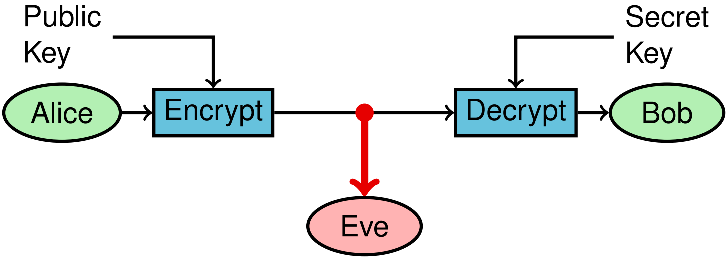
Cryptography Lecture 10

Quantum key distribution

LINKÖPING UNIVERSITY

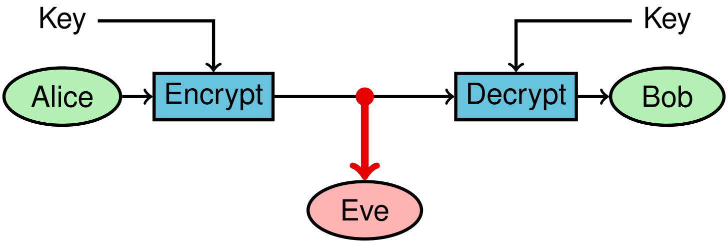
Key distribution is a problem in cryptography

Public key transfer rests on the (unproven) hardness of certain mathematical problems such as factoring



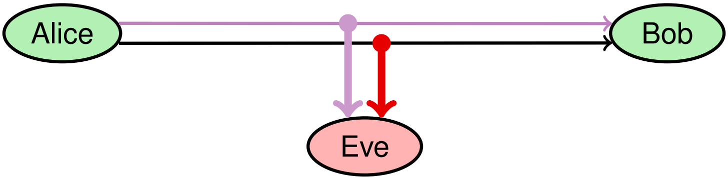
Key distribution is a problem in cryptography

Another solution: Transfer the key secretly, and use symmetric key cryptography

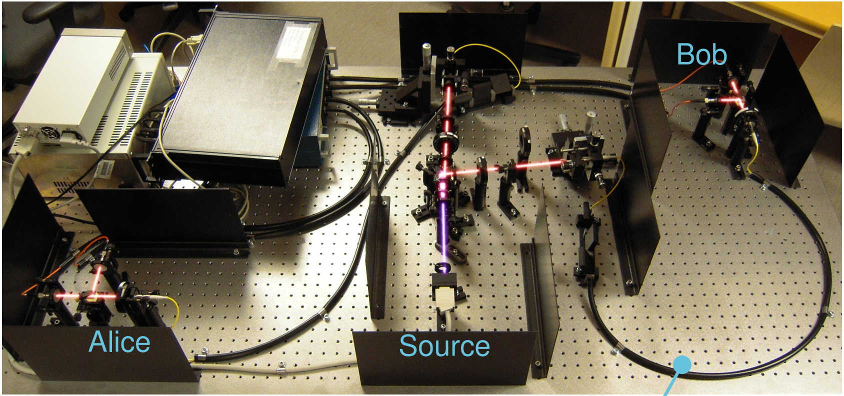


Quantum key distribution

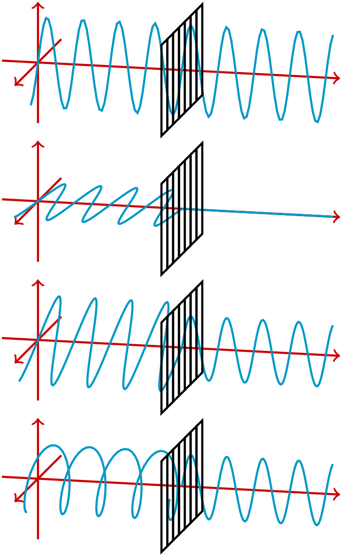
Task: to transfer (share) secret key
Idea: Content on a quantum channel changes when Eve listens
(The classical channel in the scheme is not encrypted)



