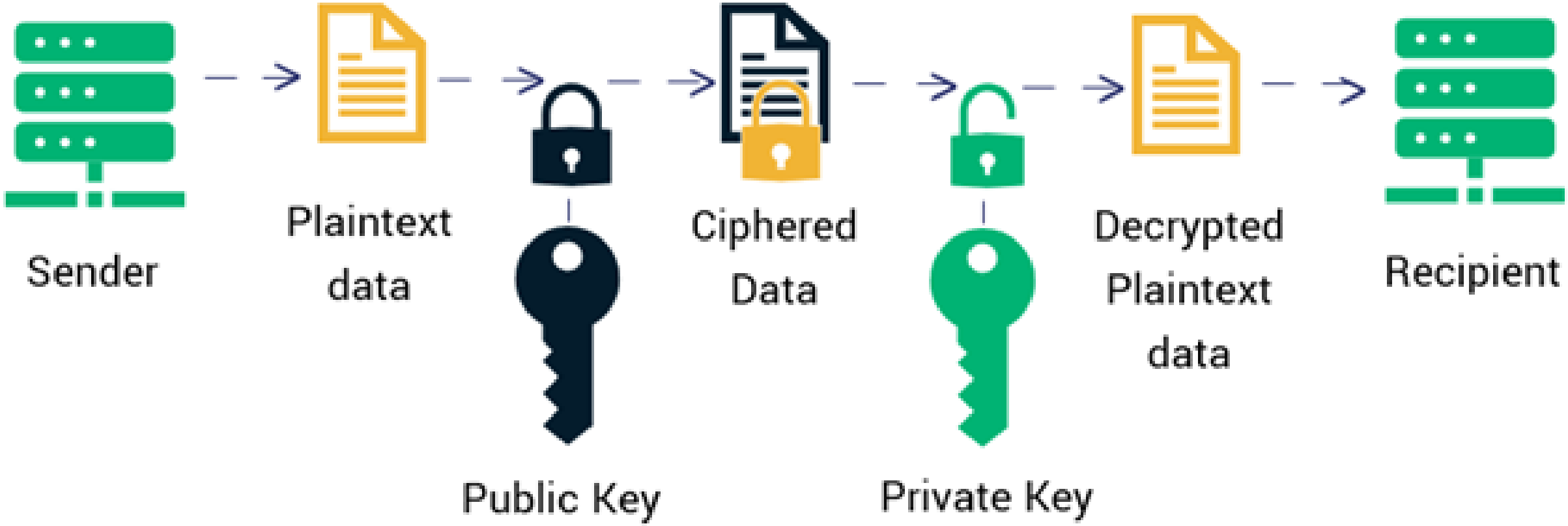

Towards MDI QKD
Roman Shakhovoy

PUBLIC KEY ENCRYPTION



RSA PROTOCOL. Key generation

1. Generate two large random (and distinct) primes p and q, each roughly the same size.
2. Compute $n = pq$ and $\varphi = (p-1)(q-1)$.
3. Select a random integer e, $1 < e < \varphi$, such that $\gcd(e, \varphi) = 1$.
4. Compute the unique integer d $(1 < d < \varphi)$, such that $ed \equiv 1 \pmod{\varphi}$ (i.e. φ divides $(ed - 1)$).
5. Alice's public key is (n, e); private key is d.

RSA PROTOCOL. Encryption and decryption

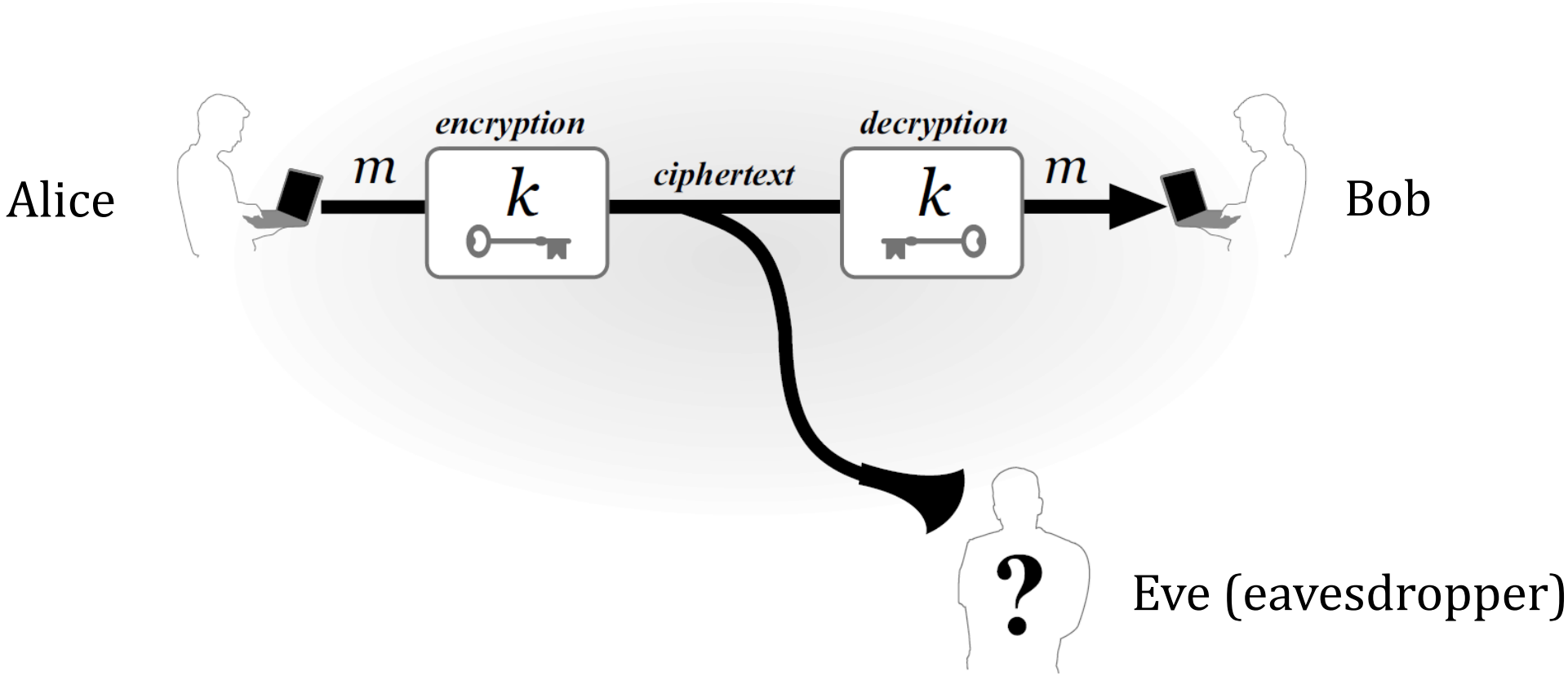
1. ***Encryption***. Bob should do the following:
   (a) Obtain Alice's authentic public key (n, e).
   (b) Represent the message as an integer m in the interval $[0, n-1]$.
   (c) Compute $c = m^e \bmod n$.
   (d) Send the ciphertext c to Alice.

2. ***Decryption***. To recover plaintext m from c, Alice should do the following:
   (a) Use the private key d to recover $m = c^d \bmod n$.

RSA PROTOCOL. Example

1. ***Key generation***. Alice chooses the primes $p = 2357$, $q = 2551$, and computes $n = pq = 6012707$ and $\varphi = (p-1)(q-1) = 6007800$. Alice chooses $e = 3674911$ and finds $d = 422191$ such that $ed = 1 (\mathrm{mod}\, \varphi)$. Alice's public key is the pair $(n = 6012707, e = 3674911)$, while Alice's private key is $d = 422191$.
2. ***Encryption***. To encrypt a message $m = 5234673$, Bob computes
$$c = m^e \bmod n = 5234673^{3674911} \bmod 6012707 = 3650502,$$
and sends this to Alice.
3. ***Decryption***. To decrypt c, Alice computes:
$$c^d \bmod n = 3650502^{422191} \bmod 6012707 = 5234673.$$

PRIVATE-KEY ENCRYPTION



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:*

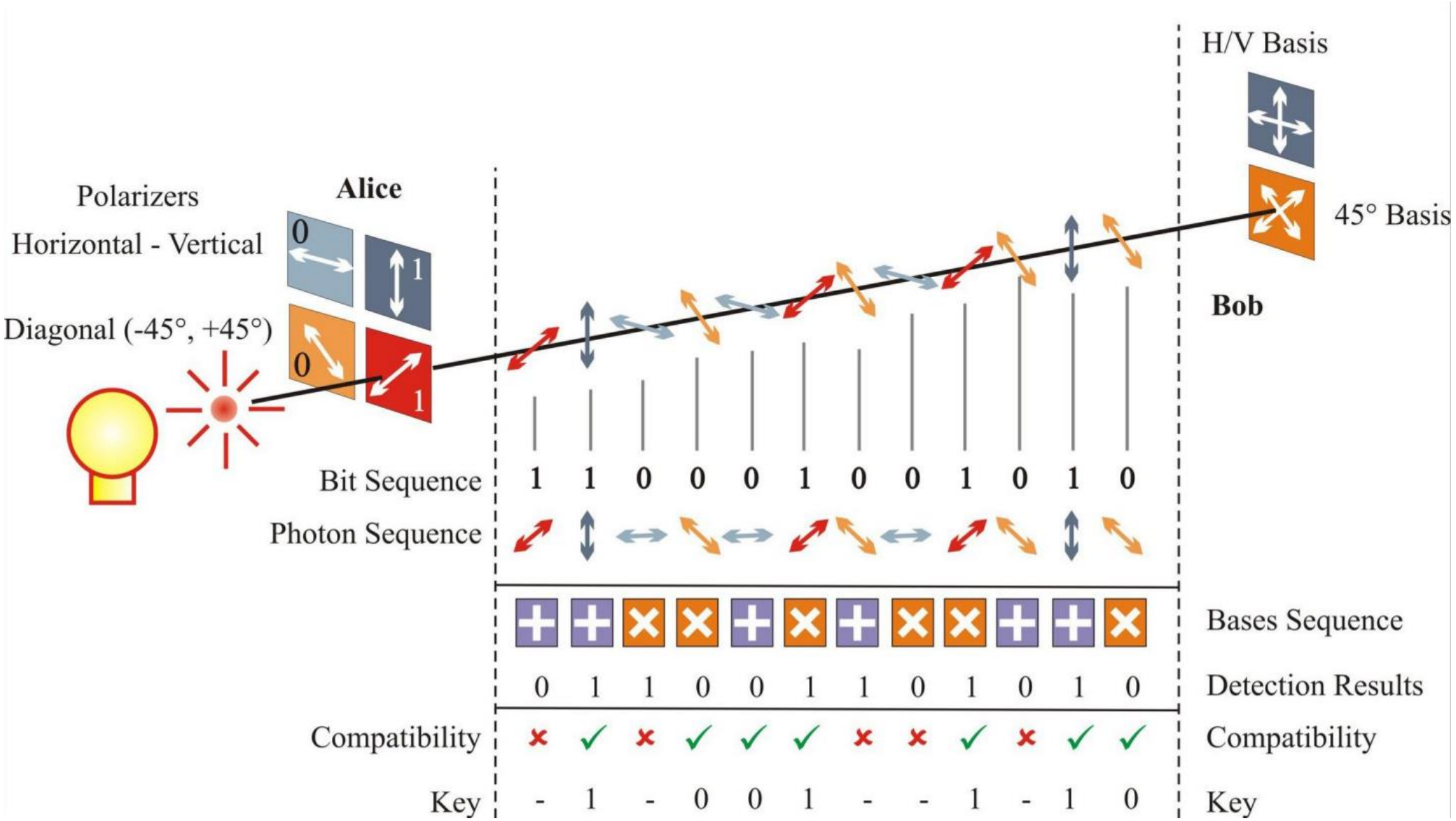
1. *Every key* $k \in \mathcal{K}$ *is chosen with (equal) probability* $1/|\mathcal{K}|$ *by algorithm* Gen.
2. *For every* $m \in \mathcal{M}$ *and every* $c \in \mathcal{C}$*, there exists a unique key* $k \in \mathcal{K}$ *such that* $\mathsf{Enc}_k(m)$ *outputs* c.

