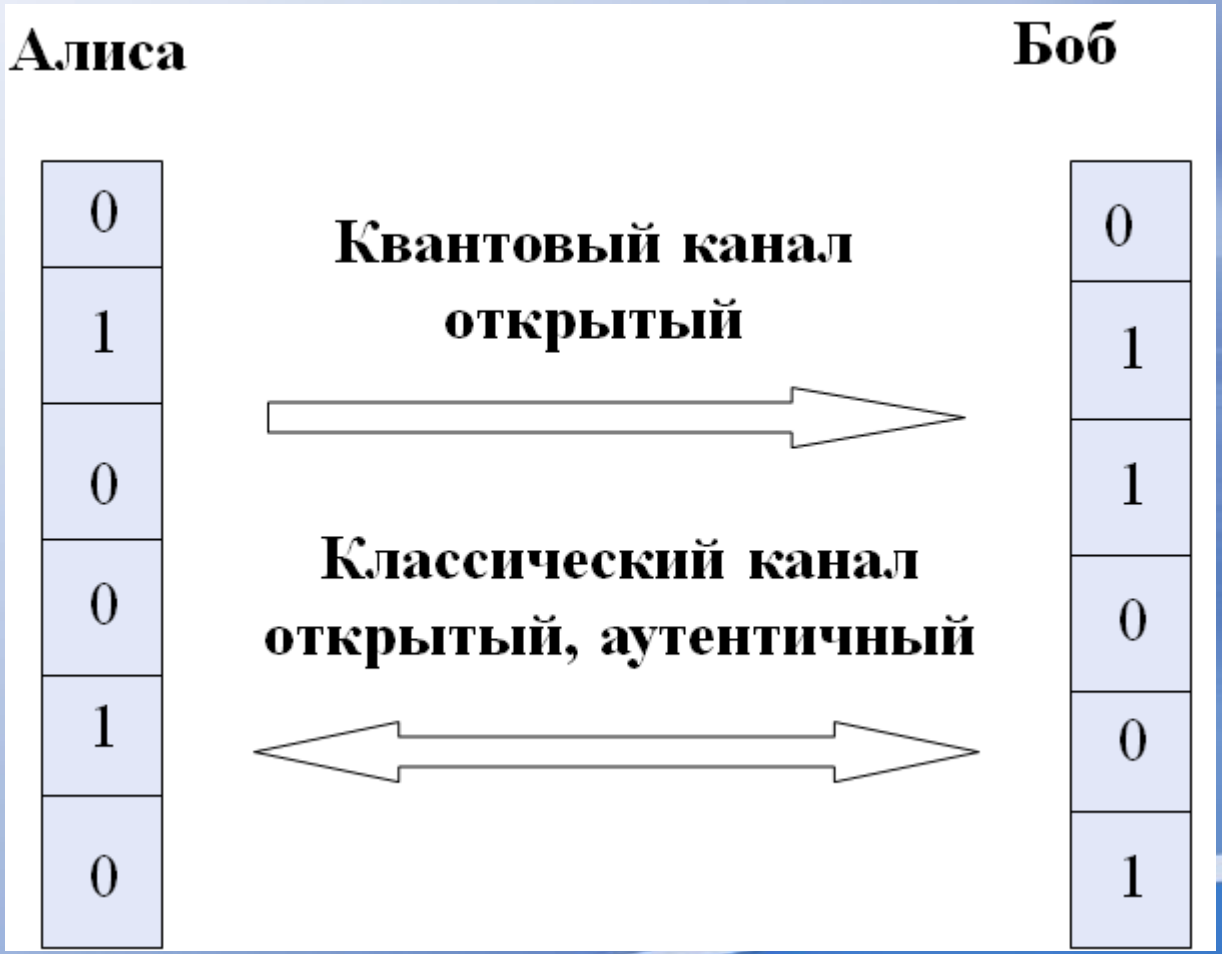
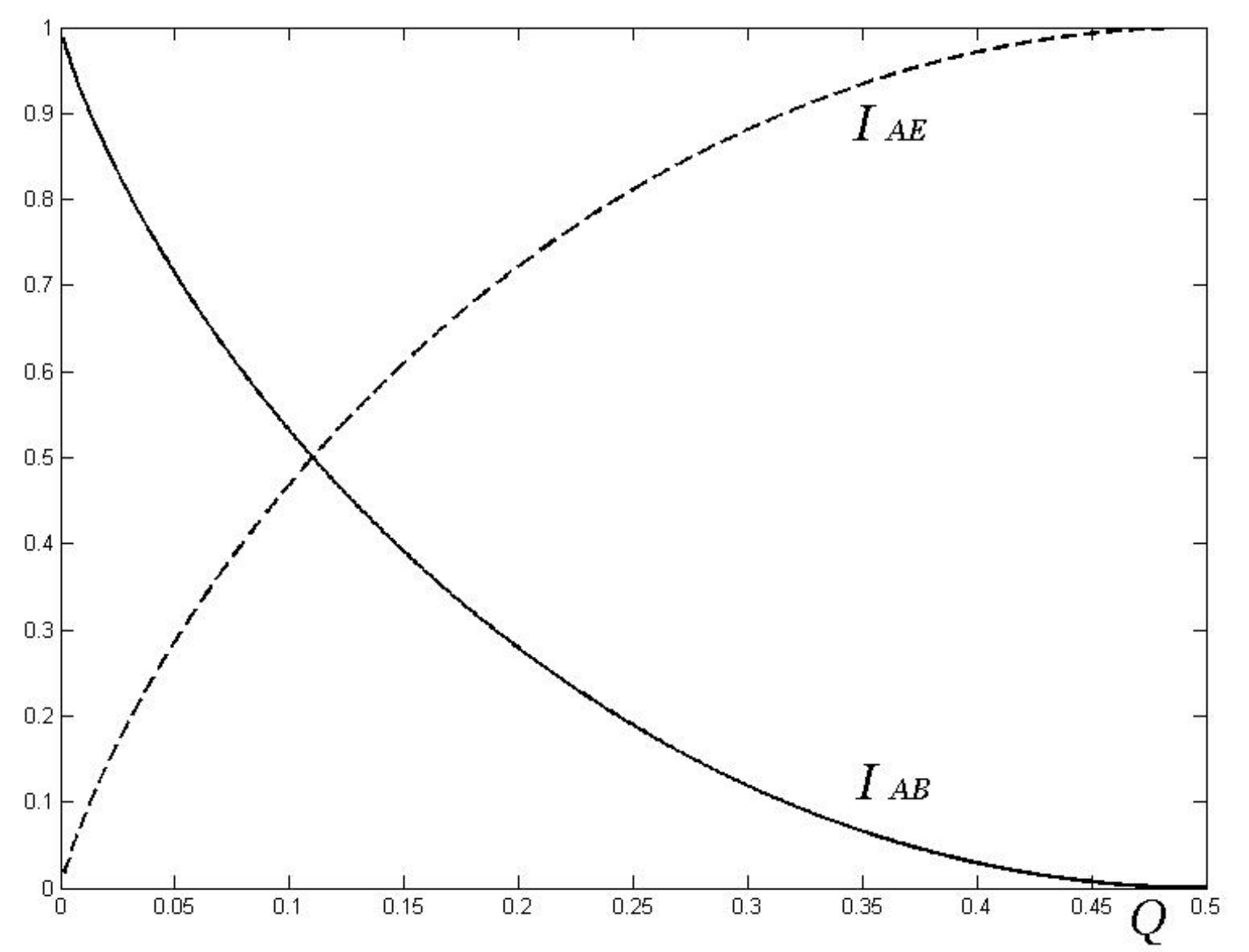
# Квантовое распределение ключей через недоверенные узлы

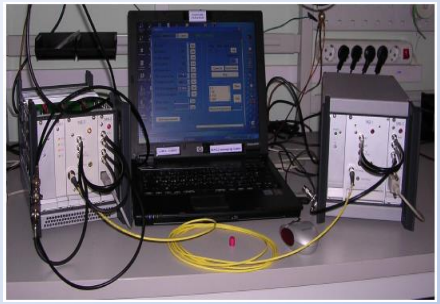
*С.Н.Молотков*

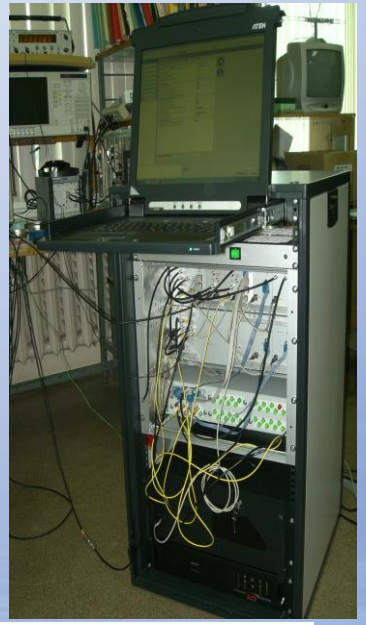
# Квантовая криптография = Квантовое распределение ключей = Согласование случайных последовательностей




1
0.9
0.8
0.7
0.6
0.5
0.4
0.3
0.2
0.1
0
0
0.05
0.1
0.15
0.2
0.25
0.3
0.35
0.4
0.45
0.5
Q
I AE
I AB

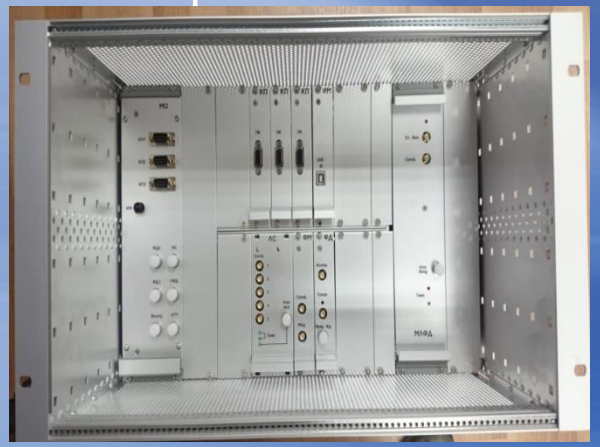
# Лаборатория волоконной квантовой криптографии

