DEPARTMENT OF NETWORKED SYSTEMS AND SERVICES

Qauntum key distribution (QKD)

2025 spring

Máté Galambos

Department of Networked Systems and Services

galambos.mate@vik.bme.hu

Budapest, 2025. 03. 23.

MŰEGYETEM 1782

Revision

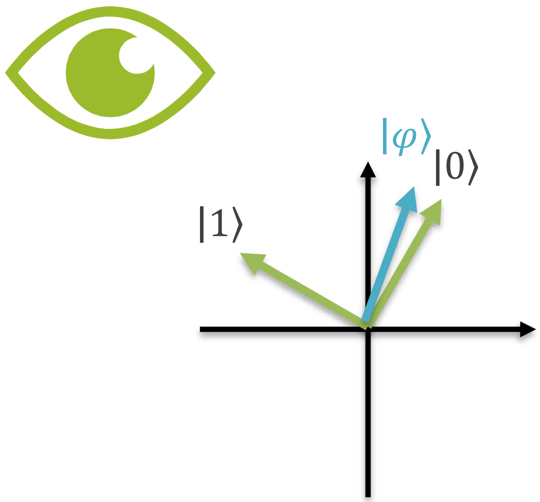
REVISION

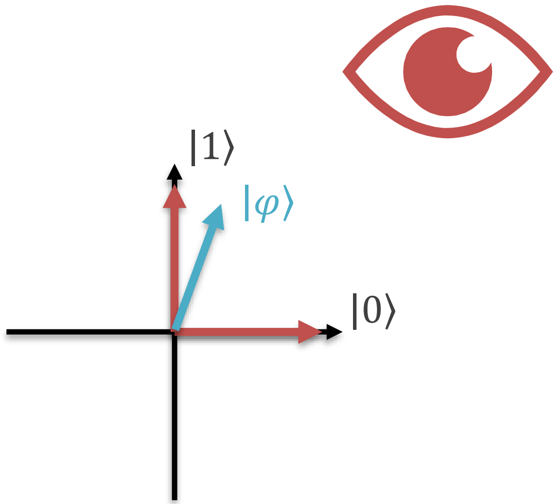
Measurement changes the state

$$p(m) = \langle\psi|M_m^\dagger M_m|\psi\rangle ,$$

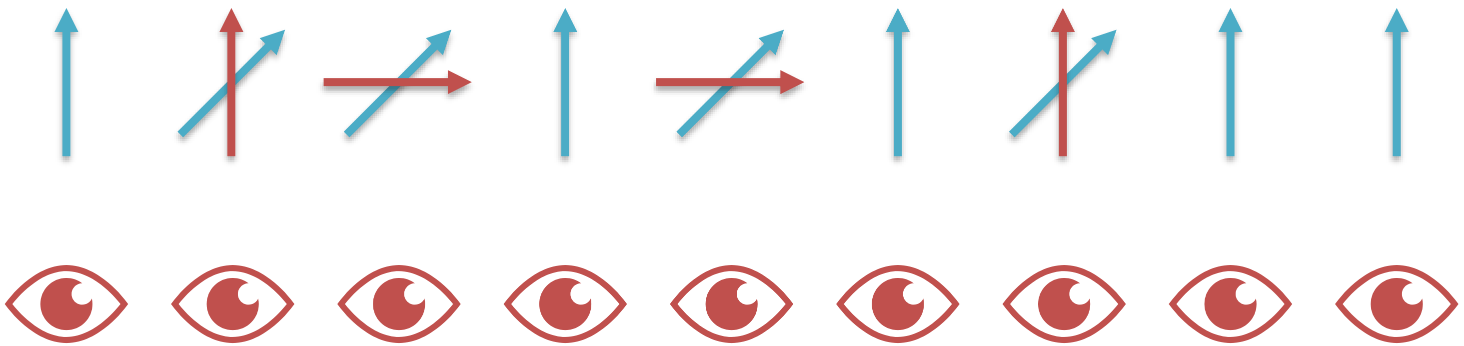
$$\frac{M_m|\psi\rangle}{\sqrt{\langle\psi|M_m^\dagger M_m|\psi\rangle}} .$$

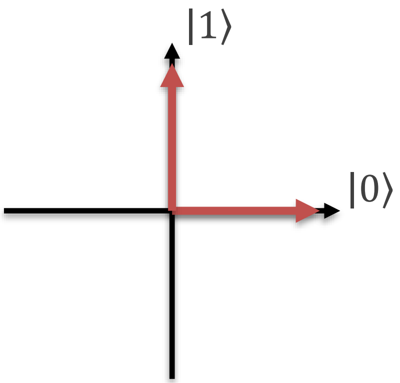
We must choose the measurement basis carefully



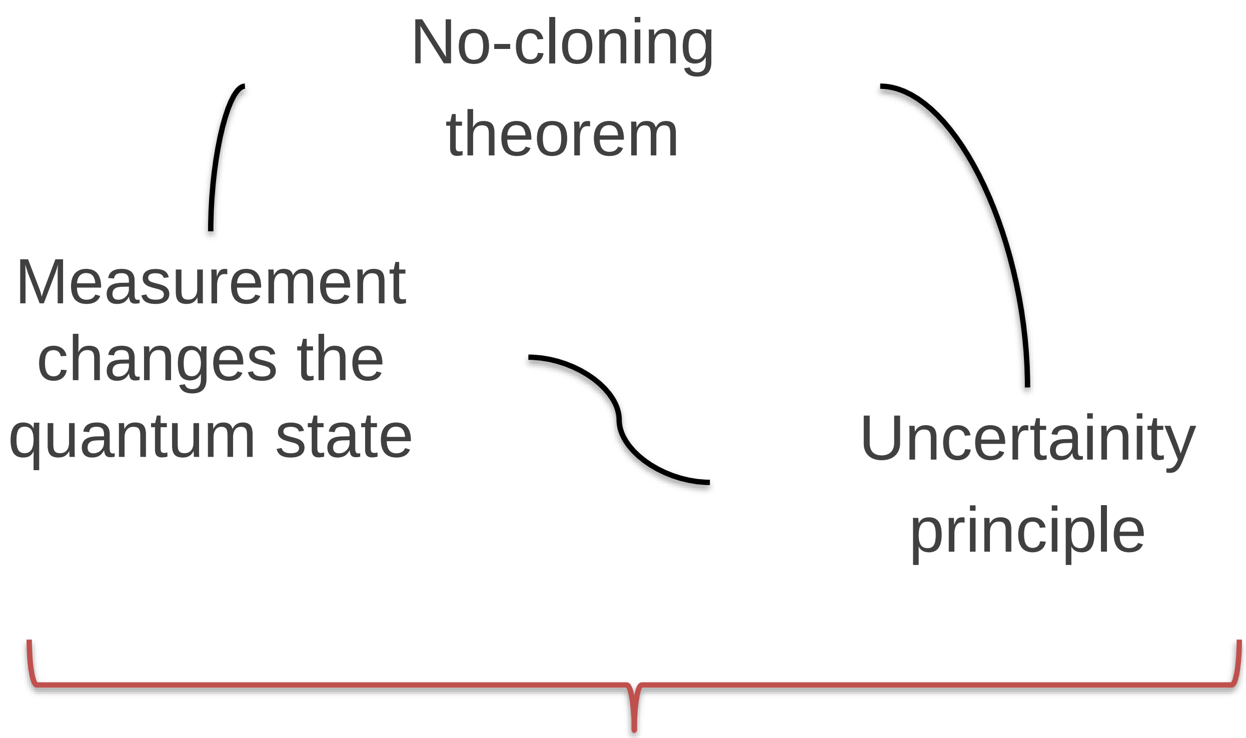


REVISION





REVISION



Quantum information cannot be known perfectly

„Its damned hard to lie my lord when one does not know the truth."

– Péter Eszterházy
(Hungarian writer)

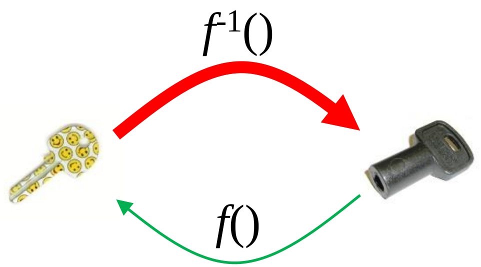
Quantum information
cannot be known perfectly

Security risk (motivation)

SECURITY RISK

Critical infrastructure must be protected from cyberattacks

Classical cryptography



Public-key cryptography

- Publick key for encryption
- Private key for decryption

- There is know proof that there is no efficient attack against it
- **Quantum threat: Shor's algorithm**

Symmetric-key cryptography

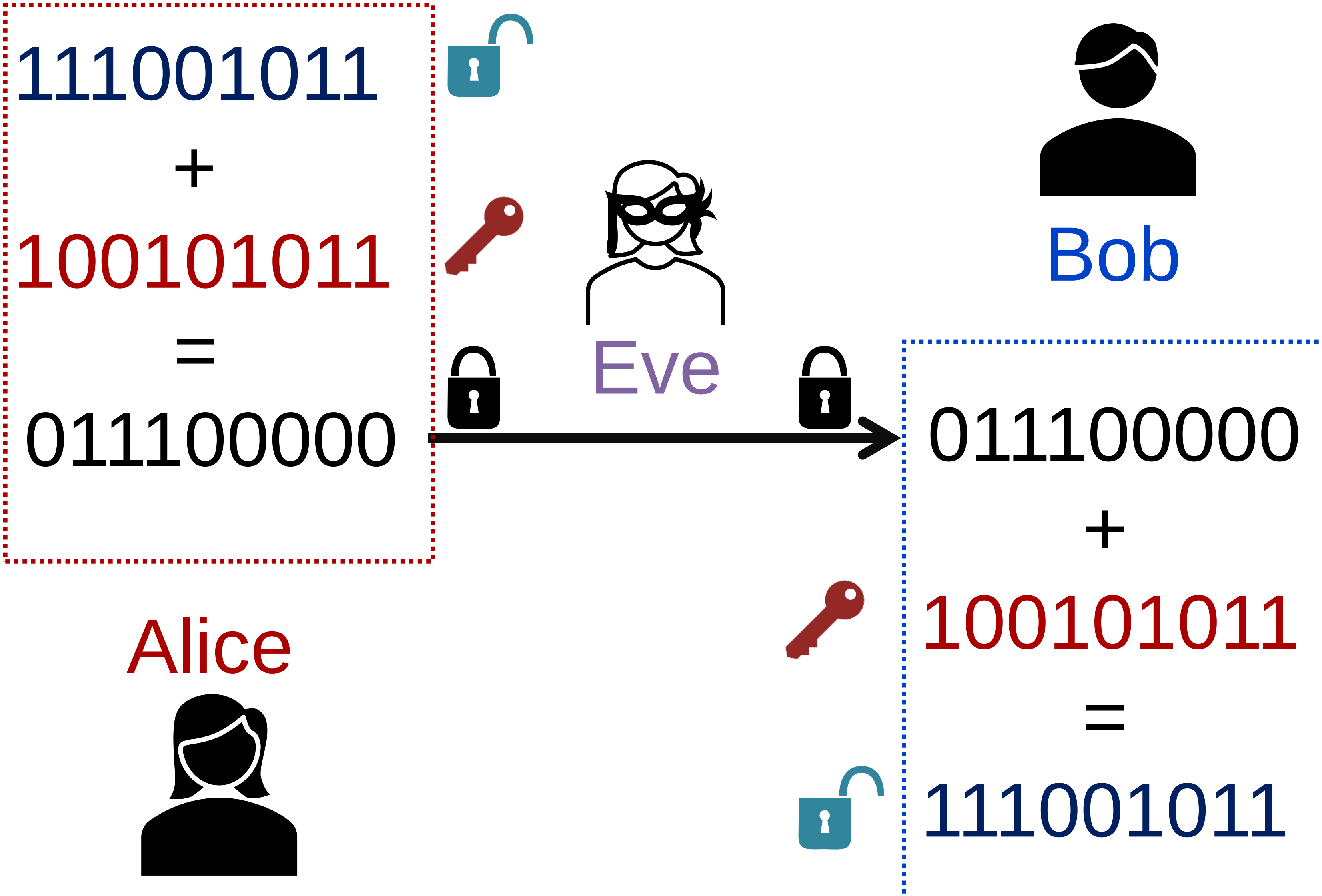
- The same key is available for both encryption and decryption

- Can be provably secure if certain constraints are met
- Problem: how to transmit the key from one side to the other???

What is the ideal password like?

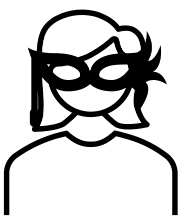
- Long
  - As long as the plaintext
- Unpredictable (random)
  - Bits are equally likely
  - Bits are independent from each other
  - Bits are independent from anything the attacker has access to

ONE TIME PAD
VERNAM CYPHER



ONE TIME PAD

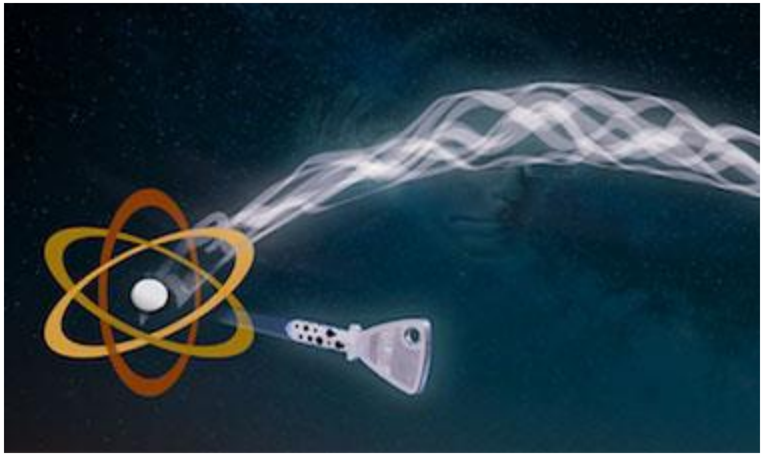
	00000	01110
	00001	01111
	00010	01100
01110		
	11110	10000
	11111	10001



But: key distribution is problematic

Solution:

Quantum Key Distribution (QKD)



Quantum key distribution (QKD)
(Also known as quantum key expansion)

BASIC IDEA OF KEY DISTRIBUTION

- Prepare and measure
  - Transmitter picks a key bit, sends it of the receiver
- Magical sticky notes:
  - You can only look at one of their sides

- Entanglement based
  - Uses (often maximally) entangled states
- Twin coins:
  - One coin flip determines the value of the other

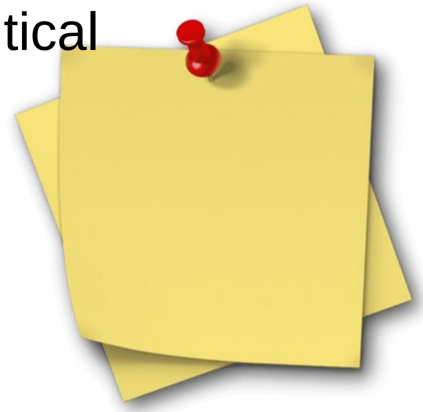
BASIC IDEA OF A PREPARE AND MEASURE PROTOCOL

- Measurement changes the state
- Magical notes:
  - I can write only one of its sides
  - If somebody looks at the other side, my message gets erased (and a random bit replaces it)
  - I write my password (each bit on a new note)
  - If somebody reads it, the integrity decreases
  - If we detect that a key leaked, we do not use that key, we send another one

Confidentialty ⟷ Integrity

BASIC IDEA OF A PREPARE AND MEASURE PROTOCOL

- How do we know which half of the sticky notes we should look at?
  - We don't
  - We consult afterwards to see who used what
  - We keep the identical ones
  - We discard notes where we used opposite sides
  - Error estimation
    - We sacrifice a portion of the key to see if it is identical



QKD PROTOCOLS

SARG04

E91

BB84

S09

B92

COMPARING TYPES OF QKD PROTOCOLS

- Prepare and measure
  - Simple to implement
  - Has the most advanced security analysis
  - Most protocols are not as secure if there is an implementation error/deviation from theory
- Entanglement based
  - Can be more robust against noise
  - Can ensure longer range communication
  - Harder and more expensive to realize

COMPARING TYPES OF QKD PROTOCOLS

- DV: discreet variable
  - The degree of freedom that we use to encode bit values can only have discreet values (e.g., number of photons)
- CV: continuous variable
  - The degree of freedom can have infinite number of values (e.g., position along the x axis)

COMPARING TYPES OF QKD PROTOCOLS

Category	Salient Features	Pros & Cons
Discrete Variable protocols	**Quantum Signal:** Single photons/ Entangled photons with information encoded as polarization, time-bin / linear momentum states[10] **Detectors:** Single Photon Detectors (SPDs) Prepare and Measure (PM) Entanglement Based (EB)	**Pros:** Compared to CV; DV schemes are optimal in case of harsh channel conditions/ attenuations **Cons:** Detector-induced dark counts; multi-photon pulse probability makes the signal more susceptible to photon number splitting PNS attacks.
Continuous Variable protocols	**Quantum Signal:** Amplitude and phase quadrature of electromagnetic fields are exploited for encoding information in coherent states of light **Detectors:** coherent homodyne or heterodyne detection.	**Pros:** Comparative to DV these protocols are easier to implement with standard telecom components offering higher key rates in metropolitan distances. **Cons:** Requires stability against channel imperfections.

