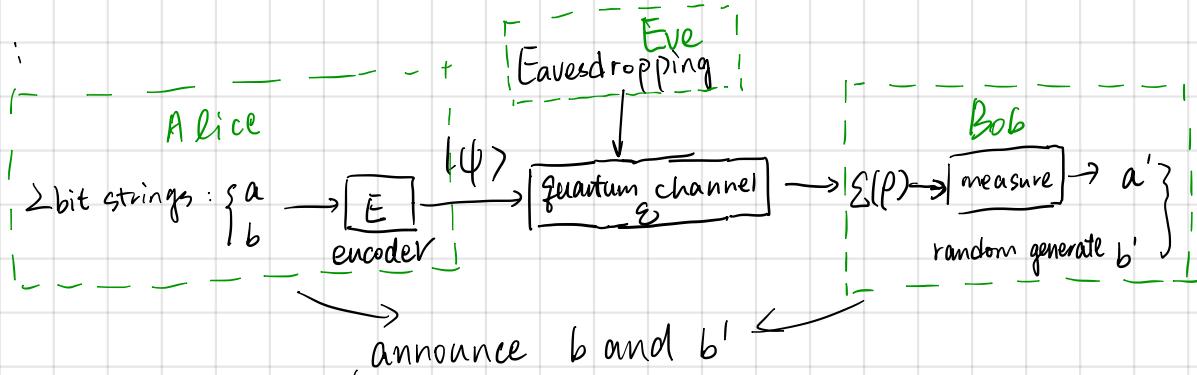
MASKL NSFLD FKJPQ $\Rightarrow 12\ 0\ 18\ 10\ | 11\ 13\ 18\ 5\ 11\ 3\ 5\ 10\ 9\ 15\ 16$

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 \Rightarrow 模26: 5 7 0 2 19 5 18 18 15 0 5 22 24 0 20

得到6加密后的: F H A C T F S S P A F W Y A U

BB84:

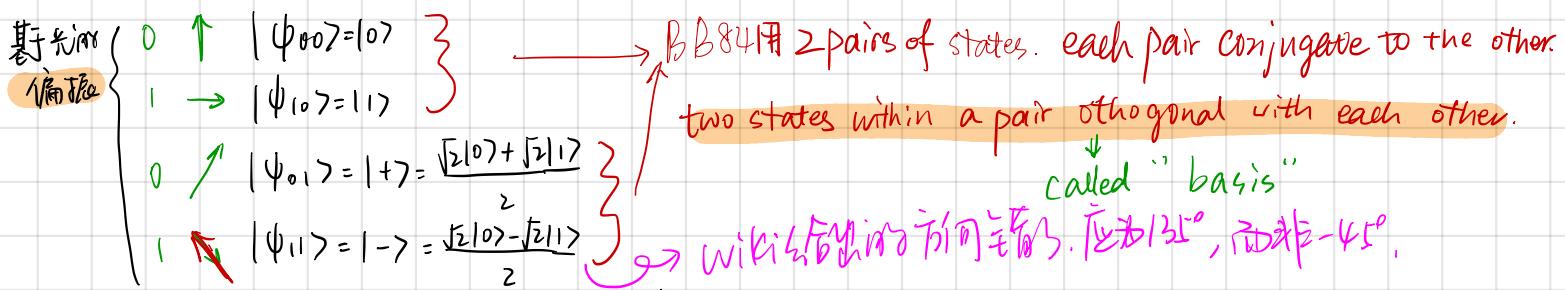


both Alice and Bob discard the qubits in a and a' where b and b' don't match
(用概率来看, 平均下来 b 和 b' 应有一半是一致的)

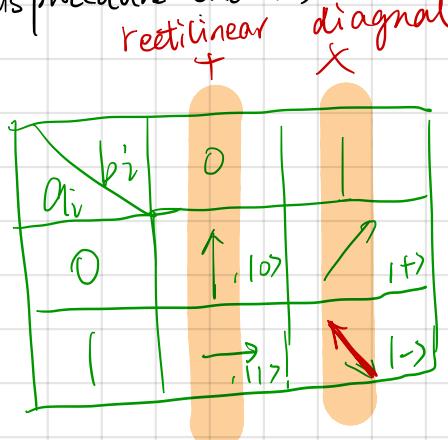
以下是对这个框图的具体解释:

1.1 Encoder:

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



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. ↓ 根据左边的图

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

1.2 $E(\rho)$: quantum channel to Bob's X state.