ISY's quantum key distribution system



Polarized light



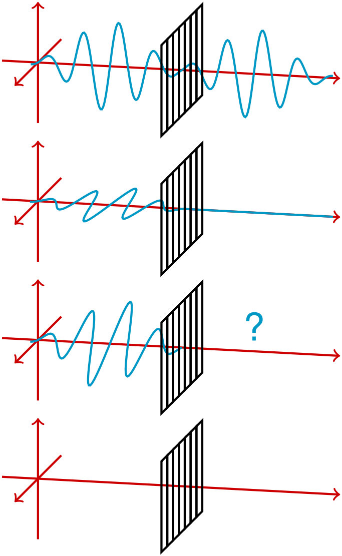
$I_{\text{after}} = I_{\text{before}}$

$I_{\text{after}} = 0$

$I_{\text{after}} = \frac{1}{2} I_{\text{before}}$

$I_{\text{after}} = \frac{1}{2} I_{\text{before}}$

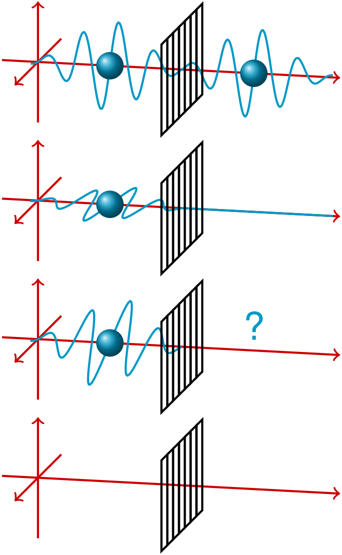
Polarized photons



$P_{\text{pass}} = 1$

$P_{\text{pass}} = 0$

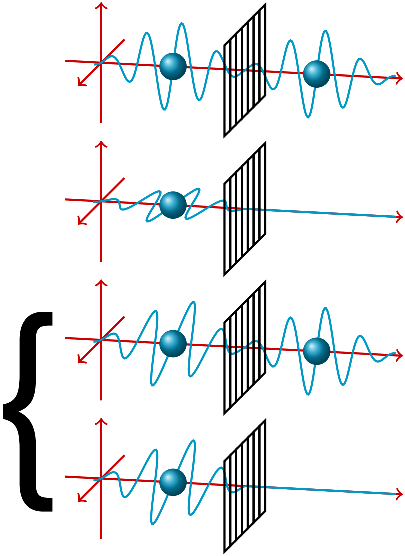
Polarized photons



$P_{\text{pass}} = 1$

$P_{\text{pass}} = 0$

Polarized photons



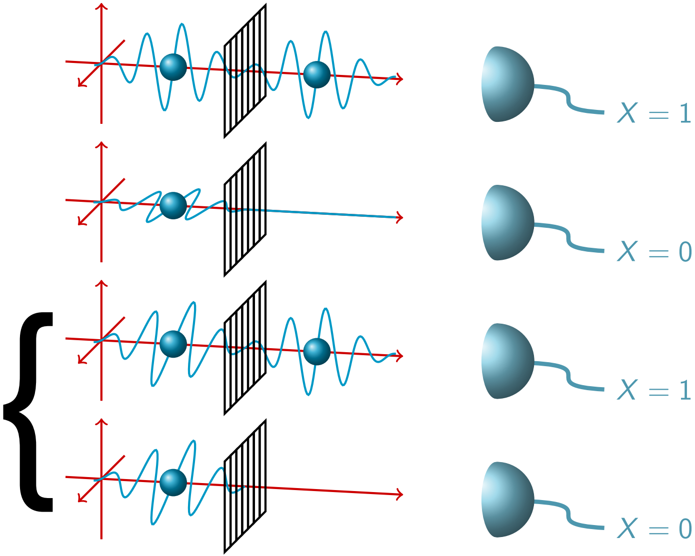
$$P_{\text{pass}} = 1$$

$$P_{\text{pass}} = 0$$

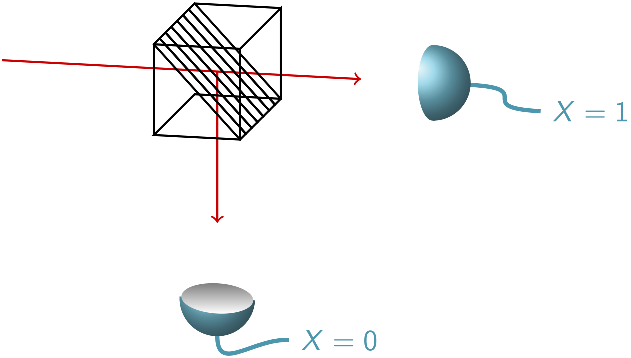
$$P_{\text{pass}} = \frac{1}{2}$$

$$P_{\text{pass}} = \frac{1}{2}$$

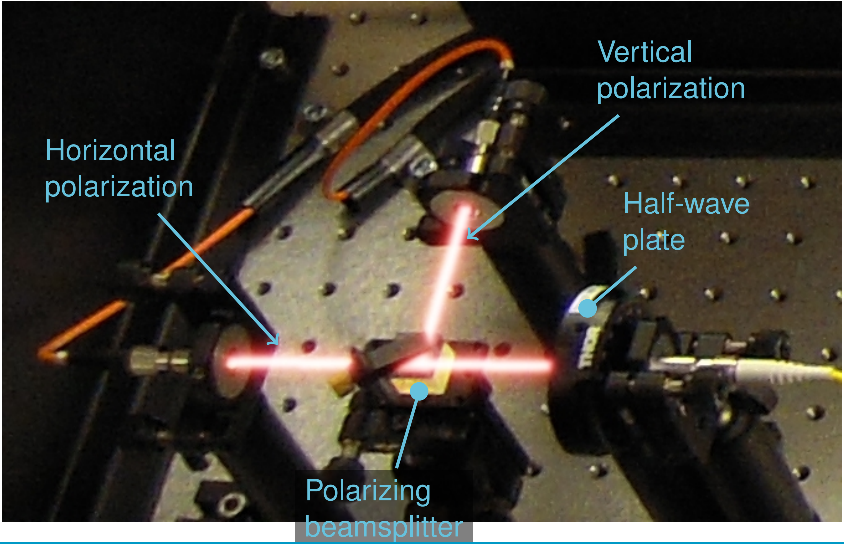
Polarized photons



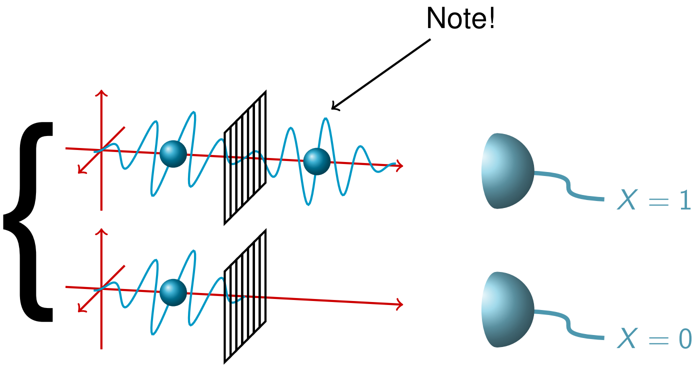