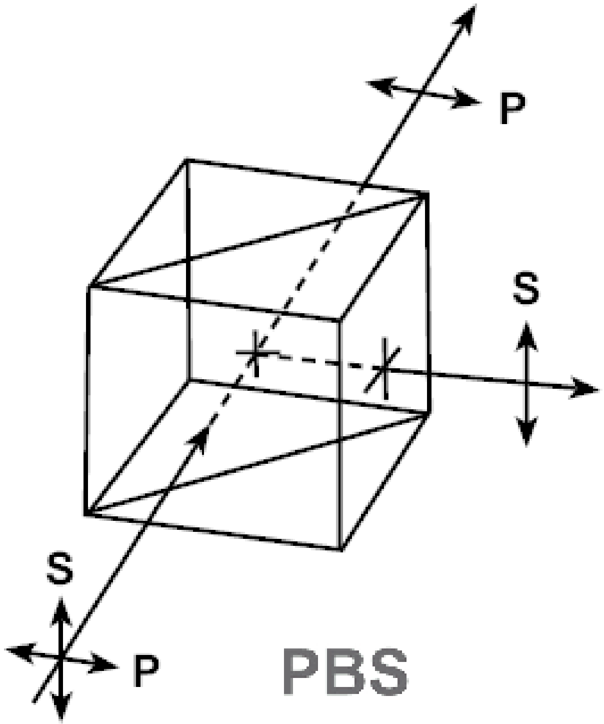
COMPARING TRANSMISSION MEDIUMS

- Optical fiber
  - Uses existing fiber optic network.
    - Dark fiber: used only for quantum communication. Well protected from noise, but wasteful and expensive to rent.
    - With classical communication: some wavelength range is reserved for quantum communication, that coexists with classical data. More noisy, shorter range, but cheaper.
- Free space
  - Photons are sent through air or the vacuum of space.
    - Distortion and losses are strongest at the lowermost layers of the atmosphere
    - Losses can be very low over large distances in space
    - Must be protected from noise with proper filters

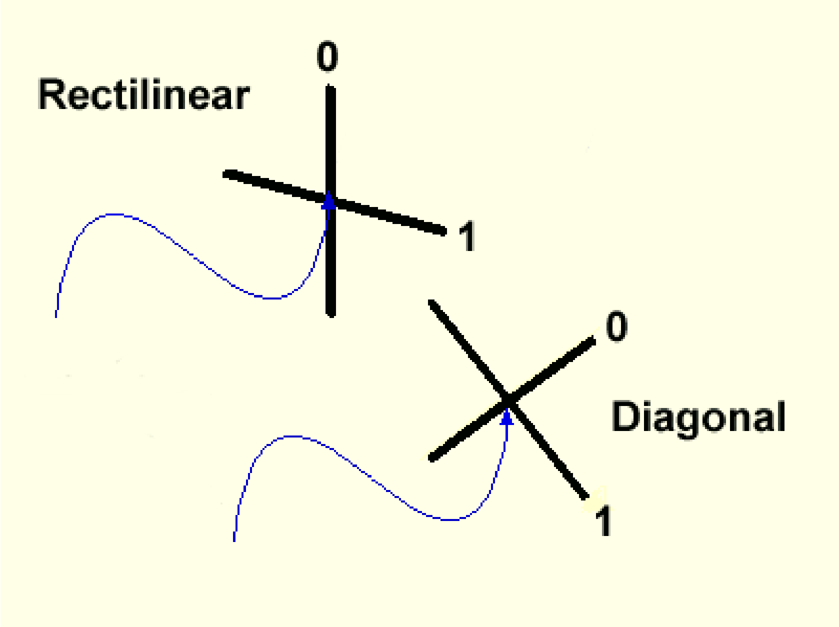
Bennett-Brassard 84 protocol (BB84)

Charles H. Bennett, Gilles Brassard, „Quantum Cryptography: Public Key Distribution and Coin Tossing", Proc. of. Int. Conf. on Computers, Systems & Signal Processing, Bangalore, India, Dec. 10-12, 1984

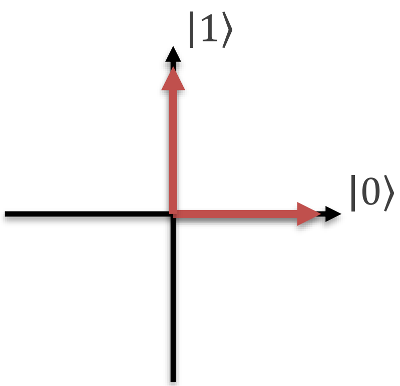
LET US MEASURE

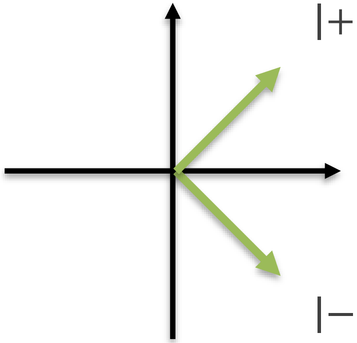


Polarization encoded
bit values



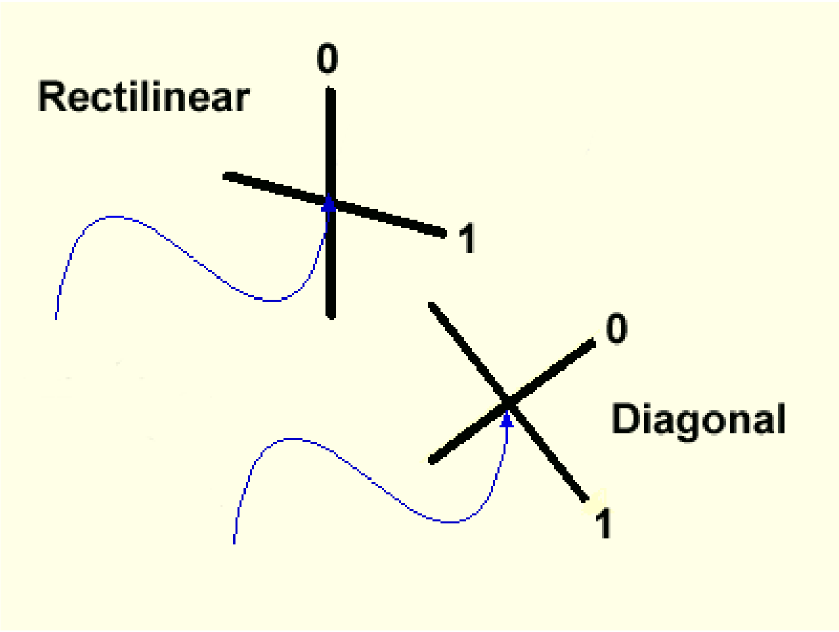
LET US MEASURE





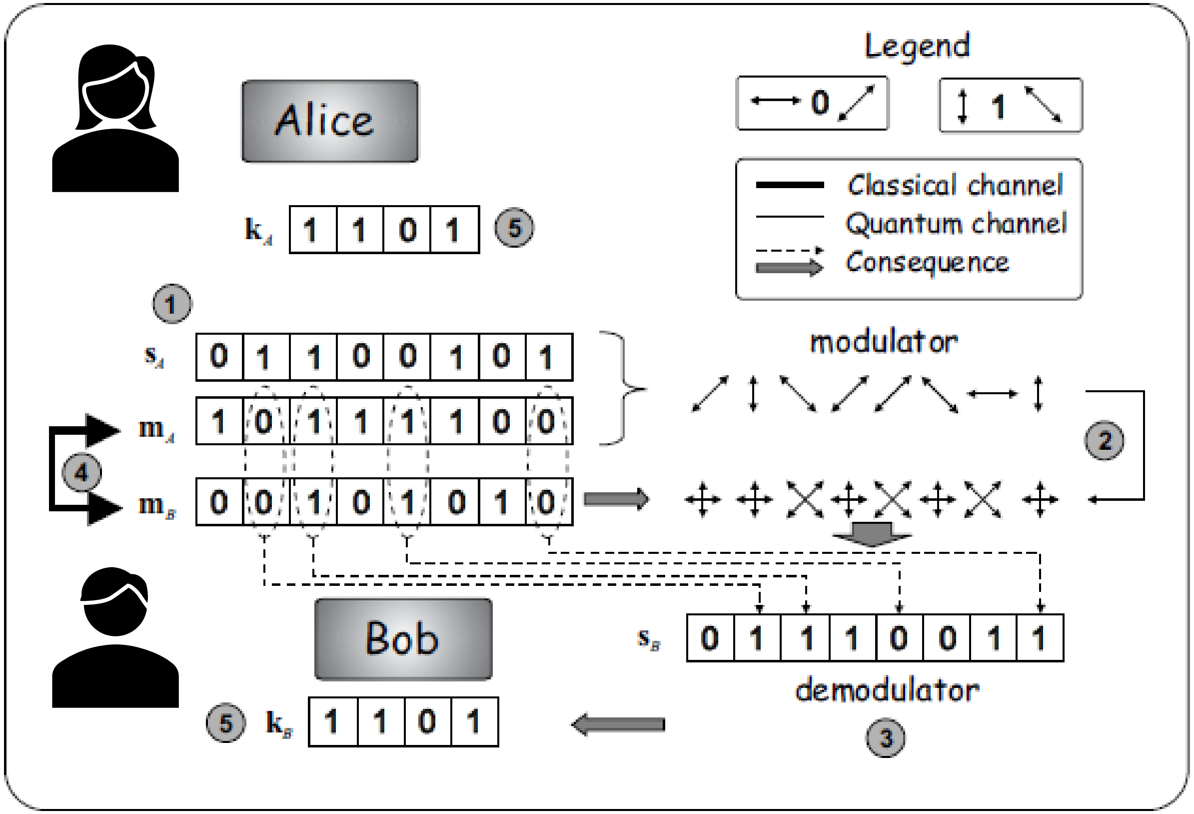
$$|+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} = H|0\rangle$$

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

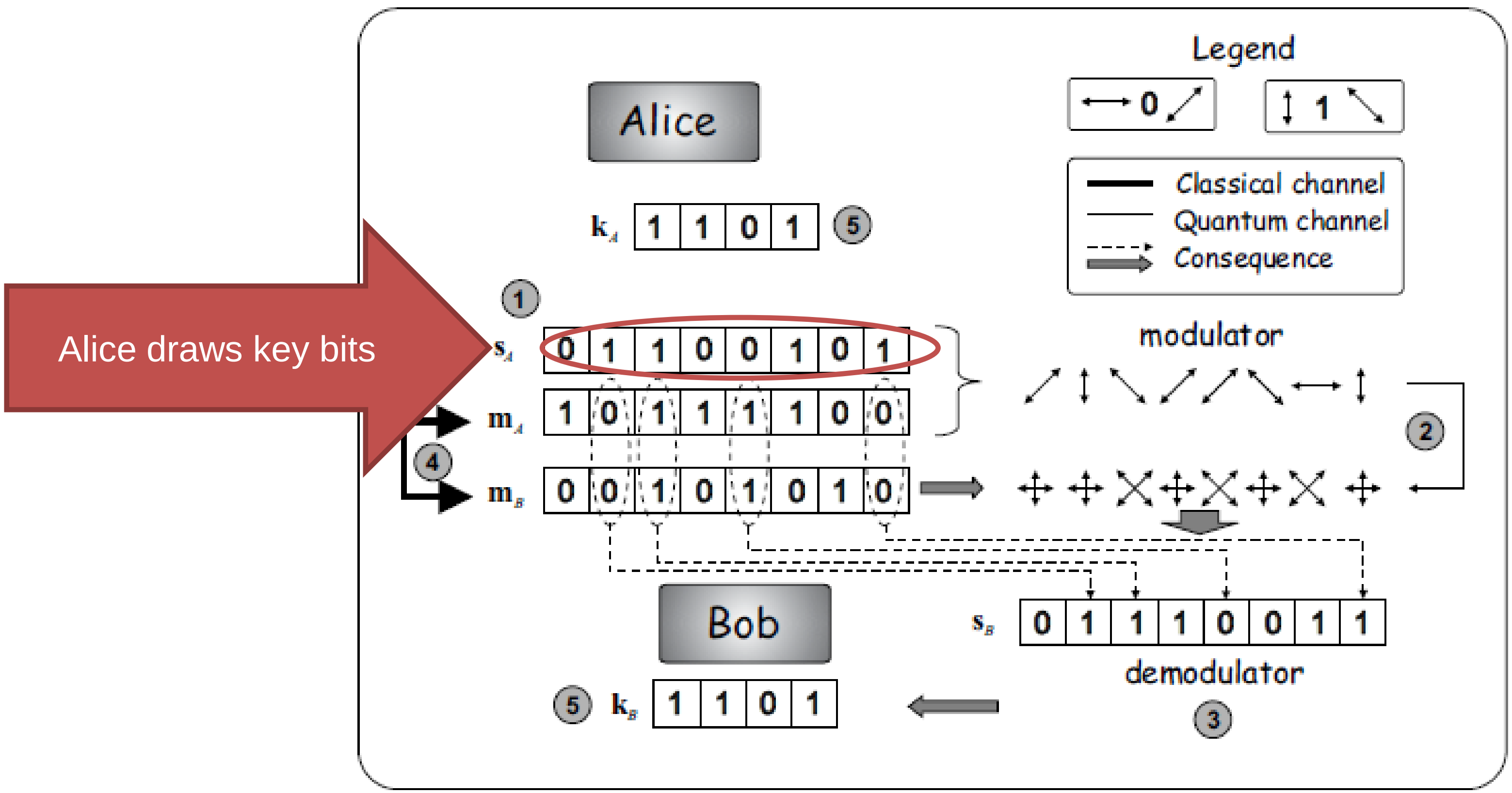


BB84

- First generation solution
  - Qubit is encoded in polarization
  - Challenge: producing and measuring single photons