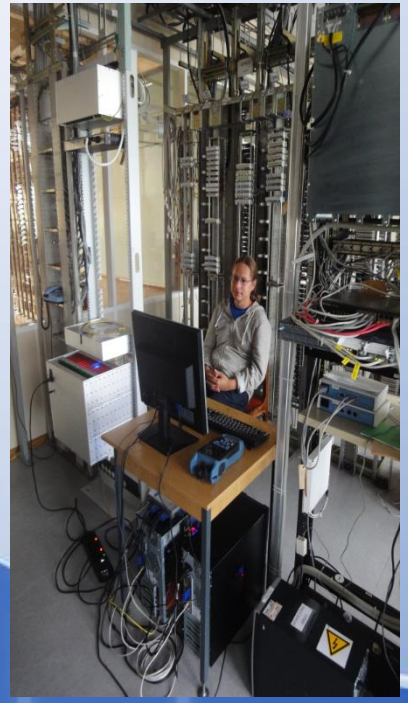


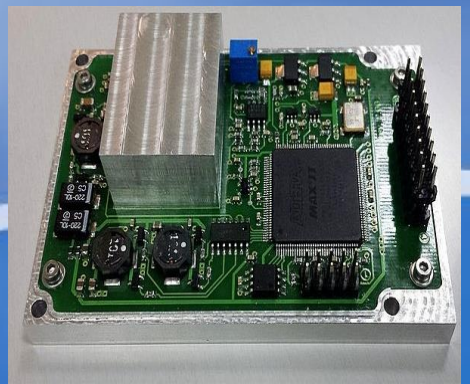


## Направления исследований:

- Волоконные ККС
- Атмосферные ККС
- Квантовые QNRNG
- Тестирование ККС







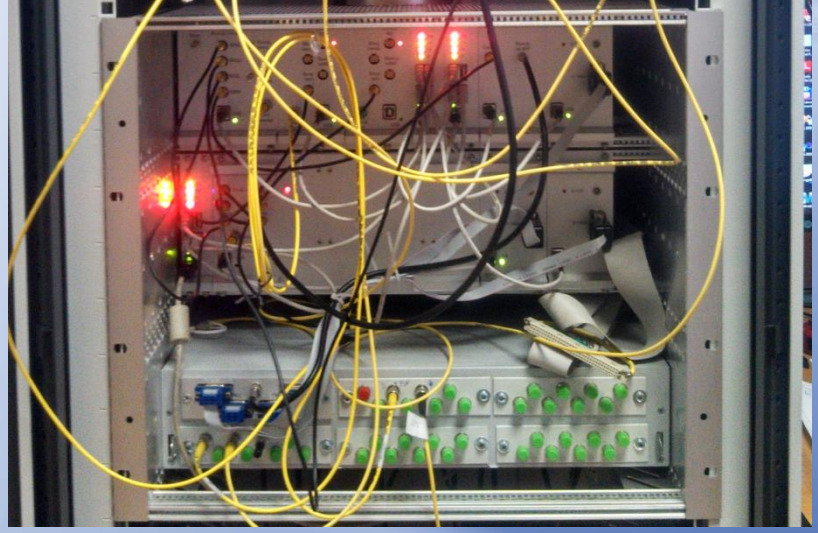
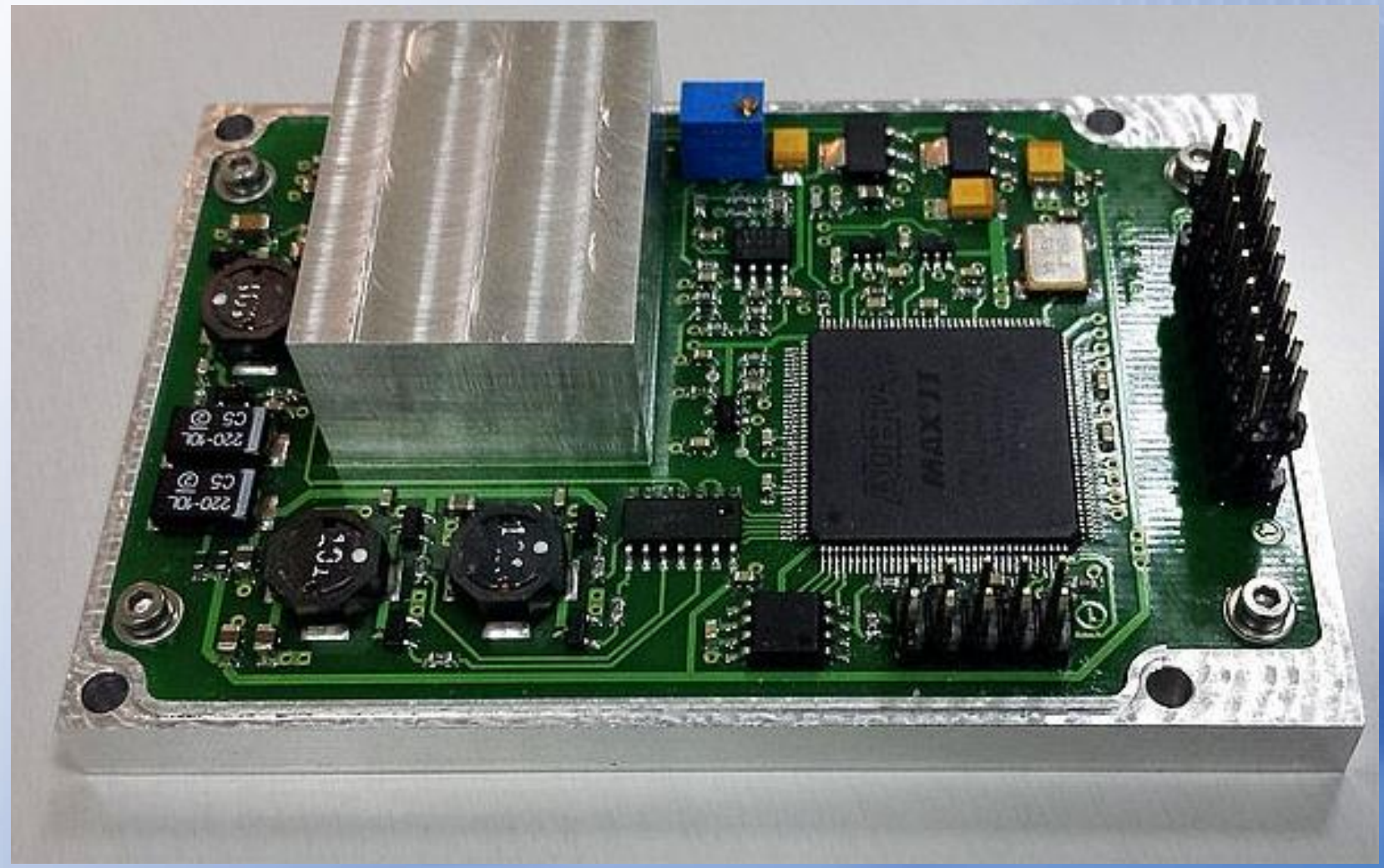
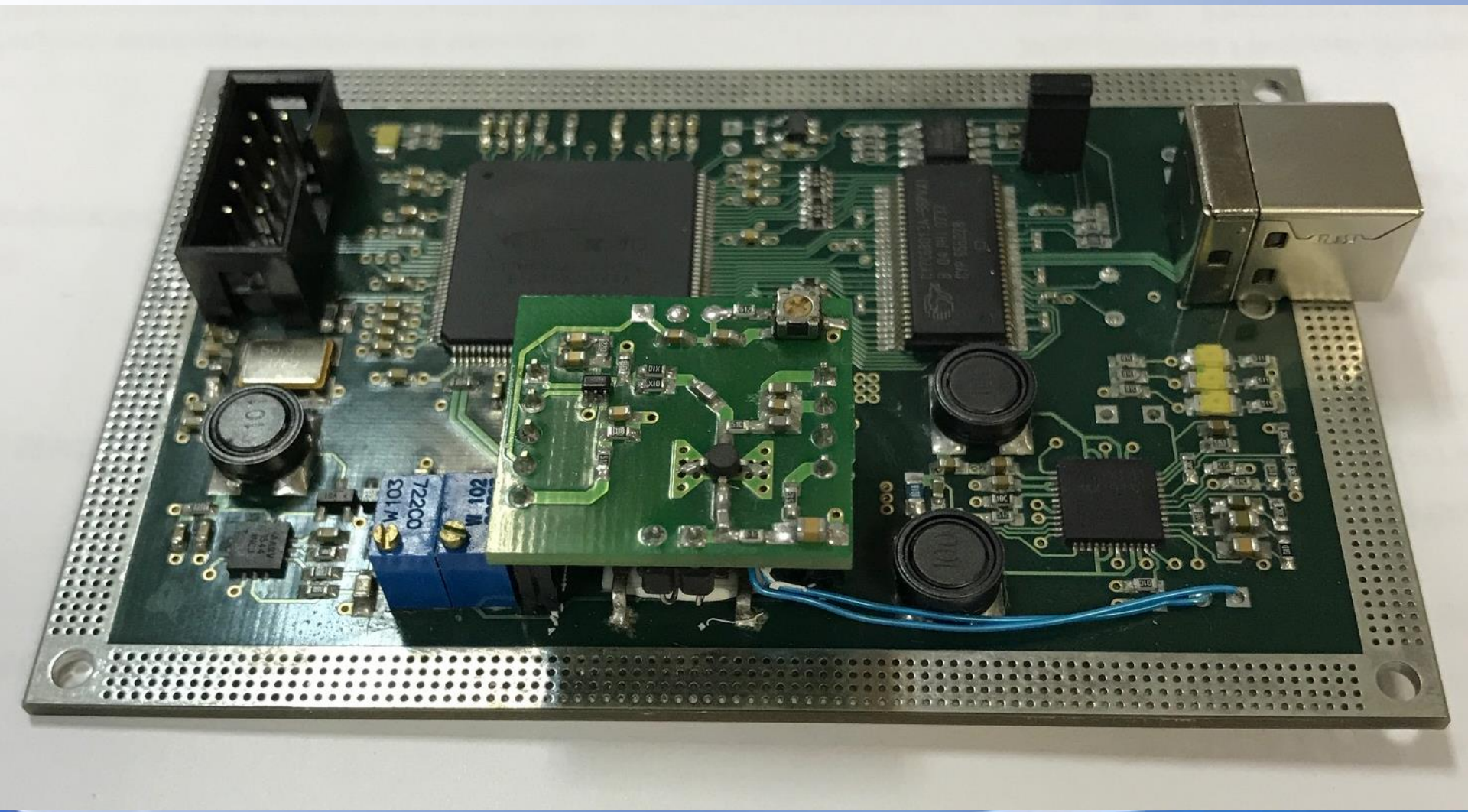
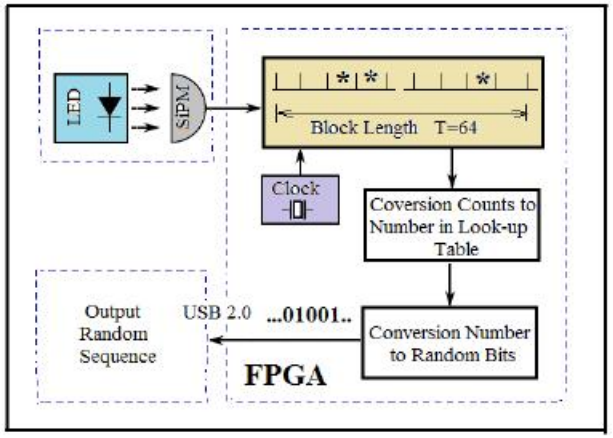


