Quantum communications

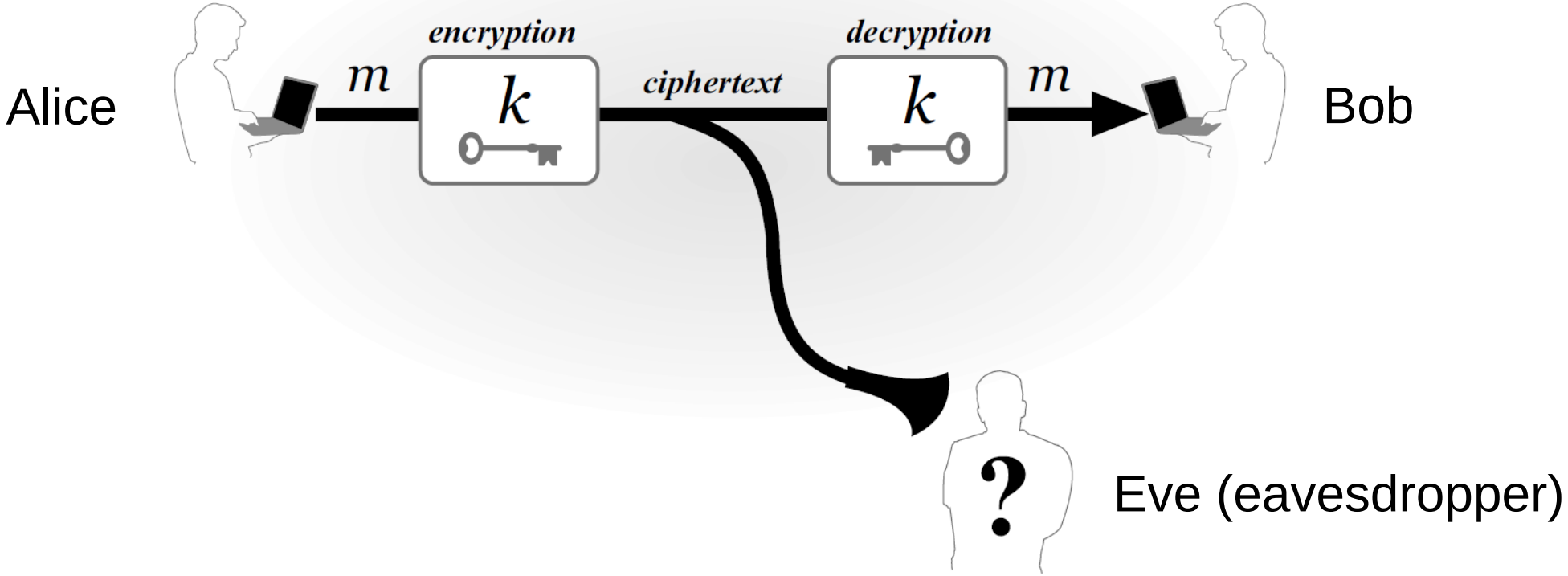
Lecture 6. Quantum key distribution

QUANTUM COMMUNICATIONS

Roman Shakhovoy

CLASSICAL CRYPTOGRAPHY: private-key encryption

Classical cryptography was concerned with designing and using codes (also called ciphers) that enable two parties to communicate secretly in the presence of an eavesdropper who can monitor all communication between them.



SYNTAX OF ENCRYPTION

Formally, a private-key encryption scheme is defined by specifying a message space ***M*** along with three algorithms: a procedure for generating keys (**Gen**), a procedure for encrypting (**Enc**), and a procedure for decrypting (**Dec**).

1. The key-generation algorithm **Gen** is a probabilistic algorithm that outputs a key ***k*** chosen according to some distribution.
2. The encryption algorithm **Enc** takes as input a key ***k*** and a message m and outputs a ciphertext ***c***. We denote by $\mathbf{Enc}_k(\boldsymbol{m})$ the encryption of the plaintext m using the key ***k***.
3. The decryption algorithm **Dec** takes as input a key ***k*** and a ciphertext ***c*** and outputs a plaintext ***m***. We denote the decryption of the ciphertext ***c*** using the key ***k*** by $\mathbf{Dec}_k(\mathbf{c})$.

$$\mathbf{Dec}_k(\mathbf{Enc}_k(\boldsymbol{m})) = \boldsymbol{m}$$

CLASSICAL CRYPTOGRAPHY: shift cipher (Caesar's cipher)

begin the attack now

⬇ k=3

EHJLQWKHDWWDFNQRZ

Encryption:

$$\mathsf{Enc}_k(m_1 \cdots m_\ell) = c_1 \cdots c_\ell, \quad \text{where } c_i = [(m_i + k) \bmod 26]$$

Decryption:

$$\mathsf{Dec}_k(c_1 \cdots c_\ell) = m_1 \cdots m_\ell, \quad \text{where } m_i = [(c_i - k) \bmod 26]$$

Any secure encryption scheme must have a key space that is sufficiently large to make an exhaustive-search attack infeasible

CLASSICAL CRYPTOGRAPHY: mono-alphabetic substitution cipher

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
X	E	U	A	D	N	B	K	V	M	R	O	C	Q	F	S	Y	H	W	G	L	Z	I	J	P	T

begin the attack now

EHJLQWKHDWWDFNQRZ

Key space: $26! \approx 2^{88}$

PRINCIPLES OF MODERN CRYPTOGRAPHY

1. Formal definitions. *If you don't understand what you want to achieve, how can you possibly know when (or if) you have achieved it*?
2. Precise Assumptions
3. Proofs of security

Kerckhoffs's principle

A cryptosystem should be secure, even if everything about the system, except the key, is public knowledge

PERFECT SECRECY: Shannon's theorem

THEOREM ***(Shannon's theorem)*** *Let* (Gen, Enc, Dec) *be an encryption scheme with message space* $\mathcal{M}$*, for which* $|\mathcal{M}| = |\mathcal{K}| = |\mathcal{C}|$*. The scheme is perfectly secret if and only if:*

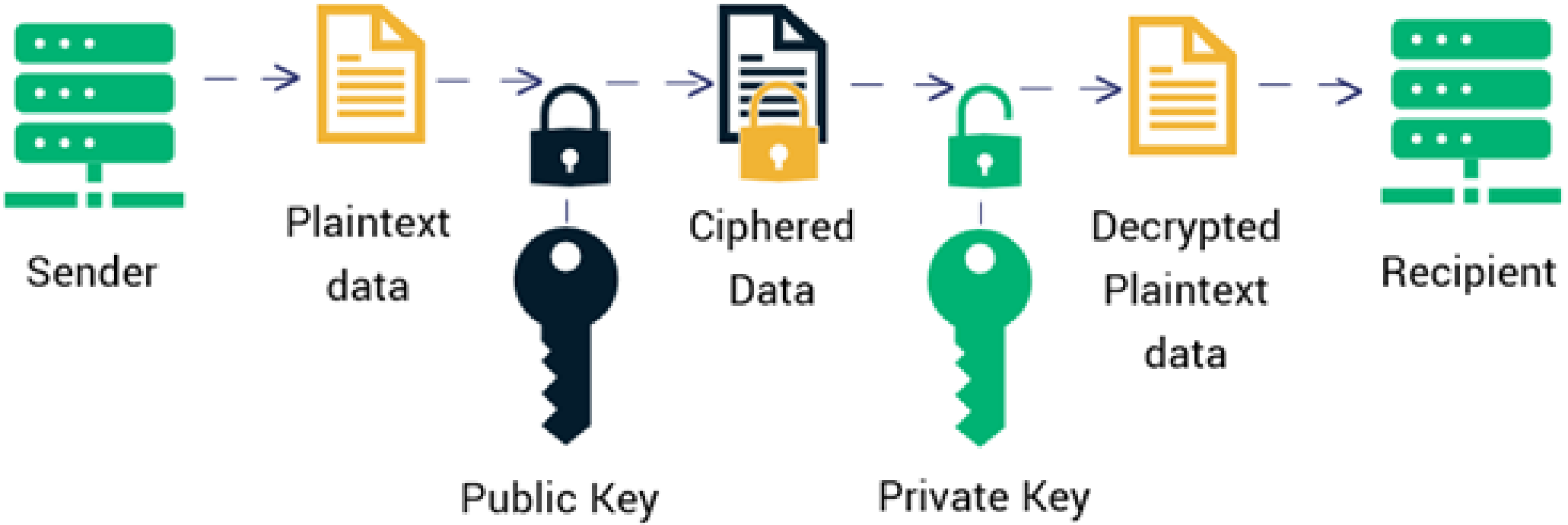
1. *Every key* $k \in \mathcal{K}$ *is chosen with (equal) probability* $1/|\mathcal{K}|$ *by algorithm* Gen.
2. *For every* $m \in \mathcal{M}$ *and every* $c \in \mathcal{C}$*, there exists a unique key* $k \in \mathcal{K}$ *such that* $\mathsf{Enc}_k(m)$ *outputs* c.