Polarized photons



Analysis station



Measurement destroys earlier state



Heisenberg's uncertainty relation

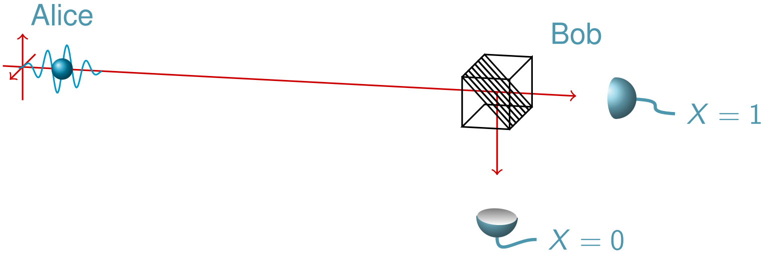
$$\Delta x \Delta p \geq \frac{\hbar}{2}$$

In our case, X is a bit value, and

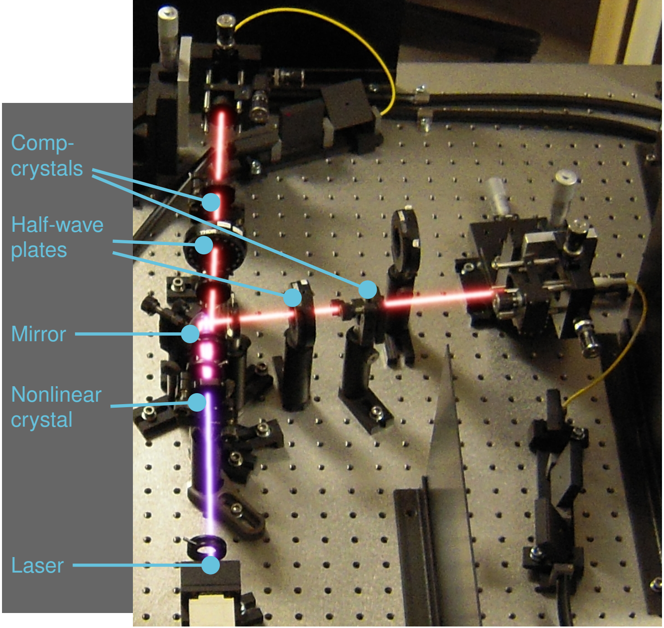
$$\Delta x_\times \Delta x_\circ \geq \frac{1}{2}\left|\langle x_+ \rangle - \frac{1}{2}\right|$$

The standard deviations on the right can only be 0 if the expectation on the left is 1/2

Quantum channel (BB84)

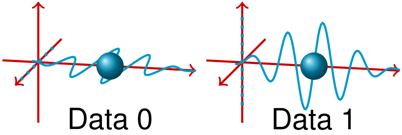


Source

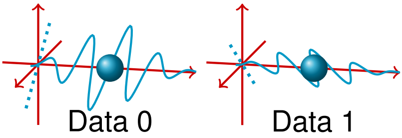

Comp-
crystals
Half-wave
plates
Mirror
Nonlinear
crystal
Laser

Encoding on the quantum channel

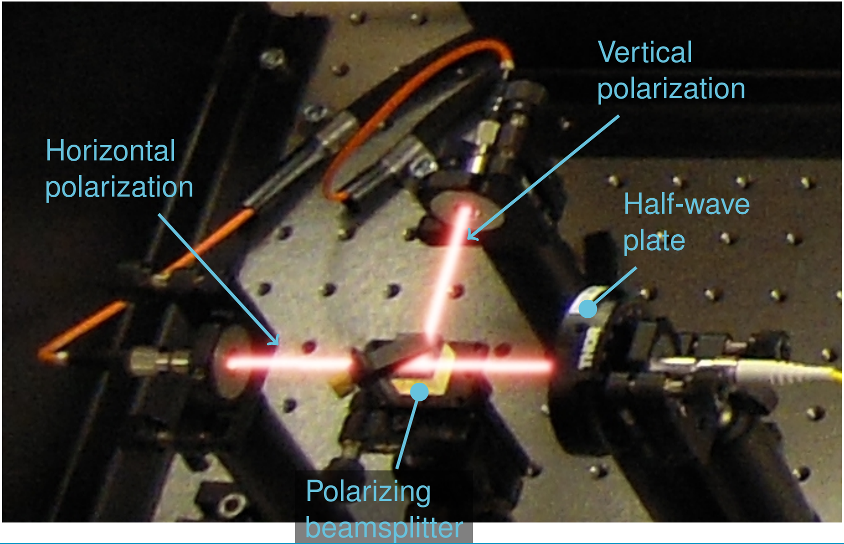
Coding HV (Horizontal-Vertical), $+$, encoding 0



