Quantum Key Distribution

PQCrypto Summer School ▪ September 30, 2014

Dr Douglas Stebila

Queensland University of Technology

Outline

1. Qubits
2. Basic QKD • BB84
3. Entanglement-based QKD
4. Classical processing
5. Authentication • Security of QKD
6. Classifying QKD schemes
7. QKD implementations
8. QKD networks

Terminology

Quantum cryptography

- coin flipping
- blind quantum computation
- …

Quantum key distribution

- a.k.a.
- quantum key exchange
- quantum key establishment

Qubits

Qubits

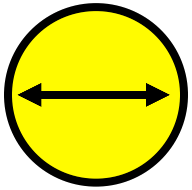
A *qubit* is a two-state quantum system.

- example: polarization of a photon, spin of an electron, spin in a quantum dot, ...

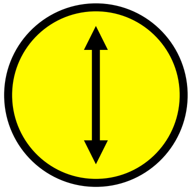
Logically, a qubit is a norm-1 vector in a 2-dimensional complex vector space.

Qubits as vectors

$$\begin{bmatrix} 1 \\ 0 \end{bmatrix} = |\,0\,\rangle$$



$$\begin{bmatrix} 0 \\ 1 \end{bmatrix} = |\,1\,\rangle$$

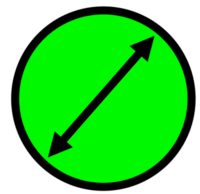


(Arrows are two-sided because there's not much difference between $|\,0\,\rangle$ and $-|\,0\,\rangle$).

Qubits as vectors

Here's another norm-1 vector:

$$\frac{1}{\sqrt{2}}\begin{bmatrix}1\\1\end{bmatrix}$$



We can write vectors as complex linear combinations:

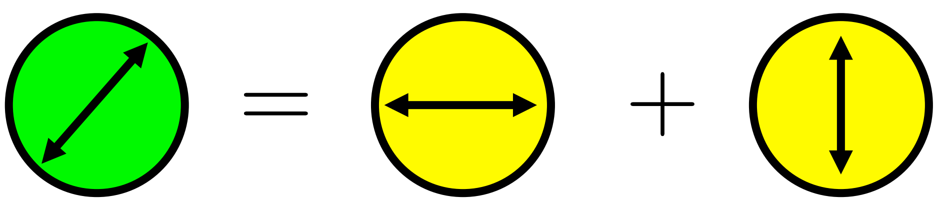
$$\frac{1}{\sqrt{2}}\begin{bmatrix}1\\1\end{bmatrix} = \frac{1}{\sqrt{2}}\left(\begin{bmatrix}1\\0\end{bmatrix} + \begin{bmatrix}0\\1\end{bmatrix}\right)$$

Qubits as vectors

We can interpret complex linear combinations as *superpositions*:

$$\frac{1}{\sqrt{2}}\begin{bmatrix}1\\1\end{bmatrix} = \frac{1}{\sqrt{2}}\left(\begin{bmatrix}1\\0\end{bmatrix} + \begin{bmatrix}0\\1\end{bmatrix}\right)$$

$$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

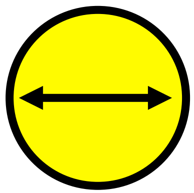


(ignoring normalization factor)

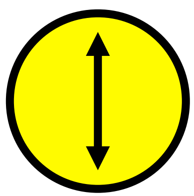
Bases

Computational basis

$$|\,0\,\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$$

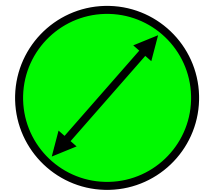


$$|\,1\,\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

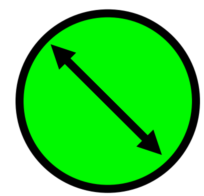


Diagonal basis

$$|\,+\,\rangle = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 1 \end{bmatrix}$$



$$|\,-\,\rangle = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ -1 \end{bmatrix}$$



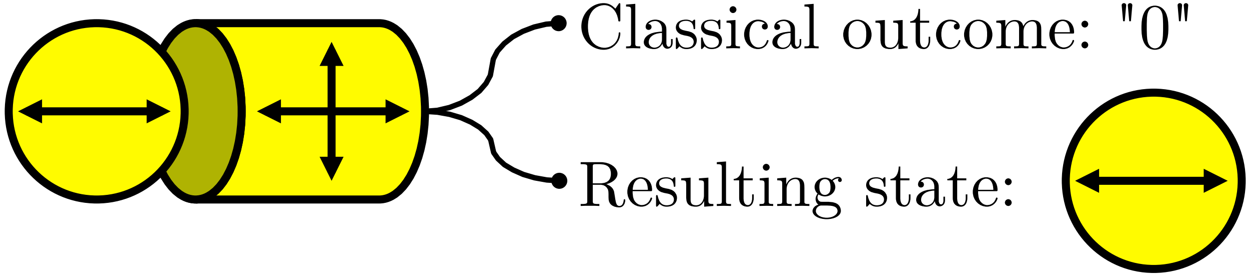
Measurement

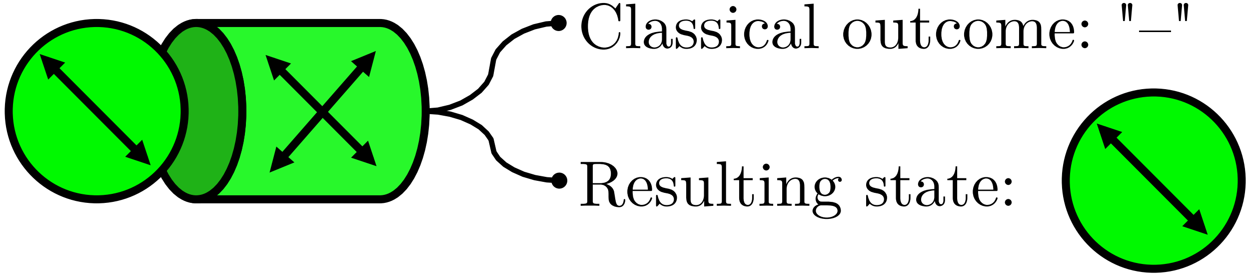
We can *measure* a qubit in a *basis* and receive a *classical outcome*.

After measurement, the qubit *collapses* to a basis state.

Rules for measurement, part 1

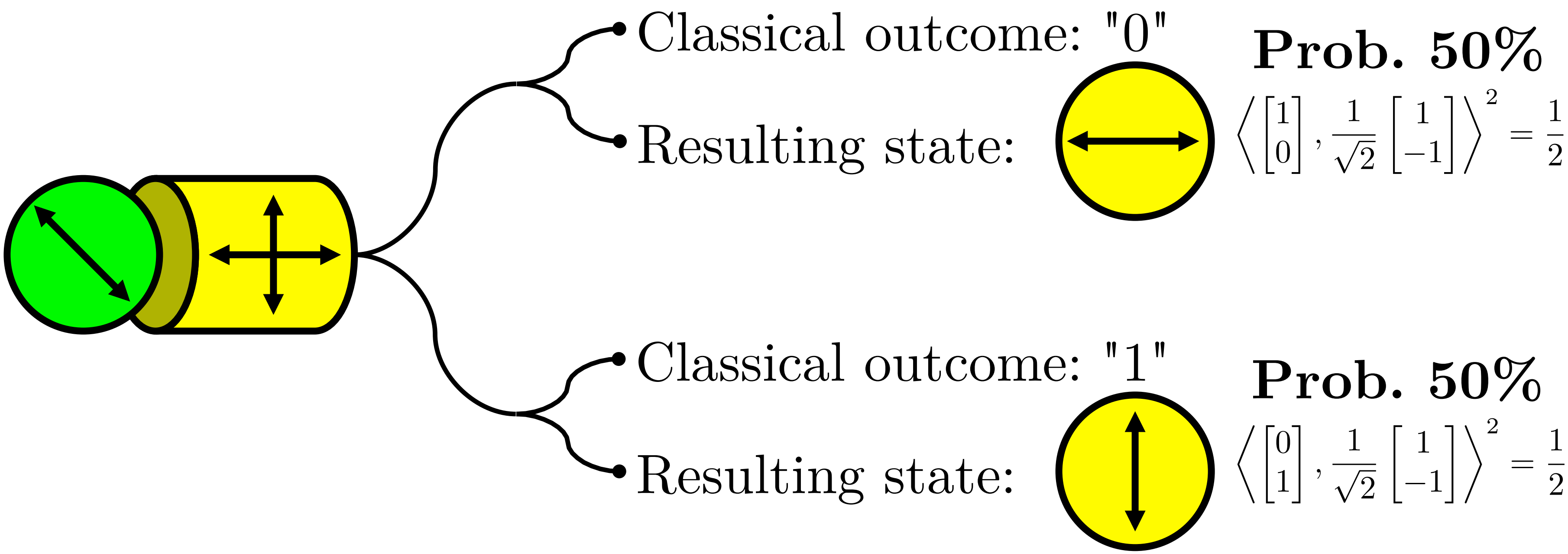
1. If we measure a basis state **in that basis**, then we get back that basis state with certainty.





Rules for measurement, part 2

2. If we measure a state **in a different basis**, then we get back either basis state with probability related to the size of the projection onto that basis state.



Another way of thinking about measurement and collapse

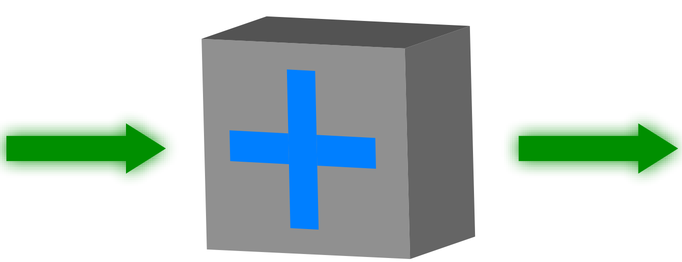
- Measurement device is a box with two perpendicular slots through it

- States are rotated line segments

Another way of thinking about measurement and collapse

- States have to be aligned to the slots to go through the box.

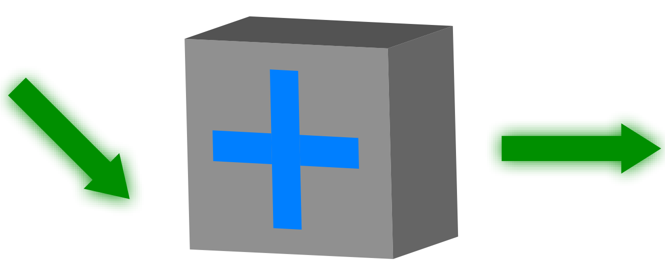
- If the state is already aligned, then it slides right through.



Another way of thinking about measurement and collapse

- States have to be aligned to the slots to go through the box.

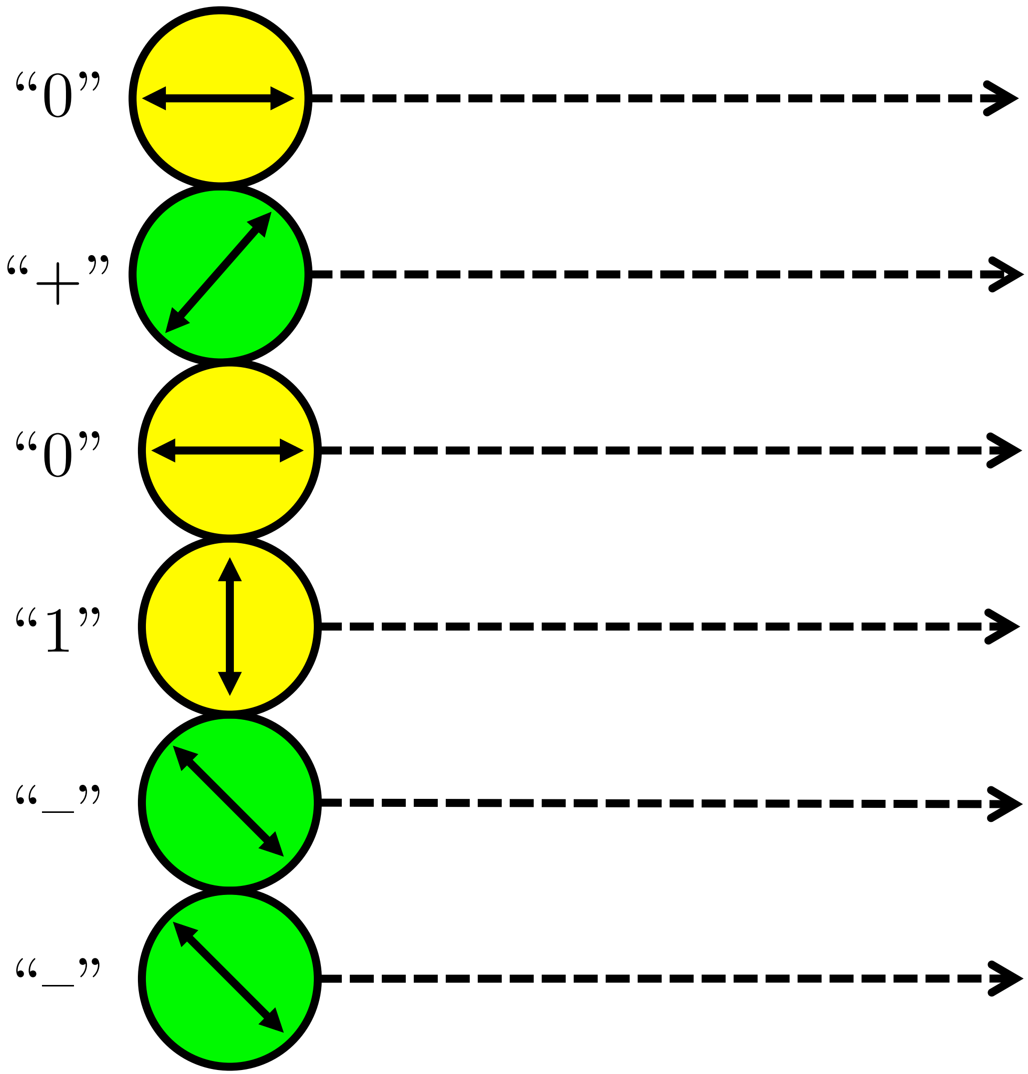
- If the state is **not aligned**, then it randomly "jiggles around" until it can slide through.



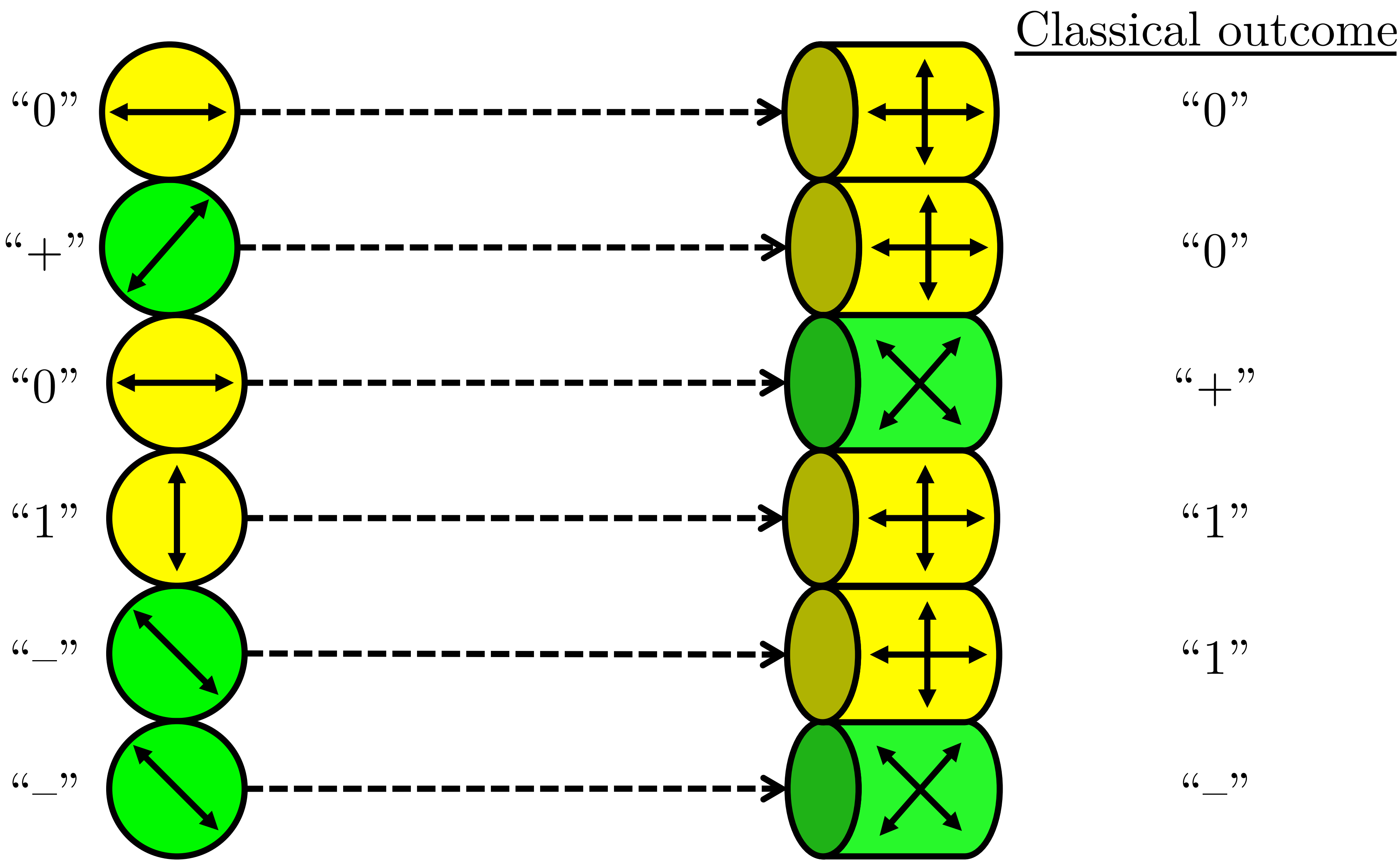
The closer the state starts off to being aligned with a slot, the more likely it is to collapse to that slot's alignment.