PROVABLY SECURE CRYPTOGRAPHY: ONE-TIME PAD

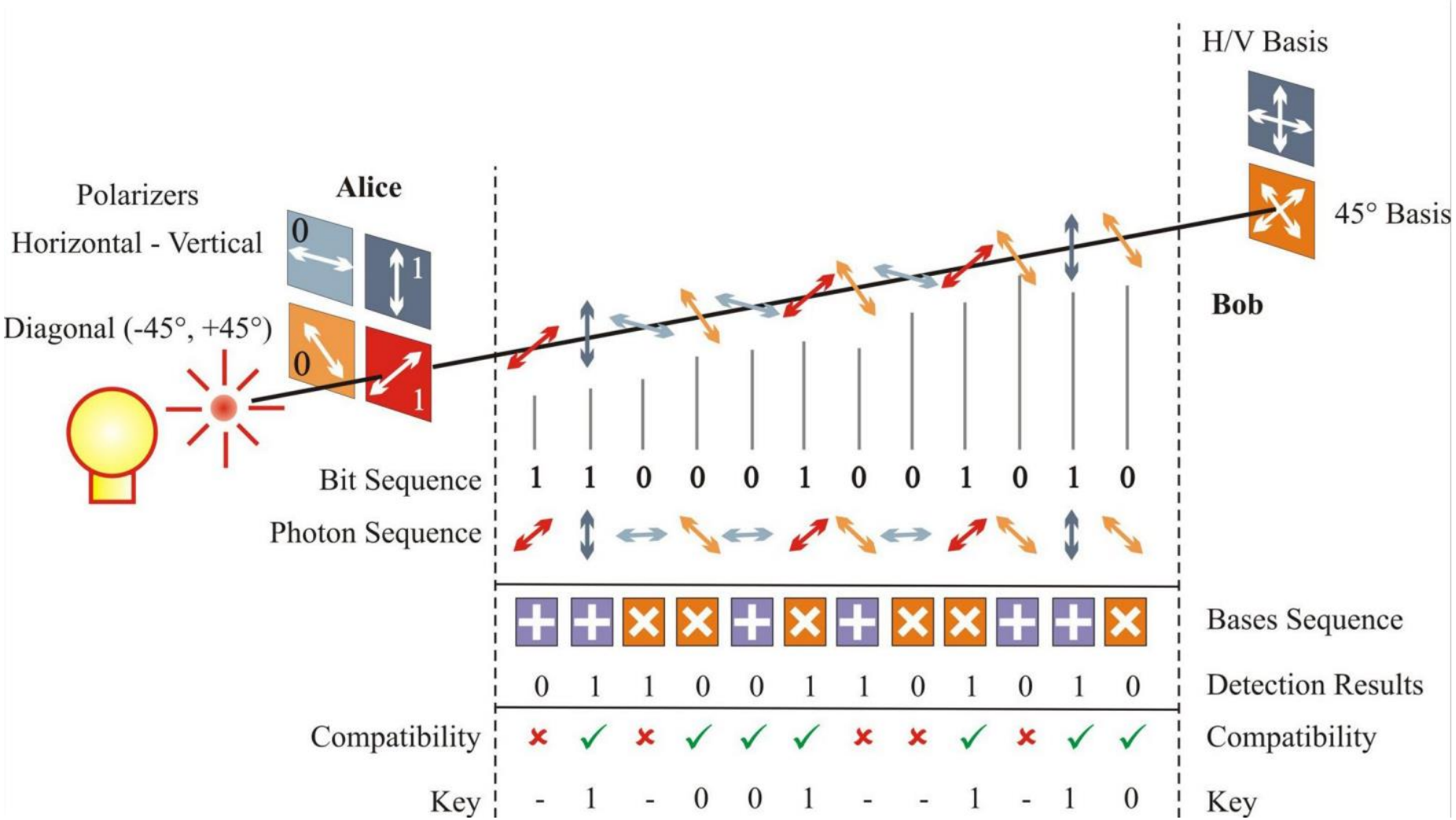
Fix an integer $\ell > 0$. The message space $\mathcal{M}$, key space $\mathcal{K}$, and ciphertext space $\mathcal{C}$ are all equal to $\{0,1\}^\ell$ (the set of all binary strings of length ℓ).

- Gen: the key-generation algorithm chooses a key from $\mathcal{K} = \{0,1\}^\ell$ according to the uniform distribution (i.e., each of the 2^ℓ strings in the space is chosen as the key with probability exactly $2^{-\ell}$).
- Enc: given a key $k \in \{0,1\}^\ell$ and a message $m \in \{0,1\}^\ell$, the encryption algorithm outputs the ciphertext $c := k \oplus m$.
- Dec: given a key $k \in \{0,1\}^\ell$ and a ciphertext $c \in \{0,1\}^\ell$, the decryption algorithm outputs the message $m := k \oplus c$.

ASYMMETRIC ENCRYPTION



QUANTUM CRYPTOGRAPHY: BB84 protocol



NO-CLONING THEOREM

Because of linearity of the Hilbert space, the cloning of an arbitrary quantum state is impossible.

$$|a\rangle \otimes |0\rangle \not\Rightarrow |a\rangle \otimes |a\rangle$$

Let us assume that cloning is possible:

$$|a\rangle \otimes |0\rangle \Longrightarrow |a\rangle \otimes |a\rangle \qquad |b\rangle \otimes |0\rangle \Longrightarrow |b\rangle \otimes |b\rangle$$

$$\left(\frac{1}{\sqrt{2}}(|a\rangle + |b\rangle)\right) \otimes |0\rangle \Longrightarrow \qquad \left(\frac{1}{\sqrt{2}}(|a\rangle + |b\rangle)\right) \otimes |0\rangle \Longrightarrow$$

$$\left(\frac{1}{\sqrt{2}}(|a\rangle \otimes |0\rangle + |b\rangle \otimes |0\rangle)\right) = \qquad \left(\frac{1}{\sqrt{2}}(|a\rangle + |b\rangle)\right) \otimes \left(\frac{1}{\sqrt{2}}(|a\rangle + |b\rangle)\right) =$$

$$\frac{1}{\sqrt{2}}(|a\rangle \otimes |a\rangle + |b\rangle \otimes |b\rangle) \neq \frac{1}{2}(|a\rangle \otimes |a\rangle + |a\rangle \otimes |b\rangle + |b\rangle \otimes |a\rangle + |b\rangle \otimes |b\rangle)$$

QUANTUM CRYPTOGRAPHY: BB84 protocol

Exercise 1

Suppose Eve intercepts Alice's photons and measures them in either the canonical or diagonal basis (she chooses at random). She then encodes the bit she measured in the same basis and re-sends it to Bob. What error rate will Alice and Bob register, i.e., what fraction of bits in the secret key they created will come out differently on average?

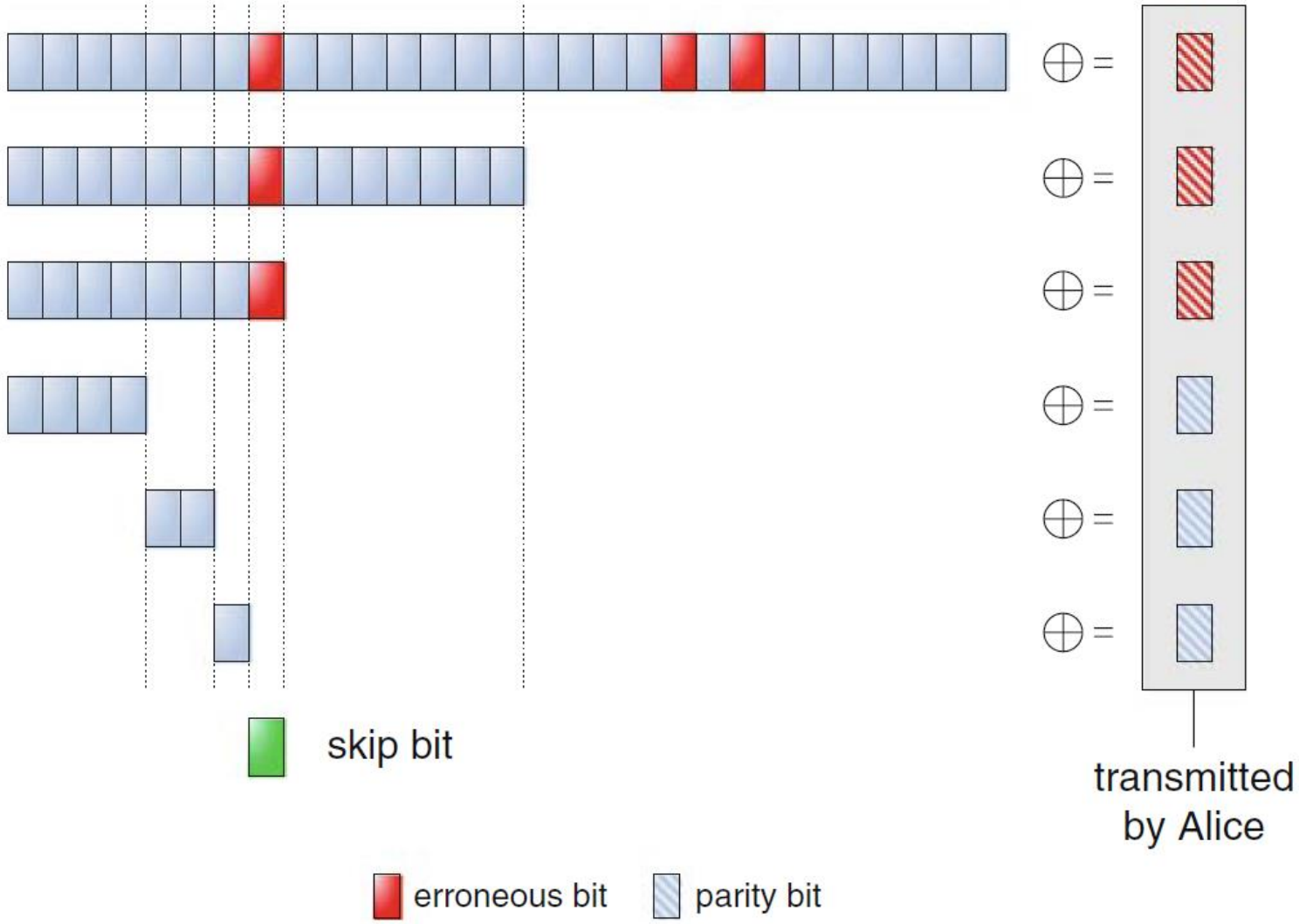
POSTPROCESSING: error estimation

Usually, in BB84, the error rate, which is called quantum bit error rate (QBER), is estimated by picking a small random subset of bits with length *r* from those given in the sifted key. This test string is publicly compared by Alice and Bob and yields in a certain number of errors *e*.

$$\mathrm{QBER} = \frac{r}{e}$$

QBER should not exceed $\approx 11\%$, because the best error correction code approaches a maximal tolerated error rate of 12,9%.

POSTPROCESSING: error correction



POSTPROCESSING: privacy amplification

Privacy amplification is the art of distilling highly secret shared information from a larger body of shared information that is only partially secret.

$$\{0,1\}^n \rightarrow \{0,1\}^m$$

“Leftover hash lemma”

$$m = n - t - 2\log(1/\varepsilon)$$

n – length of the raw key (in bits);
t – information (in bits) available to Eve about raw key;
ε – security parameter.

