

Quantum Key Distribution (QKD) 密钥分发

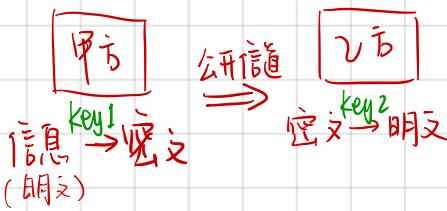
△ Key Distribution

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: 2⁵⁰ 位数的乘法很简单, 但做大数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) ↗ 基于海森堡不确定原理

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".

可以用加密而一次性密钥: MASKL NSFLD FKJPQ

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

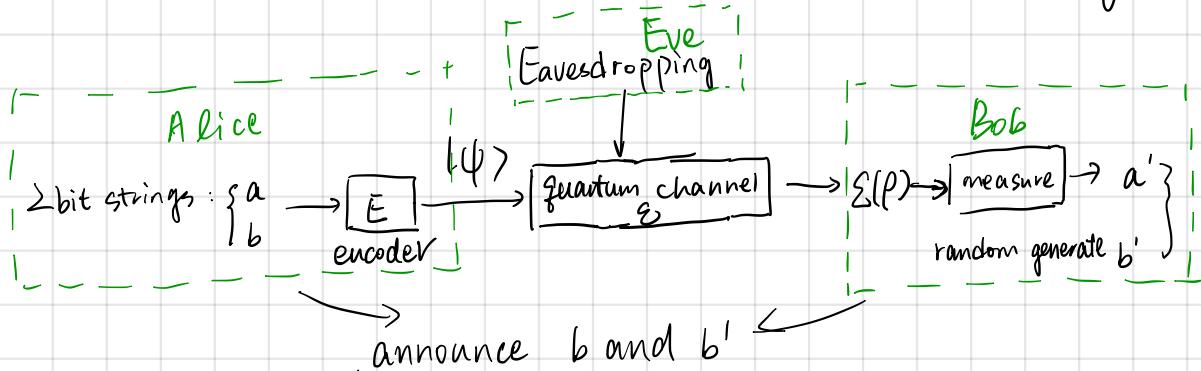
MASKL NSFLD FKJPQ $\Rightarrow 12\ 0\ 18\ 10\ | 11\ 13\ 18\ 5\ 11\ 3\ 5\ 10\ 9\ 15\ 16$

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

Part 1. 构造 - Alice 与 Bob 通过共享密钥。



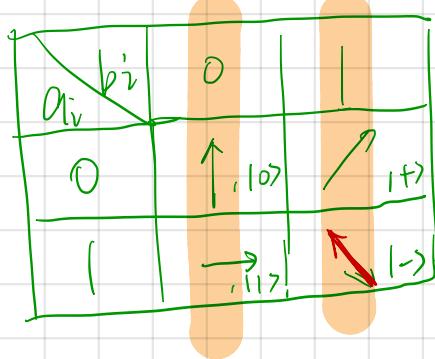
both Alice and Bob discard the qubits in a and a' where b and b' don't match
(用概率来看, 平均下来 b 和 b' 应有一半是一致的)

以下是对这个框图的具体解释：

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

$$\left. \begin{array}{l} \text{基子光波} \\ \text{偏振} \end{array} \right\} \begin{array}{l} 0 \uparrow |\psi_{00}\rangle = |0\rangle \\ 1 \rightarrow |\psi_{10}\rangle = |1\rangle \\ 0 \nearrow |\psi_{01}\rangle = |+\rangle = \frac{\sqrt{2}|0\rangle + \sqrt{2}|1\rangle}{\sqrt{2}} \\ 1 \nwarrow |\psi_{11}\rangle = |- \rangle = \frac{\sqrt{2}|0\rangle - \sqrt{2}|1\rangle}{\sqrt{2}} \end{array} \right\} \xrightarrow{\text{BB84用2对状态。每对共轭。}} \text{two states within a pair orthogonal with each other.} \xrightarrow{\text{called "basis"}} \text{wiki上说的。因为 } 135^\circ \text{, 而非 } -45^\circ.$$

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

根据左列而定

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 . \rightarrow 2 vectors orthogonal: 它们相互垂直, 点积得0.
A set of vectors $\{v_1, v_2, v_3, \dots, v_n\}$ mutually orthogonal: every pair of vectors is orthogonal

1.2 $S(P)$: quantum channel to Bob by state.

$S(P) = S(|\psi\rangle\langle\psi|)$ \square S represents both the noise and eavesdropping by a 3rd party, Eve \square
 \square $|\psi\rangle$ is what Alice sent over a public and authenticated quantum channel \square

$|\psi\rangle$ (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:

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

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

如果 Bob 收到他两个状态 b_i , Alice, Bob, Eve 都有他们自己的状态。但只有 Alice 知道 b_i (Bob 决定哪个基矢量是编码的), 所以 Bob 和 Eve 不可能区分 qubits 的状态。

而且, 根据不可克隆原理 (no-cloning theorem), 除非 Eve 做出测量, 否则她不能拥有一份发送到 Bob 那里的 qubits 的副本。每次测量都有可能得到错误的答案。

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

Quantum Information 和 Quantum Cryptography

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容易产生干扰。

的基础。

原理: 量子力学的线性特征

- 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.

信息协商和隐私放大

透露

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/a 相乘 b 编码后	Photon polarization Alice sends	↑	\rightarrow	\nwarrow	↑	\nwarrow	↗	↗	\rightarrow
$b' \Rightarrow$	Bob's random measuring basis	+	\times	\times	\times	+	\times	+	+
相乘 b' 得 a'	Photon polarization Bob measures	↑	↗	\nwarrow	↗	\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 "+"
时不变

下一页会对此过程详细说明。

但这一行会有出入

Part 2. 宿耳者 Eve

Eve 在拦截了 Alice 发送到 Bob 的信息后，必须再发送给 Bob。否则 Bob 没收到 message 就会有所察觉。

Let's explain further why Eve can be detected. If Eve intercepts a qubit from Alice, she will not know if Alice rotated its state or not. Eve can only measure a 0 or 1. And she can't measure the qubit and then send the same qubit on, because her measurement will destroy the quantum state. Consequently, Eve doesn't know when or when not to rotate to recreate Alice's original qubit. She may as well send on qubits that have not been rotated, hoping to get the rotation right 50% of the time. After she sends these qubits to Bob, Alice and Bob can compare select parts of their keys to see if they have discrepancies in places they should not.

1. Alice 发送给 Bob 他们的 qubits，但被 Eve 拦截并测量。
2. 为避免怀疑，Eve 根据她测量得到的 bits 来 prepare qubits，然后发送这些 qubits 给 Bob。
3. Bob 和 Alice 从 Part 1 中选出的那样 create keys.
4. Bob and Alice randomly select the same part of their keys to share publicly
$$\left\{ \begin{array}{l} \text{If keys don't match} \Rightarrow \text{他们怀疑 Eve 是窃听者} \\ \text{If keys match} \Rightarrow \text{他们相信 Eve 没有窃听} \end{array} \right.$$

5. They throw away the part of keys they made publicly^(in step 4)，and 用剩下的部分 of key 来加密和解密消息