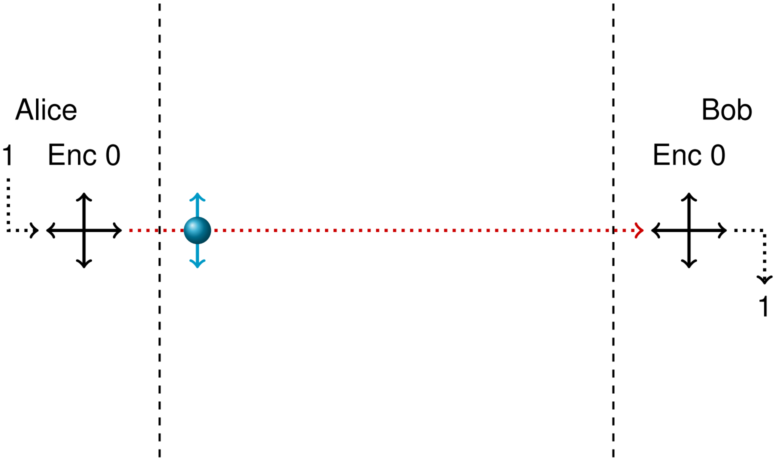
Coding PM (Plus-Minus 45°), $\times$, encoding 1



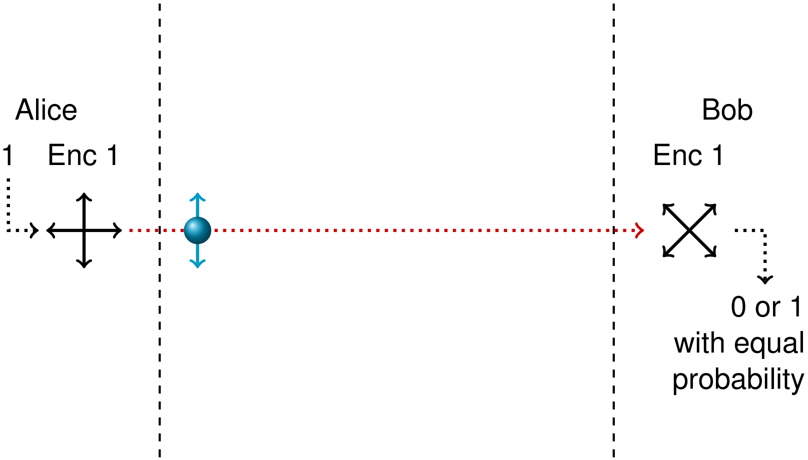
Analysis station



Example



Example



Data streams

Alice’s data `101101001011110011100101001110`

Alice’s enc

- -

- -

Bob’s enc

Bob’s data

Data streams

Alice's data	101101001011110011100101001110
Alice's enc	011010010010111010110100100111
	+××+×++×++×+×××+×+××+×++×++×××

Bob's enc

Bob's data

Data streams

Alice’s data	101101001011110011100101001110
Alice’s enc	011010010010111010110100100111
	+××+×++×++×+×××+×+××+×++×++×××
	| / \ | / | – / | – \ | \ \ / – \ | \ / – \ – | / – | \ \ /
Bob’s enc	
Bob’s data	

Data streams

Alice's data	101101001011110011100101001110
Alice's enc	011010010010111010110100100111
	+××+×++×++×+×××+×+××+×++×++×××
	| / \ | / | − / | − \ | \ \ / − \ | \ / − \ − | / − | \ \ /
Bob's enc	001101001001101111110111000010
	++××+×++×++××+××××××+×××++++×+
Bob's data	

Data streams

```
Alice's data  101101001011110011100101001110
Alice's enc   011010010010111010110100100111
              +××+×++×++×+×××+×+××+×++×++×××
------------------------------------------------
              |/\|/|—/|—\|\\/—\|\/—\—|/—|\\/






------------------------------------------------
Bob's enc     001101001001101111110111000010
              ++××+×++×++××+××××××+×××++++×+
Bob's data    101011000011100111100100101111
```

Data streams

Alice's data	101101001011110011100101001110
Alice's enc	011010010010111010110100100111
	+××+×++×++×+×××+×+××+×++×++×××
	|/\\|/|–/|–\\|\\\\/–\\|\\/–\\–|/–|\\\\/

After quantum bits have arrived, perform sifting:
compare encodings used, and remove nonmatching slots

Bob's enc	001101001001101111110111000010
	++××+×++×++××+××××××+×××++++×+
Bob's data	101011000011100111100100101111

Data streams

```
Alice's data  101101001011110011100101001110
Alice's enc   011010010010111010110100100111
              +××+×++×++×+×××+×+××+×++×++×××
- - - - - - - - - - - - - - - - - - - - - - - -
              |/\|/|−/|−\|\\/−\|\/−\−|/−|\\/
```

After quantum bits have arrived, perform sifting: compare encodings used, and remove nonmatching slots

```
- - - - - - - - - - - - - - - - - - - - - - - -
Bob's enc     001101001001101111110111000010
              ++××+×++×++××+××××××+×××++++×+
Bob's data    101011000011100111100100101111
```