$E(\rho) = E(|\psi\rangle\langle\psi|)$ [] 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]

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

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

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

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.

Bob 收到他不知道 b , Alice, Bob, Eve 都有他们自己的 states, 但只有 Alice 知道 b (Bob decides which basis air 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, 否则她不能拥有一丁发到 Bob 那里的 no qubits no copy. 任何 measurement 有 $\frac{1}{2}$ 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

原理: 是因为量子力学的线性特征

和 Quantum Cryptography

即不可能构造一个能够完全复制任意量子比特, 却不对原始量子位产生干扰的系统,

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对量子信息产生干扰.

的基础.

1. 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

透露

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.

信息加固和隐私放大

整个流程举个例子:

相当于:

$a \Rightarrow$	Alice's random bit	0	1	1	0	1	0	0	1
$b \Rightarrow$	Alice's random sending basis	+	+	\times	+	\times	\times	\times	+
a/b 相同 (偏移后)	Photon polarization Alice sends	↑	\rightarrow	↑	↑	↑	↑	↑	\rightarrow
$b' \Rightarrow$	Bob's random measuring basis	+	\times	\times	\times	+	\times	+	+
根据 b' 反向 a/b	Photon polarization Bob measures	↑	\nearrow	\nwarrow	\nearrow	\rightarrow	\nearrow	\rightarrow	\rightarrow
PUBLIC DISCUSSION OF BASIS									
Shared secret key									
		0		1			0		1

有 "X" 的地方
正弦 \rightarrow Hadamard 变换, "+" 的
不变
↓ 有 "X" 的地方反做一次
Hadamard 变换, 有 "+"
的不变

下一页会对这个过程详细说明.

但这一行会有出入.

BB84 算法过程讲解 (依据的是 Qiskit 的教程, 可能与上版教材有细微的差别)

— Alice 产生 bit string — Bob 产生 bit string

initial key a 转换单bit	0	1	/	0	/	0	0	/
randomly Hadamard transform on a if basis is "x". do nothing for "+" rotation string b	0	0	1	0	1	0	0	1
Hadamard 旋转 变换	+ +	x x	+ +	x x	x x	+ +	+ +	
行进方向的 key { 右向左 } ↑(90°) → (0°) ↑(135°) ↑(45°) ↑(135°) ↑(45°) → (0°)	10>	11>	$\frac{10>-11}{\sqrt{2}}$	$\frac{10>+11}{\sqrt{2}}$	$\frac{(0>+11)}{\sqrt{2}}$	11>		
Quantum Channel								
随机 key 转换单bit	10>	11>	$\frac{10>-11}{\sqrt{2}}$	$\frac{10>+11}{\sqrt{2}}$	$\frac{(0>+11)}{\sqrt{2}}$	11>		
Inverse Hadamard transform on a if basis is "x". do nothing for "+" rotation string b	0	1	1	0	1	0	0	0
Inverse Hada- mard 旋 转 变 换	+ +	x x	x x	x x	x x	+ +	+ +	
Bob's one qubit key 测量	0	0 或 1	1	0 或 1	0 或 1	或 1	或 1	1

→ 1. randomly choose "+" or "-" basis in Hadamard state

randomly Hadamard gate

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

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

$$\text{Hadamard gate in ket representation: } H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

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

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

②. Inverse transform of Hadamard gate:

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

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

∴ Hadamard gate = Hadamard gate

以概率 $\alpha/\alpha+\beta$ 生成单个值

Shared secret key