CCL Seminar

Survey on Quantum Key Distribution

Vu Quang Minh

Contents

1. Cybersecurity: the role, how it works
2. Motivation for QKD
3. QKD Implementation
    1. Encoding-Decoding
    2. Operating scheme
    3. Channel
    4. Post-processing procedures
4. Several well-known QKD protocols
5. Quantum hacking and countermeasures
6. Recent developments on QKD

Security threats from the Internet

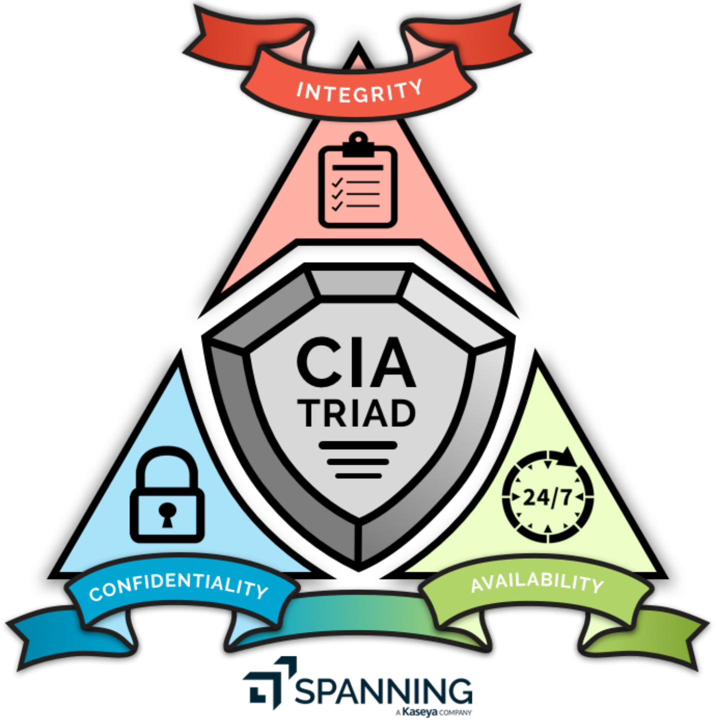
- The Internet has greatly changed the way we live, we learn, and we communicate
- The Internet connects many (really many) devices
- The Internet indeed did a lot to improve the human quality of life, however, it also brings many security threats from bad guys, e.g. steal secret information from governments, steal money from bank accounts, steal personal information…

=> Solution: Cybersecurity is the pratice of defending computers, severs, mobile devices, electronic systems, networks, and data from malicious attacks

The Internet can connect everything

Cybersecurity: What?

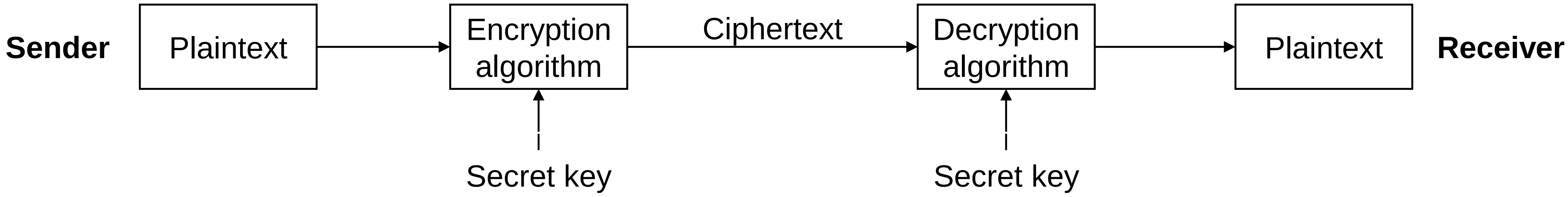
- **Confidentiality:** assures that private or confidential information is not made available or disclosed to *unauthorized individuals*
- **Integrity:** assures that information and programs are changed only in a *specified and authorized manner*
- **Availability:** assures that system works promptly and service is not denied to authorized users



Confidentiality, Integrity, Availability (CIA) Triad

Cybersecurity: How?

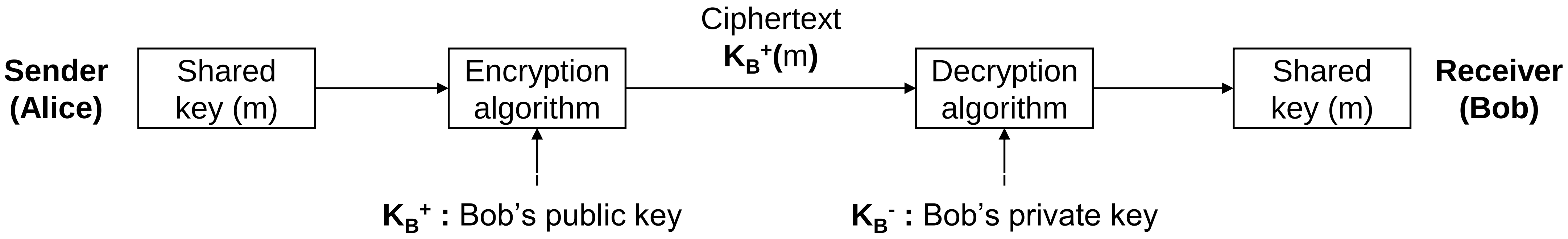
- How is it implemented?
  - Basically, based on shared-key (aka. symmetric) cryptography
  - Shared and secret keys are needed to ensure the security



- How can secret keys be shared?
  - Manually: e.g. private meetings → impratical
  - Key distribution system
    - Based on public-key cryptography

Present Key Distribution System

- Based on public-key cryptography



Sender (Alice)

Shared key (m)

Encryption algorithm

Ciphertext $\mathbf{K_B^+}$(m)

Decryption algorithm

Shared key (m)

Receiver (Bob)

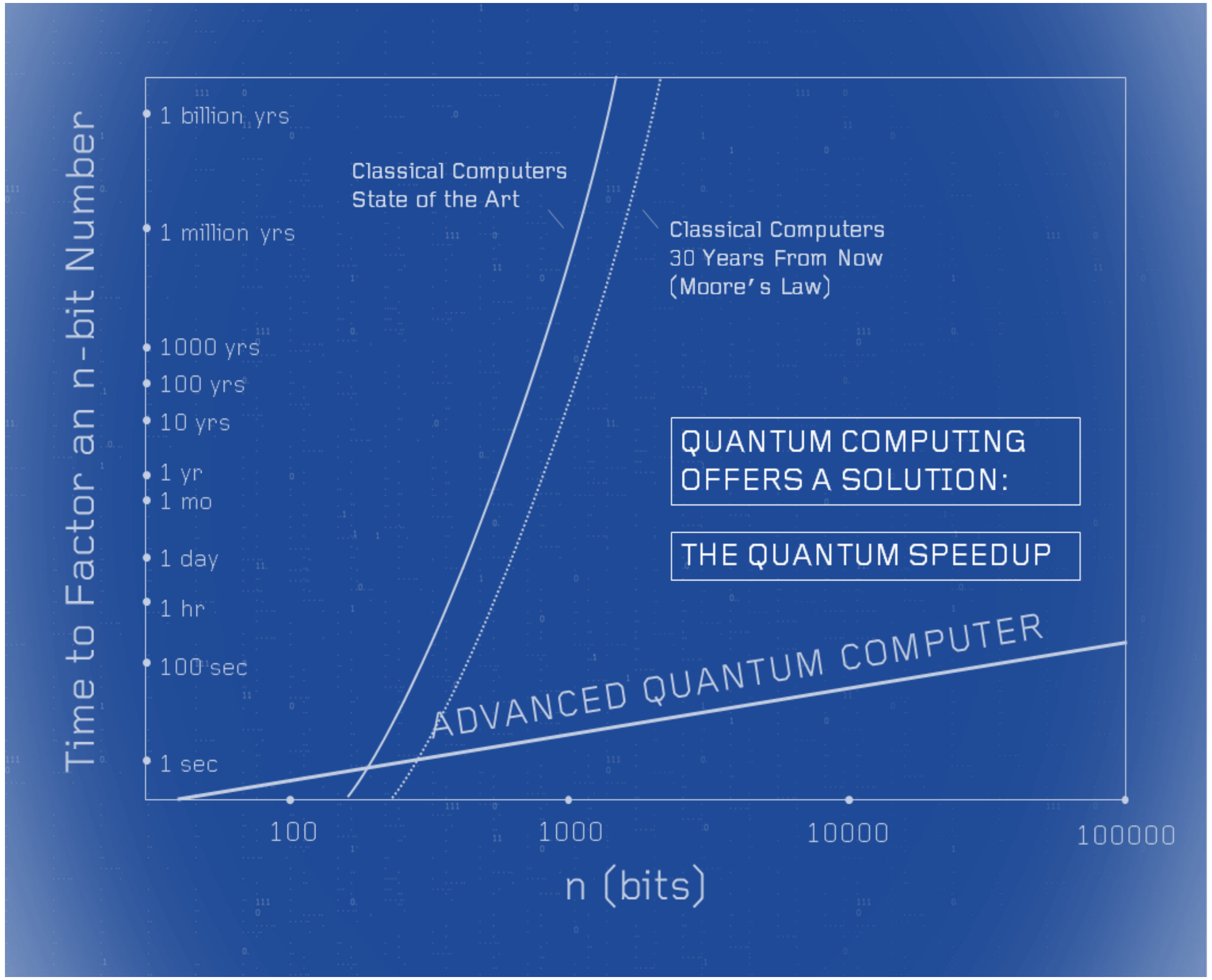
$\mathbf{K_B^+}$ **:** Bob’s public key

$\mathbf{K_B^-}$ **:** Bob’s private key

- Security of PKC is based on the mathematical complexity
  - Factoring problem: n is product of two large prime numbers (*p* and *q*)
    - n is known (in the public key) □ need to find *p* and *q* in order to find the private key
    - Difficult to find *p* and *q* when both are prime number
  - With classical computer, the computational time is exponentially increased as *p* and *q* increased (key length, in number of bits)

Issues with PKC-based Key Distribution

- With classical computer → no problem
  - Time to factoring is up to 10,000s years as number of bits → 1000.
- Recent advances on new computers, such as quantum computer: use qubit, instead of binary bit → computational power can be exponentially increased
- PKC can be broken in a much shorter time (few minutes vs. million years)

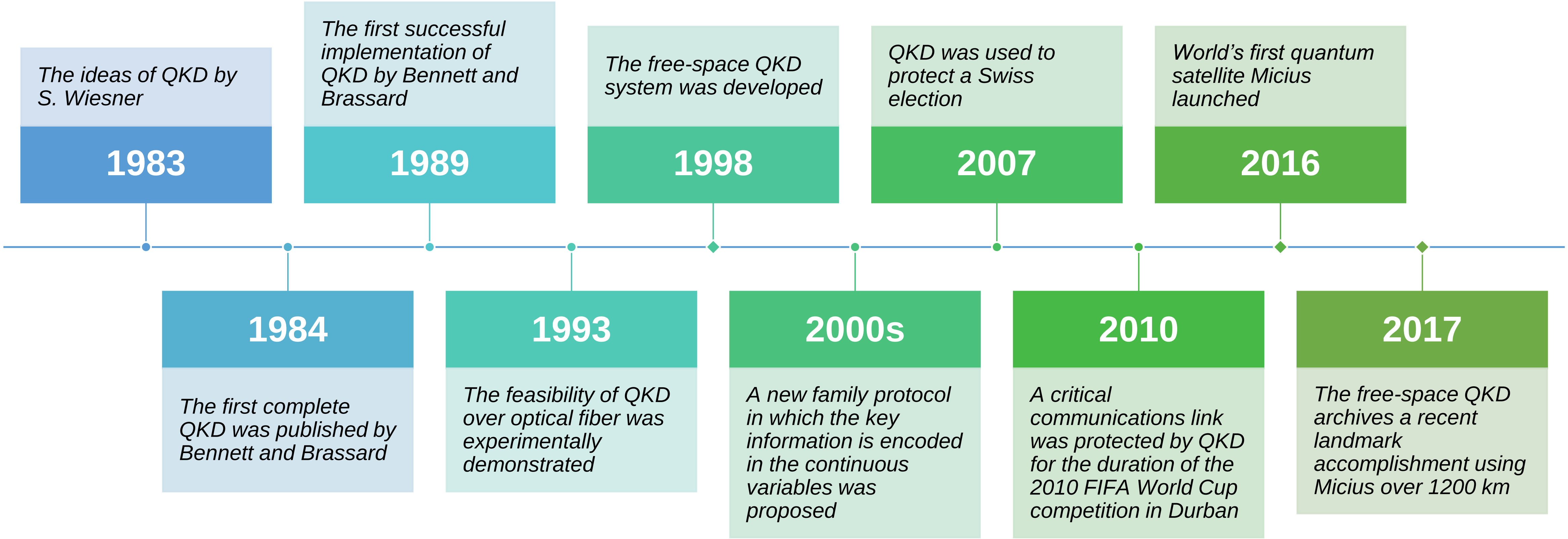


https://www.nea.com/blog/quantum-computing-time-for-venture-capitalists-to-put-chips-on-the-table

New Key Distribution Systems Needed

- Quantum key distribution (QKD)
  - QKD is being considered as a promising method to distribute secure keys secretly
  - Key distribution based on the laws of physics
    - In quantum mechanics, the **quantum no-cloning theorem** imposes that an unknown quantum state cannot be cloned reliably
    - If Alice distributes a key via quantum signals, there is no way for eavesdropper (Eve) to clone the quantum state reliably to make two copies of the same quantum state
    - If Eve tries to eavesdrop, she will introduce distubance unavoidably to the quantum signals → Alice and Bob can detect → Alice and Bob simply discard such a key and try the key distribution process again
  - First proposed by C. Bennett and G. Barassard in 1984: BB84 protocol

History of QKD



1983
The ideas of QKD by S. Wiesner

1984
The first complete QKD was published by Bennett and Brassard

1989
The first successful implementation of QKD by Bennett and Brassard

1993
The feasibility of QKD over optical fiber was experimentally demonstrated

1998
The free-space QKD system was developed

2000s
A new family protocol in which the key information is encoded in the continuous variables was proposed