Data streams

Alice's data 1 0 1 1 0 1 0 0 1 0 1 1 1 1 0 0 1 1 1 0 0 1 0 1 0 0 1 1 1 0

Alice's enc 0 ~~1~~ 1 ~~0~~ ~~1~~ ~~0~~ 0 ~~1~~ ~~0~~ 0 ~~1~~ ~~0~~ 1 ~~1~~ 1 ~~0~~ 1 ~~0~~ 1 1 0 1 ~~0~~ ~~0~~ ~~1~~ 0 0 ~~1~~ 1 ~~1~~

+ × × + × + + × + + × + × × × + × + × × + × + + × + + × × ×

- -

| / \ | / | — / | — \ | \ \ / — \ | \ / — \ — | / — | \ \ /

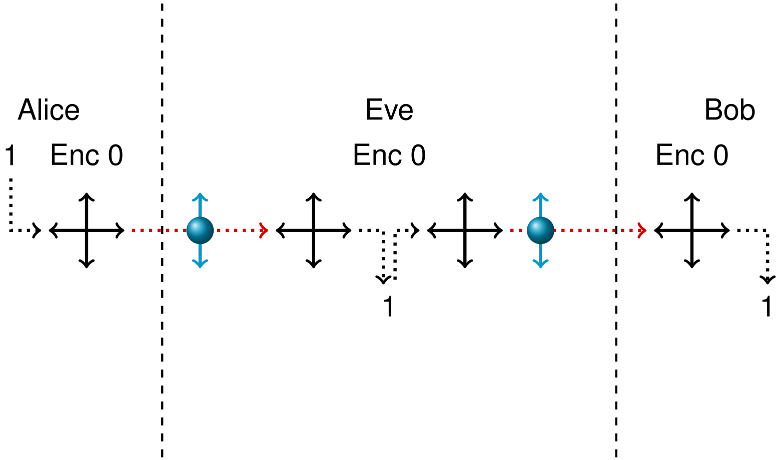
- -

Bob's enc 0 ~~0~~ 1 ~~1~~ ~~0~~ ~~1~~ 0 ~~0~~ ~~1~~ 0 ~~0~~ ~~1~~ 1 ~~0~~ 1 ~~1~~ 1 ~~1~~ 1 1 0 1 ~~1~~ ~~1~~ ~~0~~ 0 0 ~~0~~ 1 ~~0~~

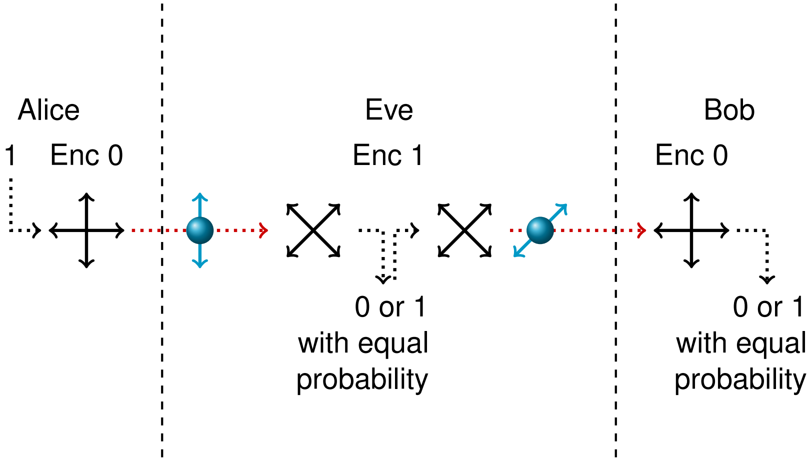
+ + × × + × + + × + + × × + × × × × × × + × × × + + + + × +

Bob's data 1 0 1 0 1 1 0 0 0 0 1 1 1 0 0 1 1 1 1 0 0 1 0 0 1 0 1 1 1 1

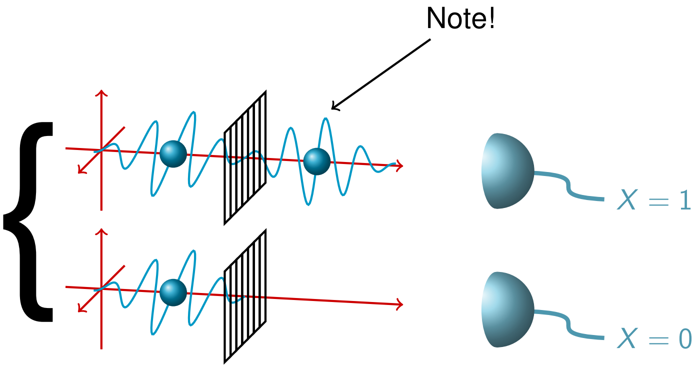
Example



Example


Alice
Eve
Bob
1
Enc 0
Enc 1
Enc 0
0 or 1
with equal
probability
0 or 1
with equal
probability

Measurement destroys earlier state



Heisenberg's uncertainty relation

$$\Delta x \Delta p \geq \frac{\hbar}{2}$$

In our case, X is a bit value, and

$$\Delta x_\times \Delta x_\circ \geq \frac{1}{2}\left|\langle x_+ \rangle - \frac{1}{2}\right|$$

The standard deviations on the right can only be 0 if the expectation on the left is 1/2