POSTPROCESSING: privacy amplification via hashing

2-universal hash functions

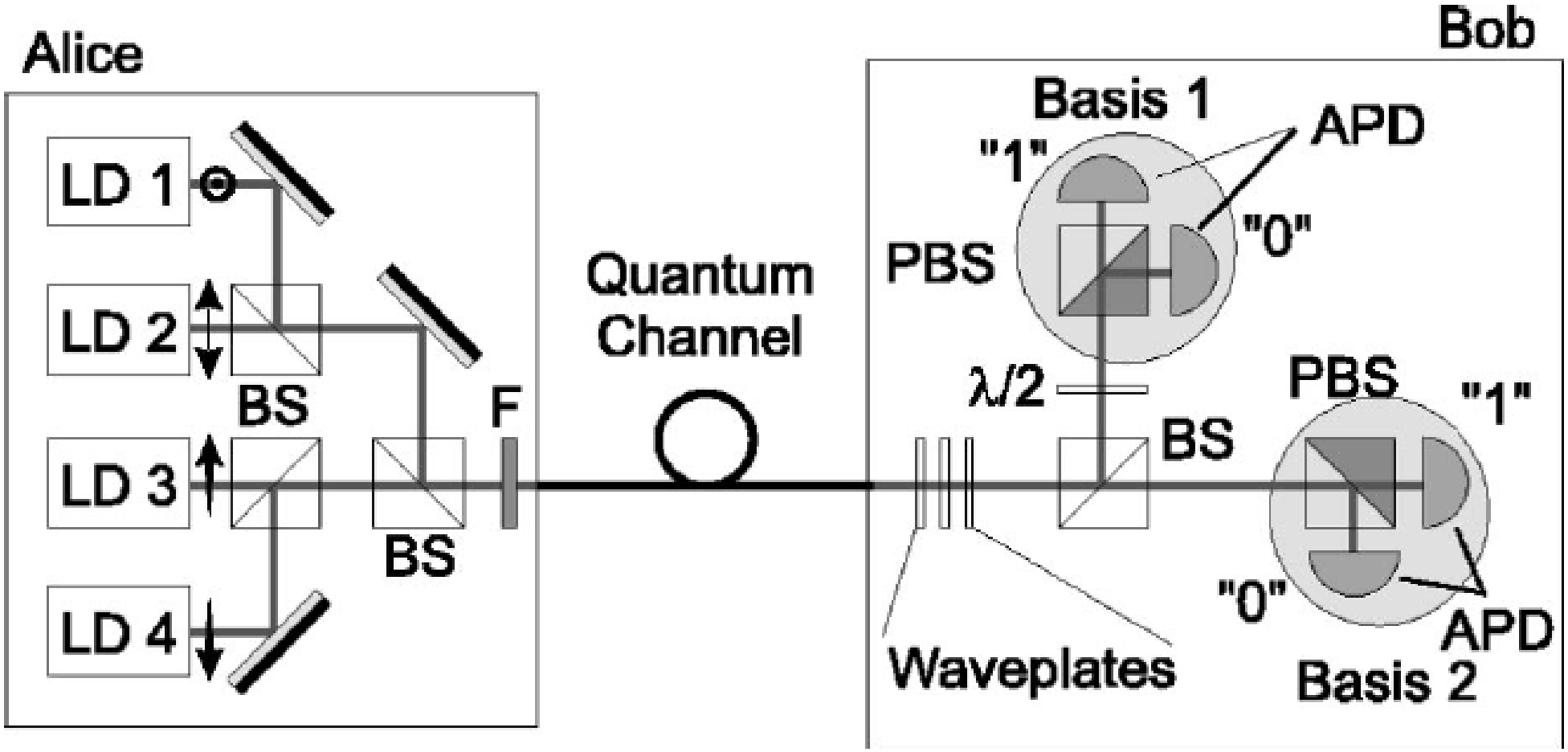
$$\{0,1\}^n \to \{0,1\}^m$$

Toeplitz matrices can be used as 2-universal hash-functions

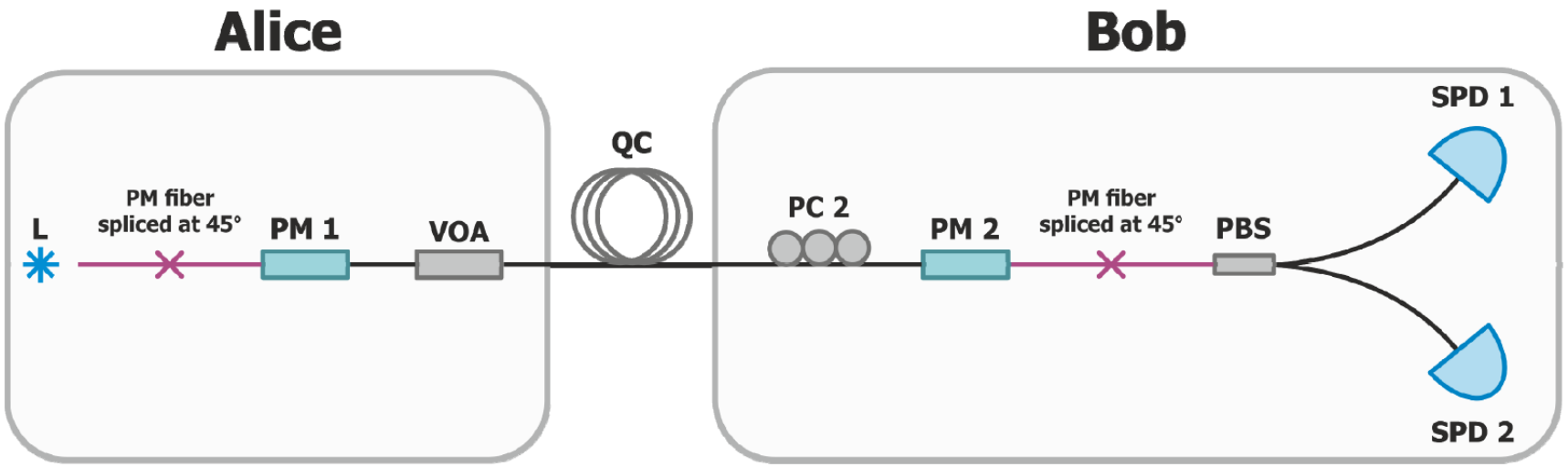
$$\begin{pmatrix} t_m & t_{m+1} & \cdots & t_{m+n-2} & t_{m+n-1} \\ t_{m-1} & t_m & \cdots & t_{m+n-3} & t_{m+n-2} \\ \vdots & t_{m-1} & \ddots & \vdots & \vdots \\ t_2 & \vdots & \ddots & t_n & t_{n+1} \\ t_1 & t_2 & \cdots & t_{n-1} & t_n \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_m \end{pmatrix}$$

$$T_{ij} = T_{kl}$$
$$k - i = l - j$$

BB84: realization of polarization encoding with bulk optics



BB84: realization of polarization encoding with fiber optics



a)

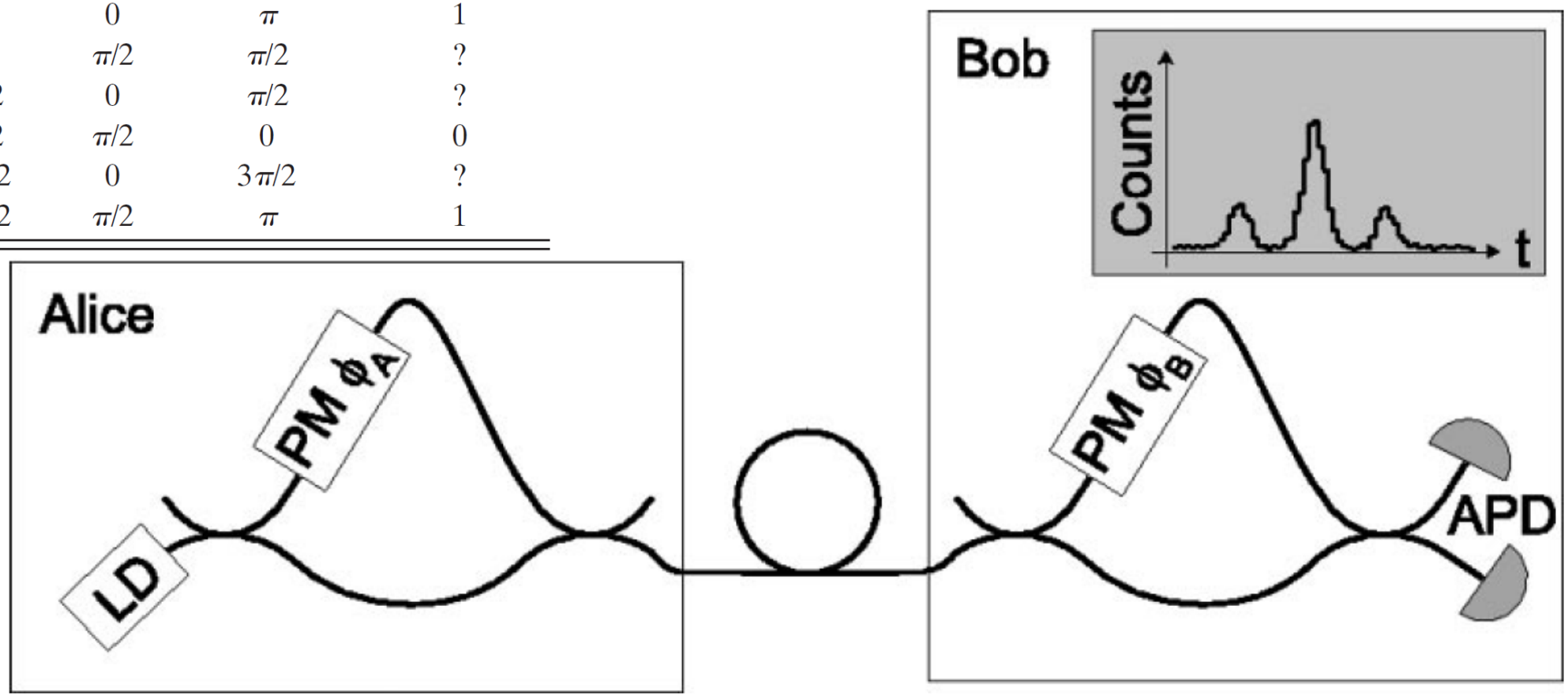
Δφ	SOP
0	
π/2	
π	
3π/2	

b)