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 $m := k \oplus c$.

QUANTUM CRYPTOGRAPHY: BB84 protocol



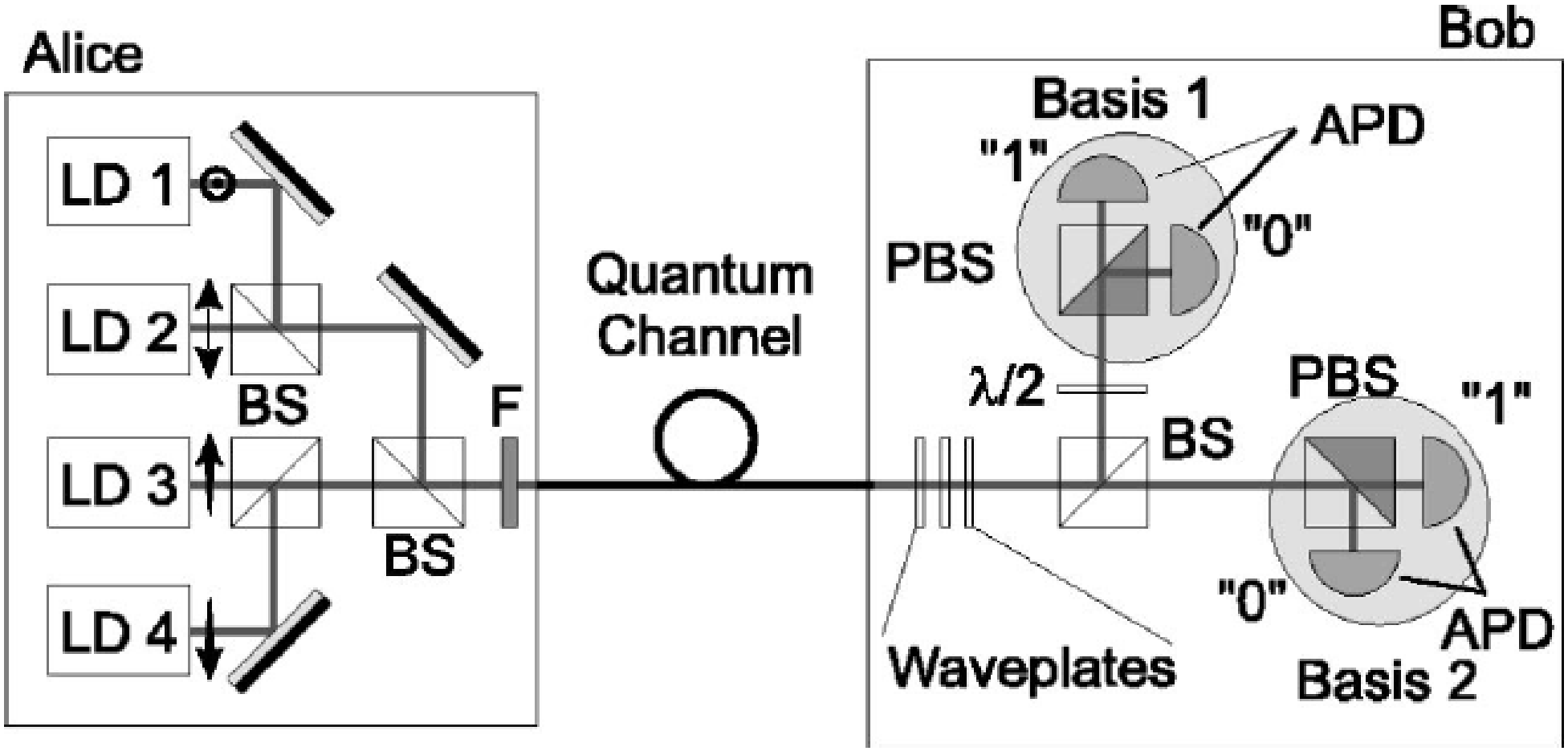
POSTPROCESSING: error estimation

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.

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

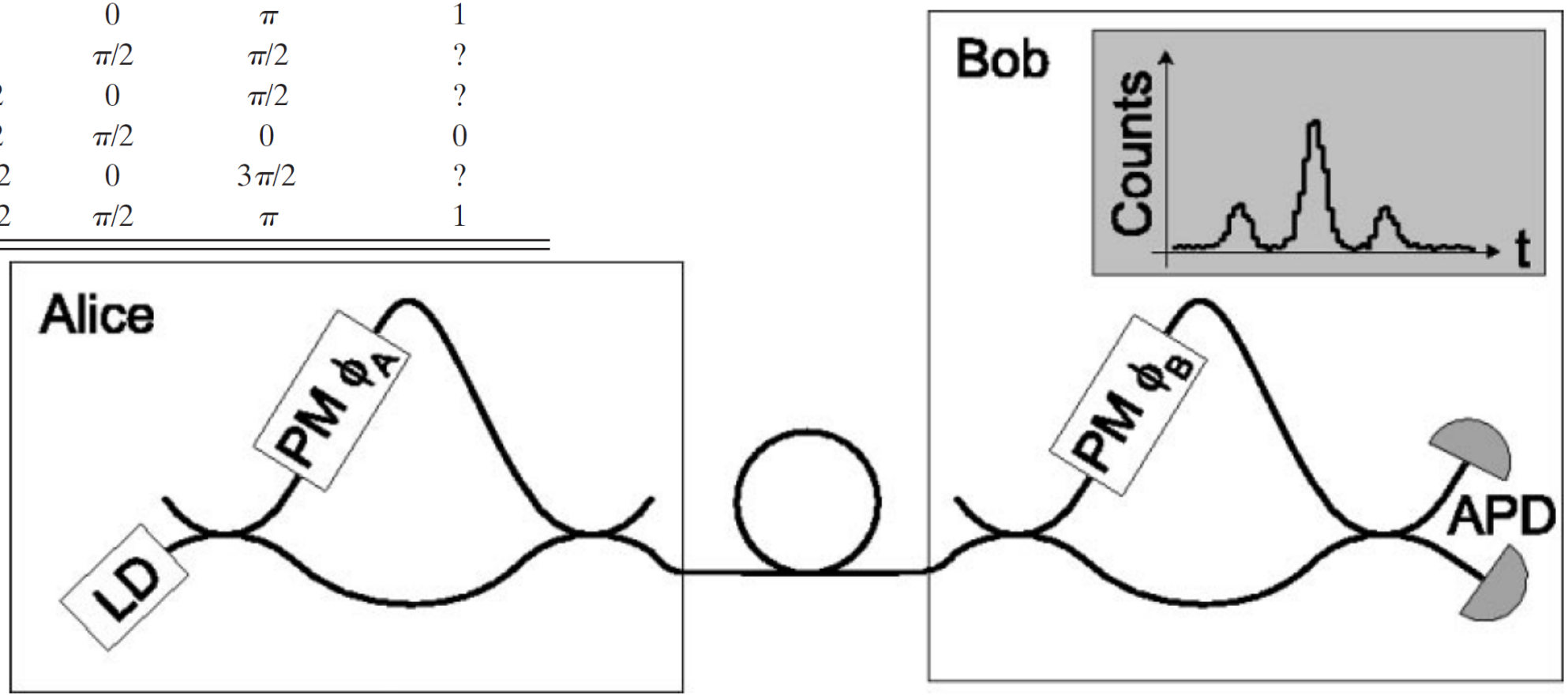
QBER should not exceed $\approx 11\%$, because the best error correction code approaches a maximal tolerated error rate of 12,9%.

BB84: realization of polarization encoding with bulk optics

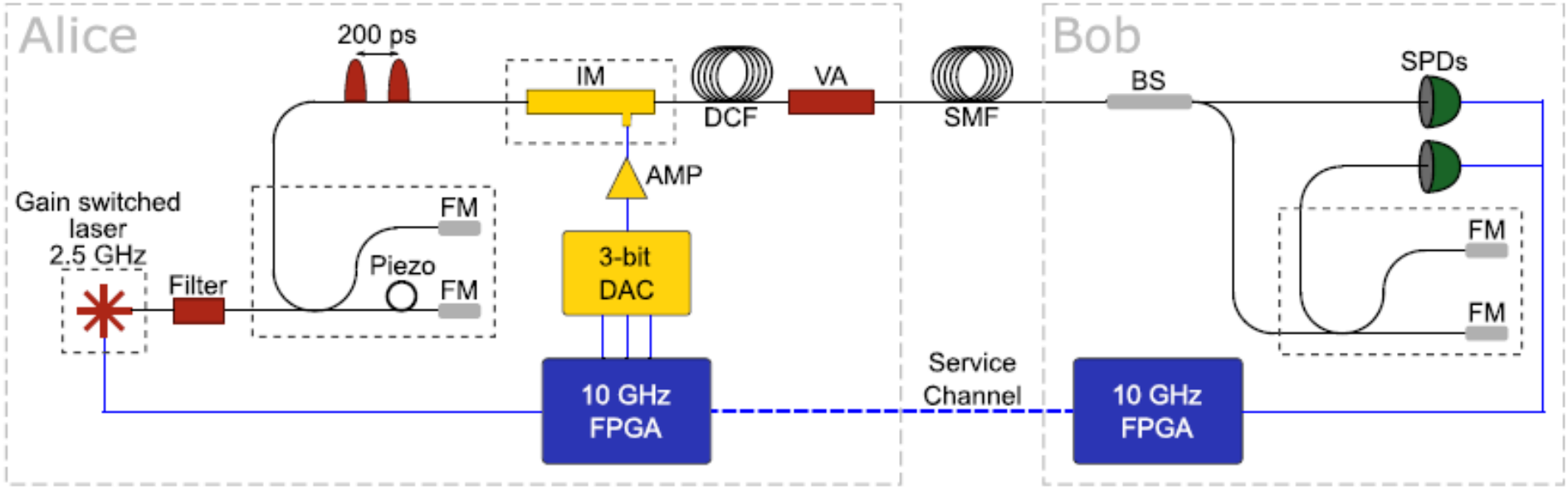


PHASE ENCODING

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	$\|\psi_+\rangle$		

CHALLENGES OF PRACTICAL QKD: losses

Beer's law

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

Exercise

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:

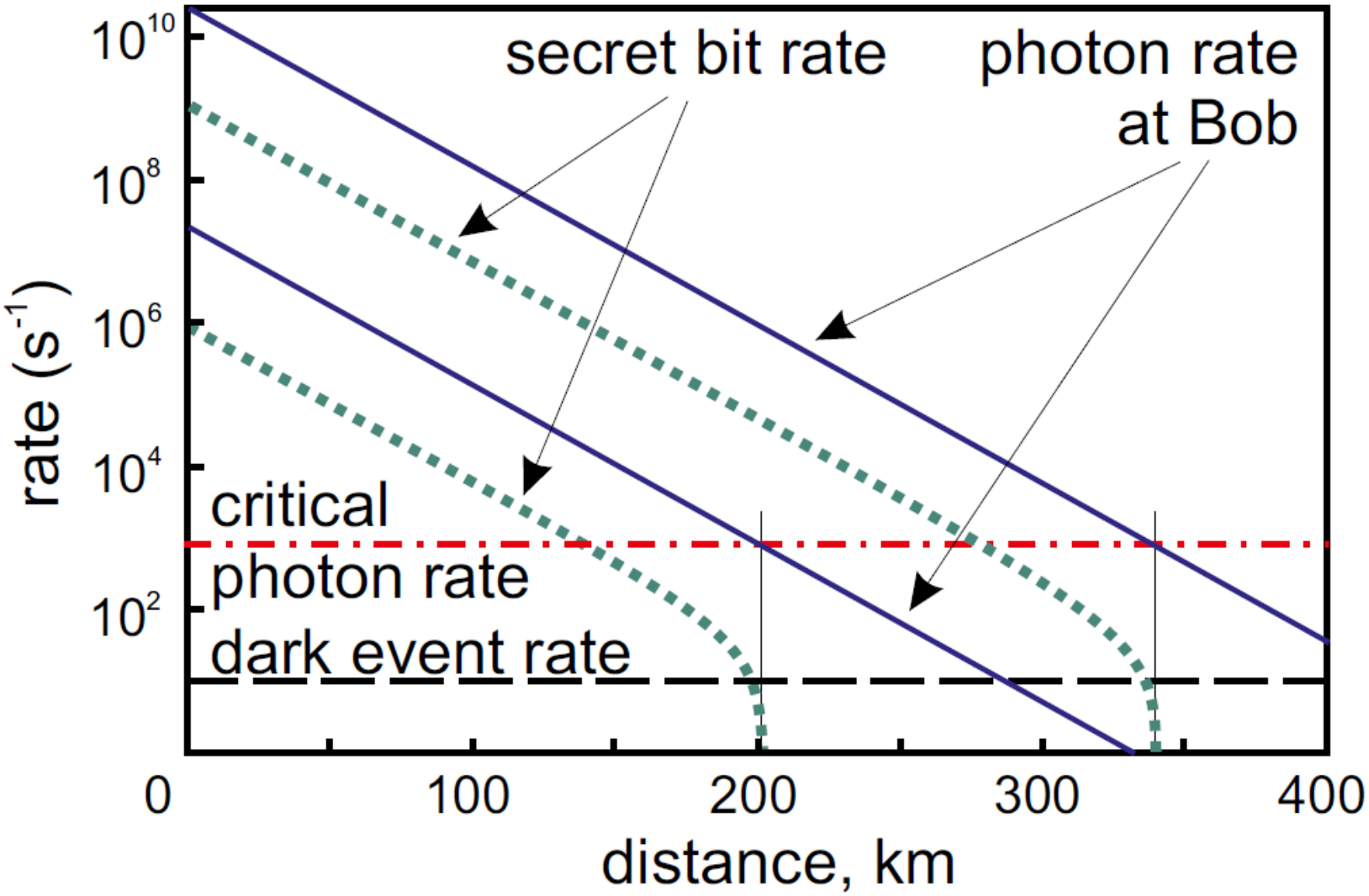
a) Find the loss coefficient β in that fiber (in km^{-1}).

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

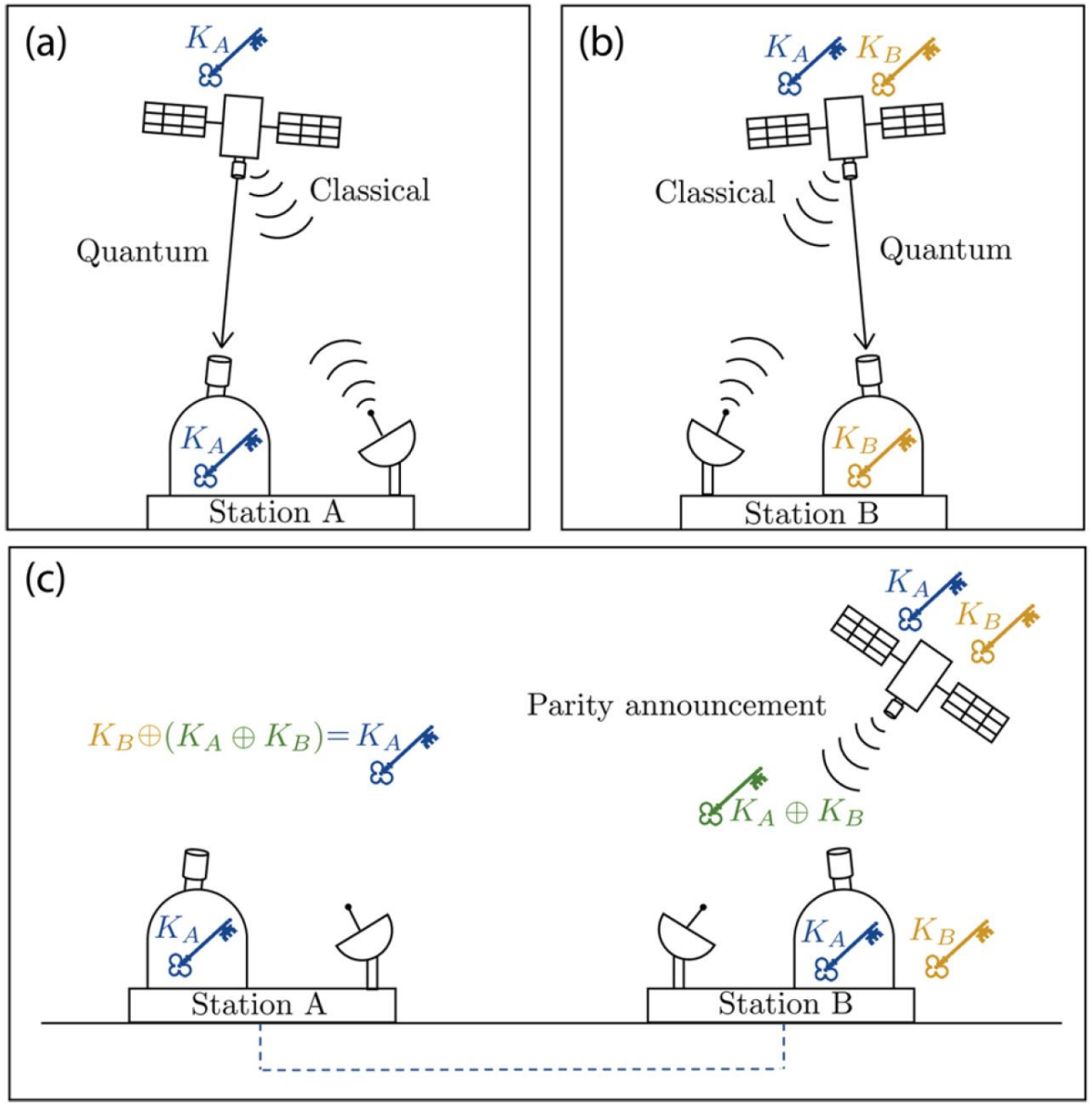
a) $n(1\ \mathrm{km}) = n_0 e^{-\beta \cdot 1} = 0.95 n_0 \rightarrow \beta = -(\ln 0.95) \approx 0.0513\ \mathrm{km}^{-1}$.

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

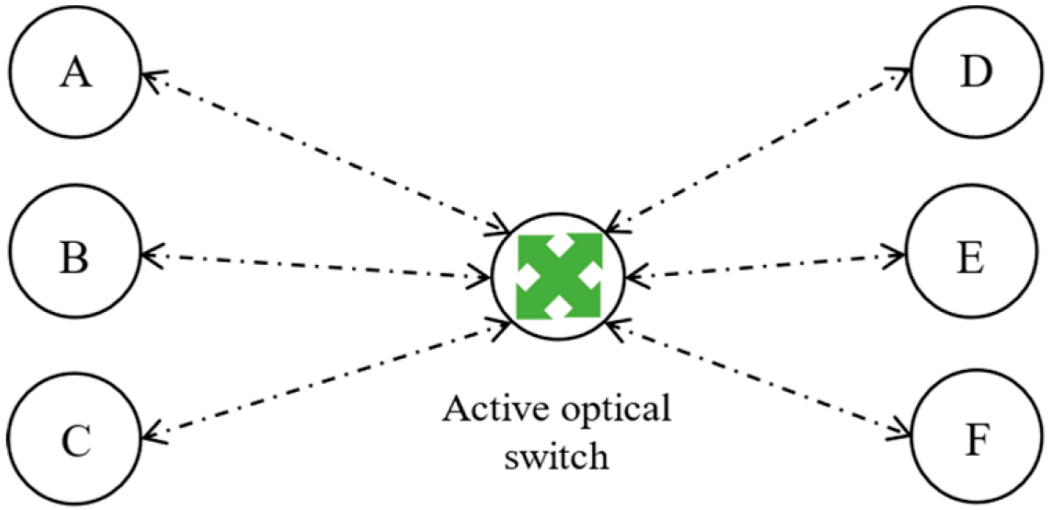
CHALLENGES OF PRACTICAL QKD: losses + dark counts



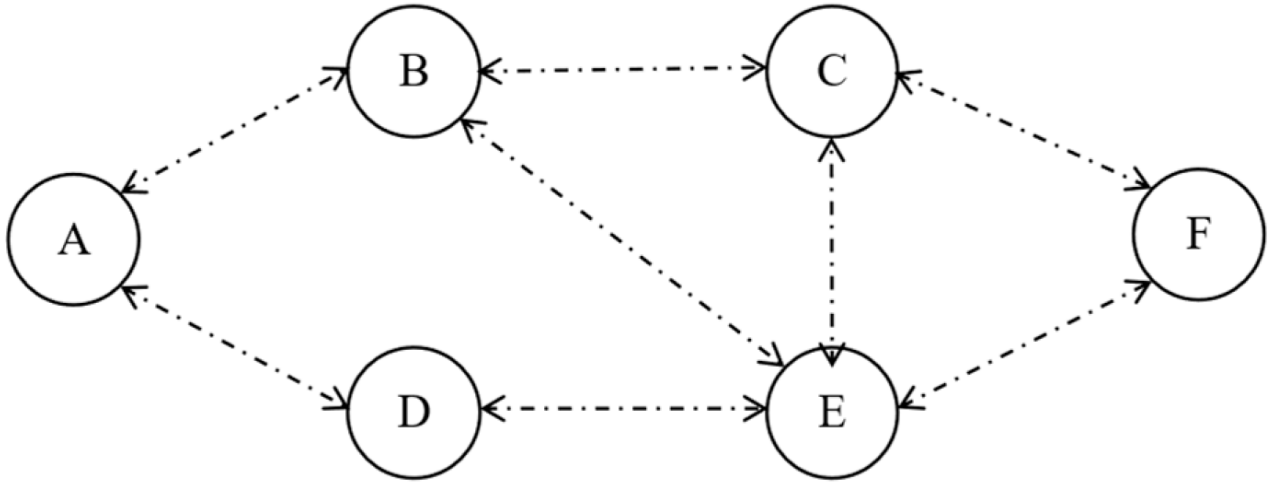
SATELLITE QKD



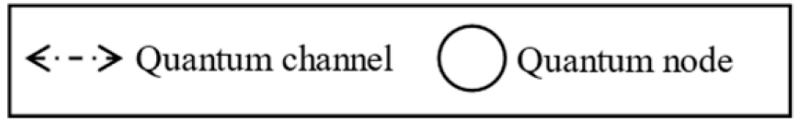
QUANTUM NETWORK (QKD NETWORK)