Data streams, with eavesdropper

Alice's data	101101001011110011100101001110
Alice's enc	011010010010111010110100100111
	+××+×++×++×+×××+×+××+×++×++×××
	| / \ | / | — / | — \ | \ \ / — \ | \ / — \ — | / — | \ \ /
Eve's enc	
Eve's data	
Bob's enc	001101001001101111110111000010
	++××+×++×++××+××××××+×××++++×+
Bob's data	

Data streams, with eavesdropper

Alice's data 101101001011110011100101001110

Alice's enc 011010010010111010110100100111

+××+×++×++×+×××+×+××+×++×++×××

- -

|/\|/|—/|—\|\\/—\|\/—\—|/—|\\/

Eve's enc 111010100100111101011101011011

×××+×+×++×++××××+×+×××+×+××+××

Eve's data

- -

Bob's enc 001101001001101111110111000010

++××+×++×++××+××××××+×××++++×+

Bob's data

Data streams, with eavesdropper

```
Alice's data   101101001011110011100101001110
Alice's enc    011010010010111010110100100111
               +××+×++×++×+×××+×+××+×++×++×××
----------------------------------------------
               |/\|/|—/|—\|\\/—\|\/—\—|/—|\\/

Eve's enc      111010100100111101011101011011
               ×××+×+×++×++××××+×+×××+×+××+××
Eve's data     001101101111110100101100010110

----------------------------------------------
Bob's enc      001101001001101111110111000010
               ++××+×++×++××+××××××+×××++++×+

Bob's data
```

Data streams, with eavesdropper

```
Alice's data  101101001011110011100101001110
Alice's enc   011010010010111010110100100111
              +××+×++×++×+×××+×+××+×++×++×××
------------------------------------------------
              |/\|/|—/|—\|\\/—\|\/—\—|/—|\\/

Eve's enc     111010100100111101011101011011
              ×××+×+×++×++××××+×+×××+×+××+××
Eve's data    001101101111110100101100010110
              //\|/|\—|\||\\/\—/|/\\—/—\/|\/
------------------------------------------------
Bob's enc     001101001001101111110111000010
              ++××+×++×++××+××××××+×××++++×+
Bob's data
```

Data streams, with eavesdropper

Alice's data 101101001011110011100101001110

Alice's enc 011010010010111010110100100111

+××+×++×++×+×××+×+××+×++×++×××

- -

| / \ | / | — / | — \ | \ \ / — \ | \ / — \ — | / — | \ \ /

Eve's enc 111010100100111101011101011011

×××+×+×++×++××××+×+×××+×+××+××

Eve's data 001101101111110100101100010110

/ / \ | / | \ — | \ | | \ \ / \ — / | / \ \ — / — \ / | \ /

- -

Bob's enc 001101001001101111110111000010

++××+×++×++××+××××××+×××++++×+

Bob's data 011110101010110110000110010111

Data streams, with eavesdropper

Alice's data	1 0 1 1 0 1 0 0 1 0 1 1 1 1 0 0 1 1 1 0 0 1 0 1 0 0 1 1 1 0
Alice's enc	0 1 1 0 1 0 0 1 0 0 1 0 1 1 1 0 1 0 1 1 0 1 0 0 1 0 0 1 1 1
	+ × × + × + + × + + × + × × × + × + × × + × + + × + + × × ×
	| / \ | / | − / | − \ | \ \ / − \ | \ / − \ − | / − | \ \ /
Eve's enc	1 1 1 0 1 0 1 0 0 1 0 0 1 1 1 1 0 1 0 1 1 1 0 1 0 1 1 0 1 1
	× × × + × + × + + × + + × × × × + × + × × × + × + × × + × ×
Eve's data	0 0 1 1 0 1 1 0 1 1 1 1 1 1 0 1 0 0 1 0 1 1 0 0 0 1 0 1 1 0
	/ / \ | / | \ − | \ | | \ \ / \ − / | / \ \ − / − \ / | \ /
Bob's enc	0 0 1 1 0 1 0 0 1 0 0 1 1 0 1 1 1 1 1 1 0 1 1 1 0 0 0 0 1 0
	+ + × × + × + + × + + × × + × × × × × × + × × × + + + + × +
Bob's data	0 1 1 1 1 0 1 0 1 0 1 0 1 1 0 1 1 0 0 0 0 1 1 0 0 1 0 1 1 1

Data streams, with eavesdropper

Alice's data 101101001011110011100101001110

Alice's enc 011010010010111010110100100111

+××+×++×++×+×××+×+××+×++×++×××

\- -

| / \ | / | — / | — \ | \ \ / — \ | \ / — \ — | / — | \ \ /

Eve's enc 111010100100111101011101011011

×××+×+×++×++××××+×+×××+×+××+××

Eve's data 001101101111110100101100010110

/ / \ | / | \ — | \ | | \ \ / \ — / | / \ \ — / — \ / | \ /

\- -

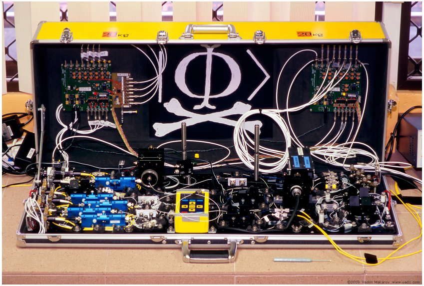
Bob's enc 001101001001101111110111000010