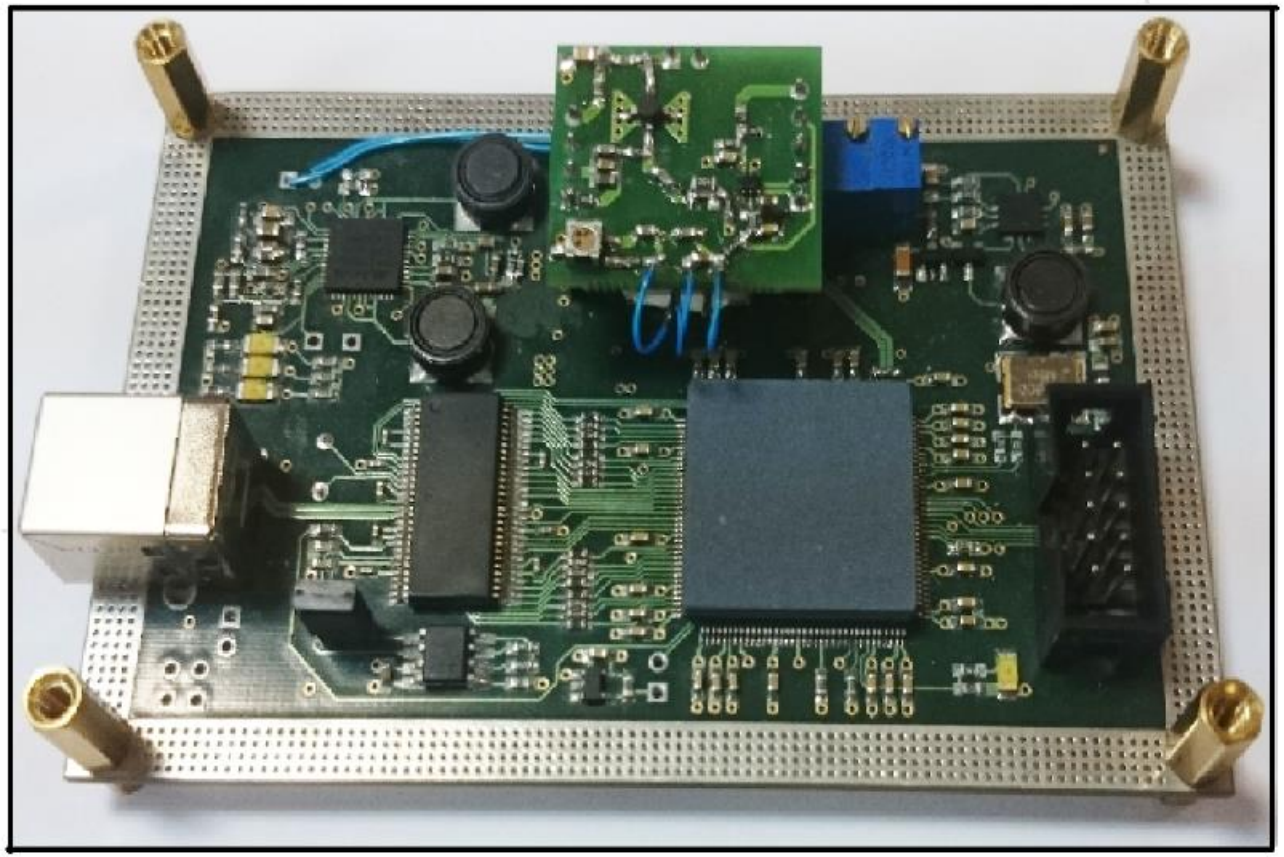
Схема сети квантового распределения ключей


220-10L
C5
220-10L
C5


W103
72200

номер позиции фотоотсчета *
i=1
i=2
i=3
i=4
i=5
i=6
$C_0^0$
$C_1^0$ $C_1^1$
$C_2^0$ $C_2^1$ $C_2^2$
$C_3^0$ $C_3^1$ $C_3^2$ $C_3^3$
$C_4^0$ $C_4^1$ $C_4^2$ $C_4^3$ $C_4^4$
$C_5^0$ $C_5^1$ $C_5^2$ $C_5^3$ $C_5^4$ $C_5^5$
k=0 k=1 k=2 k=3 k=4 k=5
порядковый номер фотоотсчета *


LED
SiPM
Block Length T=64
Clock
Coversion Counts to Number in Look-up Table
Output Random Sequence
USB 2.0
...01001..
Conversion Number to Random Bits
FPGA



# 2019

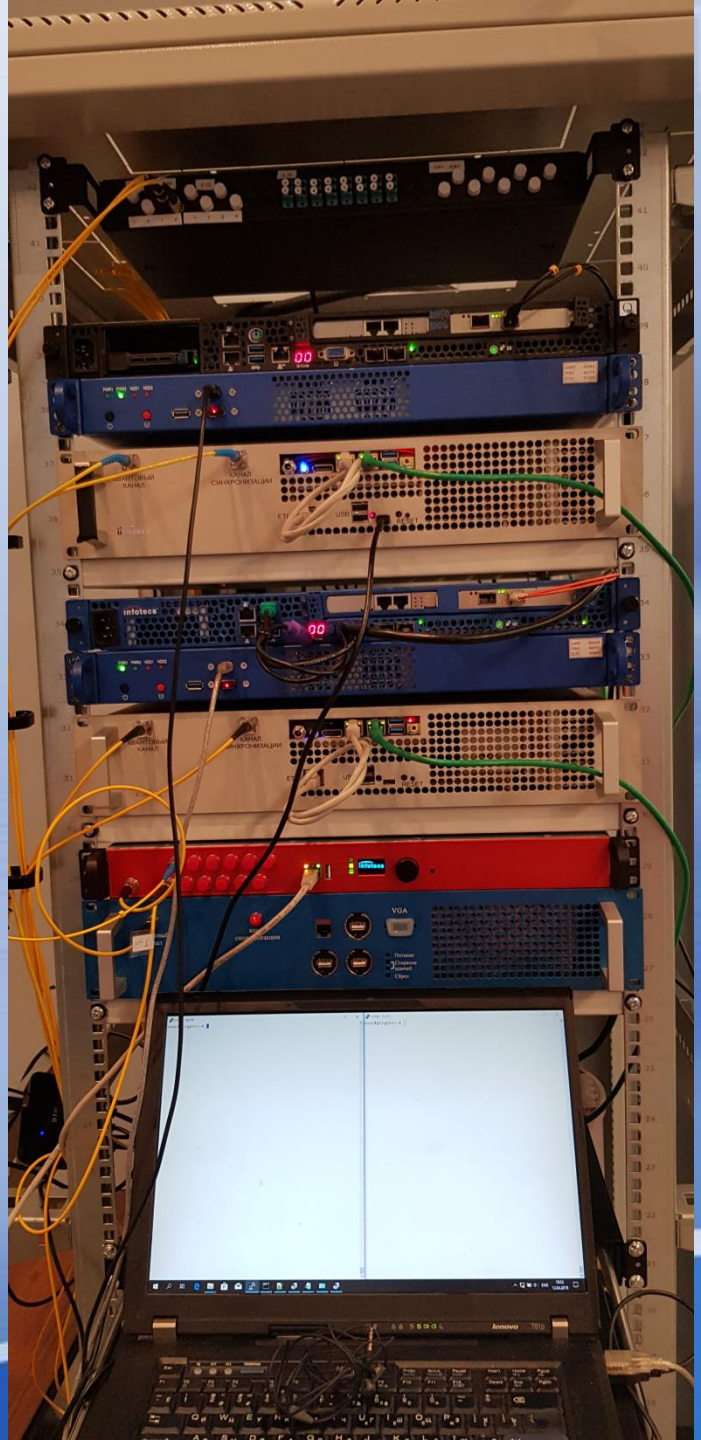
# Новое поколение интегрированных с классическими средствами шифрования систем квантовой криптографии