2007
QKD was used to protect a Swiss election

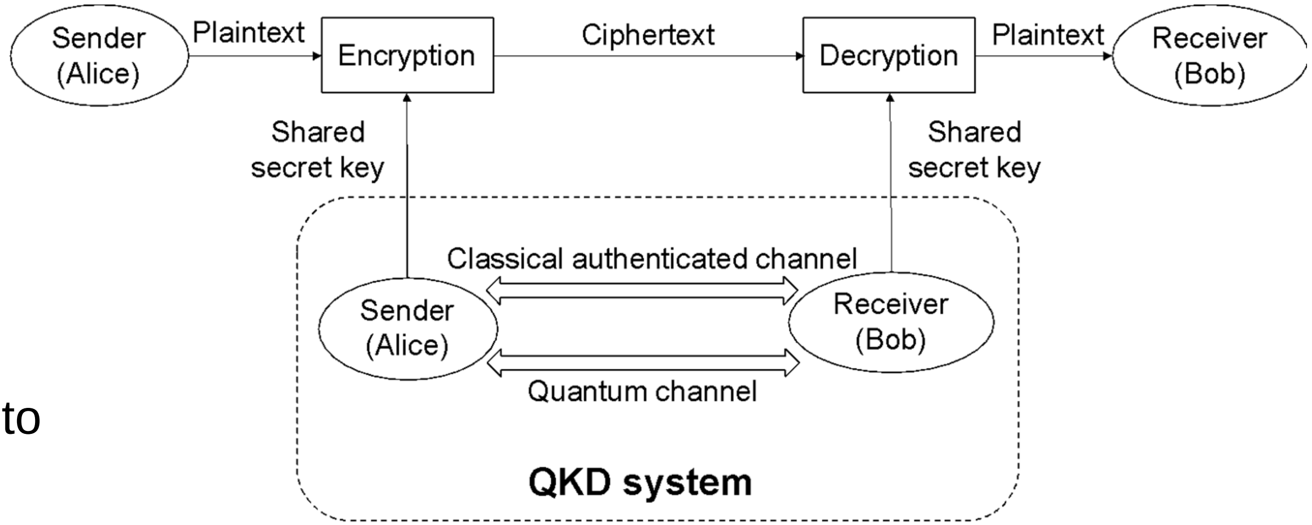
2010
A critical communications link was protected by QKD for the duration of the 2010 FIFA World Cup competition in Durban

2016
World’s first quantum satellite Micius launched

2017
The free-space QKD archives a recent landmark accomplishment using Micius over 1200 km

General steps of a QKD protocol

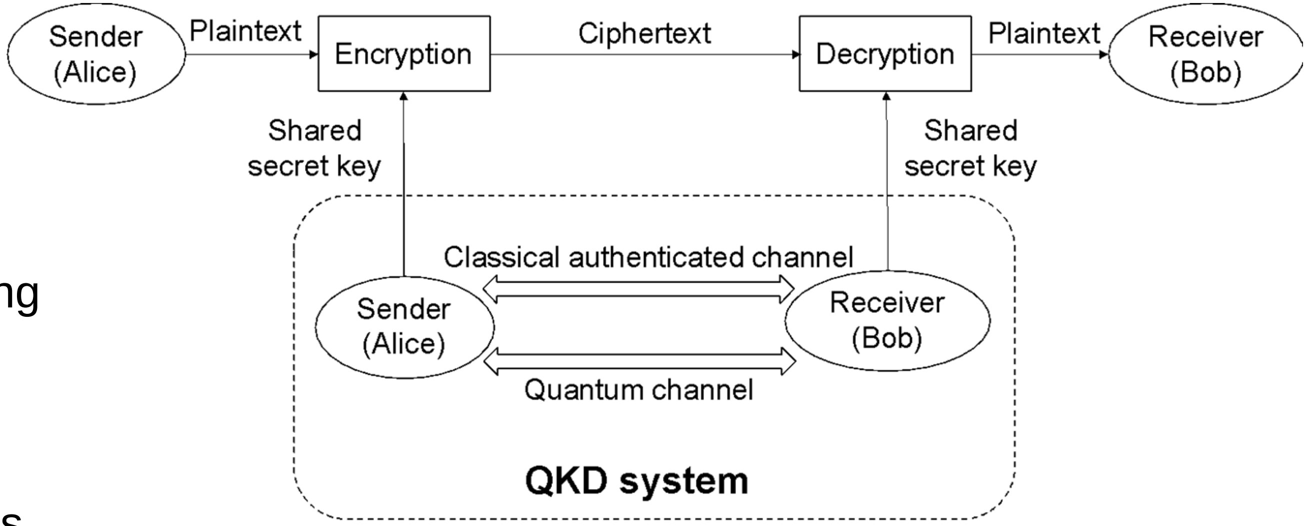
- Quantum state transmission and measurement: Alice and Bob use the quantum channel
  - *Step 1*: Alice encodes key information based on the uncertainty of quantum mechanics depending on a specific QKD protocol
  - *Step 2*: Alice transmits encoded key bits to Bob over quantum channel



A schematic of QKD system

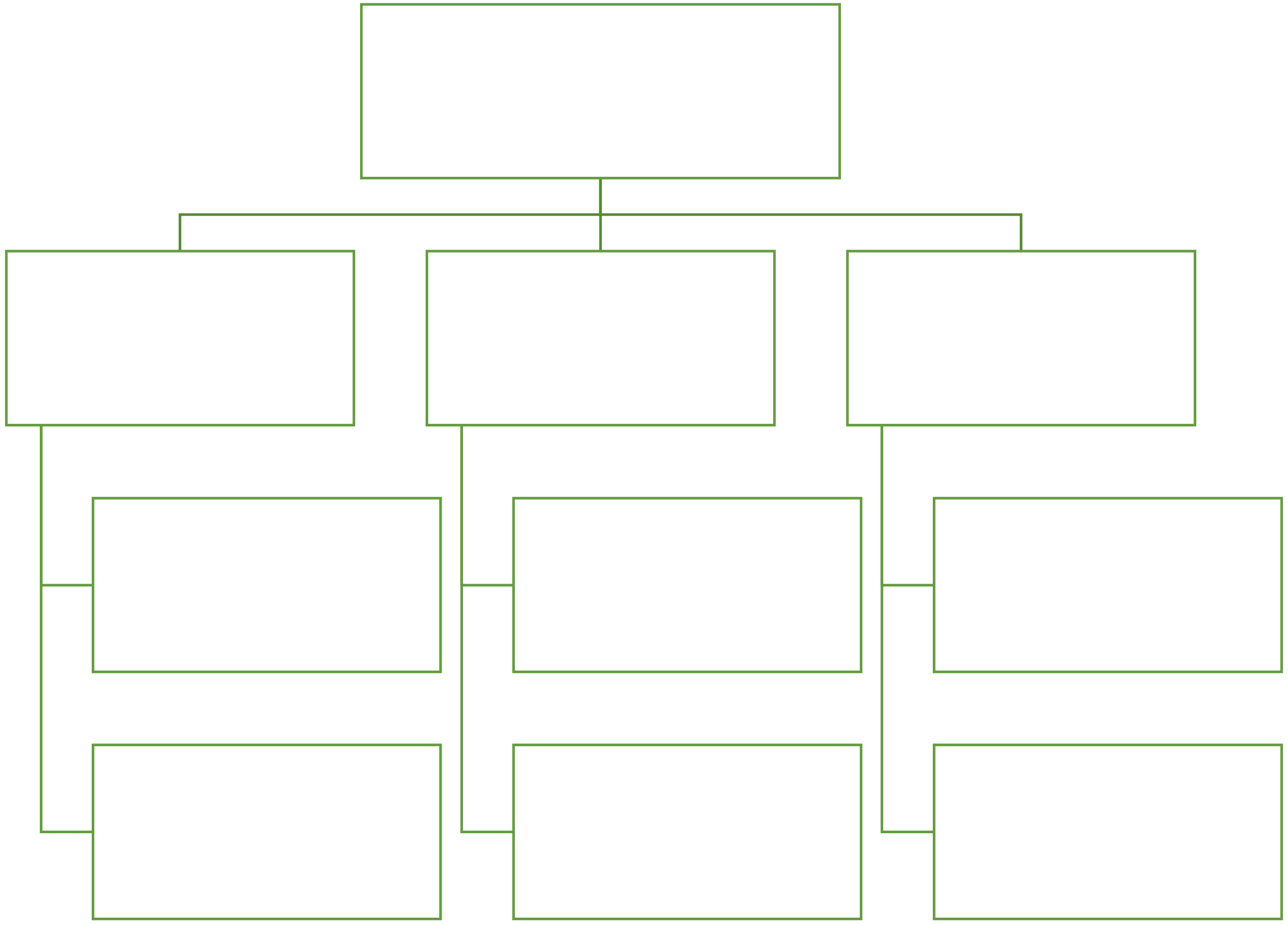
General steps of a QKD protocol

- Post-processing procedures: Alice and Bob use the classical channel
  - *Step 3*: Bob discloses to Alice the time instants that he was able to detect the encoded key bits, forming their shared *raw keys*
  - *Step 4*: Alice discloses to Bob her encoding schemes on the key bits he detected, forming their shared *sifted keys*
  - *Step 5*: Alice and Bob perform information reconciliation which use error correction techniques to identify and remove erroneous bits
  - *Step 6*: Alice and Bob perform privacy information which use hash functions to produce a new, shorter key in such a way that Eve has only negligible information about their shared secret keys



A schematic of QKD system

QKD Implementation: Overview

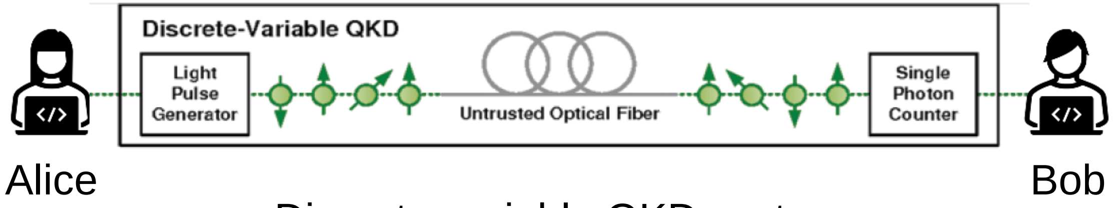


Discrete-variable QKD (DV-QKD)

- In discrete-variable encoding, the key information is encoded by modifying physical properties of single photons such as their polarization direction
- Alice generates quantum bits (qubits) using her orthonormal basis $(|a_0\rangle, |a_1\rangle)$. Bob measures the qubits that Alice sends to him using his orthonormal basis $(|b_0\rangle, |b_1\rangle)$. If Alice want to send 0, she sends a qubit in state $|a_0\rangle$. After receiving this qubit, Bob measures it with respect to his ordered basis

$$|a_0\rangle = d_0|b_0\rangle + d_1|b_1\rangle.$$

Bob detects $|b_0\rangle$ (bit 0) with probability $|d_0|^2$
Bob detects $|b_1\rangle$ (bit 1) with probability $|d_1|^2$



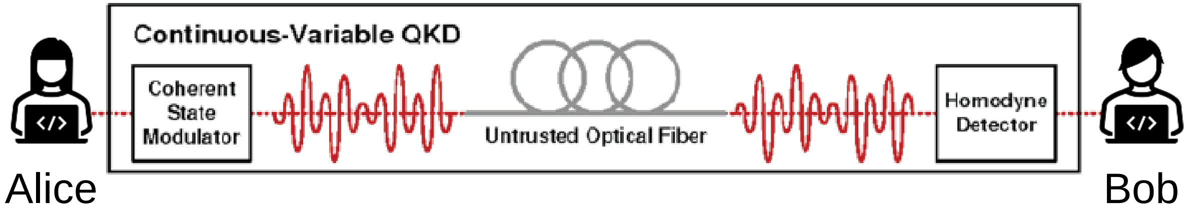
Discrete-variable QKD system

Source: Single-photon source (really hard to build)→ replacing by weak coherent-state source which can be easily realized by attenuating laser pulse (attenuate it very strongly so that the mean photon number per pulse is so small)

Detector: Single-photon counter (require cooling at low temperature)

Continuous-variable QKD (CV-QKD)

- In continuous-variable encoding, the key information is encoded in quadratures of the electromagnetic field that are shaped by a weakly modulated coherent laser
- It uses coherent detection techniques (homodyne or heterodyne) for determining the quadratures of light
- CV coding is most suitable for easy interoperability with existing telecom infrastructures and a cost-effective technique thanks to its off-the-shelf components

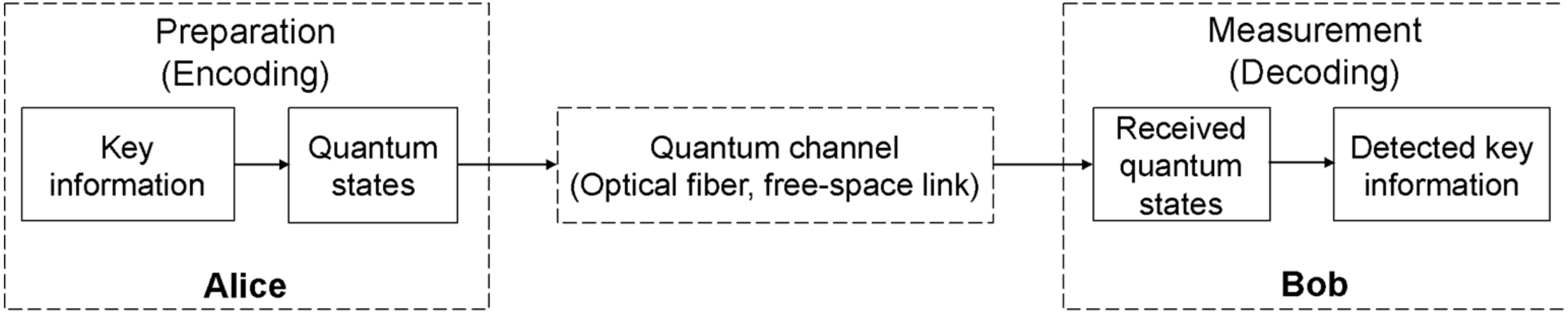


Continuous-variable QKD system

DV-QKD vs CV-QKD

Criteria	DV-QKD	CV-QKD
Source	Weak laser pulse	Laser
Modulation	Polarization	Amplitude & Phase
Detection	Single-photon detection	Coherent detection
System Complexity	Very high	High
Implementation Cost	Very high	High
Compatibility with existing telecom infrastructures	No	Yes