Basic QKD

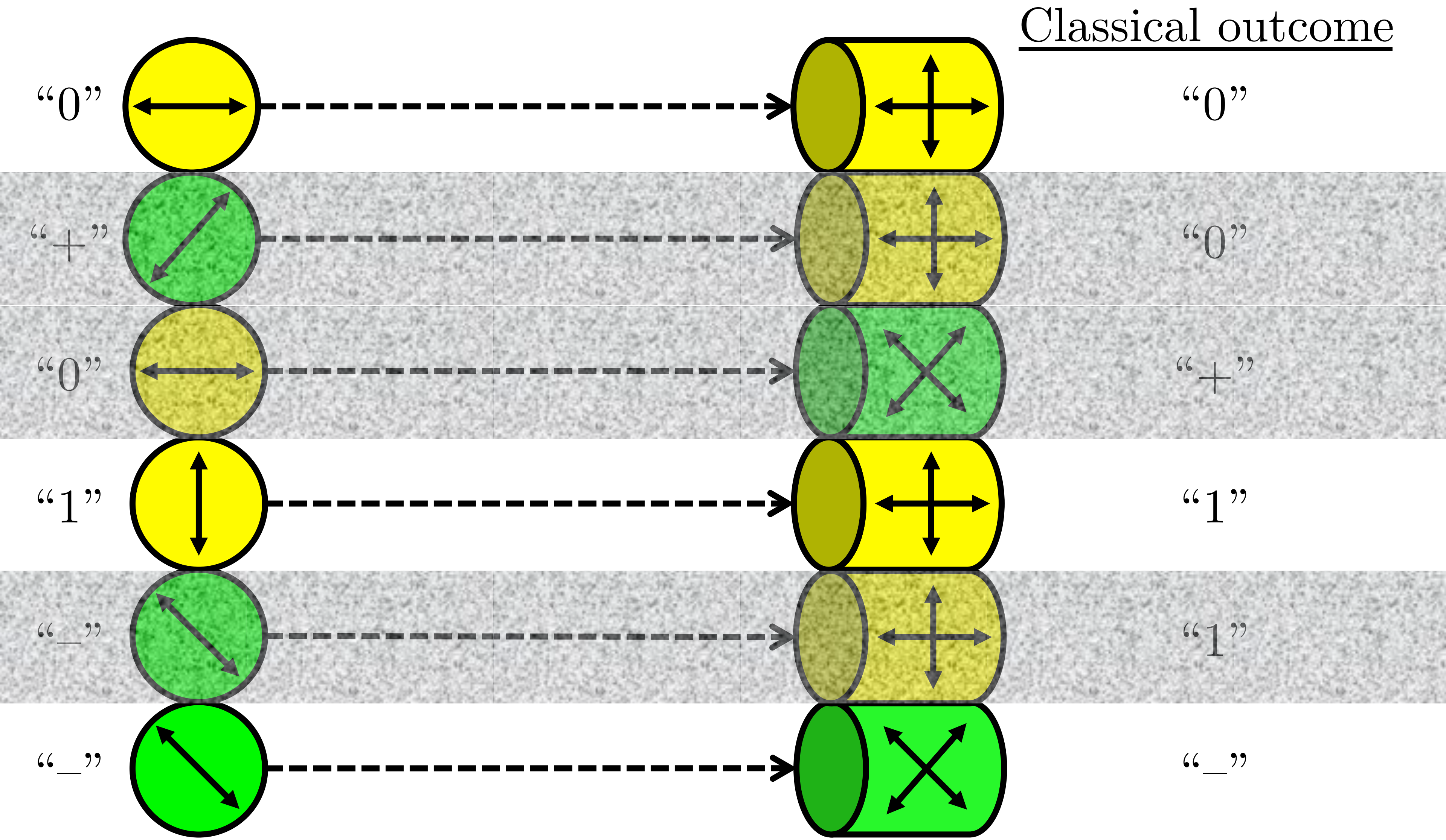
Step 1. Alice prepares random basis states and sends to Bob



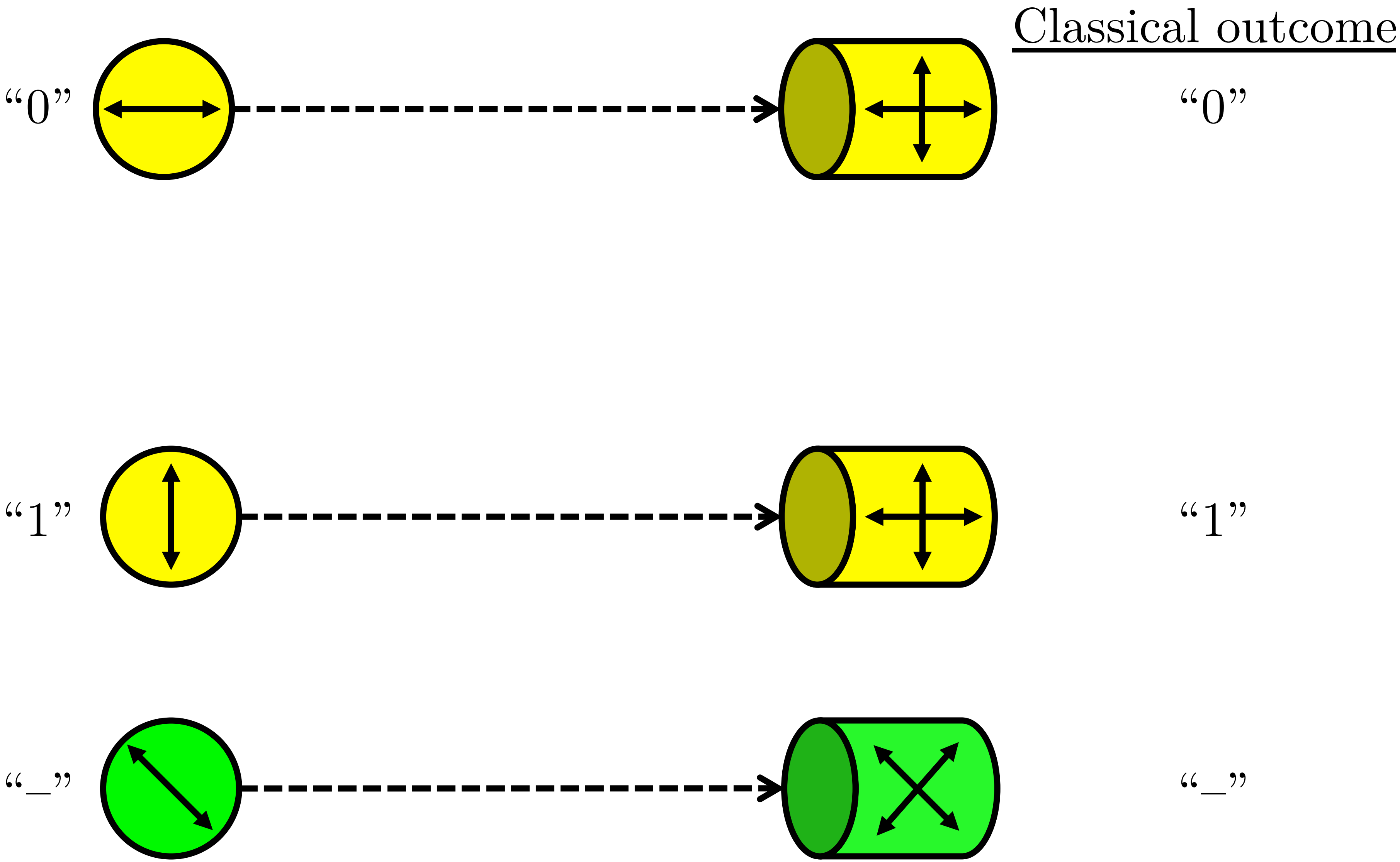
Step 2. Bob measures each qubit in a random basis



Step 3. Alice announces which basis she used for each qubit, Bob discards mismatching bases

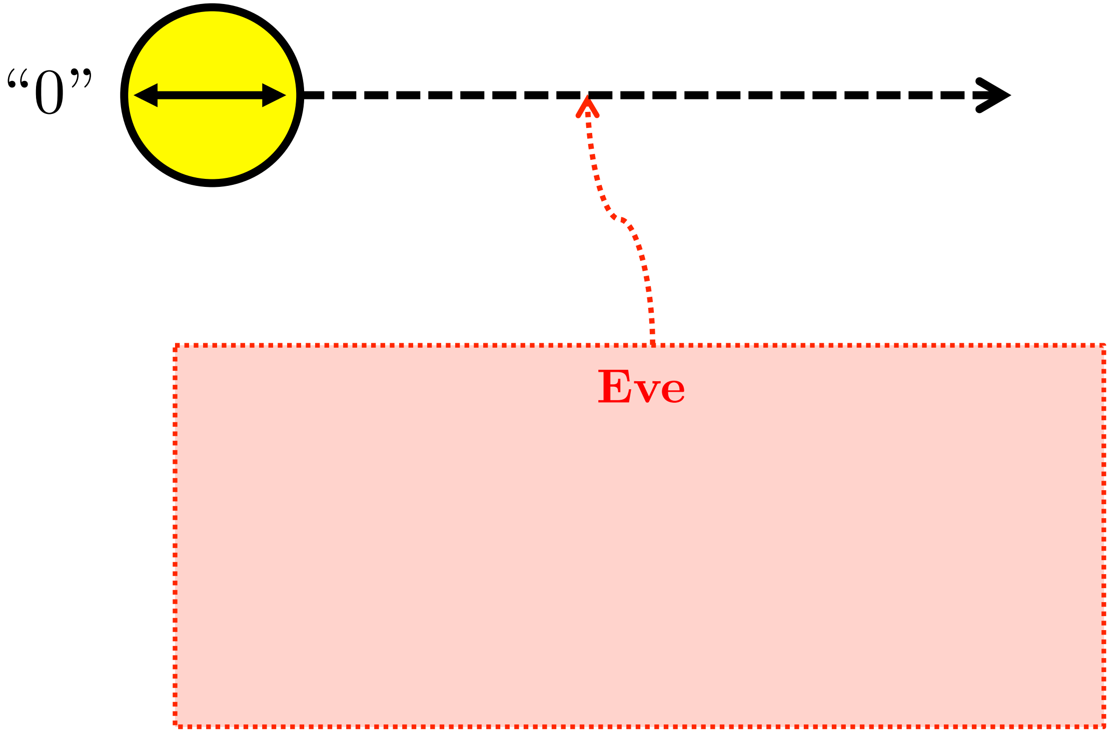


Result: Assuming a passive adversary and no noise, Alice and Bob share a secret key



Intercept-resend attack on basic QKD

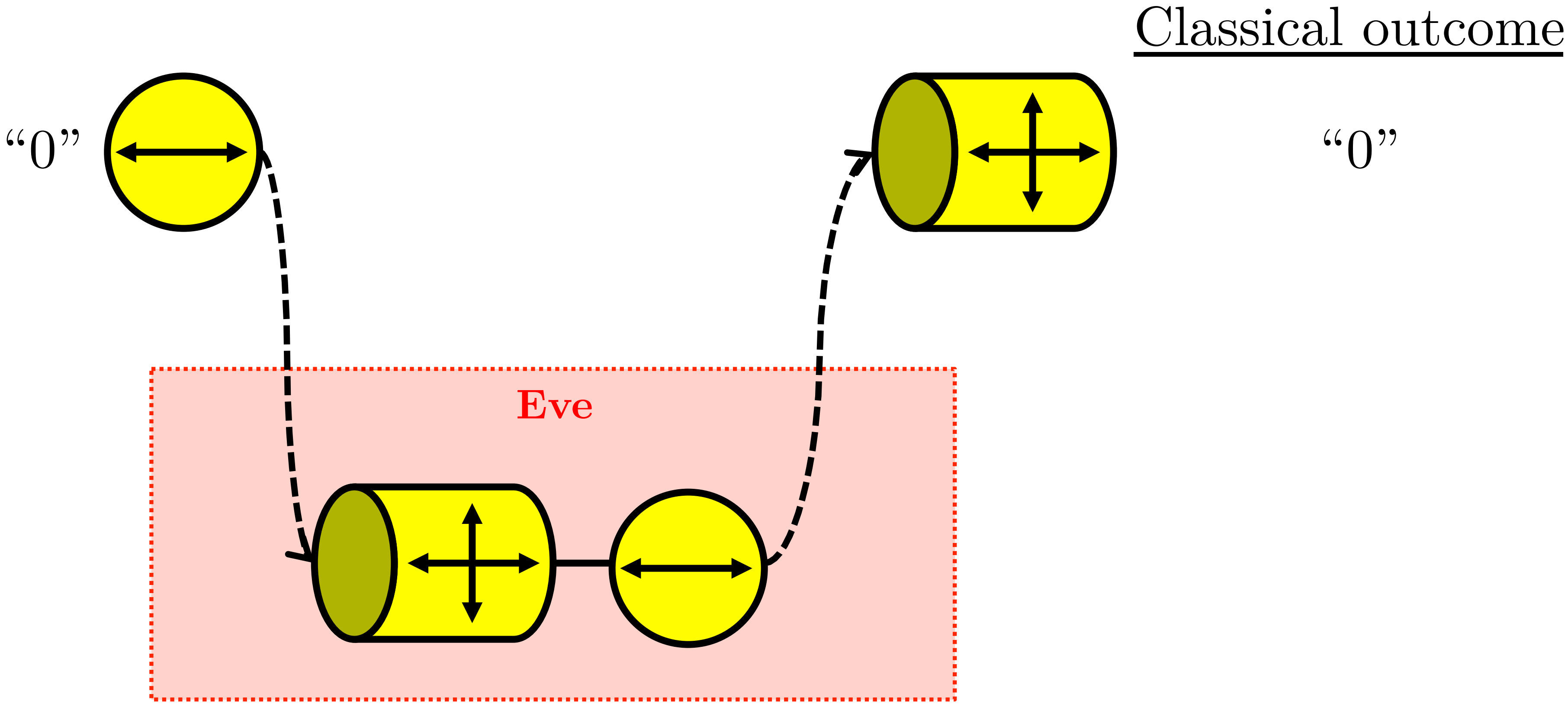
Attack model



Eve wants to learn some information about the state.

- Can’t tell which basis it’s in.
- Can only learn information by measuring.