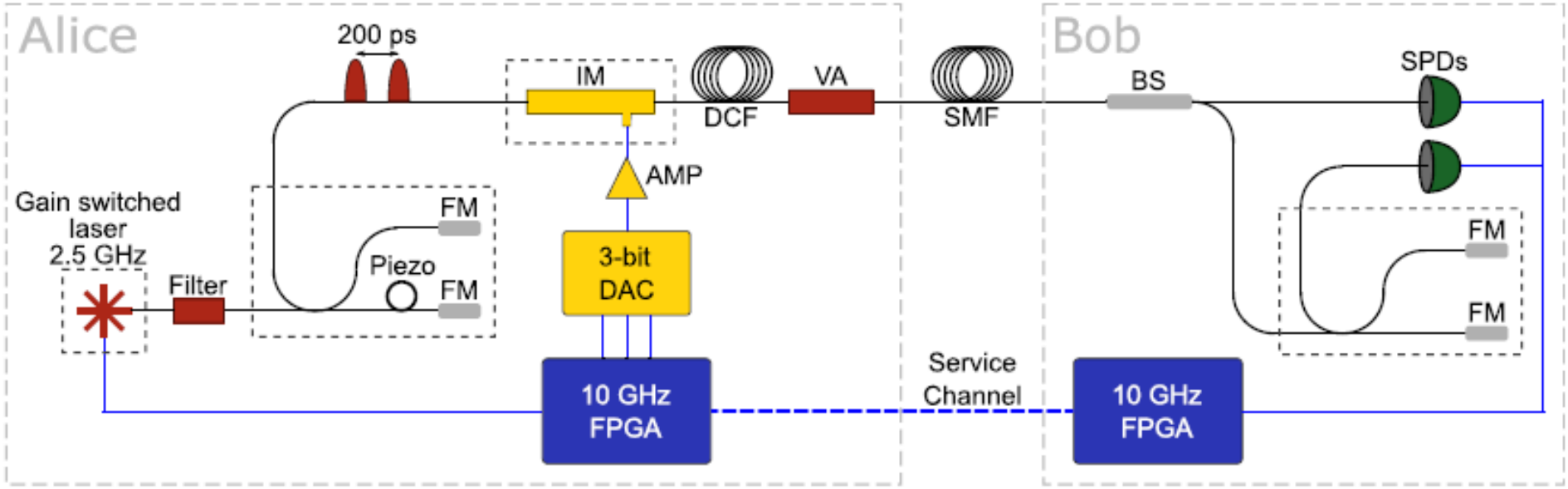
Δφ	SOP
0	
π/2	
π	
3π/2	

PHASE ENCODING

Alice			Bob	
Bit value	ϕ_A	ϕ_B	$\phi_A - \phi_B$	Bit value
0	0	0	0	0
0	0	$\pi/2$	$3\pi/2$	?
1	π	0	π	1
1	π	$\pi/2$	$\pi/2$	?
0	$\pi/2$	0	$\pi/2$	?
0	$\pi/2$	$\pi/2$	0	0
1	$3\pi/2$	0	$3\pi/2$	?
1	$3\pi/2$	$\pi/2$	π	1

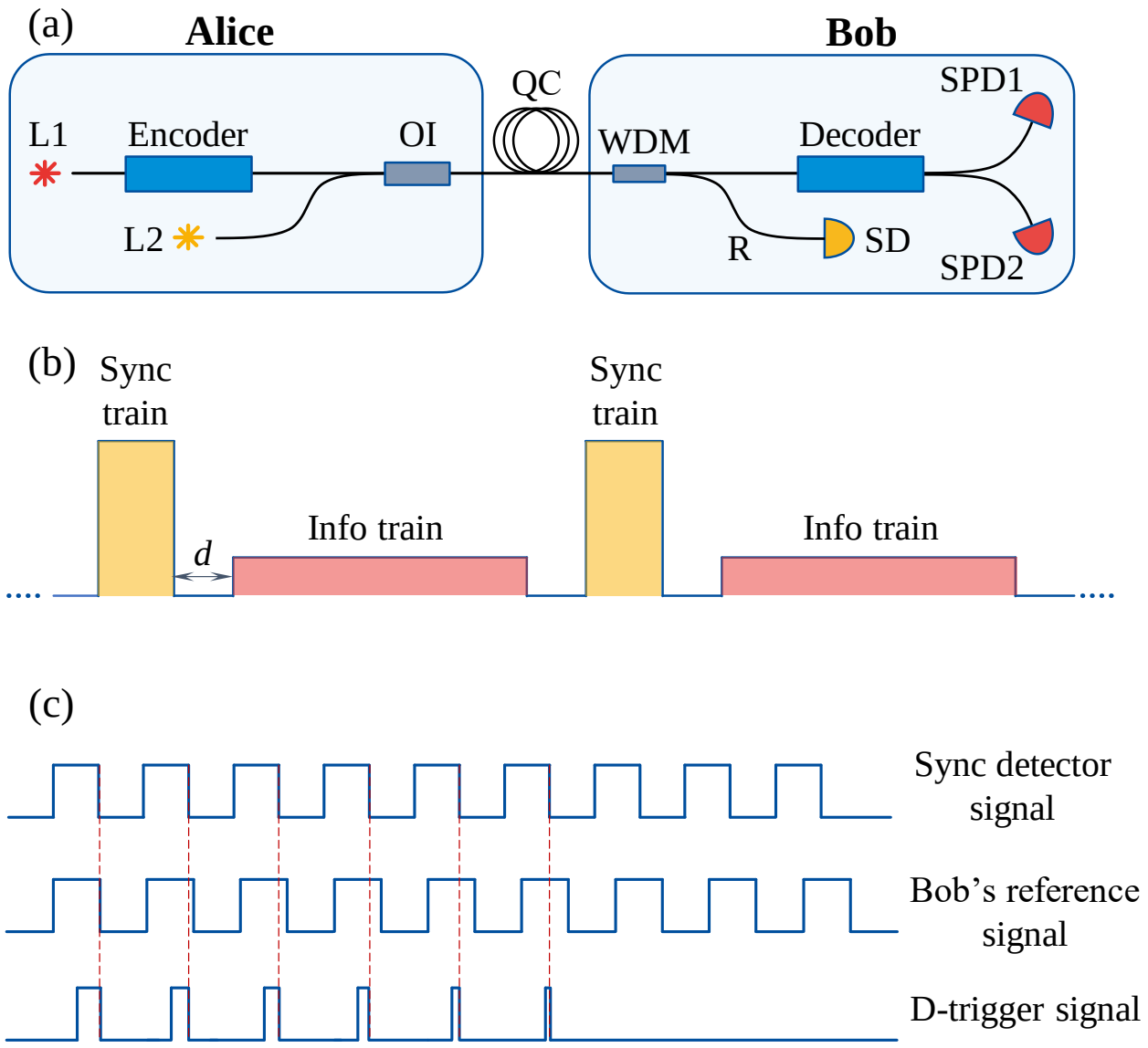


Time-bin encoding

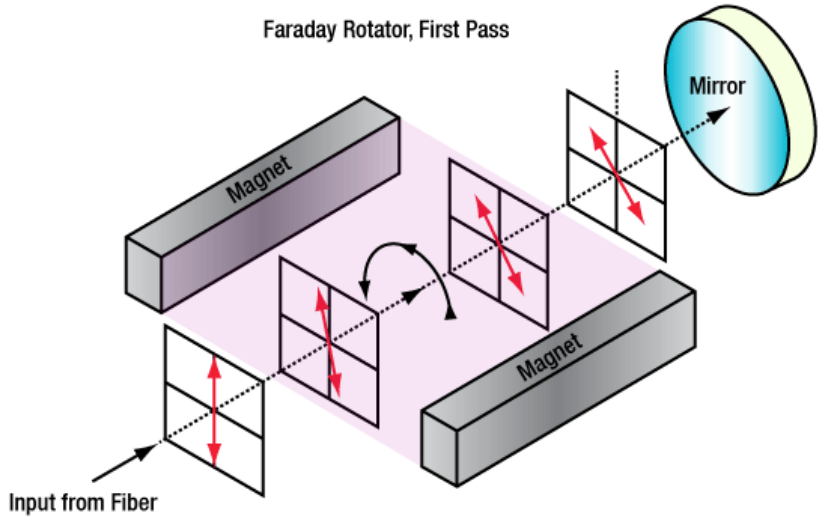


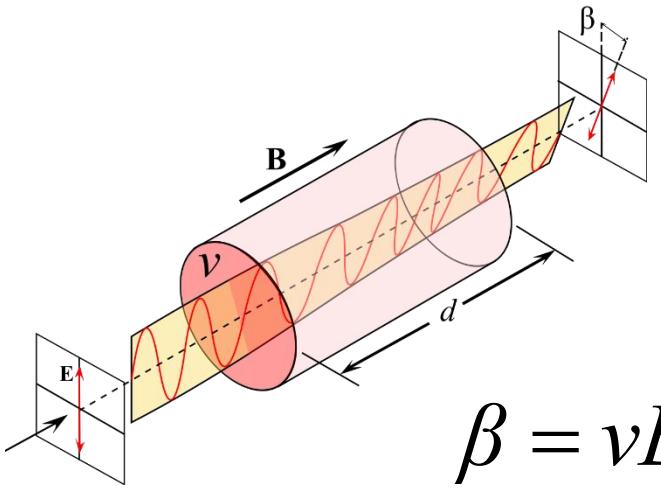
basis, bit	state	μ_1	μ_2
Z, 0	$\|\psi_0\rangle$		
Z, 1	$\|\psi_1\rangle$		
X	$\|\psi_+\rangle$		

