

# Practical quantum cryptography and communication

**W. Tittel**

*IQIS, University of Calgary*



# Practical quantum cryptography and communication

- ❑ qubits, entangled qubits & teleportation
- ❑ quantum cryptography
- ❑ improving the key rate: new protocols
- ❑ improving the distance: quantum relays & quantum repeater

# qubits & entangled qubits

## qubit

$$|\psi\rangle_A = \alpha |0\rangle_A + \beta e^{i\phi} |1\rangle_A = \begin{pmatrix} \alpha \\ \beta e^{i\phi} \end{pmatrix}$$

qubits can be measured in any basis,

$$\text{e.g. } \sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

$$\sigma_i |\psi\rangle = \pm 1 |\psi\rangle$$

→ deterministic result

otherwise probabilistic result

no perfect copying possible

## entangled qubits

$$|\psi\rangle_{AB} = \alpha |0\rangle_A |0\rangle_B + \beta e^{i\phi} |1\rangle_A |1\rangle_B$$

Bell states

$$|\psi^\pm\rangle_{AB} = 2^{-1/2} [ |0\rangle_A |1\rangle_B \pm |1\rangle_A |0\rangle_B ]$$

$$|\phi^\pm\rangle_{AB} = 2^{-1/2} [ |0\rangle_A |0\rangle_B \pm |1\rangle_A |1\rangle_B ]$$

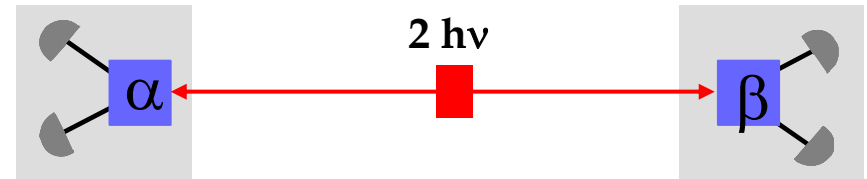
→ perfect correlation, violation of Bell inequality

→ important resource for quantum communication/computation



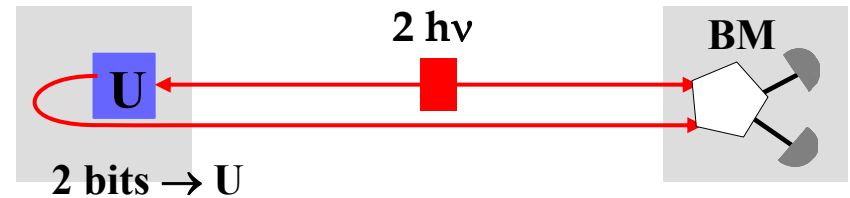
# entanglement: a resource for quantum communication

- entangled states allow to establish secret, classical bits: quantum cryptography



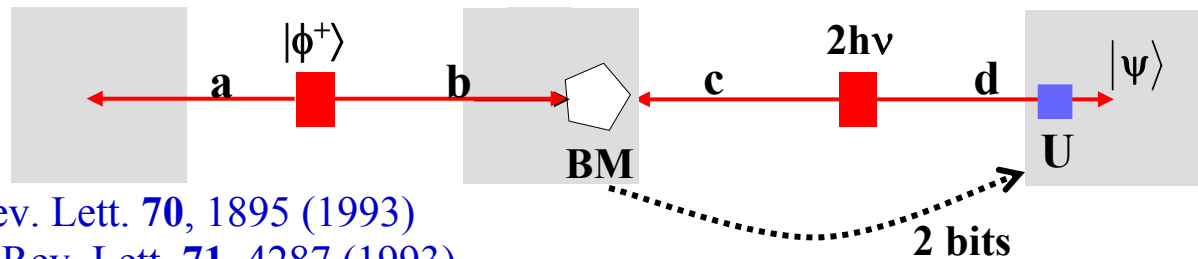
A. Ekert, Phys. Rev. Lett. **67**, 661 (1991)

- entangled states allow to transmit 2 classical bits using only one qubit: dense coding



C. Bennett *et al*, Phys. Rev. Lett. **69**, 2881 (1992)

- entangled states allow to transmit one (unknown) qubit using only classical communication: quantum teleportation & entanglement swapping



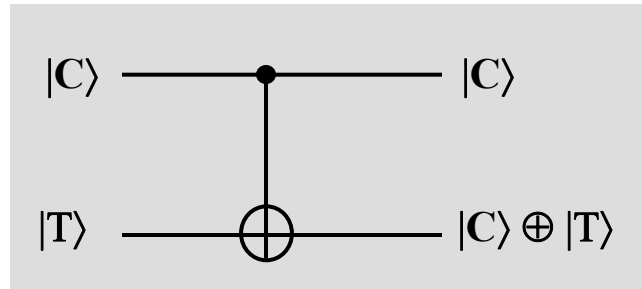
C. Bennett *et al*., Phys. Rev. Lett. **70**, 1895 (1993)

M. Żukowski *et al*., Phys. Rev. Lett. **71**, 4287 (1993)



# Bell state analyzer: the CNOT gate

$$\text{CNOT: } |C, T\rangle \rightarrow |C, C \oplus T\rangle$$



$$\left. \begin{array}{l} |00\rangle \rightarrow |00\rangle \\ |01\rangle \rightarrow |01\rangle \\ |10\rangle \rightarrow |11\rangle \\ |11\rangle \rightarrow |10\rangle \end{array} \right\} \text{Target flips when control is } |1\rangle$$

$$|\phi^+\rangle : \quad |00\rangle + |11\rangle \rightarrow |00\rangle + |10\rangle \quad = [|0\rangle + |1\rangle] \otimes |0\rangle$$

$$|\phi^-\rangle : \quad |00\rangle - |11\rangle \rightarrow |00\rangle - |10\rangle \quad = [|0\rangle - |1\rangle] \otimes |0\rangle$$

$$|\psi^+\rangle : \quad |01\rangle + |10\rangle \rightarrow |01\rangle + |11\rangle \quad = [|0\rangle + |1\rangle] \otimes |1\rangle$$

$$|\psi^-\rangle : \quad |01\rangle - |10\rangle \rightarrow |01\rangle - |11\rangle \quad = [|0\rangle - |1\rangle] \otimes |1\rangle$$

**Problem: CNOT with photons is very inefficient**



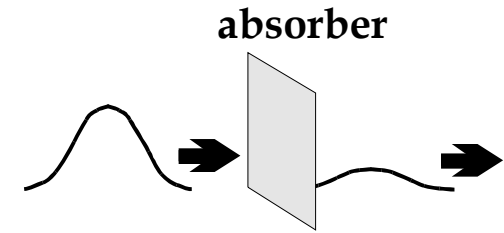
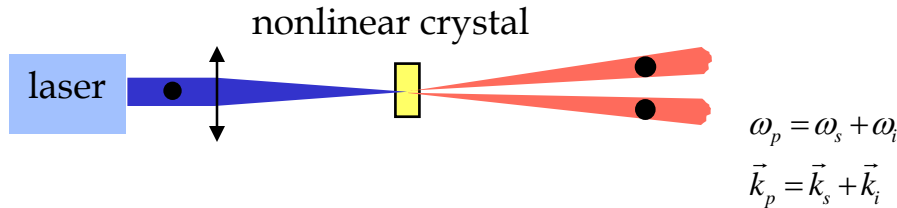
# the toolbox

- ❑ creation and detection of single photons
- ❑ preparation and measurement of qubits
- ❑ generation and measurement of pairs of entangled qubits
- ❑ transmission of qubits



# single photons: creation

- single photons approximated by faint laser pulses
- single photons based on photon pairs



$$\rho = \sum_{\mathbf{n}} \frac{\mu^{\mathbf{n}} e^{-\mu}}{\mathbf{n}!} |\mathbf{n}\rangle \langle \mathbf{n}|$$

- fluorescent single two-level quantum system (trapped atom, NV center, qudot..)

## and detection

photon: "click"	↔	quantum efficiency $\eta$
no photon: no "click"	↔	dark counts $P_D$
		afterpulses

- avalanche photo diodes

- $\lambda < 1\mu\text{m}$  (Si),  $< 1.3\mu\text{m}$  (Ge),  $< 1.6\mu\text{m}$  (InGaAs)
- $\eta = 10\text{-}60\%$ ,  $P_D = 10^{-5}\text{-}10^{-8}/\text{ns}$ , depending on type

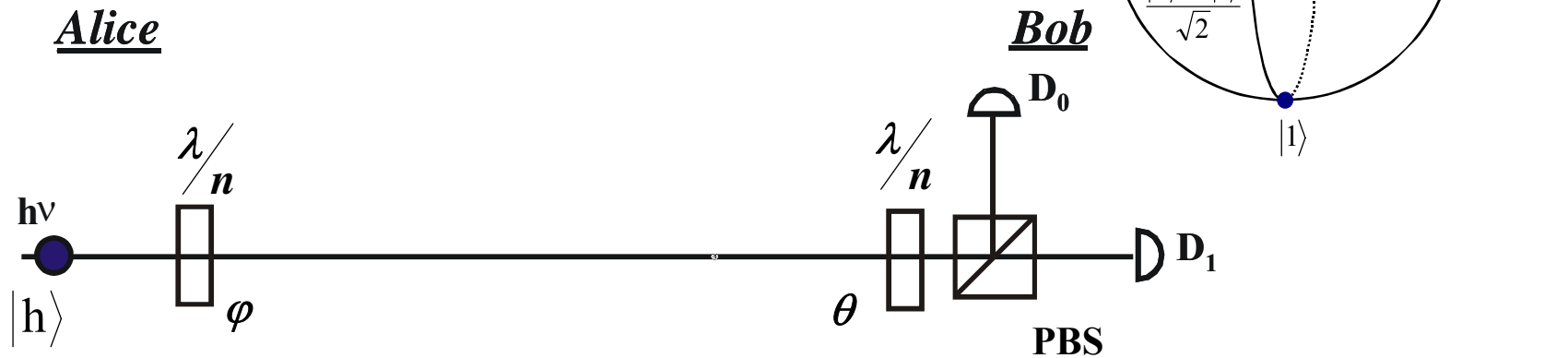
- superconducting single photon counters



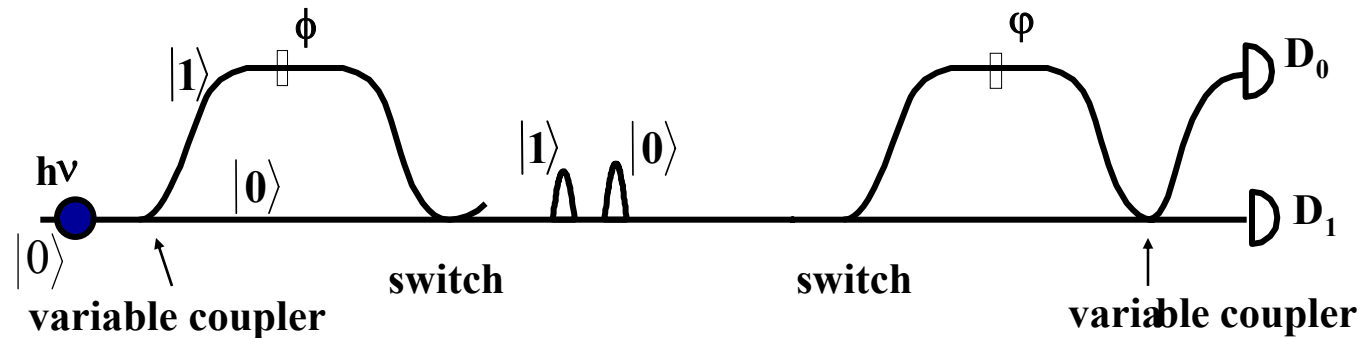
# preparation and measurement of qubits

$$\text{qubit : } |\psi\rangle = \alpha|0\rangle + \beta e^{i\phi}|1\rangle$$

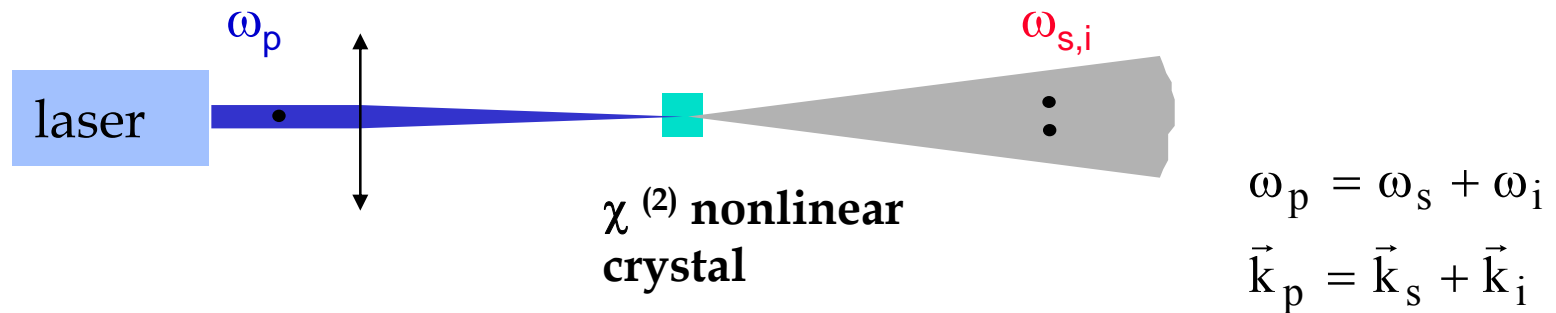
## polarization qubits



## time-bin qubits



# entangled pairs



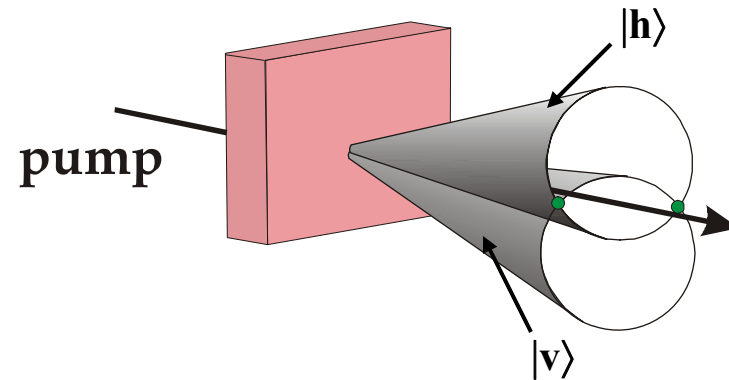
**wavelength, bandwidth, polarization and spatial modes  
depend on the specific crystal and on its orientation and  
temperature**