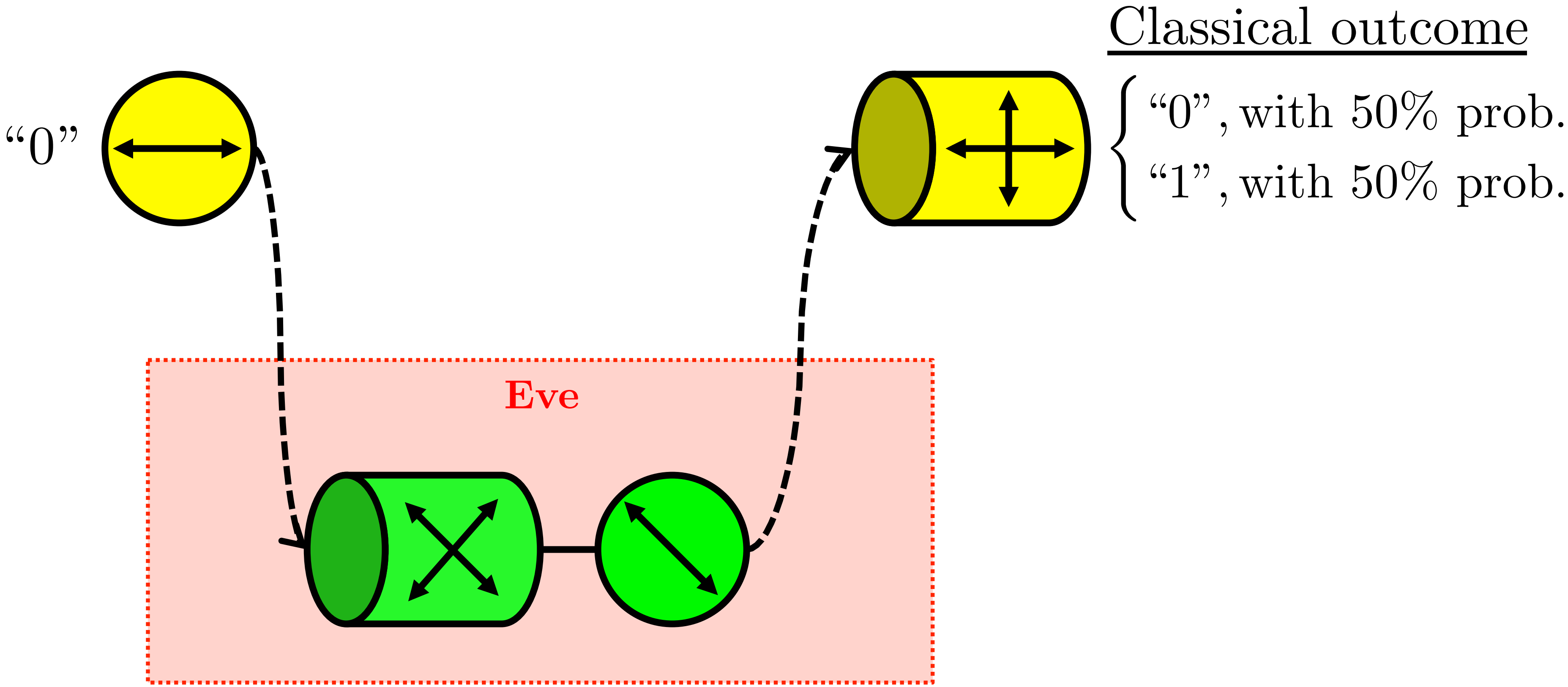
Intercept-resend attack



Eve guesses a basis to measure in,
then sends the resulting state to Bob.

- If Eve guesses **correctly**, she's undetectable.

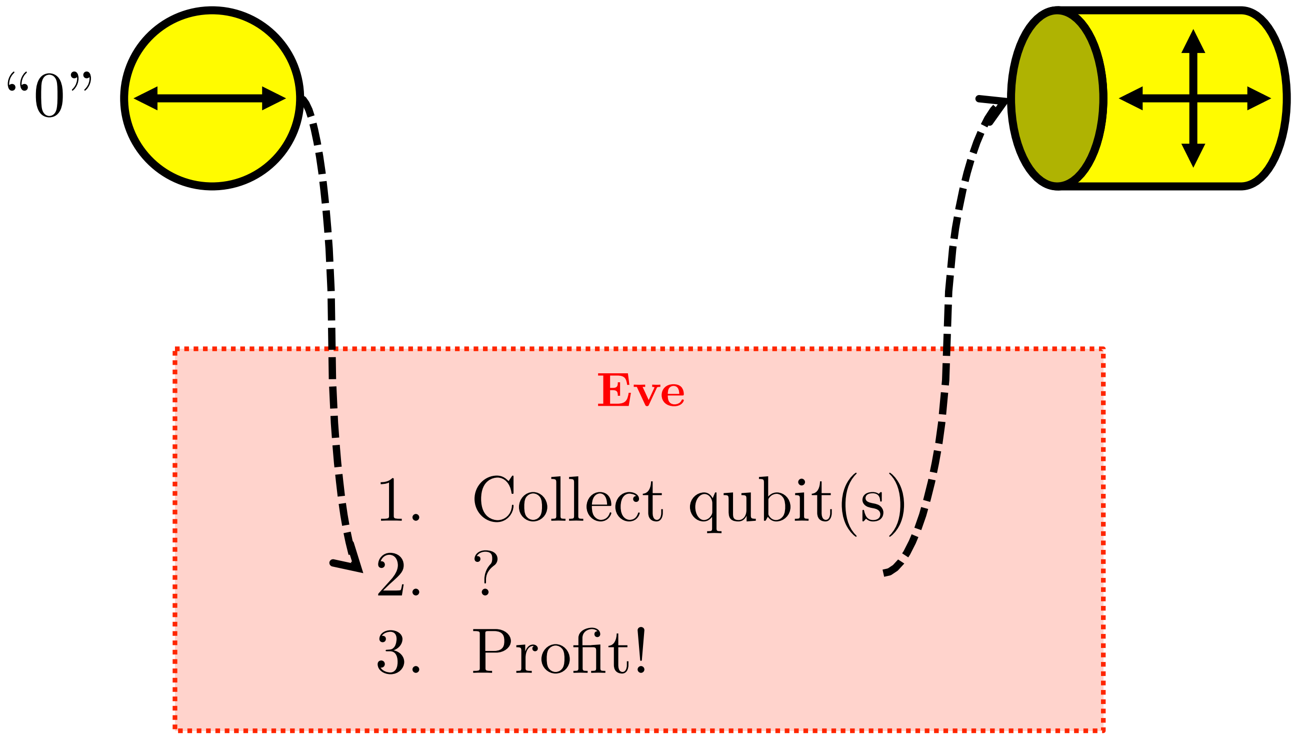
Intercept-resend attack



Eve guesses a basis to measure in,
then sends the resulting state to Bob.

- If Eve guesses **incorrectly**, she's detectable with 50% pr.

General attack



Classical outcome

something imperfect

Eve could try more clever attacks,
but will **always be detectable** with decent probability.

Uncertainty principle for qubits

- If you measure a qubit in the correct basis, you get the correct result.
- If you measure a qubit in the wrong basis, you get a random result.
- If you don't know the basis and try to gain information, you'll disturb the state with probability ¼.

Fundamental principle of QKD

information gain by adversary

=>

disturbance of state

=>

detection by Alice and Bob

BB84

Bennett–Brassard 1984

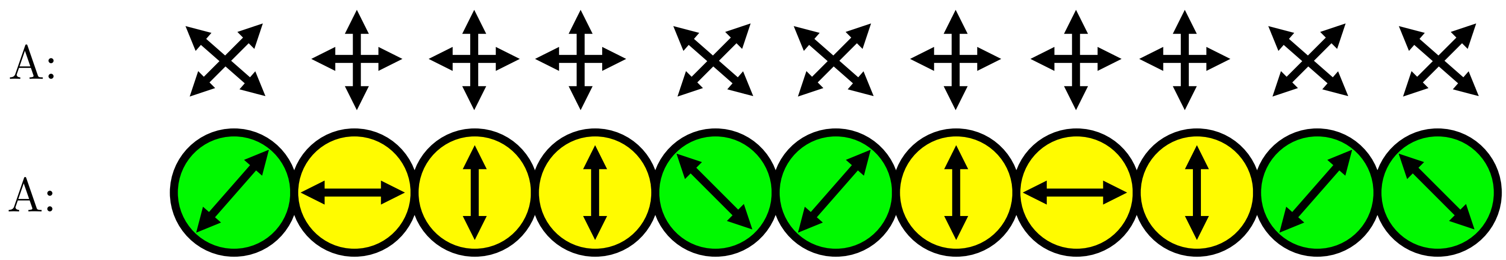
BB84 protocol

- The first QKD protocol.

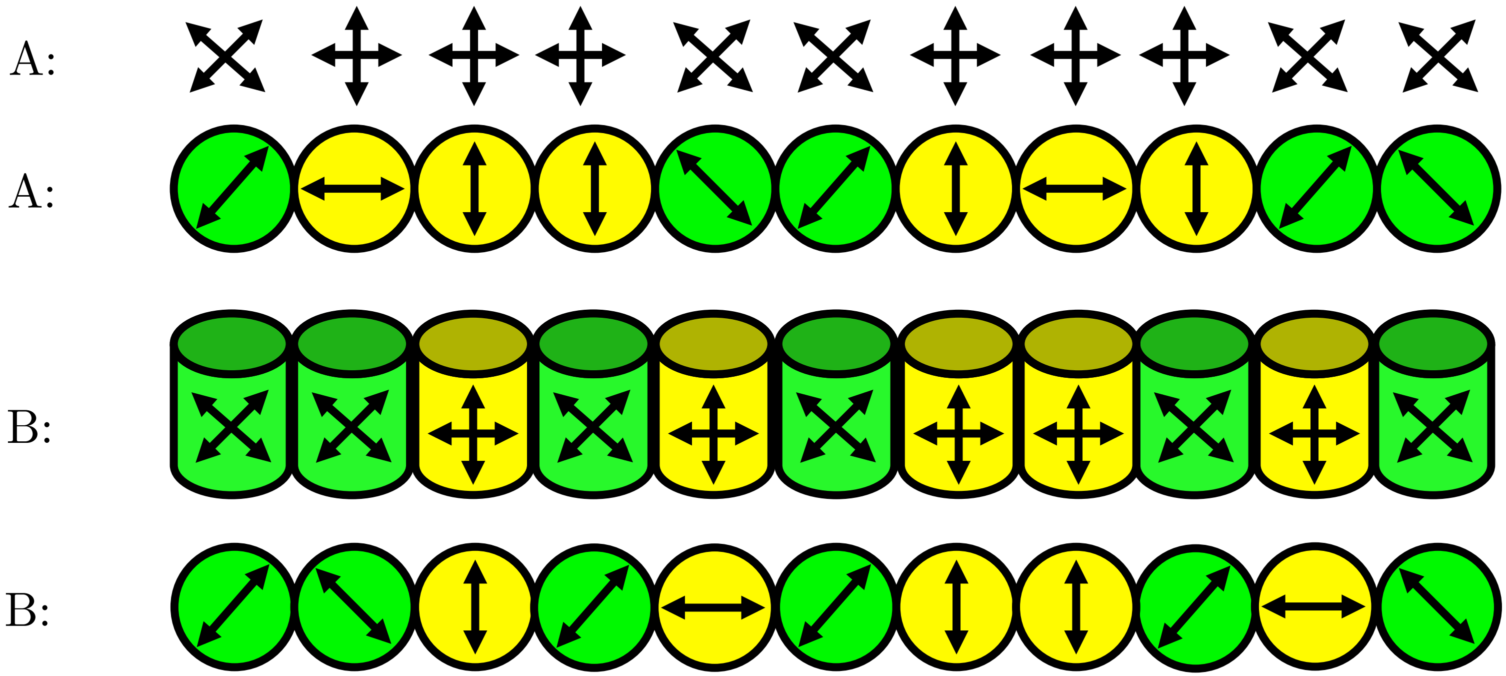
- Builds on basic QKD protocol, but with steps to detect an active adversary and to recover from noise.

[BB84] Charles H. Bennett and Gilles Brassard. Quantum cryptography: public key distribution and coin tossing. In *Proc. IEEE International Conf. on Computers, Systems and Signal Processing*, pp. 175–179. IEEE, December 1984.

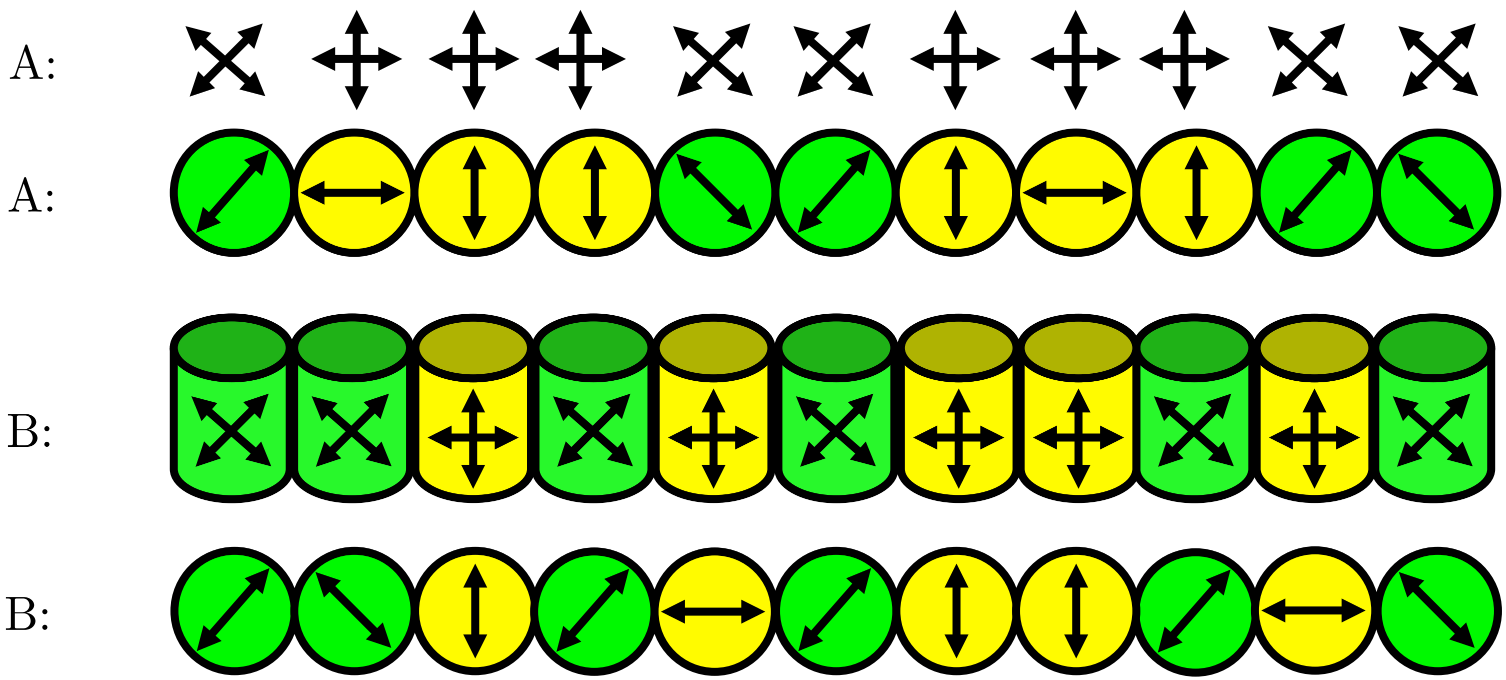
Step 1. Alice prepares $4n$ random qubits and sends them to Bob.



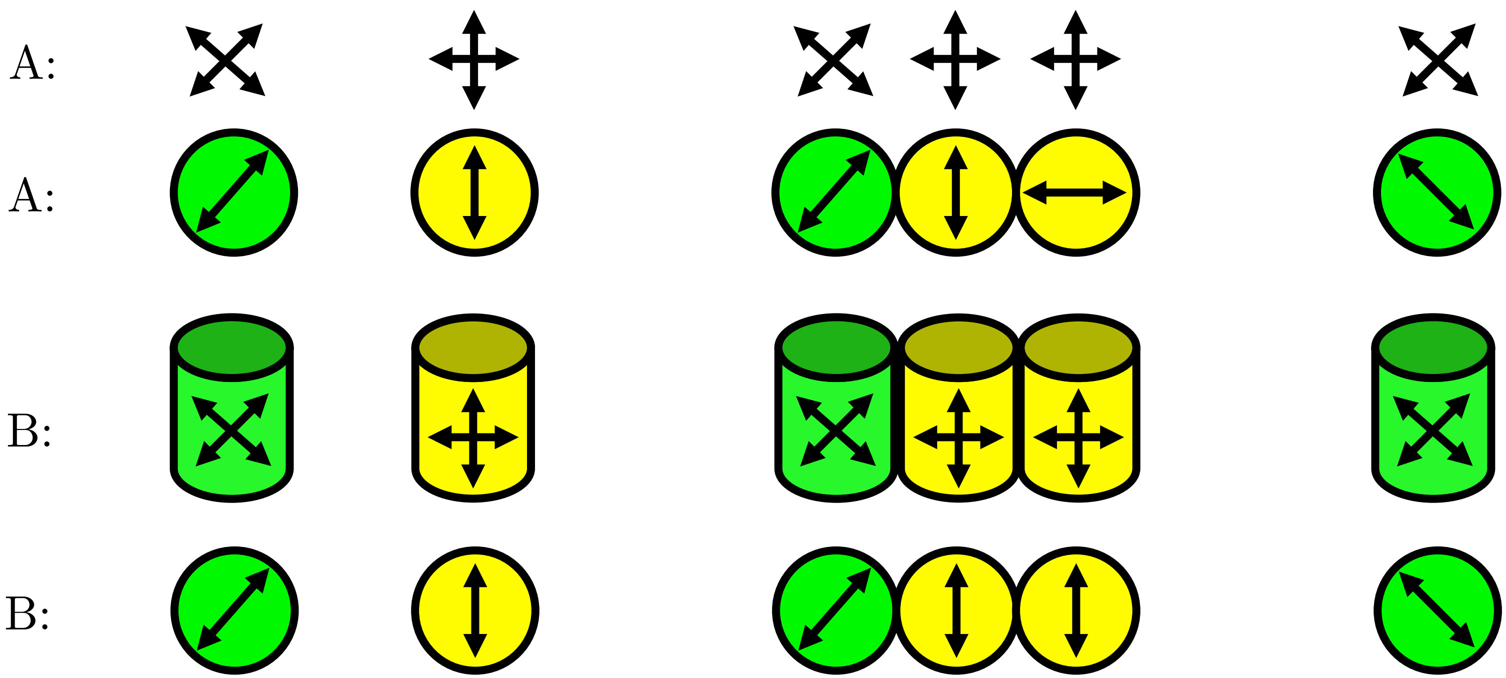
Step 2. Bob measures each qubit in a randomly chosen basis.