Prepare-and-measure (P&M) scheme



A schematic diagram of P&M scheme

- In P&M scheme, Alice prepares quantum states and encode the key information onto the quantum states (encode onto the polarization of single photon in DV-QKD, or encode onto amplitude and phase of laser pulses in CV-QKD)
- These quantum states are then sent over a quantum channel (optical fiber, free-space link) to Bob
- After receiving these quantum states, Bob measures them using single-photon detectors (DV-QKD) or coherent detectors (CV-QKD)
- Example protocol: BB84 (DV-QKD), Gaussian-modulated coherent state (GMCS) protocol (CV-QKD)

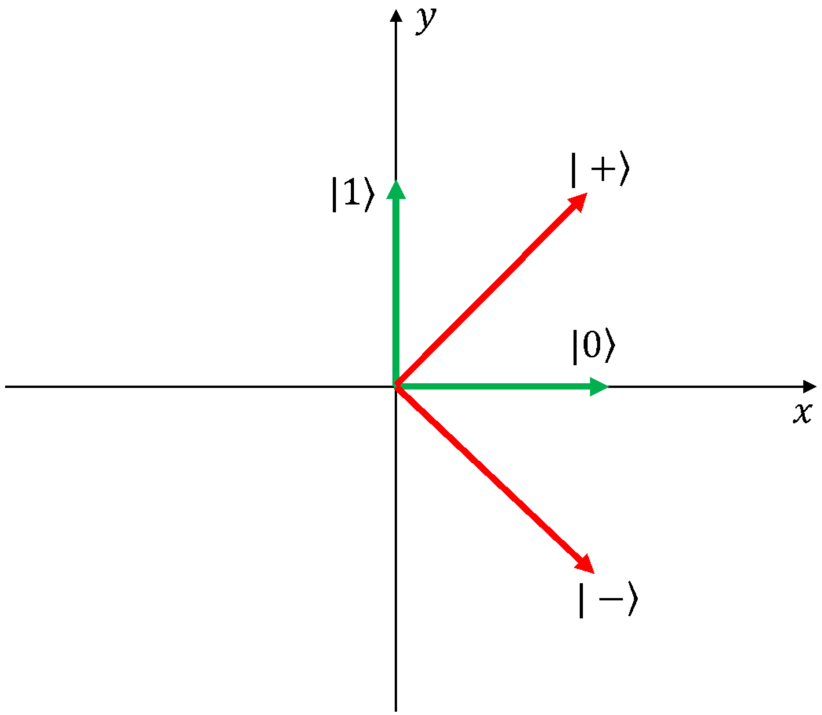
BB84 Protocol (1)

- BB84 (Bennett and Brassard, 1984) protocol is the best-known QKD protocol
- In BB84, a sequence of single photons which carries qubit states is sent by Alice to Bob through a quantum channel
- Two bases are used in BB84
  - Rectilinear basis is constituted by two polarization states

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

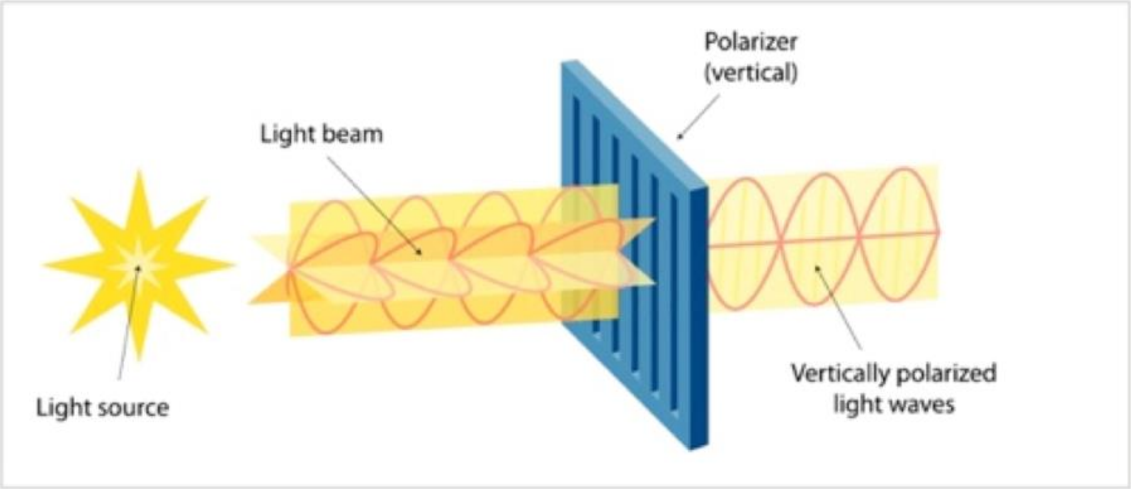
  - Diagonal basis is constituted by two polarization states

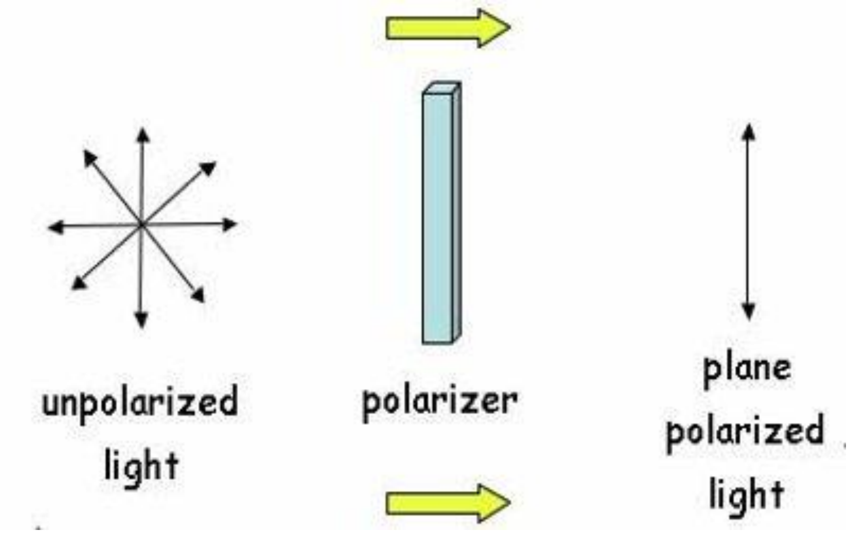
$$\begin{aligned}|+\rangle &= \frac{|0\rangle + |1\rangle}{\sqrt{2}} = \frac{1}{\sqrt{2}}\begin{bmatrix}1\\1\end{bmatrix}\\ |-\rangle &= \frac{|0\rangle - |1\rangle}{\sqrt{2}} = \frac{1}{\sqrt{2}}\begin{bmatrix}1\\-1\end{bmatrix}\end{aligned}$$



The four states being employed in BB84 protocol

Polarization





Polarization is a property of light that depends on the direction in which its electric field is oscillating

Example: a photon traveling straight at you could have an electric field oscillating vertically or horizontally

BB84 Protocol (2)

- Operational steps
  - *Step 1*: Alice generates a string of random bits
  - *Step 2*: Alice randomly chooses between rectilinear (⊕) basis and diagonal (⊗) basis to encode every bits she wants to send on single photons as qubits

$$\oplus \text{ was chosen } \begin{cases} \text{bit "0"} \rightarrow |0\rangle \\ \text{bit "1"} \rightarrow |1\rangle \end{cases} \qquad \otimes \text{ was chosen } \begin{cases} \text{bit "0"} \rightarrow |+\rangle \\ \text{bit "1"} \rightarrow |-\rangle \end{cases}$$

  - *Step 3*: At the receiver, Bob randomly chooses either between rectilinear (⊕) basis or diagonal (⊗) basis to measure the received qubits
    - Alice's encoding and Bob's decoding bases are the same, the corresponding bit value is detected correctly with high probability
    - Otherwise, the received photon is measured by one of two polarization states of the used basis at Bob's receiver
    - Example: bit "1" is encoded in the ⊗ basis but is measured in the ⊕ basis; the measure results is expressed as

$$|-\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$$

The result is equally like to collapse either to the state $|0\rangle$ or to the state $|1\rangle$

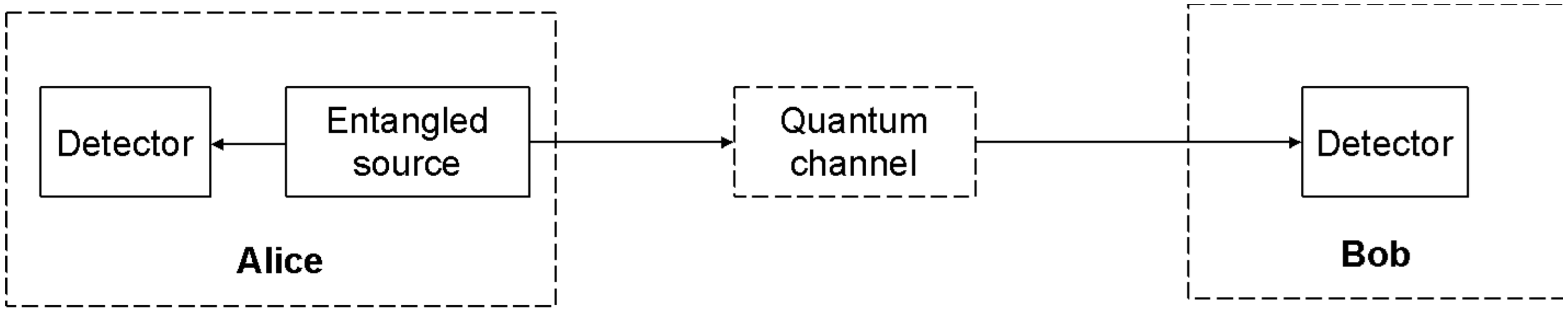
BB84 Protocol (3)

- *Step 4*: After detection, Alice and Bob publicly announces their basis choices through an authenticated classical channel
    - Alice and Bob discard the states that have been encoded and detected in different bases
    - Alice and Bob keep only those states in the same basis to form sifted key
- *Step 5*: Alice and Bob compute the quantum bit error rate (QBER). If the computed QBER is too high, they abort. By contrast, they continue to perform information reconcilliation and privacy amplification to produce the final secret key

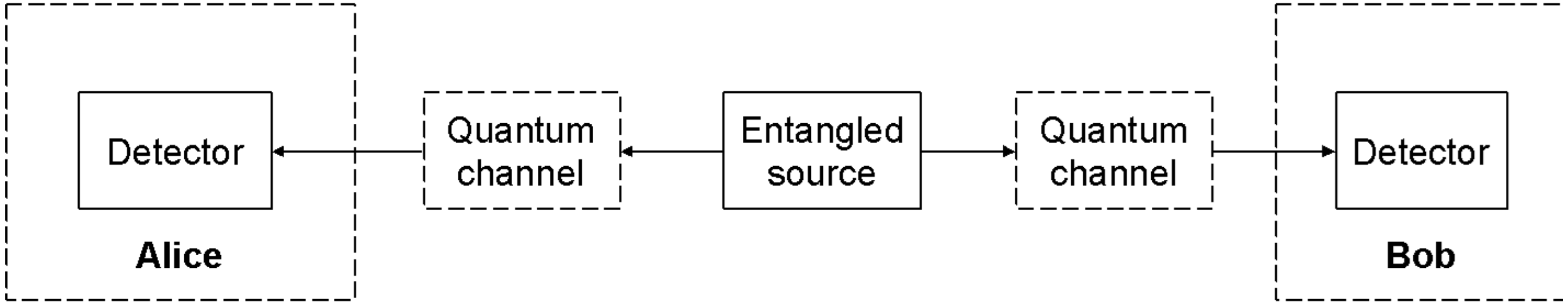
BB84 Protocol Example

Alice’s random bit	1	1	0	1	0	1	1	0	0
Alice’s random choosing basis	×	+	×	+	+	×	+	+	×
Photon states Alice sends	↘	↑	↗	↑	→	↘	↑	→	↗
Bob’s random measuring basis	+	+	×	×	+	+	+	×	×
Photon states Bob measures	↑	↑	↗	↘	→	↑	↑	↗	↗
Compatibility									
Sifted key		1	0		0		1		0

Entanglement-based (EB) scheme



a) Entangled source is equipped by Alice



b) Entangled source is equipped by a third party

- Alice (or third party) equips an entangled source which could prepare entangled pairs of quantum states and then send half of each to Alice and Bob
- Example protocol: E91, BBM92

E91 Protocol (1): Entanglement-based approach

- Preliminary concept:
  - Entangled states: can illustrated by the Schrodinger cat experiment

    Two states of atom:

    $|1\rangle$: The state of undecayded atom

    $|2\rangle$: The state of decayded atom

    Two states of cat:

    $|\mathrm{alive}\rangle$: The cat is alive

    $|\mathrm{dead}\rangle$: The cat is dead

    Combined states of atom and cat

    $|\mathrm{alive}, 1\rangle$: The atom is undecayded, the cat is alive

    $|\mathrm{dead},2\rangle$: The atom is decayded, the cat is dead

  =>It is said that the state of cat ***entangled*** with the state of atom

  The wave function of the system $|\Psi\rangle = \frac{1}{\sqrt{2}}(|\mathrm{live}, 1\rangle + |\mathrm{dead}, 2\rangle)$

The Schrodinger cat experiment

The box contains a devious mechanism such that the decay of the atom triggers a device to smash a bottle of poison, thereby killing the cat

The probability of the atom decaying is equal to 50%

E91 Protocol (2)

- The concept of mutiple qubits
  - Two classical bits: 4 possible states 00, 01, 10, 11
  - Two qubits: 4 basis states $|00\rangle, |01\rangle, |10\rangle, |11\rangle$
  - The state vector describing the two qubits: $|\psi\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}\,|10\rangle + \alpha_{11}\,|11\rangle$

