Quantum Wireless Intrusion Detection Mechanism

Tien-Sheng Lin[1,2], I-Ming Tsai[1], and Sy-Yen Kuo[1]

1. Department of Electric Engineering,
National Taiwan University, Taipei, Taiwan
2. Department of International Business Management,
Lan Yang Institute of Technology, ILan, Taiwan

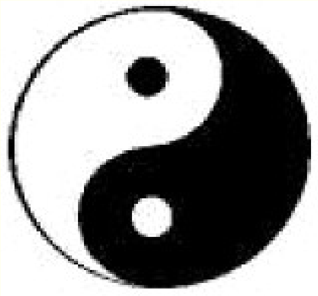
Outline

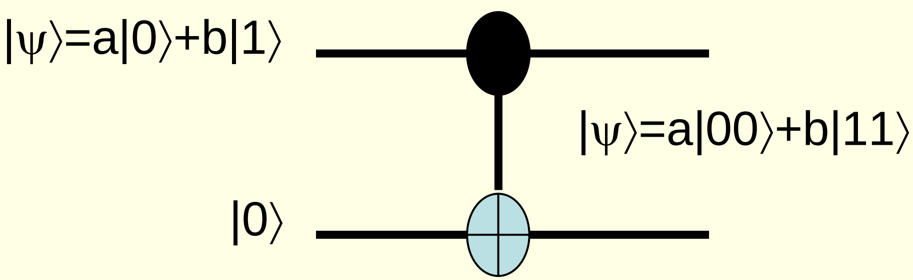
- Quantum qubits