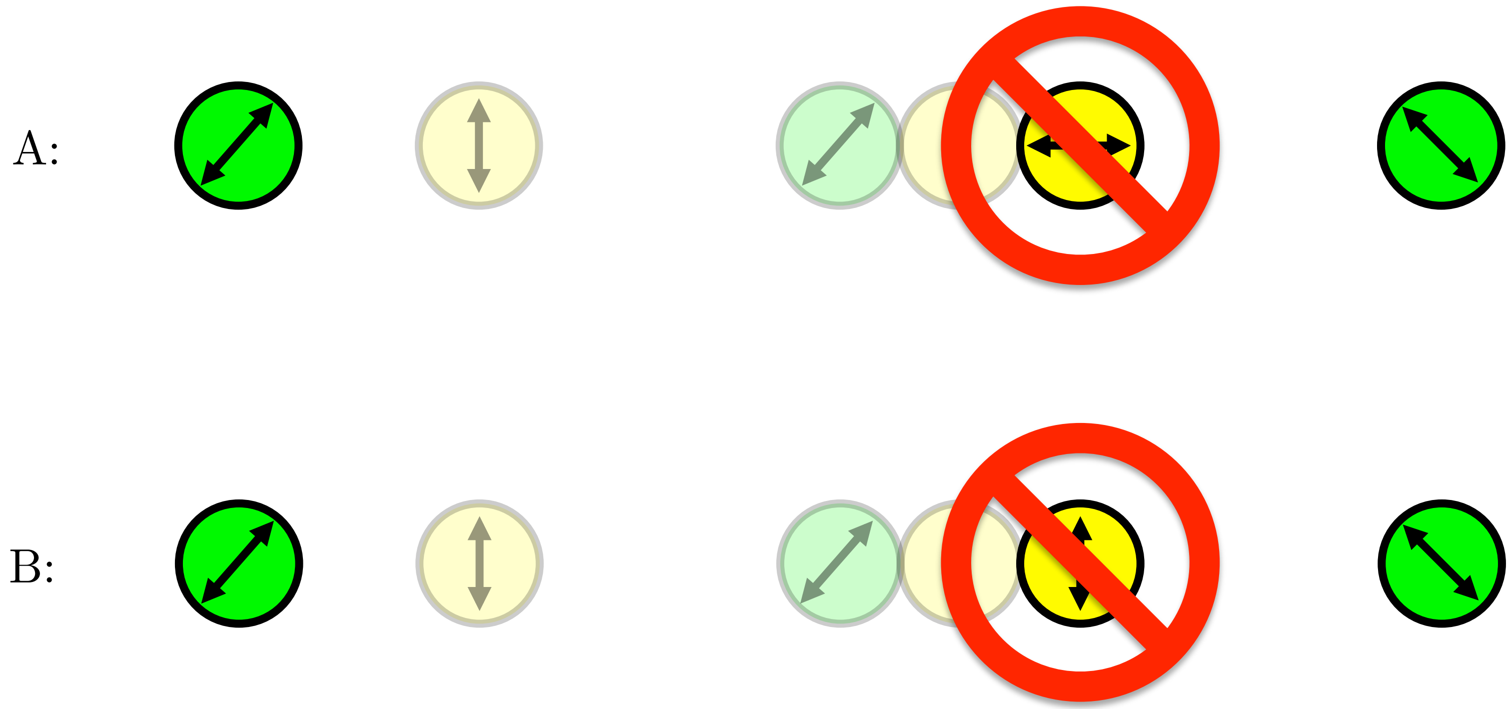
Step 3. They announce bases & discard mismatching bases ~2n.



Step 3. They announce bases & discard mismatching bases ~2n.



Step 4. They randomly pick half remaining qubits (n), announce the values, and see if they match.



Something bad happened here: either noise or eavesdropper.

Step 5.

If they find a place where the results don't match, they can:

a. abort and start over
b. try to salvage the unused half (n) of the remaining qubits:
    i. Figure out how much information and eavesdropper could have learned based on how many mismatches there are.
    ii. Do error correction on the unused remaining qubits.
    iii. Compress out the amount of information the eavesdropper could have learned.
    iv. Output: a shared secret key

BB84 protocol

1. Alice sends random qubits to Bob.
2. Bob measures in a random basis.
3. They see when they used the same basis.
4. They check how much information an eavesdropper could have learned.
5. They correct any errors, then process the remaining qubits to squeeze out the eavesdropper's information.

quantum

classical processing

Entanglement-based QKD

Two-qubit systems

- We can put two qubits next to each other to create a 2-qubit system:

$$|\,0\,\rangle_A \otimes |\,1\,\rangle_B = |\,01\,\rangle$$

- Algebraically, this corresponds to the *tensor product*.
- A 2-qubit system is a norm-1 vector in a **4**-dimensional complex vector space.

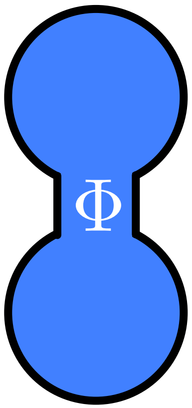
Non-separable states

There exist norm-1 vectors in $\mathbb{C}^4$ that cannot be constructed simply by putting two qubits next two each other.

$$\frac{1}{\sqrt{2}}\begin{bmatrix}1\\0\\0\\1\end{bmatrix}$$ is not the tensor product of any norm-1 vectors in $\mathbb{C}^2$

Entangled states

$$|\,\Phi^+\,\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix}1\\0\\0\\1\end{bmatrix}$$



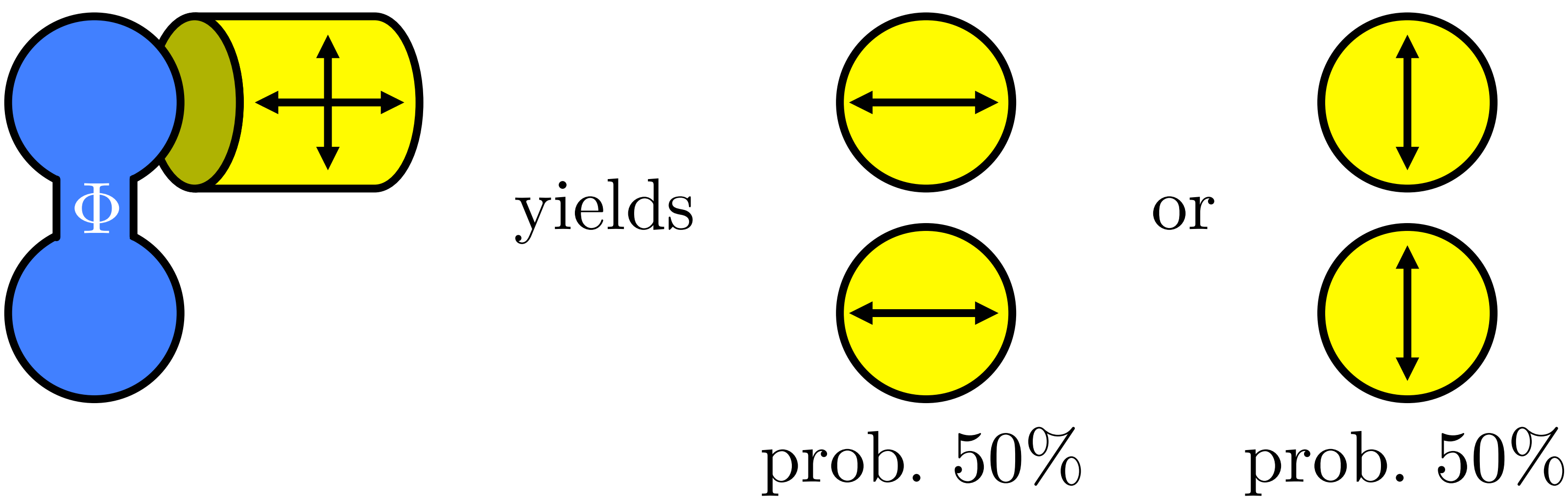
$$= \frac{|\,0\,\rangle_A \otimes |\,0\,\rangle_B + |\,1\,\rangle_A \otimes |\,1\,\rangle_B}{\sqrt{2}}$$

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

Called a *Bell state* or an *EPR pair*.

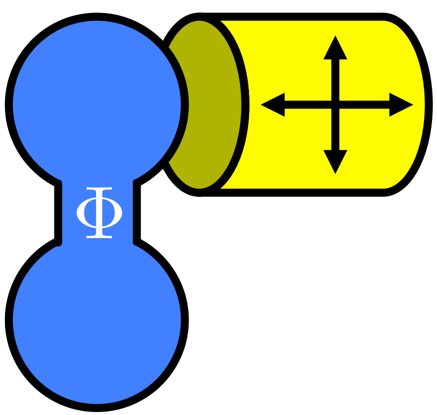
Rules for measurement, part 3

3. Measuring one of the two qubits in an entangled state collapses the whole state.

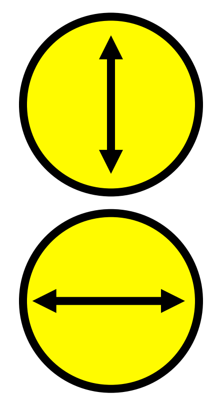


Rules for measurement, part 3

3. Measuring one of the two qubits in an entangled state collapses the whole state.



never yields



prob. 0%

Rules for measurement, part 3

3. Measuring one of the two qubits in an entangled state collapses the whole state.

$$|\,\Phi^+\,\rangle = \frac{|\,00\,\rangle + |\,11\,\rangle}{\sqrt{2}} \quad \text{yields} \quad \begin{cases} |\,00\,\rangle = |\,0\,\rangle_A \otimes |\,0\,\rangle_B\,, \text{with prob. } 50\% \\ |\,11\,\rangle = |\,1\,\rangle_A \otimes |\,1\,\rangle_B\,, \text{with prob. } 50\% \end{cases}$$

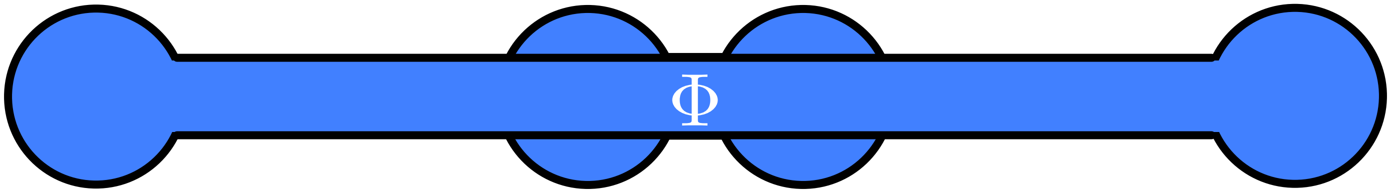
Entanglement-based QKD
Ekert 91 Protocol

- Alice and Bob each *receive* one half of an entangled pair and measure.

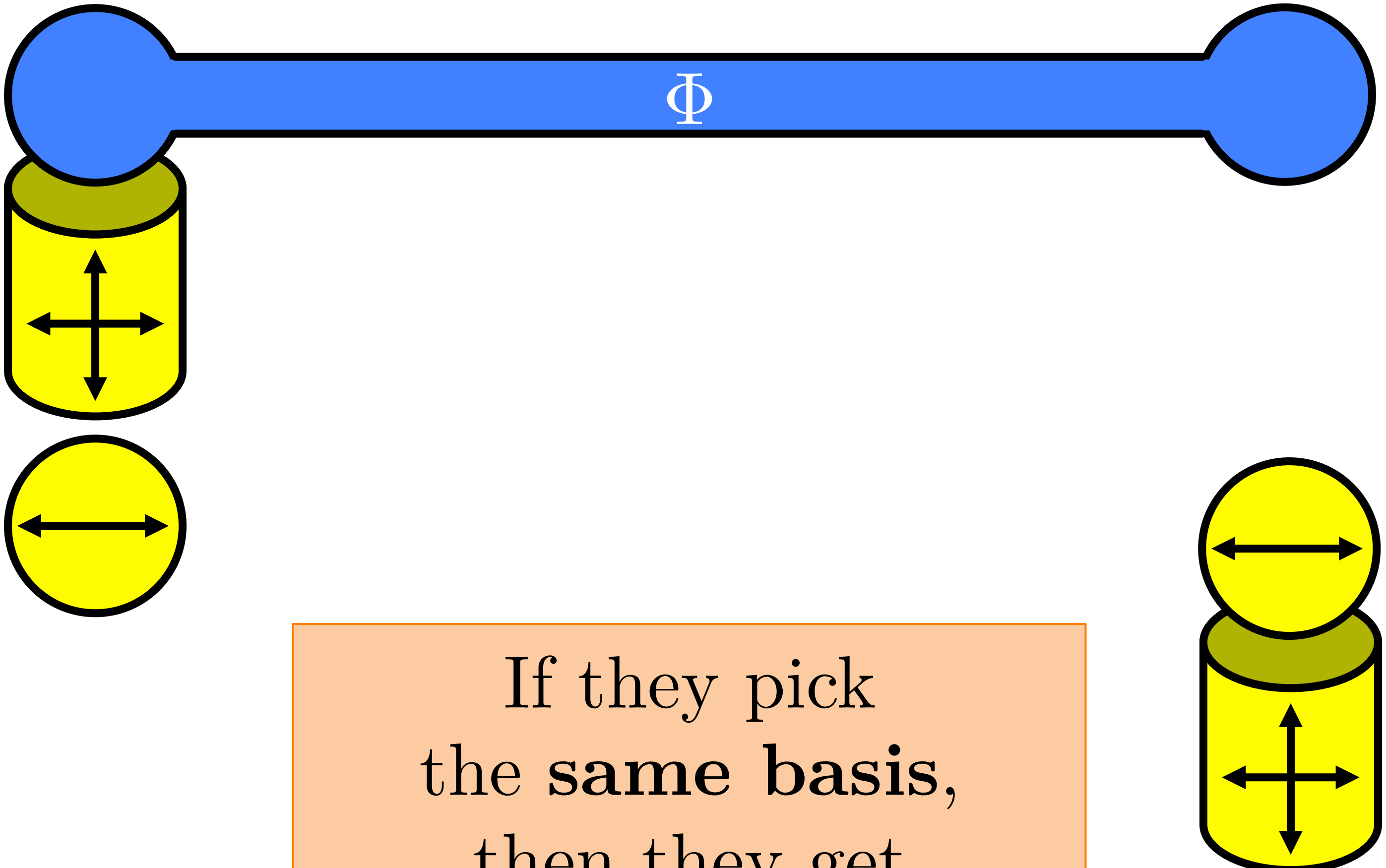
- Secure even if the adversary prepares the supposedly entangled pairs.

[Eke91] Artur K. Ekert. Quantum cryptography based on Bell's theorem. *Physical Review Letters*, **67**:661–663, August 1991. DOI:10.1103/PhysRevLett.67.661.

Step 1. A Bell pair is prepared and sent to Alice and Bob.



Step 2. Alice and Bob each pick a random basis and measure.