depending on the specific arrangement, the photons of a pair are entangled

- polarization entanglement
- energy-time entanglement
- time-bin entanglement

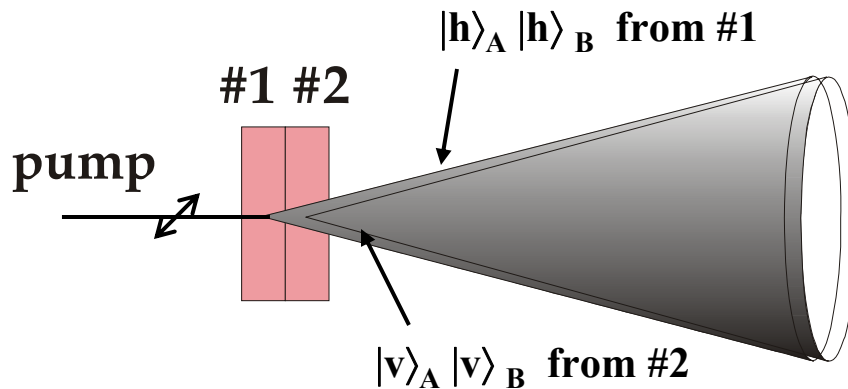


# entangled polarization qubits



$$|\psi\rangle_{AB} = [ |h\rangle_A |v\rangle_B + e^{i\phi} |v\rangle_A |h\rangle_B ] / \sqrt{2}$$

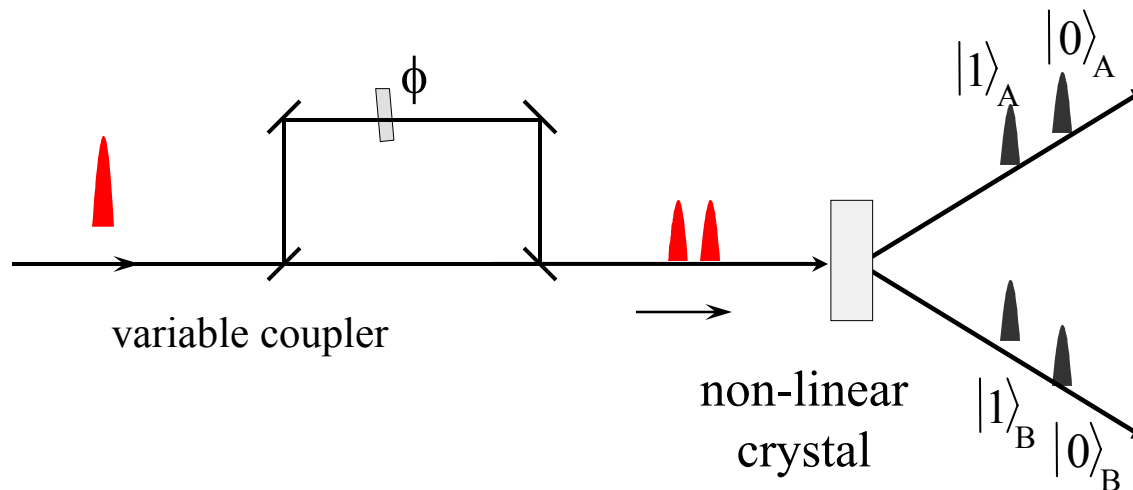
P. Kwiat *et al.*, Phys. Rev. Lett. **75**, 4337 (1995)



$$|\psi\rangle_{AB} = \alpha |h\rangle_A |h\rangle_B + \beta e^{i\phi} |v\rangle_A |v\rangle_B$$

P. Kwiat *et al.*, Phys. Rev. A **60**, R773 (1999)

# time-bin entanglement



$$\omega_p = \omega_s + \omega_i$$

$$\vec{k}_p = \vec{k}_s + \vec{k}_i$$

$$|\Phi\rangle = \alpha |0\rangle_A |0\rangle_B + \beta e^{i\phi} |1\rangle_A |1\rangle_B$$

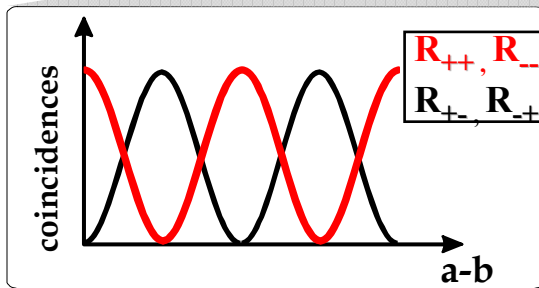
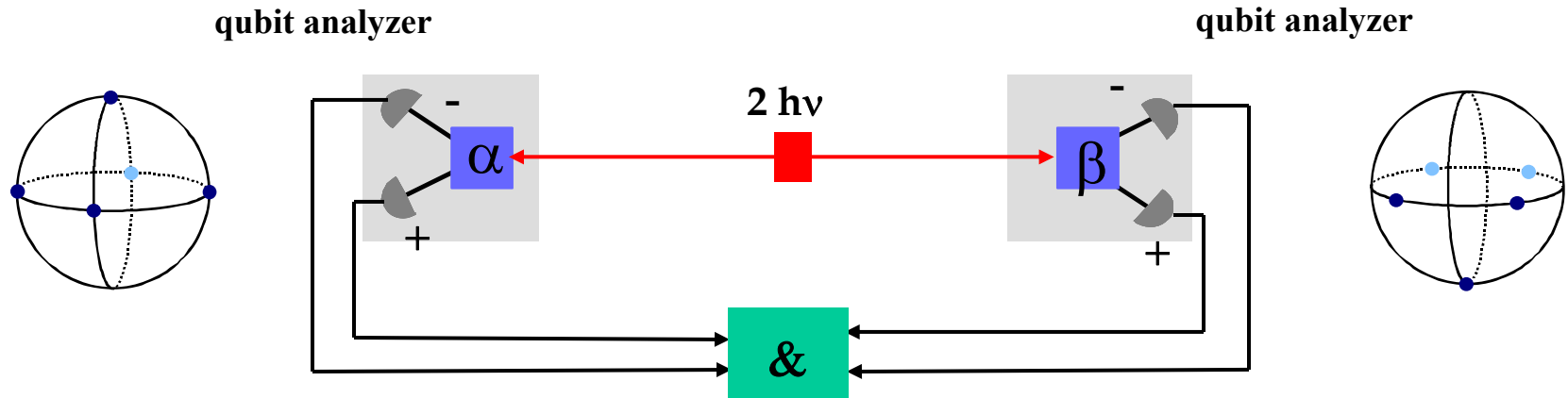
J. Brendel *et al.*, Phys.  
Rev. Lett. **82**, 2594 (1999)

- *maximally and non-maximally entangled states can be created,*  
**robust during transmission in optical fibers (10 km)**

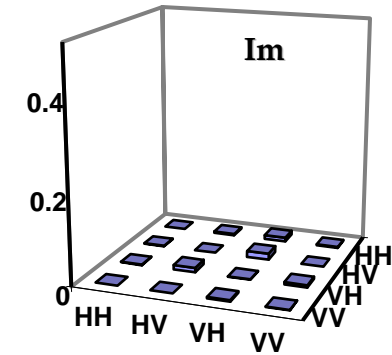
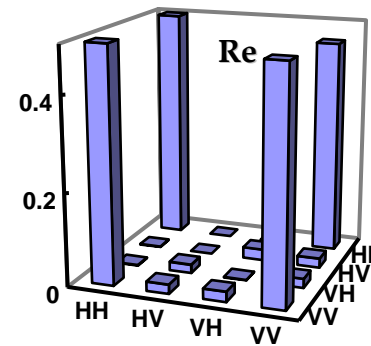
W. Tittel *et al.*, Phys.  
Rev. Lett **81**, 3563 (1998)  
R. Thew *et al.*, Phys. Rev.  
A **66**, 062304 (2002)
- **extension to entanglement in higher dimensions is possible**

H. de Riedmatten *et al.*,  
QIC **2**, 425 (2002)  
R. Thew *et al.*, quant-  
ph/0402048 & 0307122

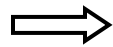
# measuring entanglement: correlation



$$|\phi^+\rangle = 2^{-1/2}[|h\rangle|h\rangle + |v\rangle|v\rangle]$$



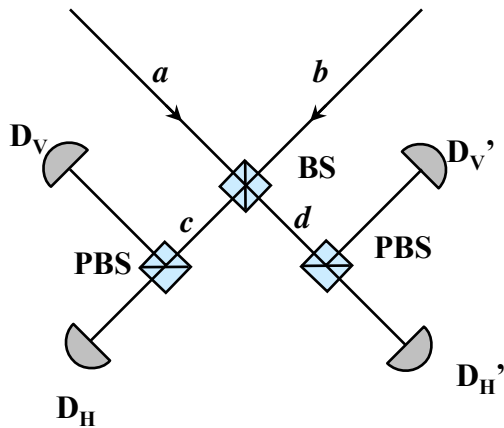
A.G. White *et al.*, PRL 83, 3103 (1999)



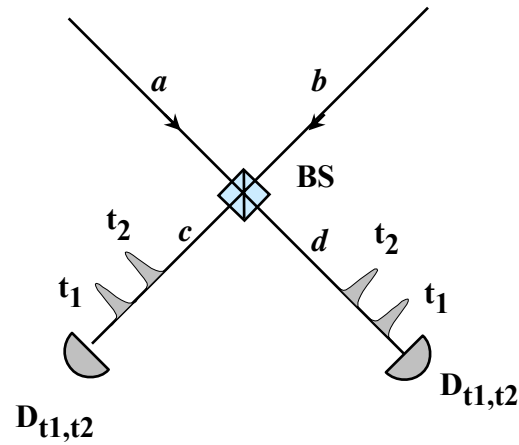
- fidelity of entanglement / non-locality
- reconstruction of density matrix

# interferometric Bell-state analyzer

## polarization qubits

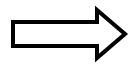


## time-bin qubits



$$|0\rangle_a |1\rangle_b \rightarrow (i|0\rangle_c + |0\rangle_d)(|1\rangle_c + i|1\rangle_d) = i|0\rangle_c |1\rangle_c - |0\rangle_c |1\rangle_d + |1\rangle_c |0\rangle_d + i|0\rangle_d |1\rangle_d$$

$$|1\rangle_a |0\rangle_b \rightarrow (i|1\rangle_c + |1\rangle_d)(|0\rangle_c + i|0\rangle_d) = i|0\rangle_c |1\rangle_c - |1\rangle_c |0\rangle_d + |0\rangle_c |1\rangle_d + i|0\rangle_d |1\rangle_d$$



$$|\psi^-\rangle = |0\rangle_a |1\rangle_b - |1\rangle_a |0\rangle_b \rightarrow -|0\rangle_c |1\rangle_d + |1\rangle_c |0\rangle_d$$

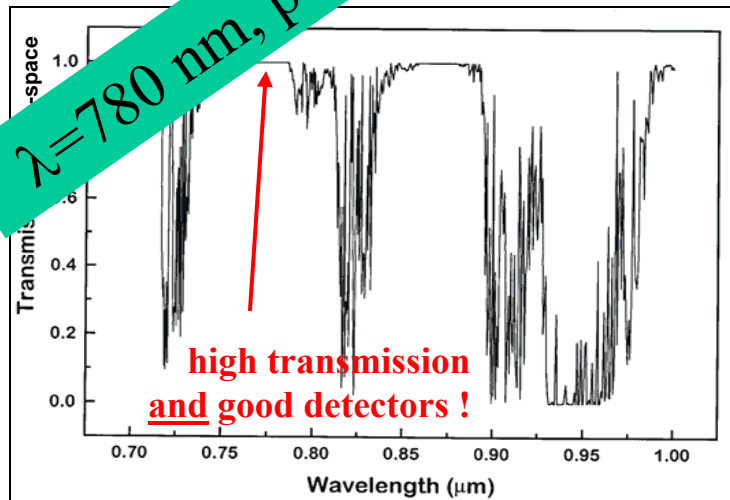
$$|\psi^+\rangle = |0\rangle_a |1\rangle_b + |1\rangle_a |0\rangle_b \rightarrow i|0\rangle_c |1\rangle_c + i|0\rangle_d |1\rangle_d$$

**Bell state measurement only 50 % efficient (lin. optics)**

# quantum channel

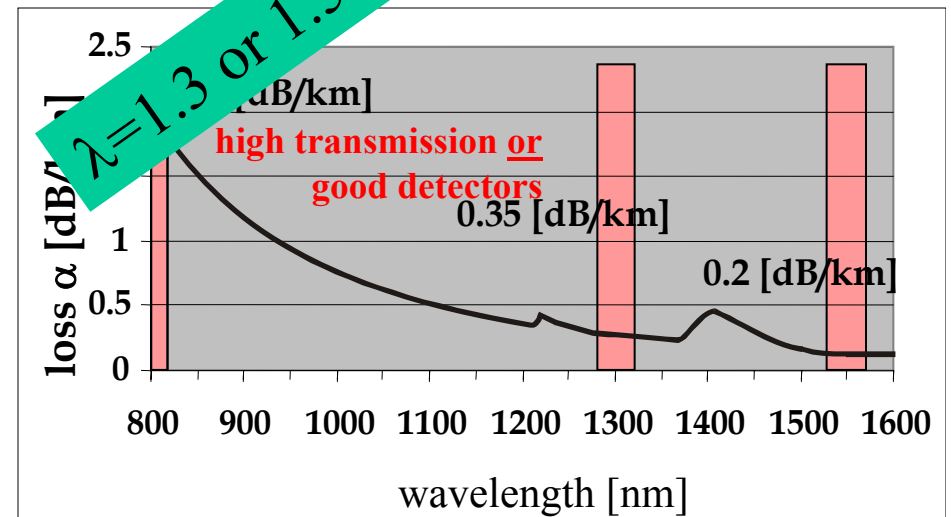
## free-space links

- transmission
  - absorption (obstacles, weather)
  - diffraction
  - atmospheric turbulence
  - ultra-long distance links?
- stray light (moon)
- negligible dispersion



