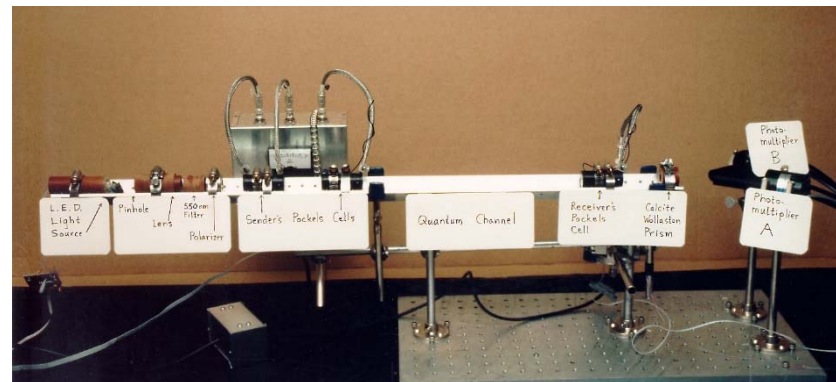




# LECTURE THREE: Introduction to Quantum Cryptography

May 7,  
2020



**Harald Weinfurter**

LMU München

# Goals of This Lecture

- **Introduction to quantum cryptography**
  - quantum physics basics,
  - quantum key distribution
    - *why*
    - *how*
      - *in combination with classical algorithms*
      - *quantum physics*
      - *classical protocol*
    - *is it really secure ?*

# QM basics



- measurement
- qubit
- entanglement
- EPR & Bell



# quantum states

- quantum system – a vector in a Hilbert space

- orthogonal basis states, e.g.  $|0\rangle, |1\rangle$

- any linear superposition possible  $|\Psi\rangle = a_0|0\rangle + a_1|1\rangle$

- evolution

- Schrödinger equation

$$\frac{d}{dt}|\Psi(t)\rangle = \mathcal{H}|\Psi(t)\rangle$$

- unitary evolution operator

$$|\Psi(t)\rangle = U(t)|\Psi(0)\rangle$$

- for time independent Hamiltonian

$$U(t) = \exp\left(-i\frac{\mathcal{H}t}{\hbar}\right)$$

# measurement

- **Observables  $A$**  (measurable quantities)

- eigenstates  $|a_i\rangle$  eigenvalues  $a_i$   $A|a_i\rangle = a_i|a_i\rangle$
- Projector  $P_i$  onto eigenstate  $|a_i\rangle$   $P_i := |a_i\rangle\langle a_i|$
- projection of qubit  $P_i|\Psi\rangle = |a_i\rangle\langle a_i|\Psi\rangle = \langle a_i|\Psi\rangle|a_i\rangle$
- length of projection  $|\langle a_i|\Psi\rangle|$

- **Measurement of observable  $A$**

- yields one of the eigenvalues  $a_i$
- with probability  $p_i = |\langle a_i|\Psi\rangle|^2$
- after measurement the system is in state  $P_i|\Psi\rangle/N = |a_i\rangle/N$

$$N = \|P_i|\Psi\rangle\|$$

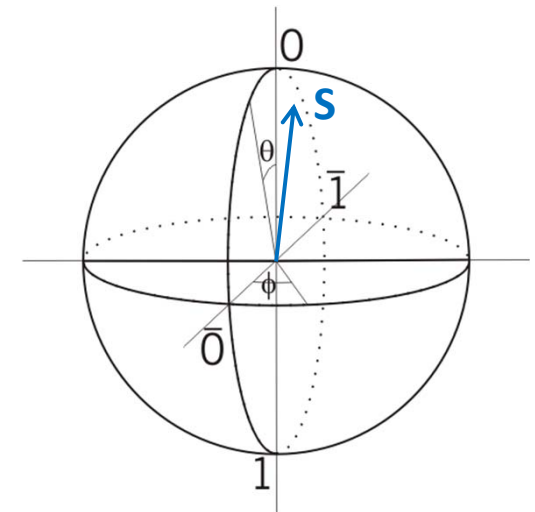
- **Measurement on ensemble**

- expectation value  $\langle A \rangle := \langle \Psi|A|\Psi\rangle$



# qubits

- two-dimensional quantum state
- Spin observable  $S$  for qubits
- Spin matrices  $\sigma_x = \frac{\hbar}{2} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$      $\sigma_y = \frac{\hbar}{2} \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$      $\sigma_z = \frac{\hbar}{2} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$
- eigenvalue +1, -1 ("spin-up", spin-down")
- eigenstates  $(|\uparrow\rangle, |\downarrow\rangle; |1\rangle, |-1\rangle) \rightarrow |0\rangle, |1\rangle$ 
  - two orthogonal basis states
  - any linear superposition possible  $|\Psi\rangle = a_0|0\rangle + a_1|1\rangle$
- general state  $\rightarrow$  Bloch sphere
  - $|\Psi\rangle = \exp\left(-i\frac{\phi}{2}\right)\cos\frac{\theta}{2}|0\rangle + \exp\left(i\frac{\phi}{2}\right)\sin\frac{\theta}{2}|1\rangle = |\theta, \phi\rangle$
  - map complex Hilbert space to three-dim space
  - $\vec{S}_{\theta, \phi} = (\sin\theta\cos\phi, \sin\theta\sin\phi, \cos\theta)^\dagger$