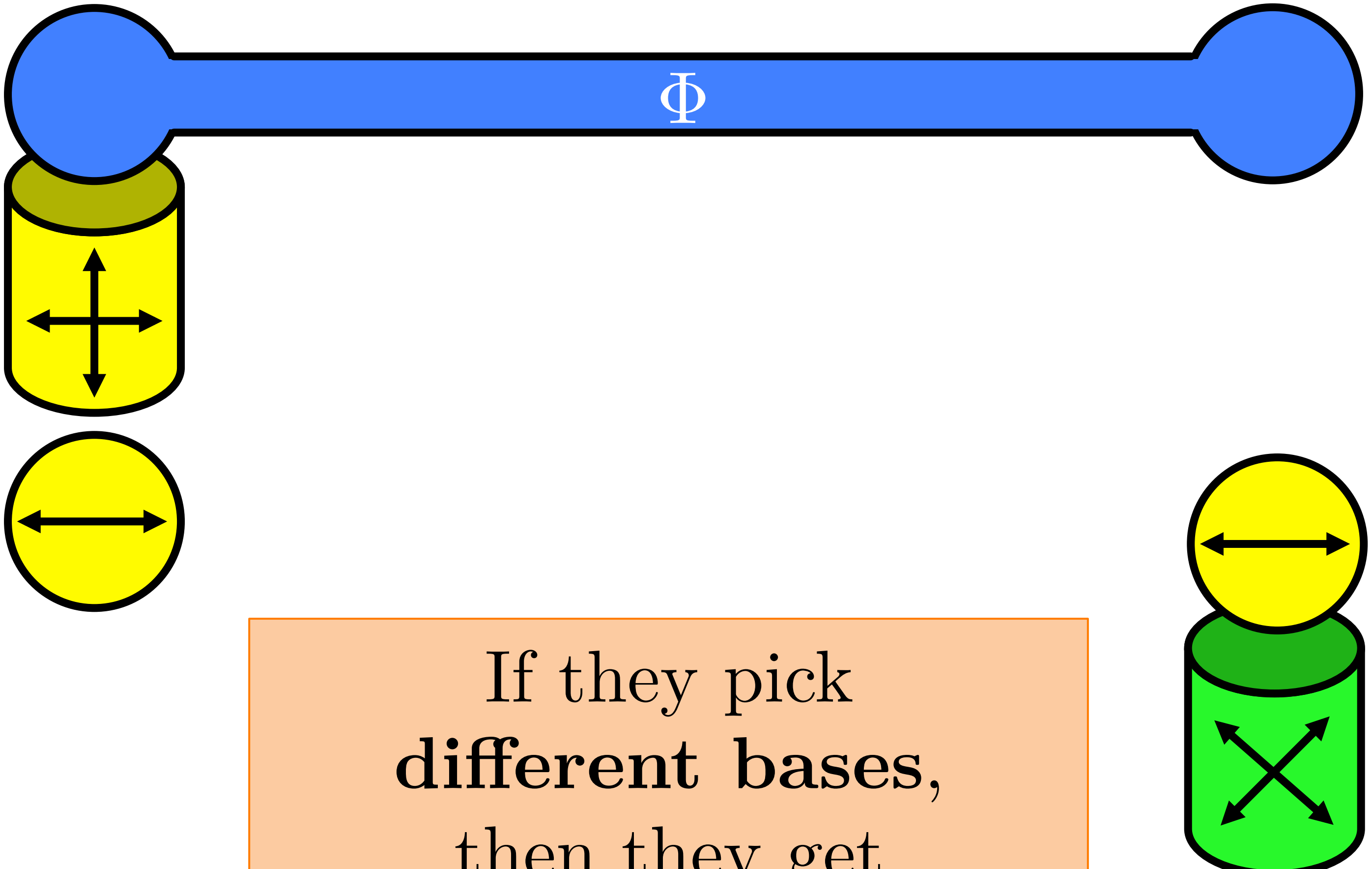
If they pick
the **same basis**,
then they get
the **same result**.

Classical
outcome

“0”

“0”

Step 2. Alice and Bob each pick a random basis and measure.



If they pick **different bases,** then they get **uncorrelated results.**

Classical <u>outcome</u> "0" "+"

Ekert 91 protocol

1. Alice and Bob receive (entangled) qubits.
2. Alice and Bob measure in a random basis.
3. They see when they used the same basis.
4. They check how much information an eavesdropper could have learned.
5. They correct any errors, then process the remaining qubits to squeeze out the eavesdropper's information.

quantum

classical processing

(Steps 3–5 same as in BB84.)

Monogamy of entanglement

- If two qubits are maximally entangled, then they cannot be correlated at all with a third qubit.

- If an eavesdropper has some information about Alice and Bob's qubits, then Alice and Bob's correlations are not maximal.

- This holds even if Eve prepares the entangled states!

Fundamental principle of QKD

information gain by adversary

=>

disturbance of state

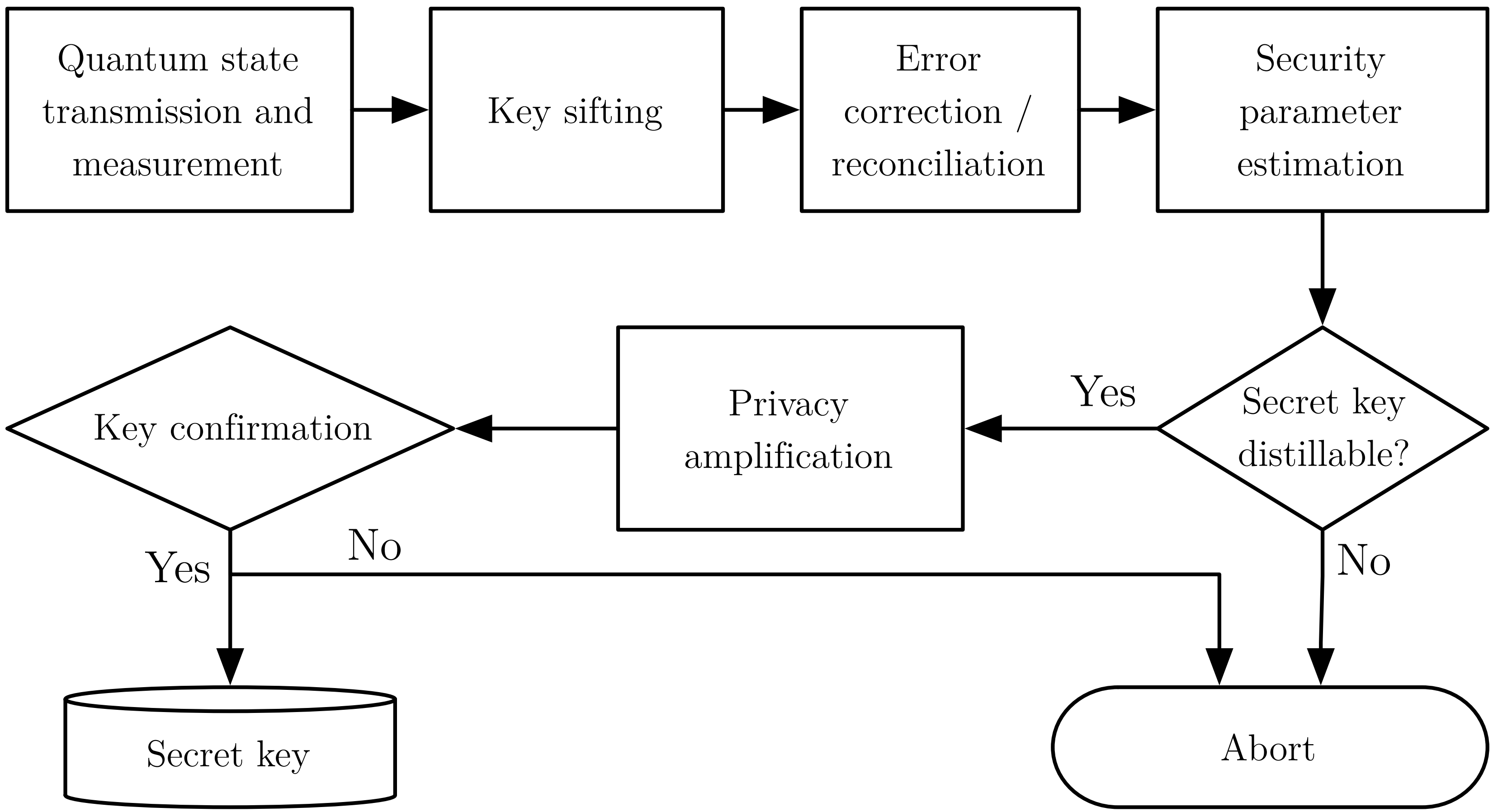
=>

detection by Alice and Bob

Classical Processing

sifting • error correction • parameter estimation • privacy amplification

Classical processing



Classical processing steps

1. Key sifting
   – Discard mismatching bases.

2. Error correction / reconciliation
   – one-way or two-way
   – e.g. low-density parity check codes
   – leaks partial information about the secret

3. Security parameter estimation
   – disclose a constant fraction of bits (doesn't need to be half as in basic QKD example)
   – obtain estimate of *quantum bit error rate* (QBER) e
   – can also be done as part of error correction / reconciliation

Classical processing steps

4. If quantum bit error rate is sufficiently small, use privacy amplification to distill secret key.
   - use random permutation and 2-universal hash function

2-universal hash functions

A family of *2-universal hash functions* is a set of hash functions $\mathcal{H}$ mapping a set U to bit strings of length r' if, for all $x, y \in U$ with $x \neq y$,

$$\Pr_{H \in \mathcal{H}} (H(x) = H(y)) \leq 2^{-r'} \quad .$$

For any distinct x and y, the proportion of functions in the family where x and y end up in the same bucket is ideally small.

2-universal hash functions

Fix r'. Let $U = \{0, 1, \ldots, 2^w - 1\}$, with $w > r'$. Let a be a randomly chosen positive odd integer with $a < 2^w$ and let $b = i2^{w/2}$ where i is chosen at random from $\{0, \ldots, 2^{w/2} - 1\}$. Define

$$H_{a,b}(x) = ((ax + b) \mod 2^w) \operatorname{div} 2^{w-r'}$$

where div denotes integer division. Then $\mathcal{H} = \{H_{a,b} : a, b \text{ as above}\}$ is a family of 2-universal hash functions.

[DHKP97] Martin Dietzfelbinger, Torben Hagerup, Jyrki Katajainen, and Martti Penttonen. A reliable randomized algorithm for the closest-pair problem. *Journal of Algorithms*, 25(1):19–51, 1997. DOI:10.1006/jagm.1997.0873.

2-universal hash functions for privacy amplification

Suppose Alice and Bob's check bits disagree on e proportion.

Assume Alice and Bob share an identical, partially secret binary string k_{AB} of n bits.

1. Alice chooses a random permutation P on n elements.
2. Alice chooses a random 2-universal hash function G mapping n bits to (approx.) $n(1-2h(e))$ bits.
3. Alice and Bob compute the shared secret as $k' = G(P(k_{\mathrm{AB}}))$.

Trade off between quantum bit error rate (QBER) and key rate

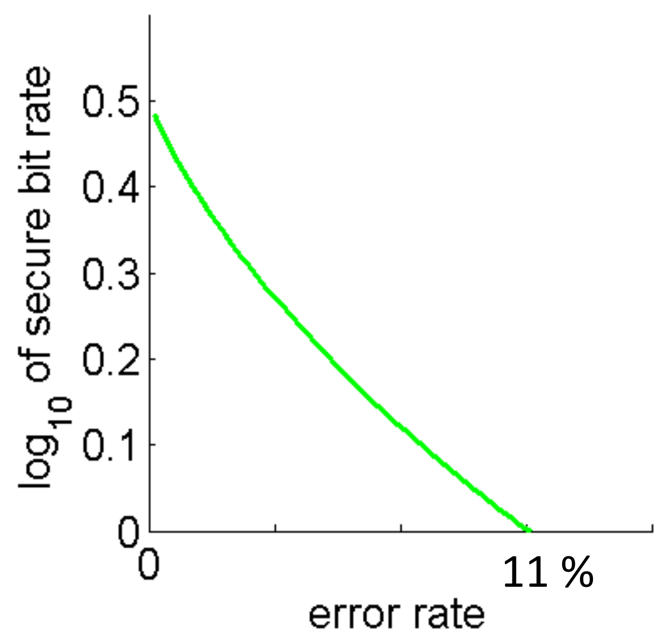
The *gain formula* gives the number of secure bits after error correction and privacy amplification per signal sent by Alice:

$$G = \frac{1}{2}\left(1 - h(e) - h(e)\right)$$

due to basis mismatch

due to error correction

due to privacy amplification



Norbert Lutkenhaus

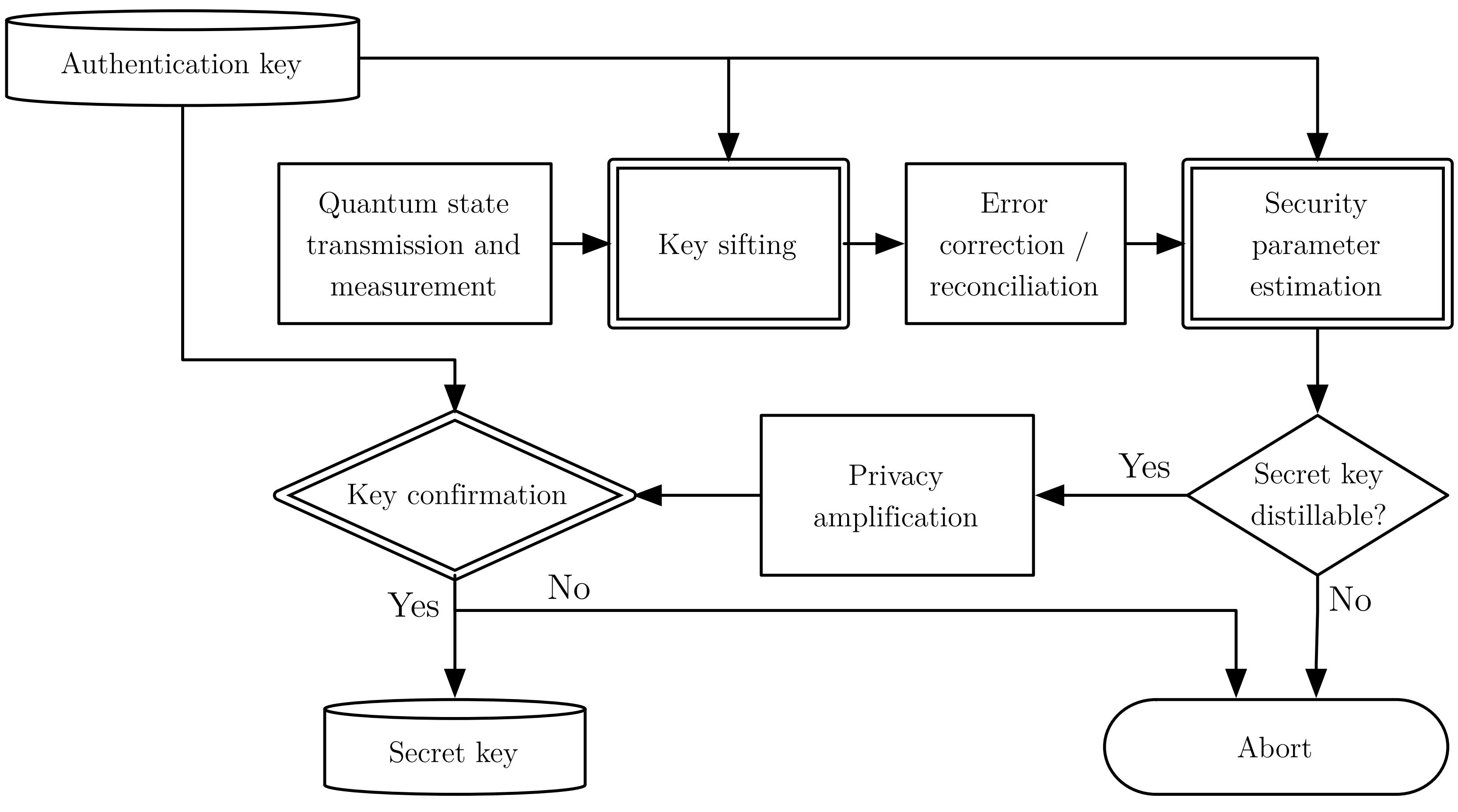
Authentication

information theoretic • computational

Authentication

- Like unauthenticated Diffie–Hellman key exchange, QKD requires its (classical) communication to be authenticated for security against active adversaries

Authenticating classical processing



Types of authentication

Information-theoretic

- Wegman–Carter message authentication code
- Secure against unbounded classical or quantum adversary
- Requires pre-shared symmetric key
- Consumes symmetric key

- QKD is "quantum key growing"

Computational

- Digital signatures or computationally secure message authentication codes
- Secure against adversaries who cannot break the authentication *at the time of the key exchange*

Wegman–Carter MAC

- Let k be a secret key.
- Let H be a 2-universal hash function.