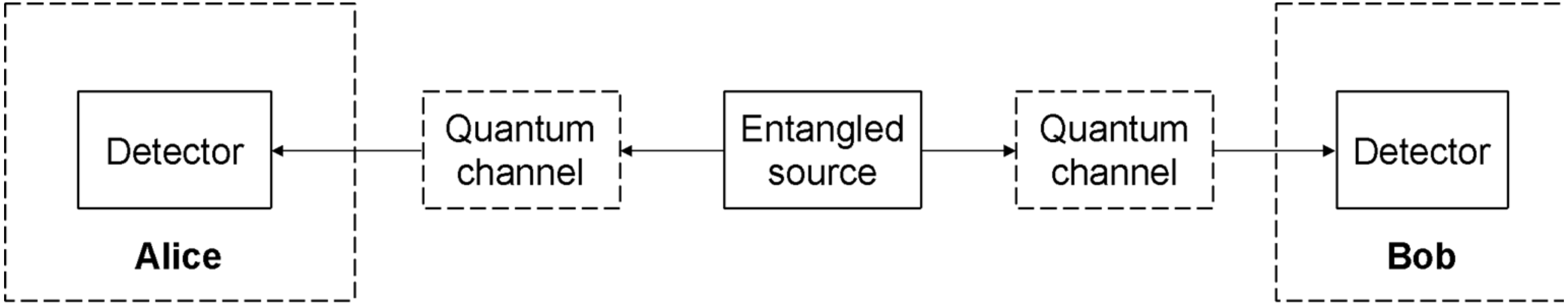
    The measurement result x (= 00, 01, 10, or 11) occurs with probability $|\alpha_x|^2$
  - $|0\rangle_A$, $|1\rangle_A$: states of qubit of Alice
  - $|0\rangle_B$, $|1\rangle_B$: states of qubit of Bob
  - An important two-qubit state $|\psi\rangle_{AB}$ shared between Alice and Bob (*the Bell state* or *Einstein, Podolsky, and Rosen (EPR) pair*):

$$|\psi\rangle_{AB} = \frac{|0\rangle_A|0\rangle_B+|1\rangle_A|1\rangle_B}{\sqrt{2}} = \frac{|00\rangle_{AB}+|11\rangle_{AB}}{\sqrt{2}} = \frac{|00\rangle+|11\rangle}{\sqrt{2}}$$

    Upon measuring the first qubit, one obtains two possible results
    - 0 with probability 1/2 → the post measurement state $|\psi'\rangle = |00\rangle$
    - 1 with probability 1/2 → the post measurement state $|\psi'\rangle = |11\rangle$
    - A measurement of the second qubit always gives the same result as the measurement of the first qubit → the measurement outcomes are correlated

    The Bell state is the entangled state

E91 Protocol (3)



b) Entangled source is equipped by a third party

- Based on the characteristic of the entangled state, Artur Ekert proposed E91 protocol
  - In E91 protocol, instead of Alice sending particles to Bob, there is a central source creating pairs of entangle states (*the Bell states* or *EPR pairs*)
- Operational steps
  - *Step 1*: The central source emits entangled pairs of qubits in the Bell state

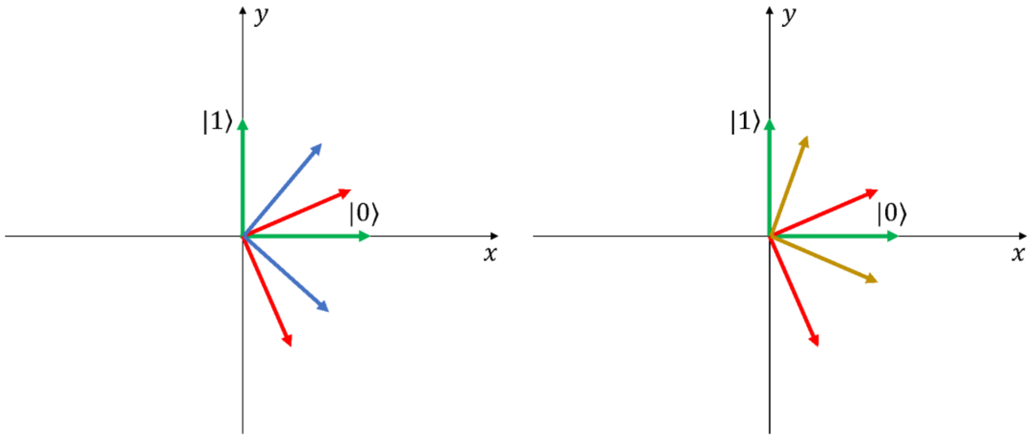
$$|\psi\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

One half of each pair are then sent to Alice and Bob

E91 Protocol (4)

- Operational steps (cont.):
  - *Step 2*: Both Alice and Bob randomly pick a basis out of three possible bases to measure the received particles
  - *Step 3*: If Alice and Bob choose compatible bases
    - Alice measures the first qubit and get the result of 0, the probability of Bob measuring the second qubit and get the result of 0 is high (up to 100% in ideal cases)
    - Alice measures the first qubit and get the result of 1, the probability of Bob measuring the second qubit and get the result of 1 is high (up to 100% in ideal cases)

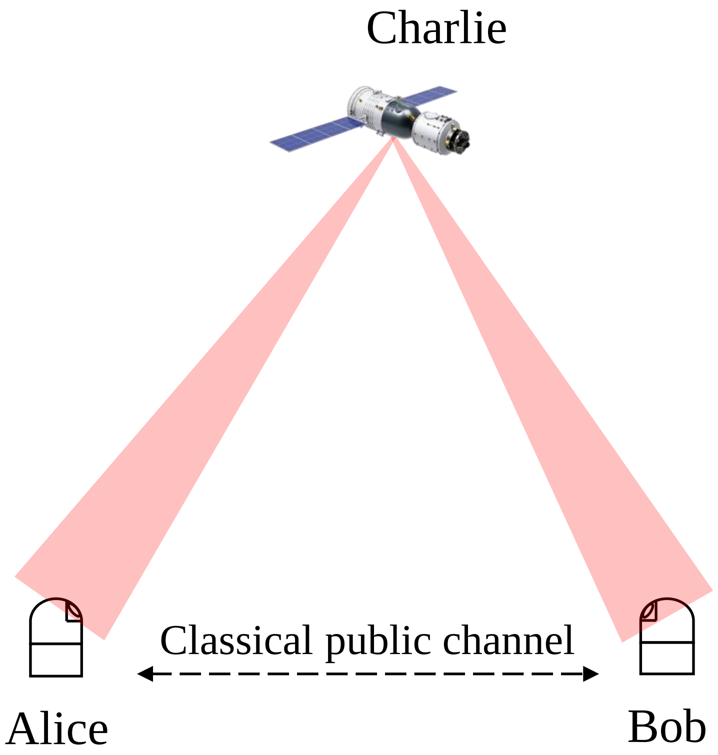
    Otherwise, the measurement results of Alice and Bob will be different
  - *Step 4*: Alice and Bob use classical channel to announce which bases they use. They discard results obtained in incompatible basis
  - *Step 5*: Alice and Bob perform information reconcilliation and privacy amplification

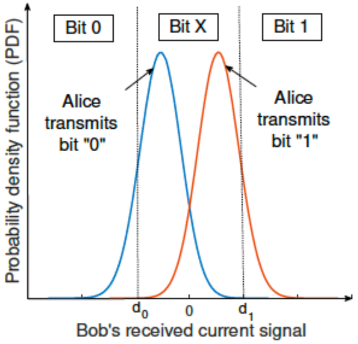


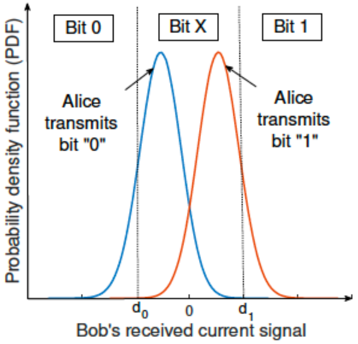
Alice

Bob

- Alice's bases are located at 0, $\pi/8$, and $\pi/4$ angles
- Bob's bases are located at 0, $\pi/8$, and $-\pi/8$ angles







- Step 1: Charlie transmits SIM/BPSK signal modulated signal to Alice and Bob with a small modulation depth corresponding to binary random bits “0” or “1” over atmospheric turbulence.

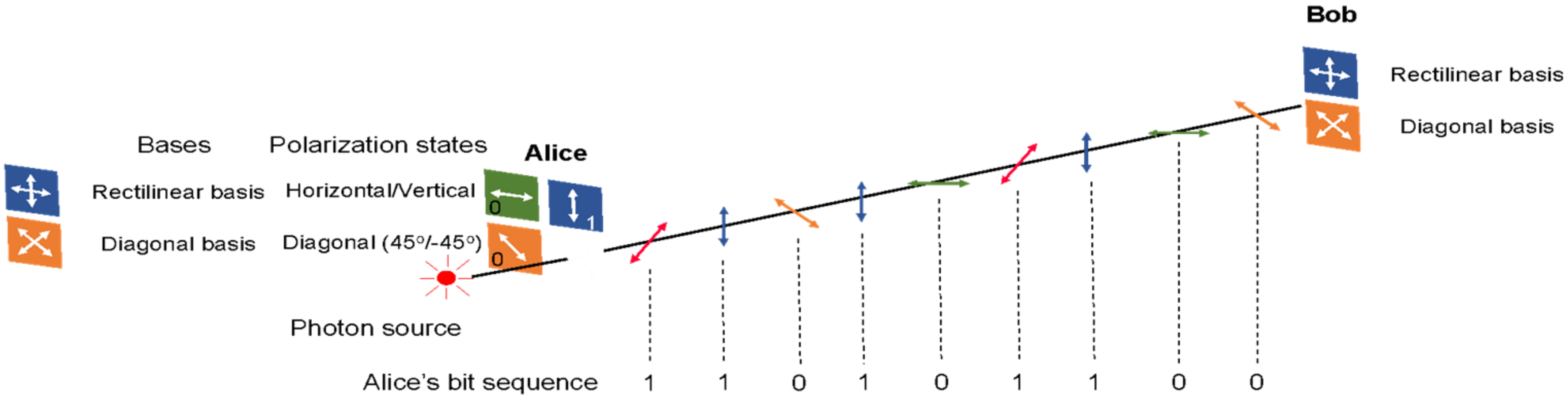
- Step 2: The transmitting modulated signal are then directly detected at Alice’s and Bob’s receivers. For the detected value *i* of the received current signal, the detection rule can be expressed as

$$\text{Decision} = \begin{cases} 0 & \text{if} \quad i \le d_0, \\ 1 & \text{if} \quad i \ge d_1, \\ \text{X} & \text{otherwise}, \end{cases}$$

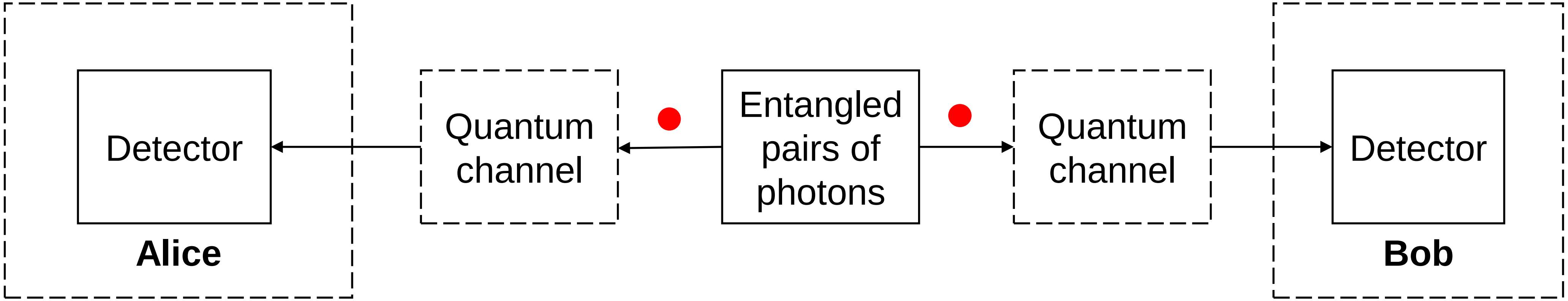
- Step 3: Using a classical public channel, Alice and Bob notify each other of the time instants they were able to create binary bits from detected signals. Alice and Bob then discards bit values at time instants that Alice or Bob created no bit. Alice and Bob then share an identical bit string, which is the *sifted key.* Two threshold d_0 and d_1 can be adjusted, the probability of sift at Alice’s and Bob’s receiver can be controlled.

- Step 4: To identify and remove the errorneous bits, Alice and Bob perform *information reconciliation* by using error correction techniques to correct the transmission errors, which ensures both key are identical, forming their shared error-free secret key. Moreover, to reduce Eve’s knowledge of the shared key, Alice and Bob apply the *privacy amplification* process by using their shared keys to produce a new, shorter key based on hash functions.