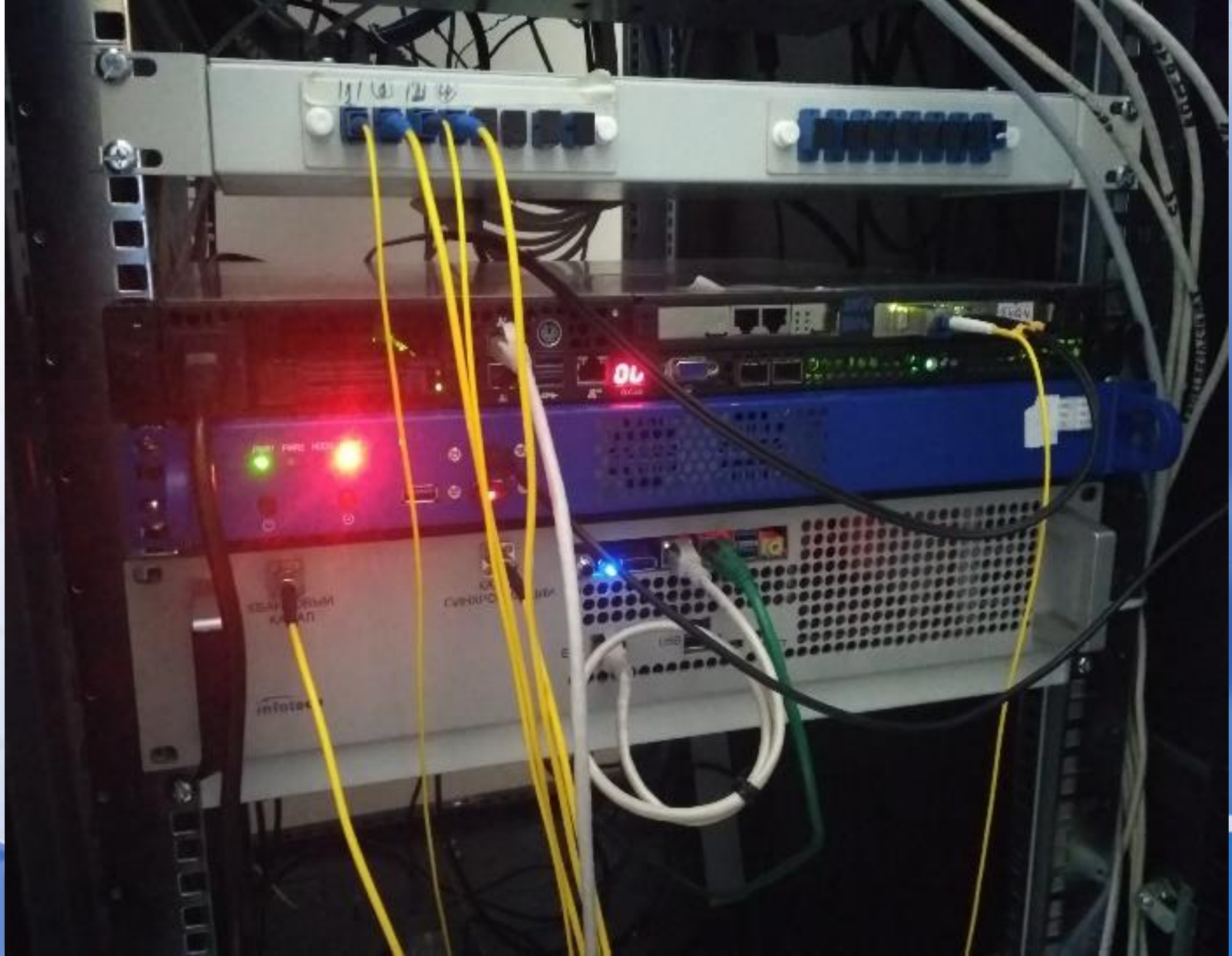
## -- единая замкнутая система

Проекты Quandor и QuanTel

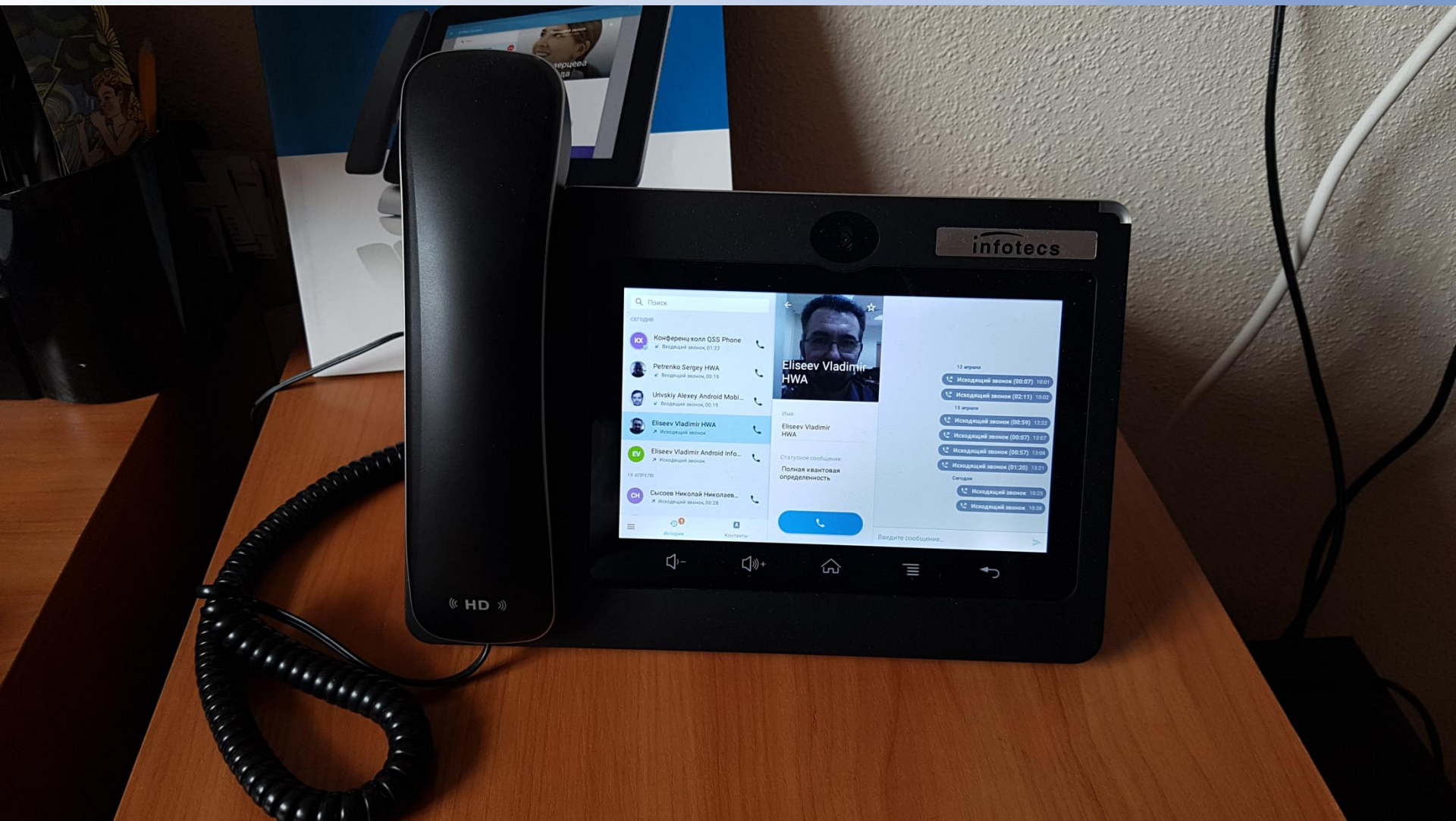
# 2019

## Квантовая Криптография + 10G шифратор связь ЦОД – ЦОД

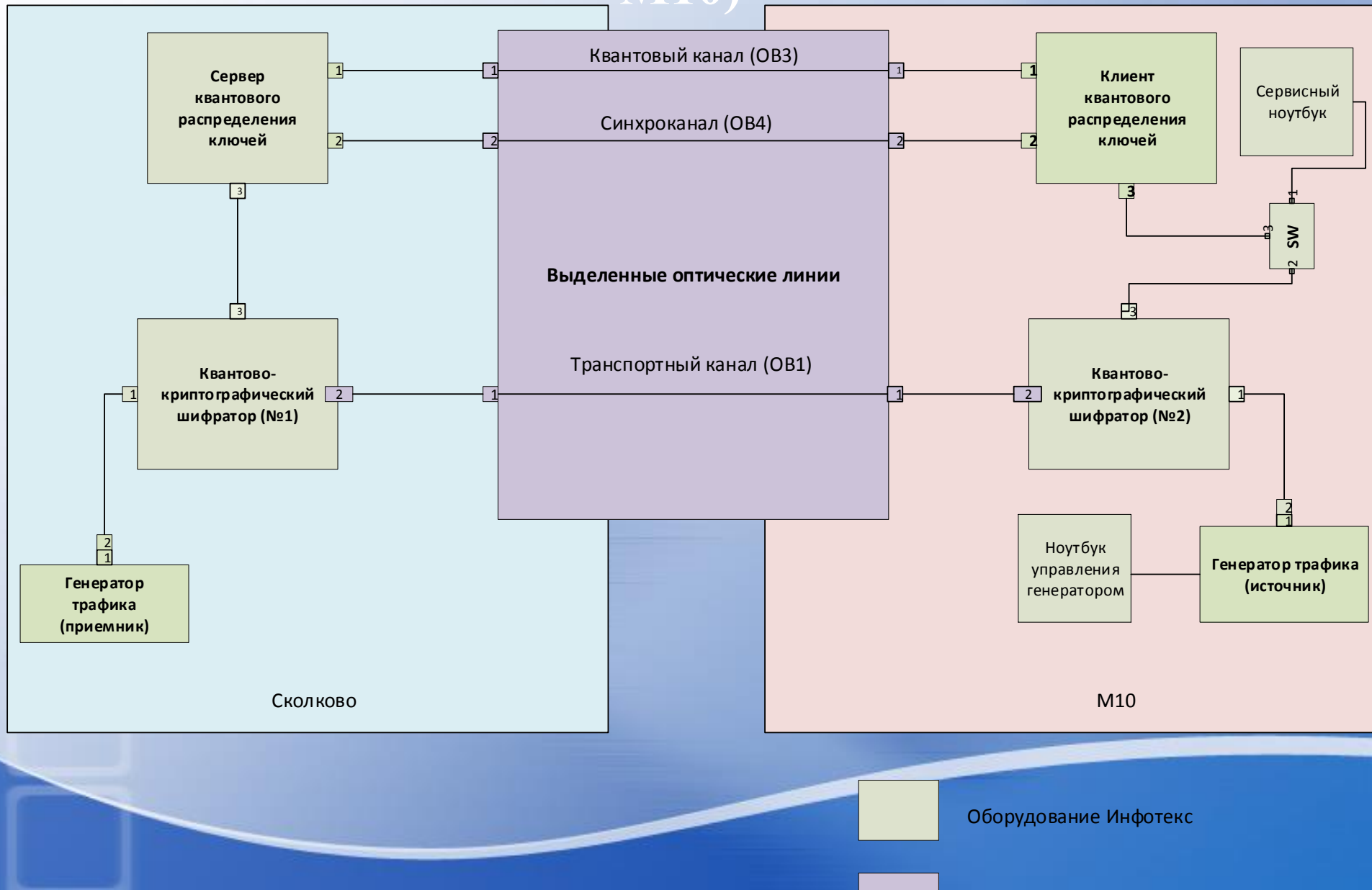




# Квантовый телефон волоконная линия Инфотекс - МГУ

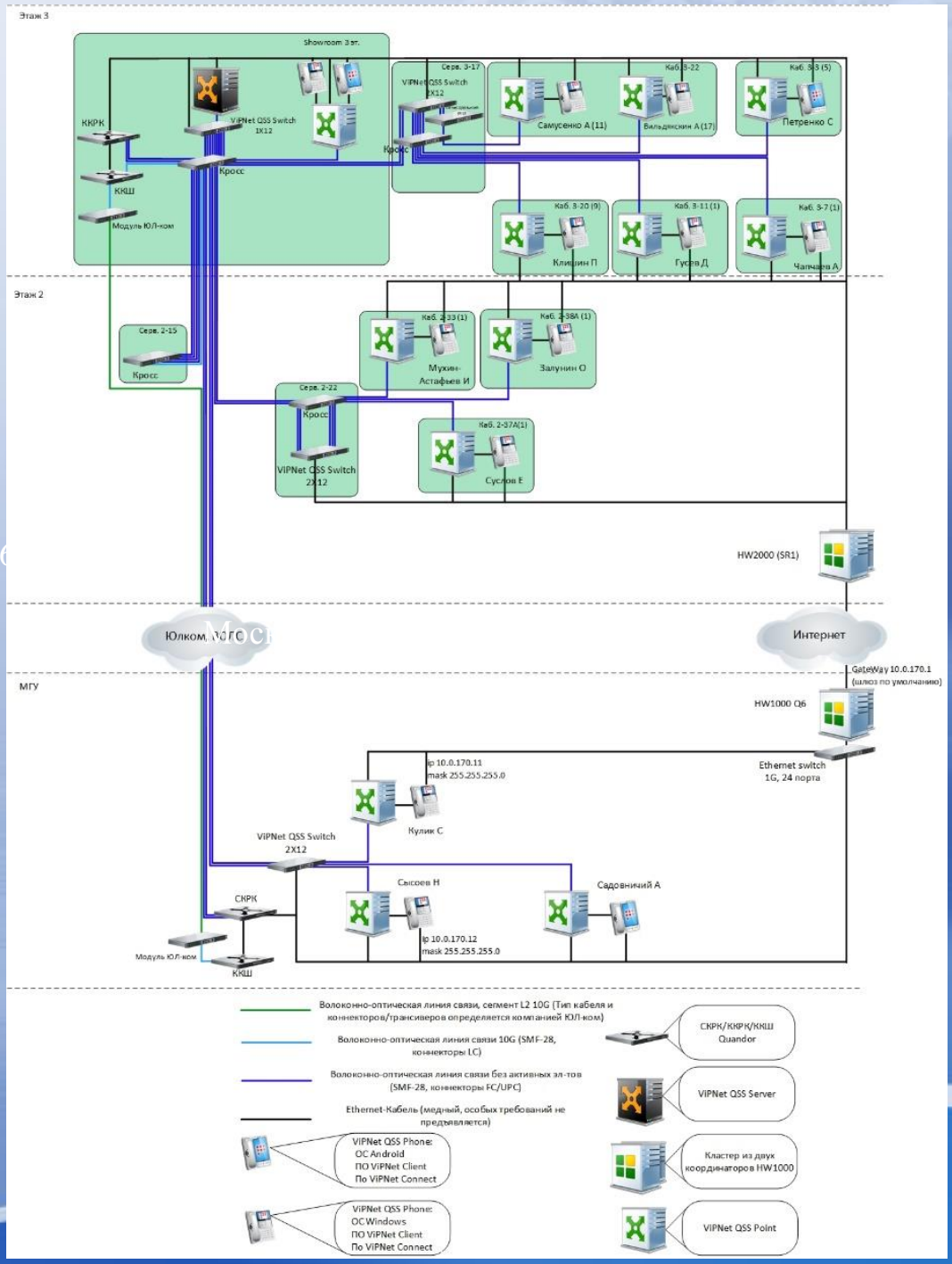


# Испытаниях на площадках Ростелекома (Сколково и М10)



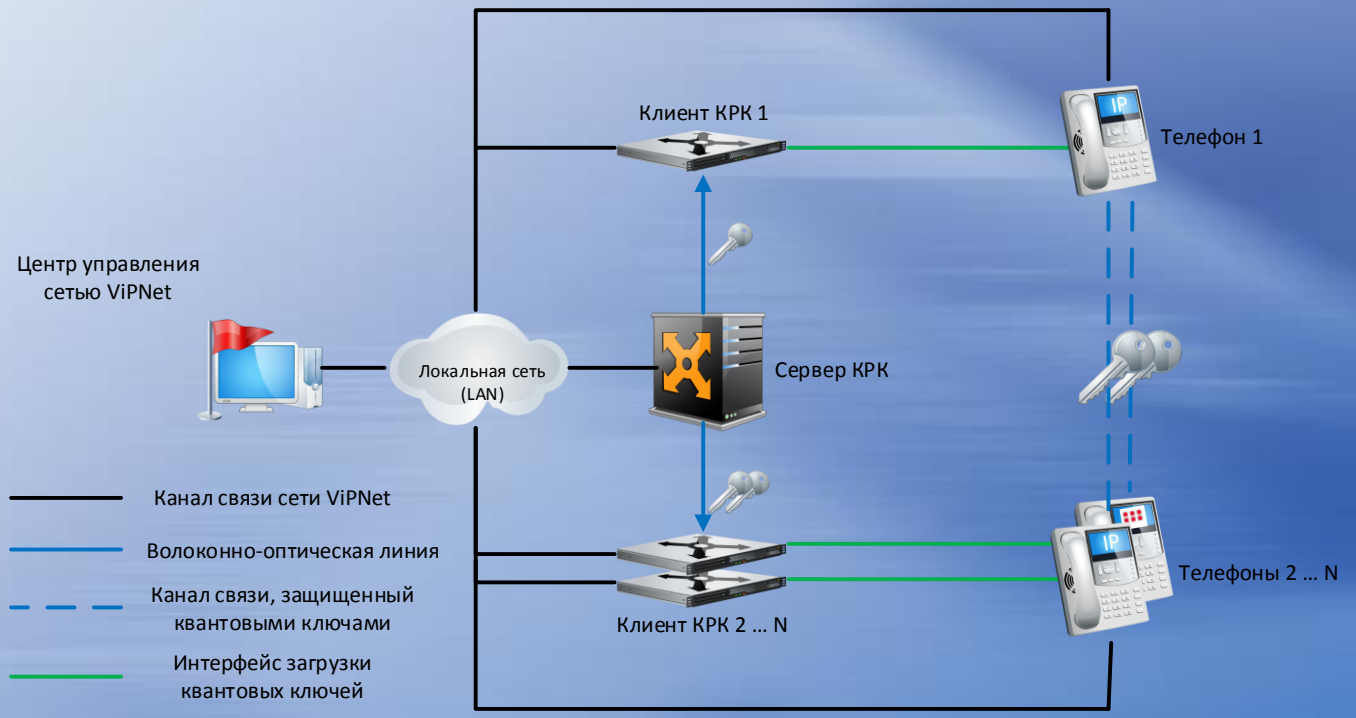
# Квантовая сеть ИнфоТеКС-МГУ

## им. М.В. Ломоносова

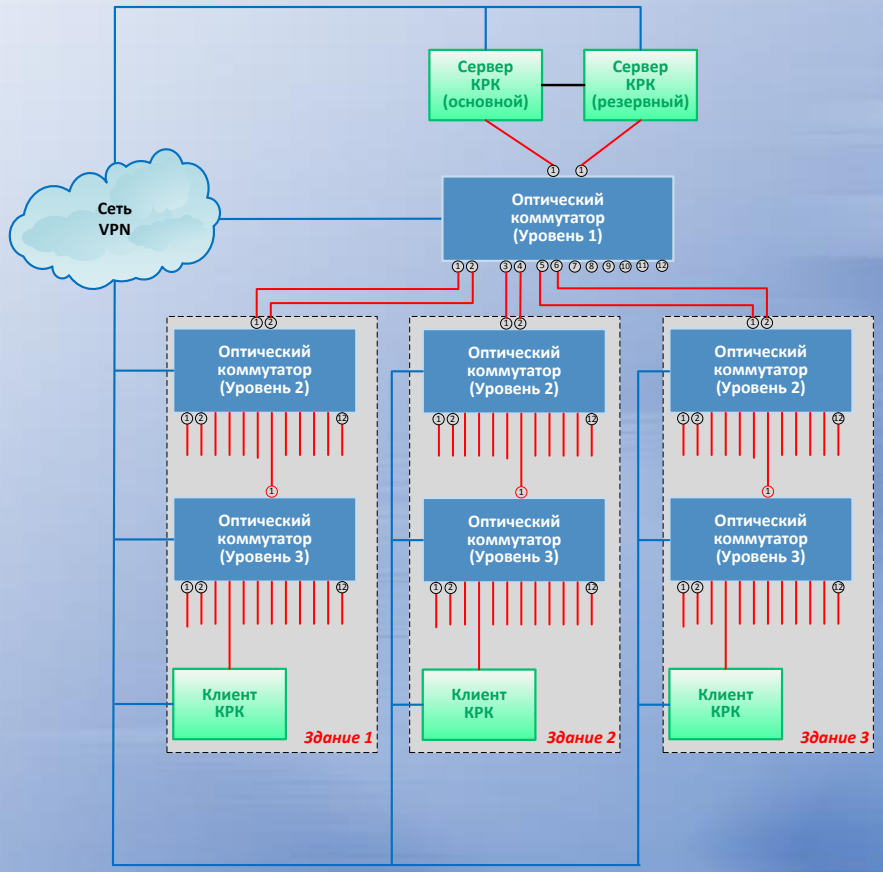


# ViPNet Quantum Security System

**Оборудование квантового распределения ключей (КРК) сопряженное с с ПО ViPNet Client и Connect на телефонах абонентов**



# Иерархическая квантовая сеть



# Особенности ViPNet QSS

- Не содержит ни одного ассиметричного криптографического механизма
- Имеет 2 ключевые системы и обеспечивает защиту от компрометации ключей администраторами
- Скомпрометировать систему можно только путем одновременного подкупа двух администраторов (ViPNet и КРК) в период развертывания системы!