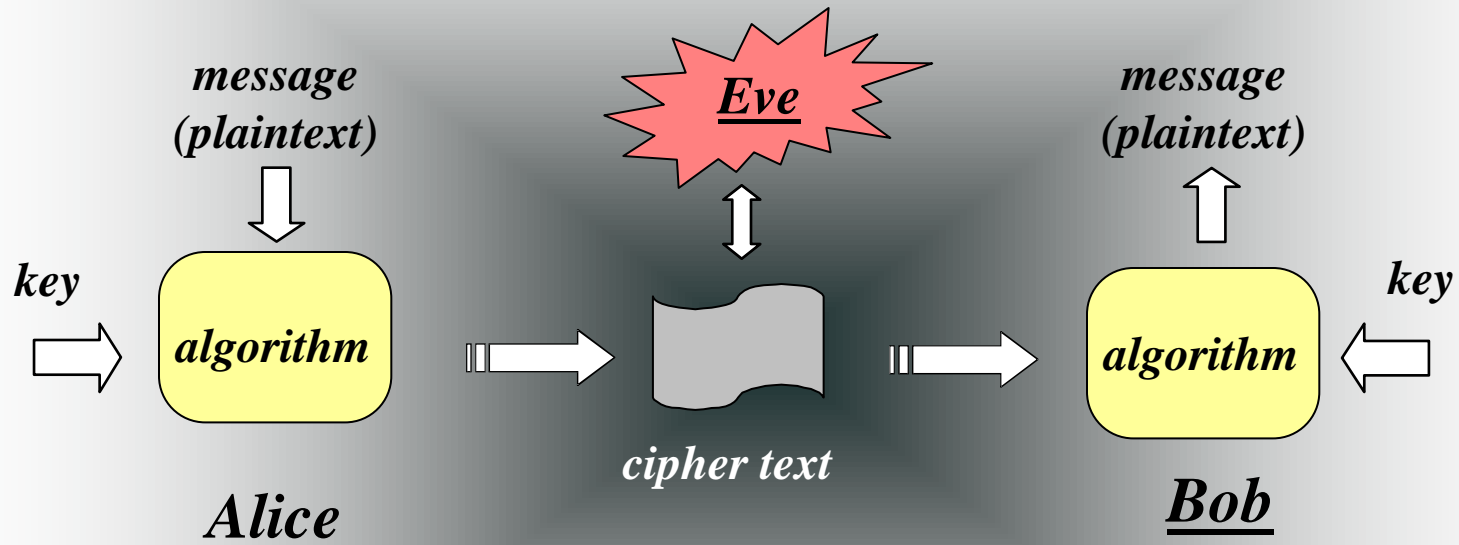
## optical fibers

- transmission (absorption)
- CD, polarization effects
- modern telecommunication fiber network already exists



# cryptology

cryptology: the science to hide the meaning of a message



cryptoanalysis: the science to unscramble a message without knowing the key

*Only the one-time pad has been proven to be secure !*

# proven security: the one-time pad

<u>Alice</u>								
message	0	1	1	0	1	0	0	1
key	1	0	0	1	1	0	1	0
sum (modulo 2) = cipher text	1	1	1	1	0	0	1	1

transmission ↓

<u>Bob</u>								
cipher text	1	1	1	1	0	0	1	1
key	1	0	0	1	1	0	1	0
sum (modulo 2) = message	0	1	1	0	1	0	0	1

the one time pad has been proven to be secure if

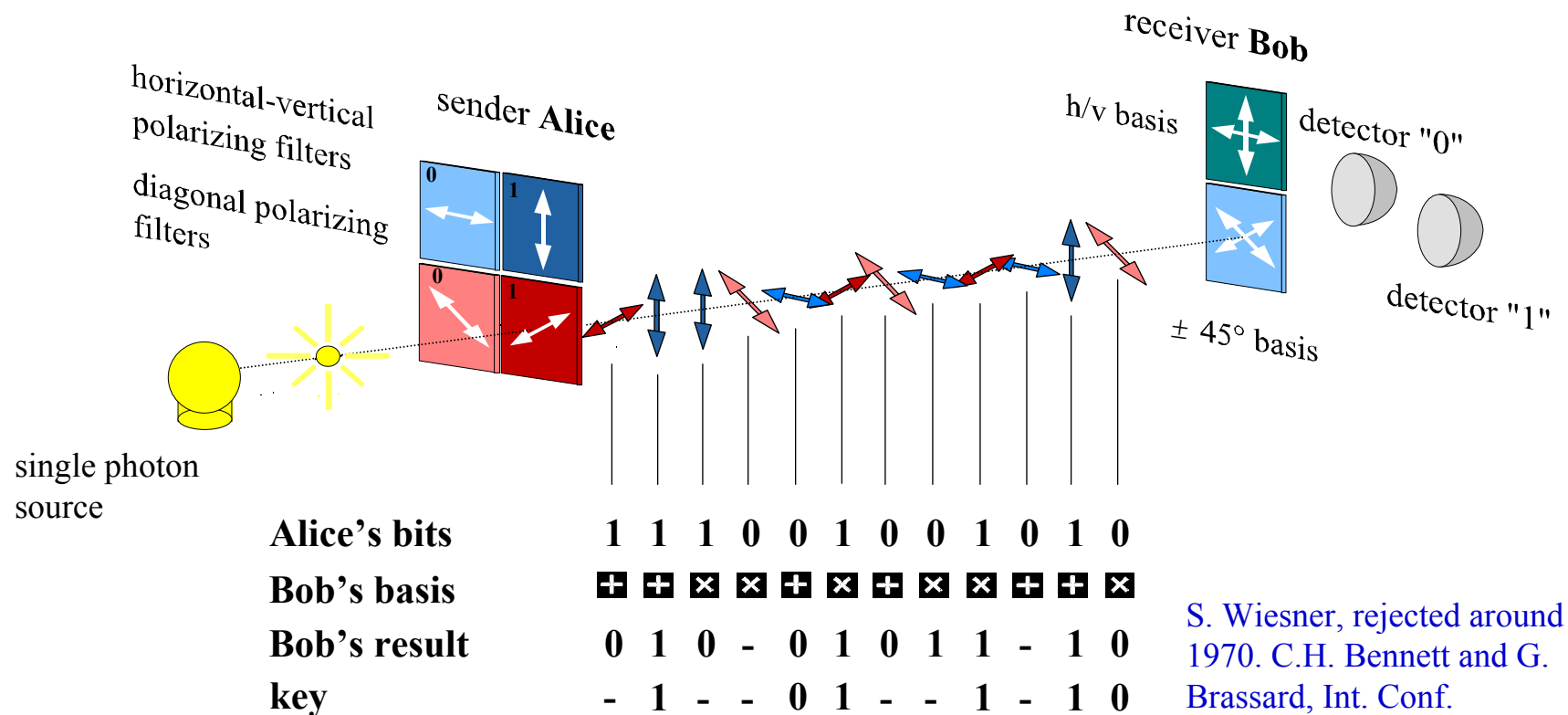
- ✓ key is as long as message and used only once
- ✓ key is random
- ✓ key is only known to Alice and Bob

**Problems: randomness, key distribution**

G. Vernam, J. Am. Institute of Electrical Engineers Vol. XLV, 109 (1926)

C.E. Shannon, Bell System Technical Journal 28, 656 (1949)

# the "BB84" protocol



S. Wiesner, rejected around 1970. C.H. Bennett and G. Brassard, Int. Conf. Computers, Systems & Signal Processing, Bangalore, India, Dec. 10-12, 1984

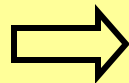
- basis reconciliation (key sifting) → identical bits
- measurement (cloning) perturbs the system (QBER<sub>intercept resend</sub> = 25%)  
→ eavesdropper gains information but introduces errors

**use confidential key, discard unsecure key**



# the "BB84" protocol

- quantum cryptography is not a new coding method
- it allows to create a **secret key**, based on the **laws of quantum physics**
- it provides the one-time pad with the required secret key