BB84 vs E91



BB84 protocol



Detector

Alice

Quantum channel

Entangled pairs of photons

Quantum channel

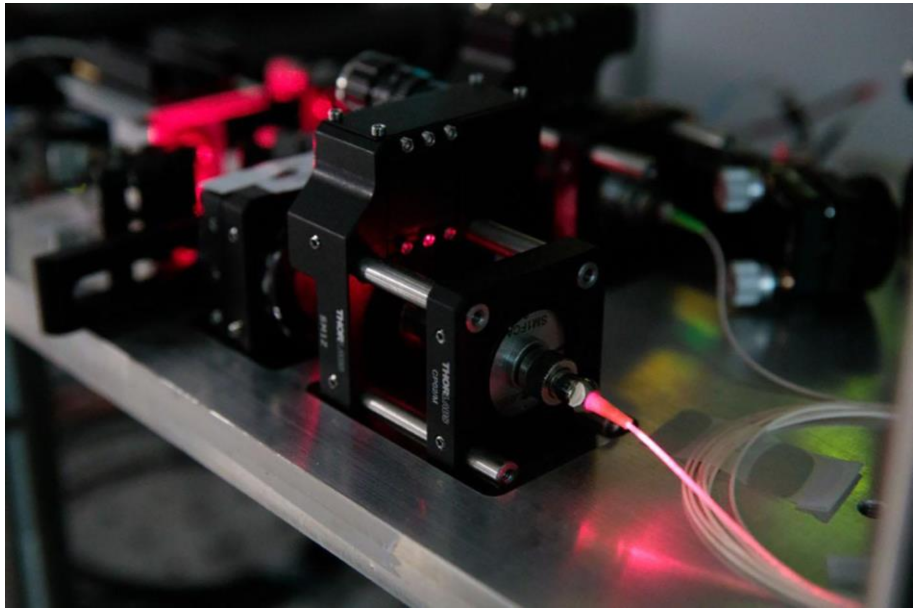
Detector

Bob

E91 protocol

Optical Fiber

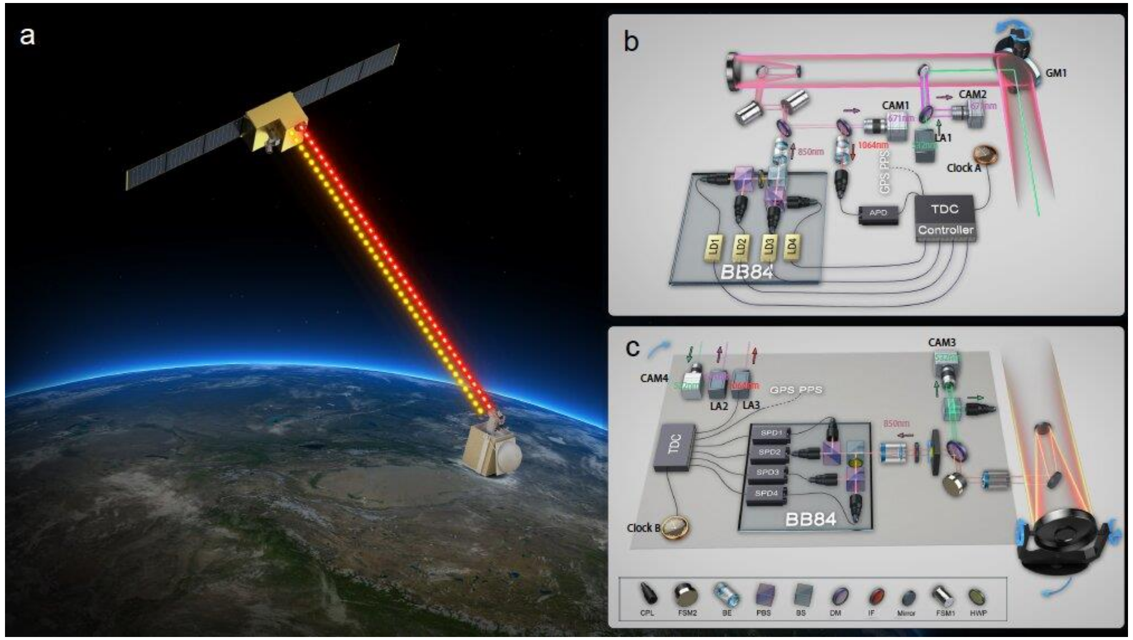
- Optical fiber is the most common channel used in QKD
- Optical fibers introduce loss which causes the intensity of the optical signals to decay as they propagate
- Due to the pratical imperfection of optical fibers, it can suffer from birefringence which can modify the state of polarization of photons while they propagate in the fiber
- The attainable distance distance of fiber-based QKD is limitted to a few hundred kilometers (the best record of 421 km in 2018)



QKD demonstration over commercial optical fiber

Free-space optics (FSO)

- FSO features some advantages compared to optical fiber: high data-rate, cost-effectiveness, and convenient flexibility in terms of infrastructure deployment and redeployment
- The first pratical demonstration of QKD used FSO was reported in 1992
- QKD is implemented in both terrestrial FSO links and satellite FSO links
- Nevertheless, the transmission distance is significantly limited by atmospheric turbulence, background noise…



QKD demonstration over free-space optics

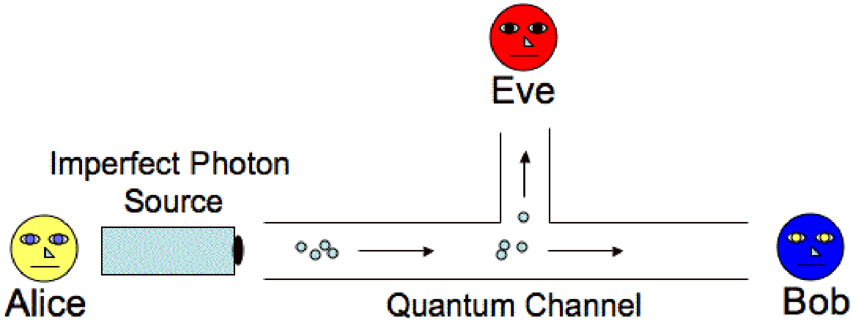
Quantum Hacking

- Normally, security proofs for QKD protocols was provided based on some security assumptions
- Practically, the operation of QKD protocols deviates from the ideal because of imperfect components that make up the practical QKD systems

=> Eve can try to exploit the imperfections in QKD systems and initiate *quantum hacking* which is not covered by the original security proofs

- Two examples of quantum hacking strategies
  - Photon-number-splitting attack
  - Detector-blinding attack

Photon-number-splitting attack



Photon-number-splitting attack [1]

- Ideally, DV-QKD requires perfect single-photon sources which emits one photon at a time
- In pratical, the standard procedure for producing single-photon source is to take a pulse laser and attenuate it very strongly so that the mean photon number per pulse is so small

⇒A fraction of time that a pulse can contain 2 or more photons can be existed

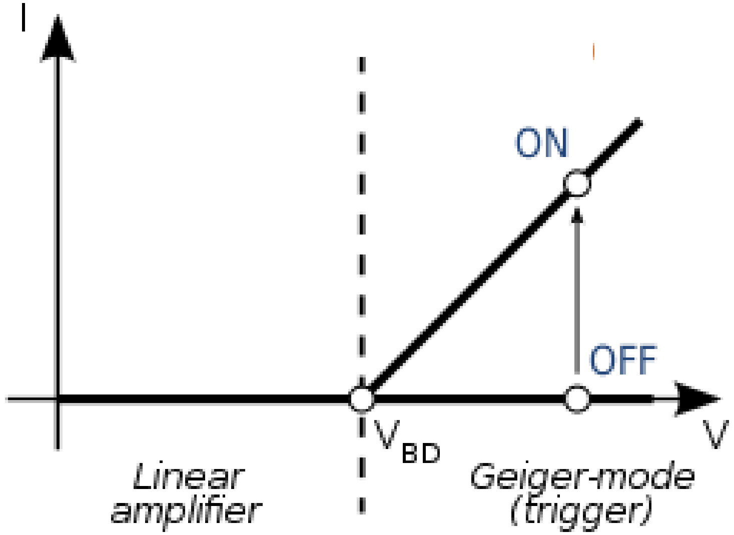
- Eve may exploit the multiple-photon pulses, keep one part of these pulses and send the other part to Bob
- After the classical communication is complete, Eve can obtain the secret-key information without introducing any errors

[1] https://www.cse.wustl.edu/~jain/cse571-07/ftp/quantum/

Detector-blinding attack

- This is the most powerful attack: Eve illuminates strong light to control detectors
- Most available single-photon detector (SPD) are InGaAs/InP APDs operating in Geiger mode, in which they are sensitive to a single photon
- By sending a strong light to Bob, Eve can force Bob’s SPDs to work in a linear mode in which the SPD is only sensitive to bright illumination → detector blinding
- Eve sends Bob a bright pulse with tailored optical power such that Bob’s SPD always report a detection event

=> Eve can perform intercept-and-resend attack



Linear-mode and Geiger-mode APD operation

V_{BD} : the breakdown voltage

Countermeasure: Decoy-state

- It is a countermeasure to overcome PNS attack
- First proposed by W. Hwang in 2003
- The basic idea:
    - Alice can intentionally and randomly replace photon pulses from signal sources (to distribute the key) by multi-photon pulses (decoy states)
    - Eve cannot distinguish multi-photon pulses of signal source from those of decoy source

    ⇒ Alice and Bob can detect PNS by checking the yield of decoy source
- Specifically, Alice adopts two photon sources: signal source, decoy source
    - Signal source: mostly emits single-photon pulses (e.g. BB84 states) to distribute the key
    - Decoy source: mostly emits multi-photon pulses
    - Alice randomly replaces the signal source by decoy source
    - After Bob detects all photon pulses, Alice announces which pulses are from decoy source
- If Eve performs PNS attack
    - The probability she can get the information of the key is low
    - The number of decoy states is changed => Eve is detected

Countermeasure: MDI-QKD

- Measurement-device-independent QKD (MDI-QKD) can close all detection attacks and is fully practical with current technology
- MDI-QKD does not rely on the security of measurement side: the measurement side could be handled by a completely untrustworthy person
- The idea of MDI-QKD inspired from time-reversed EPR-based QKD protocol
- Based on performing Bell state measurement (BSM) for entanglement swapping
  - Bell state measurement: the projection of two qubits onto one of the four entangled Bell states

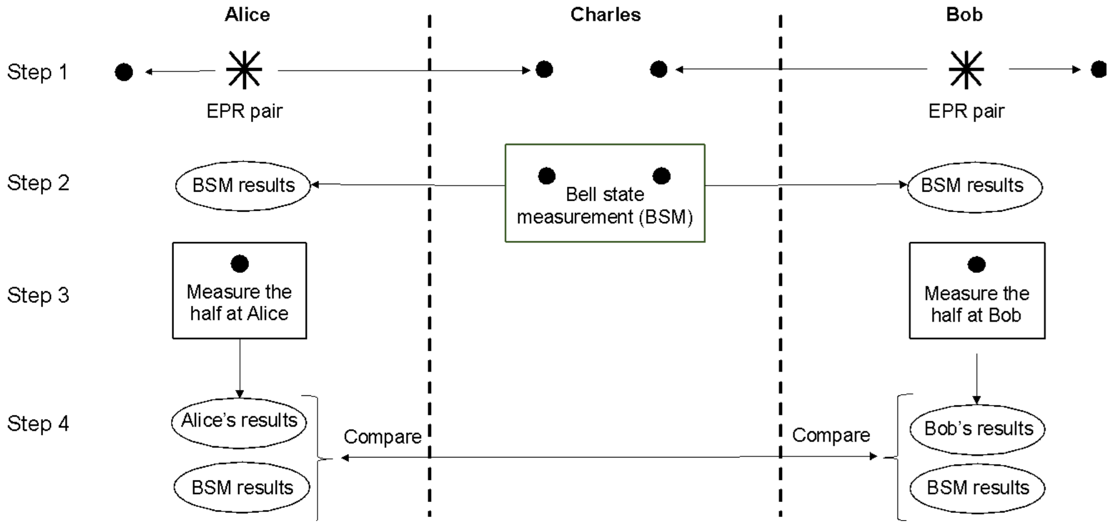
$$|\psi^{+}\rangle = \frac{|00\rangle+|11\rangle}{\sqrt{2}}, |\psi^{-}\rangle = \frac{|00\rangle-|11\rangle}{\sqrt{2}}, |\phi^{+}\rangle = \frac{|01\rangle+|10\rangle}{\sqrt{2}}, |\phi^{-}\rangle = \frac{|01\rangle-|10\rangle}{\sqrt{2}}$$

  - Entanglement swapping:
    - Alice prepare an EPR pair $|\psi^{+}\rangle_{AC_1}$ and send half of it (the C_1 member of the pair) to Charles
    - Bob prepare an EPR pair $|\psi^{+}\rangle_{BC_2}$ and send half of it (the C_2 member of the pair) to Charles
    - Charlie performs BSM on them
      - If he sucessful, entanglement is swapped to the A and B member of two pairs which are kept by Alice and Bob
      - Fact: The A and B member never interacted with one another in the past

EPR-based QKD

- *Step 1*: Each of Alice and Bob prepares an EPR pair and send half of it to an untrusted party Charles
- *Step 2*: Charles then performs a Bell state measurement for entanglement swapping
  - If the BSM is successful, entanglement is swapped to the A and B member which are kept by Alice and Bob
  - After Charles has the BSM measurement results, he will broadcast these results to Alice and Bob
- *Step 3*: Alice and Bob measure their halves of the entangled pairs by using two conjugate bases (⊕ or ⊗)
- *Step 4*: Alice and Bob compare a randomly choosen subset of their measurement results from step 3 whether it satisfies the expected correlations associated with BSM results declared by Charles

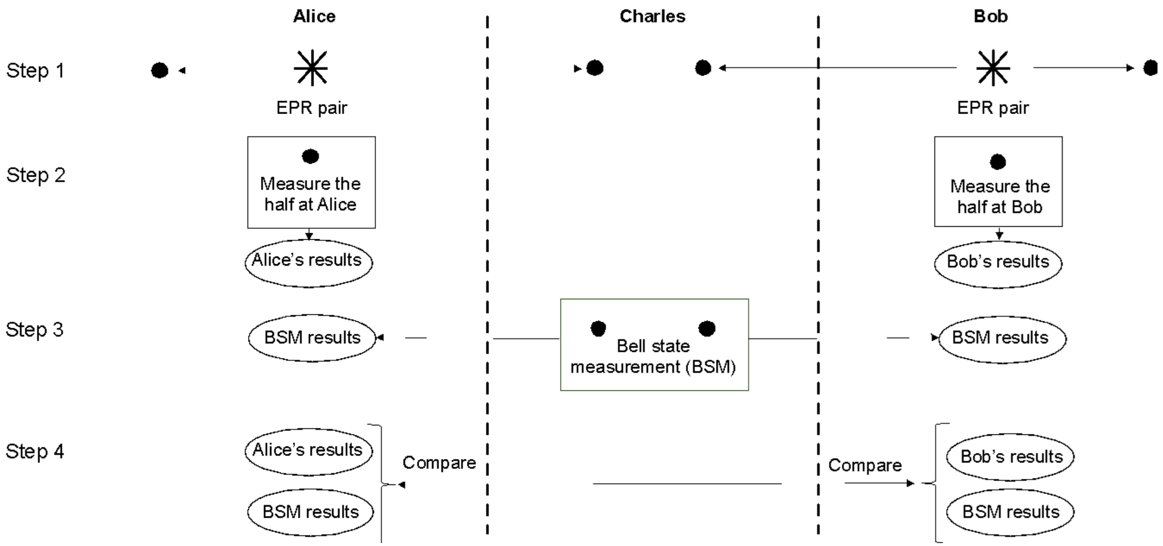
→ Alice and Bob can test the honesty of Charles



Einstein, Podolsky, Rosen (EPR)-based QKD

Time-reversed version of EPR-based QKD

- EPR-based QKD can be implemented in time-reversed version
- In this version, Alice and Bob can measure their halves of EPR pair beforehand. Then, Charles performs BSM for entanglement swapping
- The proposal of MDI-QKD is based on time-reversed version of EPR-based QKD



The time-reversed version of EPR- based QKD

MDI-QKD

- The proposed protocol can be summarized
  - *Step 1*: Each of Alice and Bob uses decoy states and weak coherent pulses generated by a laser source to randomly prepare one of four possible BB84 polarization states $|0\rangle, |1\rangle, |+\rangle, |-\rangle$ (together with decoy states) and send them to an untrusted party, Charles
  - *Step 2*: Charles performs a BSM that projects the incoming signal from Alice and Bob. Then, he uses a classical channel to announce whether his measurements are succesful
  - *Step 3*: Alice and Bob keep the data that correspond to Charles's succesful measurement results and discard the rest.