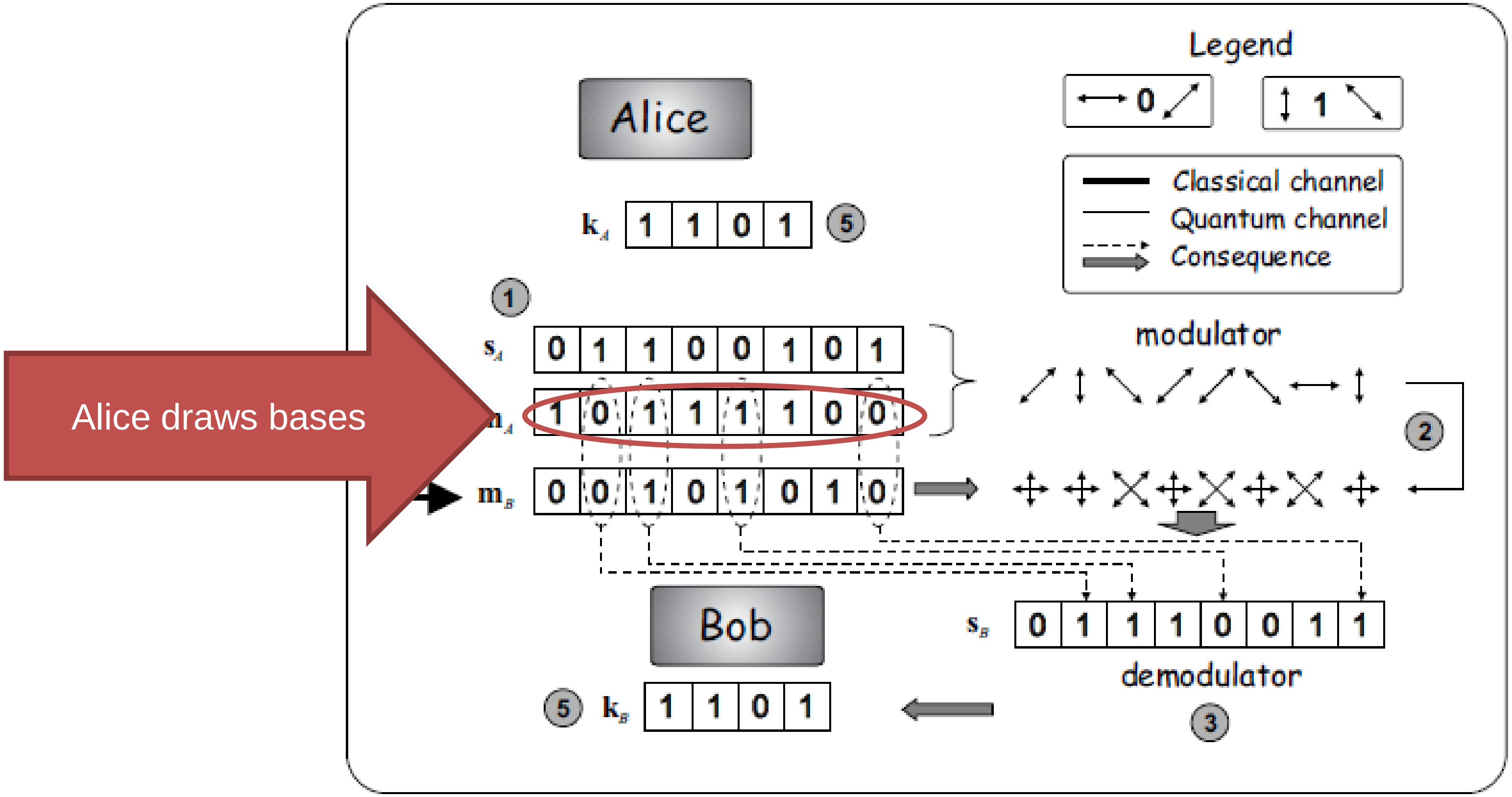


- First generation solution
  - Qubit is encoded in polarization
  - Challenge: producing and measuring single photons



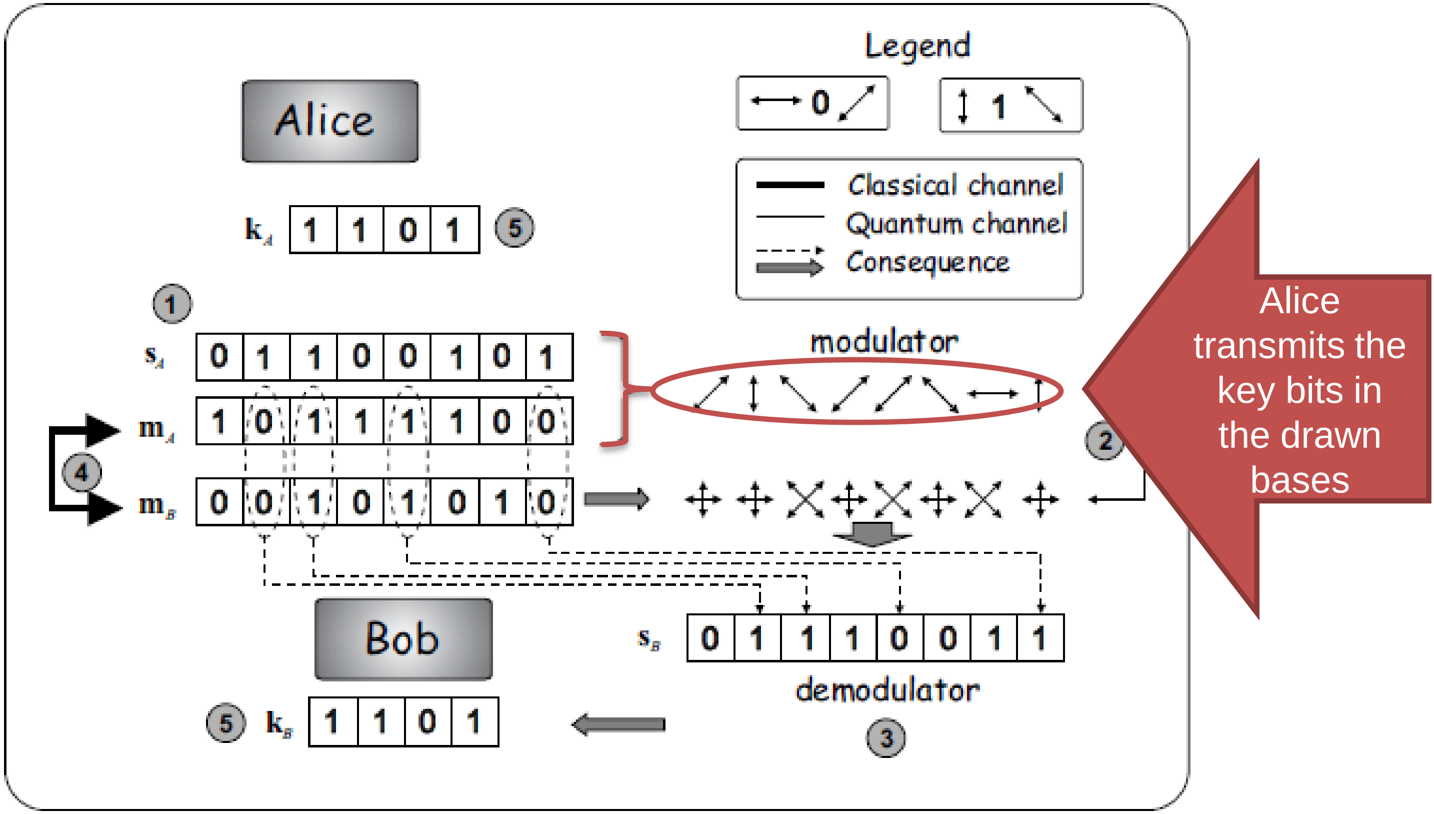
BB84

- First generation solution
  - Qubit is encoded in polarization
  - Challenge: producing and measuring single photons



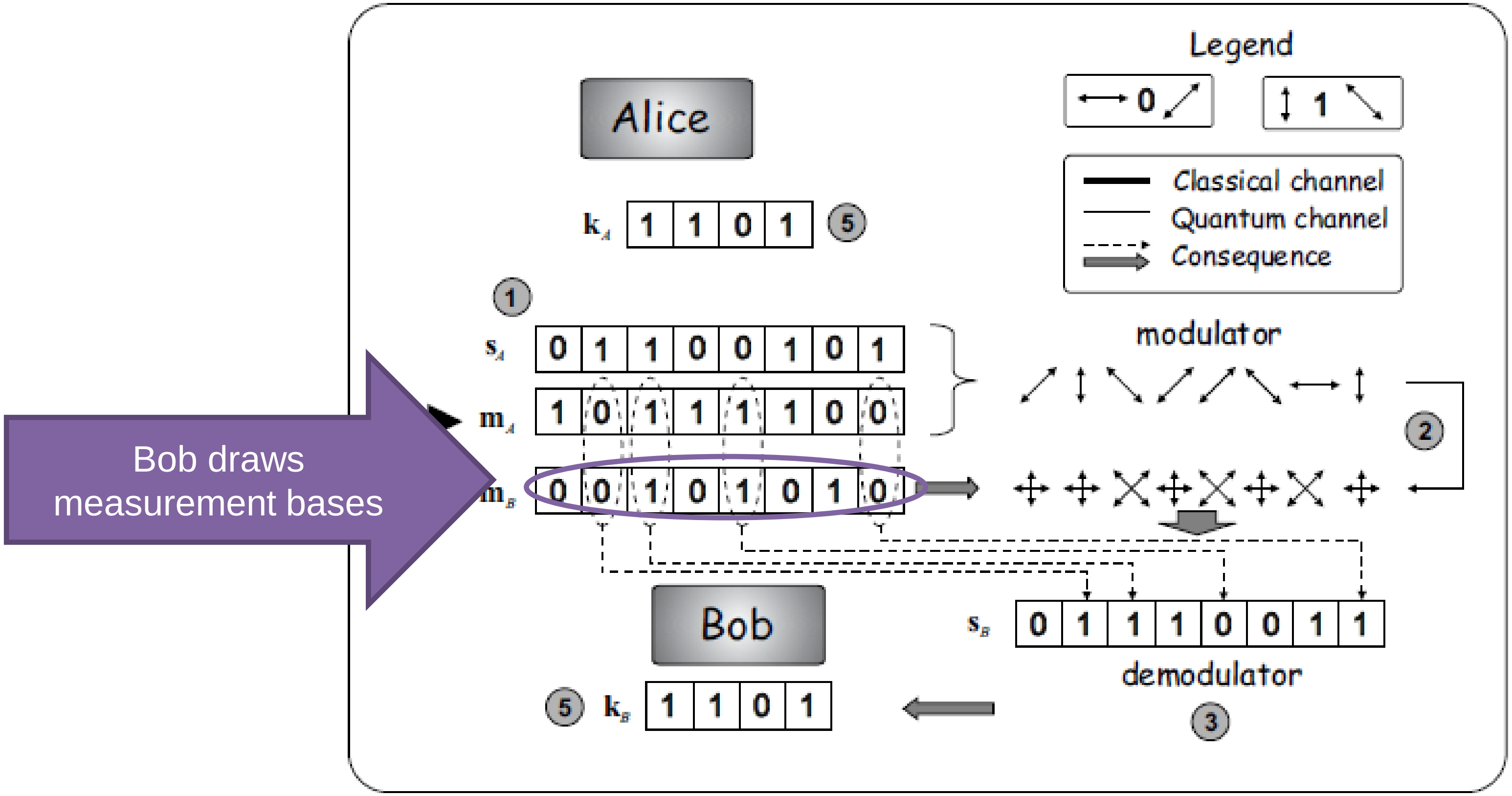
BB84

- First generation solution
  - Qubit is encoded in polarization
  - Challenge: producing and measuring single photons



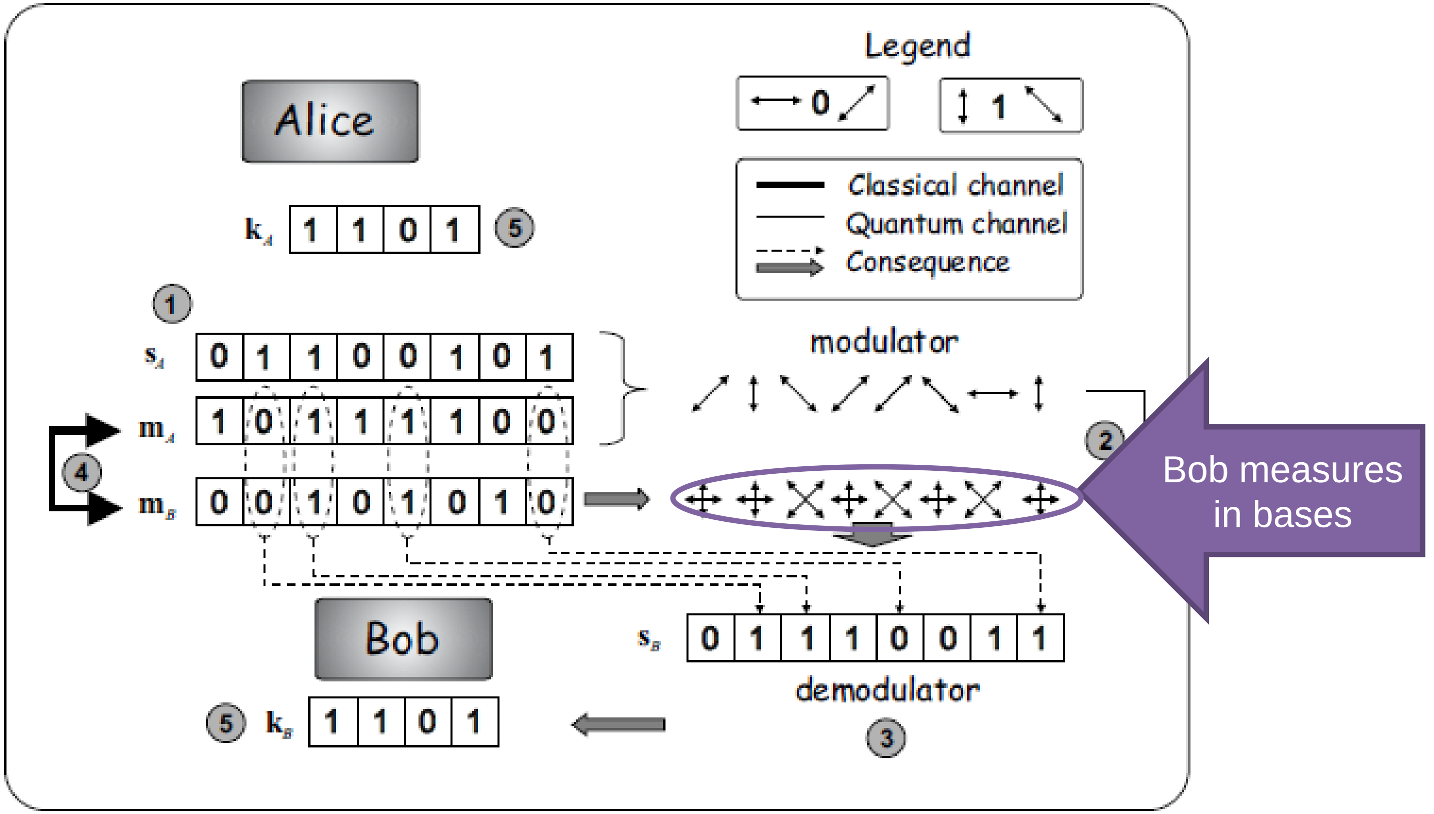
BB84

- First generation solution
  - Qubit is encoded in polarization
  - Challenge: producing and measuring single photons