- The *basic (one-time) Wegman–Carter MAC* is simply the application of a 2-universal hash function:
$$\mathrm{BasicWC}_k(m) = H_k(m)$$

[WC81] Mark N. Wegman and J. Lawrence Carter. New hash functions and their use in authentication and set equality. *Journal of Computer and System Sciences*, **22**(3):265–279, 1981. DOI:10.1016/0022-0000(81)90033-7.

Wegman–Carter MAC

- The *(full) Wegman–Carter MAC* is:

$$\mathrm{WC}_k(m) = k_1 \oplus H_{k_2}(m)$$

- This allows for partial reuse of key.

- More modern constructions as well, e.g., UMAC, which incorporate pseudorandom functions.

[BHK+99] J. Black, Shai Halevi, Hugo Krawczyk, T. Krovetz, and Phillip Rogaway. UMAC: Fast and secure message authentication. In Michael Wiener, editor, *Advances in Cryptology – Proc. CRYPTO '99*, LNCS, volume 1666, pp. 216–233. Springer, 1999. DOI:10.1007/3-540-48405-1_14.

Security of QKD

Informal theorem

Thm. If

- quantum mechanics is correct, and
- authentication is secure, and
- our devices are secure,

then with high probability the key established by quantum key distribution is a random secret key independent (up to a negligible difference) of input values.

Security condition

- Let ρ_{ABE} be the joint state of Alice, Bob, and Eve after the protocol.

- Let $\rho_{UU} = \sum_{s\in\{0,1\}^\lambda} |\, s\,\rangle \otimes |\, s\,\rangle$ denote a uniformly distributed classical key (equal superposition of all computational basis states).

Security condition

The QKD protocol is *secure* if, for every adversary, there exists a state $\rho_{E'}$ such that

$$\text{real system } \rho_{ABE} \\ \approx \\ \text{random } AB\text{-key} \otimes \text{adversary state } \rho_{E'}$$

(adversary state is unentangled with the key)

Security condition

The QKD protocol is ϵ-*secure* if, for every adversary, there exists a state $\rho_{E'}$ such that

$$\frac{1}{2}\|\rho_{ABE} - \rho_{UU} \otimes \rho_{E'}\|_{\mathrm{tr}} \leq \epsilon$$

- $\|\cdot\|_{\mathrm{tr}}$ denotes the *trace* distance, roughly a quantum analogue of statistical distance
- No quantum process can ever distinguish these states with probability greater than ϵ

QKD security proofs

- First proofs by Mayers and Lo–Chau.
  - General idea: convert QKD into an entanglement distillation protocol then make use of monogamy of entanglement.
- QKD is universally composable.
- Many variants: imperfect devices, continuous variable QKD, one-way/two-way error correction, ...

[May96] Dominic Mayers. Quantum key distribution and string oblivious transfer in noisy channels. In *Advances in Cryptology – Proc. CRYPTO '96*, LNCS, volume 1109, pp. 343–357. Springer, 1996. DOI:10.1007/3-540-68697-5_26.
[LC99] Hoi-Kwong Lo and H. F. Chau. Unconditional security of quantum key distribution over arbitrarily long distances. *Science*, 283(5410):2050–2056, 1999. DOI:10.1126/science.283.5410.2050.
[BOHL+05] Michael Ben-Or, M. Horodecki, Debbie W. Leung, Dominic Mayers, and Jonathan Oppenheim. The universal composable security of quantum key distribution. In *Theory of Cryptography Conference (TCC) 2005*, LNCS, volume 3378, pp. 386–406. Springer, 2005. DOI:10.1007/b106171.

Using QKD keys

QKD is just one part of establishing secure communication, which requires:

- *key agreement*: two parties agree upon a shared private key
- *authentication*: prevents man-in-the-middle attacks
- *key usage*: key used for encryption using a one-time pad or a cipher like AES

Long-term security

QKD with information-theoretic authentication is information-theoretically secure.

QKD with computationally secure authentication is

- *computationally secure* against a quantum adversary at the time of protocol execution.
- *information-theoretically secure* against a bounded adversary at the time of protocol execution and a future unbounded adversary.

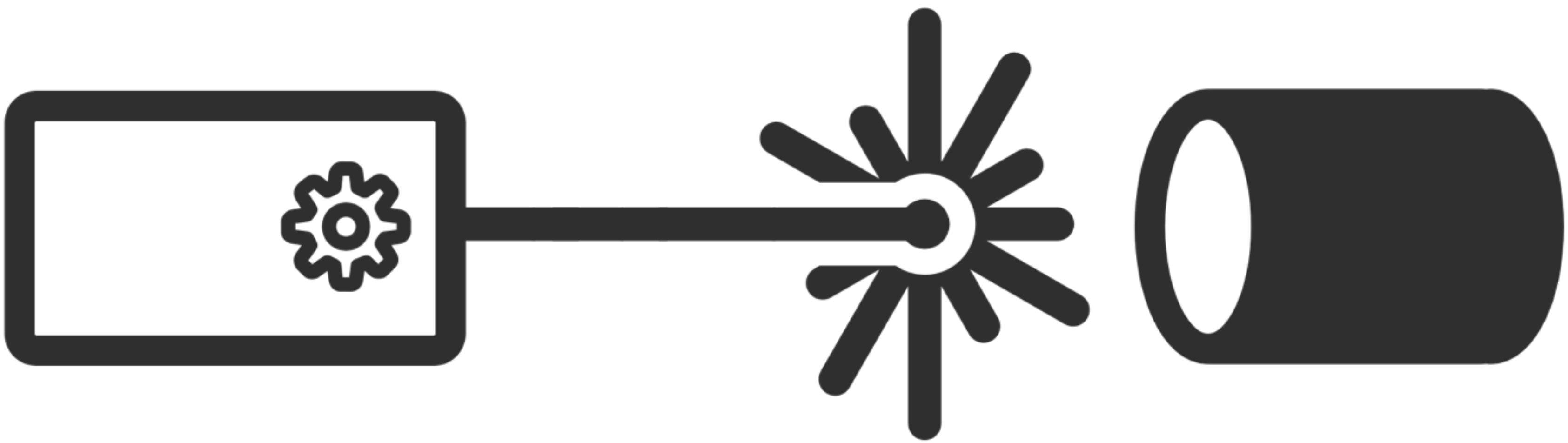
Complexity assumptions for long-term security

Protocol ingredients	Computational assumptions
Symmetric key authentication + QKD + one-time pad	No computational assumptions
Hash-based signatures + QKD + one-time pad	Short-term security of one-way function
Hash-based signatures + QKD + AES	Short-term security of one-way function + long-term security of AES
Trapdoor-based signatures + QKD + AES	Short-term security of trapdoor function + long-term security of AES
Trapdoor-based signatures + trapdoor-based key establishment + AES	Long-term security of trapdoor function + long-term security of AES

Classifying QKD schemes

prepare-send-measure • measure-only • prepare-send-only

Prepare-send-measure



- One party prepares states, sends them, the other party measures
- Examples: BB84, six-state protocol, ...
- Can reveal all local randomness after protocol execution *except* data bits

Measure-only

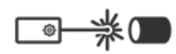
- Adversary prepares states, the parties measure
- Examples: Ekert 91 entanglement-based
- Can reveal all local randomness after protocol execution

Prepare-send-only

- Parties prepare states,
  the adversary (or a party) measures
- Can reveal all local randomness after protocol execution *except* data bits

[BHM96] Eli Biham, Bruno Huttner, and Tal Mor. Quantum cryptographic network based on quantum memories. *Physical Review A*, 54(4):2651–2658, 1996. DOI:10.1103/PhysRevA.54.2651.
[Ina02] Hitoshi Inamori. Security of practical time-reversed EPR quantum key distribution. *Algorithmica*, 34(4):340–365, 2002. DOI:10.1007/s00453-002-0983-4.

Classifying QKD systems

Protocol	Signed Diffie– Hellman [CK01]	`UP` [Ust09]	BB84 [BB84]	EPR [Eke91]	BHM96 [BHM96,Ina02]
Protocol type	classical	classical	quantum prepare-send-measure	quantum measure-only	quantum prepare-send-only
Classical key exchange Security model	CK01	eCK [LLM07]			
Randomness revealable **before** protocol run?	× static key × ephemeral key	at most 1 of static key, ephemeral key	× static key × basic choice × data bits × info. recon. × priv. amp.	× static key × basis choice × info. recon. × priv. amp.	× static key × basis choice × data bits × info. recon. × priv. amp.
Randomness revealable **after** protocol run?	✓ static key × ephemeral key	at most 1 of static key, ephemeral key	✓ static key ✓ basis choice × data bits ✓ info. recon. ✓ priv. amp.	✓ static key ✓ basis choice ✓ info. recon. ✓ priv. amp.	✓ static key ✓ basis choice × data bits ✓ info. recon. ✓ priv. amp.
Short-term security	computational assumption	computational assumption	computational or inf.-th.	computational or inf.-th.	computational or inf.-th.
Long-term security w/short-term-secure authentication	×	×	✓	✓	✓

Point-to-point implementations

fibre • free-space

Point-to-point implementations

- Most implementations based on polarization of photons

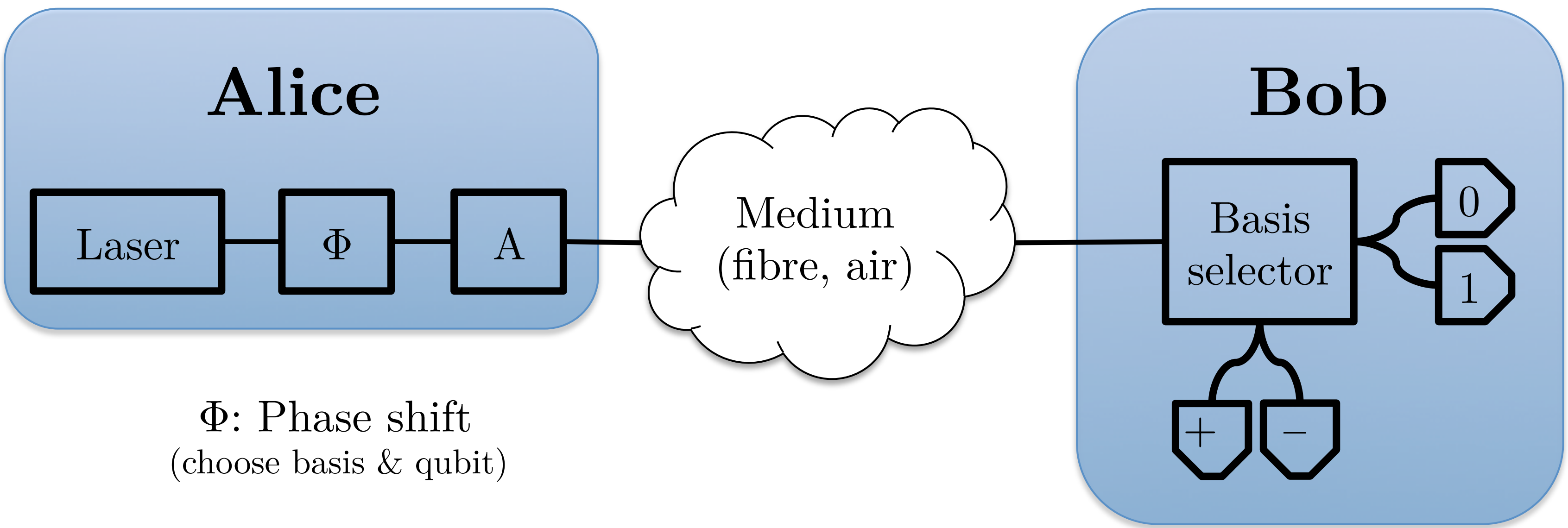
Fibre optics

- distance limited by fibre absorption
- noise from depolarization

Free space (air)

- distance limited by atmosphere
- noise from sun
- beam strays => telescopes

Basic BB84 implementation

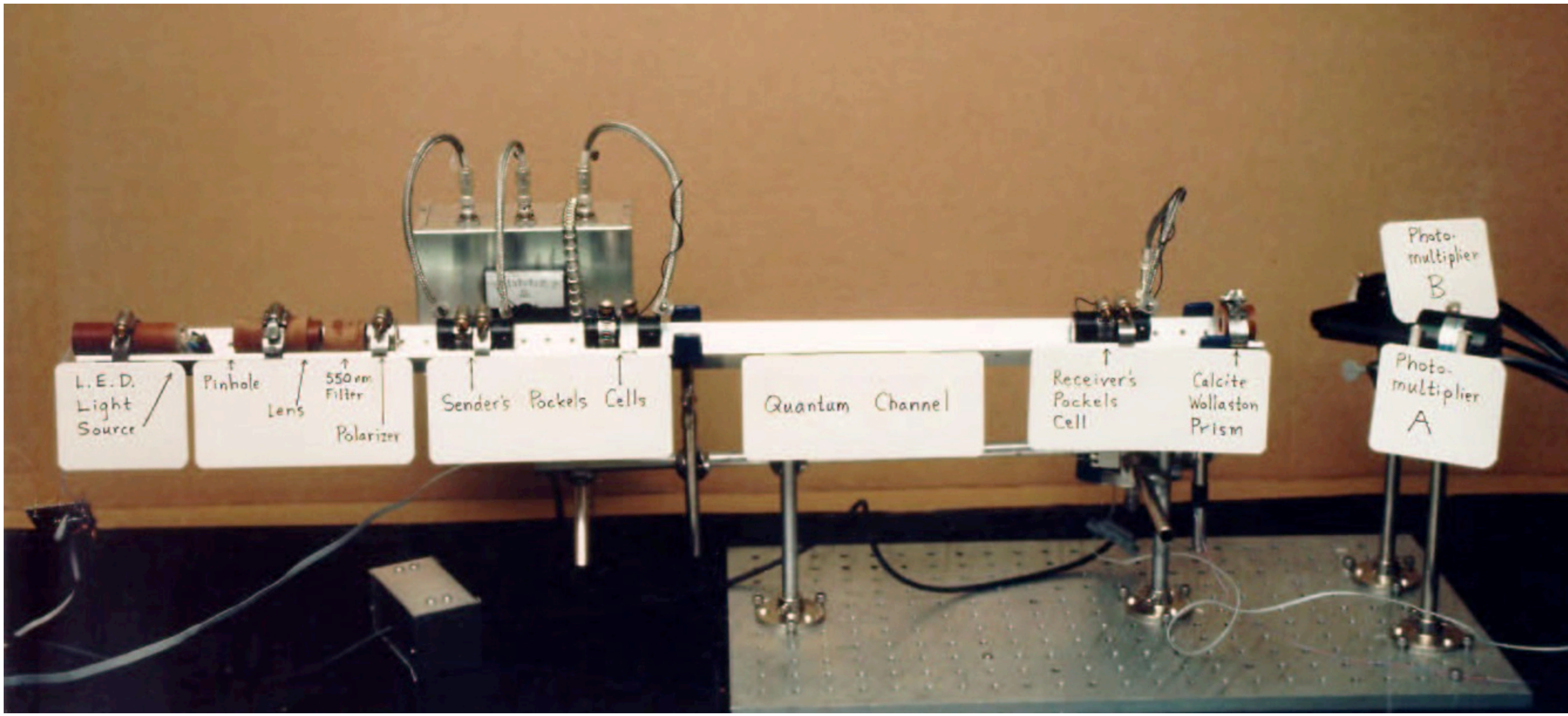


Φ: Phase shift
(choose basis & qubit)

A: Attenuator
($\leq$ 1 photon / pulse
with high prob.)