    Next, Alice and Bob annouce their basis choice and keep the event using same bases
  - *Step 4*: Alice and Bob can compare a randomly chosen subset of their results to check the honesty of Charles

    Then, Alice and Bob perform post-processing procedure to produce secret key
- In MDI-QKD, Alice and Bob are senders, and they transmit signals to an untrusted party, who performs BSM→ This party can be treated as an entirely *black box*

→ MDI-QKD can remove all attack on detection sides

Recent Developments (1)

Recent achievement milestones for fiber-based QKD experiments

Years	Authors	Encoding /Decoding	Scheme	Distance	Secret-key rate	Notes
2018	N. Wang et al. [1]	CV-QKD	Entangled-based	50 km	N/A	Homodyne detection
2018	A. Boaron et al. [2]	DV-QKD	Prepare-and-measure	421 km	6.5 bps	Decoy-state
2019	H. Liu et al. [3]	DV-QKD	Prepare-and-measure	100 km	14.5 bps	Decoy-state, MDI-QKD
2020	K. Wei et al. [4]	DV-QKD	Prepare-and-measure	180 km	6.2 kbps	Decoy-state, MDI-QKD
2020	Y. Zang et al. [5]	CV-QKD	Prepare-and-measure	202.81 km	6.214 bps	Homodyne detection

[1] N. Wang et al., “Long-distance continuous-variable quantum key distribution with entangled states,” Phys. Rev. Applied, vol. 10, no. 6, Art. no. 064028, Dec. 2018.

[2] A. Boaron et al., “Secure quantum key distribution over 421 km of optical fiber,” Phys. Rev. Lett., vol. 121, no. 19, Art. no. 190502, Nov. 2018.

[3] H. Liu et al., “Experimental demonstration of high-rate measurement device- independent quantum key distribution over asymmetric channels,” Phys. Rev. Lett., vol. 122, no. 16, Art. no. 160501, Apr. 2019.

[4] K. Wei et al., “High-speed measurement-device-independent quantum key distribution with integrated silicon photonics,” Phys. Rev. X, vol. 10, no. 3, Art. no. 031030, Aug. 2020.

[5] Y. Zang et al., “Long-distance continuous-variable quantum key distribution over 202.81 km of fiber,” Phys. Rev. Lett., vol. 125, no. 1, Art. no. 010502, Jun. 2020.

Recent Developments (2)

Recent achievement milestones for terrestrial FSO/QKD experiments

Years	Authors	Encoding /Decoding	Scheme	Distance	Secret-key rate	Notes
2015	B. Heim et al. [1]	CV-QKD	Prepare-and-measure	1.6 km	N/A	Homodyne detection
2017	S. K. Liao et al. [2]	DV-QKD	Prepare-and-measure	53 km	0.4 kbps	Decoy-state
2019	S. Shen et al. [3]	CV-QKD	Entangled-based	460 m	0.152 kbps	Homodyne detection
2020	Y. Cao et al. [4]	DV-QKD	Prepare-and-measure	19.2 km	6.11 bps	Decoy-state, MDI-QKD

[1] B. Hem et al., “Atmospheric continous-variable quantum communication,” New J. Phys., vol. 16, Art. no. 113018, 2015.
[2] S. K. Liao et al., “Long-distance free-space quantum key distribution in daylight towards inter-satellite communication,” Nature Photonics, vol. 11, pp. 509-513, Jul. 2017.
[3] S. Shen et al., “Free-space continuous-variable quantum key distribution of unidimensional Gaussian modulation using polarized coherent states in an urban environment,” Phys. Rev. A, vol. 100, no. 1, Art. no.
012325, Jul. 2019.
[4] Y. Cao et al., “Long-distance free-space measurement-device independent quantum key distribution,” Phys. Rev. Lett., vol. 125, no. 26, Art. no. 260503, Dec. 2020.

Recent Developments (3)

Recent achievement milestones for satellite FSO/QKD experiments

Years	Authors	Encoding /Decoding	Scheme	Distance	Secret-key rate	Notes
2017	S. K. Liao et al. [1]	DV-QKD	Prepare-and-measure	388-719 km	91 bps	Decoy state, LEO satellite (Tiangong-2 space lab)
2017	K. Gunthner et al. [2]	CV-QKD	Prepare-and-measure	38600 km	N/A	Homodyne detector, GEO satellite (Alphasat)
2017	H. Takenaka et al. [3]	DV-QKD	Prepare-and-measure	650- 1000 km	N/A	LEO microsatellite (SOCRATES)
2018	S. K. Liao et al. [4]	DV-QKD	Prepare-and-measure	600- 1000 km	3 kbps-9 kbps	Decoy state, LEO satellite (Micius)
2020	J. Yin et al. [5]	DV-QKD	Entangled-based	750 km	0.12 bps	LEO satellite (Micius)

[1] S. K. Liao et al., “Space-to-ground quantum key distribution using a small-sized payload on Tiangong-2 space lab,” Chin. Phys. Lett., vol. 34, no. 9, Art. no. 090302, 2017.

[2] K. Gunthner et al., “Quantum-limited measurements of optical signals from a geostationary satellite,” Optica, vol. 4, Art. no. 611, 2017.

[3] H. Takenaka et al., “Satellite-to-ground quantum-limited communication using a 50-kg-class microsatellite,” Nat. Photon., vol. 11, no. 8, pp. 502-508, 2017.

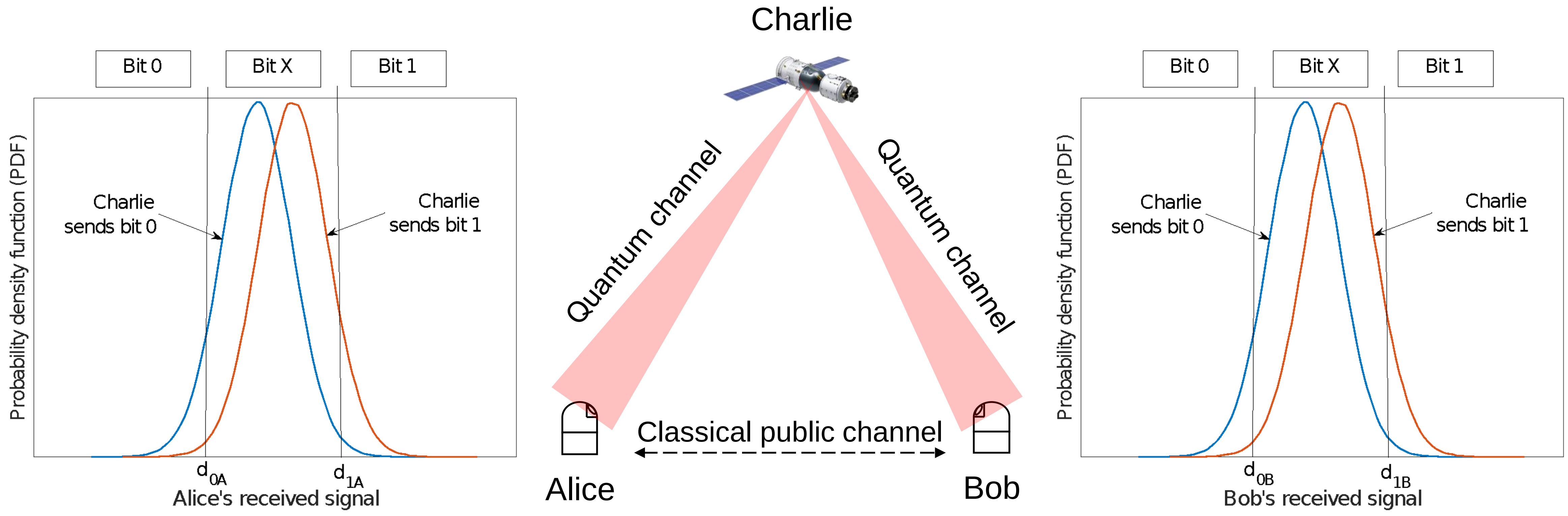
[4] S. K. Liao et al., “Satellite-relayed intercontinental quantum network,” Phys. Rev. Lett., vol. 120, no. 3, Art. no. 030501, Jan. 2018.

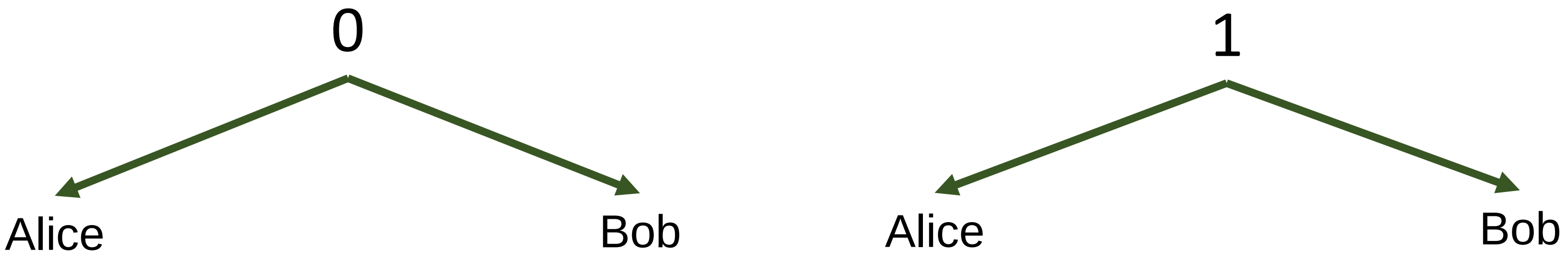
[5] J. Yin et al., “Entanglement-based secure quantum cryptography over 1,120 kilometres,” Nature, vol. 582, pp. 501-505, Jun. 2020.

Conclusion

- This presentation surveys the fundamentals of QKD, aspects of QKD implementation, QKD protocols, typically practical attacks, and countermeasures for these attacks
- The recent developments of optical fiber-based QKD, terrestrial FSO-based QKD, and satellite FSO-based QKD are also presented

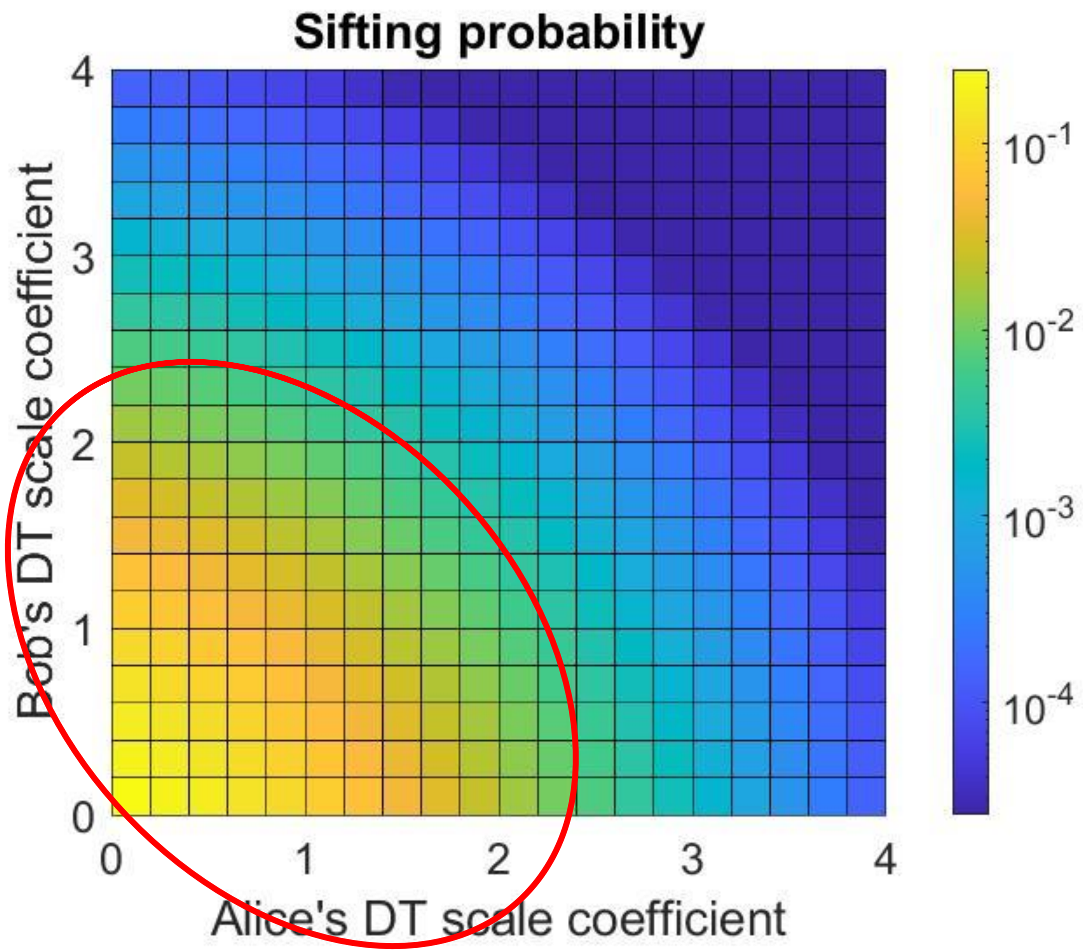
Thank you!