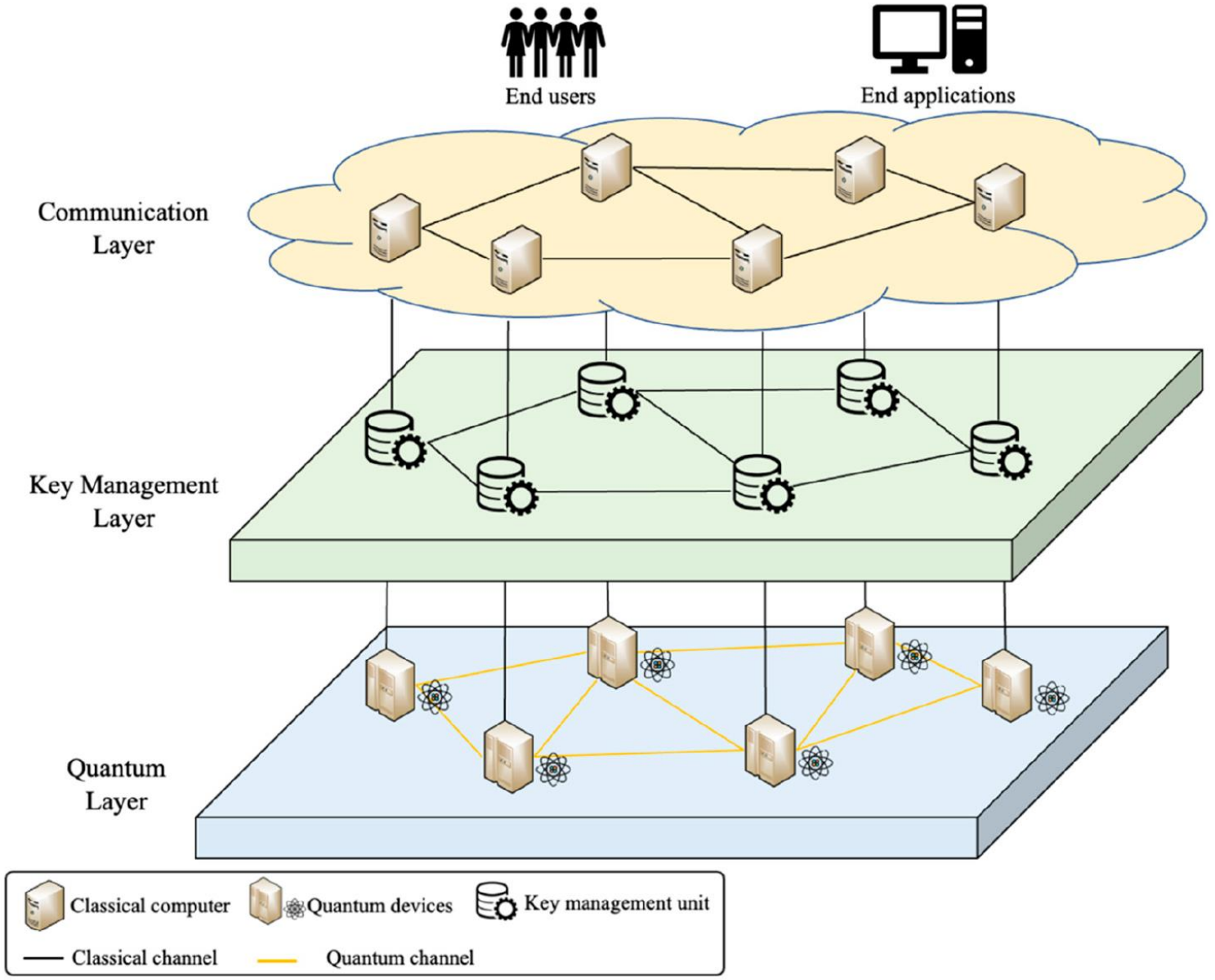
(a)



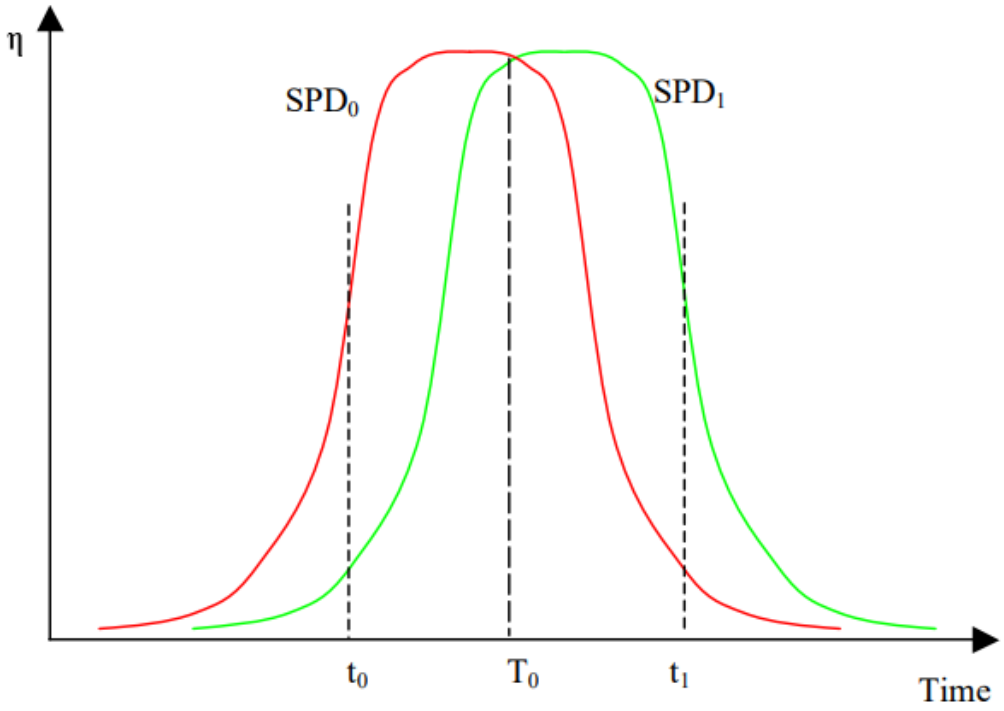
(b)

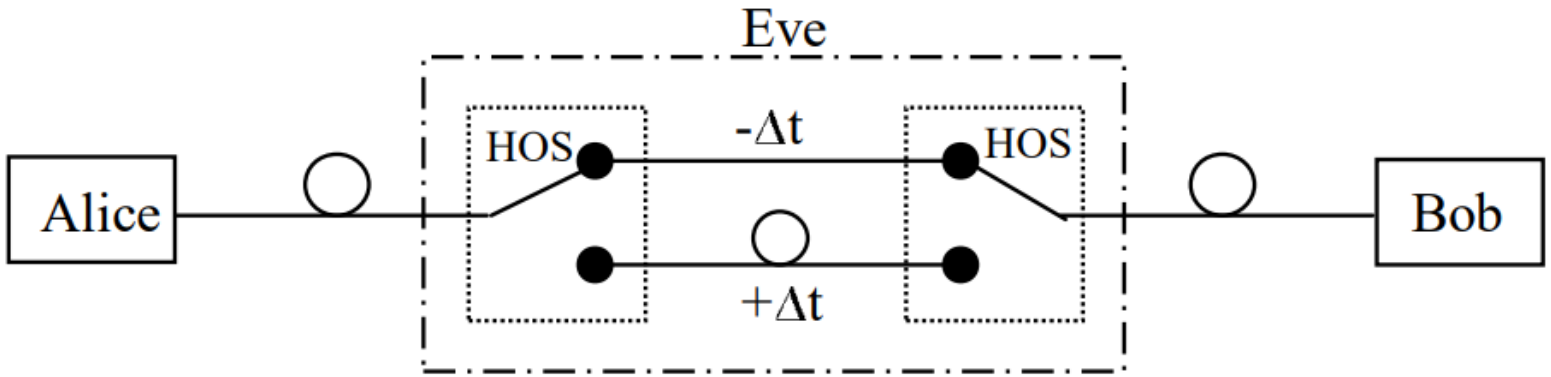


QUANTUM NETWORK (QKD NETWORK)