++××+×++×++××+××××××+×××++++×+

Bob's data 011110101010110110000110010111

Attack possibilities for Eve

- Intercept-resend (Heisenberg)
- Entangling probe (Monogamy of entanglement)
- Cloning (No-cloning theorem)
- Coherent attacks (more advanced versions of the above)
- Side channel attacks
  - Photon-number splitting
  - Trojan horse
  - Weaknesses of the equipment



Quantum Key Distribution, version 1

- Generate raw key
- Sift the key
- Check the noise level

Problem 1

- A real-life quantum channel has noise even without Eve

Quantum Key Distribution, version 2

- Generate raw key
- Sift the key
- Reduce and check the noise level

Reconciliation (Error correction)

- Bob takes two random bit values (e.g., nr 137 and 501)
- He calculates their XOR and sends the bit indices and the XOR value to Alice
- Alice compares with her XOR value
- If the XOR values are the same, keep the first bit value, otherwise none of them

Quantum Key Distribution, version 2

- Generate raw key
- Sift the key
- Reduce and check the noise level

Problem 2

- A real-life quantum channel has noise even without Eve
- Eve might have better technology than Alice and Bob (less noisy quantum channel)
- In that case, she can change to her quantum channel and also eavesdrop, up to the former noise level

Quantum Key Distribution, version 3

- Generate raw key
- Sift the key
- Reduce and check the noise level
- Reduce Eve's information on the new key

Privacy amplification

- Bob takes two random bit indices (e.g., nr 43 and 212)
- He sends the bit indices to Alice (but not the XOR value)
- Alice and Bob individually computes the XOR value
- They remove their bit values and insert the XOR value (without having sent them on the classical channel)

Quantum Key Distribution, version 3

- Generate raw key
- Sift the key
- Reduce and check the noise level
- Reduce Eve's information on the new key

Noise limit

- BB84 can manage a QBER of 11%

Quantum Key Distribution, version 3

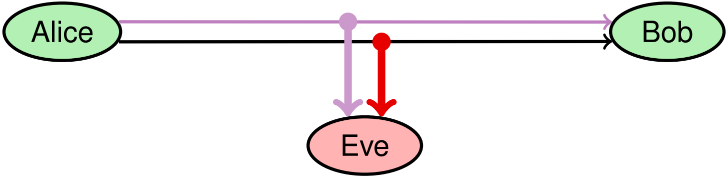
- Generate raw key
- Sift the key
- Reduce and check the noise level
- Reduce Eve's information on the new key

Problem 3

- Messages on real-life classical channels can be modified

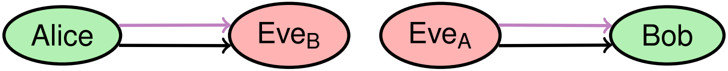
Man-in-the-middle

Eve can pretend to be Bob when she speaks to Alice and pretend to be Alice when she speaks to Bob



Man-in-the-middle

Eve can pretend to be Bob when she speaks to Alice and pretend to be Alice when she speaks to Bob



Quantum Key Distribution, final version

- Generate raw key
- Sift the key
- Reduce and check the noise level
- Reduce Eve's information on the new key
- Authenticate the messages on the classical channel

Quantum Key Distribution, final version

On the quantum channel

- Generate raw key

- Sift the key
- Reduce and check the noise level
- Reduce Eve's information on the new key
- Authenticate the messages on the classical channel

On the classical channel

Quantum Key Distribution, final version

On the quantum channel

- Generate raw key

- Sift the key
- Reduce and check the noise level
- Reduce Eve's information on the new key
- Authenticate the messages on the classical channel

On the classical channel

Eve's presence is noticed in this step

Or in this step

Wegman-Carter-authentication

If you try to generate an authentication tag for a message without knowing the secret key, all tag values have equal probability

This is (almost) true even after having seen a message-tag pair

One-time-pad

If you try to decrypt a cryptotext without knowing the secret key, all cleartexts have equal probability

Wegman-Carter-authentication

Uses a secret key value k to select a function from an "ε-Almost Strongly Universal-2 hash function family" $\{h_k\}$

The key value k is unknown to Eve, and then, the family is such that

$$P\Big(h_k(m_\mathsf{E}) = t_\mathsf{E}\Big) = 2^{-T}$$

Seeing a message-tag pair reveals some of the key to Eve, but even then

$$P\Big(h_k(m_\mathsf{E}) = t_\mathsf{E}\Big| h_k(m_\mathsf{A}) = t_\mathsf{A}\Big) \leq \epsilon$$

One-time-pad

$$P\Big(D_k(c_\mathsf{A}) = m_\mathsf{A}\Big) = 2^{-M}$$

Wegman-Carter-authentication

Uses a secret key value k to select a function from an "ε-Almost Strongly Universal-2 hash function family" $\{h_k\}$

The key value k is unknown to Eve, and then, the family is such that

$$P\Big(h_k(m_\mathrm{E}) = t_\mathrm{E}\Big) = 2^{-T}$$

Seeing a message-tag pair reveals some of the key to Eve, but even then

$$P\Big(h_k(m_\mathrm{E}) = t_\mathrm{E}\Big|h_k(m_\mathrm{A}) = t_\mathrm{A}\Big) \le \epsilon \overset{\text{often}}{=} 2 \cdot 2^{-T}$$