- The BB84 protocol
- The topology
- Quantum sharing table
- Quantum detection circuit
- Conclusions

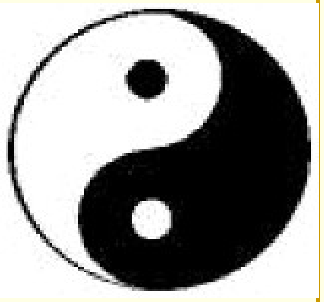
Superposition and Entanglement

$|\psi\rangle = a|0\rangle + b|1\rangle$

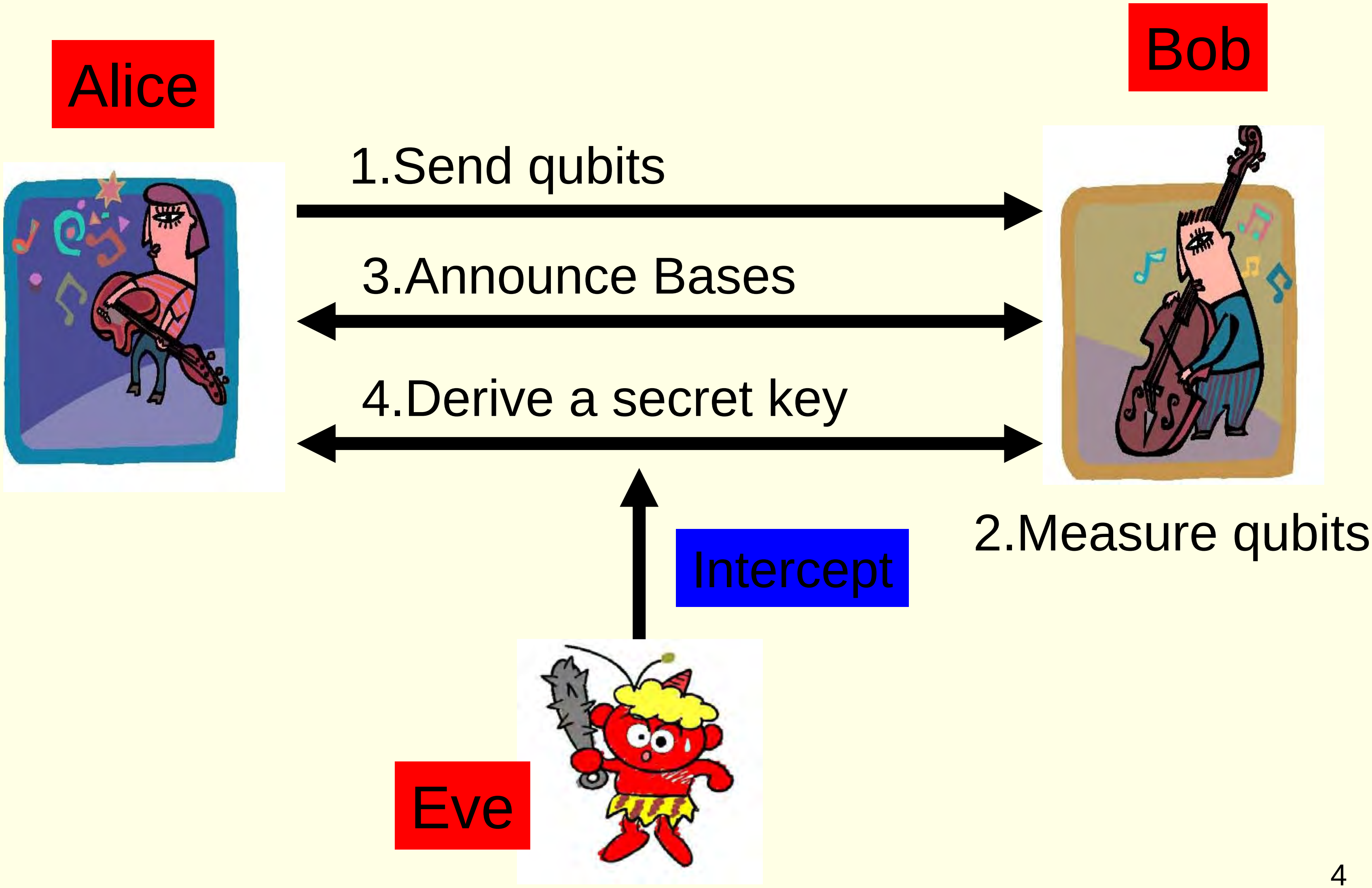
- Where $|0\rangle$ and $|1\rangle$ are two quantum states
- Where a and b are complex numbers, and $|a|^2+|b|^2=1$