# qubit

- **quantum system, two-dimensional**

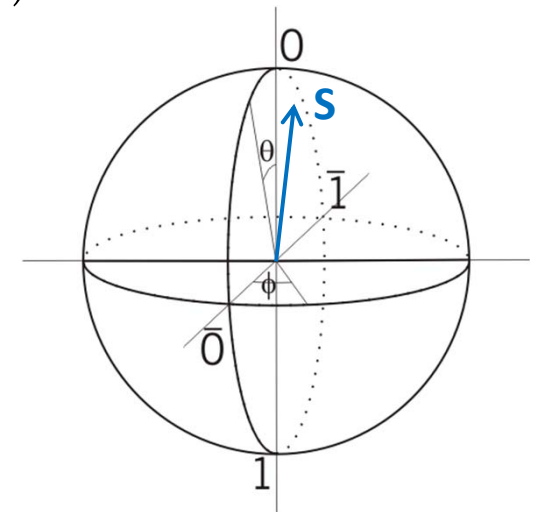
- two orthogonal basis states:  $|0\rangle, |1\rangle$
- any linear superposition possible  $|\Psi\rangle = a_0|0\rangle + a_1|1\rangle$

- **evolution**

- Schrödinger equation  $\frac{d}{dt}|\Psi(t)\rangle = \mathcal{H}|\Psi(t)\rangle$
- unitary evolution operator  $|\Psi(t)\rangle = U(t)|\Psi(0)\rangle$
- for time independent Hamiltonian  $U(t) = \exp(-i\frac{\mathcal{H}t}{\hbar})$

- **Bloch sphere**

- $|\Psi\rangle = \exp(-i\frac{\phi}{2})\cos\frac{\theta}{2}|0\rangle + \exp(i\frac{\phi}{2})\sin\frac{\theta}{2}|1\rangle = |\theta, \phi\rangle$
- map complex Hilbert space to three-dim space



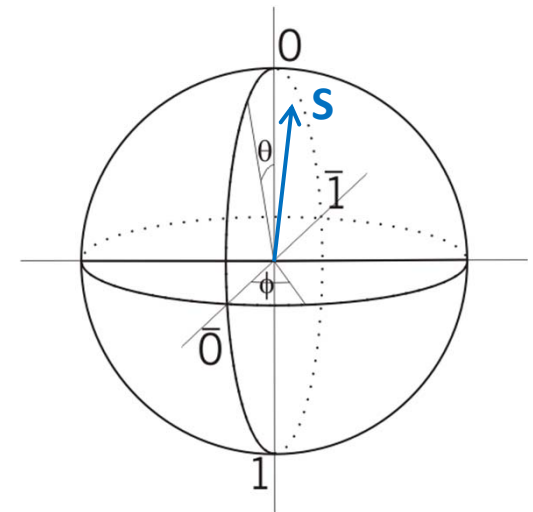
# measurement of single qubits

- e.g., measure qubits in state  $|0\rangle$ 
  - $\sigma_z$ :  $p_0=1, p_1=0$  result predetermined
  - $\sigma_x, \sigma_y$ :  $p_0=0.5, p_1=0.5$  result absolutely random
- measure qubits in state  $|\bar{0}\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$ 
  - $\sigma_x$ :  $p_0=1, p_1=0$  result predetermined
  - $\sigma_y, \sigma_z$ :  $p_0=0.5, p_1=0.5$  result absolutely random

- expectation value for spin – polarisation

$$\langle S \rangle = \begin{pmatrix} \langle \sigma_x \rangle \\ \langle \sigma_y \rangle \\ \langle \sigma_z \rangle \end{pmatrix}$$

$$\vec{S} = (\sin\theta \cos\phi, \sin\theta \sin\phi, \cos\theta)^\dagger$$



# density operators

- $|\alpha\rangle$  describes only **pure states**  
(pure state  $\rightarrow$  there is always an observable giving results with  $p=1$ )
- use **density operators** to describe **incoherent mixtures of states**

– e.g., ensemble consisting of 60%  $|\alpha\rangle$  and 40%  $|\beta\rangle$

–  $\rho := \sum w_i |\alpha^{(i)}\rangle \langle \alpha^{(i)}|$

– density matrix elements

$$\langle b'' | \rho | b' \rangle = \sum_i w_i \langle b'' | \alpha^{(i)} \rangle \langle \alpha^{(i)} | b' \rangle$$

- **examples:**

– pure states:

$$|0\rangle: \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \quad |1\rangle: \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}, \quad |\bar{0}\rangle: \frac{1}{2} \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}, \quad |\bar{1}\rangle: \frac{1}{2} \begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix}$$

– incoherent mixtures:

$$\frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1| = \frac{1}{2} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

# entanglement basics

- superposition of 2-particle states !
- basis:  $|0\rangle|0\rangle, |0\rangle|1\rangle, |1\rangle|0\rangle, |1\rangle|1\rangle$
- general state:  $|\Psi\rangle = a_{00}|0\rangle|0\rangle + a_{01}|0\rangle|1\rangle + a_{10}|1\rangle|0\rangle + a_{11}|1\rangle|1\rangle$
- different types of states:
- product states:

$$\begin{aligned} |\Psi\rangle_{product} &= |\varphi\rangle \otimes |\chi\rangle = (a_0|0\rangle + a_1|1\rangle) \otimes (b_0|0\rangle + b_1|1\rangle) \\ &= a_0b_0|0\rangle|0\rangle + a_0b_1|0\rangle|1\rangle + a_1b_0|1\rangle|0\rangle + a_1b_1|1\rangle|1\rangle \end{aligned}$$

$$|\Psi\rangle_{entangled} = (|0\rangle|0\rangle + |1\rangle|1\rangle) / \sqrt{2} \quad a_{00} = a_{11} = \frac{1}{\sqrt{2}}$$