Charlie
Bit 0
Bit X
Bit 1
Probability density function (PDF)
Charlie sends bit 0
Charlie sends bit 1
d_{0A}
d_{1A}
Alice's received signal
Quantum channel
Quantum channel
Classical public channel
Alice
Bob
Bit 0
Bit X
Bit 1
Probability density function (PDF)
Charlie sends bit 0
Charlie sends bit 1
d_{0B}
d_{1B}
Bob's received signal

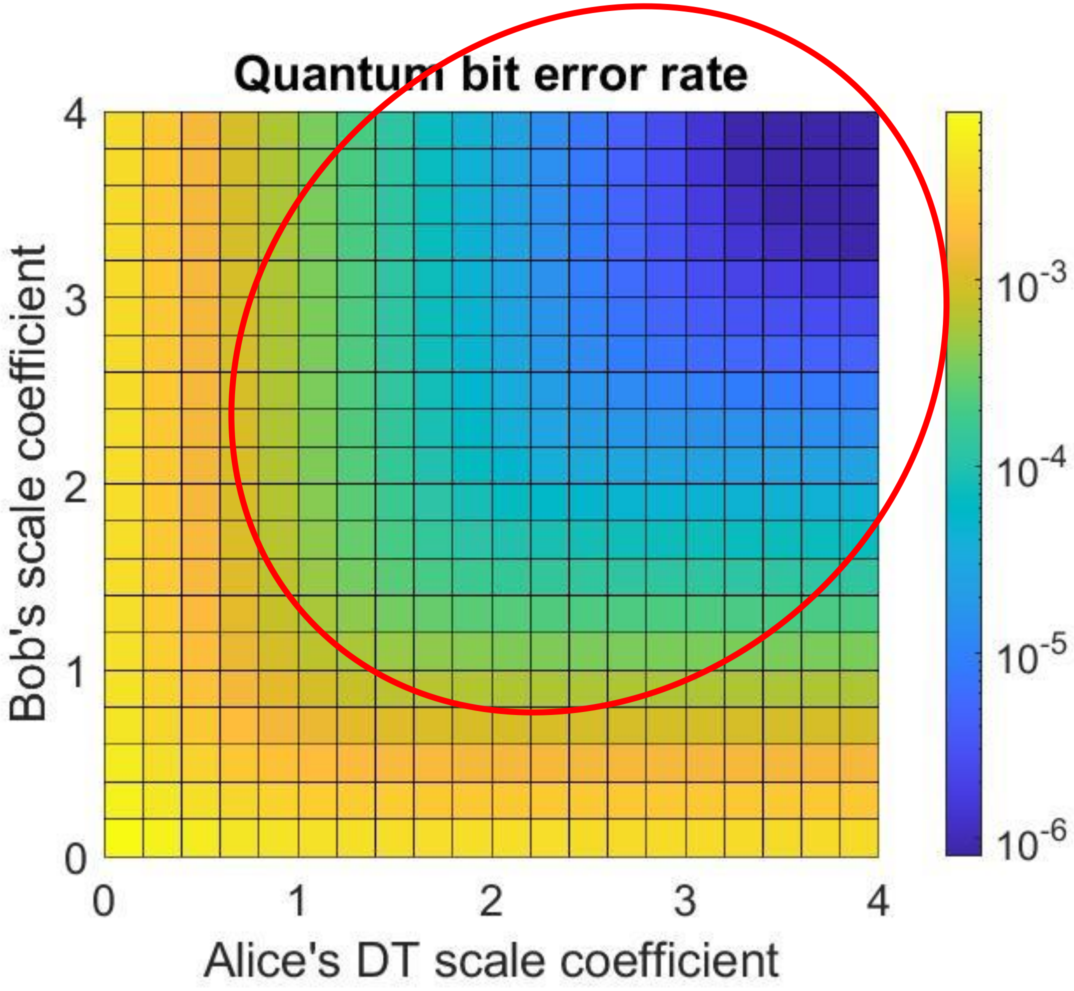

0
Alice
Bob
1
Alice
Bob

No.	Charlie	Alice			Bob			Sifted key
	Bit	Thresholds	Time	Bit	Thresholds	Time	Bit	
1	0	d_0	t_0	X	d_0	t_0	0	discarded
2	1	d_1	t_1	1	d_1	t_1	X	discarded
3	0	d_0	t_2	X	d_0	t_2	X	discarded
4	1	d_1	t_3	1	d_1	t_3	1	1
5	0	d_0	t_4	0	d_0	t_4	0	0
6	1	d_1	t_5	0	d_1	t_5	1	error
7	0	d_0	t_6	1	d_0	t_6	0	error

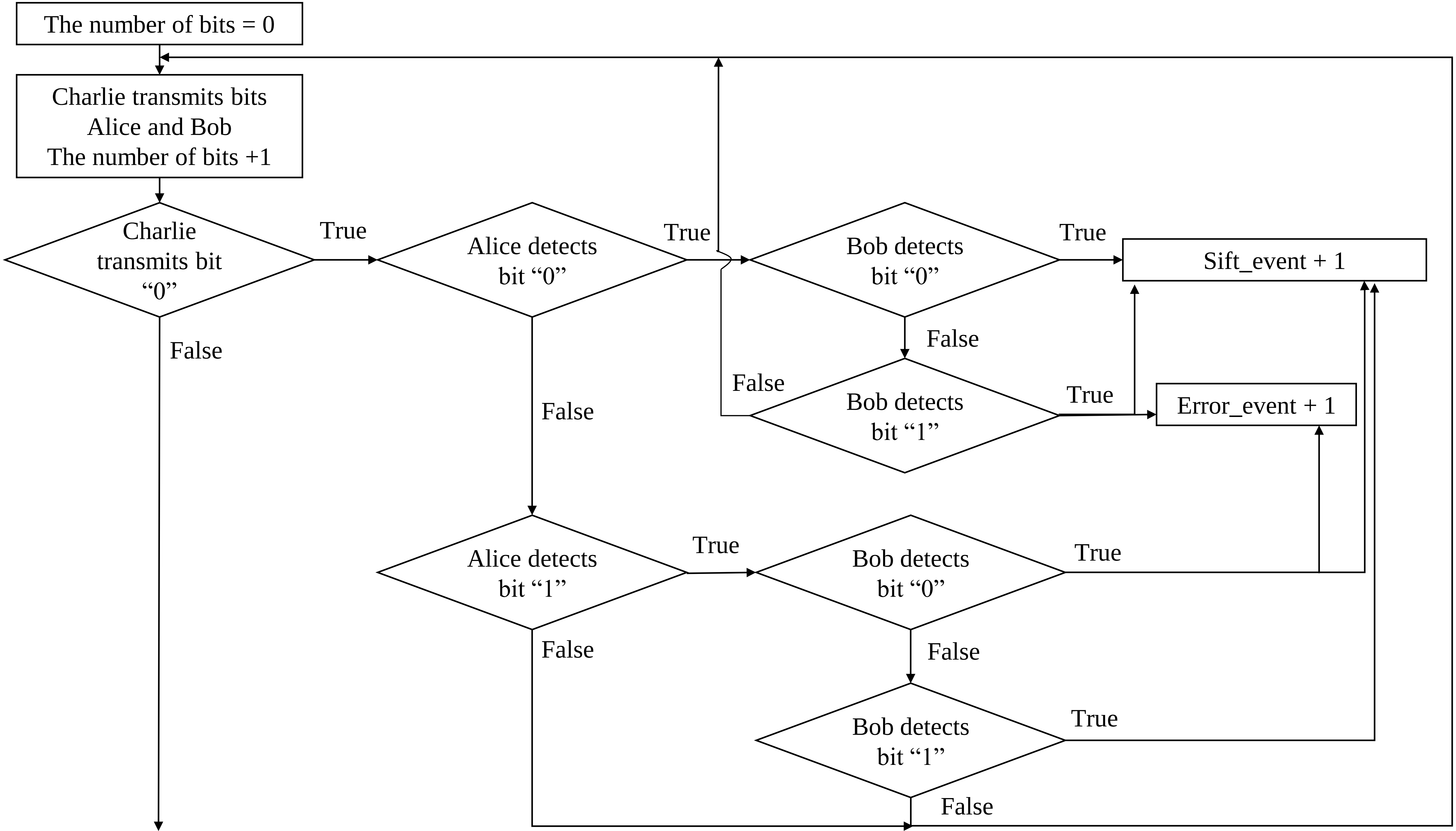
Case 6 and case 7 is corrected based on the detected bits of Alice in step 4 by *information reconcilliation*