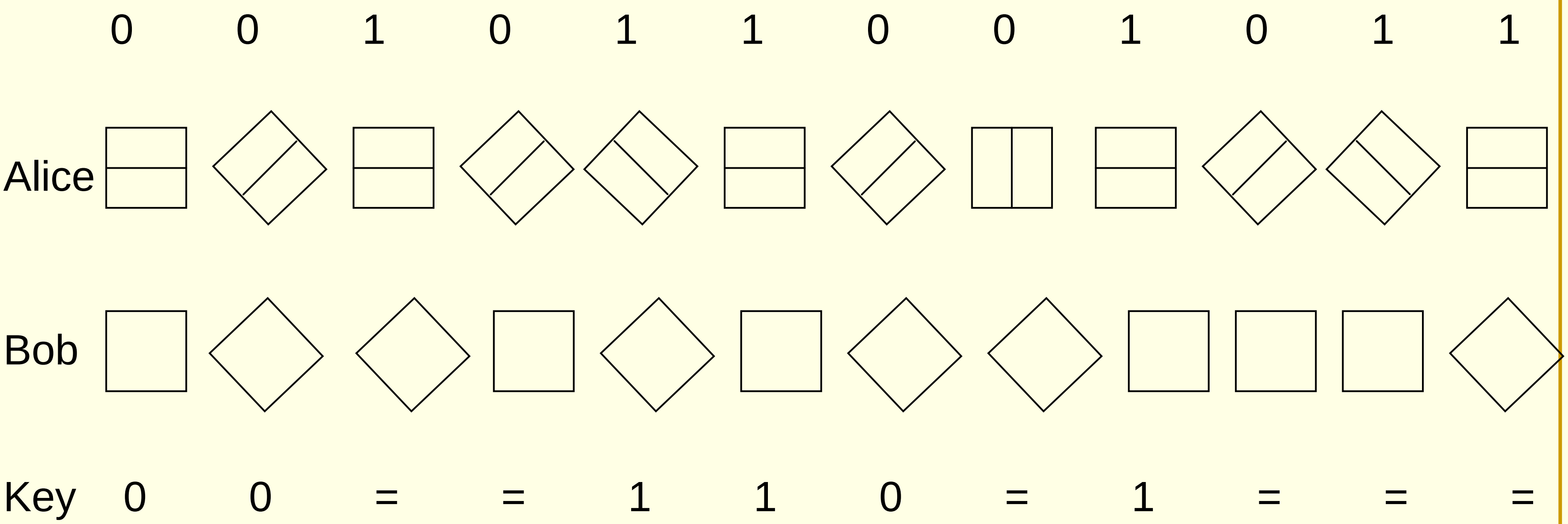
The BB84 Protocol



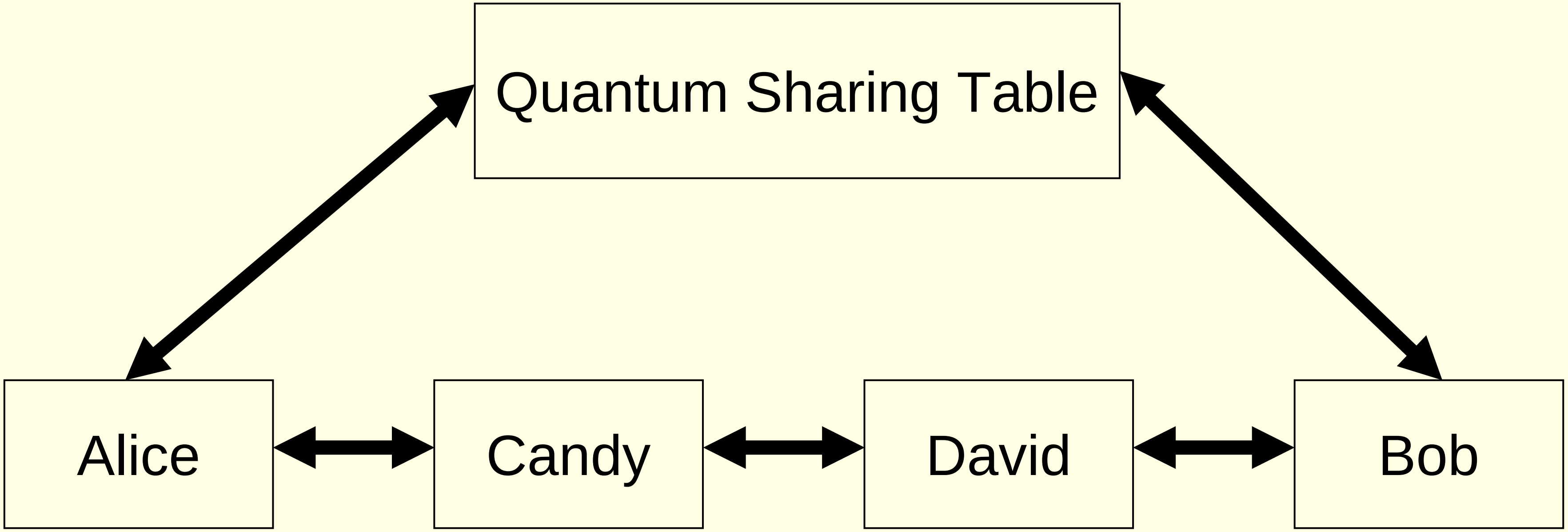
The BB84 Protocol

- 1.Alice sends Bob a stream of photons which have been randomly polarized to one of four states (0^0, 45^0, 90^0, 135^0)
- 2.Bob measures the photons in a random sequence of bases
- 3.Alice and Bob publicly announces the sequence of bases they used
- 4.Alice and Bob discard the results that have been measured using different bases, the results left can be used to derive a secret key.