- entangled states
- Def.: a state is entangled if it is not factorizable

$$|\Psi\rangle_{entangled} \neq |\varphi\rangle|\chi\rangle$$

# entanglement basics

- max. entangled states:  $|\Psi\rangle = (|0\rangle|0\rangle + |1\rangle|1\rangle)/\sqrt{2}$ 
    - not factorizable
    - pure state  $\Rightarrow$  measurement results **predetermined**
    - single particle states are reduced states  $\rho_A = Tr_B(\rho)$ 
      - $\Rightarrow$  **incoherent mixtures**
- $\Rightarrow$  observation of a pair of entangled particles:  $\langle \sigma_i \sigma_i \rangle = Tr(\sigma_i \sigma_i \rho) = \pm 1$   
**measurement results are random but correlated**
- $\Rightarrow$  observation of a single particle of the pair does not  
reveal any information about the state  $\langle \sigma_{i,A} \rangle = Tr(\sigma_{i,A} \rho_A) = 0$

check:

- e.g., 2-party state:  
 $|\Psi\rangle = (|0\rangle|0\rangle + |1\rangle|1\rangle) / \sqrt{2}$

for vector in basis ( $e_{ij} = |i\rangle|j\rangle$  with  $i, j \in \{0,1\}$ ):  $|\Psi\rangle \triangleq \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix}$       $\rho = |\Psi\rangle\langle\Psi| = \frac{1}{2} \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix}$

$$\langle \sigma_i \sigma_i \rangle = \text{Tr}(\sigma_i \rho) = \pm 1$$

$$\begin{aligned} & \text{Tr} \left( \frac{1}{2} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \otimes \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix} \right) \\ &= \text{Tr} \left( \frac{1}{2} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix} \right) = 1 \end{aligned}$$

$$\begin{aligned} \langle \sigma_{i,A} \rangle &= \text{Tr}(\sigma_{i,A} \rho_A) = 0 \\ \rho_A &= \text{Tr}_B(\rho) \end{aligned}$$

$$\rho_A = \text{Tr}_B \frac{1}{2} \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix} = \frac{1}{2} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad \text{Tr} \left( \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \otimes \frac{1}{2} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right) = 0$$

# consequences (used against eavesdropper!)

- Heisenberg's uncertainty principle  $\langle (\Delta A)^2 \rangle \langle (\Delta B)^2 \rangle \geq \frac{1}{4} |\langle [A, B] \rangle|^2$   
 $[\sigma_i, \sigma_j] = 2i\epsilon_{ijk}\sigma_k \Rightarrow$  after measuring/preparing in  $\sigma_z$ ,  
 result of measurement in  $\sigma_x$  is maximally uncertain  $\rightarrow$  noise!

- copy single qubits?

$\Rightarrow$  no-cloning theorem

– imagine, there is a copy machine (initialized in  $|0\rangle$ ):

$$|0\rangle_{qubit} |0\rangle_{copy} \xrightarrow{copy} |0\rangle_{qubit} |0\rangle_{copy}$$

$$|1\rangle_{qubit} |0\rangle_{copy} \xrightarrow{copy} |1\rangle_{qubit} |1\rangle_{copy}$$

– but, try to copy  $|\bar{0}\rangle$ :  $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)_{qubit} |0\rangle_{copy} \xrightarrow{copy} \frac{1}{\sqrt{2}}(|0\rangle_{qubit} |0\rangle_{copy} + |1\rangle_{qubit} |1\rangle_{copy})$

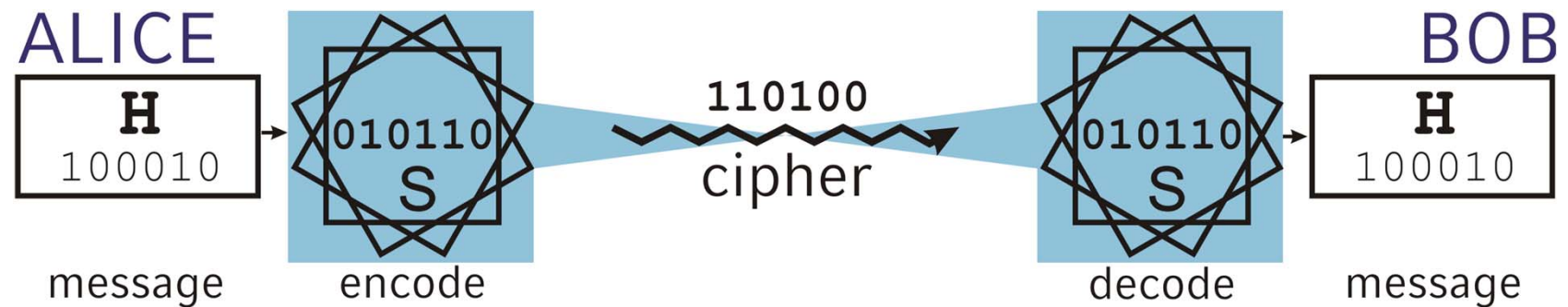
– state is maximally entangled!  
 not factorizable, ie.  $\neq \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)_{qubit} \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)_{copy}$

$\Rightarrow$  only one set of orthogonal states can be copied

$\Rightarrow$  for other states entanglement with eavesdropper  $\rightarrow$  noise!