1 : Avalanche
photodetector

The first QKD implementation

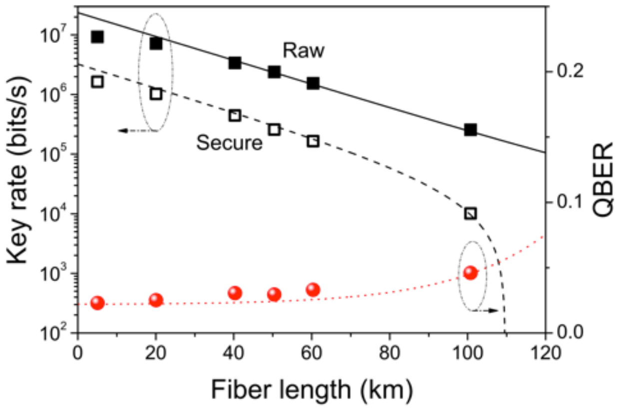


- IBM, 1984/1992

QKD in fibre optics

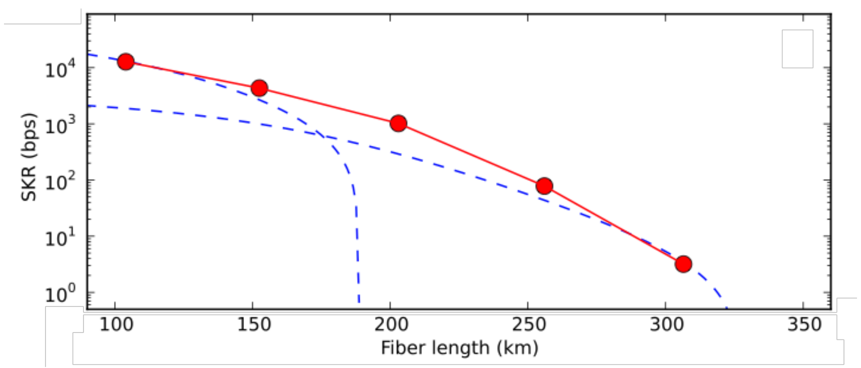
Speed

- 2008:
  - 1 Mbit/sec over 20km fibre
  - 10 Kbit/sec over 100km fibre



Distance

- 2014: 307km of fibre by U.Geneva and Corning

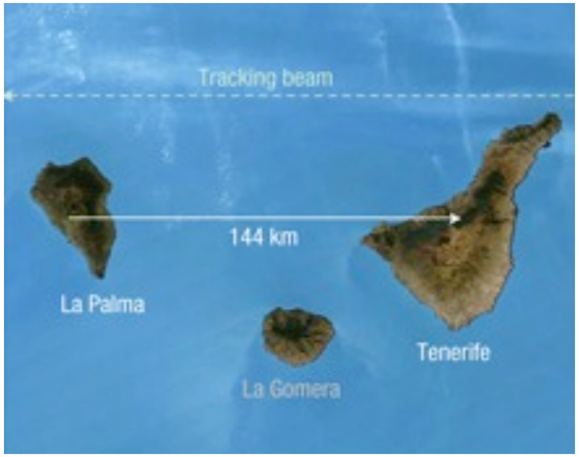


[DYD+08] A.R. Dixon, Z.L. Yuan, J.F. Dynes, A.W. Sharpe, A.J. Shields. Gigahertz decoy quantum key distribution with 1 Mbit/s secure key rate. *Optics Express*, 16(23):18790-18979, 2008.
[K+14] B. Korzh et al. Provably Secure and Practical Quantum Key Distribution over 307 km of Optical Fibre. arXiv:1407.7427, July 2014.

QKD in free space

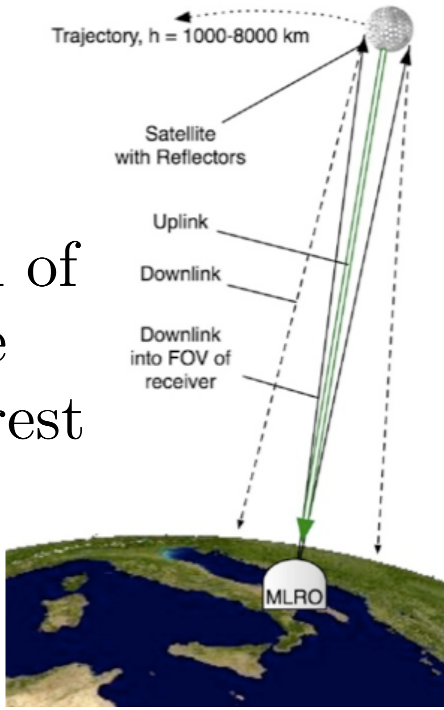
Distance

- 2007: 144km between two Canary Islands



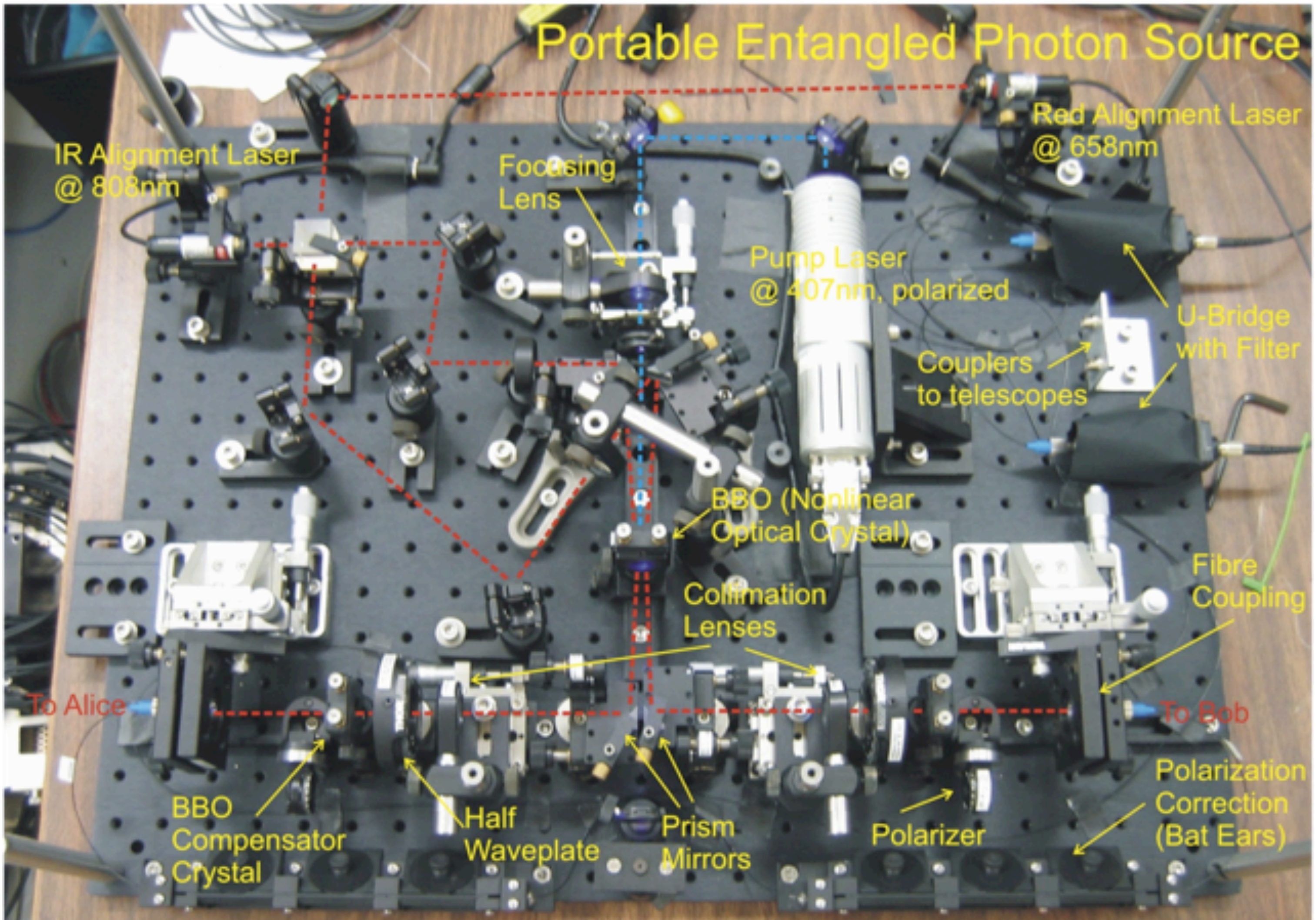
Satellite QKD

- Free-space distance limited by atmospheric interference
- Only a few km of air atmosphere above us, the rest is vacuum



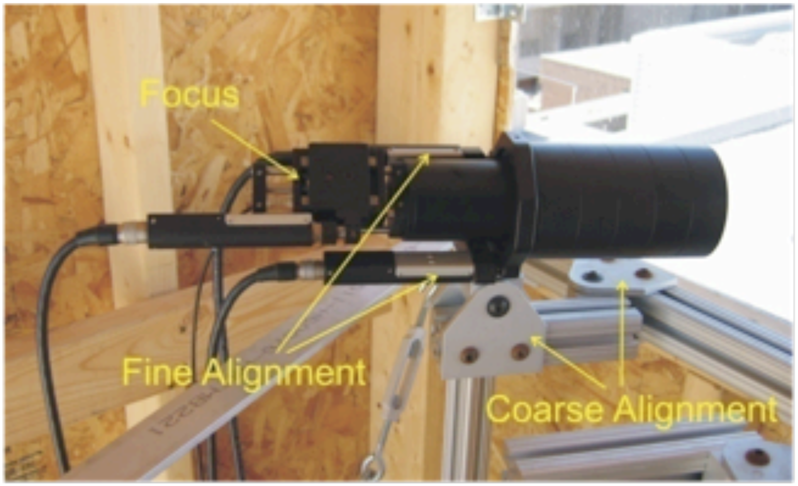
[U+07] R. Usrin et al. Entanglement-based quantum communication over 144 km. *Nature Physics* **3**:481–486, 2007.

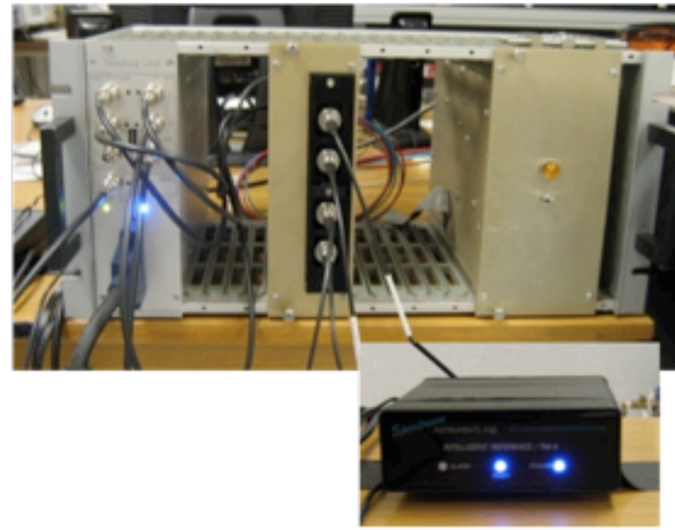
Entanglement-based source

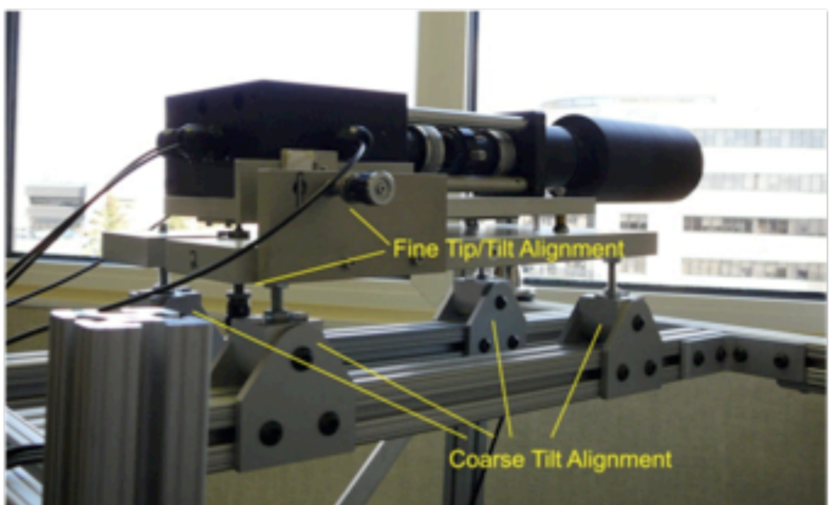


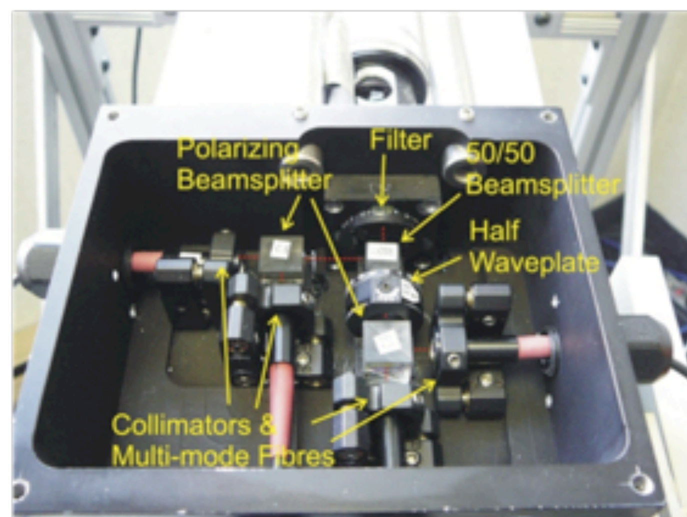
Chris Erven

Entanglement-based receivers







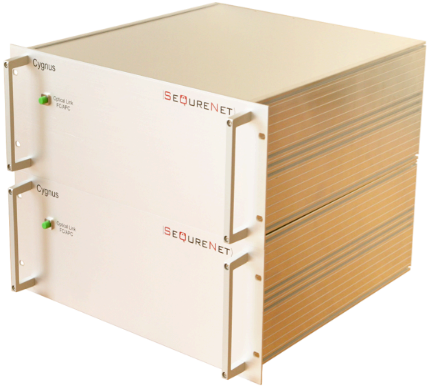


Chris Erven

Commercial QKD

idQuantique

SeQureNet

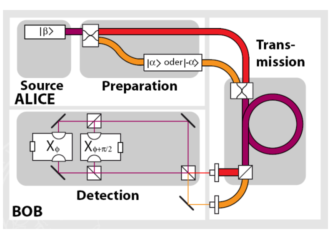


MagiQ

Quintessence Labs

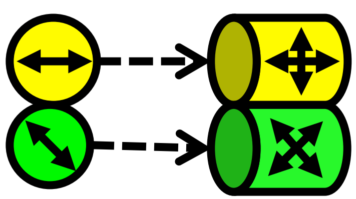
Security: implementations -> proofs ??

actual physical device



quantum optical model

e.g. mode-based



logical QKD protocol

e.g. qubit-based

$$\frac{1}{2}\,\|\rho_{ABE} - \rho_{UU} \otimes \rho_{E'}\|_{\mathrm{tr}} \leq \epsilon$$

security proof

At every level of abstraction, we make modelling assumptions.

Quantum hacking

Trojan horse attack

- Eve sends large pulse of light into Alice's lab
- Alice's equipment reflects some light, revealing the state of Alice's system

More attacks

- Side-channel attacks
  - first QKD implementation made different noises for different qubits
- Photon number splitting
- Time-shift attacks

Published online 29 August 2010 | Nature | doi:10.1038/news.2010.436

News

Hackers blind quantum cryptographers

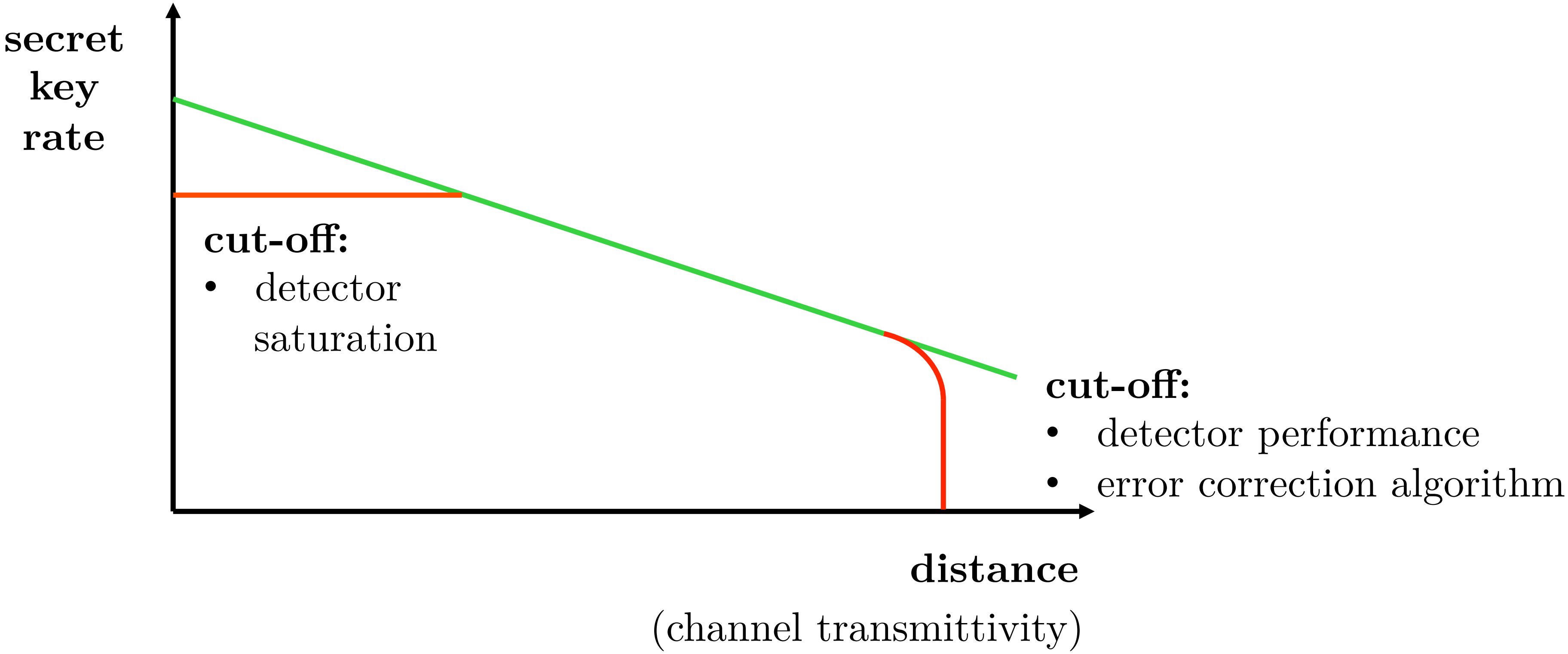
Lasers crack commercial encryption systems, leaving no trace.