SYNCHRONIZATION



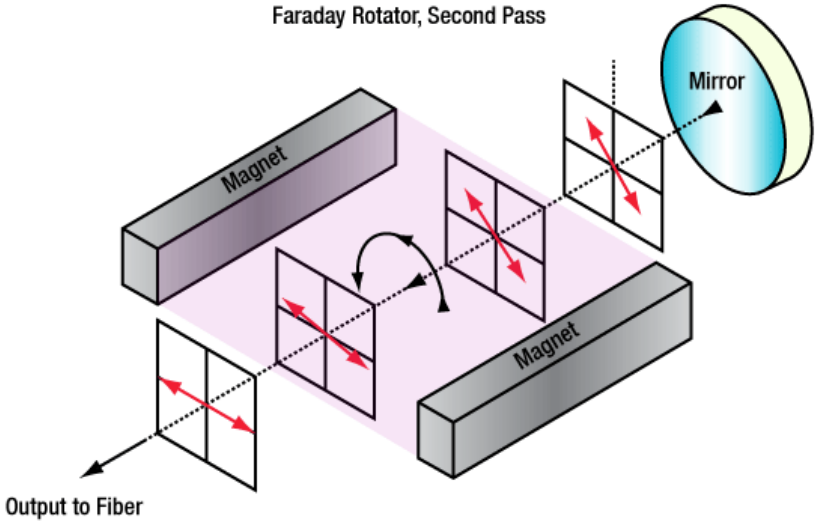
BB84: components to build a real system (Faraday mirror)





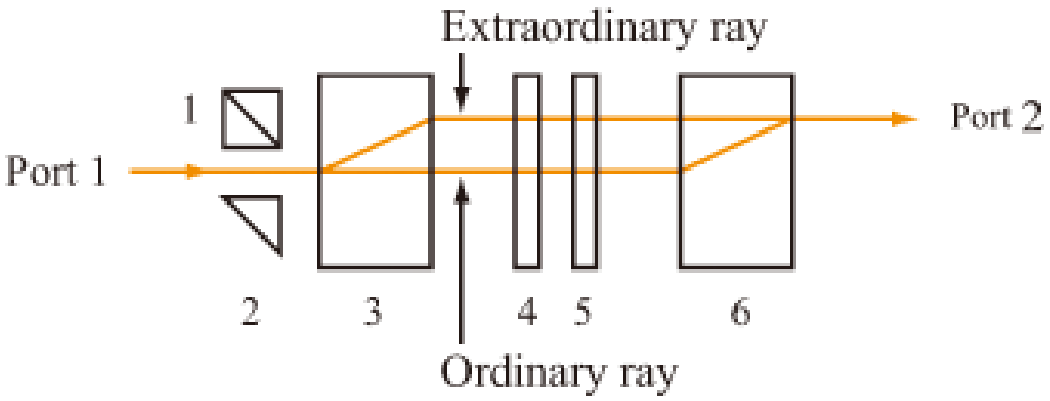
$$\beta = \nu B l$$

ν – Verdet constant

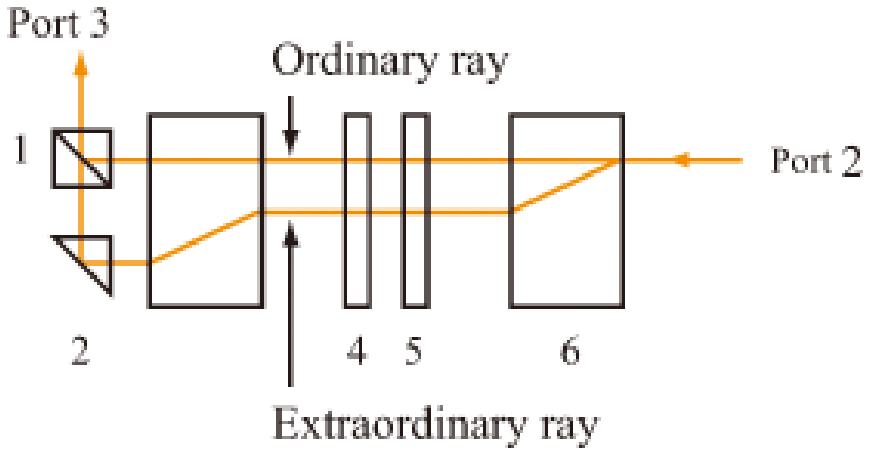


$Tb_3Ga_5O_{12}$

BB84: components to build a real system (optical circulator)



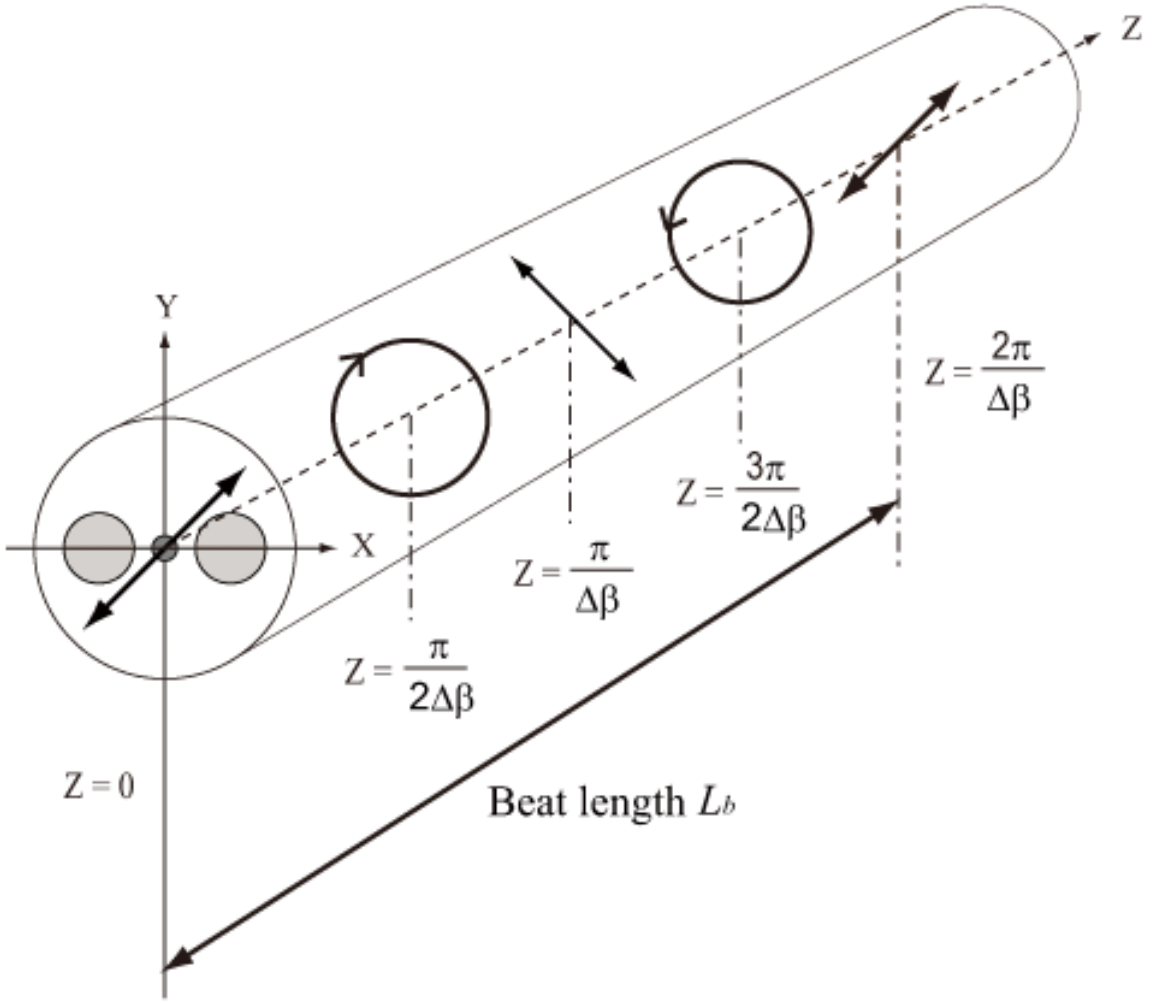
$$|V\rangle \xrightarrow{F} |+\rangle \xrightarrow{\lambda/2} |H\rangle$$
$$|H\rangle \xrightarrow{F} |-\rangle \xrightarrow{\lambda/2} |V\rangle$$



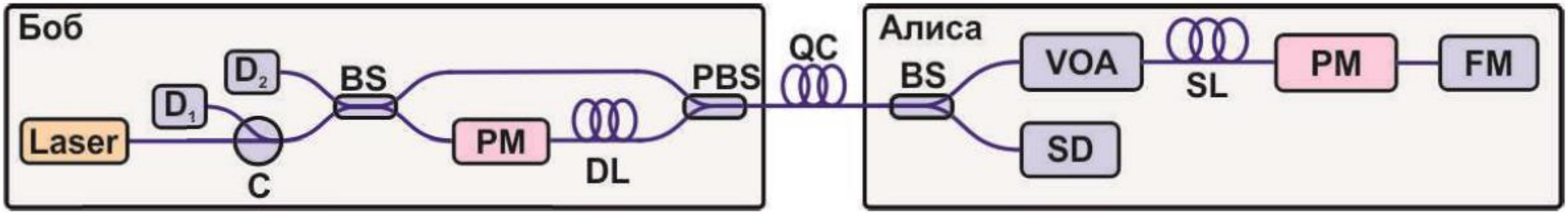
$$|V\rangle \xrightarrow{\lambda/2} |+\rangle \xrightarrow{F} |V\rangle$$
$$|H\rangle \xrightarrow{\lambda/2} |-\rangle \xrightarrow{F} |V\rangle$$

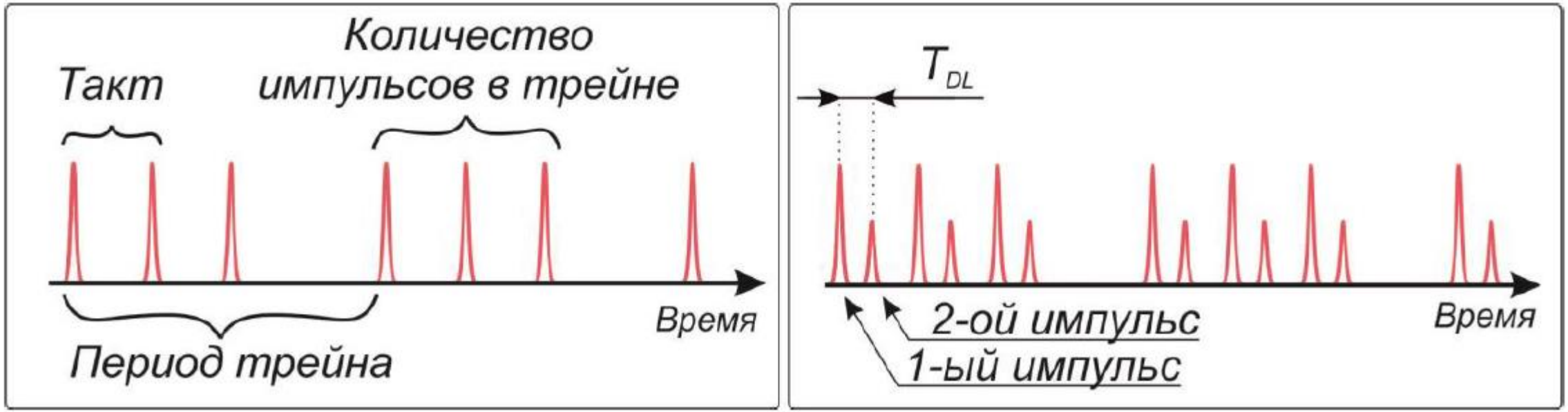
1 – PBS, 2 – reflecting prism, 3, 6 – birefringent crystal, 4 – Faraday rotator, 5 – half-wave plate