# why : secure communication

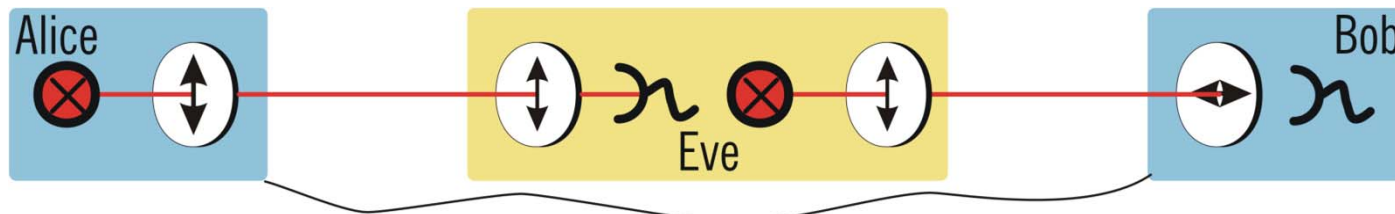
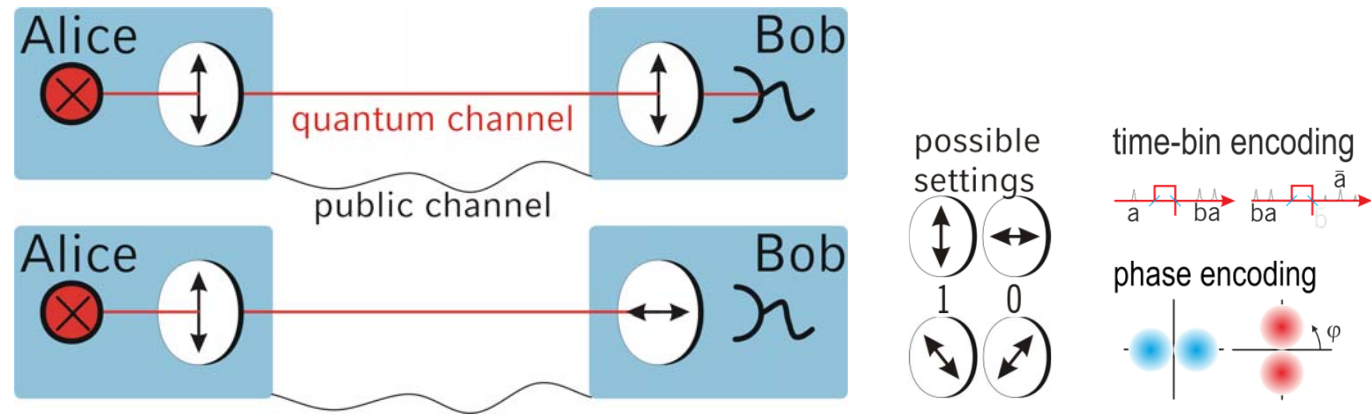
- one time pad
  - encode every bit of the message with a bit of the key



“the perfect method to communicate securely  
– provided one can communicate securely”

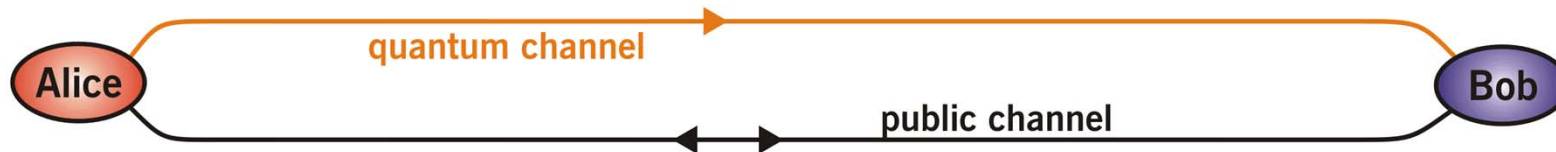
# how: quantum cryptography – – quantum key distribution

exchange key with single quanta



eavesdropper causes errors ! → security check

C.H. Bennett, G. Brassard (1984) (BB84)



No.	Bit	Basis	Pol.
1	0	1: P/M	+45°
2	0	0: H/V	0°
3	1	1: P/M	-45°
4	1	0: H/V	90°
5	1	0: H/V	90°
6	1	1: P/M	-45°
7	1	1: P/M	-45°
8	0	1: P/M	+45°
9	0	1: P/M	+45°
10	0	0: H/V	0°
11	0	1: P/M	+45°
12	1	0: H/V	90°
13	1	1: P/M	-45°
14	0	1: P/M	+45°
15	1	0: H/V	90°
16	1	1: P/M	-45°
17	1	0: H/V	90°
18	0	0: H/V	0°
19	1	0: H/V	90°
20	0	0: H/V	0°
21	1	1: P/M	-45°
22	1	0: H/V	90°
23	0	1: P/M	+45°
24	0	0: H/V	0°
25	0	1: P/M	+45°
26	0	0: H/V	0°
27	0	1: P/M	+45°
28	1	1: P/M	-45°
29	1	0: H/V	90°
30	1	0: H/V	90°
31	1	1: P/M	-45°
32	1	1: P/M	-45°