The BB84 Protocol



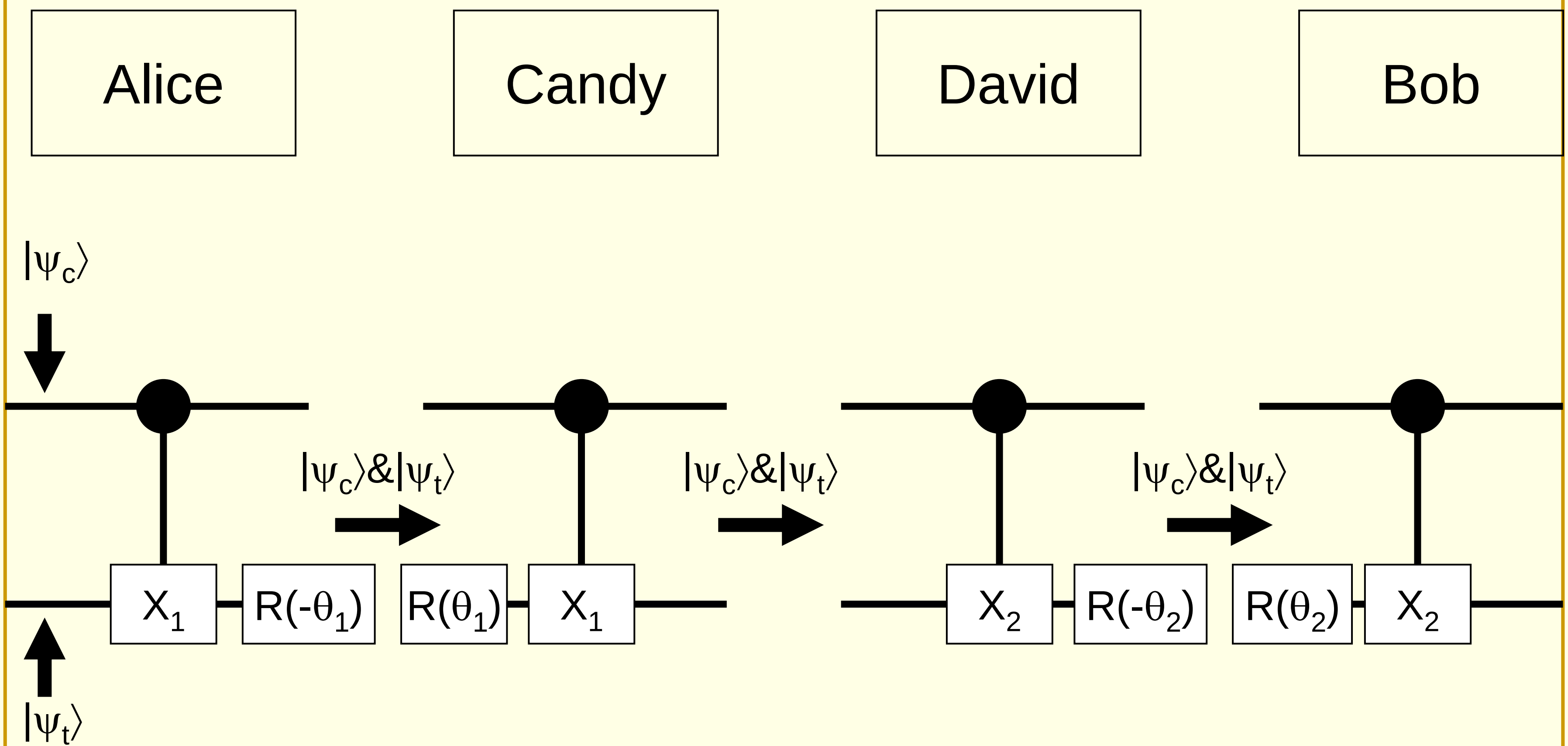
Indirect Communication



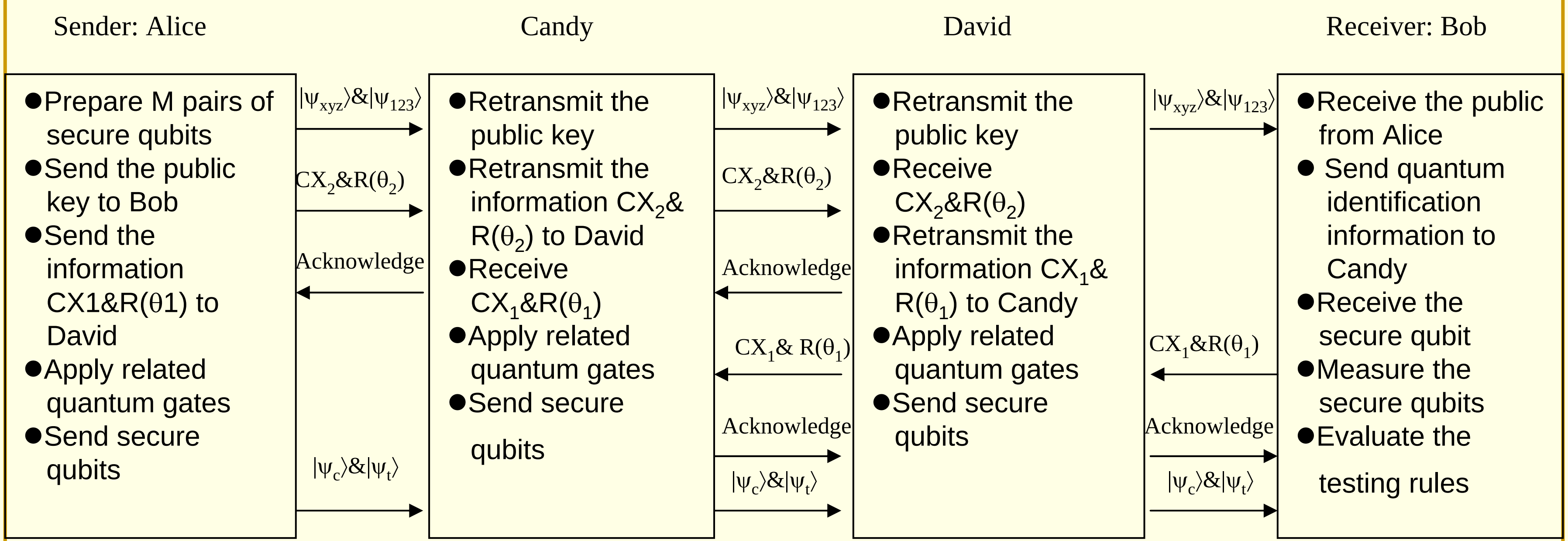
Quantum Sharing Table

$\vert\psi_{123}\rangle$	Bases	$\vert\psi_c\rangle$	$\vert\psi_t\rangle$	CX_1	CX_2	$R(\theta_1)$	$R(\theta_2)$
$\vert 000\rangle$	$b_1b_1b_3$	$\vert z^-\rangle$	$\vert y^-\rangle$	$C\sigma_Z$	$C\sigma_x$	$R(90^0)$	$R(30^0)$
$\vert 001\rangle$	$b_2b_1b_3$	$\vert z^-\rangle$	$\vert y^-\rangle$	$C\sigma_x$	$C\sigma_y$	$R(60^0)$	$R(90^0)$
$\vert 010\rangle$	$b_1b_1b_1$	$\vert z^-\rangle$	$\vert z^+\rangle$	CH	$C\sigma_x$	$R(90^0)$	$R(30^0)$
$\vert 011\rangle$	$b_2b_2b_3$	$\vert x^+\rangle$	$\vert y^-\rangle$	$C\sigma_y$	$C\sigma_y$	$R(60^0)$	$R(60^0)$
$\vert 100\rangle$	$b_3b_1b_2$	$\vert z^-\rangle$	$\vert x^-\rangle$	$C\sigma_z$	$C\sigma_x$	$R(90^0)$	$R(45^0)$
$\vert 101\rangle$	$b_2b_2b_2$	$\vert x^-\rangle$	$\vert x^+\rangle$	CH	$C\sigma_x$	$R(80^0)$	$R(50^0)$
$\vert 110\rangle$	$b_3b_3b_1$	$\vert y^+\rangle$	$\vert z^-\rangle$	$C\sigma_x$	CH	$R(60^0)$	$R(40^0)$
$\vert 111\rangle$	$b_1b_2b_2$	$\vert x^-\rangle$	$\vert x^+\rangle$	CH	$C\sigma_y$	$R(90^0)$	$R(90^0)$

Quantum Detection Circuit



The procedure



- First, quantum information: $|\psi_{xyz}\rangle\&|\psi_{123}\rangle$
- Second, quantum information: $CX_2\&R(\theta_2)$ and the acknowledge
- Third, quantum information: $CX_1\&R(\theta_1)$ and the acknowledge
- Fourth, quantum information: the secure qubits, $|\psi_c\rangle\&|\psi_t\rangle$

Conclusions

- Quantum cryptography is unconditional security.
- Quantum sharing table can act as a secret quantum key.
- Quantum detection circuit can resist man-in-the-middle attack.
- The detection circuit can reconstruct the original quantum states of the secure qubits.