**quantum key distribution**

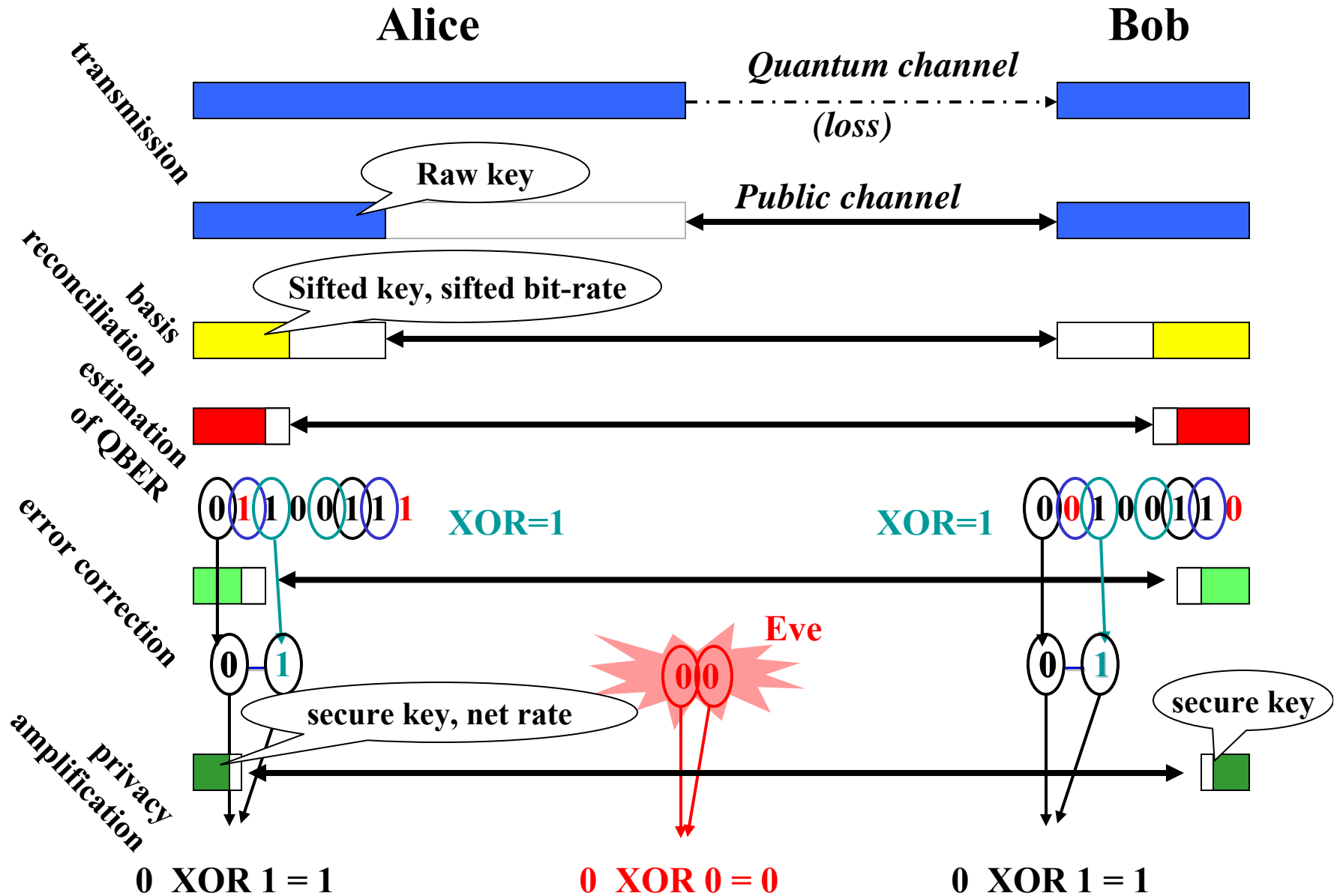
sing  
sour



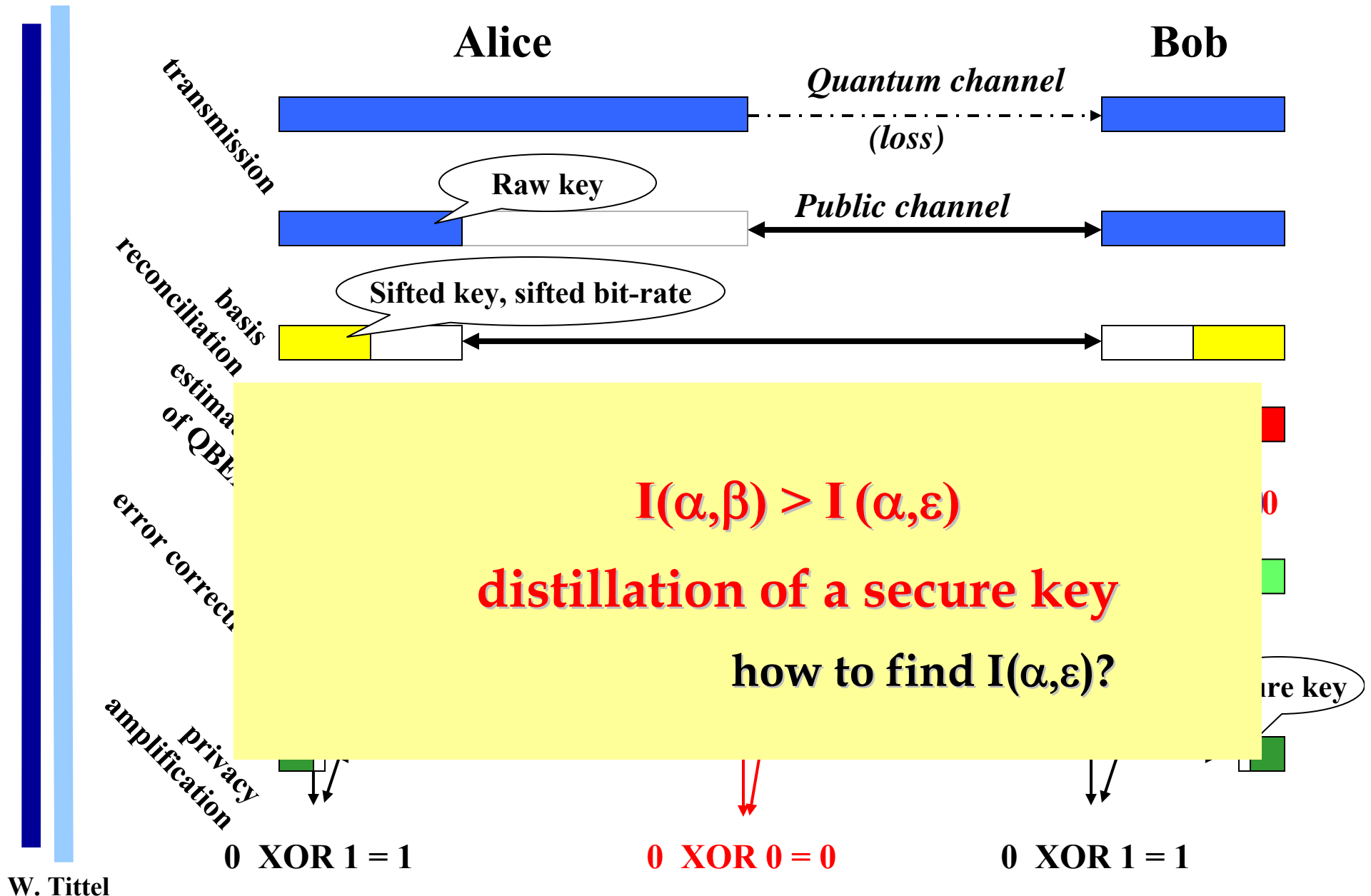
eavesdropper gains information but introduces errors

**use confidential key, discard unsecure key**

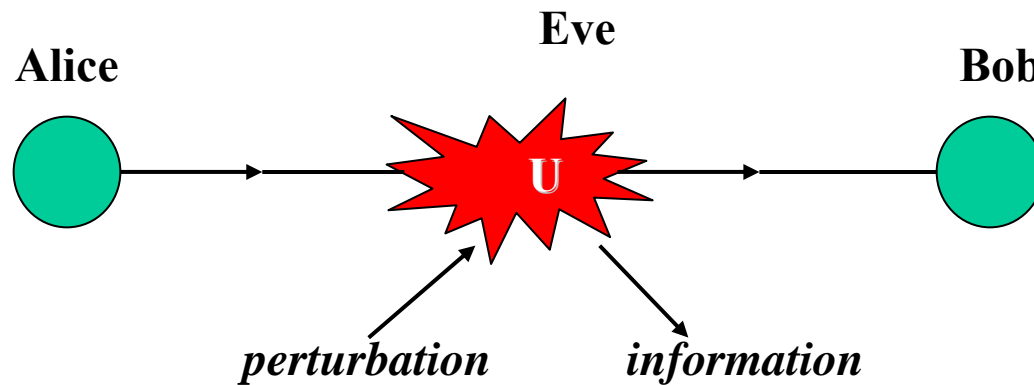
# from raw to net key



# from raw to net key



# eavesdropping



- incoherent attacks : Eve attaches independent probes to each qubit and measures them individually after basis reconciliation
- coherent attacks : process several (all) probes coherently after privacy amplification

**It is still unknown if infinite attacks are more efficient than finite attacks or than individual attacks!**

# eavesdropping and BB'84

$$R_{\text{secret}} = R_{\text{sifted}} [I(\alpha, \beta) - \text{Min} \{I(\alpha, \epsilon), I(\beta, \epsilon)\}]$$

$$I(\alpha, \beta) = 1 - H_2(\text{QBER})$$

(Shannon Information)

$$H_2(x) = -x \log_2(x) - (1-x) \log_2(1-x)$$

(binary entropy function)

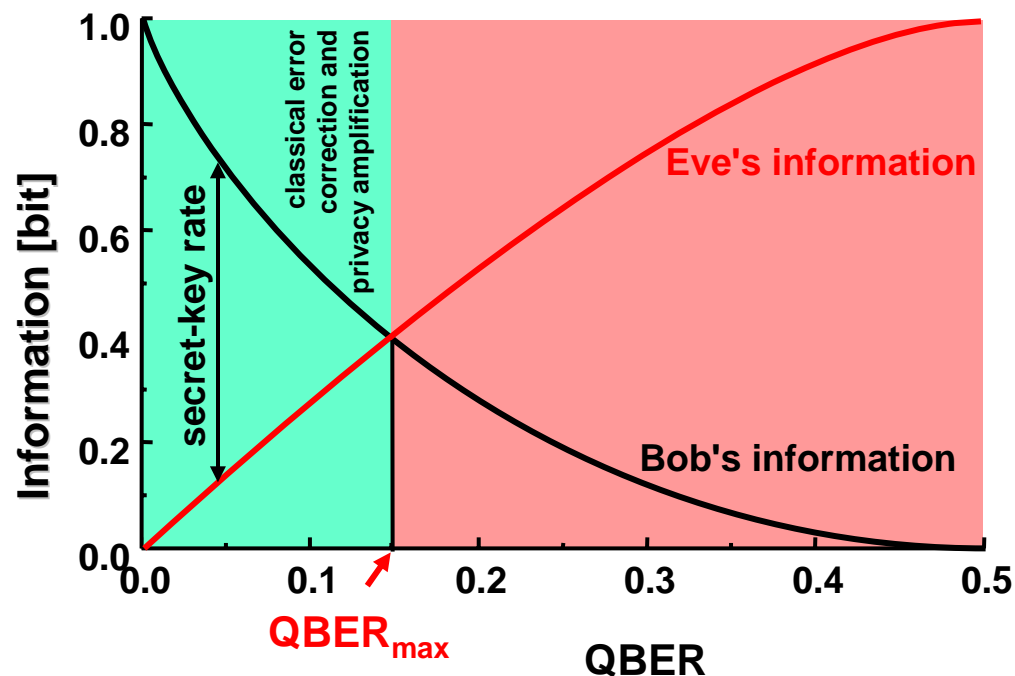
- individual, symmetric attacks  
(conditional security)

$$I(\alpha, \epsilon) \approx \frac{2}{\ln 2} \text{QBER} + O(\text{QBER}^2)$$

$$\approx 2.9 \text{ QBER}$$

$$\Rightarrow \text{QBER}^{\text{max}} = \frac{1}{2} (1 - 1/\sqrt{2})$$

$$\approx 15\%$$



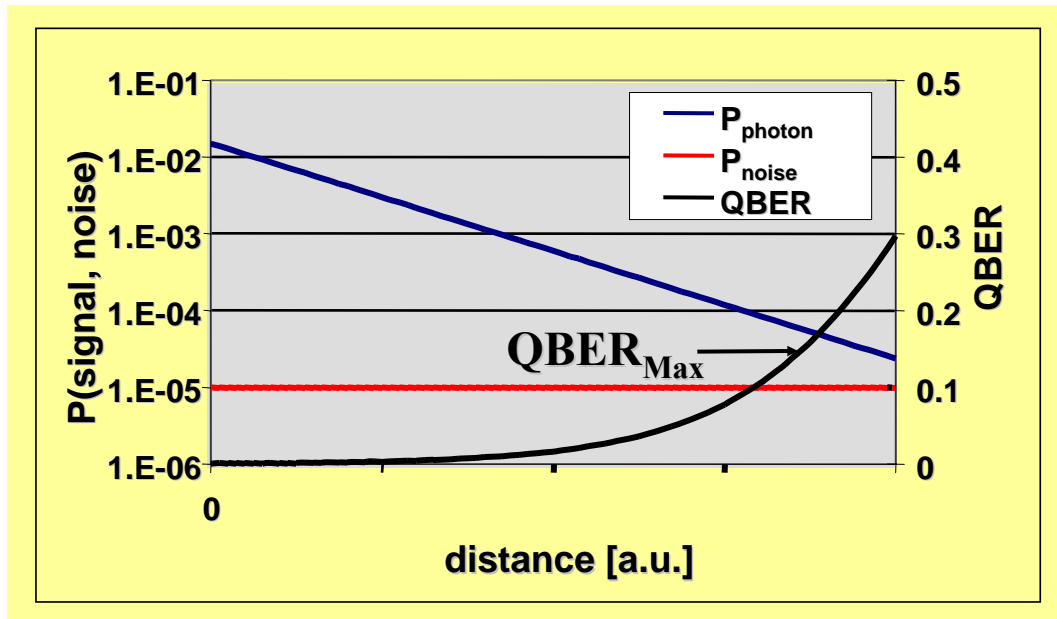
- coherent attacks (information  
theoretical security)

$$R_{\text{secret}} \geq R_{\text{sifted}} [1 - H_2(\text{QBER}) - H_2(\text{QBER})]$$

$$\Rightarrow \text{QBER}^{\text{max}} \approx 11\%$$

privacy amplification

# secret bit-rate and distance

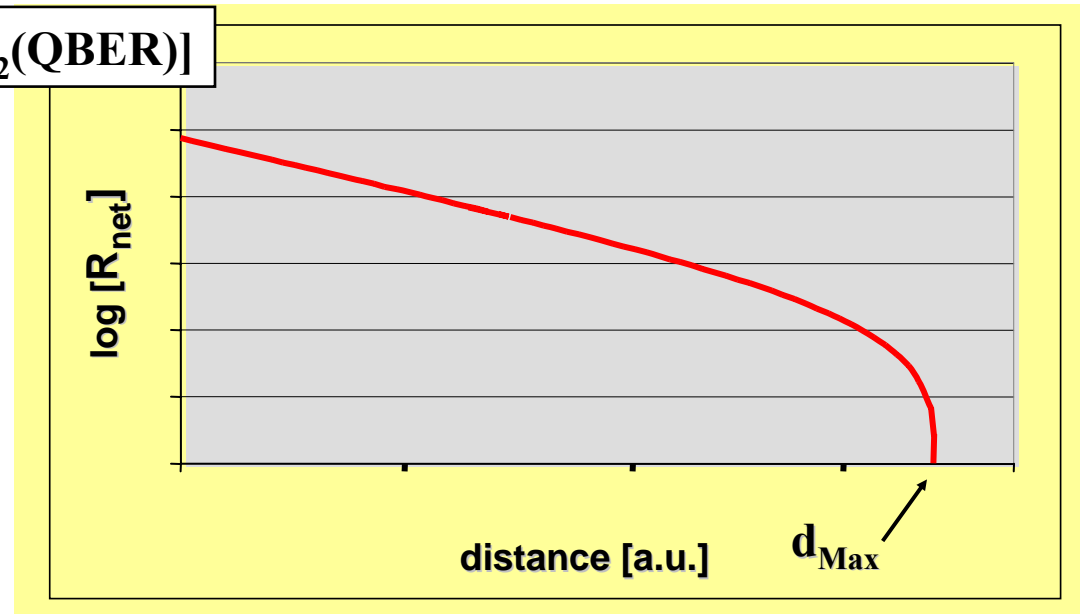


$$\text{QBER} = \frac{\text{wrong events}}{\text{all events}}$$

$$\approx \frac{P_{\text{noise}}}{2(P_{\text{photon}} + P_{\text{noise}})}$$

$$P_{\text{photon}} = \mu \eta e^{-\alpha l/10}$$

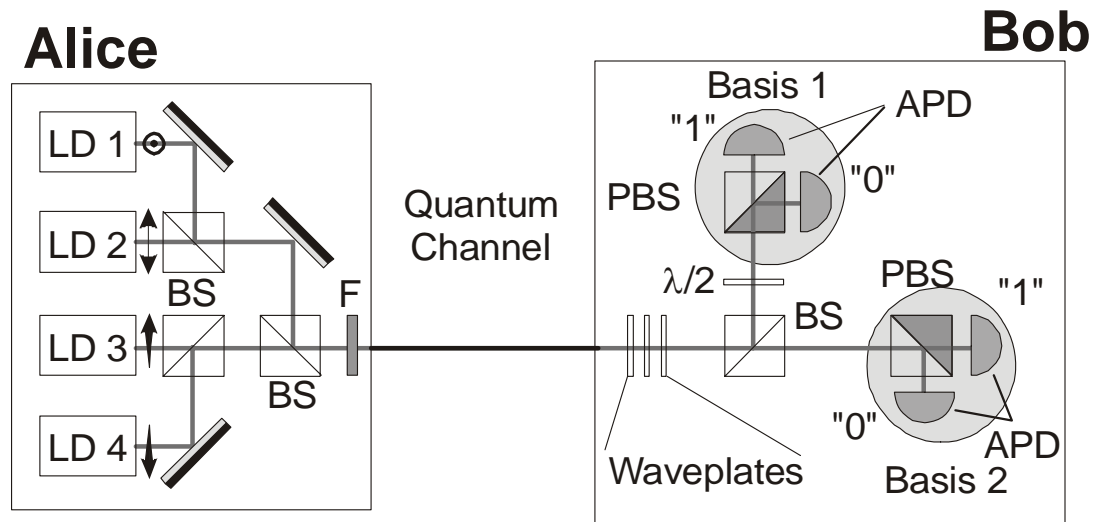
$$R_{\text{secret}} \geq R_{\text{sifted}} [1 - H_2(\text{QBER}) - H_2(\text{QBER})]$$