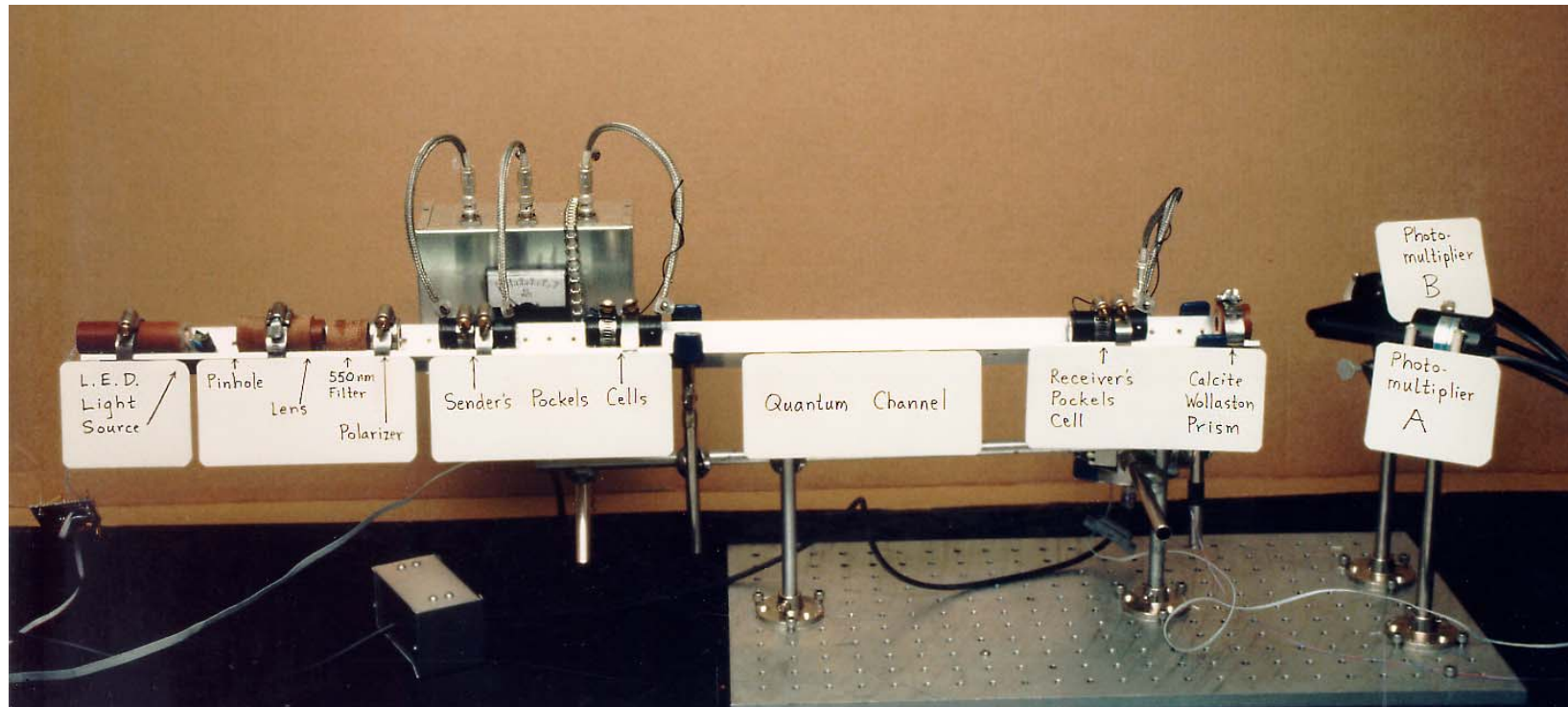
sends photons with randomly chosen polarization



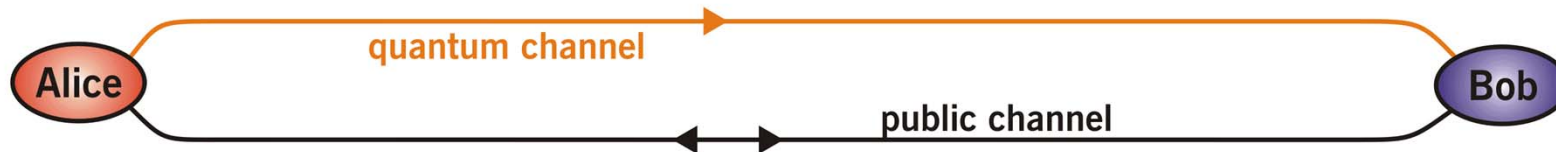
detects photons in randomly chosen basis

No.	Bit	Det.	Pol.
1	1: P/M	+45°	0
2	0: H/V	0°	0
3	0: H/V	90°	1
4	0: H/V	90°	1
5	1: P/M	+45°	0
6	0: H/V	0°	0
7	0: H/V	■	
8	1: P/M	+45°	0
9	1: P/M	■	
10	0: H/V	0°	0
11	1: P/M	+45°	0
12	0: H/V	90°	1
13	1: P/M	-45°	1
14	0: H/V	90°	1
15	1: P/M	+45°	0
16	1: P/M	■	
17	1: P/M	-45°	1
18	0: H/V	0°	0
19	1: P/M	+45°	0
20	1: P/M	■	
21	0: H/V	90°	1
22	1: P/M	-45°	1
23	1: P/M	+45°	0
24	0: H/V	0°	0
25	0: H/V	■	
26	1: P/M	+45°	0
27	0: H/V	0°	0
28	0: H/V	■	
29	1: P/M	-45°	1
30	0: H/V	■	
31	0: H/V	90°	1
32	1: P/M	-45°	1

# Aunt Martha



C.H. Bennett, F. Besette, G. Brassard, L. Savail, J. Smolin (1992)



No.	Bit	Basis	Pol.
1	0	1: P/M	+45°
2	0	0: H/V	0°
3	1	1: P/M	-45°
4	1	0: H/V	90°
5	1	0: H/V	90°
6	1	1: P/M	-45°
7	1	1: P/M	-45°
8	0	1: P/M	+45°
9	0	1: P/M	+45°
10	0	0: H/V	0°
11	0	1: P/M	+45°
12	1	0: H/V	90°
13	1	1: P/M	-45°
14	0	1: P/M	+45°
15	1	0: H/V	90°
16	1	1: P/M	-45°
17	1	0: H/V	90°
18	0	0: H/V	0°
19	1	0: H/V	90°
20	0	0: H/V	0°
21	1	1: P/M	-45°
22	1	0: H/V	90°
23	0	1: P/M	+45°
24	0	0: H/V	0°
25	0	1: P/M	+45°
26	0	0: H/V	0°
27	0	1: P/M	+45°
28	1	1: P/M	-45°
29	1	0: H/V	90°
30	1	0: H/V	90°
31	1	1: P/M	-45°
32	1	1: P/M	-45°