Zeeya Merali

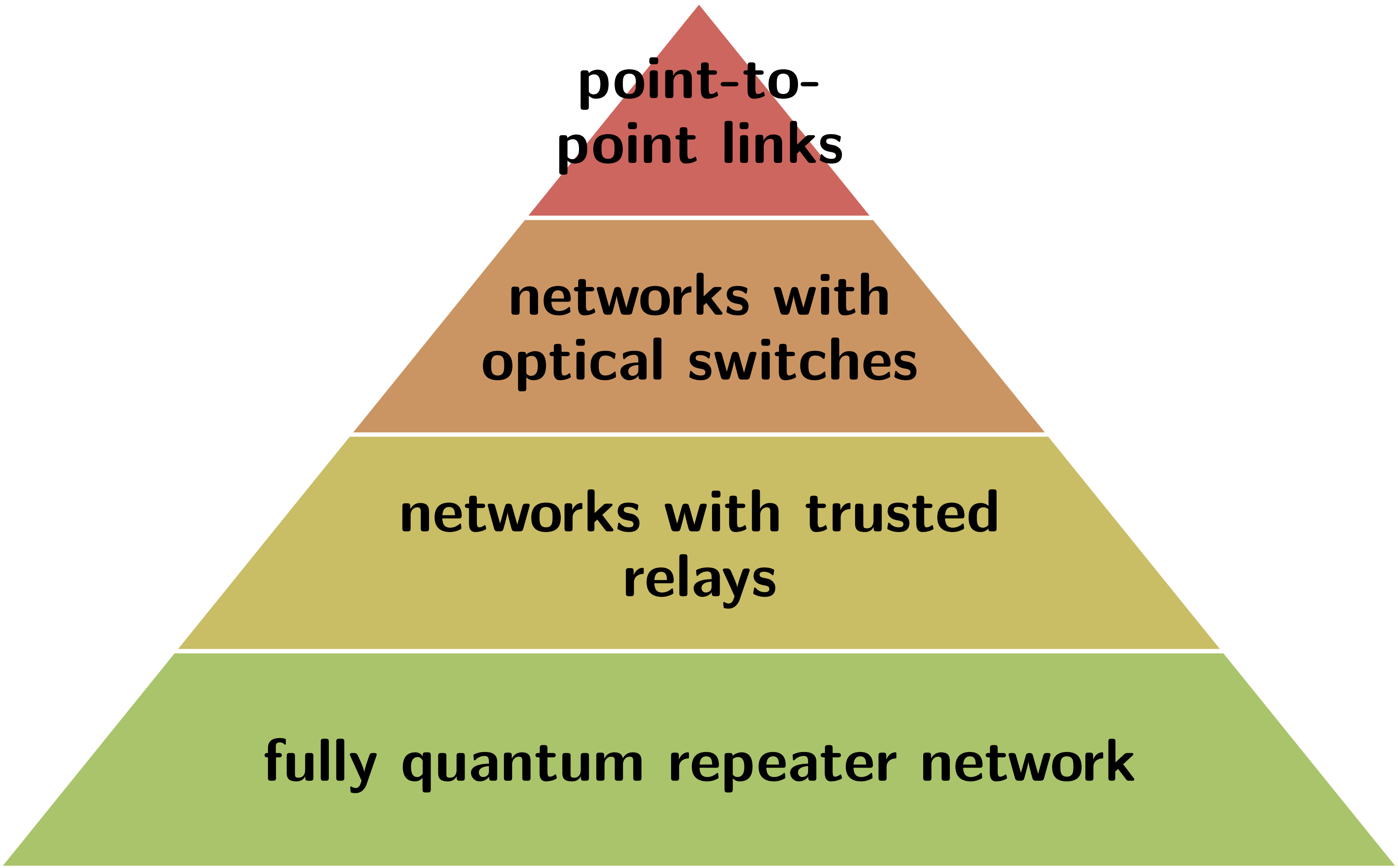
Quantum hackers have performed the first 'invisible' attack on two commercial quantum cryptographic

QKD networks

Limitations of point-to-point links

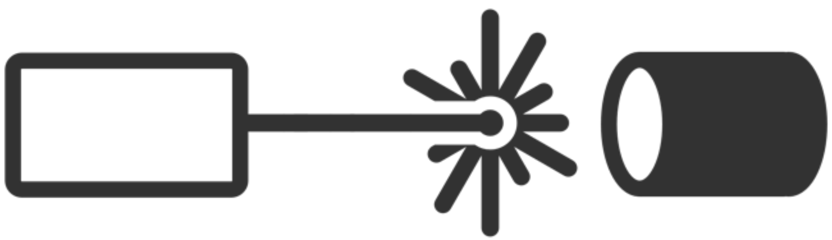


Networks of QKD devices



Point-to-point links

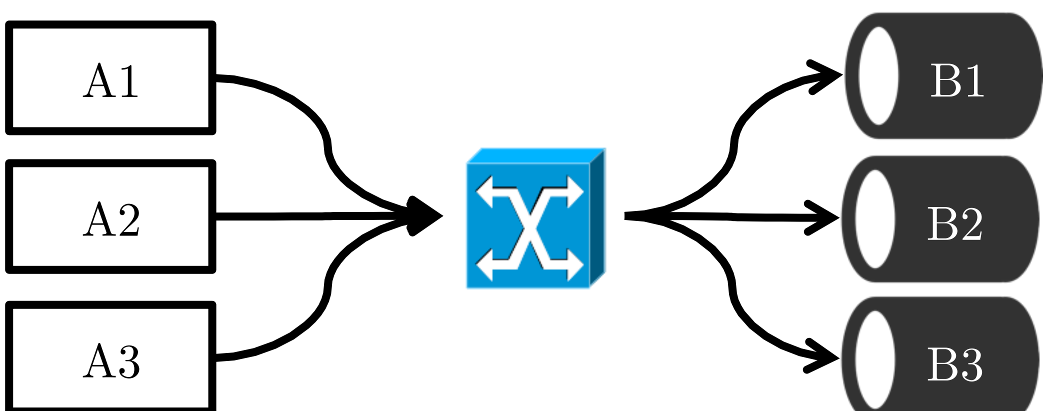
2 QKD devices are connected directly over a relatively short distance



Networks with optical switches

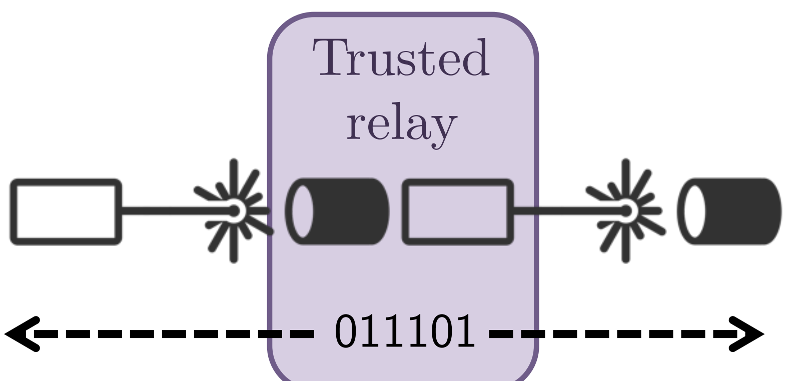
Several Alice and Bob devices are connected via *optical switches* (mirrors) that can direct photons along different paths.

- Example: DARPA quantum network
  http://arxiv.org/abs/quant-ph/0503058
- Still limited by total distance between endpoints



Network with trusted relays

Nodes are connected to *trusted relays* which does separate QKD connections with Alice and Bob, then sends keys to both parties.

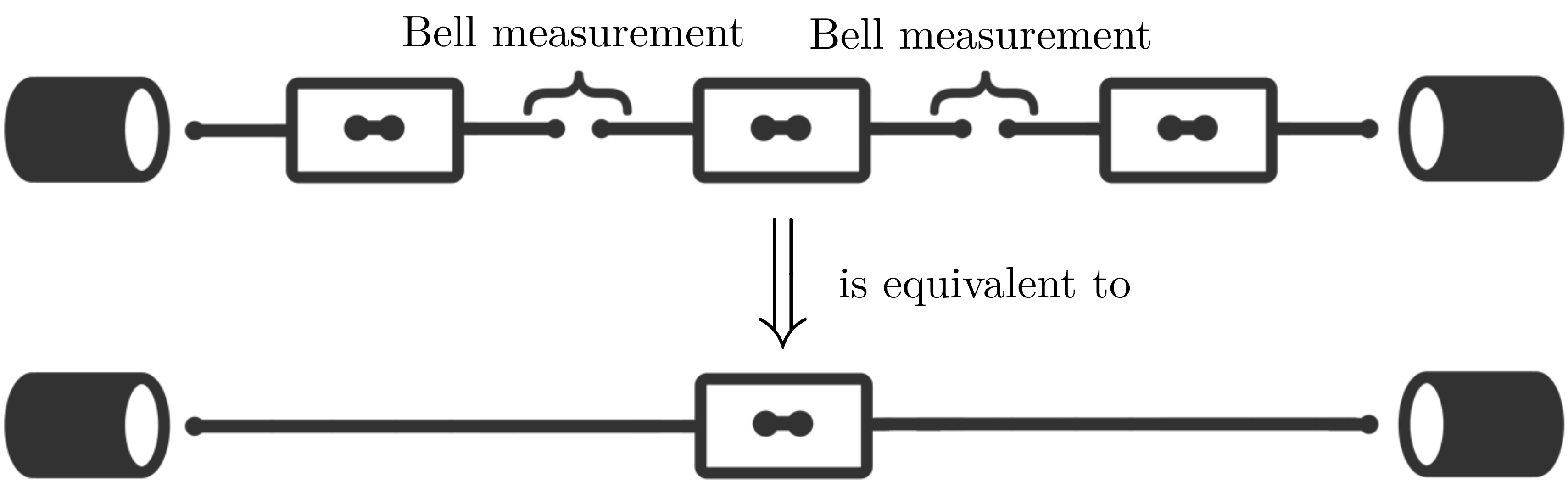


- Example: Tokyo QKD network, SECOQC, China trusted node network
  http://www.uqcc.org/QKDnetwork/
  http://www.secoqc.net

- No end-to-end security: relies on trusted relays (can use secret sharing to reduce trust)

Quantum repeater network

Nodes are connected via many intermediate *quantum repeaters* which entangle received photons, ultimately creating an entangled state between sender and receiver.



Quantum repeater network

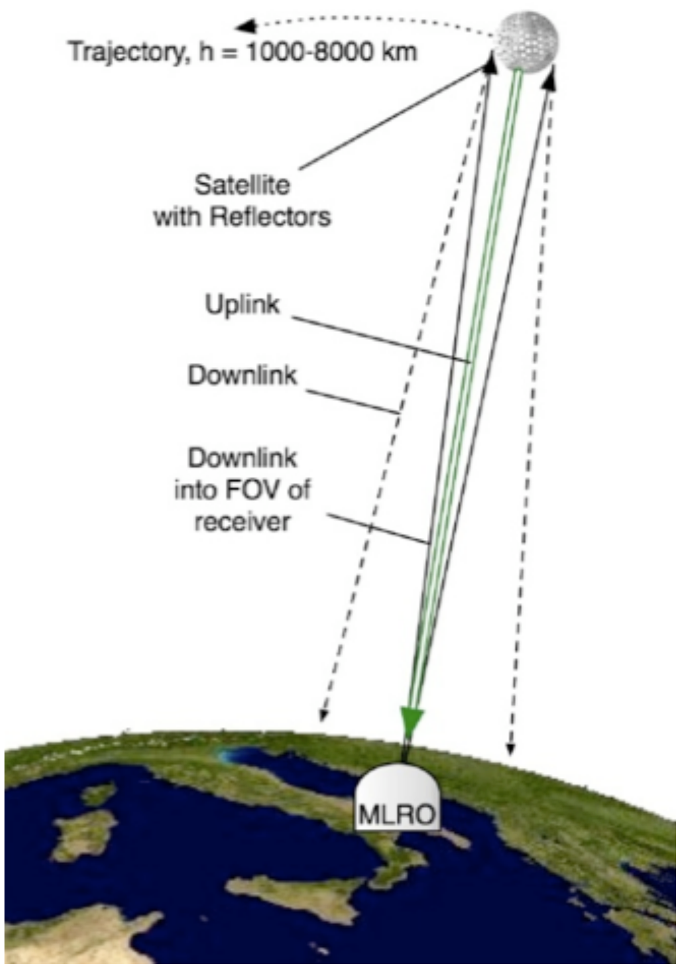
Would allow for secure end-to-end communication between arbitrarily distant nodes.

- Requires ability to store incoming qubits and jointly measure.
- Beyond current technology, but probably easier than a quantum computer.

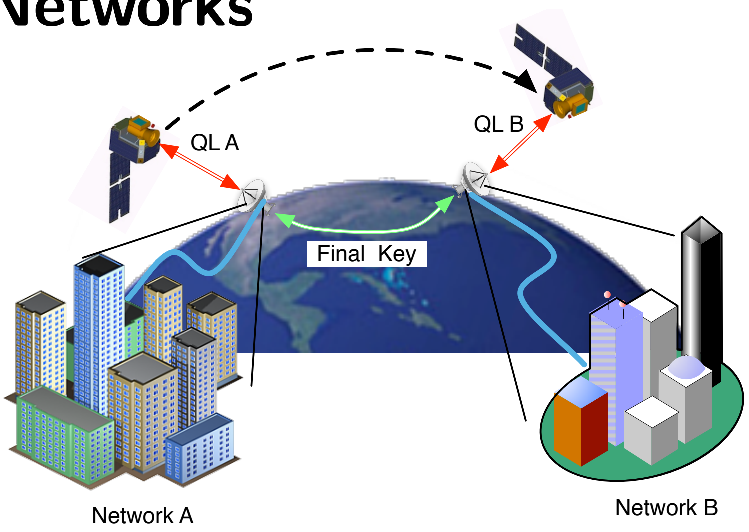
[SSRG11] N. Sangouard, C. Simon, H. de Riedmatten, and N. Gisin. Quantum repeaters based on atomic ensembles and linear optics. *Rev. Mod. Phys.* 83:33, March 2011. DOI:10.1103/RevModPhys.83.33.

Satellite QKD

Reflectors



Networks



- A quantum satellite in LEO can interconnect ground networks located anywhere on Earth.
  - Active research in Canada (QEYSSAT), USA, Europe (Space-QUEST), Japan, China, Singapore.

Summary

BB84 protocol

1. Alice sends random qubits to Bob.
2. Bob measures in a random basis.
3. They see when they used the same basis.
4. They check how much information an eavesdropper could have learned.
5. They correct any errors, then process the remaining qubits to squeeze out the eavesdropper's information.

quantum

classical processing

Fundamental principle of QKD

information gain by adversary

=>

disturbance of state

=>

detection by Alice and Bob

More information

- M.A. Nielsen and I.L. Chuang. *Quantum Computation and Information*. Cambridge University Press, 2000. QKD section 12.6.

- Renato Renner's PhD thesis, *Security of Quantum Key Distribution*. [arXiv:quant-ph/0512258]