BB84: components to build a real system (polarization maintaining fiber)



BB84: Plug&Play system



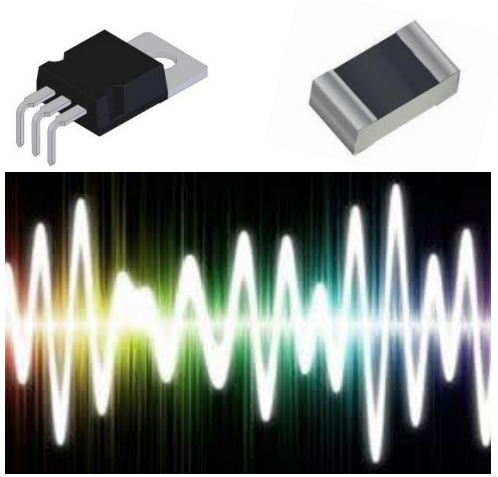


QUANTUM RANDOM NUMBER GENERATOR

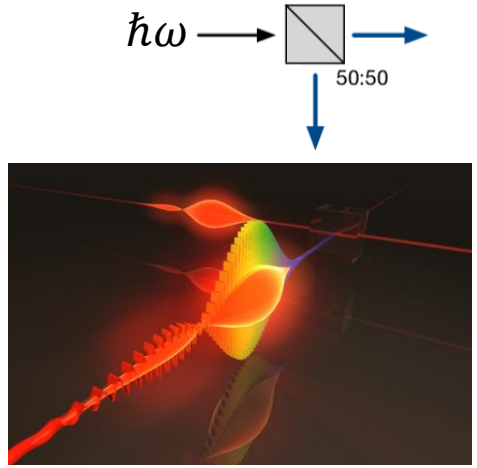
Pseudorandom

True random

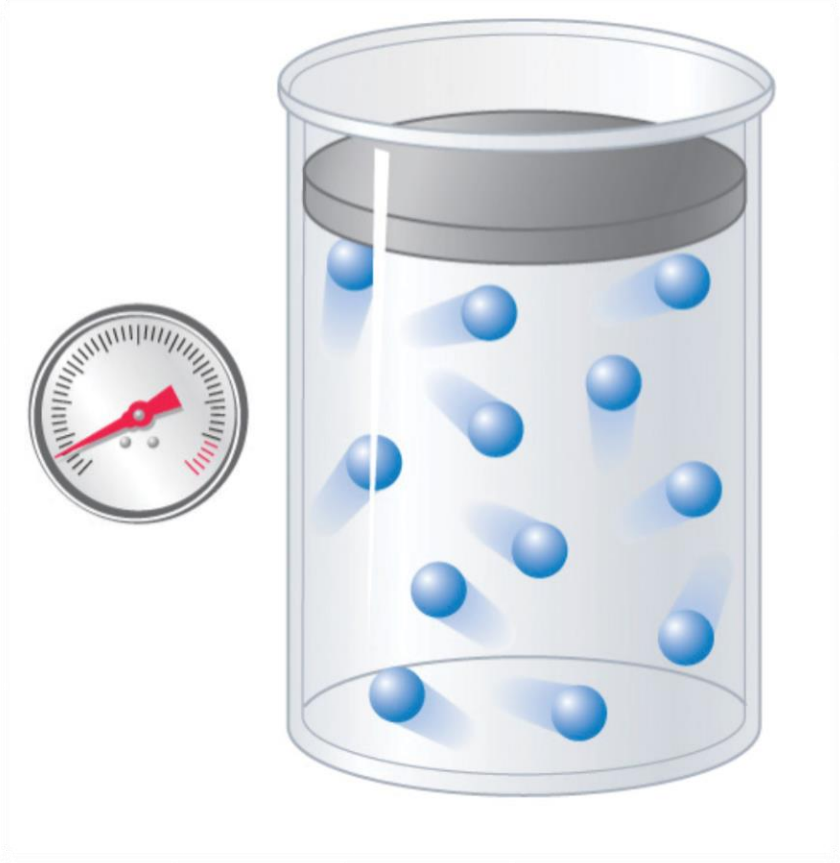
Classical



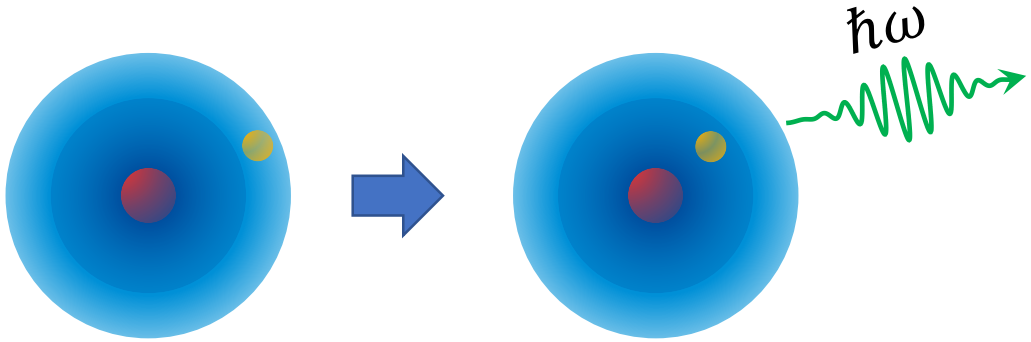
Quantum



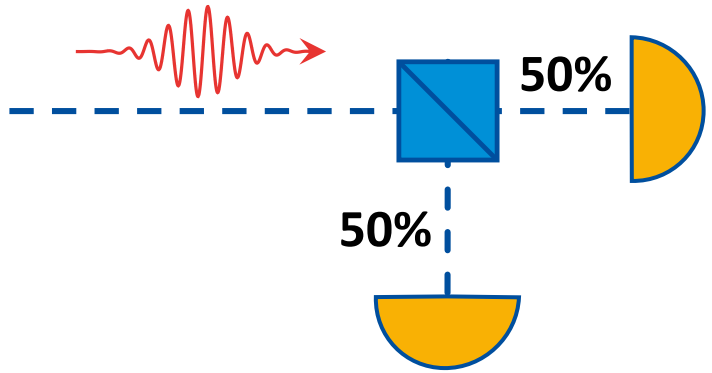
CLASSICAL vs QUANTUM PROCESS



The gas pressure can be predicted in any moment of time (at least at principle) **exactly**