sends photons with randomly chosen polarization



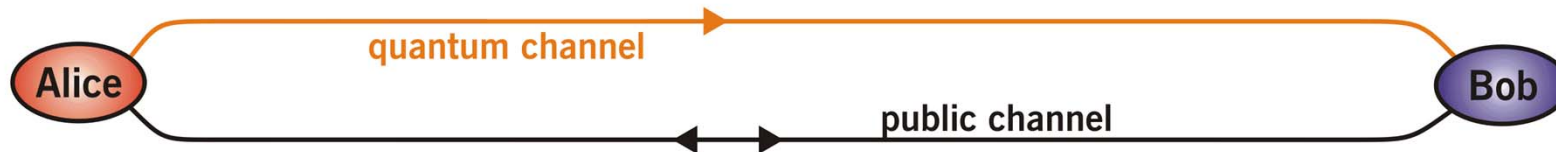
detects photons in randomly chosen basis

erases bit, if no detection



erases bit, if no detection

No.	Bit	Det.	Pol.
1	1: P/M	+45°	0
2	0: H/V	0°	0
3	0: H/V	90°	1
4	0: H/V	90°	1
5	1: P/M	+45°	0
6	0: H/V	0°	0
7	0: H/V	■	
8	1: P/M	+45°	0
9	1: P/M	■	
10	0: H/V	0°	0
11	1: P/M	+45°	0
12	0: H/V	90°	1
13	1: P/M	-45°	1
14	0: H/V	90°	1
15	1: P/M	+45°	0
16	1: P/M	■	
17	1: P/M	-45°	1
18	0: H/V	0°	0
19	1: P/M	+45°	0
20	1: P/M	■	
21	0: H/V	90°	1
22	1: P/M	-45°	1
23	1: P/M	+45°	0
24	0: H/V	0°	0
25	0: H/V	■	
26	1: P/M	+45°	0
27	0: H/V	0°	0
28	0: H/V	■	
29	1: P/M	-45°	1
30	0: H/V	■	
31	0: H/V	90°	1
32	1: P/M	-45°	1



No.	Bit	Basis	Pol.
1	0	1: P/M	+45°
2	0	0: H/V	0°
3	1	1: P/M	-45°
4	1	0: H/V	90°
5	1	0: H/V	90°
6	1	1: P/M	-45°
7	1	1: P/M	-45°
8	0	1: P/M	+45°
9	0	1: P/M	+45°
10	0	0: H/V	0°
11	0	1: P/M	+45°
12	1	0: H/V	90°
13	1	1: P/M	-45°
14	0	1: P/M	+45°
15	1	0: H/V	90°
16	1	1: P/M	-45°
17	1	0: H/V	90°
18	0	0: H/V	0°
19	1	0: H/V	90°
20	0	0: H/V	0°
21	1	1: P/M	-45°
22	1	0: H/V	90°
23	0	1: P/M	+45°
24	0	0: H/V	0°
25	0	1: P/M	+45°
26	0	0: H/V	0°
27	0	1: P/M	+45°
28	1	1: P/M	-45°
29	1	0: H/V	90°
30	1	0: H/V	90°
31	1	1: P/M	-45°
32	1	1: P/M	-45°

sends photons with randomly chosen polarization



detects photons in randomly chosen basis

erases bit, if no detection



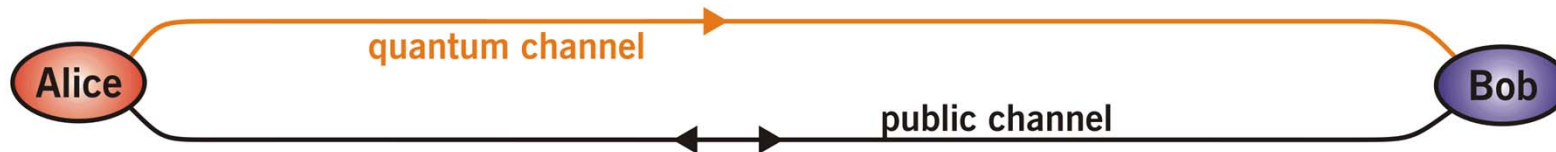
erases bit, if no detection

erases bit, if wrong basis



erases bit, if wrong basis

No.	Bit	Det.	Pol.
1	1: P/M	+45°	0
2	0: H/V	0°	0
3	0: H/V	90°	1
4	0: H/V	90°	1
5	1: P/M	+45°	0
6	0: H/V	0°	0
7	0: H/V	0°	0
8	1: P/M	+45°	0
9	1: P/M	■	■
10	0: H/V	0°	0
11	1: P/M	+45°	0
12	0: H/V	90°	1
13	1: P/M	-45°	1
14	0: H/V	90°	1
15	1: P/M	+45°	0
16	1: P/M	■	■
17	1: P/M	-45°	1
18	0: H/V	0°	0
19	1: P/M	+45°	0
20	1: P/M	■	■
21	0: H/V	90°	1
22	1: P/M	-45°	1
23	1: P/M	+45°	0
24	0: H/V	0°	0
25	0: H/V	■	■
26	1: P/M	+45°	0
27	0: H/V	0°	0
28	0: H/V	■	■
29	1: P/M	-45°	1
30	0: H/V	■	■
31	0: H/V	90°	1
32	1: P/M	-45°	1