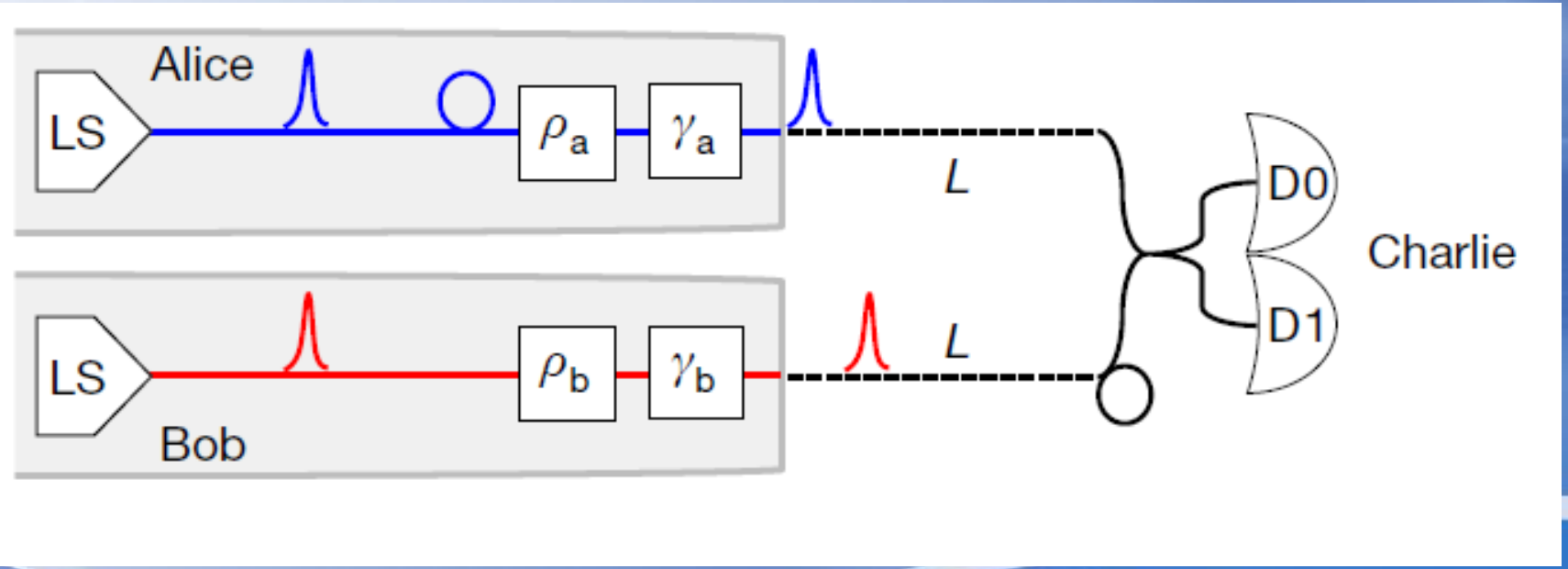
# Передача ключей через НЕДОВЕРЕННЫЕ узлы

# 2018, Nature

LETTER

https://doi.org/10.1038/s41586-018-0066-6

## Overcoming the rate–distance limit of quantum key distribution without quantum repeaters



Письма в ЖЭТФ, том 66, вып.11, стр.736 - 741 © 1997г. 10 декабря

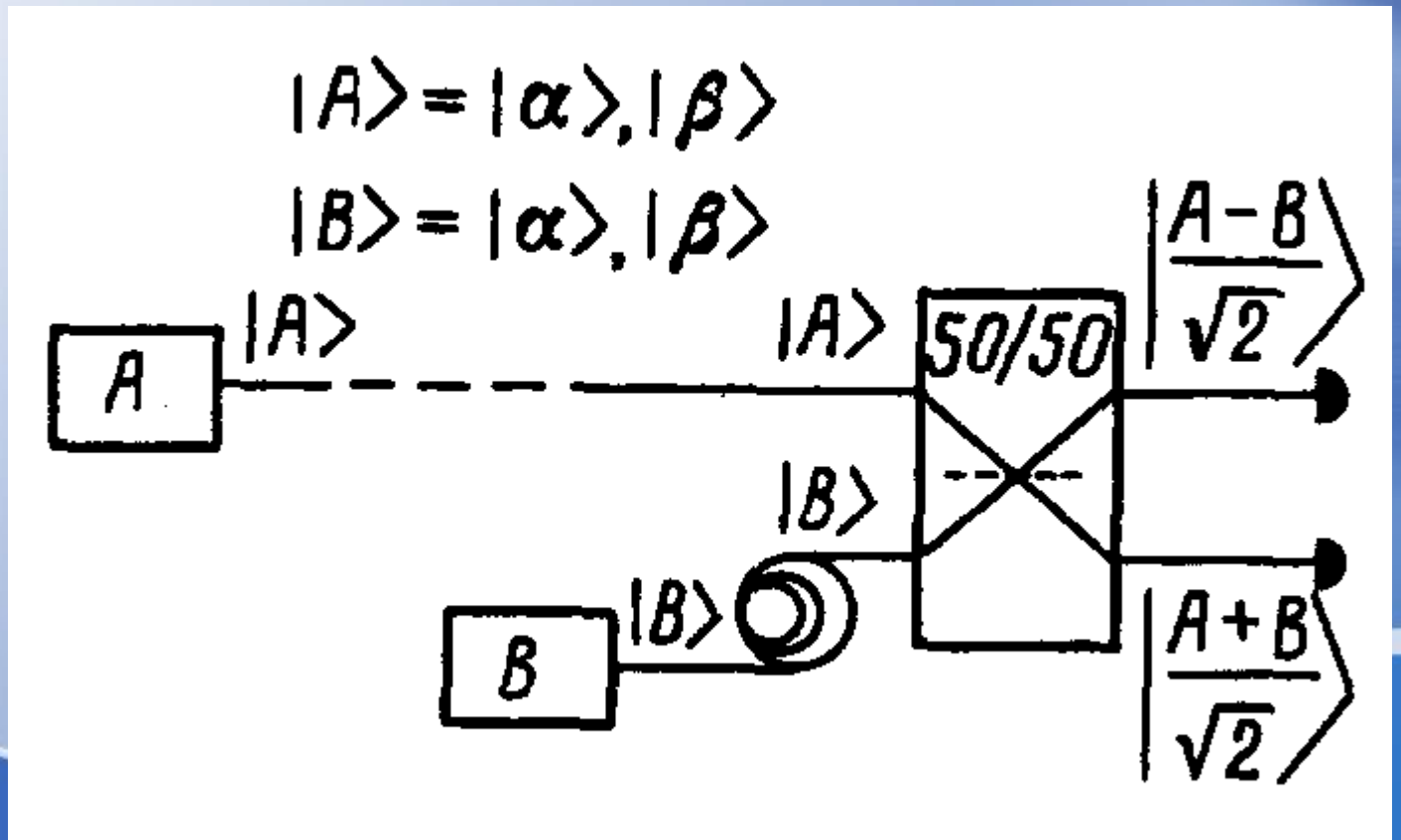
# КВАНТОВАЯ КРИПТОГРАФИЯ НА КОГЕРЕНТНЫХ СОСТОЯНИЯХ НА ОСНОВЕ КВАНТОВОГО КОМПАРАТОРА