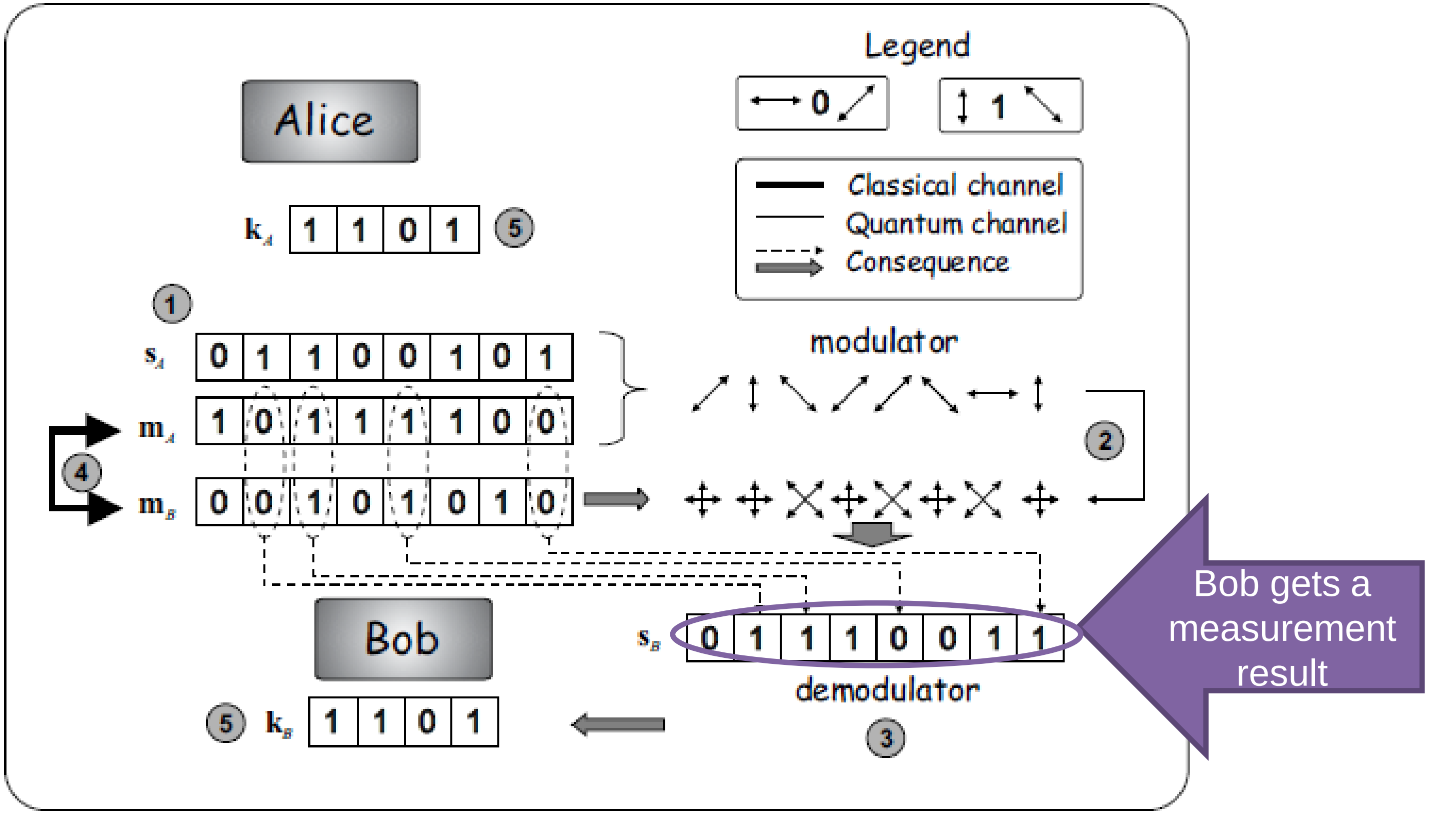
BB84

- First generation solution
  - Qubit is encoded in polarization
  - Challenge: producing and measuring single photons



BB84

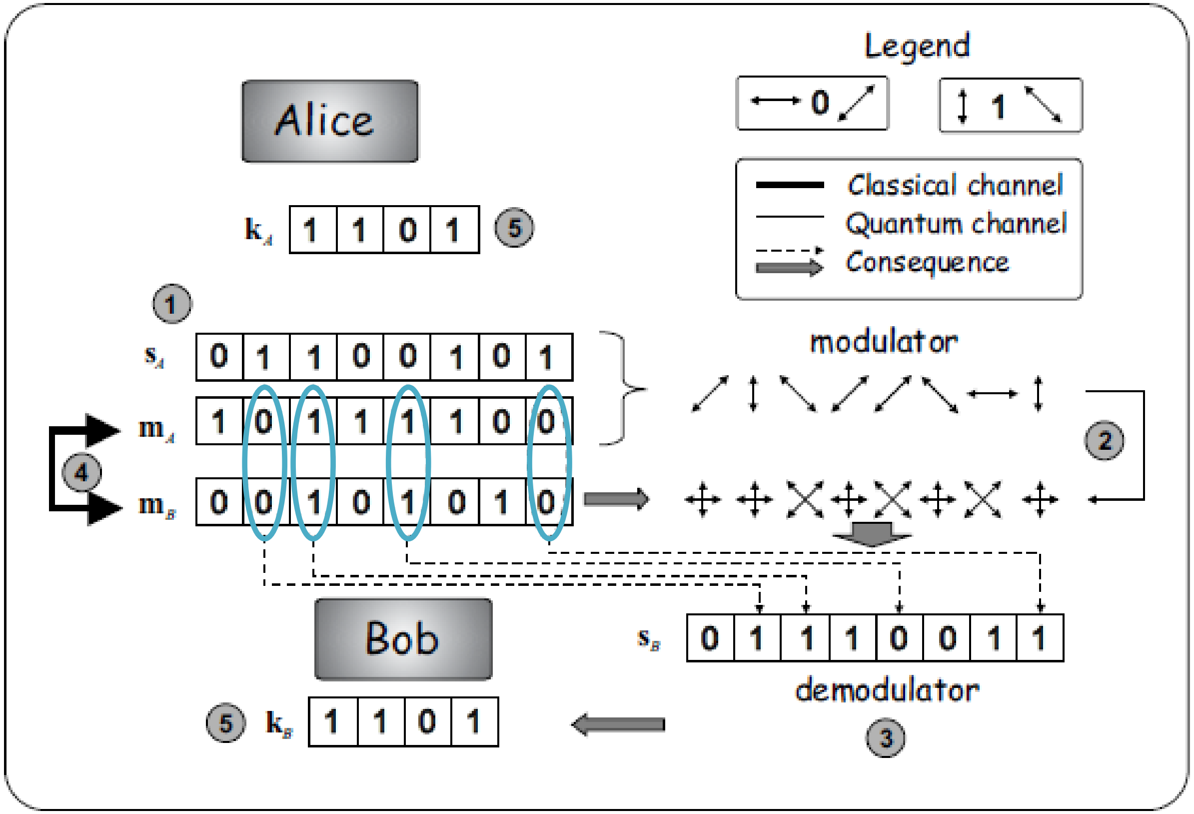
- First generation solution
  - Qubit is encoded in polarization
  - Challenge: producing and measuring single photons



BB84

- First generation solution
  - Qubit is encoded in polarization
  - Challenge: producing and measuring single photons

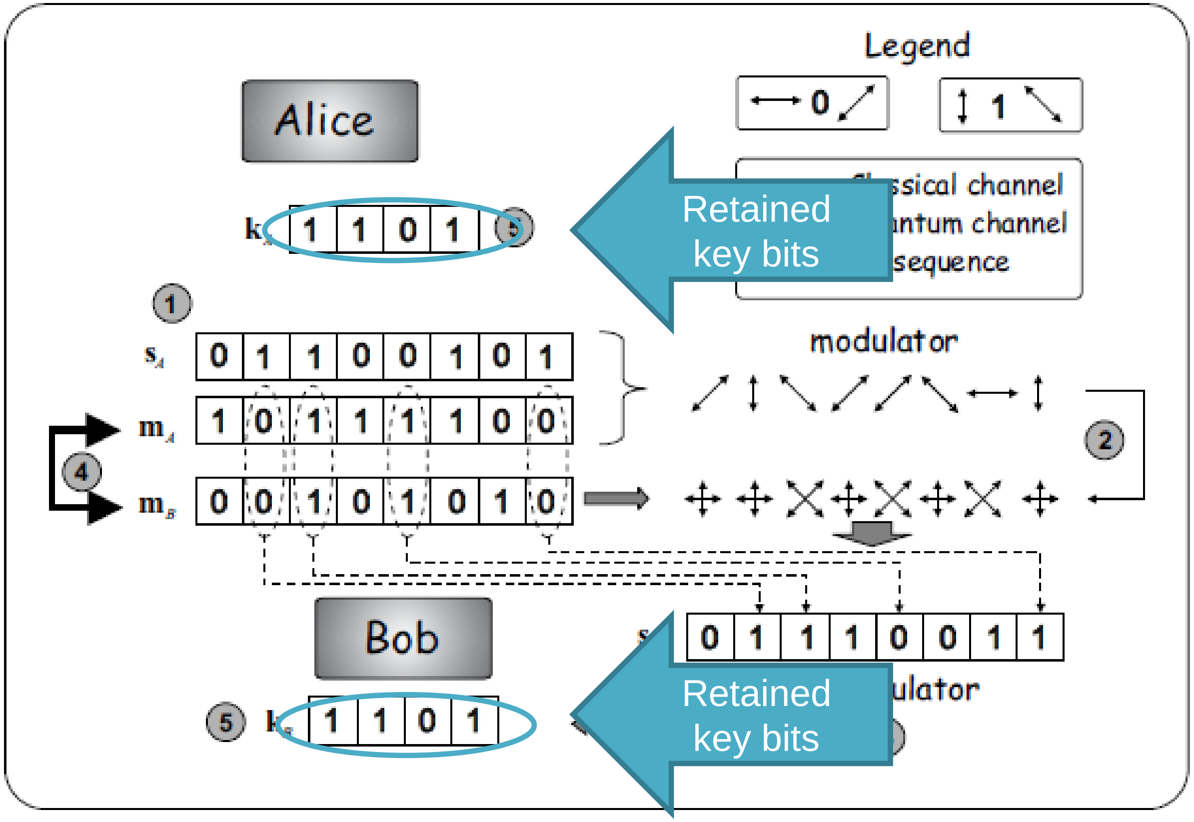
Where the bases are the same, the transmitted and measured bit values are the same



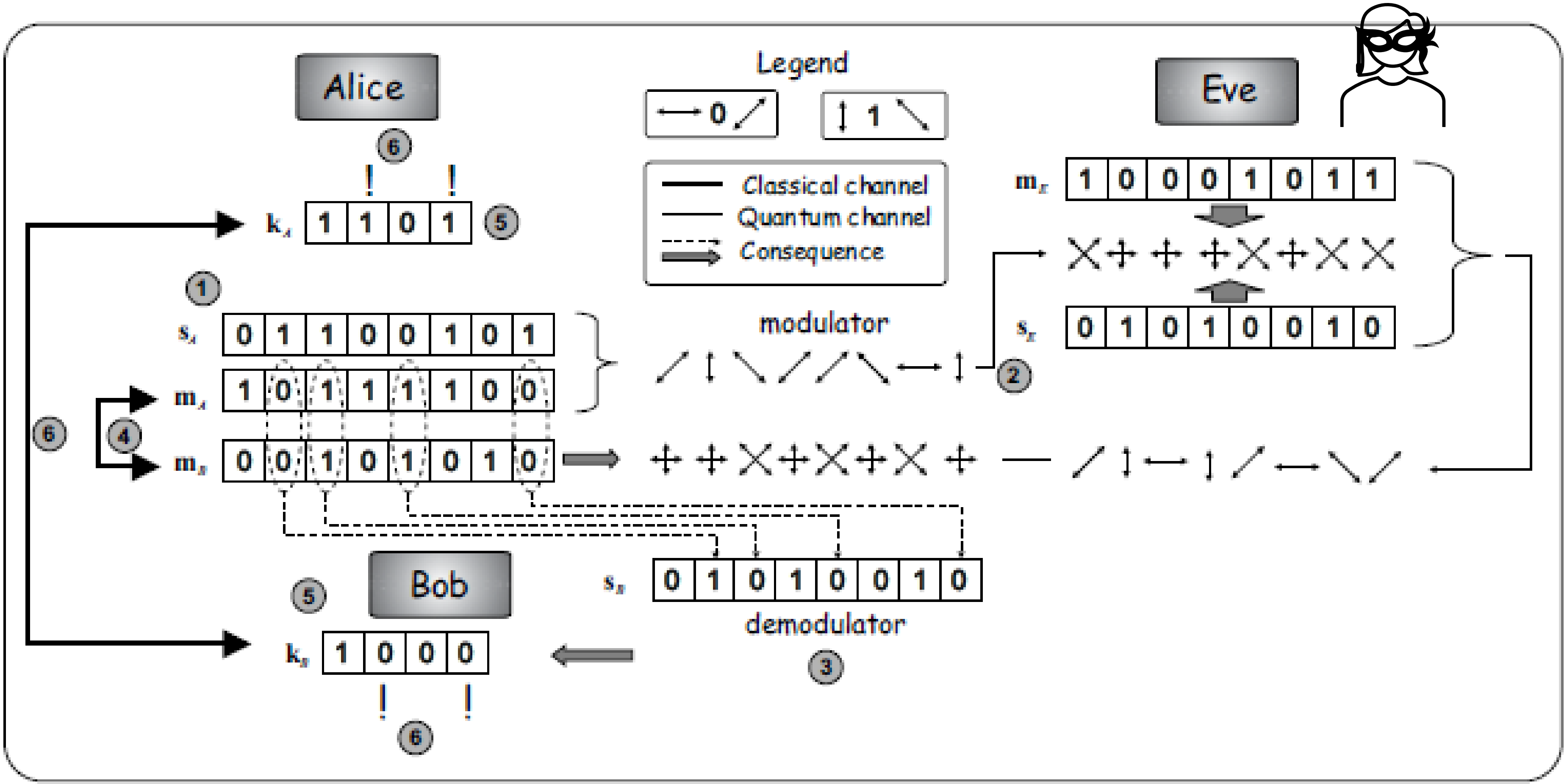
BB84

- First generation solution
  - Qubit is encoded in polarization
  - Challenge: producing and measuring single photons