No.	Bit	Basis	Pol.
1	0	1: P/M	+45°
2	0	0: H/V	0°
3	1	1: P/M	-45°
4	1	0: H/V	90°
5	1	0: H/V	90°
6	1	1: P/M	-45°
7	1	1: P/M	-45°
8	0	1: P/M	+45°
9	0	1: P/M	+45°
10	0	0: H/V	0°
11	0	1: P/M	+45°
12	1	0: H/V	90°
13	1	1: P/M	-45°
14	0	1: P/M	+45°
15	1	0: H/V	90°
16	1	1: P/M	-45°
17	1	0: H/V	90°
18	0	0: H/V	0°
19	1	0: H/V	90°
20	0	0: H/V	0°
21	1	1: P/M	-45°
22	1	0: H/V	90°
23	0	1: P/M	+45°
24	0	0: H/V	0°
25	0	1: P/M	+45°
26	0	0: H/V	0°
27	0	1: P/M	+45°
28	1	1: P/M	-45°
29	1	0: H/V	90°
30	1	0: H/V	90°
31	1	1: P/M	-45°
32	1	1: P/M	-45°

sends photons with randomly chosen polarization



detects photons in randomly chosen basis

erases bit, if no detection



erases bit, if no detection

erases bit, if wrong basis



erases bit, if wrong basis

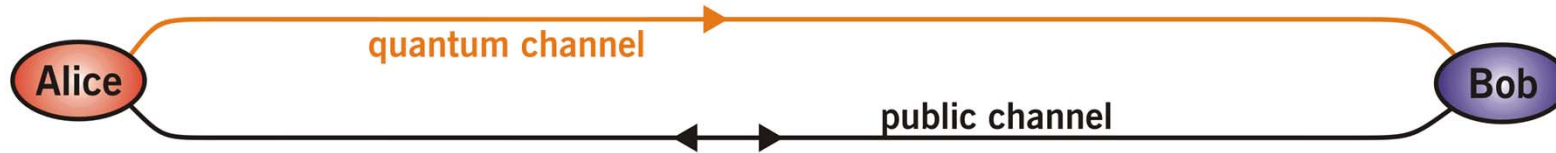
erases test bits error correction



erases test bits error correction

$$\text{QBER} = \frac{\text{\#wrong bits}}{\text{\# all bits}}$$

No.	Bit	Det.	Pol.
1	1: P/M	+45°	0
2	0: H/V	0°	0
3	0: H/V	90°	1
4	0: H/V	90°	1
5	1: P/M	+45°	0
6	0: H/V	0°	0
7	0: H/V	0°	0
8	1: P/M	+45°	0
9	1: P/M	■	■
10	0: H/V	0°	0
11	1: P/M	+45°	0
12	0: H/V	90°	1
13	1: P/M	-45°	1
14	0: H/V	90°	1
15	1: P/M	+45°	0
16	1: P/M	■	■
17	1: P/M	-45°	1
18	0: H/V	0°	0
19	1: P/M	+45°	0
20	1: P/M	■	■
21	0: H/V	90°	1
22	1: P/M	-45°	1
23	1: P/M	+45°	0
24	0: H/V	0°	0
25	0: H/V	■	■
26	1: P/M	+45°	0
27	0: H/V	0°	0
28	0: H/V	■	■
29	1: P/M	-45°	1
30	0: H/V	■	■
31	0: H/V	90°	1
32	1: P/M	-45°	1



No.	Bit	Basis	Pol.
1	0	1: P/M	+45°
2	0	0: H/V	0°
3	1	1: P/M	-45°
4	1	0: H/V	90°
5	1	0: H/V	90°
6	1	1: P/M	-45°
7	1	1: P/M	-45°
8	0	1: P/M	+45°
9	0	1: P/M	+45°
10	0	0: H/V	0°
11	0	1: P/M	+45°
12	1	0: H/V	90°
13	1	1: P/M	-45°
14	0	1: P/M	+45°
15	1	0: H/V	90°
16	1	1: P/M	-45°
17	1	0: H/V	90°
18	0	0: H/V	0°
19	1	0: H/V	90°
20	0	0: H/V	0°
21	1	1: P/M	-45°
22	1	0: H/V	90°
23	0	1: P/M	+45°
24	0	0: H/V	0°
25	0	1: P/M	+45°
26	0	0: H/V	0°
27	0	1: P/M	+45°
28	1	1: P/M	-45°
29	1	0: H/V	90°
30	1	0: H/V	90°
31	1	1: P/M	-45°
32	1	1: P/M	-45°

sends photons with randomly chosen polarization



detects photons in randomly chosen basis

erases bit, if no detection



erases bit, if no detection

erases bit, if wrong basis



erases bit, if wrong basis

erases test bits error correction



erases test bits error correction

encrypts message

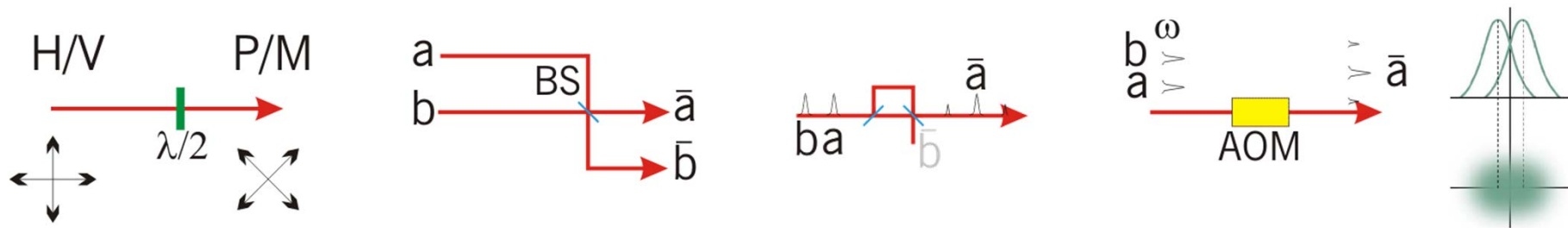


decrypts cifer

No.	Bit	Det.	Pol.
1	1: P/M	+45°	0
2	0: H/V	0°	0
3	0: H/V	90°	1
4	0: H/V	90°	1
5	1: P/M	+45°	0
6	0: H/V	0°	0
7	0: H/V	0°	0
8	1: P/M	+45°	0
9	1: P/M	0°	0
10	0: H/V	0°	0
11	1: P/M	+45°	0
12	0: H/V	90°	1
13	1: P/M	-45°	1
14	0: H/V	90°	1
15	1: P/M	+45°	0
16	1: P/M	0°	0
17	1: P/M	-45°	1
18	0: H/V	0°	0
19	1: P/M	+45°	0
20	1: P/M	0°	0
21	0: H/V	90°	1
22	1: P/M	-45°	1
23	1: P/M	+45°	0
24	0: H/V	0°	0
25	0: H/V	0°	0
26	1: P/M	+45°	0
27	0: H/V	0°	0
28	0: H/V	0°	0
29	1: P/M	-45°	1
30	0: H/V	0°	0
31	0: H/V	90°	1
32	1: P/M	-45°	1