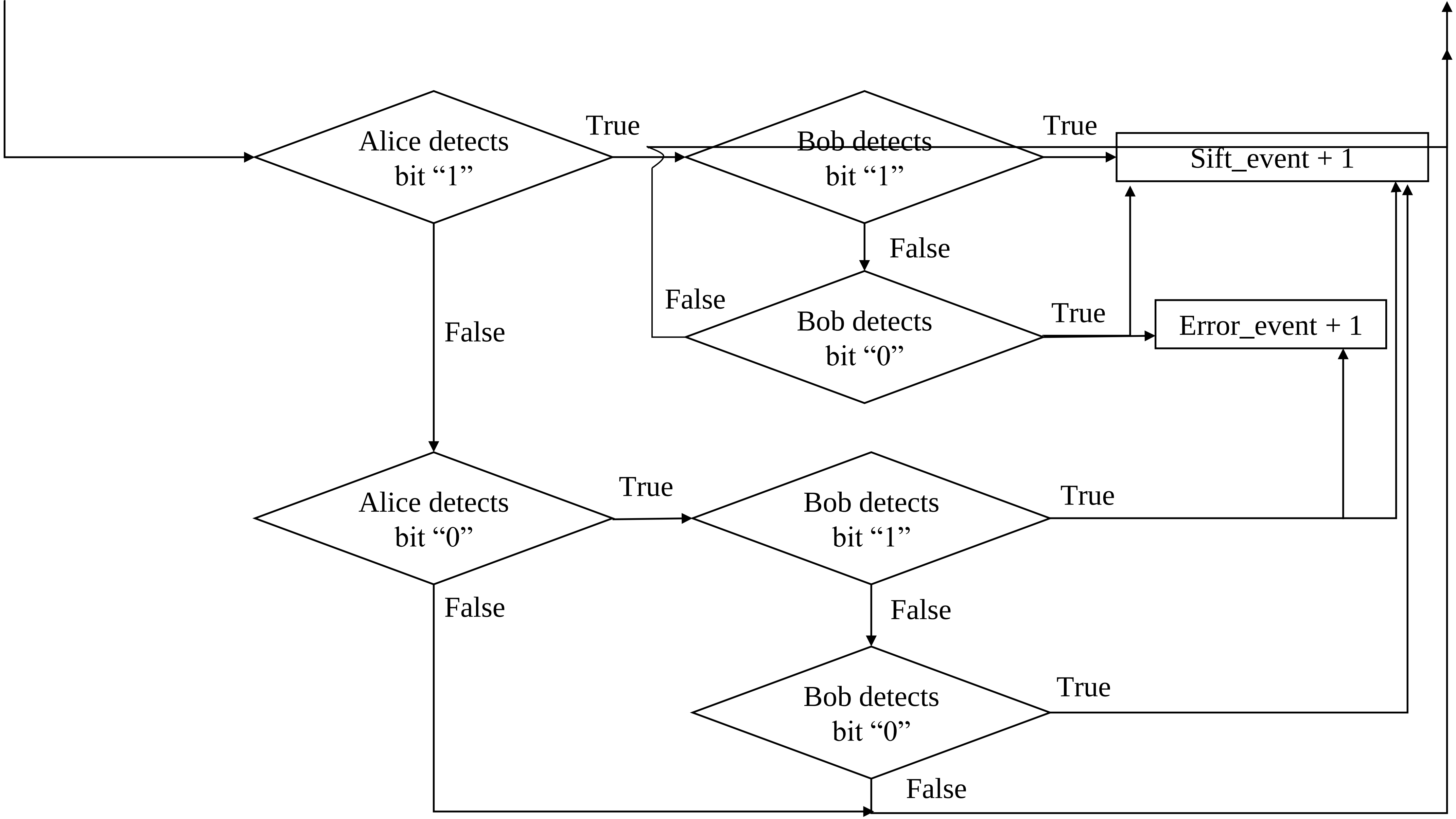


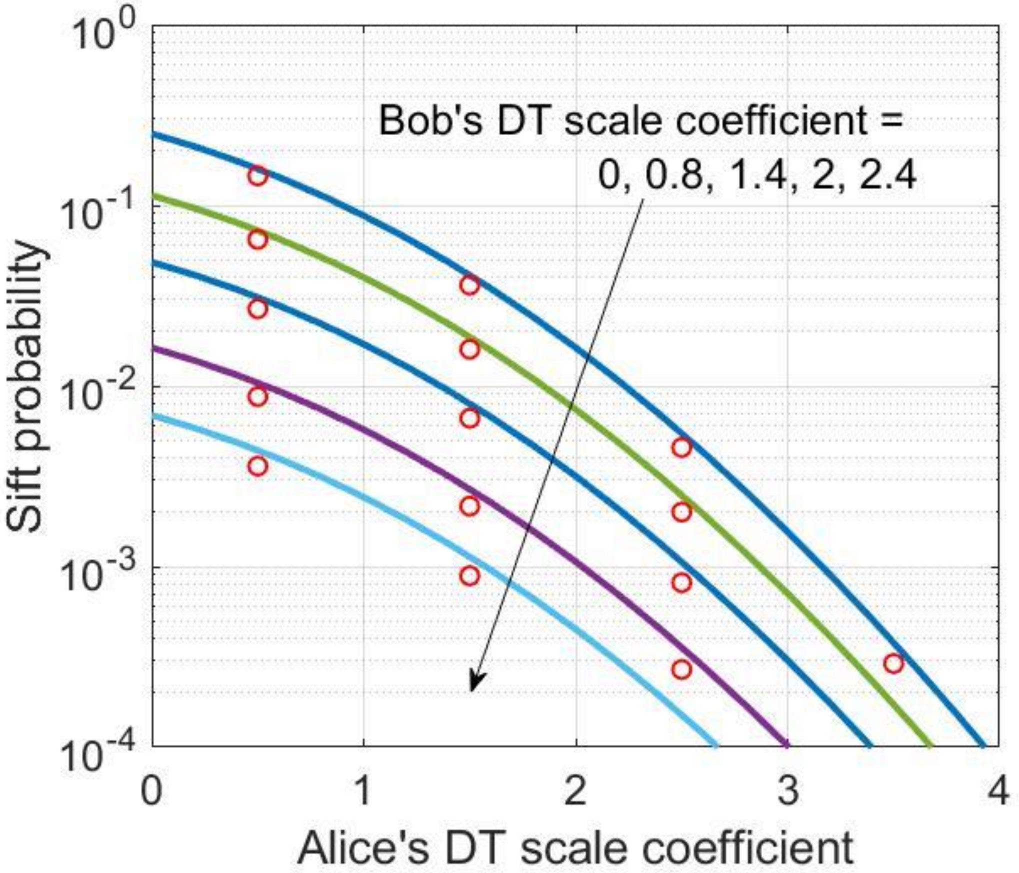
Sifting probability

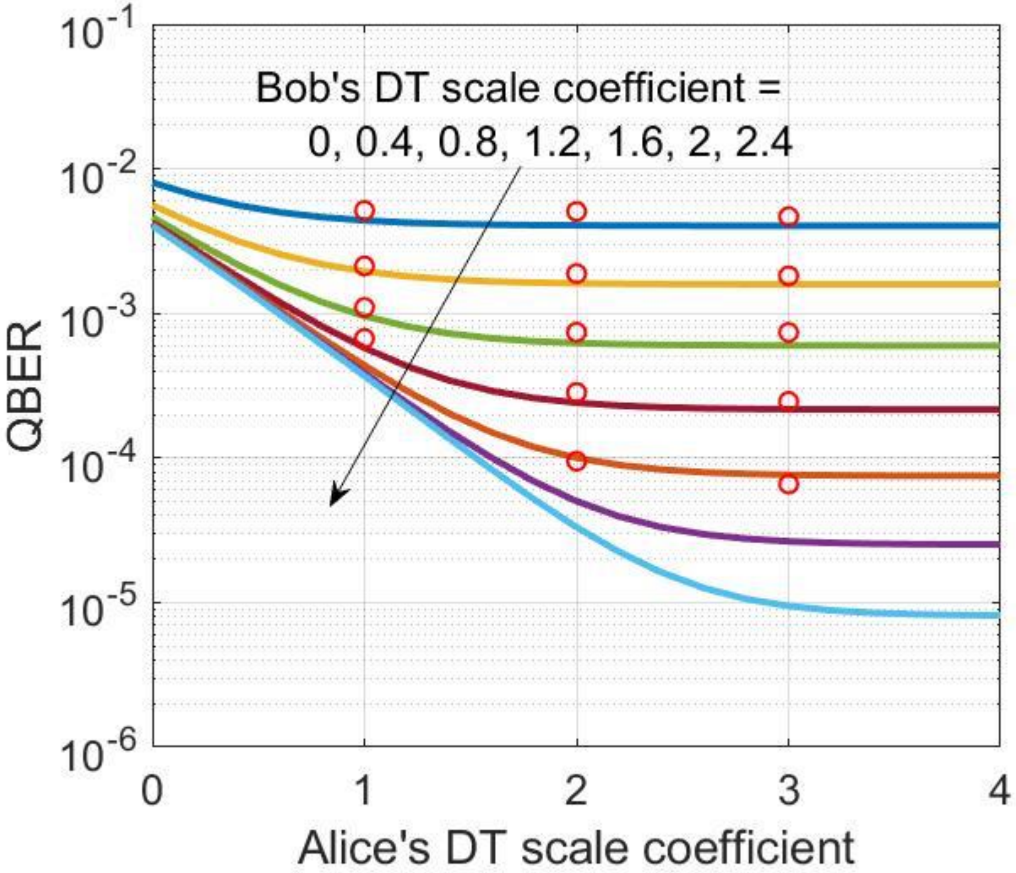


Quantum bit error rate


The number of bits = 0
Charlie transmits bits
Alice and Bob
The number of bits +1
Charlie
transmits bit
“0”
True
False
Alice detects
bit “0”
True
False
Bob detects
bit “0”
True
Sift_event + 1
False
Bob detects
bit “1”
True
Error_event + 1
False
Alice detects
bit “1”
True
False
Bob detects
bit “0”
True
False
Bob detects
bit “1”
True
False

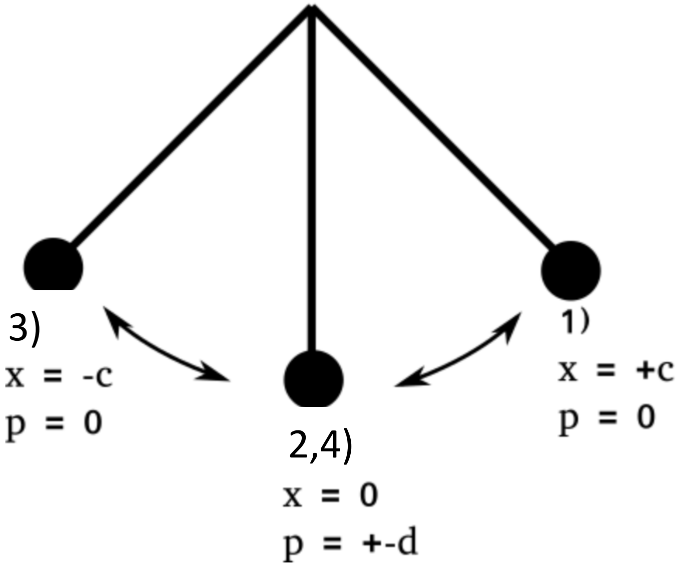

Alice detects bit “1”
True
Bob detects bit “1”
True
Sift_event + 1
False
False
Bob detects bit “0”
True
Error_event + 1
False
Alice detects bit “0”
True
Bob detects bit “1”
True
False
False
Bob detects bit “0”
True
False

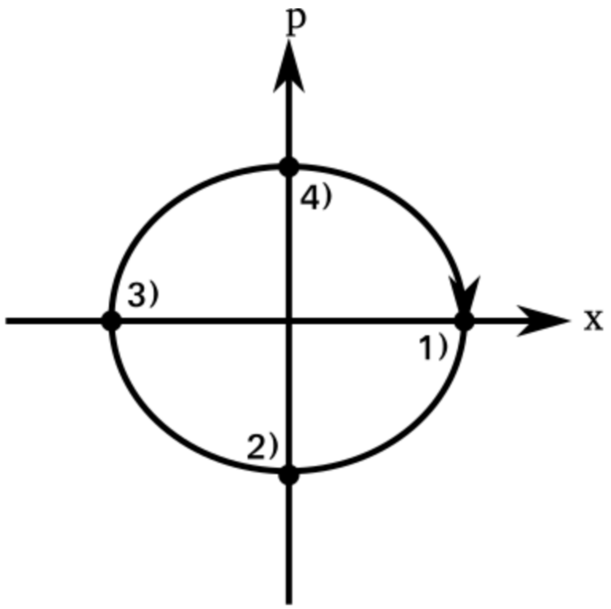

Bob's DT scale coefficient =
0, 0.8, 1.4, 2, 2.4
Sift probability
10^{0}
10^{-1}
10^{-2}
10^{-3}
10^{-4}
0
1
2
3
4
Alice's DT scale coefficient


Bob's DT scale coefficient =
0, 0.4, 0.8, 1.2, 1.6, 2, 2.4
QBER
10^{-1}
10^{-2}
10^{-3}
10^{-4}
10^{-5}
10^{-6}
0
1
2
3
4
Alice's DT scale coefficient

CV-QKD

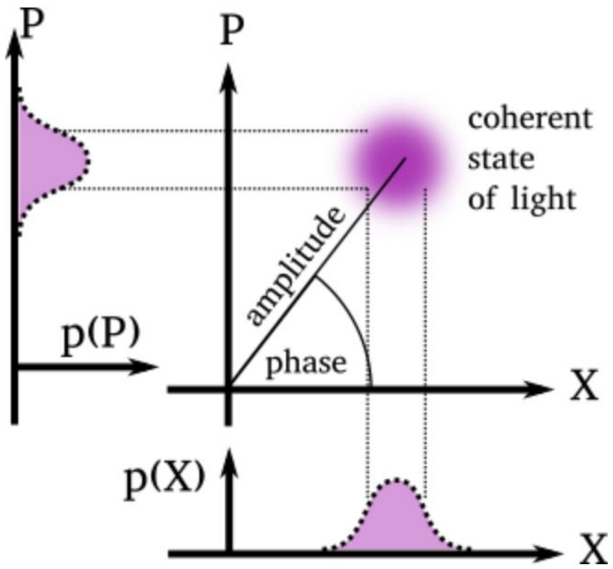
- A good tool to depict states of light: optical phase space
- To illustrate optical phase space, let make an analogy to classical mechanics: classical phase space
  - A pendulum has two major physical quantities: the position *x* of the pendulum, and its momentum *p*





CV-QKD

- States of light can be depicted in the optical phase space
- Light describes as an electromagnetic waves: it is similar to the periodic oscillation of the pendulum
- The position X and momentum P are used to describe the electric field of light in the optical phase space



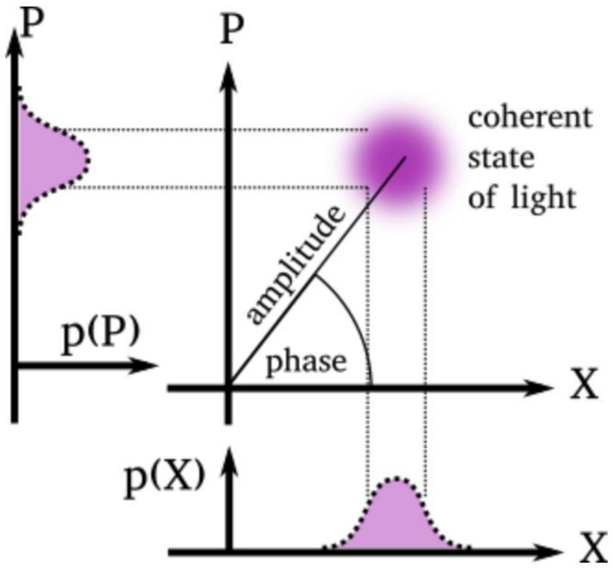
A typical state of light, emitted by a laser

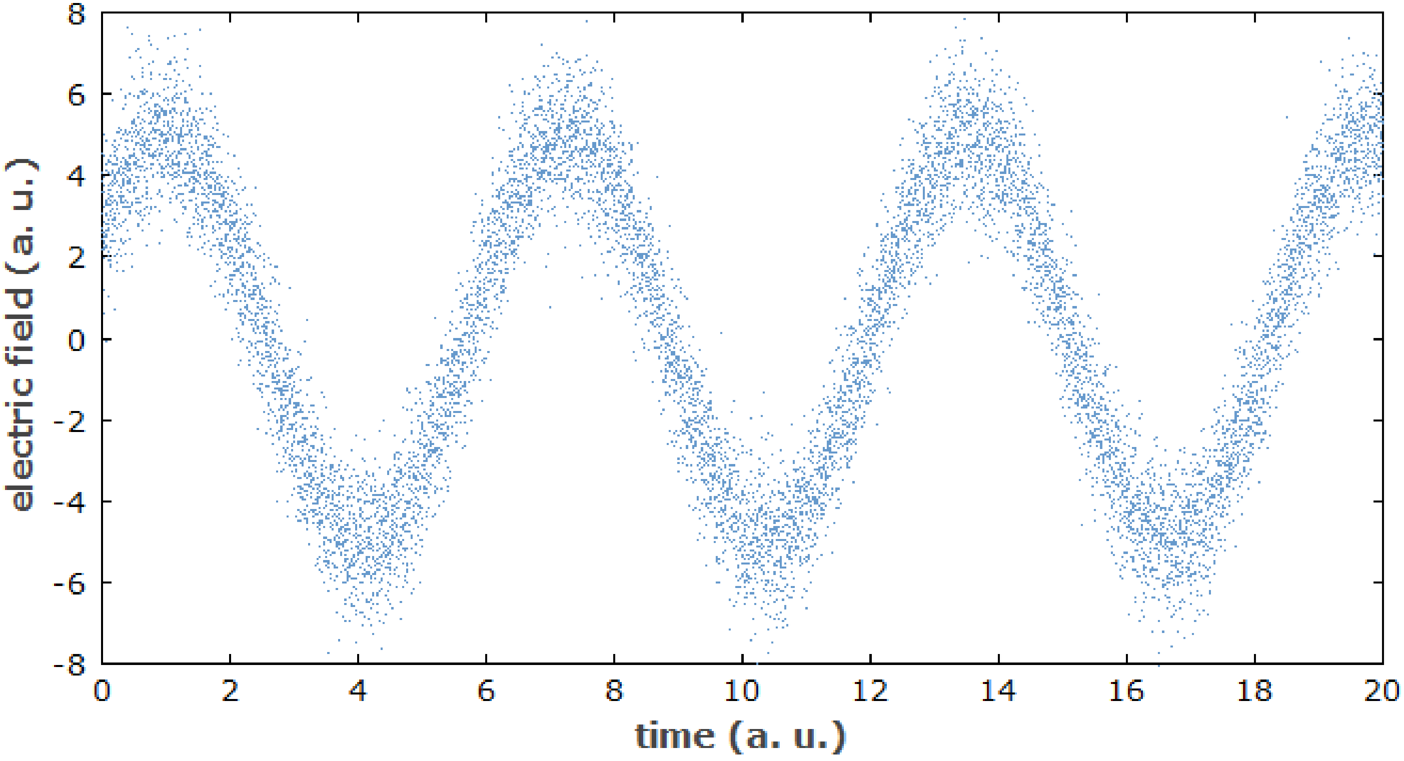
Why does the coherent state have a probability distribution instead of single point?

The reason is Heisenberg’s uncertainty relation which causes the exact position and momentum of classical mechanics to be fuzzy probability distribution in quantum mechanics

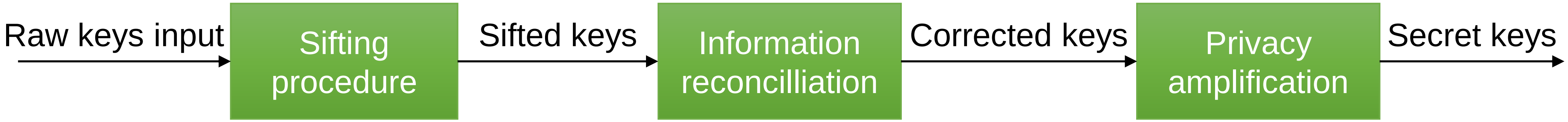
Heisenberg’s uncertainty relation states that simultaneous precise measurement of the position and momentum is not possible

CV-QKD


P
P
coherent
state
of light
amplitude
phase
p(P)
X
p(X)
X


8
6
4
2
0
-2
-4
-6
-8
0
2
4
6
8
10
12
14
16
18
20
electric field (a. u.)
time (a. u.)

Post-processing procedures



- Alice and Bob use the classical authenticated channel (e.g. the Internet) to perform post-processing procedures
- Bob discloses to Alice the time instants that he was able to detect the encoded key bits → forming their shared raw keys
- Alice discloses to Bob her encoding scheme on the key bits he detected, they keep the detected bits which have the same encoding scheme → forming their sifted key
- The sifted keys may contain error, Alice and Bob perform the information reconcilliation procedure (using error correction code) on the sifted key
- To exclude the information which can be leaked out to Eve, Alice and Bob perform the privacy amplification (using hash function) on the corrected keys to make new, shorter keys