Questions and Discussion

☺

Three measurement bases: Conjugate

$$b_1 = \{|z^+\rangle = |0\rangle, |z^-\rangle = |1\rangle\}$$

$$b_2 = \{|x^+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), |x^-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\}$$

$$b_3 = \{|y^+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle), |y^-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - i|1\rangle)\}$$

Eve attacks

- A. The BB84 protocol: Based on the no-cloning theorem, Eve can not know the measurement bases and measurement position
- B. The detection mechanism: Eve can not know the quantum states of the secure qubits and Bob can detect it.

Question and answer

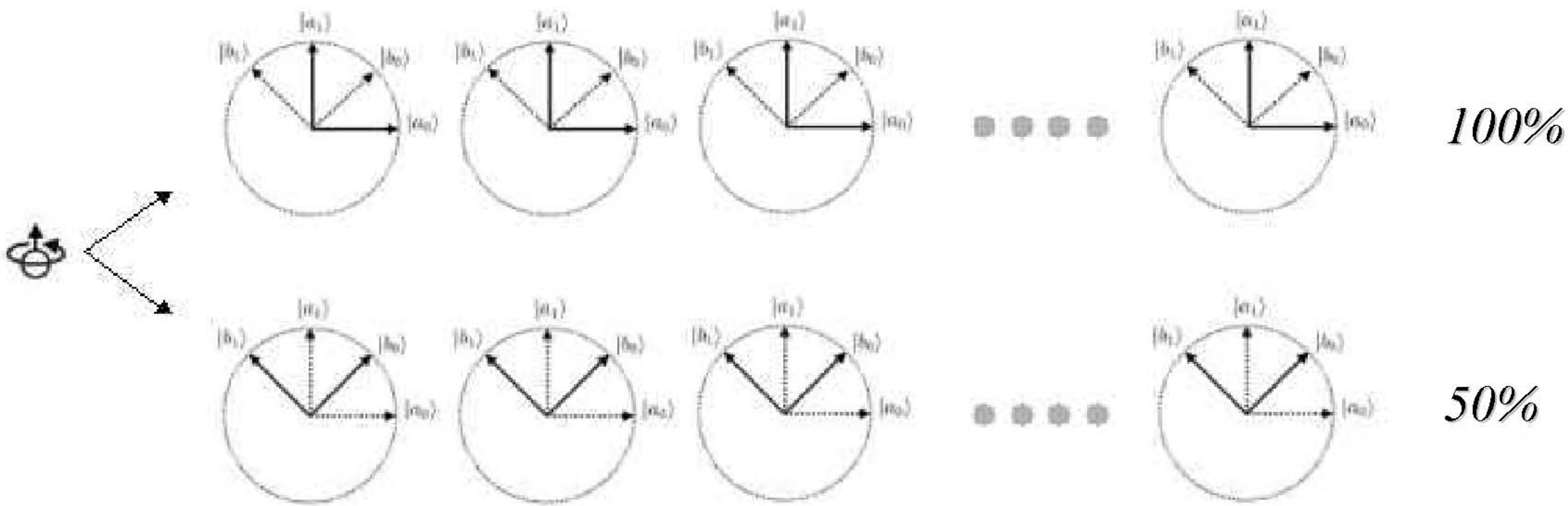
- 1.What is the major difference between classical cryptography and quantum cryptography
- Quantum cryptography is the unconditionally security and classical cryptography is conditional security; The property of the quantum cryptography is based on the laws of the physics such as no-cloning theorem, uncertainly principle and quantum teleportation. The property of the classical cryptography is based on the computing power.