# quantum cryptography protocols

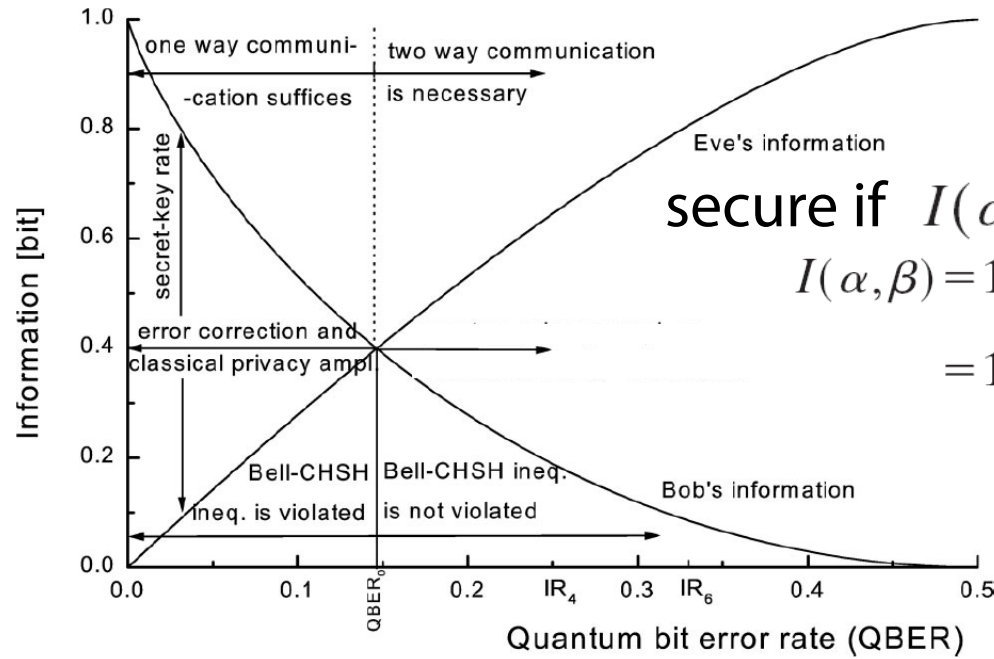
- encoding in **different degree of freedom**
  - polarization → path, time-bin, frequency



– phase and amplitude of E-field ("continuous variable")

- **three bases:** H/V, P/M, L/R (left/right circular)
- **Bennett 92:** two nonorthogonal states
- **SARG:** different coding: H/V=1, P/M=0
- **higher dimensional systems:** qubit → qutrit...qunit
  - many paths, times; combinations of pol/time/path
  - higher capacity/photon, deterministic

# is it secure?

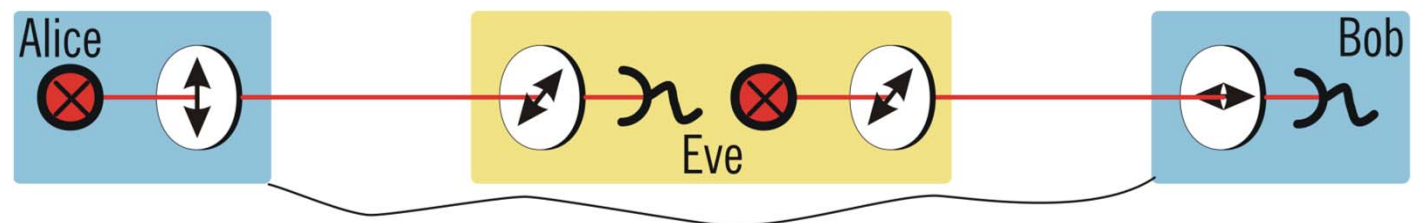


secure if  $I(\alpha, \beta) > I(\alpha, \epsilon)$  or  $I(\alpha, \beta) > I(\beta, \epsilon)$   
 $I(\alpha, \beta) = 1 - h(\mathcal{D})$

$$= 1 + \mathcal{D} \log_2(\mathcal{D}) + (1 - \mathcal{D}) \log_2(1 - \mathcal{D})$$

$$I^{\max}(\alpha, \epsilon) = 1 - h\left(\frac{1 + \sin x}{2}\right)$$

for  $\text{QBER} = \mathcal{D} = [1 - \cos(x)]/2$



eavesdropper causes errors ! → security check  
 C.H. Bennett, G. Brassard (1984) (BB84)

# quantum key distribution

- A and B connected via quantum and authenticated classical channel
- A sends quantum systems in **nonorthogonal quantum states** to B
- A chooses states randomly, B observes randomly
- A and B use classical communication to distill a key
- any eavesdropping attack is revealed by noise (bit errors) in the key
- A and B **determine maximal information** an eavesdropper could have. **QBER**
- A and B perform error correction
- A and B perform privacy amplification (reduce key length by amount of information an eavesdropper could have gained during attack + information leaked during error correction across classical channel)
- A and B can use the key