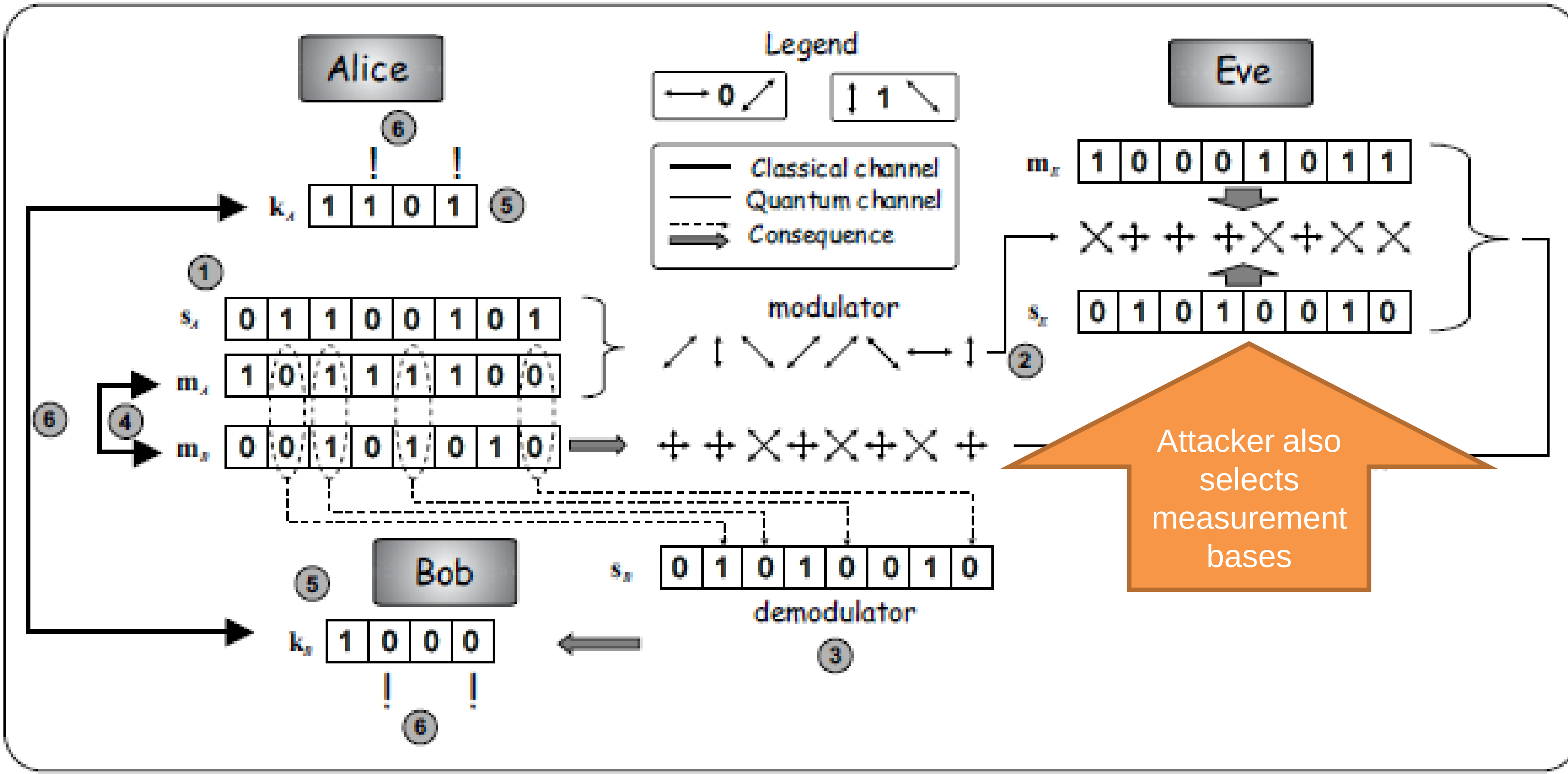
Alice and Bob reconcile the bases on a public channel. (But not the sent/measured bit value.) If the same basis is used, they keep the bit value.



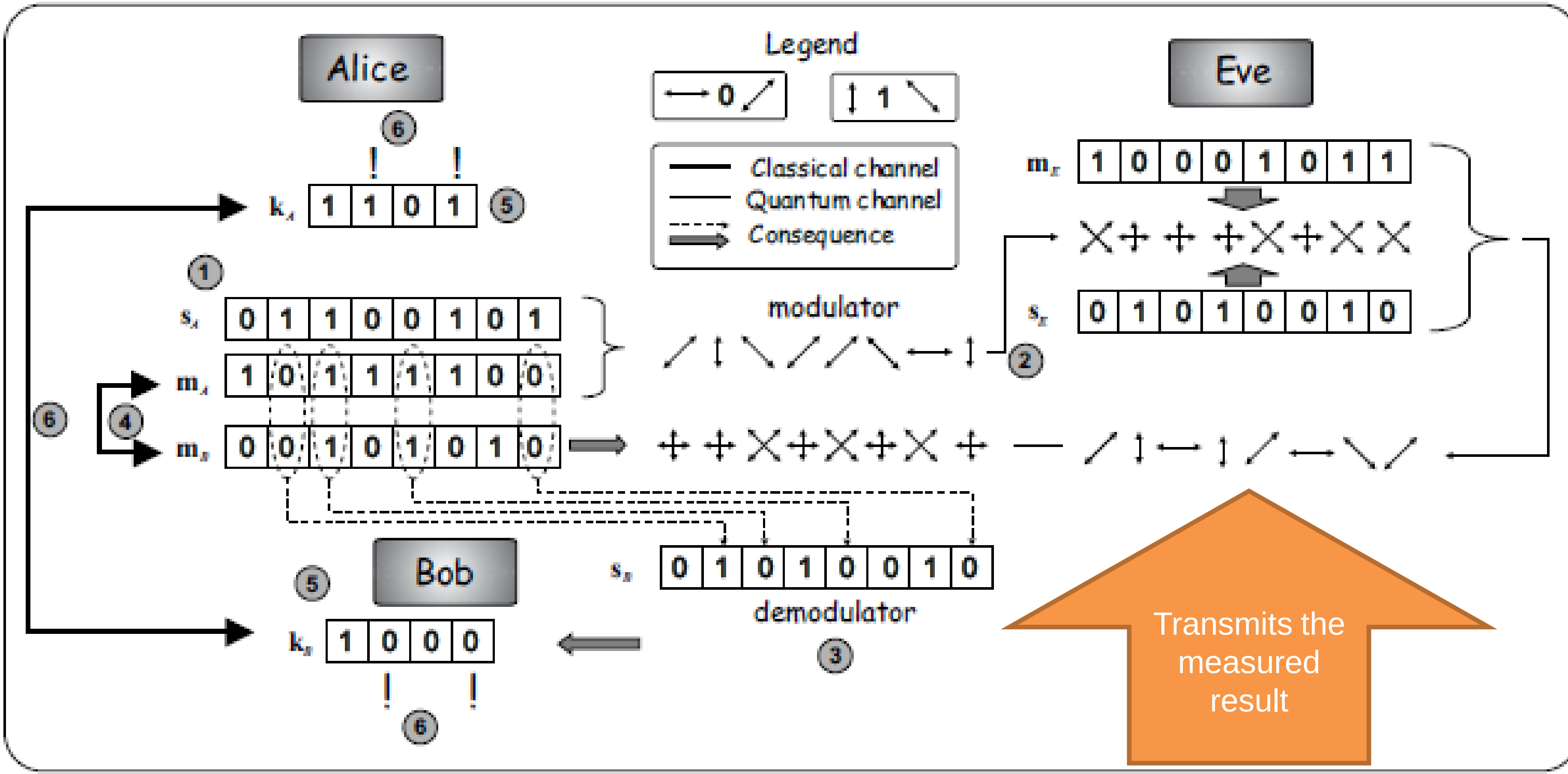
EAVESDROPPING ATTEMPT



EAVESDROPPING ATTEMPT

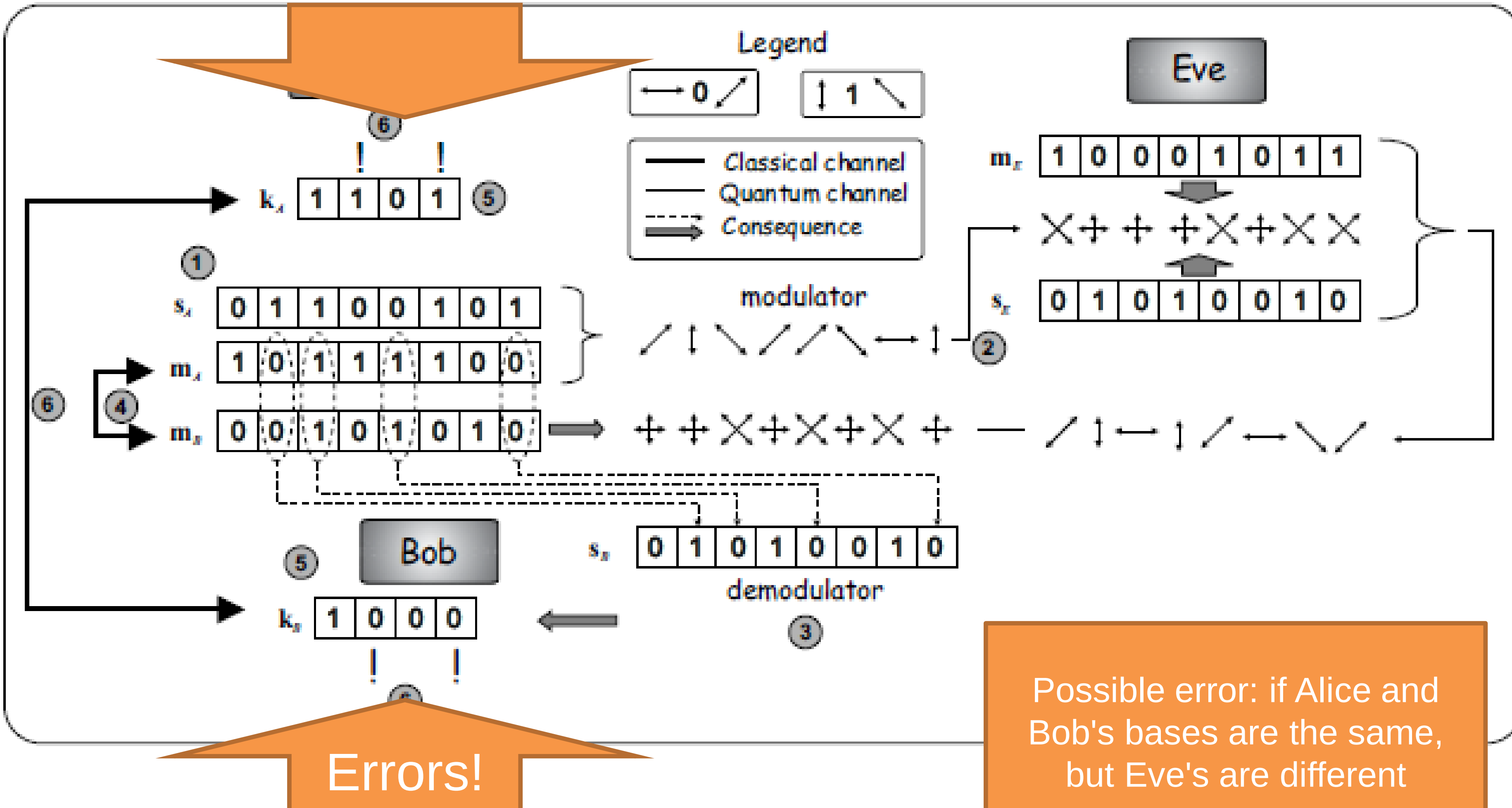


EAVESDROPPING ATTEMPT



DEPARTMENT OF
NETWORKED SYSTEMS
AND SERVICES
www.hit.bme.hu

EAVESDROPPING ATTEMPT

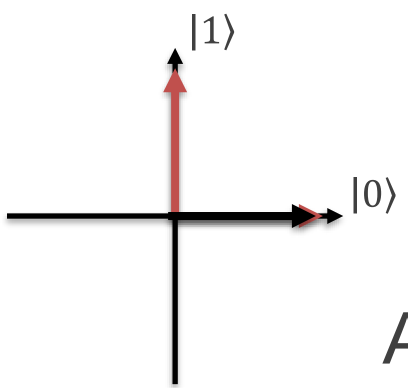


Possible error: if Alice and Bob's bases are the same, but Eve's are different

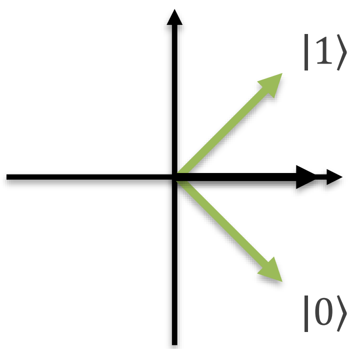
B92 protokoll

B92

- Basic idea:
  - If Bob gets a different measurement result than the one Alice sends (0 instead of 1), then they know that Bob measured in the wrong basis
  - Alice and Bob discuss the bit value in public and keep the basis secret
  - **The basis itself can serve as a key**