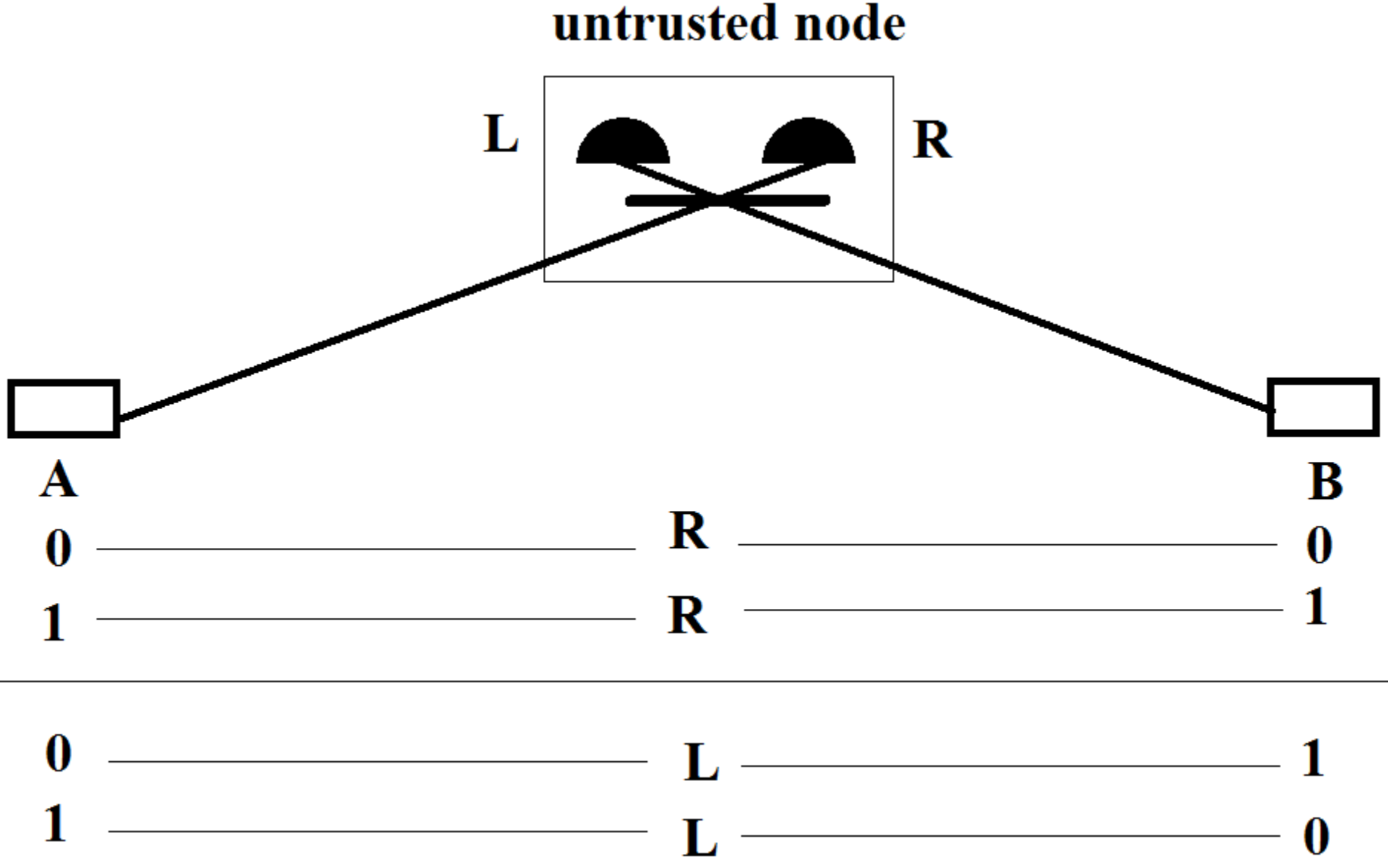
*С.Н.Молотков*

*Институт физики твердого тела РАН*

*142432, Черноголовка, Московская обл., Россия*

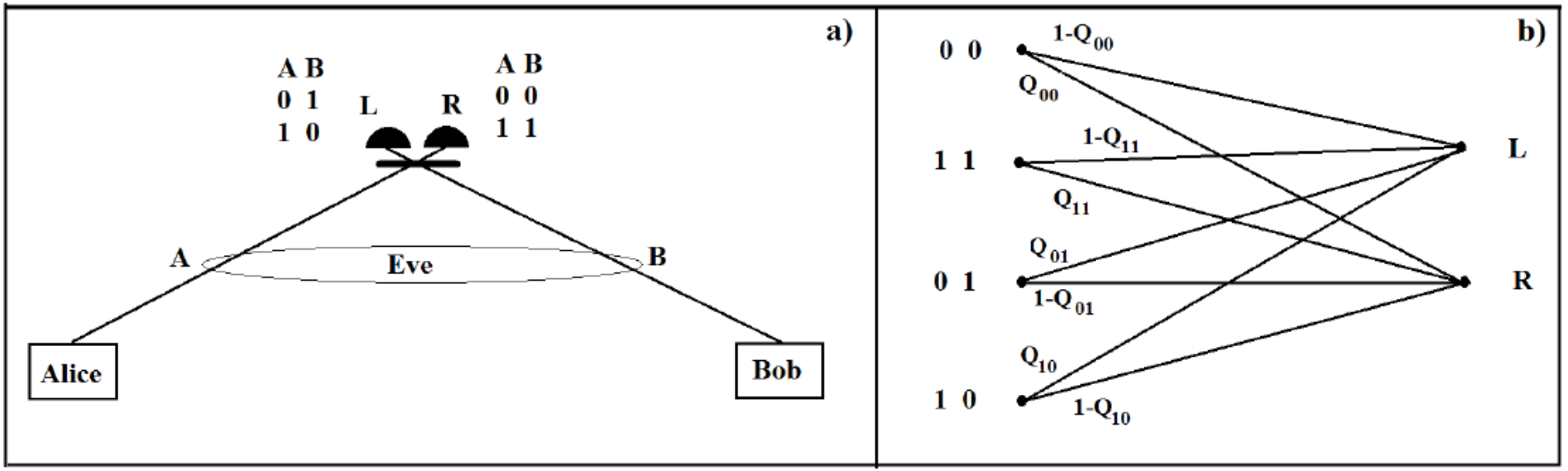
Поступила в редакцию 16 сентября 1997 г.




untrusted node
L
R
A
B
0
R
0
1
R
1
0
L
1
1
L
0

# Оценка длины секретного ключа

$$\ell = \lim_{n\to\infty} \frac{\ell_n}{n} = H(X^{\times}|E) - leak$$



$$|\alpha\rangle_{1A} \otimes |e^{i\varphi_A}\rangle_{2A}, \quad |\alpha\rangle_{1B} \otimes |e^{i\varphi_B}\rangle_{2B},$$

базис $+$ $\begin{cases} \varphi_A = 0, \pi \\ \varphi_B = 0, \pi \end{cases}$, базис $\times$ $\begin{cases} \varphi_A = \frac{\pi}{2}, \frac{3\pi}{2} \\ \varphi_B = \frac{\pi}{2} \end{cases}$

Detector R $\quad |\frac{\alpha(e^{i\varphi_A} - e^{i\varphi_A})}{\sqrt{2}}\rangle_2 = |\sqrt{2}\overline{\alpha}\sin(\frac{\Delta\varphi}{2})\rangle_2$

Detector L $\quad |\frac{\alpha(e^{i\varphi_A} + e^{i\varphi_A})}{\sqrt{2}}\rangle_2 = |\sqrt{2}\overline{\alpha}\cos(\frac{\Delta\varphi}{2})\rangle_2$

$$\Delta\varphi = \varphi_A - \varphi_B$$

$$\Pr\{R, \Delta\varphi, \eta, l\} \propto 2\mu \sin^2(\frac{\Delta\varphi}{2})\eta_R T(l)$$

$$\Pr\{L, \Delta\varphi, \eta, l\} \propto 2\mu \cos^2(\frac{\Delta\varphi}{2})\eta_L T(l),$$

$$|\Phi\rangle_{\overline{A}A} =$$

$$= \frac{1}{\sqrt{2}}\left(|\overline{0}^{+}\rangle_{\overline{A}} \otimes |\overline{0}^{+}\rangle_{A} + |\overline{1}^{+}\rangle_{\overline{A}} \otimes |\overline{1}^{+}\rangle_{A}\right) = \frac{1}{\sqrt{2}}\left(|\overline{0}^{\times}\rangle_{\overline{A}} \otimes |\overline{0}^{\times}\rangle_{A} + |\overline{1}^{\times}\rangle_{\overline{A}} \otimes |\overline{1}^{\times}\rangle_{A}\right)$$

$$|\Phi\rangle_{\overline{B}B} =$$

$$= \frac{1}{\sqrt{2}}\left(|\overline{0}^{+}\rangle_{\overline{B}} \otimes |\overline{0}^{+}\rangle_{B} + |\overline{1}^{+}\rangle_{\overline{B}} \otimes |\overline{1}^{+}\rangle_{B}\right) = \frac{1}{\sqrt{2}}\left(|\overline{0}^{\times}\rangle_{\overline{B}} \otimes |\overline{0}^{\times}\rangle_{B} + |\overline{1}^{\times}\rangle_{\overline{B}} \otimes |\overline{1}^{\times}\rangle_{B}\right)$$

$$|\Phi\rangle_{\overline{AB}AB} = |\Phi\rangle_{\overline{A}A} \otimes |\Phi\rangle_{\overline{B}B};$$

$$I_{\overline{A}} = |\overline{0}^{+}\rangle_{\overline{AA}}\langle\overline{0}^{+}| + |\overline{1}^{+}\rangle_{\overline{AA}}\langle\overline{1}^{+}| = |\overline{0}^{\times}\rangle_{\overline{AA}}\langle\overline{0}^{\times}| + |\overline{1}^{\times}\rangle_{\overline{AA}}\langle\overline{1}^{\times}|$$

$$I_{\overline{B}} = |\overline{0}^{+}\rangle_{\overline{BB}}\langle\overline{0}^{+}| + |\overline{1}^{+}\rangle_{\overline{BB}}\langle\overline{1}^{+}| = |\overline{0}^{\times}\rangle_{\overline{BB}}\langle\overline{0}^{\times}| + |\overline{1}^{\times}\rangle_{\overline{BB}}\langle\overline{1}^{\times}|$$

# Атака подслушивателя

$$\rho_{ABE}(00) = \mathcal{T}_{EAB}\left(|0^+0^+\rangle_{ABAB}\langle 0^+0^+|\right), \quad \rho_{ABE}(01) = \mathcal{T}_{EAB}\left(|0^+1^+\rangle_{ABAB}\langle 0^+1^+|\right)$$

$$\rho_{ABE}(10) = \mathcal{T}_{EAB}\left(|1^+0^+\rangle_{ABAB}\langle 1^+0^+|\right), \quad \rho_{ABE}(11) = \mathcal{T}_{EAB}\left(|1^+1^+\rangle_{ABAB}\langle 1^+1^+|\right)$$

$$\rho_{\overline{AB}AB} = (\mathcal{T}_{EAB}\,(I_{\overline{AB}}|\Phi\rangle_{\overline{AB}AB\overline{AB}AB}\Phi|I_{\overline{AB}})) =$$

$$= \frac{1}{4}\Big(|\overline{0}^+\overline{0}^+\rangle_{\overline{AB}AB}\langle\overline{0}^+\overline{0}^+| \otimes \rho_{ABE}(00) + |\overline{0}^+\overline{1}^+\rangle_{\overline{AB}\overline{AB}}\langle\overline{0}^+\overline{1}^+| \otimes \rho_{ABE}(01) +$$

$$+|\overline{1}^+\overline{0}^+\rangle_{\overline{AB}AB}\langle\overline{1}^+\overline{0}^+| \otimes \rho_{ABE}(10) + |\overline{1}^+\overline{1}^+\rangle_{\overline{AB}AB}\langle\overline{1}^+\overline{1}^+| \otimes \rho_{ABE}(11)\Big),$$