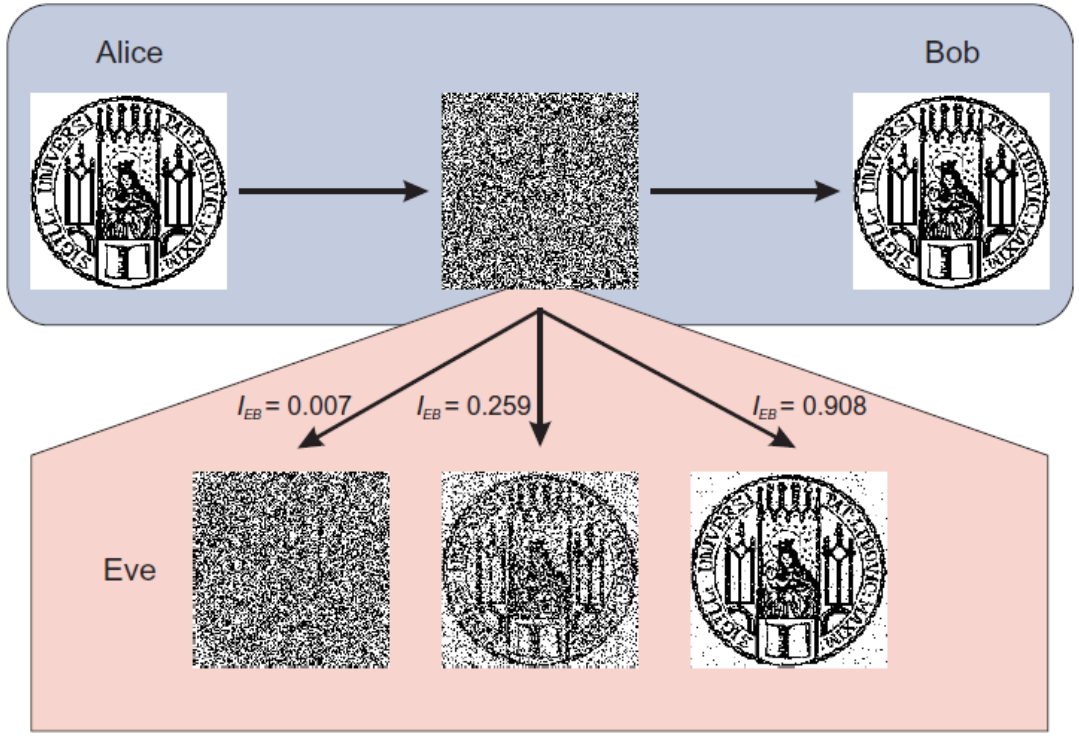


TIME-SHIFT ATTACK

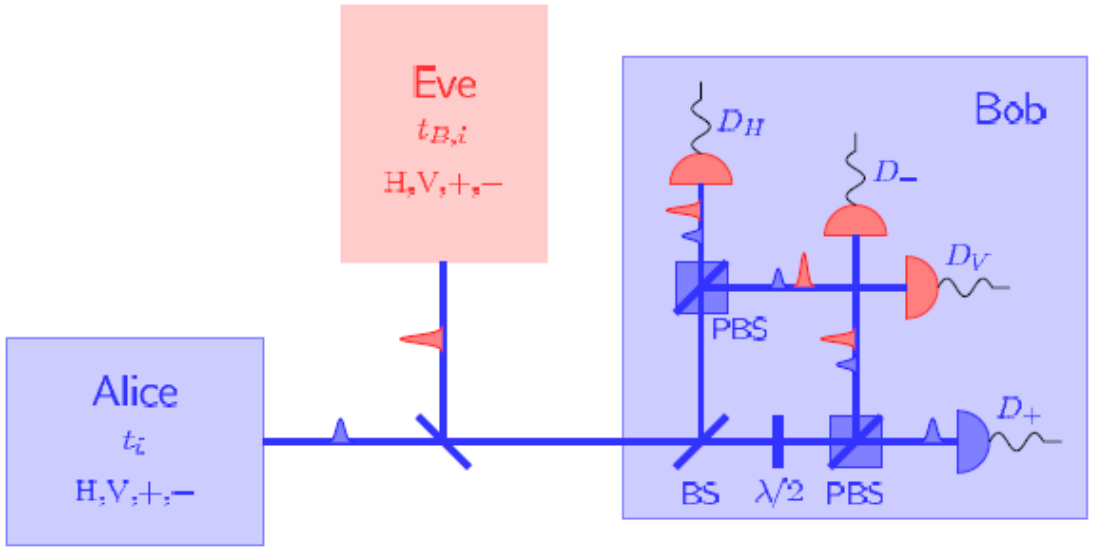




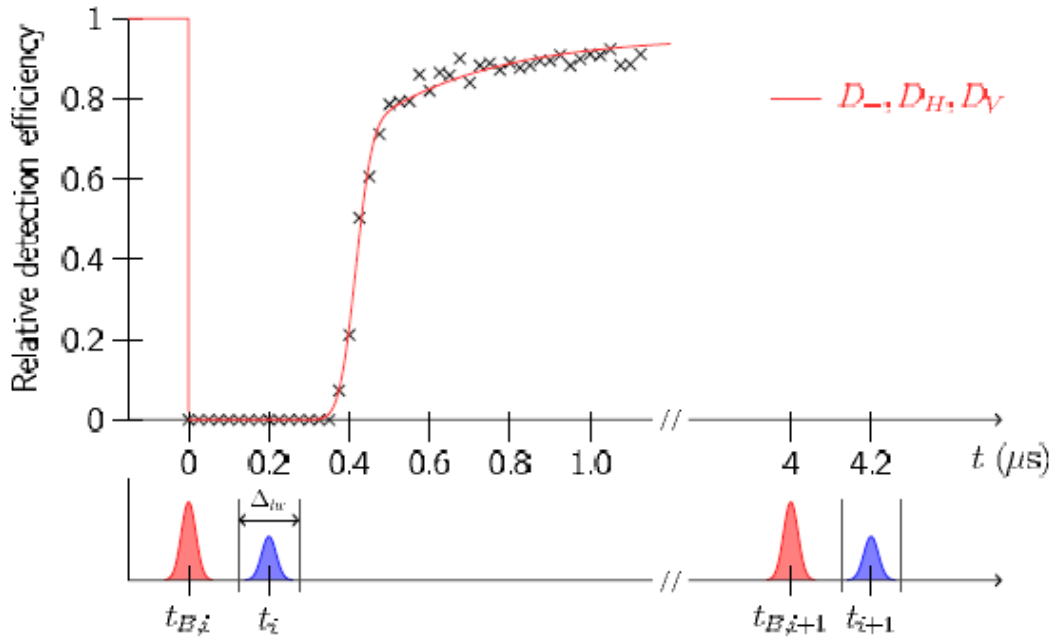
DETECTOR DEAD-TIME ATTACK



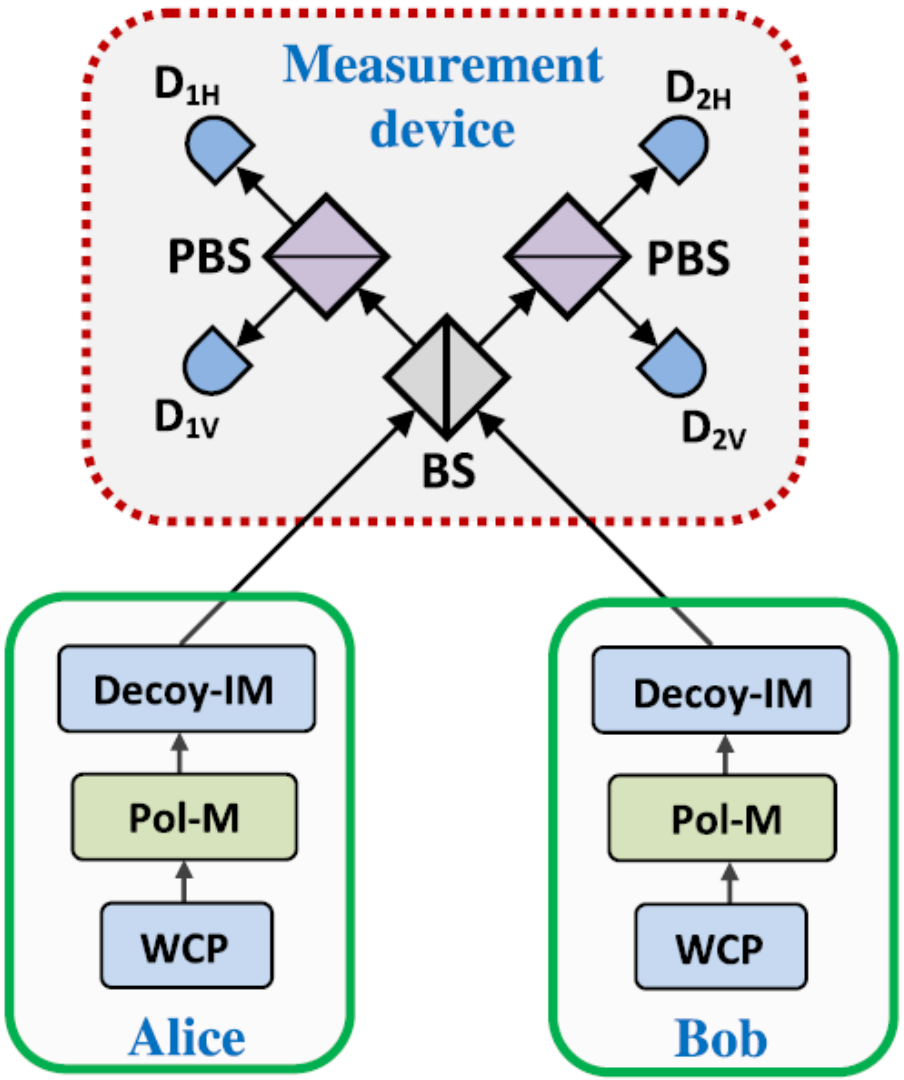
a)



b)



MEASUREMENT-DEVICE-INDEPENDENT QKD



Bell states

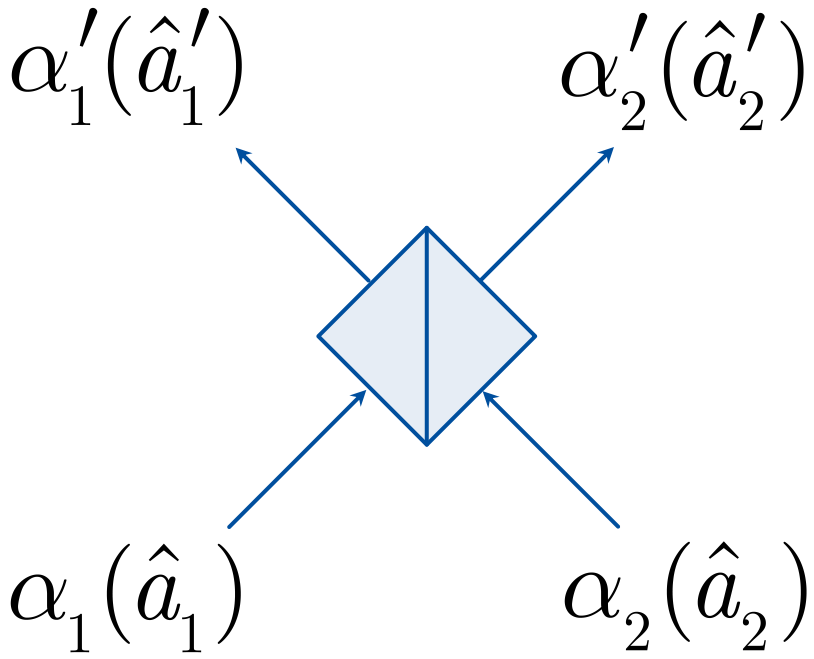
$$|\Psi^{\pm}\rangle = \frac{1}{\sqrt{2}}(|HV\rangle \pm |VH\rangle),$$

$$|\Phi^{\pm}\rangle = \frac{1}{\sqrt{2}}(|HH\rangle \pm |VV\rangle).$$

$$\{D_{1H}, D_{1V}\} \rightarrow |\Psi^{+}\rangle\,; \quad \{D_{2H}, D_{2V}\} \rightarrow |\Psi^{+}\rangle$$
$$\{D_{1H}, D_{2V}\} \rightarrow |\Psi^{-}\rangle\,; \quad \{D_{2H}, D_{1V}\} \rightarrow |\Psi^{-}\rangle$$

Alice & Bob	Relay output $\lvert\psi^{-}\rangle$	Relay output $\lvert\psi^{+}\rangle$
Rectilinear basis	Bit flip	Bit flip
Diagonal basis	Bit flip	No bit flip

BEAMSPLITTER OPTICS

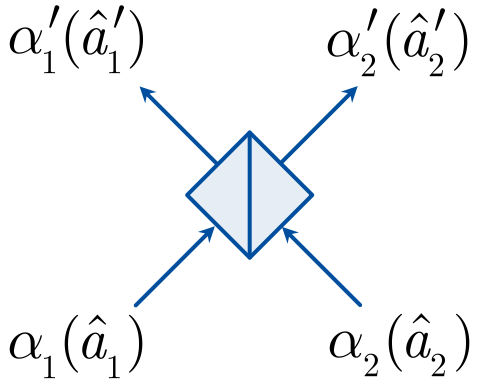


$$\begin{pmatrix} \alpha_1' \\ \alpha_2' \end{pmatrix} = B \begin{pmatrix} \alpha_1 \\ \alpha_2 \end{pmatrix}$$

$$\begin{pmatrix} \hat{a}_1' \\ \hat{a}_2' \end{pmatrix} = B \begin{pmatrix} \hat{a}_1 \\ \hat{a}_2 \end{pmatrix} \qquad \begin{pmatrix} \hat{a}_1'^{\dagger} \\ \hat{a}_2'^{\dagger} \end{pmatrix} = B^* \begin{pmatrix} \hat{a}_1^{\dagger} \\ \hat{a}_2^{\dagger} \end{pmatrix}$$

$$B = \begin{pmatrix} B_{11} & B_{12} \\ B_{21} & B_{22} \end{pmatrix} \qquad \hat{a}_i' = \sum_{j=1}^{2} B_{ij} \hat{a}_j .$$

BEAMSPLITTER OPTICS



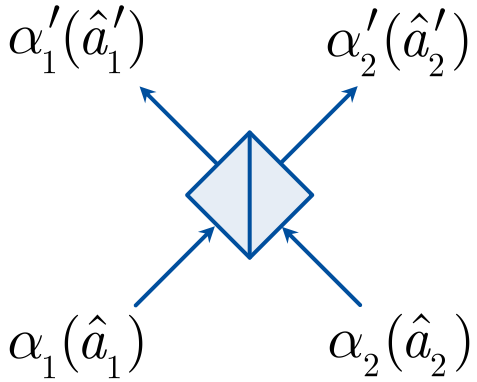
$$[\hat{a}'_\nu, \hat{a}'^\dagger_\mu] = [\hat{a}_\nu, \hat{a}^\dagger_\mu] = \delta_{\nu\mu},$$
$$[\hat{a}'_\nu, \hat{a}'_\mu] = [\hat{a}_\nu, \hat{a}_\mu] = 0.$$

$$\begin{aligned}
[\hat{a}'_1, \hat{a}'^\dagger_1] &= \hat{a}'_1\hat{a}'^\dagger_1 - \hat{a}'^\dagger_1\hat{a}'_1 = (B_{11}\hat{a}_1 + B_{12}\hat{a}_2)(B^*_{11}\hat{a}^\dagger_1 + B^*_{12}\hat{a}^\dagger_2) \\
&\quad - (B^*_{11}\hat{a}^\dagger_1 + B^*_{12}\hat{a}^\dagger_2)(B_{11}\hat{a}_1 + B_{12}\hat{a}_2) \\
&= |B_{11}|^2 \underbrace{[\hat{a}_1, \hat{a}^\dagger_1]}_{1} + |B_{12}|^2 \underbrace{[\hat{a}_2, \hat{a}^\dagger_2]}_{1} + B_{12}B^*_{11} \underbrace{[\hat{a}_2, \hat{a}^\dagger_1]}_{0} + B_{11}B^*_{12} \underbrace{[\hat{a}_1, \hat{a}^\dagger_2]}_{0} \\
&= |B_{11}|^2 + |B_{12}|^2 = 1.
\end{aligned}$$

$$|B_{11}|^2 + |B_{12}|^2 = |B_{21}|^2 + |B_{22}|^2 = 1, \quad B_{11}B^*_{21} + B_{12}B^*_{22} = 0,$$

$$B^{-1} = B^\dagger$$

BEAMSPLITTER OPTICS



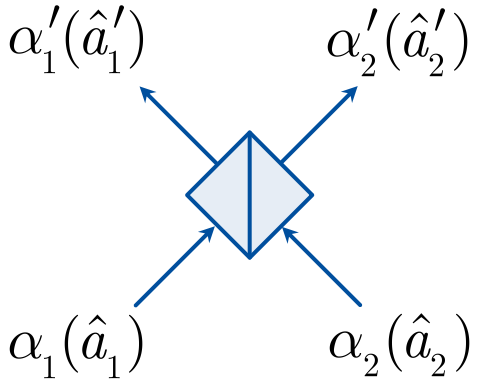
$$\hat{a}_i' = \sum_{j=1}^{2} B_{ij}\hat{a}_j$$

or

$$\hat{a}_1' = \hat{U}_B^\dagger \hat{a}_1 \hat{U}_B, \quad \hat{a}_2' = \hat{U}_B^\dagger \hat{a}_2 \hat{U}_B \quad \Rightarrow \quad |\psi\rangle' = \hat{U}_B |\psi\rangle$$

$$\hat{U}_B^\dagger \hat{a}_i \hat{U}_B = \sum_{j=1}^{2} B_{ij}\hat{a}_j \qquad \hat{U}_B \hat{a}_i^\dagger \hat{U}_B^\dagger = \sum_{j=1}^{2} B_{ji}\hat{a}_j^\dagger$$