# QKD with *weak pulses*

1984	idea	C.H. Bennett and G. Brassard, Int. Conf. Computers, Systems & Signal Processing, Bangalore, India, Dec. 10-12, 175 (1984)
1989/1992	first lab demonstration, 30 cm in air	C.H. Bennett <i>et al.</i> , J. Cryptology <b>5</b> , 3 (1992)
1995	first proof of principle demonstration over 23 km (fiber)	A. Muller <i>et al.</i> , Nature <b>378</b> , 449 (1995)
since then	several prototypes, working at distances > 20 km (fiber)	
1998	> 1km free space	N. Gisin <i>et al.</i> , Rev. Mod. Phys. <b>74</b> , 145 (2002)
2002	67 km fiber	D. Stucki <i>et al.</i> New J. Phys. <b>4</b> , 41.1 (2002)
	10 km and 23 km free space	R. Hughes <i>et al.</i> New J. Phys <b>4</b> , 43.1 (2002) C. Kurtsiefer <i>et al.</i> , Nature <b>419</b> , 450 (2002)
	single photons	A. Beveratos <i>et al.</i> , Phys. Rev. Lett. <b>89</b> , 187901 (2002) E. Waks, <i>et al.</i> , Nature <b>420</b> , 762 (2002)
2003	> 100 km fiber	H. Kosaka <i>et al.</i> , Electr. Lett . <b>39</b> , 1199 (2003) C. Gobby <i>et al.</i> , Appl. Phys. Lett <b>84</b> , 3762 (2004)
2005	decoy state QKD	Y. Zhao <i>et al.</i> , Phys. Rev. Lett. <b>96</b> , 070502 (2006)

# free-space QKD over 23 km

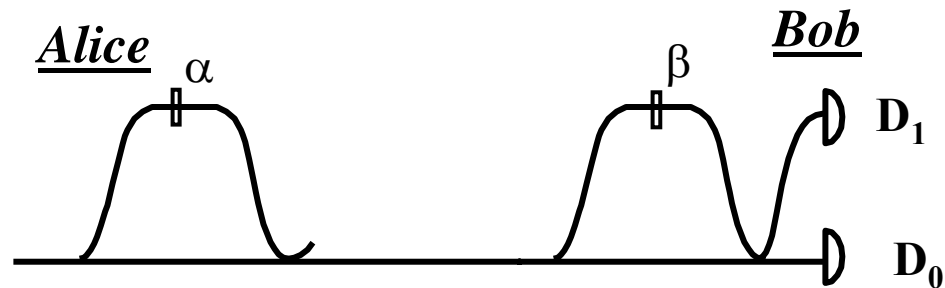


$$\mu=0.1$$

$$\text{QBER (night)} < 5\%$$

$$R_{\text{net}}=500 \text{ Hz}$$

# the double Mach-Zehnder interferometer

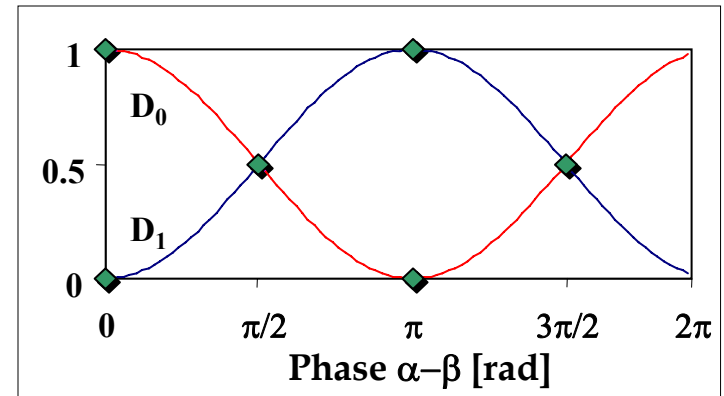
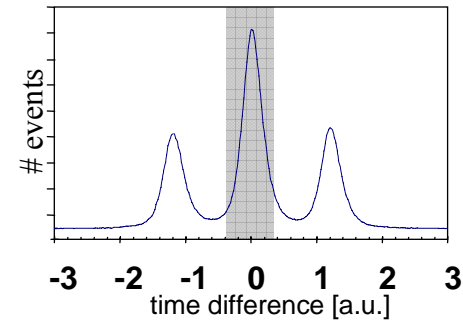


Basis 1:  $\alpha = 0; \pi$

Basis 2:  $\alpha = \pi/2; 3\pi/2$

Basis 1:  $\beta = 0$

Basis 2:  $\beta = \pi/2$



## Basis reconciliation

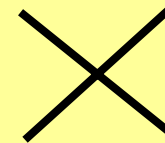
compatible bases ( $\alpha - \beta = n\pi$ )

$\Rightarrow$  Alice knows  $\alpha, \beta$

$\Rightarrow D_i$

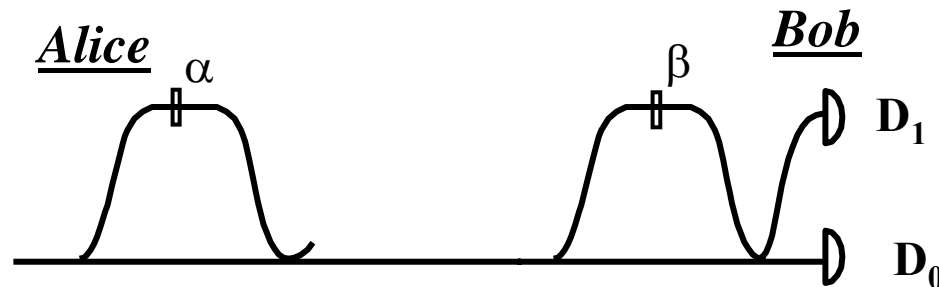
$\Rightarrow$  identical Bit

incompatible bases ( $\alpha - \beta = \pm \pi/2$ )





# the double Mach-Zehnder interferometer

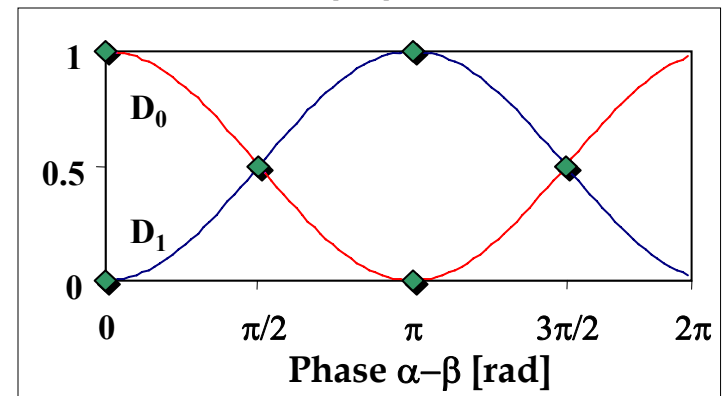
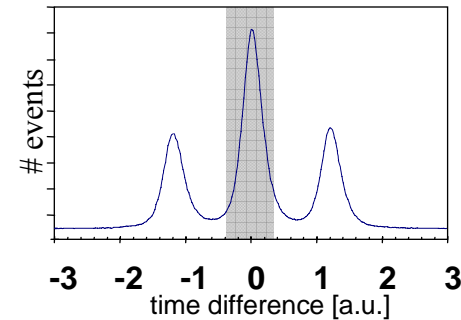


Basis 1:  $\alpha = 0; \pi$

Basis 2:  $\alpha = \pi/2; 3\pi/2$

Basis 1:  $\beta = 0$

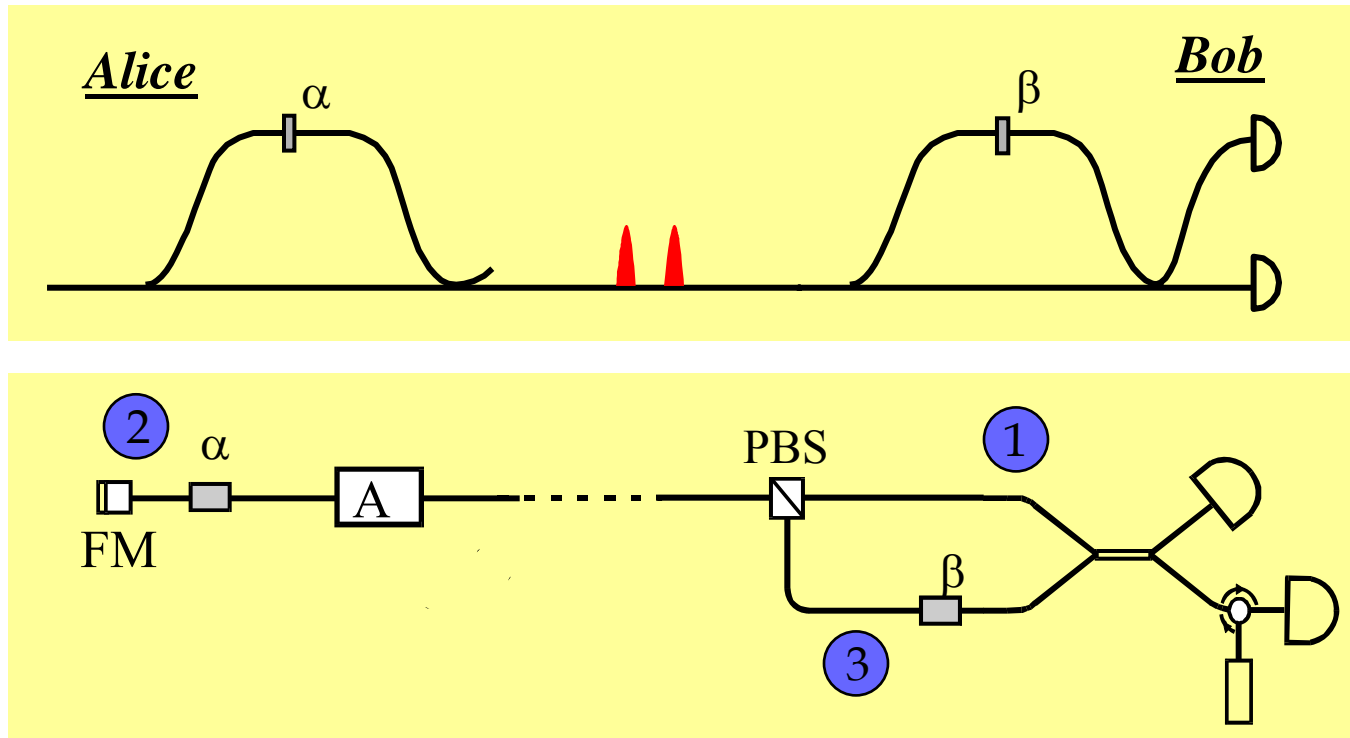
Basis 2:  $\beta = \pi/2$



- ❑ developed by DERA and British Telecom (1993), LANL (1996)
- ❑ requires stabilization of interferometers (phase, polarization)
- ❑ PBS to suppress side peaks, or polarization dependent phase modulators  $\implies$  polarization control between A and B



# "Plug&Play" quantum cryptography

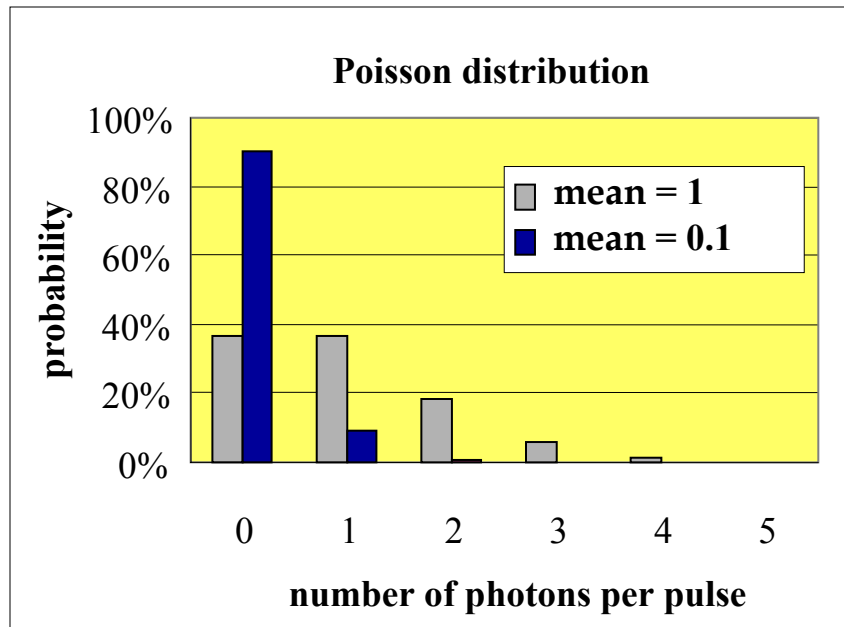


- ❑ developed by GAP (1997, 1998), IBM, KTH Stockholm, Aarhus, ..
- ❑ automatic path-length adjustment
- ❑ Faraday mirrors compensate for polarization effects

H. Zbinden *et al.*, *Electr. Lett* **33**, 586 (1997)  
G. Ribordy *et al.*, *Electr. Lett* **34**, 2116 (1998)

⇒ outstanding stability ( $V = 99.8\%$ ) !