One-time-pad

$$P\Big(D_k(c_\mathrm{A}) = m_\mathrm{A}\Big) = 2^{-M}$$

A 2^{-T}-Almost Strongly Universal-2 hash function family

Messages are integers mod 2^M and tags are integers mod $2^T \ll 2^M$

Select a (public) prime $p > 2^M$ and a secret key $k = (a, b)$ where a and b are integers mod p, and let

$$h_k(m) = (am + b \bmod p) \bmod 2^T$$

One-time-pad

$$E_k(m) = m + k \bmod 2^M, \quad D_k(c) = c - k \bmod 2^M$$

A 2^{-T}-Almost Strongly Universal-2 hash function family

Messages are integers mod 2^M and tags are integers mod $2^T \ll 2^M$

Select a (public) prime $p > 2^M$ and a secret key $k = (a, b)$ where a and b are integers mod p, and let

$$h_k(m) = (am + b \bmod p) \bmod 2^T$$

Two uses of h_k reveals the values of a and b

Key consumption is twice the message length M (!)

By increasing ε to $2 \cdot 2^{-T}$ and using a clever construction Wegman and Carter reduced this to $\log M$

Quantum Key Distribution = Quantum Key Expansion

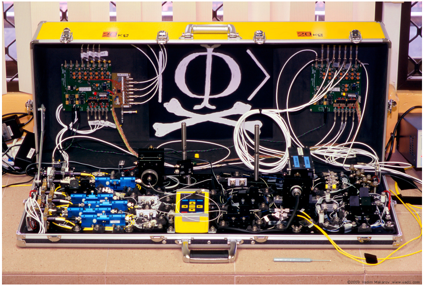
- Raw key generation
- Sifting
- Reconciliation
- Privacy amplification
- Authentication

Key consumption of the system

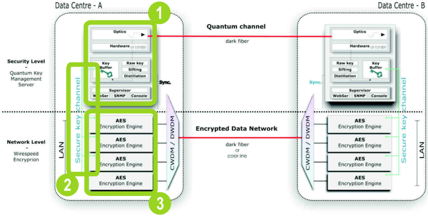
- Information-theoretically secure auth uses secret key
- The system needs secret key to start
- Key consumption is logarithmic in message length
- Key production is linear in message length

Attack possibilities for Eve

- Intercept-resend (Heisenberg)
- Entangling probe (Monogamy of entanglement)
- Cloning (No-cloning theorem)
- Coherent attacks (more advanced versions of the above)
- Side channel attacks
  - Photon-number splitting
  - Trojan horse
  - Weaknesses of the equipment



Commercial products



QKD Server Performance 1

- Plug&Play Optical Platform
- BB84/SARG Protocol
- Range: < 50km (> 50 Km on request)
- Secret key rate: > 1'000 bps over 25 km
- One Quantum Key Server can:
  - serve up to 12 encryptors
  - serve encryptors for different protocols

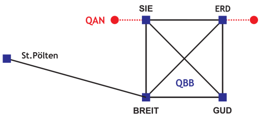
Key Channel (idQ3P) 2

- Serial link
- Encrypted (AES-256)
- Authenticated (HMAC-SHA-1)
- Key Exchange rate: 1/minute

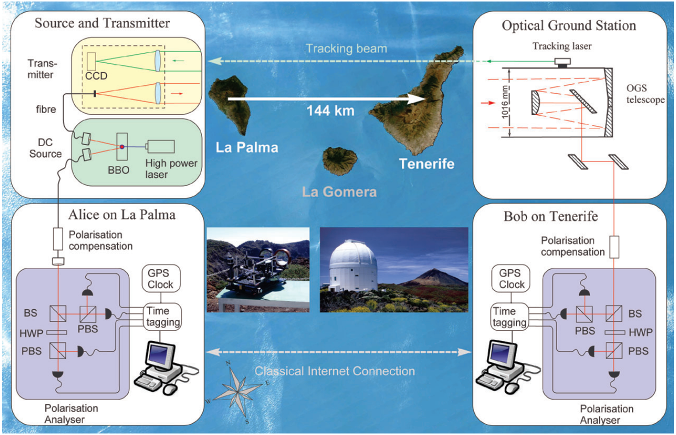
Encryption Appliance 3

- Up to 10 Gbps
- Multiprotocol
  - Ethernet
  - SONET/SDH
  - Fibre Channel (FC)
  - ATM
- Accredited (FIPS, Common Criteria)

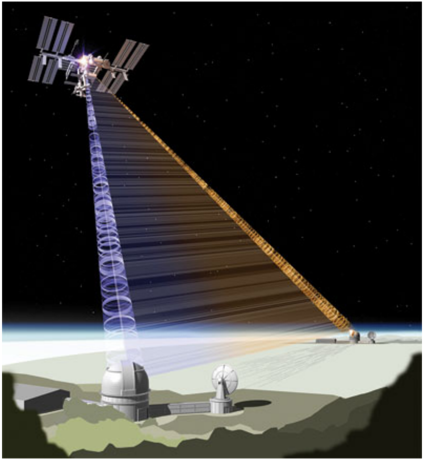
Network in Vienna (2008)



A long-range system has been tested on the Canary islands



There are also plans of a repeater on ISS



ISY's quantum key distribution system