BEAMSPLITTER OPTICS



$$\hat{a}_i' = \sum_{j=1}^{2} B_{ij}\hat{a}_j$$

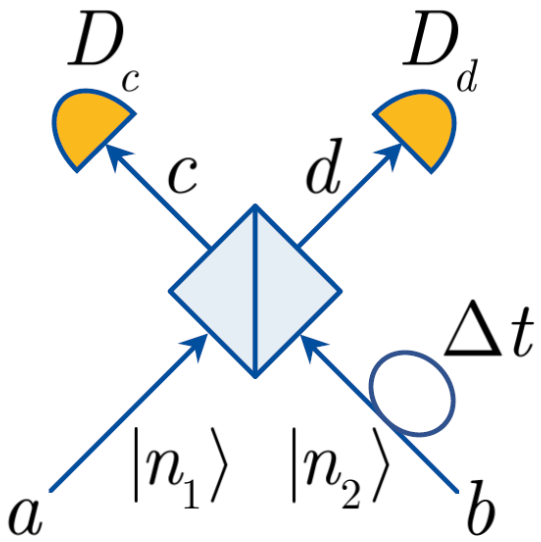
or

$$\hat{a}_1' = \hat{U}_B^\dagger \hat{a}_1 \hat{U}_B, \quad \hat{a}_2' = \hat{U}_B^\dagger \hat{a}_2 \hat{U}_B \quad \Rightarrow \quad |\psi\rangle' = \hat{U}_B |\psi\rangle$$

$$\hat{U}_B^\dagger \hat{a}_i \hat{U}_B = \sum_{j=1}^{2} B_{ij}\hat{a}_j \qquad \hat{U}_B \hat{a}_i^\dagger \hat{U}_B^\dagger = \sum_{j=1}^{2} B_{ji}\hat{a}_j^\dagger$$

BEAMSPLITTER OPTICS

$$|n_1, n_2\rangle = \frac{1}{\sqrt{n_1! n_2!}} \hat{a}^{\dagger n_1} \hat{b}^{\dagger n_2} |0, 0\rangle$$



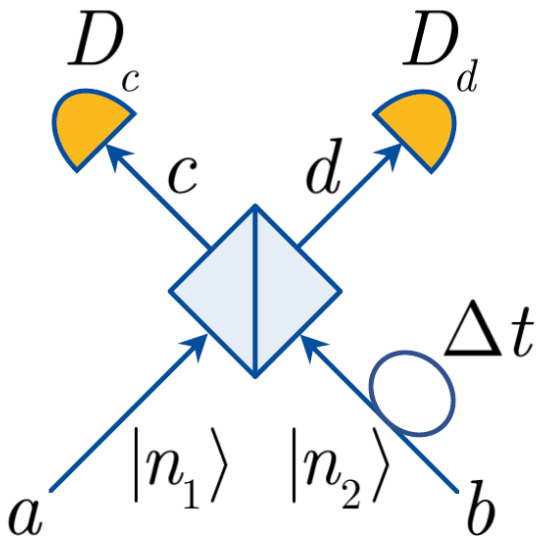
$$|n_1, n_2\rangle' = \hat{U}_B |n_1, n_2\rangle = \frac{1}{\sqrt{n_1! n_2!}} \hat{U}_B \hat{a}^{\dagger n_1} \underbrace{\hat{U}_B^\dagger \hat{U}_B}_{\hat{\mathbb{1}}} \hat{b}^{\dagger n_2} \underbrace{\hat{U}_B^\dagger |0, 0\rangle}_{|0,0\rangle}$$

$$= \frac{1}{\sqrt{n_1! n_2!}} \left(B_{11} \hat{a}^\dagger + B_{21} \hat{b}^\dagger \right)^{n_1} \left(B_{12} \hat{a}^\dagger + B_{22} \hat{b}^\dagger \right)^{n_2} |0, 0\rangle$$

BEAMSPLITTER OPTICS

$$(a+b)^n = \sum_{k=0}^{n} C_n^k a^{n-k} b^k,$$

$$C_n^k = \frac{n!}{k!(n-k)!},$$

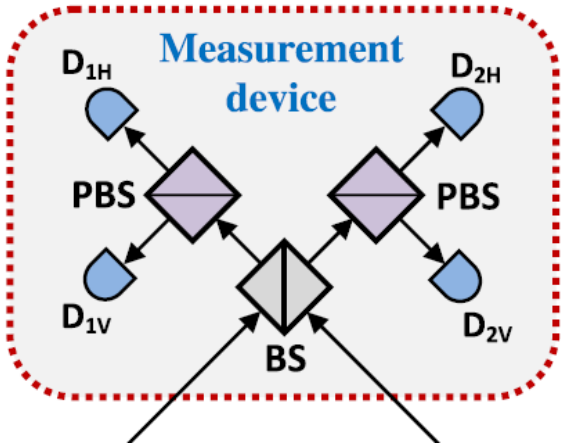


$$|n_1, n_2\rangle' = \frac{1}{\sqrt{n_1! n_2!}} \sum_{k_1,k_2=0}^{n_1,n_2} C_{n_1}^{k_1} C_{n_2}^{k_2} (B_{11})^{k_1} (B_{21})^{n_1-k_1}$$
$$\times (B_{12})^{k_2} (B_{22})^{n_2-k_2} \sqrt{(k_1+k_2)!(n_1+n_2-k_1-k_2)!}$$
$$\times |k_1+k_2, n_1+n_2-k_1-k_2\rangle .$$

Hong-Ou-Mandel effect $\quad |1,1\rangle' = \frac{1}{\sqrt{2}} (|0,2\rangle - |2,0\rangle)$

MDI QKD. Polarization encoding. Single photons

$$|\Psi^{\pm}\rangle = \frac{1}{\sqrt{2}}(|HV\rangle \pm |VH\rangle),$$
$$|\Phi^{\pm}\rangle = \frac{1}{\sqrt{2}}(|HH\rangle \pm |VV\rangle).$$



Alice 1 **Alice 2**

$$|H\rangle, |V\rangle, |D\rangle, |A\rangle$$

$$|D\rangle = \frac{1}{\sqrt{2}}(|H\rangle + |V\rangle)$$
$$|A\rangle = \frac{1}{\sqrt{2}}(|H\rangle - |V\rangle)$$

Let us calculate probabilities for states

$$|HH\rangle, |VV\rangle, |HV\rangle, |VH\rangle, |AA\rangle, |DD\rangle, |AD\rangle, |DA\rangle$$

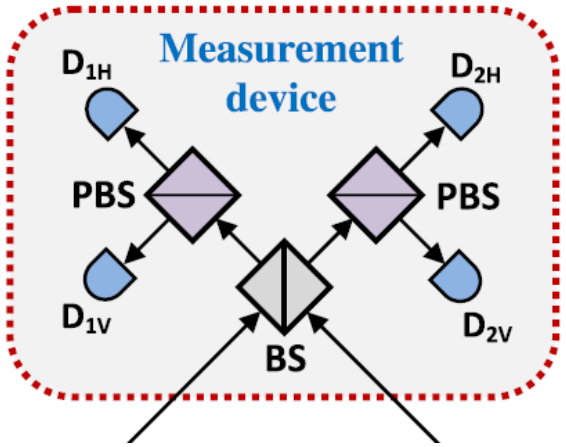
to be projected onto Bell states $|\Psi^{\pm}\rangle$, $|\Phi^{\pm}\rangle$:

$$\left|\langle\Psi^{-}|HH\rangle\right|^2 = \frac{1}{2}\left|\langle HV|HH\rangle - \langle VH|HH\rangle\right|^2 = 0$$

$$\left|\langle\Psi^{\pm}|HH\rangle\right|^2 = \left|\langle\Psi^{\pm}|VV\rangle\right|^2 = 0,$$
$$\left|\langle\Phi^{\pm}|HV\rangle\right|^2 = \left|\langle\Phi^{\pm}|VH\rangle\right|^2 = 0.$$

MDI QKD. Polarization encoding. Single photons

$$|\Psi^{\pm}\rangle = \frac{1}{\sqrt{2}}(|HV\rangle \pm |VH\rangle),$$
$$|\Phi^{\pm}\rangle = \frac{1}{\sqrt{2}}(|HH\rangle \pm |VV\rangle).$$



Alice 1 **Alice 2**

$$|H\rangle, |V\rangle, |D\rangle, |A\rangle$$

$$|D\rangle = \frac{1}{\sqrt{2}}(|H\rangle + |V\rangle)$$
$$|A\rangle = \frac{1}{\sqrt{2}}(|H\rangle - |V\rangle)$$

Let us calculate probabilities for states

$$|HH\rangle, |VV\rangle, |HV\rangle, |VH\rangle, |AA\rangle, |DD\rangle, |AD\rangle, |DA\rangle$$

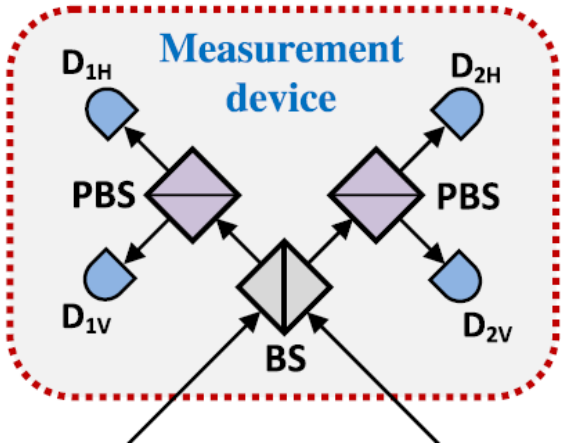
to be projected onto Bell states $|\Psi^{\pm}\rangle$, $|\Phi^{\pm}\rangle$:

$$\left|\langle\Psi^{-}|HV\rangle\right|^2 = \frac{1}{2}\left|\langle HV|HV\rangle - \langle VH|HV\rangle\right|^2 = \frac{1}{2}$$

$$\left|\langle\Psi^{\pm}|HV\rangle\right|^2 = \left|\langle\Psi^{\pm}|VH\rangle\right|^2 = 1/2,$$
$$\left|\langle\Phi^{\pm}|HH\rangle\right|^2 = \left|\langle\Phi^{\pm}|VV\rangle\right|^2 = 1/2.$$