# what is "wrong" with faint pulses?

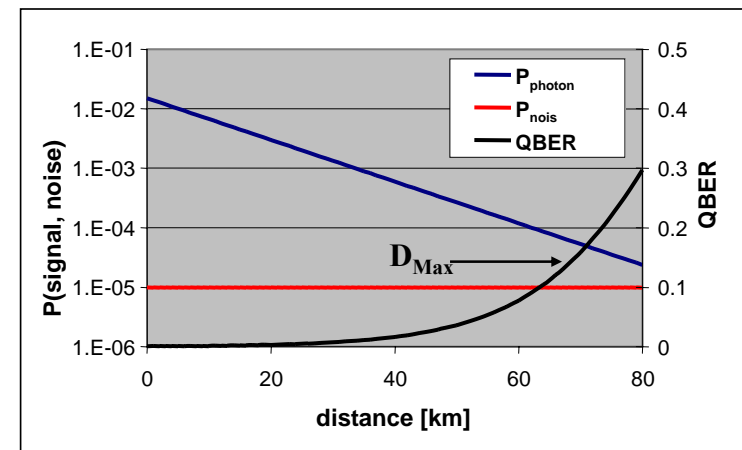


$$P(n, \mu) = \frac{\mu^n}{n!} e^{-\mu}$$

Alice sometimes sends **more than one photon** (identically prepared)

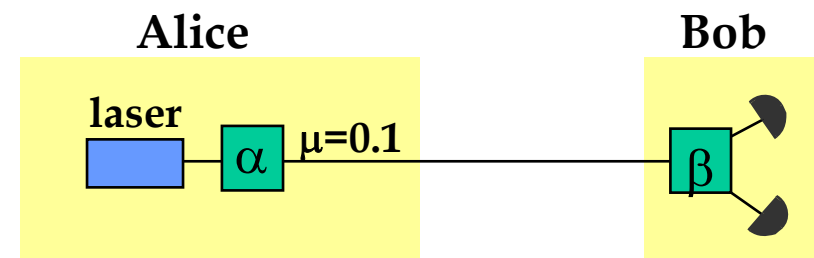
→ possibility of unidentified eavesdropping

Alice often sends **no photon**  
→ reduced bit rate and distance

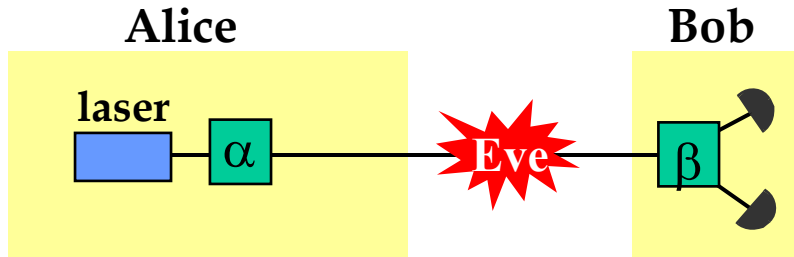


$$\text{QBER} = \frac{\text{wrong events}}{\text{all events}} \approx \frac{P_{\text{noise}} / 2}{P_{\text{photon}} + P_{\text{noise}}}$$

$$P_{\text{photon}} = \mu \eta e^{-\alpha l / 10}$$



# photon-number splitting attacks



$$\rho = \sum_n p(n, \mu) |n\rangle\langle n|$$

$$P(n, \mu) = \frac{\mu^n}{n!} e^{-\mu}$$

$$R_{raw} = f \sum_{n=1}^{\infty} P_n \left( 1 - (1 - \eta t)^n \right)$$

$$\approx f \mu e^{-\mu} \eta t \quad (n=1)$$

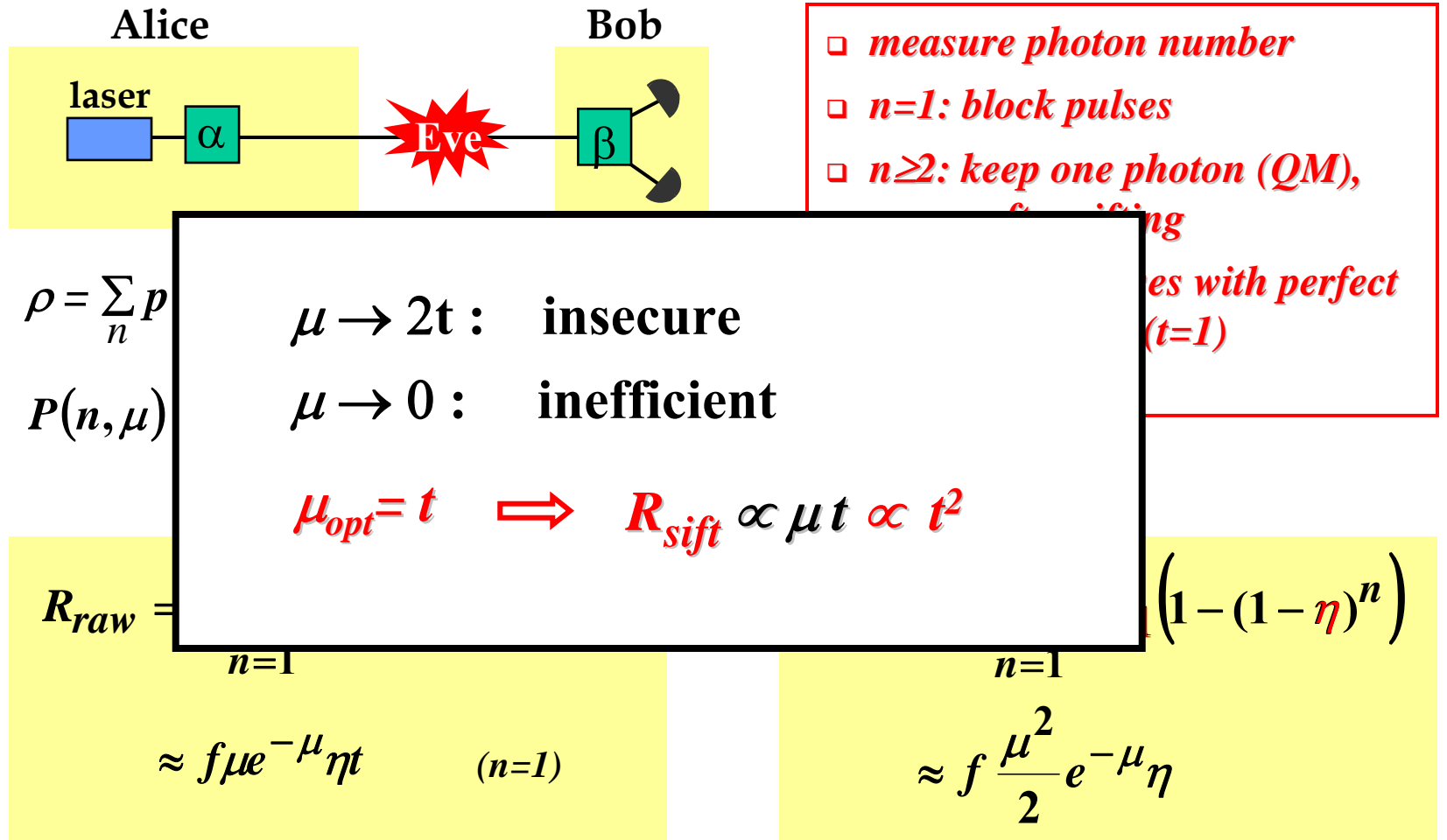
$$R_{raw}' = f \sum_{n=1}^{\infty} P_{n+1} \left( 1 - (1 - \eta)^n \right)$$

$$\approx f \frac{\mu^2}{2} e^{-\mu} \eta$$

$$R_{raw} = R_{raw}' \quad \Rightarrow \quad t = \mu / 2$$

- ❑ *measure photon number*
- ❑ *n=1: block pulses*
- ❑ *n≥2: keep one photon (QM), measure after sifting*
- ❑ *compensate losses with perfect quantum channel (t=1)*  
→ *same rate*

# photon-number splitting attacks





# Improving the key-rate: measures against PNS attacks

- **new protocols**

  - **non-orthogonal states**

Scarani, PRL 2004; Acin, PRA 2004

  - **decoy states**

Hwang, PRL 2003; Lo, PRL 2005

Wang, PRL 2005

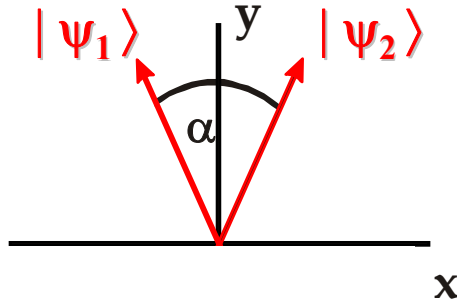
- **quantum cryptography based on entanglement**

A. Ekert, PRL 1991

- **true single-photon sources**

Beveratos, PRL 2002; Waks, Nature 2002

# unambiguous discrimination of non-orthogonal states



$$|\langle \psi_1 | \psi_2 \rangle| = \cos \alpha \neq 0$$

van Neumann measurement

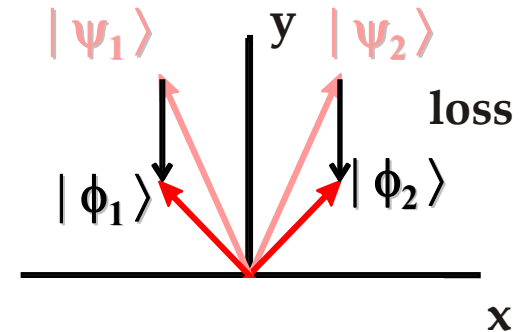
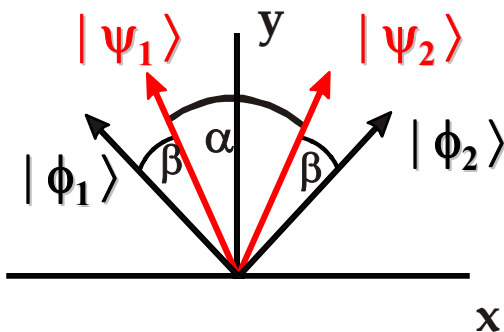
$\Rightarrow$  conclusive results but sometimes incorrect

$$P_e = |\langle \psi_1 | \phi_2 \rangle|^2 = \frac{1}{2} [1 - \sin \alpha]$$

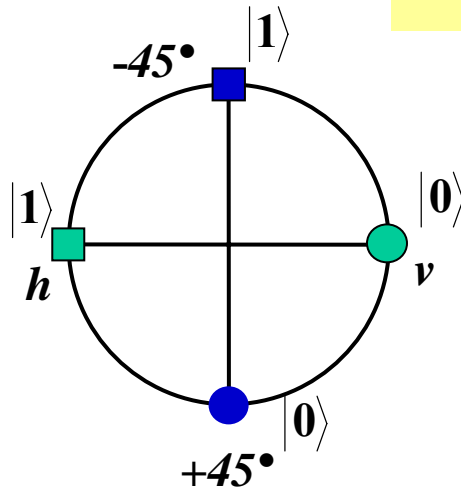
generalized measurement

$\Rightarrow$  not always conclusive but then unambiguous

$$P_? = \cos \alpha$$



## BB84



✓ Alice chooses a **bit value** and a **basis**

✓ Bob chooses a basis

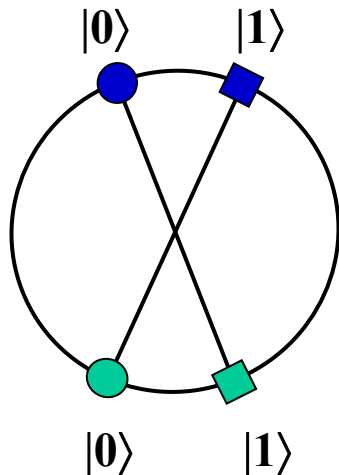
✓ whenever they use the same basis, Bob knows **with certainty** what state has been prepared by Alice

⇒ identical bit values



Eve has full information whenever she keeps a photon

## SARG04



✓ Alice chooses a **bit value** and a **set**

✓ Bob chooses a set

✓ whenever they use the same set, Bob knows **for a fraction  $f=1-\cos \alpha$  with certainty** what state has been prepared by Alice ( $\langle 0|1 \rangle = \cos \alpha \neq 0$ )

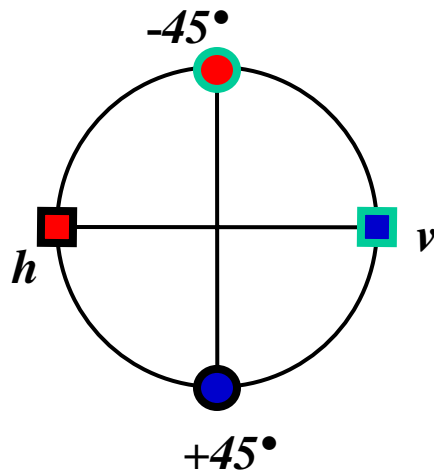
⇒ identical bit values, reduced bit rate  $R'=fR$



Eve has partial information whenever she keeps a photon

# SARG with BB84 settings

Set 1:  $v, +45^\circ$  Set 2:  $v, -45^\circ$  Set 3:  $h, -45^\circ$  Set 4:  $h, +45^\circ$



*orthogonal states encode same classical bit!*

Alice chooses a bit value, e.g. "0"= $h$   
and announces a set, e.g. **set 3:  $h, -45^\circ$** ,

Bob's basis	$h/v$	$\pm 45^\circ$
Bob's result	$h$ $\times$	$+45^\circ$ $-45^\circ$
Bob's knowledge about the state	? $\times$	$h$ ?