$\overline{AB}$ $\mathcal{X}^+ = \{0^+0^+, 0^+1^+, 1^+0^+, 1^+1^+\}.$

$$\rho_{X^+(AB)E} = \frac{1}{4} \sum_{x^+ \in \mathcal{X}^+} |x^+\rangle_X \langle x^+| \otimes \rho^{x^+}_{(AB)E},$$

$$\mathcal{X}^+ = \{0^\times 0^\times, 0^\times 1^\times, 1^\times 0^\times, 1^\times 1^\times\}$$

$$\rho_{X^\times(AB)E} = \frac{1}{4} \sum_{x^\times \in \mathcal{X}^\times} |x^\times\rangle_X \langle x^\times| \otimes \rho^{x^\times}_{(AB)E};$$

# Измерения на недоверенном узле

$$\mathcal{K}^{+}_{(00),L} = |0^{+}0^{+}\rangle_{(AB)Y}\langle L|, \quad \mathcal{K}_{(00),L} = |L\rangle_{Y(AB)}\langle 0^{+}0^{+}|,$$

$$\mathcal{K}^{+}_{(11),L} = |1^{+}1^{+}\rangle_{(AB)Y}\langle L|, \quad \mathcal{K}_{(11),L} = L\rangle_{Y(AB)}\langle 1^{+}1^{+}|L|,$$

$$\mathcal{K}^{+}_{(01),R} = |0^{+}1^{+}\rangle_{(AB)Y}\langle R|, \quad \mathcal{K}_{(01),R} = |R\rangle_{Y(AB)}\langle 0^{+}1^{+}|,$$

$$\mathcal{K}^{+}_{(10),R} = |1^{+}0^{+}\rangle_{(AB)Y}\langle R|, \quad \mathcal{K}_{(10),R} = |R\rangle_{Y(AB)}\langle 1^{+}0^{+}|.$$

$$\rho_{X^+Y\,E} = \frac{1}{4} \sum_{x^+ \in \mathcal{X}^+} \sum_{y \in \mathcal{Y}} |x^+\rangle_X \langle x^+| \otimes |y\rangle_Y \langle y| \otimes \rho_E^{x^+ y}$$

$$\rho_E^{x^+ y} = \sum_{i=0,1} \sum_{j=0,1} \mathcal{K}_{(ij),y} \rho_{(AB)E}^{x^+} \mathcal{K}_{(ij),y}^+.$$

# Энтропийные соотношения неопределенностей

$$H(X^{\times}|E) + H(X^{+}|Y) \geq -\log|c|^2 = 2, \quad |c|^2 = \max_{i,j,i',j'=0,1} |{}_{\overline{AB}}\langle i^{+}j^{+}|i'^{\times}j'^{\times}\rangle_{\overline{AB}}|^2 = \frac{1}{4}$$

$$H(X^{\times}|E) = H(\rho_{X^{\times}E}) - H(\rho_E), \quad H(X^{+}|Y) = H(\rho_{X^{+}Y}) - H(\rho_Y).$$

$$\rho_{X+Y} =$$

$$= \frac{1}{4}|0^{+}0^{+}\rangle_{XX}\langle 0^{+}0^{+}| \otimes \{(1-Q_{00})|L\rangle_{YY}\langle L| + Q_{00}|R\rangle_{YY}\langle R|\} +$$

$$+\frac{1}{4}|0^{+}1^{+}\rangle_{XX}\langle 0^{+}1^{+}| \otimes \{(1-Q_{01})|R\rangle_{YY}\langle R| + Q_{01}|L\rangle_{YY}\langle L|\} +$$

$$+\frac{1}{4}|1^{+}0^{+}\rangle_{XX}\langle 1^{+}0^{+}| \otimes \{(1-Q_{10})|R\rangle_{YY}\langle R| + Q_{10}|L\rangle_{YY}\langle L|\} +$$

$$\frac{1}{4}|1^{+}1^{+}\rangle_{XX}\langle 1^{+}1^{+}| \otimes \{(1-Q_{11})|L\rangle_{YY}\langle L| + Q_{11}|R\rangle_{YY}\langle R|\}.$$

$$P_{X|Y}(y|X=(ij)) = Q_{ij}$$

$$Q_{ij} = Q$$

$$H(\rho_{X+Y}) = 2 + \frac{1}{4}\sum_{i,j=0,1} h(Q_{ij})$$

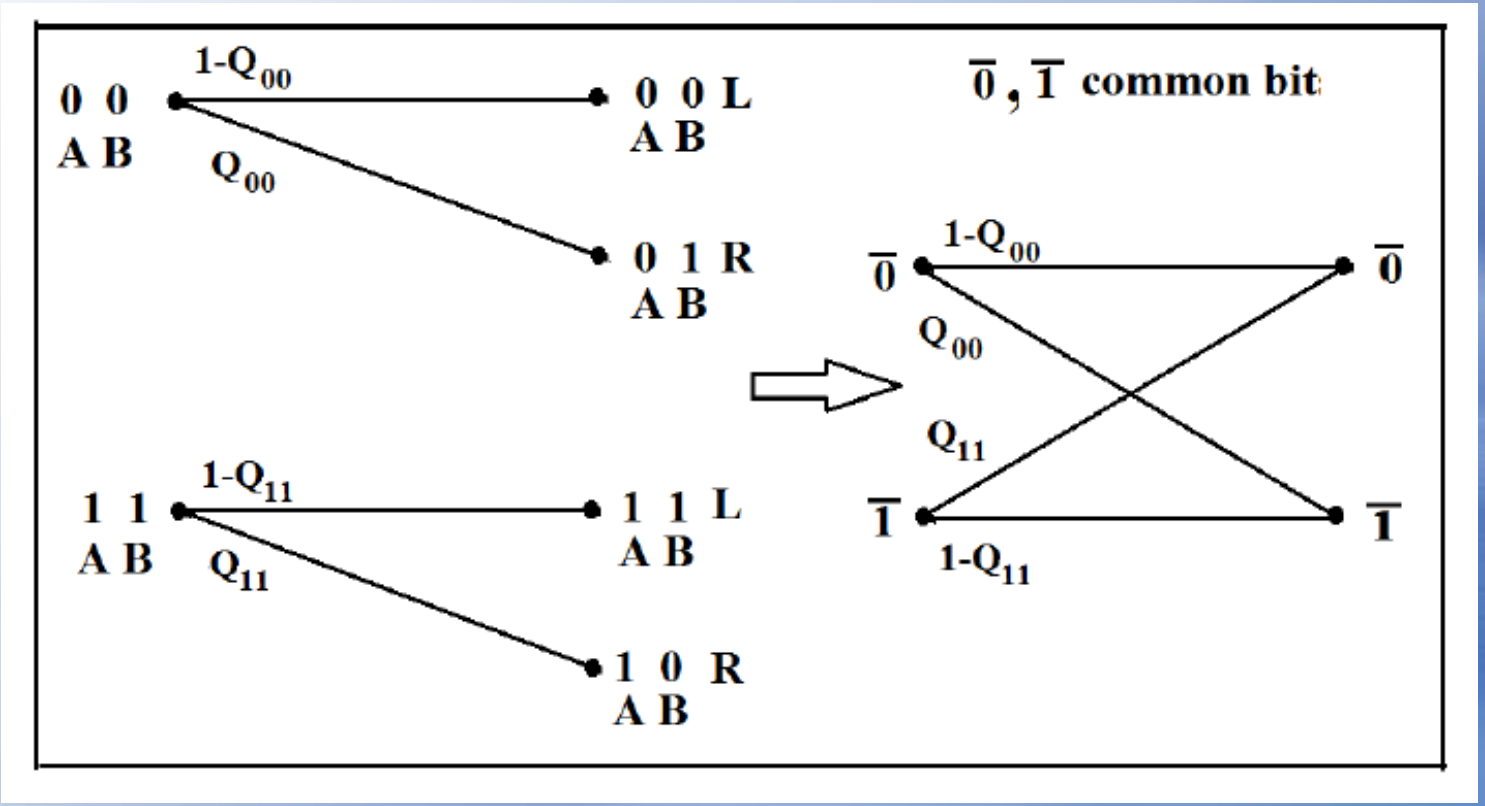
$$H(\rho_{X+Y}) = 2 + h(Q)$$

$$H(X^+|Y) = 1 + \frac{1}{4}\sum_{i,j=0,1} h(Q_{ij}) - \overline{h}(q).$$

$$\overline{h}(q) = -(1-q)\log(1-q) - (1+q)\log(1+q)$$

$$q = \frac{1}{2}(Q_{00} + Q_{11} - Q_{01} - Q_{10})$$

# Утечка информации при коррекции ошибок



$$n \cdot leak = n\left[\frac{1}{2}\left(\frac{h(Q_{00})+h(Q_{11})}{2}\right)+\frac{1}{2}\left(\frac{h(Q_{01})+h(Q_{10})}{2}\right)\right]$$

$$H(X^{\times}|E) \geq 2 - H(X^{+}|Y) = 2 - \left(1+\frac{1}{2}\sum_{i,j=0,1} h(Q_{ij}) - \overline{h}(q)\right),$$

$$\ell = H(X^{\times}|E) - leak = 2 - H(X^{+}|Y) - leak = 1 - \left(\frac{1}{2}\sum_{i,j=0,1} h(Q_{ij}) - \overline{h}(q)\right)$$

$$Q_{ij} = Q \qquad \ell = 1 - 2h(Q)$$

$$\ell = 1 - (h(Q_0) + h(Q_1))$$

$$Q_0 = Q_1 = Q \qquad \ell = 1 - 2h(Q)$$

**СПАСИБО ЗА ВНИМАНИЕ.**