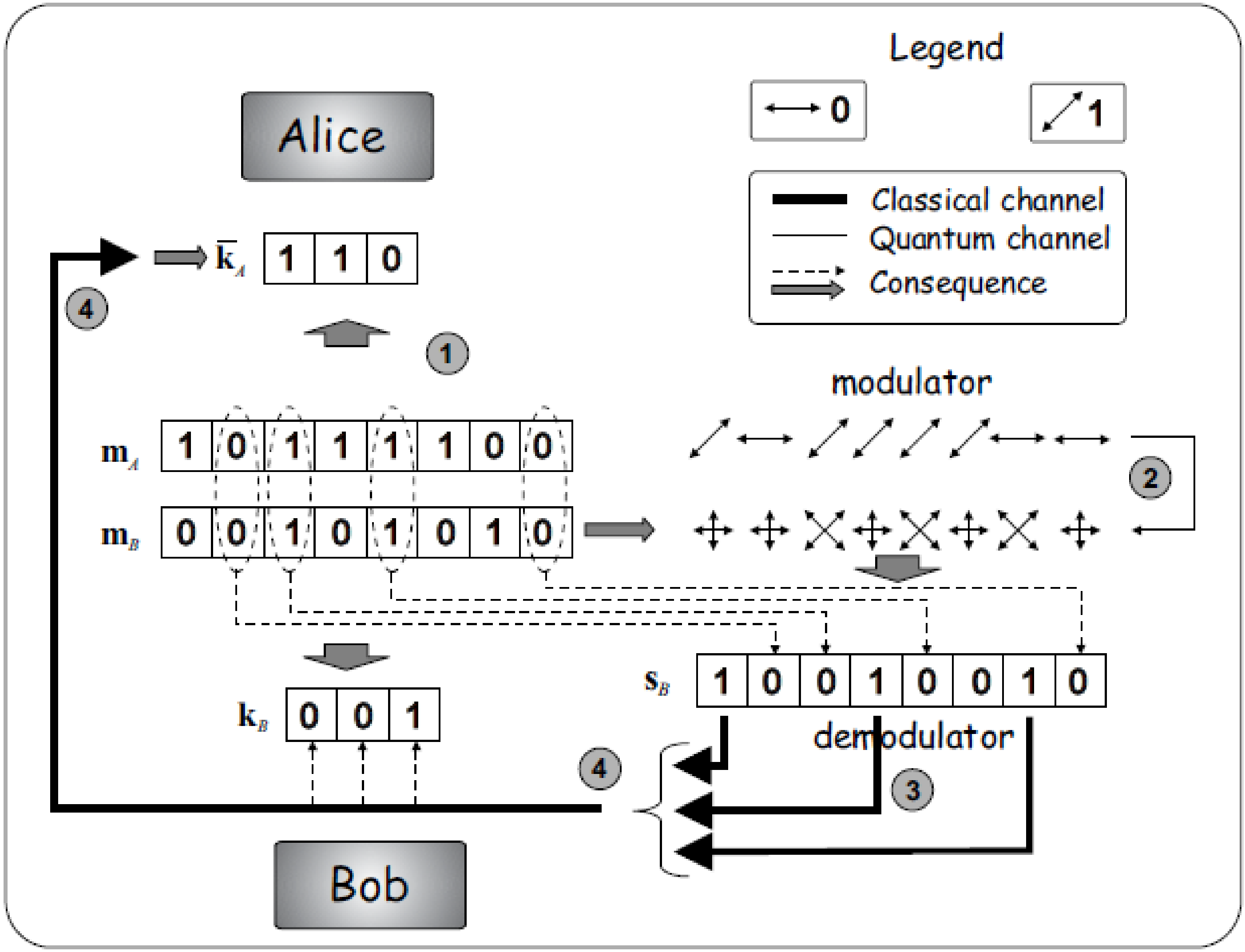


Alice

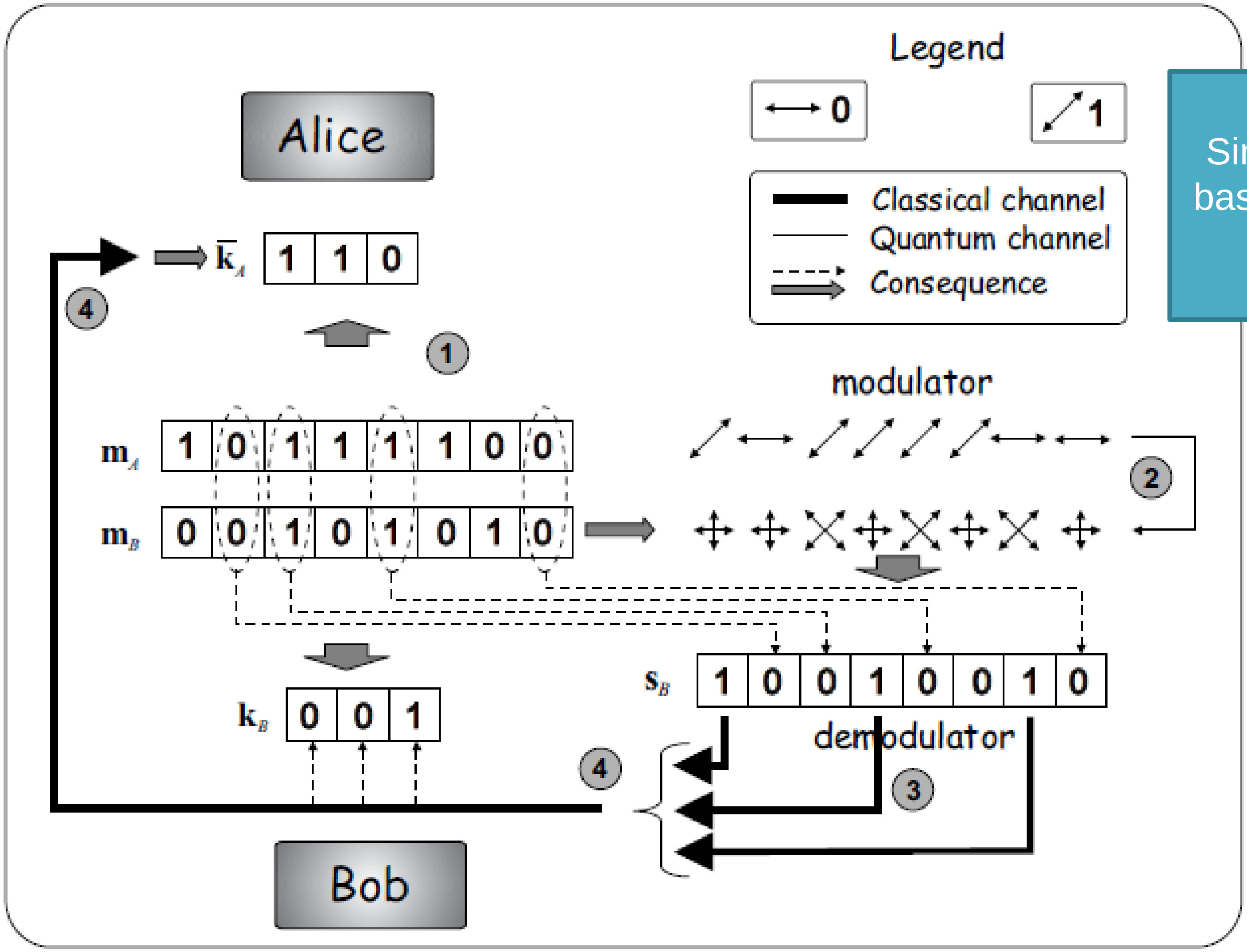


Bob

B92

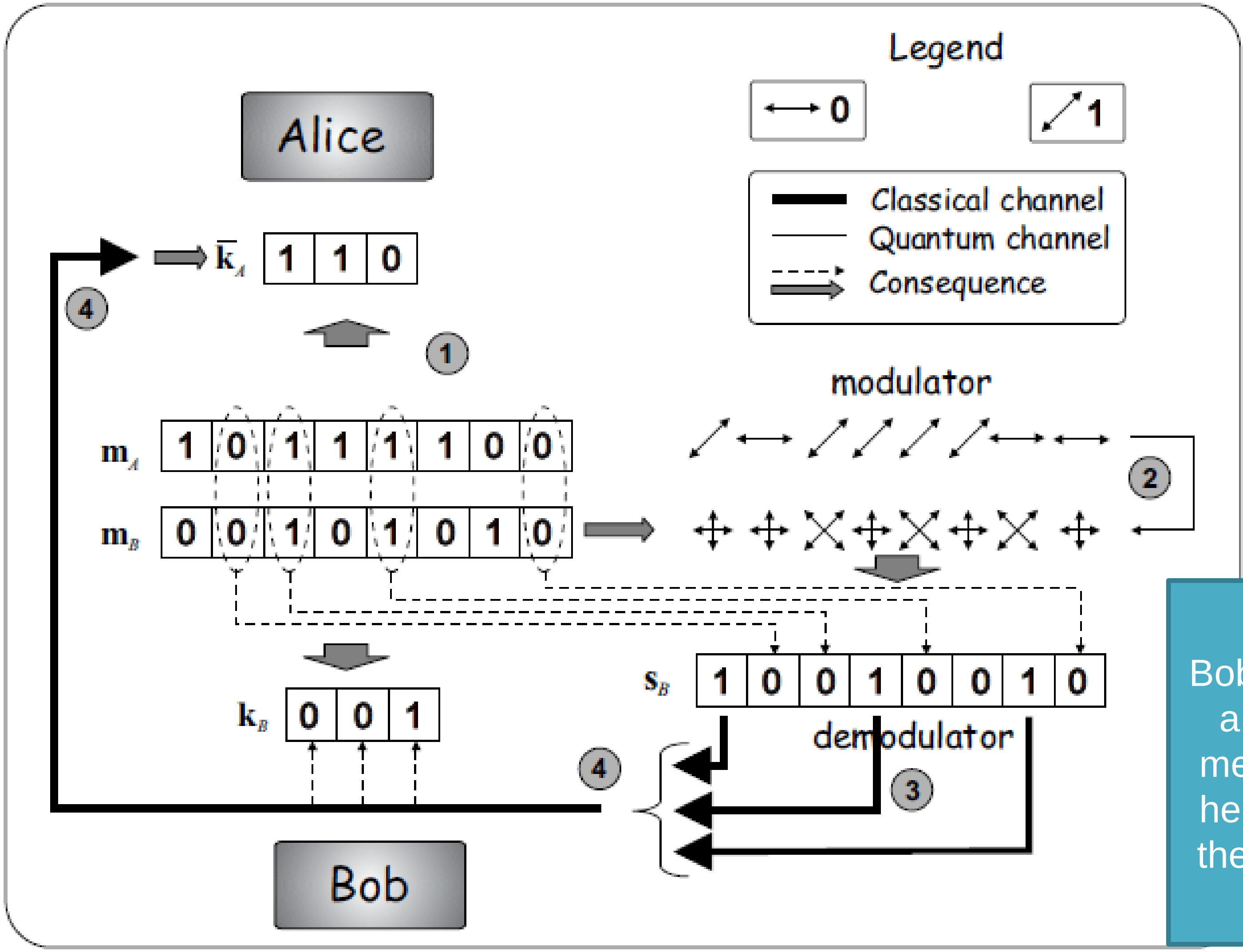

Legend
0
1
Classical channel
Quantum channel
Consequence
Alice
$\bar{k}_A$ 1 1 0
1
4
modulator
2
m_A 1 0 1 1 1 1 0 0
m_B 0 0 1 0 1 0 1 0
s_B 1 0 0 1 0 0 1 0
demodulator
3
4
k_B 0 0 1
Bob

B92



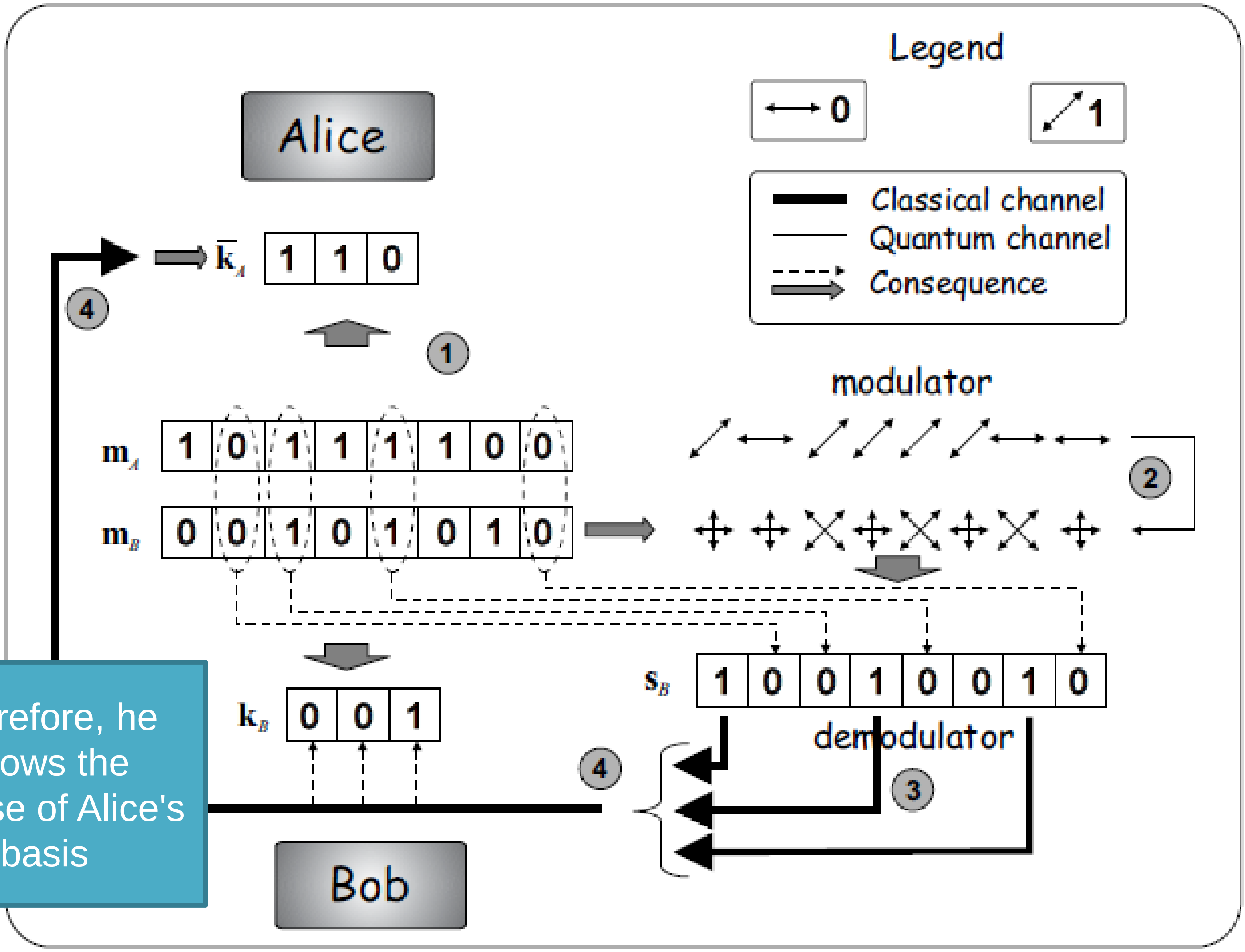
Similar, but the basis carries the bit value