Question and answer

- The major difference between the technology of quantum superposition and the technology of quantum entangled particles.
- To generate, to distribute, to maintain multiple entanglement qubits is the problem.
- The reliability of the quantum computing
- The reliability of the quantum communication

Cloning Attack

- *If the qubit can be cloned, the security would be compromised.*



- *However, it is impossible to exactly copy an unknown quantum state.*

Single Qubit

- *A single qubit can be modeled by*

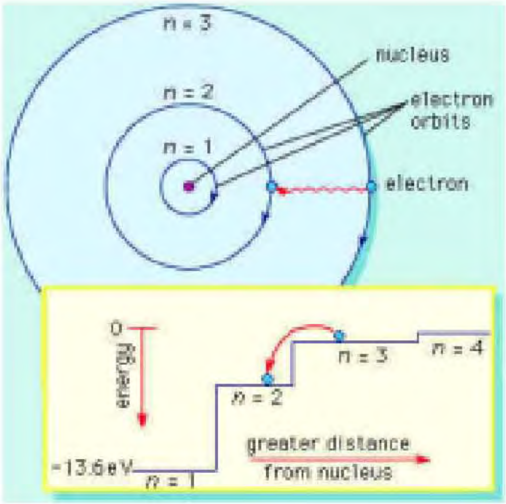
$$|\psi\rangle = c_0|0\rangle + c_1|1\rangle \qquad \text{where}$$

$$c_0, c_1 \in \mathcal{C}, \text{ and } |c_0|^2 + |c_1|^2 = 1.$$

- *In column matrix form :* $|\psi\rangle = \begin{pmatrix} c_0 \\ c_1 \end{pmatrix}$

- *Principle of superposition*

- *Probability amplitude*



More on Entanglement

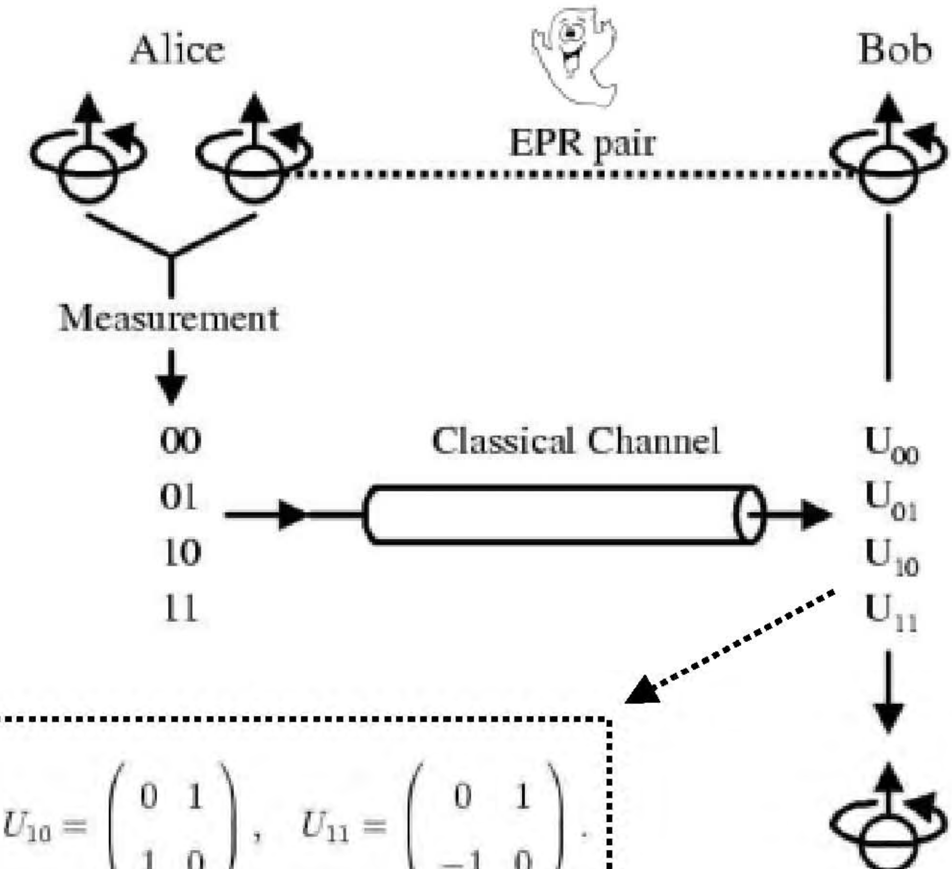
- *Spooky action-at-a-distance*

$$\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$$

- *Faster than light communication ?*

Teleportation

$$|\psi^{+}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$
$$|\psi^{-}\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$$
$$|\phi^{+}\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$$
$$|\phi^{-}\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$$



$$U_{00} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad U_{01} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad U_{10} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad U_{11} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$