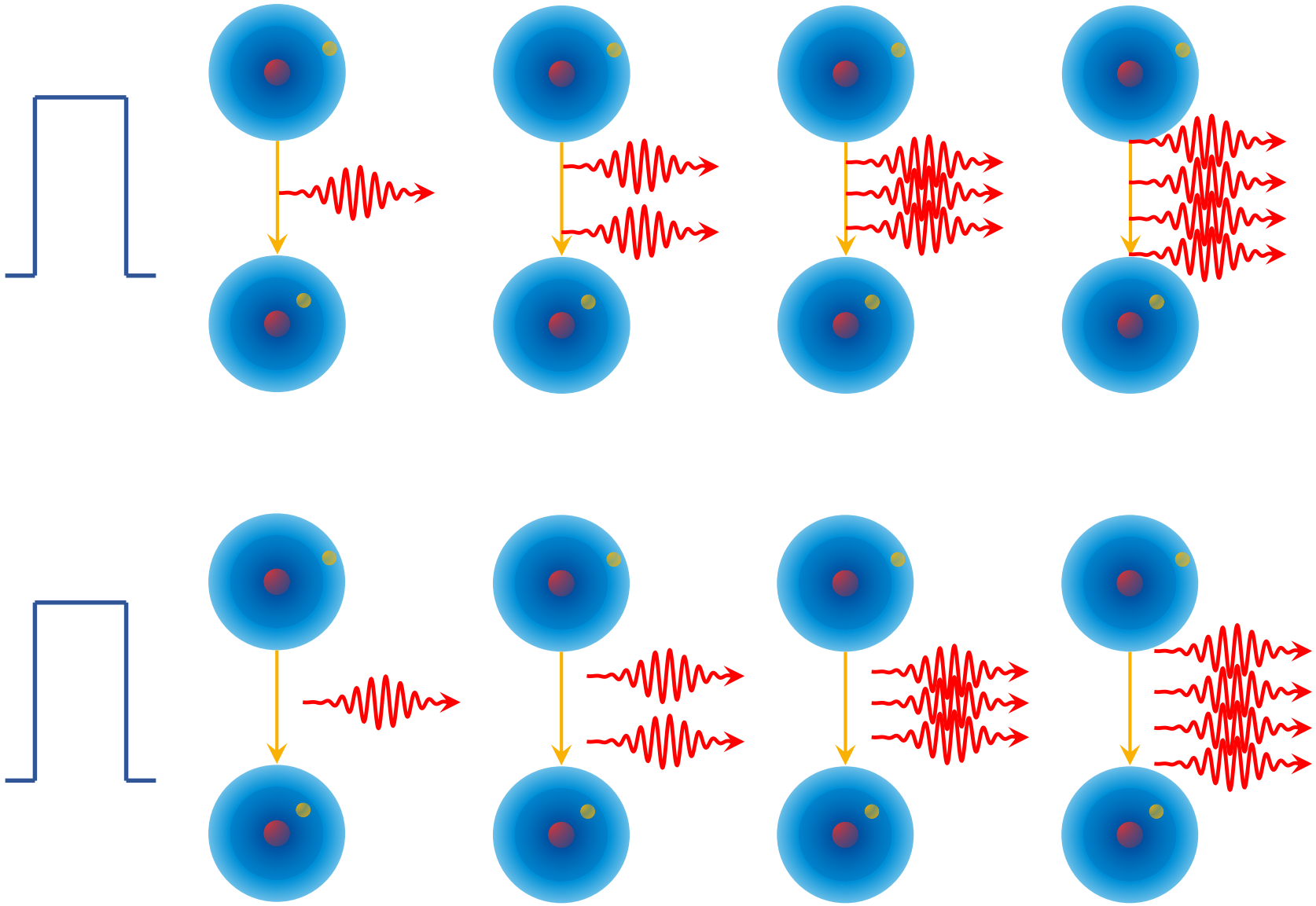


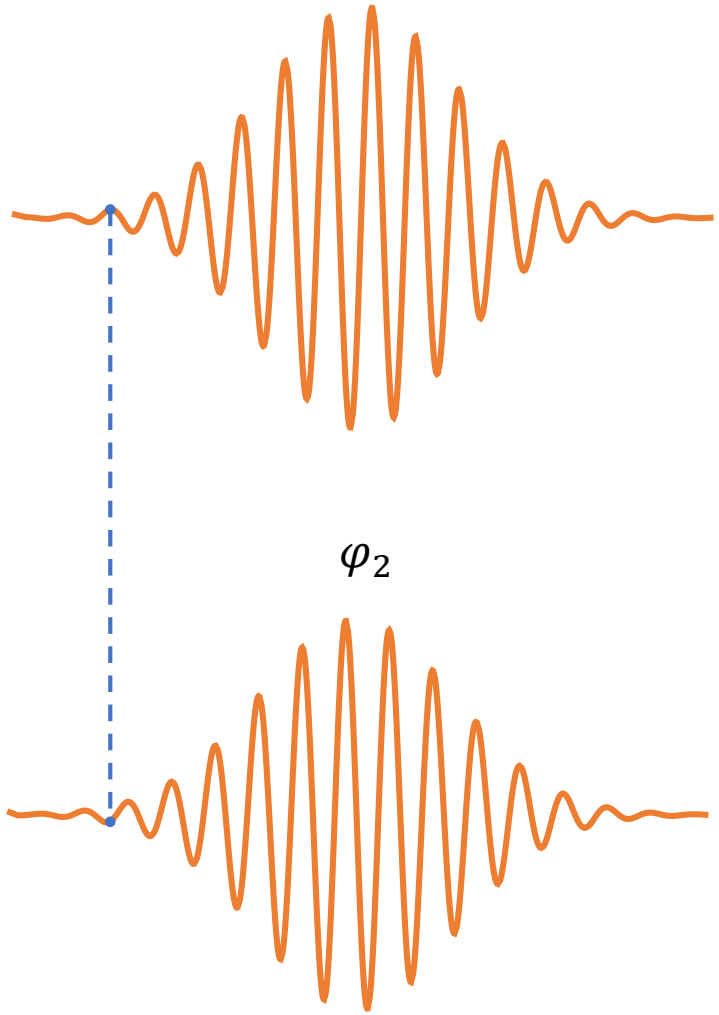
The moment of time when the atom emits a photon can be predicted only with **some probability**



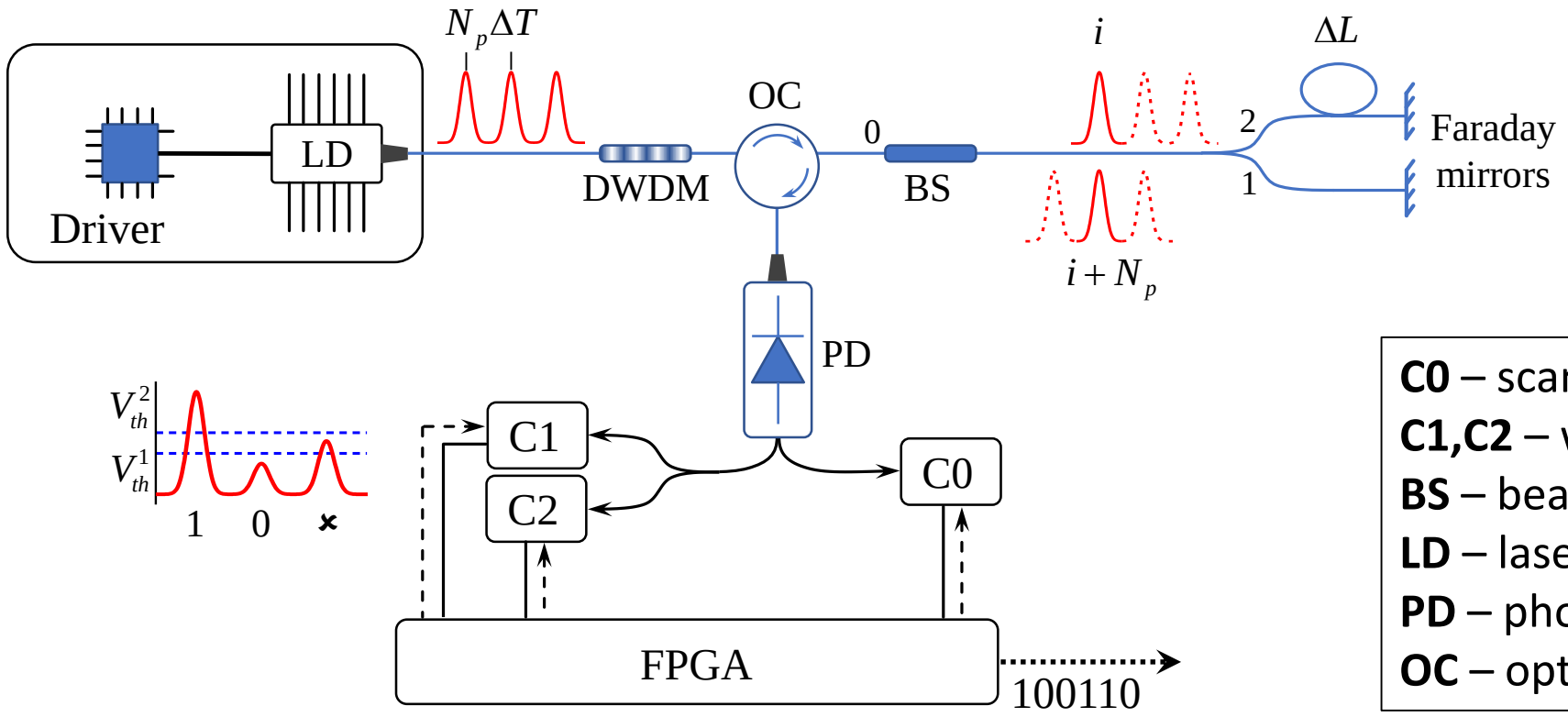
A single photon will be reflected or transmitted in the 50:50 beamsplitter with the **probability 50%**

QUANTUM NOISE IN A LASER





QRNG ON PHASE NOISE IN A SEMICONDUCTOR LASER



C0 – scanning comparator
C1,C2 – working comarators
BS – beamsplitter
LD – laser diode
PD – photodetector
OC – optical circlator

CHALLENGES OF PRACTICAL QKD: losses

Beer's law

$$n(L) = n_0 e^{-\beta L}$$

Exercise 1

Alice sends a photon to Bob, who is 300 km away, via a fiber line. The fiber has a loss rate of 5% per kilometer:

a) Find the loss coefficient β in that fiber (in km^{-1}).

b) What fraction of the photons sent by Alice will reach Bob?

CHALLENGES OF PRACTICAL QKD: losses

Beer's law

$$n(L) = n_0 e^{-\beta L}$$

Exercise 1

Alice sends a photon to Bob, who is 300 km away, via a fiber line. The fiber has a loss rate of 5% per kilometer:

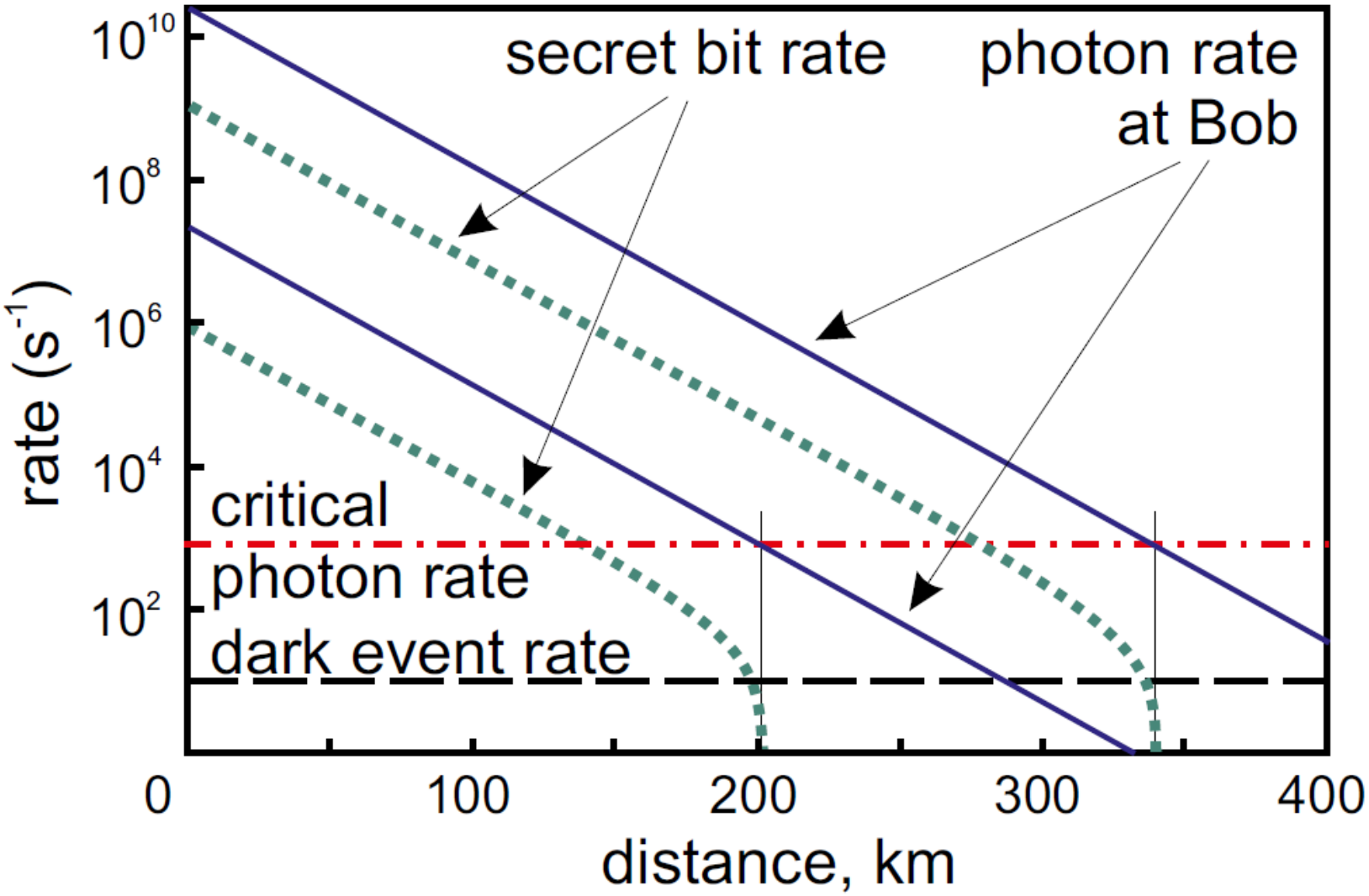
a) Find the loss coefficient β in that fiber (in km^{-1}).