MDI QKD. Polarization encoding. Single photons

$$|\Psi^{\pm}\rangle = \frac{1}{\sqrt{2}}(|HV\rangle \pm |VH\rangle),$$
$$|\Phi^{\pm}\rangle = \frac{1}{\sqrt{2}}(|HH\rangle \pm |VV\rangle).$$



$$|H\rangle, |V\rangle, |D\rangle, |A\rangle$$

$$|D\rangle = \frac{1}{\sqrt{2}}(|H\rangle + |V\rangle)$$

$$|A\rangle = \frac{1}{\sqrt{2}}(|H\rangle - |V\rangle)$$

Let us calculate probabilities for states

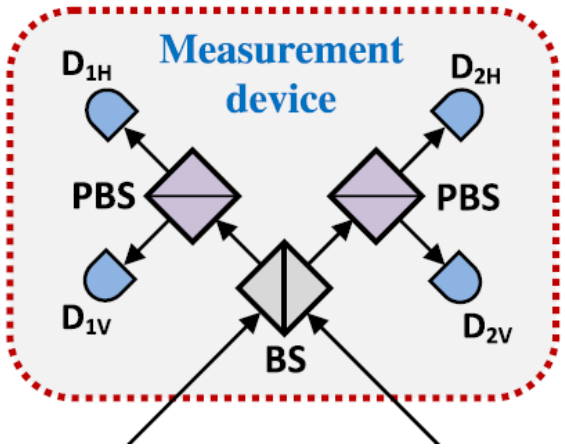
$$|HH\rangle, |VV\rangle, |HV\rangle, |VH\rangle, |AA\rangle, |DD\rangle, |AD\rangle, |DA\rangle$$

to be projected onto Bell states $|\Psi^{\pm}\rangle$, $|\Phi^{\pm}\rangle$:

$$|AA\rangle = \frac{1}{\sqrt{2}}(|H\rangle - |V\rangle) \otimes \frac{1}{\sqrt{2}}(|H\rangle - |V\rangle)$$
$$= \frac{1}{2}(|HH\rangle - |HV\rangle - |VH\rangle + |VV\rangle)$$
$$= \frac{1}{\sqrt{2}}(|\Phi^{+}\rangle - |\Psi^{+}\rangle).$$

$$\langle\Phi^{+}|AA\rangle = \frac{1}{\sqrt{2}}(\langle\Phi^{+}|\Phi^{+}\rangle - \langle\Phi^{+}|\Psi^{+}\rangle) = \frac{1}{\sqrt{2}},$$

MDI QKD. Polarization encoding. Single photons



$$|H\rangle, |V\rangle, |D\rangle, |A\rangle$$

$$|D\rangle = \frac{1}{\sqrt{2}}(|H\rangle + |V\rangle)$$

$$|A\rangle = \frac{1}{\sqrt{2}}(|H\rangle - |V\rangle)$$

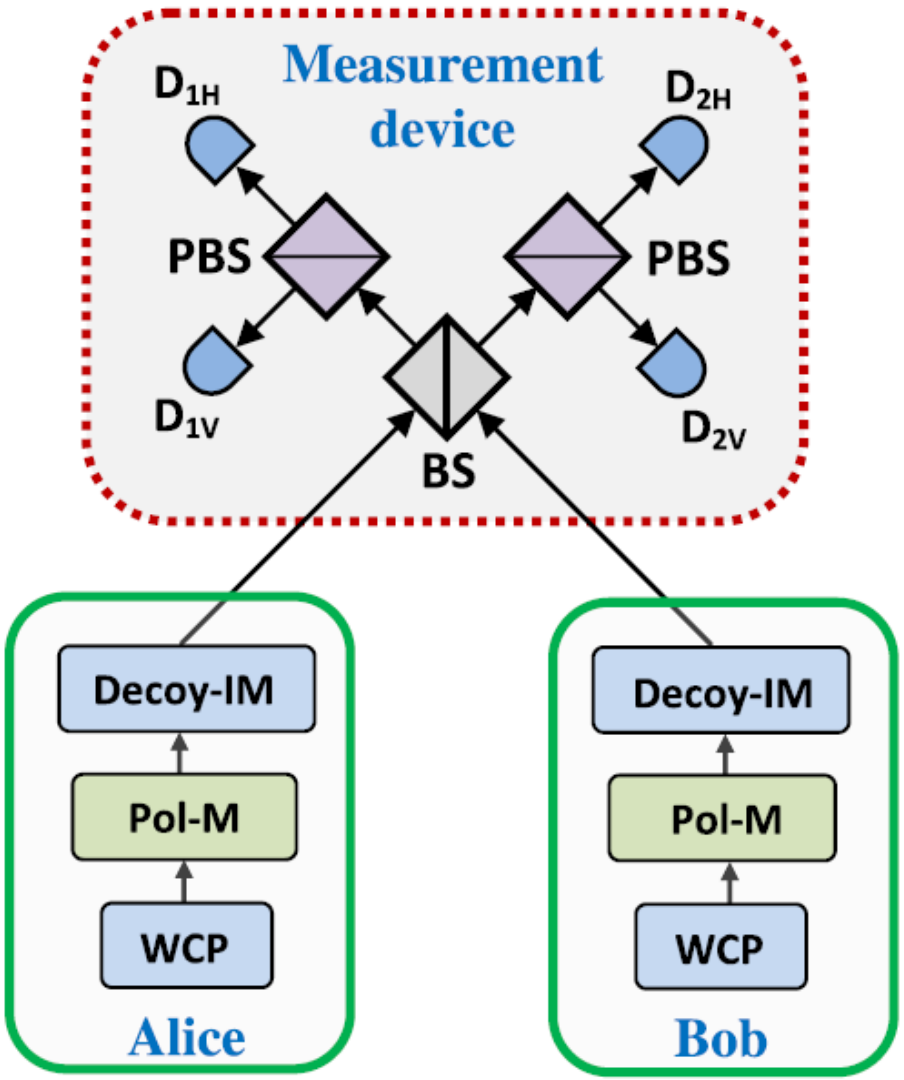
Let us calculate probabilities for states

$$|HH\rangle, |VV\rangle, |HV\rangle, |VH\rangle, |AA\rangle, |DD\rangle, |AD\rangle, |DA\rangle$$

to be projected onto Bell states $|\Psi^{\pm}\rangle$, $|\Phi^{\pm}\rangle$:

	$\|HH\rangle$	$\|VV\rangle$	$\|HV\rangle$	$\|VH\rangle$	$\|AA\rangle$	$\|DD\rangle$	$\|AD\rangle$	$\|DA\rangle$
$\langle\Psi^-\|$	0	0	1/2	1/2	0	0	1/2	1/2
$\langle\Psi^+\|$	0	0	1/2	1/2	1/2	1/2	0	0
$\langle\Phi^-\|$	1/2	1/2	0	0	0	0	1/2	1/2
$\langle\Phi^+\|$	1/2	1/2	0	0	1/2	1/2	0	0

MEASUREMENT-DEVICE-INDEPENDENT QKD



Bell states

$$|\Psi^{\pm}\rangle = \frac{1}{\sqrt{2}}(|HV\rangle \pm |VH\rangle),$$

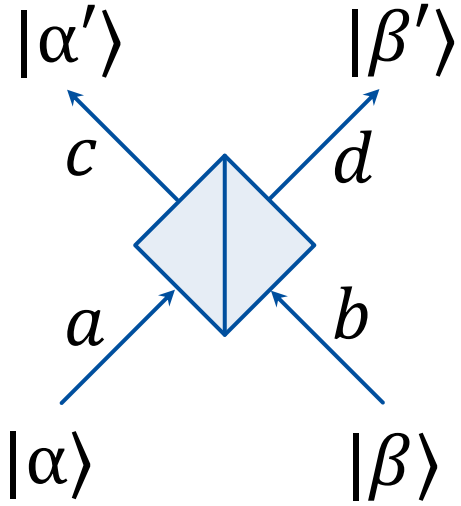
$$|\Phi^{\pm}\rangle = \frac{1}{\sqrt{2}}(|HH\rangle \pm |VV\rangle).$$

$$\{D_{1H}, D_{1V}\} \rightarrow |\Psi^{+}\rangle\,; \quad \{D_{2H}, D_{2V}\} \rightarrow |\Psi^{+}\rangle$$
$$\{D_{1H}, D_{2V}\} \rightarrow |\Psi^{-}\rangle\,; \quad \{D_{2H}, D_{1V}\} \rightarrow |\Psi^{-}\rangle$$

Alice & Bob	Relay output $\|\psi^{-}\rangle$	Relay output $\|\psi^{+}\rangle$
Rectilinear basis	Bit flip	Bit flip
Diagonal basis	Bit flip	No bit flip

INTERFERENCE OF COHERENT STATES

$$|\alpha\rangle = e^{-\frac{|\alpha|^2}{2}} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}} |n\rangle$$ – coherent state



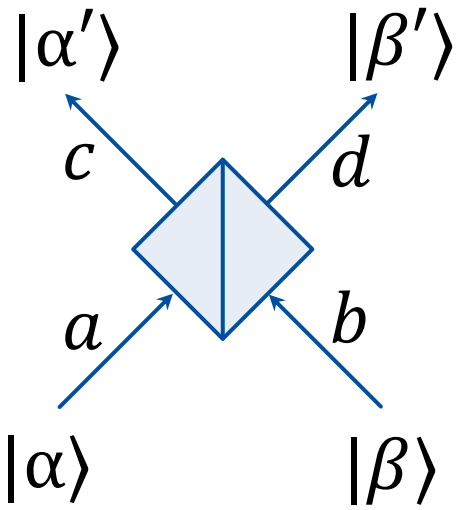
$$|\alpha\rangle = e^{\alpha\hat{a}^\dagger - \alpha^*\hat{a}} |0\rangle = e^{-|\alpha|^2/2} e^{-\alpha^*\hat{a}} e^{\alpha\hat{a}^\dagger} |0\rangle \equiv \hat{D}(\alpha) |0\rangle ,$$

$$|\beta\rangle = e^{\beta\hat{b}^\dagger - \beta^*\hat{b}} |0\rangle = e^{-|\beta|^2/2} e^{-\beta^*\hat{b}} e^{\beta\hat{b}^\dagger} |0\rangle \equiv \hat{D}(\beta) |0\rangle ,$$

$$\hat{D}_b(\beta)\hat{D}_a(\alpha) |0,0\rangle_{ab}$$

After BS: $$\hat{a} = \frac{\hat{c} + \hat{d}}{\sqrt{2}}, \quad \hat{a}^\dagger = \frac{\hat{c}^\dagger + \hat{d}^\dagger}{\sqrt{2}}, \quad \hat{b} = \frac{\hat{c} - \hat{d}}{\sqrt{2}}, \quad \hat{b}^\dagger = \frac{\hat{c}^\dagger - \hat{d}^\dagger}{\sqrt{2}},$$

INTERFERENCE OF COHERENT STATES



$$\hat{a} = \frac{\hat{c} + \hat{d}}{\sqrt{2}}, \quad \hat{a}^\dagger = \frac{\hat{c}^\dagger + \hat{d}^\dagger}{\sqrt{2}}, \quad \hat{b} = \frac{\hat{c} - \hat{d}}{\sqrt{2}}, \quad \hat{b}^\dagger = \frac{\hat{c}^\dagger - \hat{d}^\dagger}{\sqrt{2}},$$

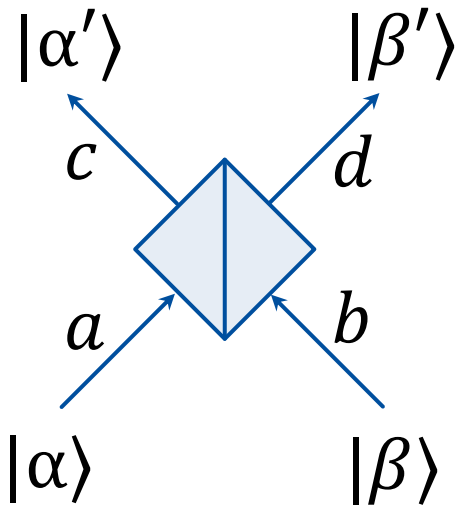
$$\hat{D}_b(\beta)\hat{D}_a(\alpha)\,|0,0\rangle_{ab} \xrightarrow{\text{BS}} e^{\hat{A}}e^{\hat{B}}\,|0,0\rangle_{cd}\,,$$

$$\hat{A} = \beta\frac{\hat{c}^\dagger - \hat{d}^\dagger}{\sqrt{2}} - \beta^*\frac{\hat{c} - \hat{d}}{\sqrt{2}},$$

$$\hat{B} = \alpha\frac{\hat{c}^\dagger + \hat{d}^\dagger}{\sqrt{2}} - \alpha^*\frac{\hat{c} + \hat{d}}{\sqrt{2}}.$$