Bob knows the state (the bit) whenever

he measures in the basis the photon has not been prepared in

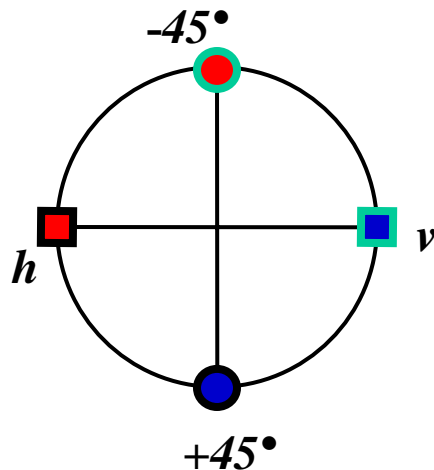
he gets a result that is not element of the set announced

$\Rightarrow$  **sifted key =  $\frac{1}{4}$  raw key**

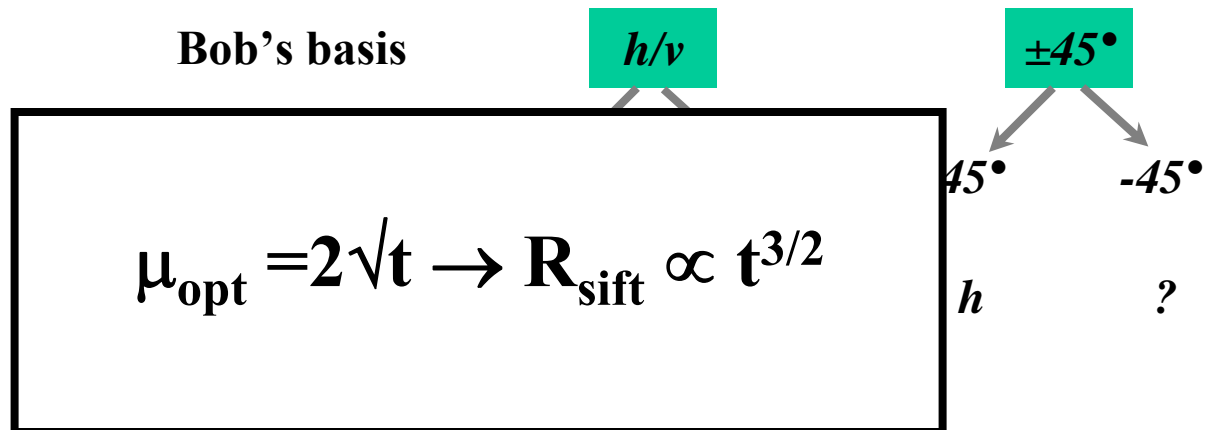
# SARG with BB84 settings

Set 1:  $v, +45^\circ$  Set 2:  $v, -45^\circ$  Set 3:  $h, -45^\circ$  Set 4:  $h, +45^\circ$

Alice chooses a bit value, e.g. "0"= $h$   
and announces a set, e.g. set 3:  $h, -45^\circ$ ,



*orthogonal states encode same classical bit!*



Bob knows the state (the bit) whenever

he measures in the basis the photon has not been prepared in

he gets a result that is not element of the set announced

$\Rightarrow$  sifted key =  $\frac{1}{4}$  raw key

# Decoy-state QKD

only single-photon pulses emitted by Alice are secure

$$R \geq \underbrace{Q_1}_{\text{error correction}} \left\{ -Q_\mu H_2(E_\mu) + Q_1 [1 - H_2(e_1)] \right\}$$

**privacy amplification**

$$Q_\mu = \sum Q_i = \sum Y_i P_i = \sum Y_i \frac{\mu^i e^{-\mu}}{i!}$$

$$E_\mu Q_\mu = \sum e_i Q_i = \sum e_i Y_i P_i$$

$Q_i$  : gain - probability that  $i$ -photon state is created and leads to a detection

$Y_i$  : yield - probability that  $i$ -photon state leads to a detection:  $Y_i = 1 - (1 - \eta)^i$

$e_i$  : error rate caused by a  $i$ -photon state

$\eta$  : single photon detection probability (incl. transmission)

**Problem:**  $Q_1, e_1$  can not be extracted from  $Q_\mu, E_\mu$

**Solution:** Decoy-state QKD

# Decoy-state QKD

$$R \geq q \{ -Q_\mu H_2(E_\mu) + P_1(\mu) Y_1 [1 - H_2(e_1)] \}$$

signal states: mean photon number  $\mu$



*Random choice*

$$Q_\mu = \sum Y_i P_i(\mu)$$

$$E_\mu Q_\mu = \sum e_i Y_i P_i$$

decoy states: mean photon number  $v_i$



Eve can only measure photon number in a pulse

→ can not distinguish decoy from signal states, hence does not know the class the detected pulse belongs to

$$\rightarrow e_i^\mu = e_i^{v_1} = e_i^{v_2} = \dots = e_i^{v_n} = e_i$$

$$Y_i^\mu = Y_i^{v_1} = Y_i^{v_2} = \dots = Y_i^{v_n} = Y_i$$

$$Q_{v_1} = \sum Y_i P_i(v_1)$$

$$E_{v_1} Q_{v_1} = \sum e_i Y_i P_i(v_1)$$

⋮

⋮

$$Q_{v_n} = \sum Y_i P_i(v_n)$$

$$E_{v_n} Q_{v_n} = \sum e_i Y_i P_i(v_n)$$

allows determination of  $Y_i, e_i$  for  $n \rightarrow \infty$

great, but not practical

# Decoy state QKD

$$R \geq q \{ -Q_\mu H_2(E_\mu) + P_1(\mu) Y_1 [1 - H_2(e_1)] \}$$

Only a few decoy states are needed to derive a good lower bound on  $Y_1$  and upper bound on  $e_1$ , e.g. one decoy state, ( $v \approx 0.1$ ) and one vacuum state!

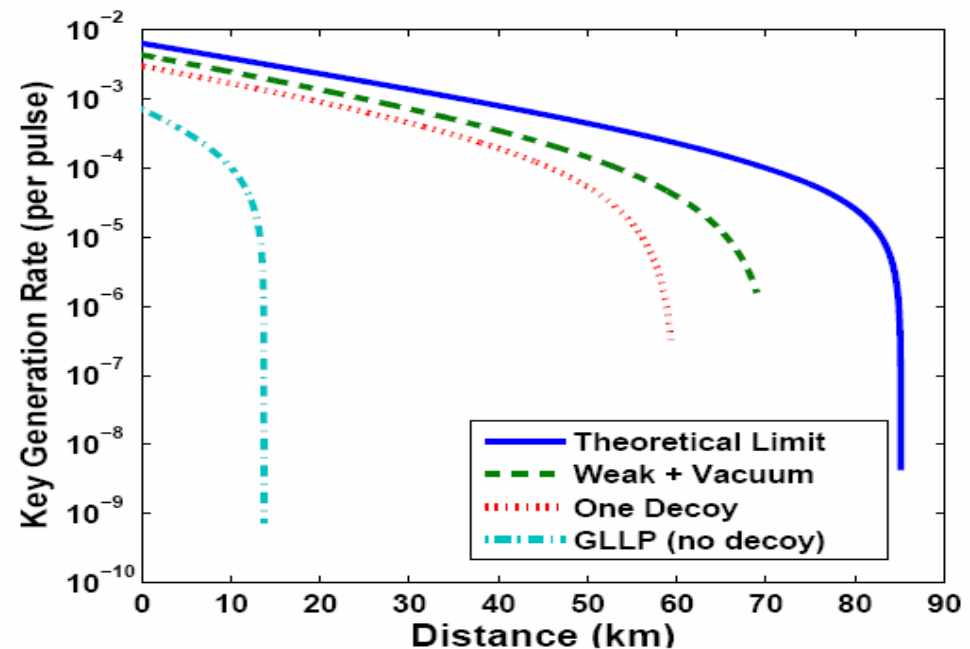
$$(1-\mu) e^{-\mu} = \frac{H_2(e_{\text{optic.}})}{1-H_2(e_{\text{optic.}})} \quad \rightarrow \mu_{\text{opt}} \approx 0.5$$

$$Y_1^{v,0} = \frac{\mu}{\mu v - v^2} (Q_v e^v - Q_\mu e^\mu \frac{v^2}{\mu^2} - \frac{\mu^2 - v^2}{\mu^2} Y_0)$$

$$e_1^{v,0} = \frac{E_v Q_v e^v - e_0 Y_0}{Y_1^{v,0} v}$$

$Y_0$ : dark count probability  $\approx 10^{-5}$

$e_0$ : error probability of dark count =  $1/2$



# Decoy state QKD

$$R \geq q \{ -Q_\mu H_2(E_\mu) + P_1(\mu) Y_1 [1 - H_2(e_1)] \}$$

Only a few decoy states are needed to derive a good lower bound on  $Y_1$  and upper bound on  $e_1$ , e.g. one decoy state, ( $v \approx 0.1$ ) and one vacuum state!

$$(1-\mu) e^{-\mu} = \frac{H_2(e_{\text{optic.}})}{1-H_2(e_{\text{optic.}})} \quad \rightarrow \mu_{\text{opt}} \approx 0.5$$

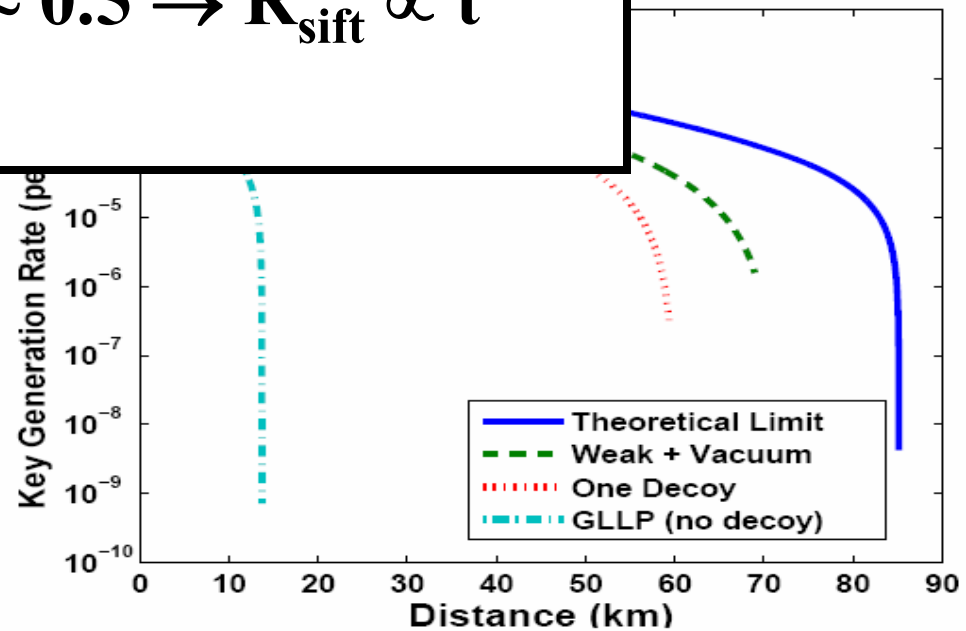
$Y_0$ : dark count probability  $\approx 10^{-5}$

$$Y_1^{v,0} = \frac{\mu}{\mu v - v^2} (Q_v - Y_0)$$

$$e_1^{v,0} = \frac{E_v Q_v e^v - Y_0}{Y_1}$$

$$\mu_{\text{opt}} \approx 0.5 \rightarrow R_{\text{sift}} \propto t$$

fraction of dark count =  $1/2$

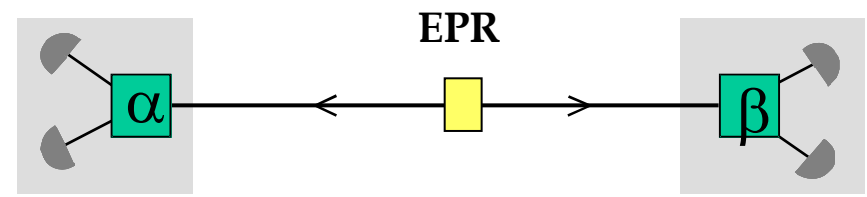
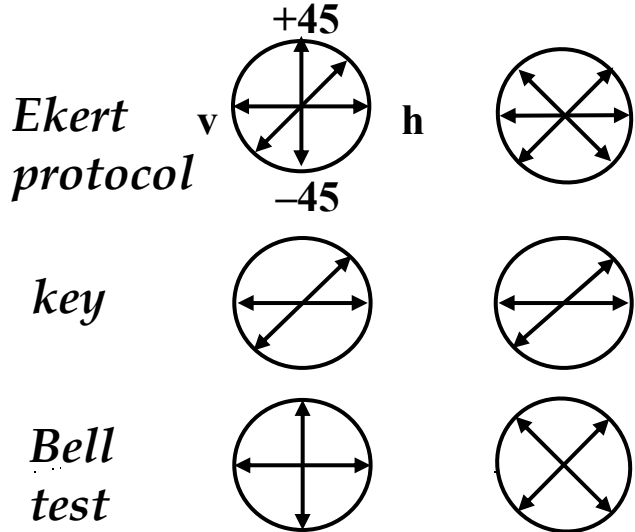




Alice

Bob

# the Ekert'91 protocol



- A and B choose randomly between three different settings
- depending on the bases chosen, the pair detections are divided into three groups
  - settings to establish perfect correlations  $\implies$  key
  - settings to test Bell inequality  $\implies$  test for eavesdropper
  - incompatible settings  $\implies$  measurement discarded
- standard BB84 protocol can be applied
  - measurement of A  $\implies$  non-local state preparation of B
  - QBER reveals eavesdropper
  - passive state choice  $\implies$  no PNS attack