B92



Bob can only get a 1 out of the measurement if he measured in the wrong basis

B92



Therefore, he knows the inverse of Alice's basis

Reality is not ideal

NON-IDEAL QUANTUM CHANNEL

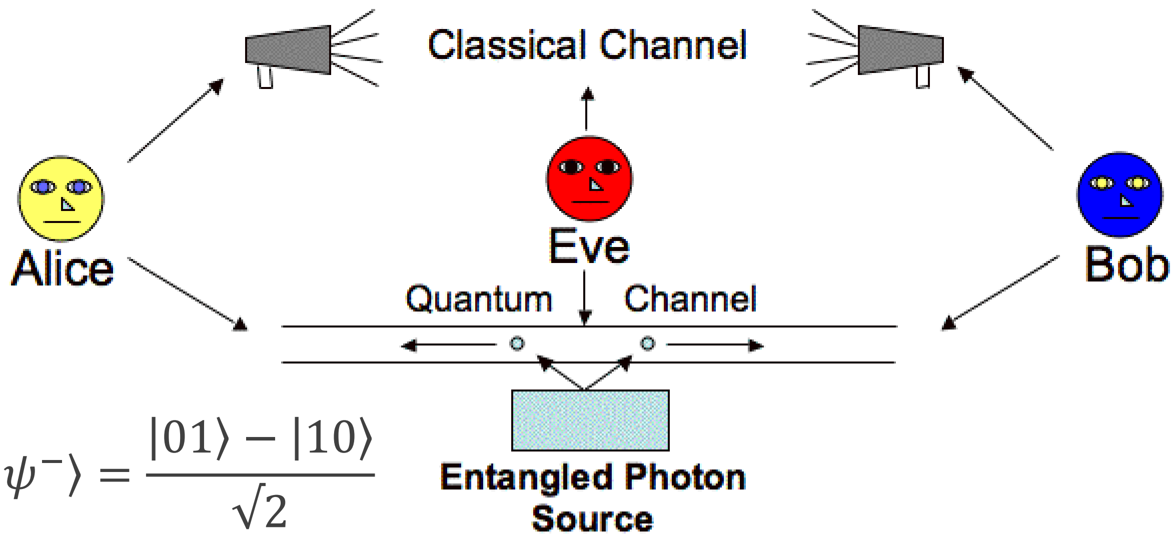
- Eavesdropping increases the BER (bit error rate)
  - In the quantum case: QBER (quantum bit error rate)
- In practice, the quantum channel is noisy, If the QBER is not zero even without eavesdropping
- How do we distinguish an attacker from noise?
  - Eve's appearance increases the noise floor of the channel
- As long as there are only a few errors
  - Privacy amplification
  - Smaller but more secure key
  - Requires that the capacity of the channel between Alice and Bob is larger than the channel between Alice and Eve

$$C(N) = \max_{p(x)} I(A:B) \qquad C_{AB}\text{-}C_{AE} > 0$$

Entanglement based QKD

TESTING ENTANGLEMENT

0°
45°



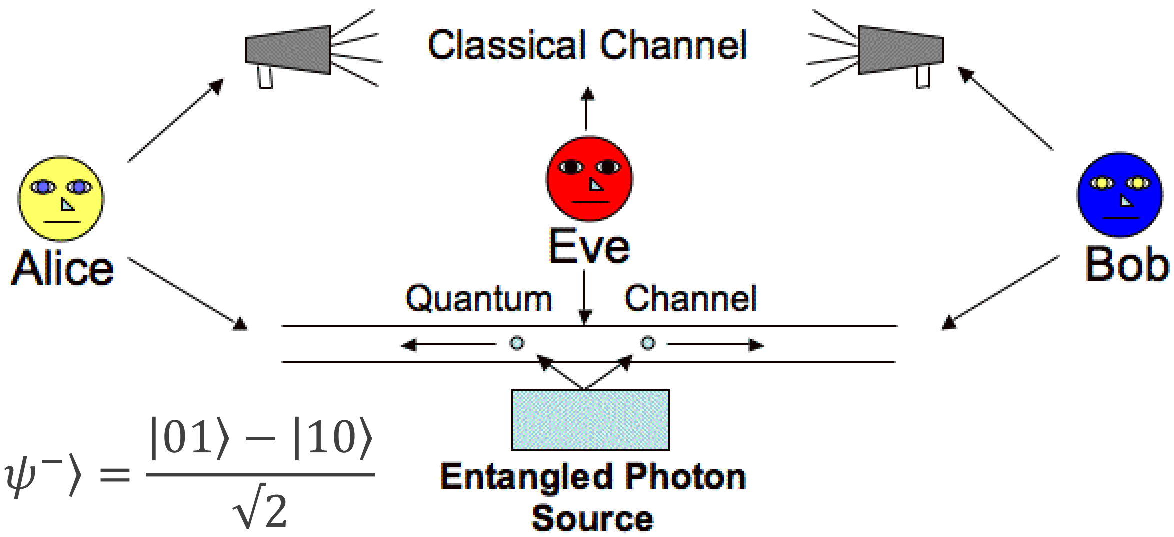
22,5°
67,5°

$$|\psi^-\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}}$$

- Bell-test experiment: is this really an entangled pair?
  - Alice and Bob randomly chooses their measurement bases from a set
  - Measurement results must be compared using statistical tests (using for example the CHSH inequality)
  - If the qubits were measured by an attacker or they are part of more entangled qubits, the Bell-test fails

E91 PROTOCOL

0°
22,5°
45°



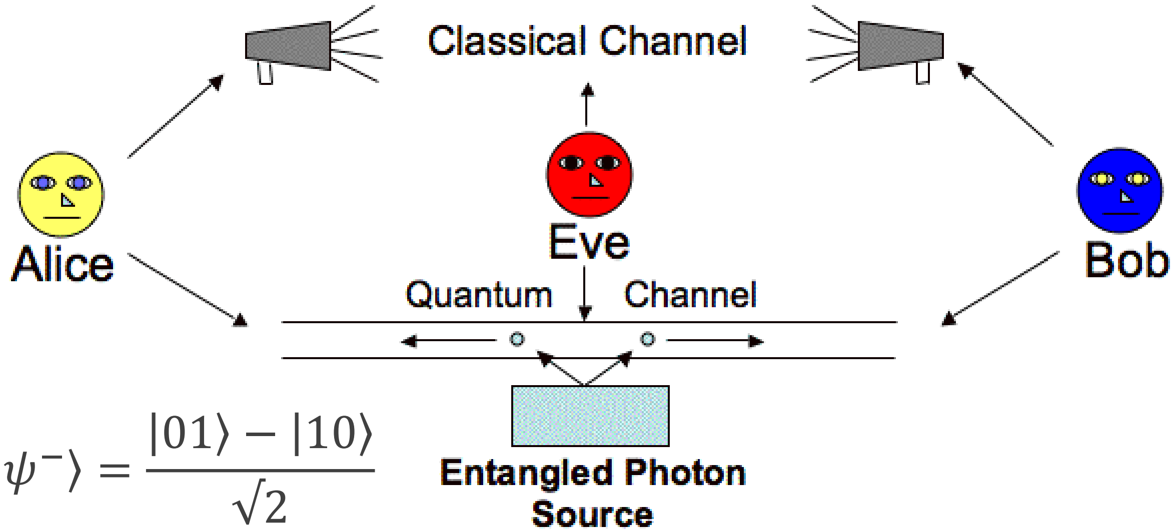
22,5°
45°
67,5°

$$|\psi^-\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}}$$

- E91 QKD
  - The set of bases Alice and Bob uses for a Bell-test is extended to allow for identical bases (where the mesurement results should correlate)
  - Alice and Bob randomly choose bases, then publicly discuss their choice (and measurement results if the basis correspondst to a Bell test)
  - If the Bell-test fails, the key is discarded

E91 PROTOCOL

0°
22,5°
45°



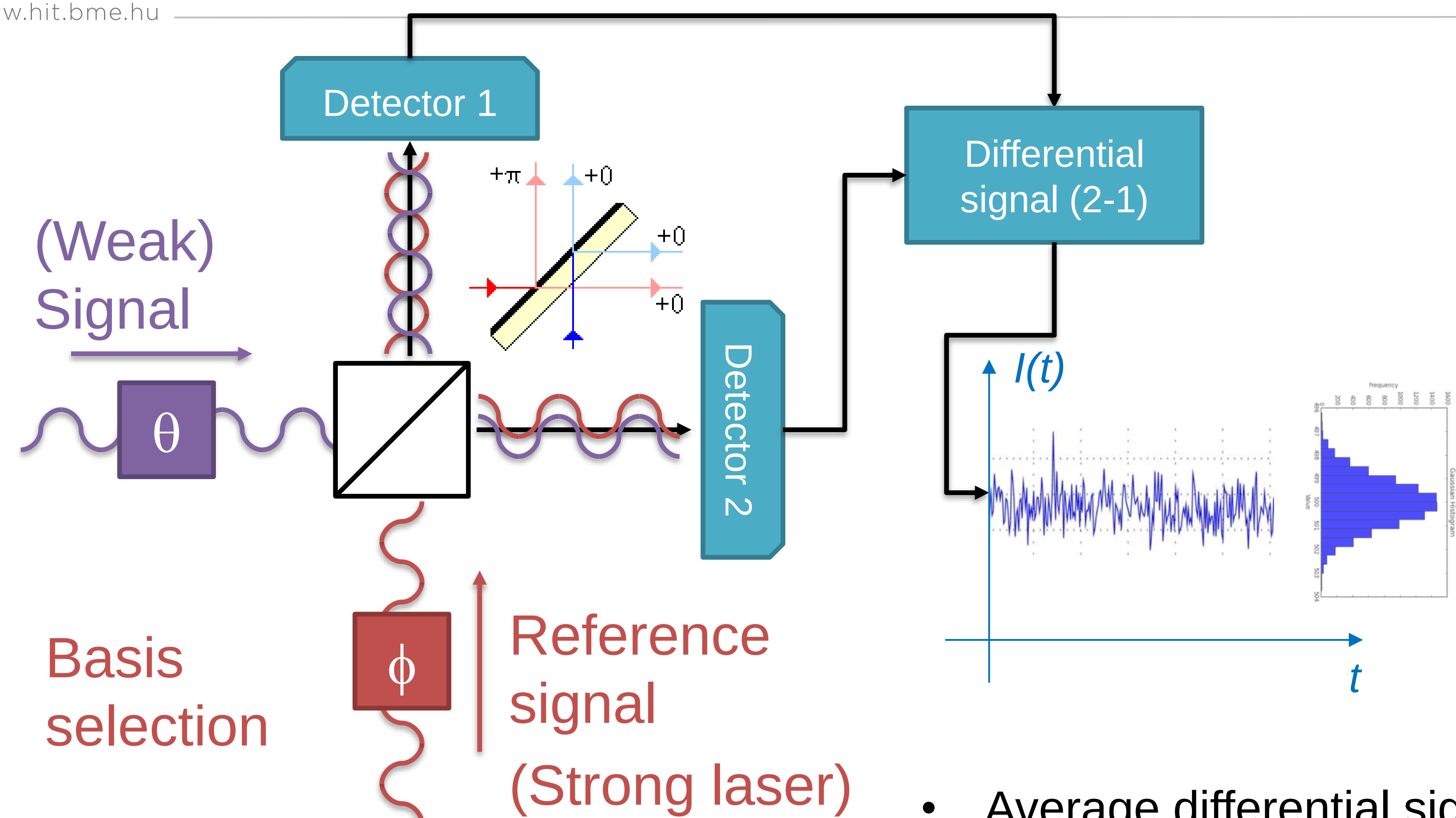
22,5°
45°
67,5°

$$|\psi^-\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}}$$

		Bob		
		22,5°	**45°**	**67,5°**
Alice	**0°**	Bell test	-	Bell test
	22,5°	Key	-	-
	45°	Bell test	Key	Bell test

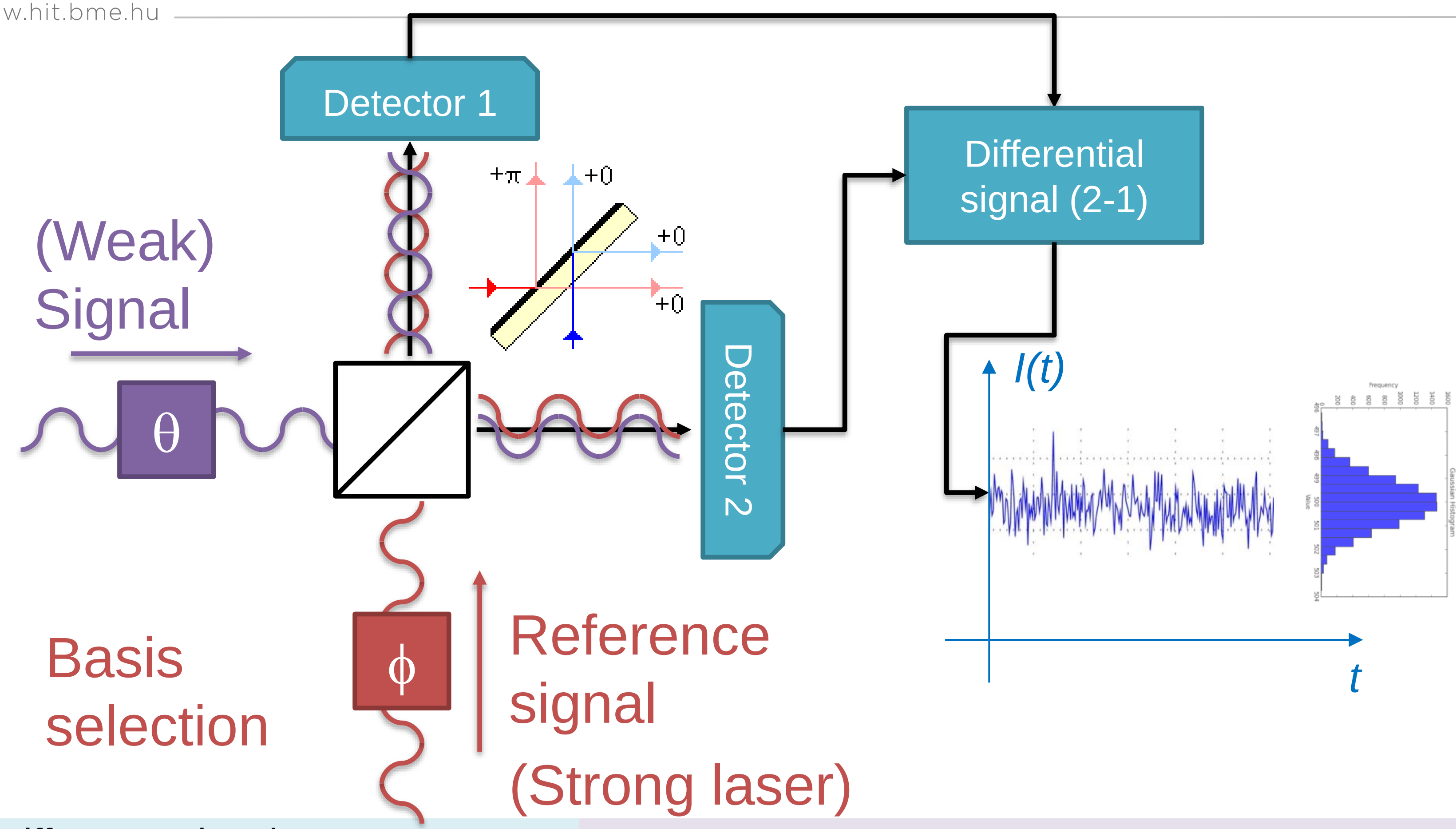
Quantum Key Distribution
2. Generation
Continuous Variable QKD

HOMODYNE DETECTION



- Average differential signal level = sine of phase difference
- Quantum noise

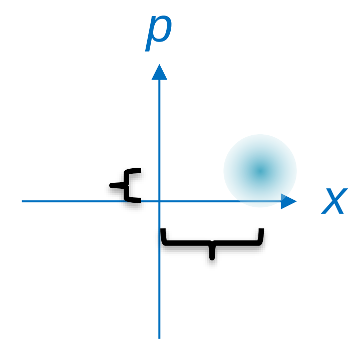
HOMODYNE DETECTION

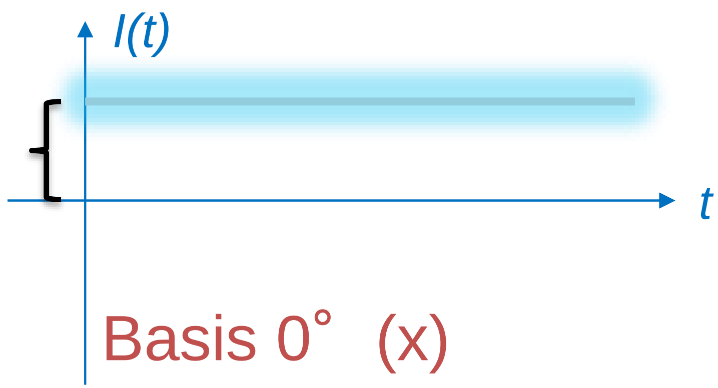


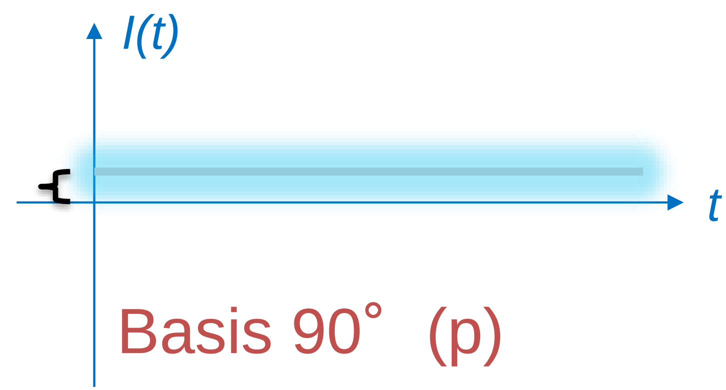
Difference signal		Phase of the measured signal			
		0°	**90°**	**180°**	**270°**
Basis phase	**0°**	+1	0	-1	0
(Local oscillator)	**90°**	0	+1	0	-1