INTERFERENCE OF COHERENT STATES

$$\hat{D}_b(\beta)\hat{D}_a(\alpha)\,|0,0\rangle_{ab} \xrightarrow{\text{BS}} e^{\hat{A}}e^{\hat{B}}\,|0,0\rangle_{cd}\,,$$



$$\hat{A} = \beta\frac{\hat{c}^\dagger - \hat{d}^\dagger}{\sqrt{2}} - \beta^*\frac{\hat{c} - \hat{d}}{\sqrt{2}},$$

$$\hat{B} = \alpha\frac{\hat{c}^\dagger + \hat{d}^\dagger}{\sqrt{2}} - \alpha^*\frac{\hat{c} + \hat{d}}{\sqrt{2}}.$$

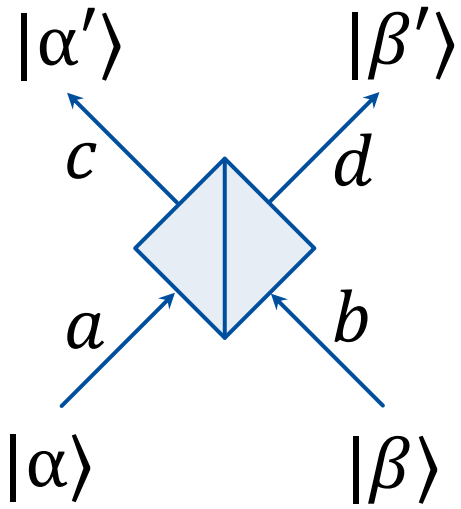
$$[\hat{c}^\dagger, \hat{d}^\dagger] = [\hat{c}, \hat{d}] = [\hat{c}^\dagger, \hat{d}] = [\hat{c}, \hat{d}^\dagger] = 0$$

$$[\hat{c}^\dagger, \hat{c}] = [\hat{d}^\dagger, \hat{d}] = -1$$

$$\Rightarrow \quad [\hat{A}, \hat{B}] = 0$$

Baker-Housdorff formula: $e^{\hat{A}}e^{\hat{B}} = e^{[\hat{A},\hat{B}]/2}e^{\hat{A}+\hat{B}} = e^{\hat{A}+\hat{B}}$

INTERFERENCE OF COHERENT STATES



$$\hat{A} + \hat{B} = \hat{C} + \hat{D}$$

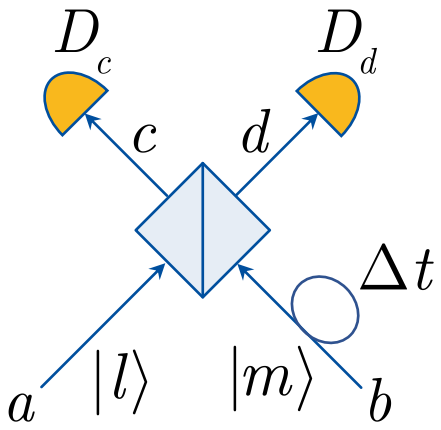
$$\hat{C} = \frac{\alpha + \beta}{\sqrt{2}}\hat{c}^\dagger - \frac{\alpha^* + \beta^*}{\sqrt{2}}\hat{c},$$

$$\hat{D} = \frac{\alpha - \beta}{\sqrt{2}}\hat{d}^\dagger - \frac{\alpha^* - \beta^*}{\sqrt{2}}\hat{d},$$

$$\hat{D}_b(\beta)\hat{D}_a(\alpha)\,|0,0\rangle_{ab} \xrightarrow{\text{BS}} e^{\hat{C}}e^{\hat{D}}\,|0,0\rangle_{cd} = \hat{D}_c\underbrace{\left(\frac{\alpha+\beta}{\sqrt{2}}\right)}_{|\alpha'\rangle}\hat{D}_d\underbrace{\left(\frac{\alpha-\beta}{\sqrt{2}}\right)}_{|\beta'\rangle}|0,0\rangle_{cd}$$

INTERFERENCE OF COHERENT STATES

$$|\alpha\rangle = e^{-\frac{|\alpha|^2}{2}} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}} |n\rangle$$



Probabilities of detector's events

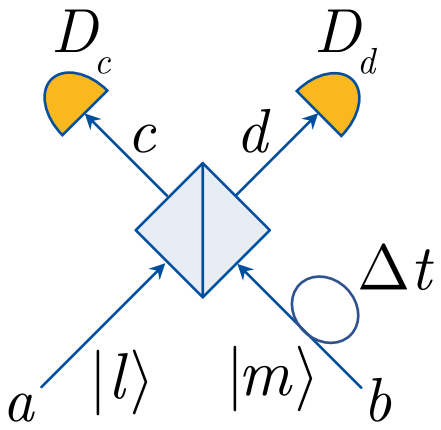
$$P_{lm}(0,0) = (1-\eta_c)^l (1-\eta_d)^m,$$
$$P_{lm}(1,0) = (1-(1-\eta_c)^l)(1-\eta_d)^m,$$
$$P_{lm}(0,1) = (1-\eta_c)^l (1-(1-\eta_d)^m),$$
$$P_{lm}(1,1) = (1-(1-\eta_c)^n)(1-(1-\eta_d)^m),$$

$\Delta t = 0$:

$$P_n = \exp\left(-\frac{|\alpha+\beta|^2}{2}\right) \exp\left(-\frac{|\alpha-\beta|^2}{2}\right)$$
$$\times \sum_{l=0}^{\infty}\sum_{m=0}^{\infty} \frac{P_{lm}(1,1)}{l!m!} \left(\frac{|\alpha+\beta|^2}{2}\right)^l \left(\frac{|\alpha-\beta|^2}{2}\right)^m$$
$$= \left[1-\exp\left(-\frac{|\alpha+\beta|^2}{2}\eta_c\right)\right] \times \left[1-\exp\left(-\frac{|\alpha-\beta|^2}{2}\eta_d\right)\right]$$

INTERFERENCE OF COHERENT STATES

$$|\alpha\rangle = e^{-\frac{|\alpha|^2}{2}} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}} |n\rangle$$



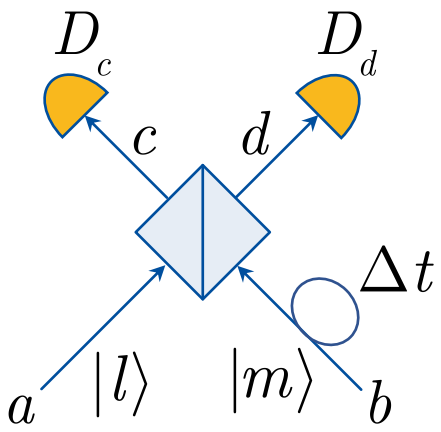
Probabilities of detector's events

$$P_{lm}(0,0) = (1-\eta_c)^l (1-\eta_d)^m,$$
$$P_{lm}(1,0) = (1-(1-\eta_c)^l)(1-\eta_d)^m,$$
$$P_{lm}(0,1) = (1-\eta_c)^l (1-(1-\eta_d)^m),$$
$$P_{lm}(1,1) = (1-(1-\eta_c)^n)(1-(1-\eta_d)^m),$$

$\Delta t >> w$:

$$P_N = \left[1 - \exp\left(-\frac{|\alpha|^2 + |\beta|^2}{2}\eta_c\right)\right] \times \left[1 - \exp\left(-\frac{|\alpha|^2 + |\beta|^2}{2}\eta_d\right)\right]$$

INTERFERENCE OF COHERENT STATES



Assume $|\beta\rangle = |\alpha\rangle e^{i\theta}$

$$P_n = \left(1 - e^{-|\alpha|^2(1+\cos\theta)\eta_c}\right)\left(1 - e^{-|\alpha|^2(1-\cos\theta)\eta_d}\right)$$

$$P_N = \left(1 - e^{-|\alpha|^2\eta_c}\right)\left(1 - e^{-|\alpha|^2\eta_d}\right).$$

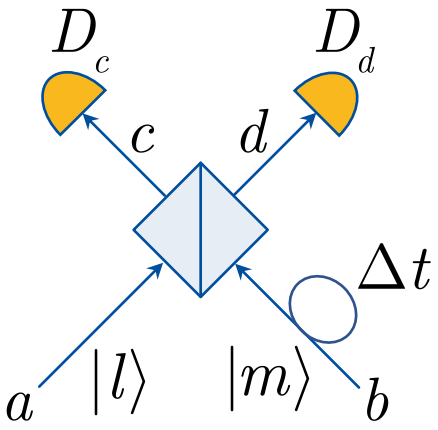
$$n = \frac{1}{2\pi}\int_0^{2\pi}\left(1 - e^{-|\alpha|^2(1+\cos\theta)\eta_c}\right)\left(1 - e^{-|\alpha|^2(1-\cos\theta)\eta_d}\right)d\theta$$

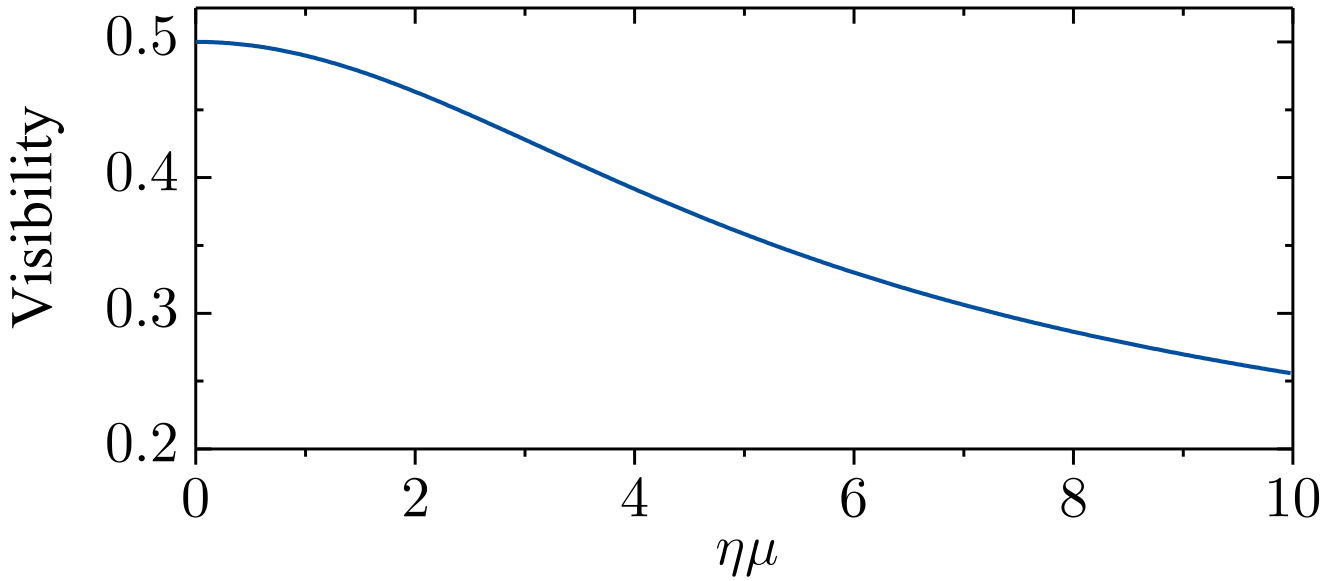
$$= 1 - e^{-\mu\eta_c}I_0[\mu\eta_c] - e^{-\mu\eta_d}I_0[\mu\eta_d] + e^{-\mu(\eta_c+\eta_d)}J_0[\mu(\eta_c - \eta_d)],$$

$$N = \left(1 - e^{-|\alpha|^2\eta_c}\right)\left(1 - e^{-|\alpha|^2\eta_d}\right)$$

VISIBILITY

$$V = \frac{N - n}{N} = \frac{I_0(\mu\eta) - 1}{\cosh(\mu\eta) - 1}$$





$$QBER = \frac{1 - V}{2} = 25\%$$

СЕТЬ ТОПОЛОГИИ ЗВЕЗДА