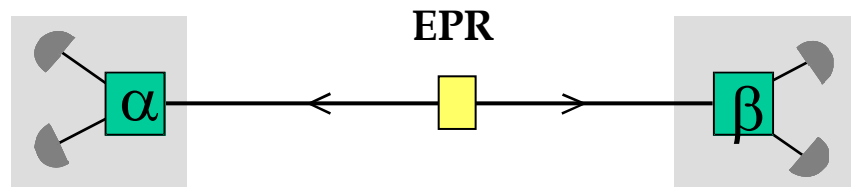
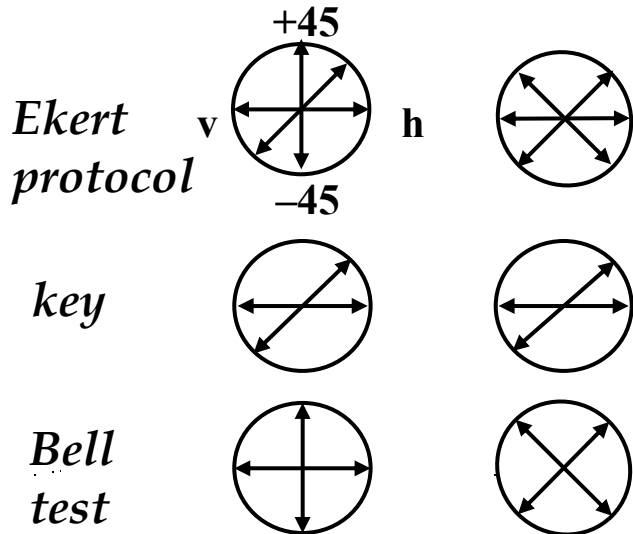
Ekert, PRL 67, 661 (1991)  
Bennett *et al*, PRL 68, 557 (1992)



Alice

Bob

# the Ekert'91 protocol



- A
- de
- in
- 
- 
- 
- sta

Link between violation of Bell inequality  
and possibility to exchange a secret key !!!

$$S > 2 \implies I(\alpha, \beta) > I^{\max}(\alpha, \epsilon)$$

For CHSH-Bell and BB84

C.A. Fuchs *et al*, Phys. Rev. A **56**, 1163 (1997)

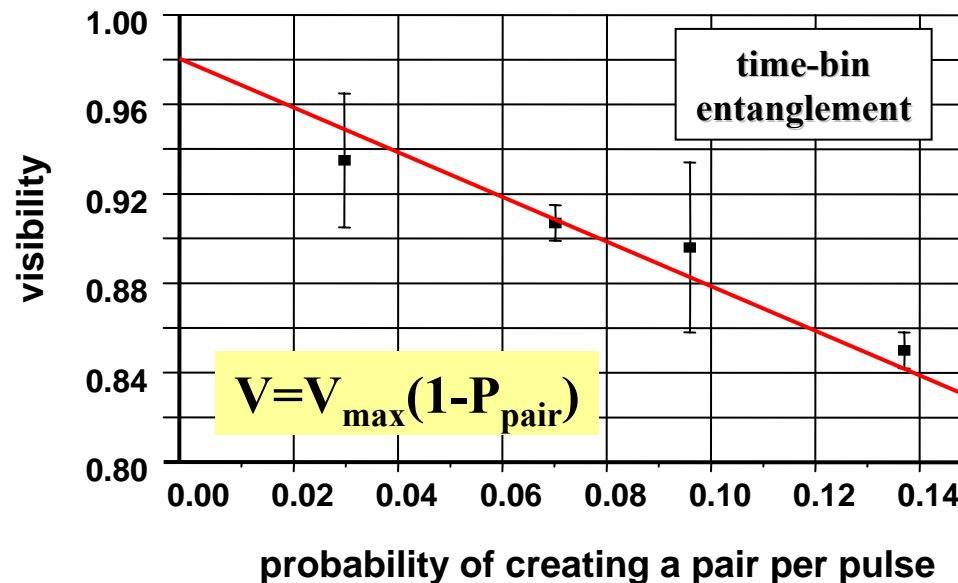
- QBER reveals eavesdropper
- passive state choice  $\implies$  no PNS attack

Ekert, PRL **67**, 661 (1991)  
 Bennett *et al*, PRL **68**, 557 (1992)

# PNS eavesdropping



- the two photons traveling to Bob are independent
  - analysis of one photon does not lead to information about state of remaining one
  - PNS attacks do not apply !
  - however, multi-photon pulses lead to increase of QBER



$$P_{n=2} = \frac{P_{n=1}^2}{2}$$

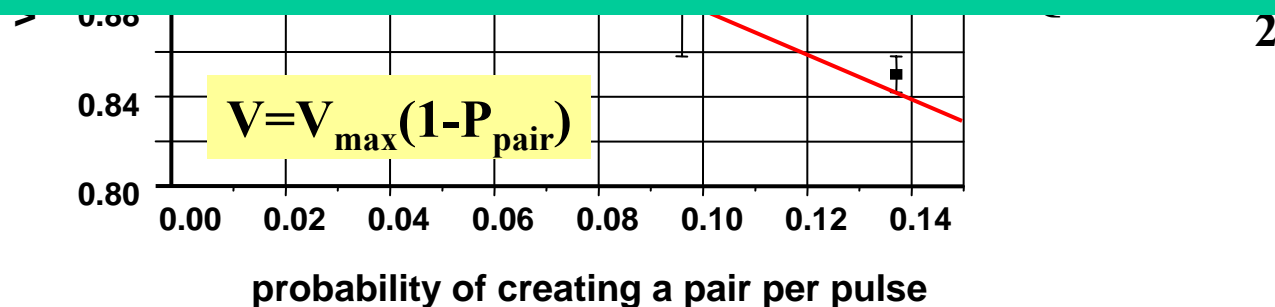
$$\text{QBER} = \frac{1 - V}{2}$$

# PNS eavesdropping



- the two photons traveling to Bob are independent
  - analysis of one photon does not lead to information about state of remaining one

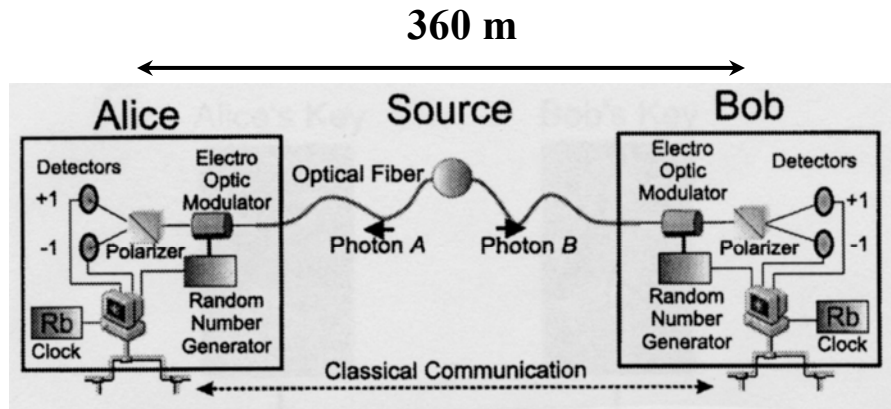
**Multi-photon pulses are still undesired,  
however, they only lead to higher QBER  
without increasing  $I(\alpha, \epsilon)$  !**



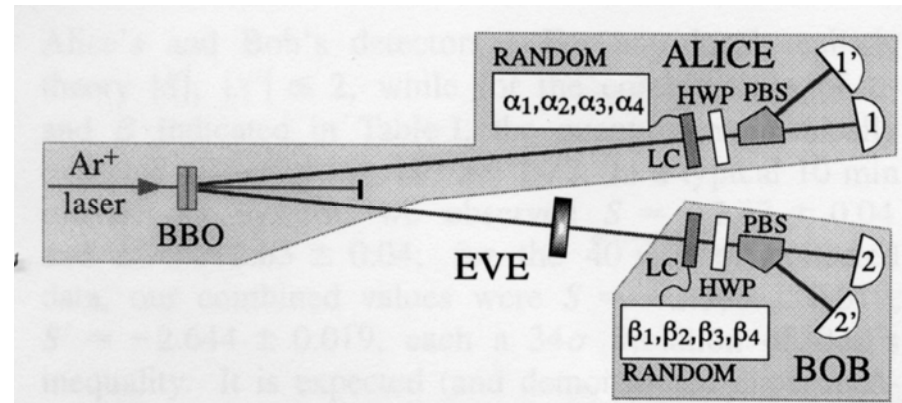
# entanglement - a selection

- 1935/1964 « Verschränkung », EPR paradox, Bell inequality
- since 1972 tests of Bell-inequalities  
*Freedman et al., PRL 28, 938 (1972)*
- 1981/1982 the « Aspect » experiments  
*Aspect et al., PRL 49, 91 (1982) & PRL 49, 1804 (1982)*
- 1991 Ekert protokol  
*Ekert, PRL 67, 661 (1991)*
- 1997 entanglement over 10 km (fiber)  
*Tittel et al., PRA 57, 3229 (1997) & PRL 81, 3563 (1998)*
- 1998 closing the locality loophole  
*Weih's et al., PRL 81, 5039 (1998)*
- 2000 quantum key distribution (up to 360 m)  
*Jennewein et al., PRL 84, 4727 (2000)*  
*Naik et al., PRL 84, 4733 (2000)*  
*Tittel et al., PRL 84, 4737 (2000)*
- 2001 QKD over 8.5 km (fiber)  
*Ribordy et al., PRA. 63, 012309 (2001)*
- 2001 closing the detection loophole (atoms)  
*Rowe et al., Nature 409, 791 (2001)*
- 2003 entanglement over 600 m (free space)  
*Aspelmeyer et al., Science 301, 621 (2003)*
- 2004 entanglement and QKD over 50 km (fiber)  
*Marcikic et al., PRL 93, 180502 (2004)*
- 2005 entanglement / QKD over 7.8&13 km (free space)  
*Resch et al. Optics Express 13, 202 (2005). Peng et al., PRL 94, 150501 (2005)*

# quantum cryptography with polarization entangled qubits

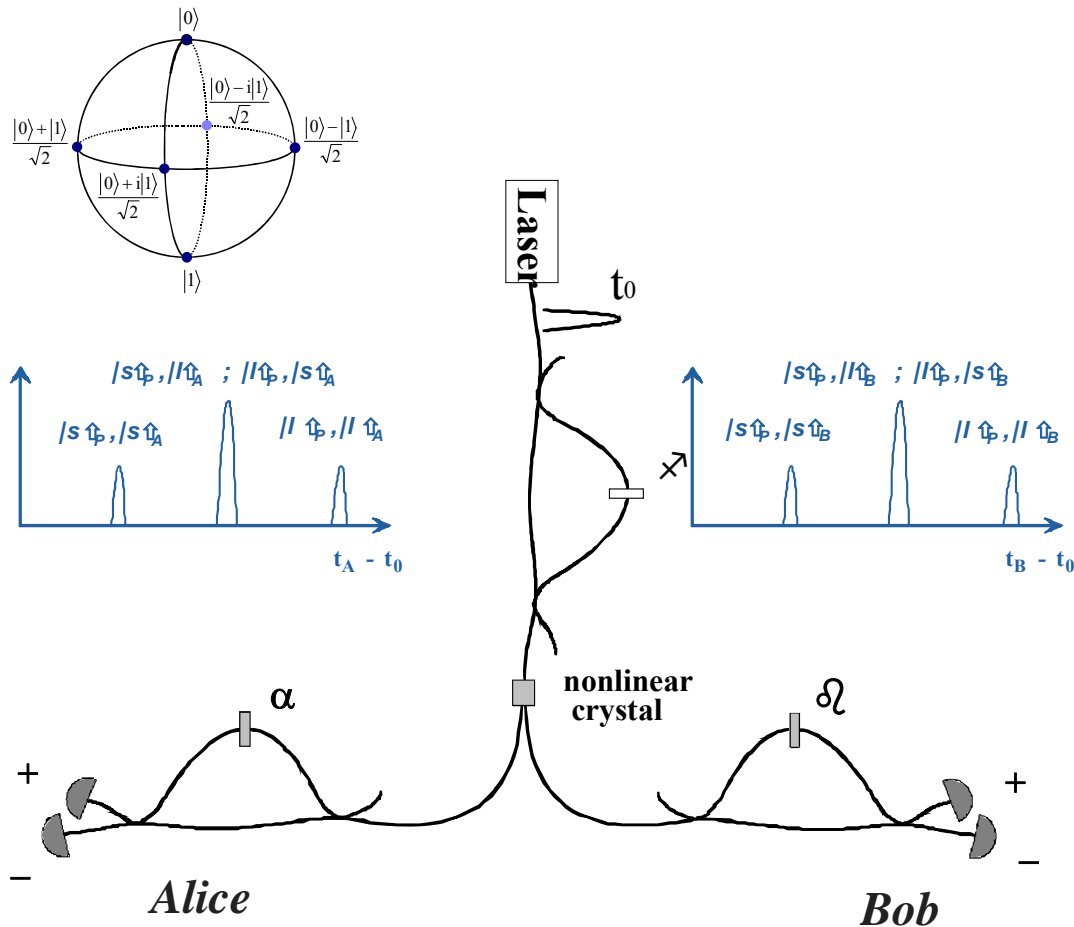


T. Jennewein *et al.* Phys. Rev. Lett. 2000.



D. Naik *et al.* Phys. Rev. Lett. 2000.

# quantum cryptography using time-bin entangled qubits



- satellite peaks (*pole states*)
  - ➔ correlated detection times
  - ➔ correlated bits
- central peaks (*equatorial states*)
  - $P_{ij} = 1/4 [1 + ij \cos(\alpha + \beta - \phi)]$
  - ➔ correlated detectors ( $\alpha + \beta - \phi = 0$ )
  - ➔ correlated bits

- use of complementary bases ensures detection of eavesdropper
- passive choice of basis: simple implementation, no PNS attacks possible

# Photon Pairs or Faint Laser Pulses ?

inefficient

- standard BB84

$$\mu_{\text{opt}} = t; R_{\text{sift}} \propto t^2$$

- new protocols

- non-orthogonal states

$$\mu_{\text{opt}} = 2\sqrt{t}; R_{\text{sift}} \propto t^{3/2}$$

- decoy states

$$\mu \approx 0.5; R_{\text{sift}} \propto t$$

- quantum cryptography based on entanglement

$$\mu = O(1); R_{\text{sift}} \propto t$$

addtl. errors

- true single-photon sources

$$\mu = 1; R_{\text{sift}} \propto t$$

efficient

simple

difficult