b) What fraction of the photons sent by Alice will reach Bob?

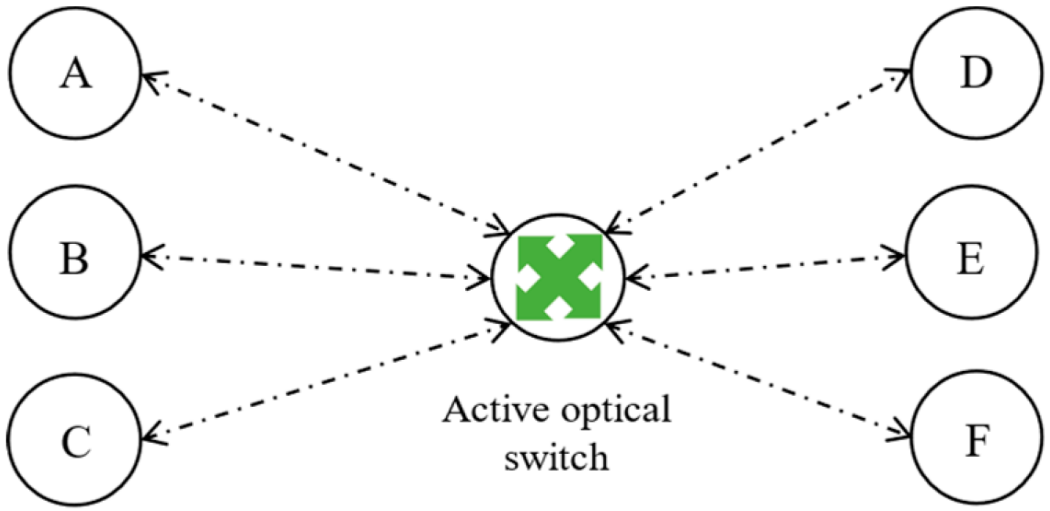
a) $n(1\ \mathrm{km}) = n_0 e^{-\beta \cdot 1} = 0.95 n_0 \rightarrow \beta = -(\ln 0.95) \approx 0.0513\ \mathrm{km}^{-1}$.

b) At $L = 300$ km we have: $e^{-\beta L} = e^{-15} \approx 2 \times 10^{-7}$.

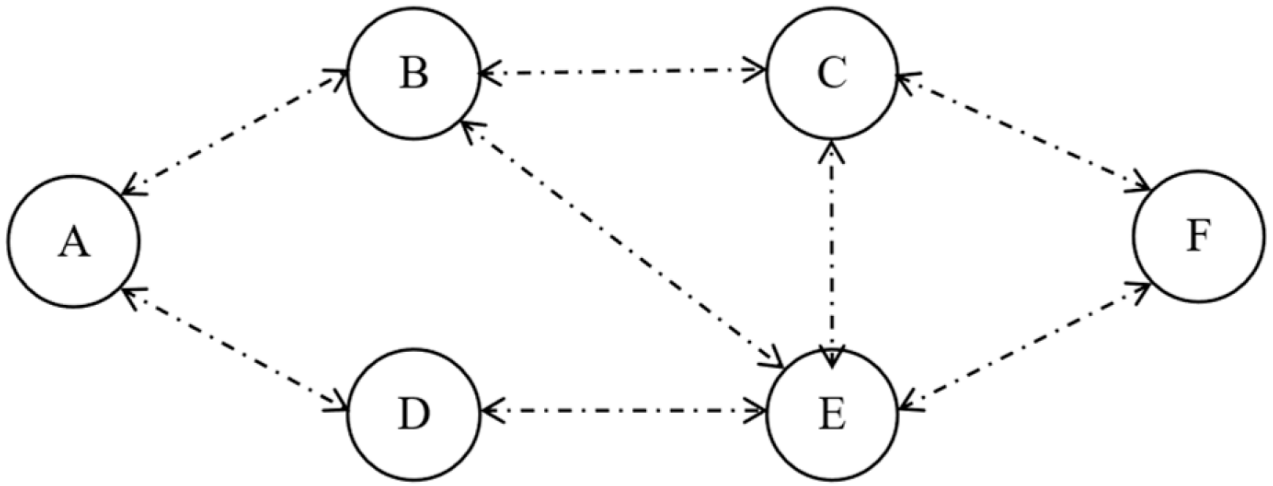
CHALLENGES OF PRACTICAL QKD: losses + dark counts



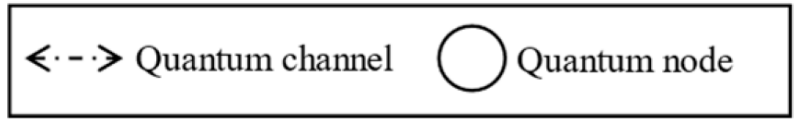
QUANTUM NETWORK (QKD NETWORK)



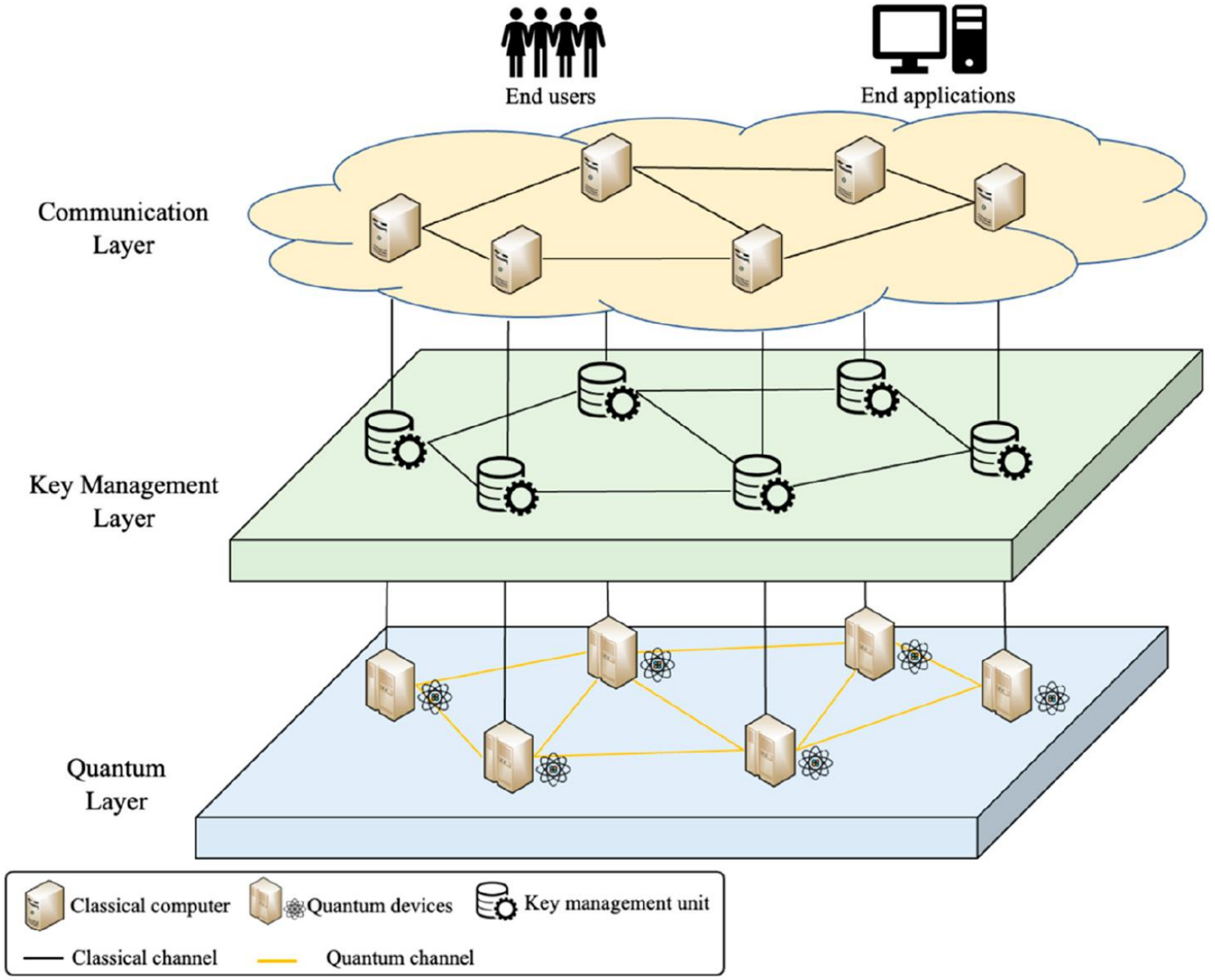
(a)



(b)



QUANTUM NETWORK (QKD NETWORK)



SATELLITE QKD