HOMODYNE DETECTION

- For strong signals: copy the signal and measure in both bases
- But copying (dividing) a weak signal increases noise



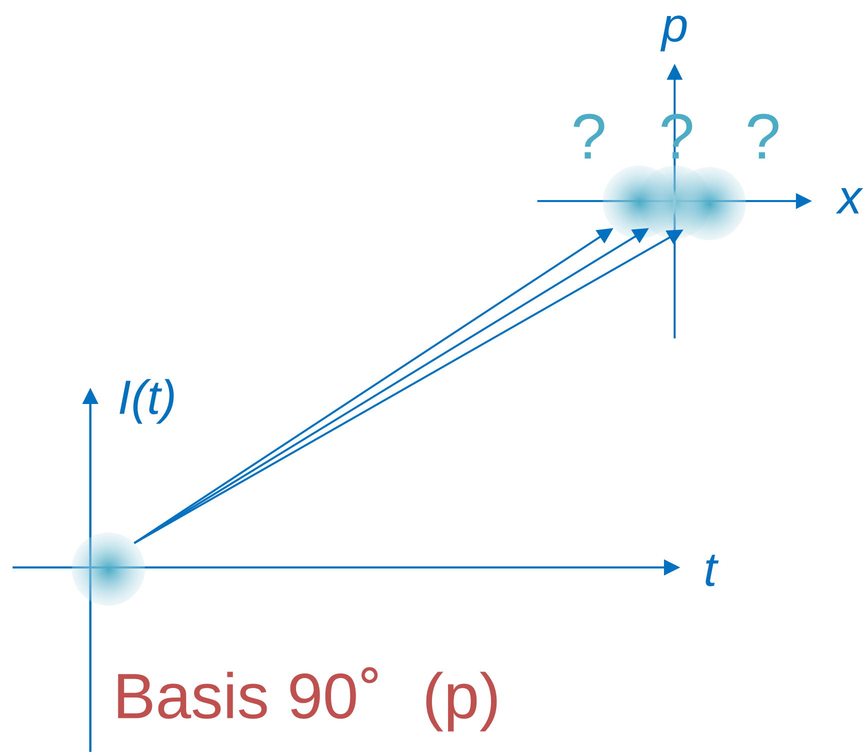




Difference signal		Phase of the measured signal			
		0°	**90°**	**180°**	**270°**
Basis phase	**0°**	+1	0	-1	0
(Local oscillator)	**90°**	0	+1	0	-1

HOMODYNE DETECTION

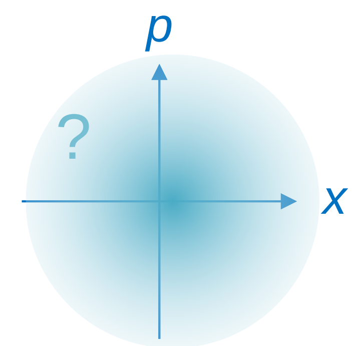
- If I pick one basis to minimize noise, and get a value close to zero, I do not know that the phase was in the other basis
- If I try to measure in both bases, I increase the noise and get less information

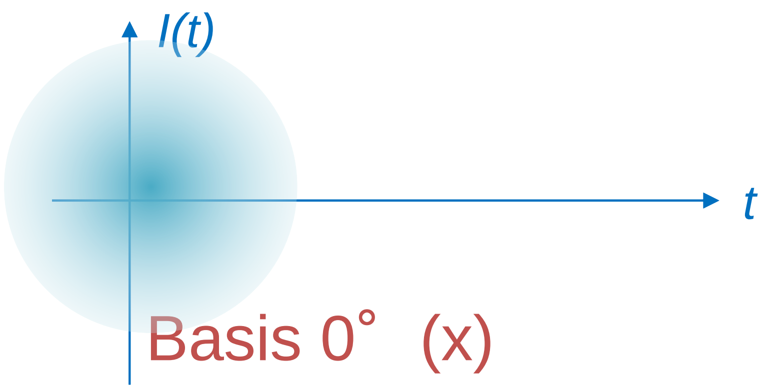


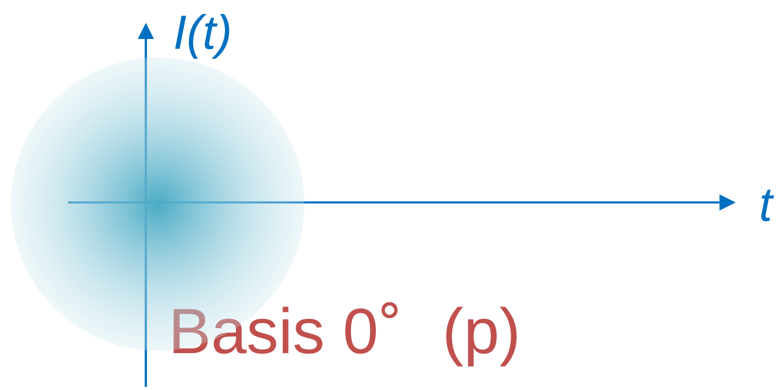
Difference signal		Phase of the measured signal			
		0°	**90°**	**180°**	**270°**
Basis phase	**0°**	+1	0	-1	0
(Local oscillator)	**90°**	0	+1	0	-1

HOMODYNE DETECTION

- If I try to measure in both bases, I increase the noise and get less information
- There is a high chance of error



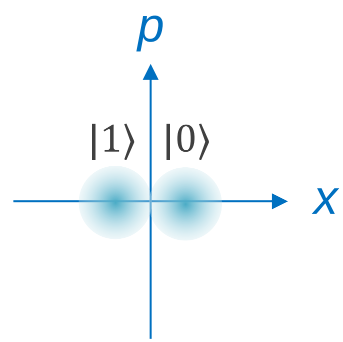


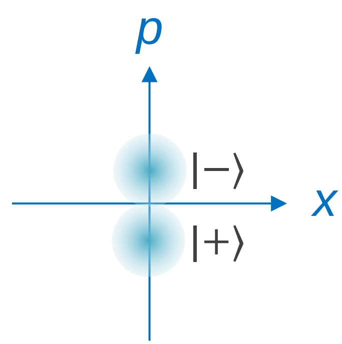


Difference signal		Phase of the measured signal			
		0°	**90°**	**180°**	**270°**
Basis phase	**0°**	+1	0	-1	0
(Local oscillator)	**90°**	0	+1	0	-1

HOMODYNE DETECTION

- QKD: weak signals
  - 10-100 photons/pulse
  - Close to origin comapred to noise
- Discretization of measured differential signal power
  - Simplest case: abowe or below 0
  - More complicated cases exist



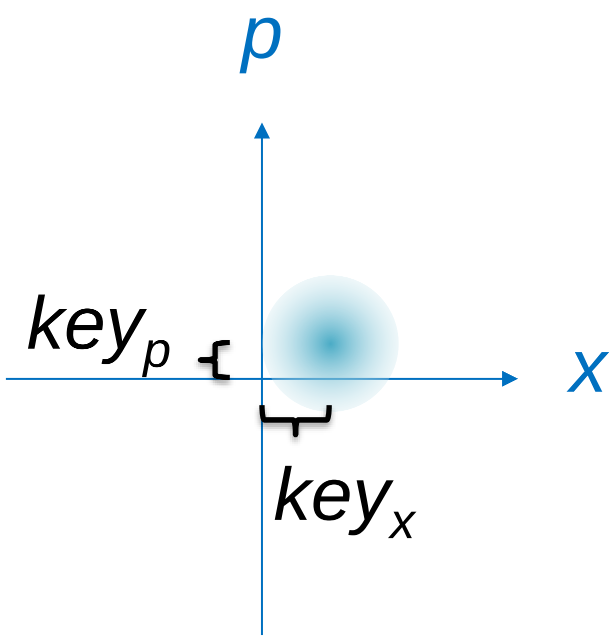


Difference signal		Phase of the measured signal			
		0°	**90°**	**180°**	**270°**
Basis phase	**0°**	+1	0	-1	0
(Local oscillator)	**90°**	0	+1	0	-1

Variants

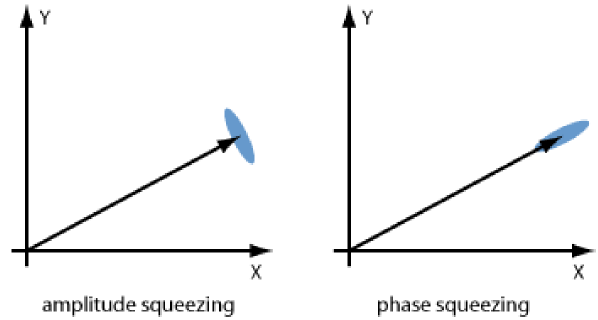
ENCODING AND ERROR DETECTION

- Alice can write in both bases
- Bob can measure in only one
  - But can inform Alice about his measurement choice, in which Alice knows what the result should be
- More than one key bit can be encoded in a single pulse
  - More complicated encoding, discretization and error correction



SQUEEZED LIGHT

- Squeezed light
  - Can be physically created (e.g. with nonlinear crystals)
- Low noise in one basis, but very high in the other
  - Fundamentally quantum behavior
  - Different forms of squeezing („directions” of high and low uncertainty) are possible
  - Follows an uncertainty principle



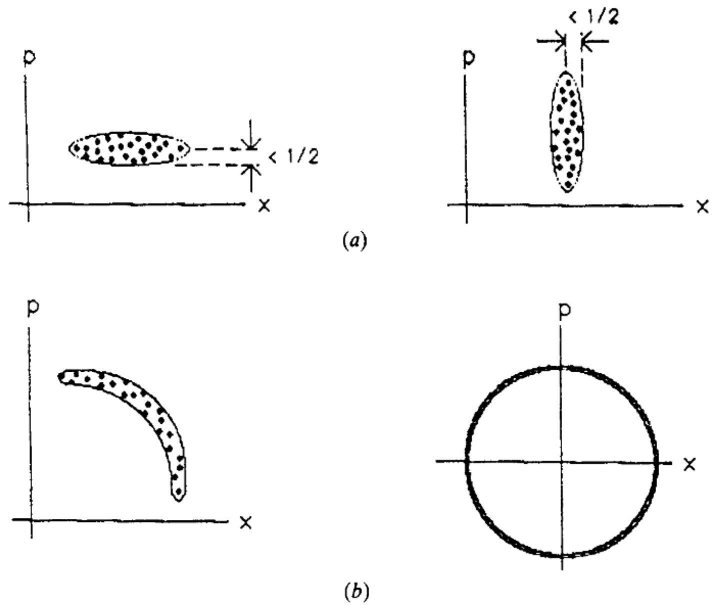
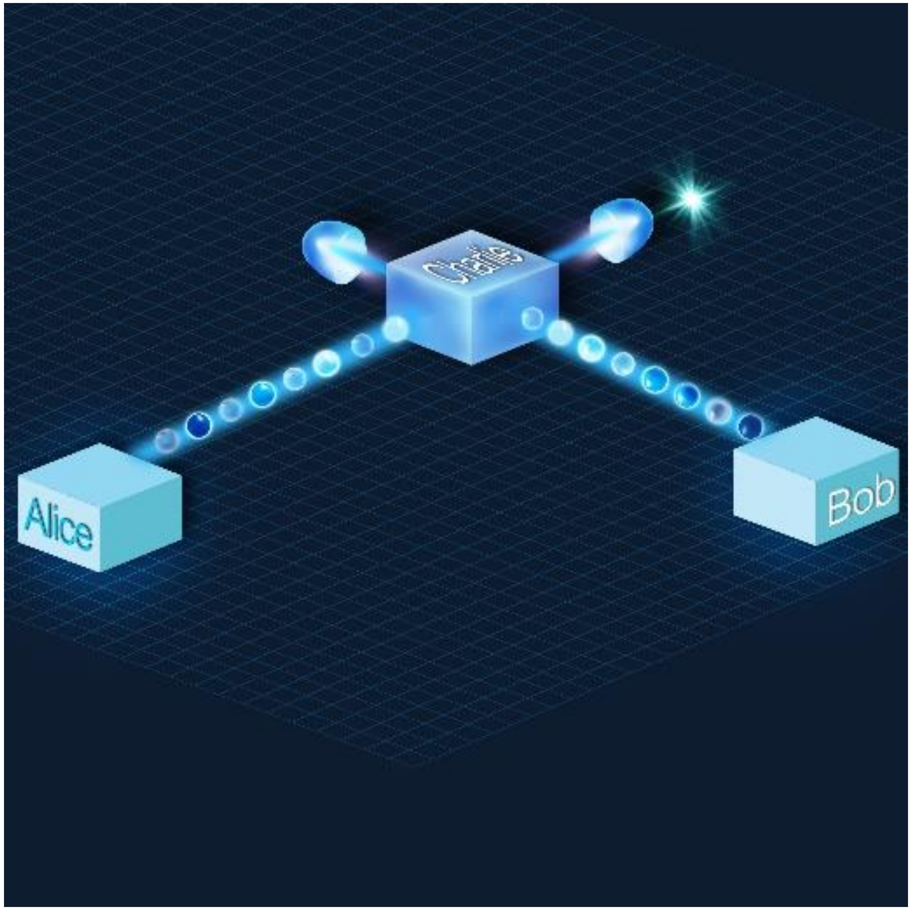


Figure 8. Definitions of squeezed-state light: (*a*) quadrature squeezed, (*b*) photon-number squeezed.

TWIN FIELD QKD

- Twin field detection
  - Reference signal (local oscillator) is also weak
  - There is a third party who perforsm the measurement, and publicly announces the result
- Measurement device independent
  - The third party (and their equipment) can be untrusted and controlled by Eve
- Doubles the distance
  - Current distance record holder protocol



DEPARTMENT OF
NETWORKED SYSTEMS
AND SERVICES

MŰEGYETEM 1782

ACKNOWLEDGEMENTS

The development of this course material has received funding from the European Union under grant agreement No 101081247 (QCIHungary project) and has been implemented with the support provided by the Ministry of Culture and Innovation of Hungary from the National Research, Development and Innovation Fund.

Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Commission. Neither the European Union nor the granting authority can be held responsible for them.

QCIHungary