Квантовая криптография: основные понятия и применения

С.Н.Молотков

Кафедра Суперкомпьютеров и Квантовой Информатики

ВМК МГУ имени М.В.Ломоносова,

QOT Лаборатория Квантовых Оптических Технологий

Часть I

1. Зачем это нужно. Проблема распределения секретных ключей -- центральная проблема в криптографии.

2. Как это выглядит сегодня и как может выглядеть в будущем.

3. Как это работает – общие принципы.

4. Необходимость квантового генератора случайных чисел.

5. Доказательства секретности ключей. Криптостойкость относительно любых атак, включая квантовую память и квантовый компьютер.

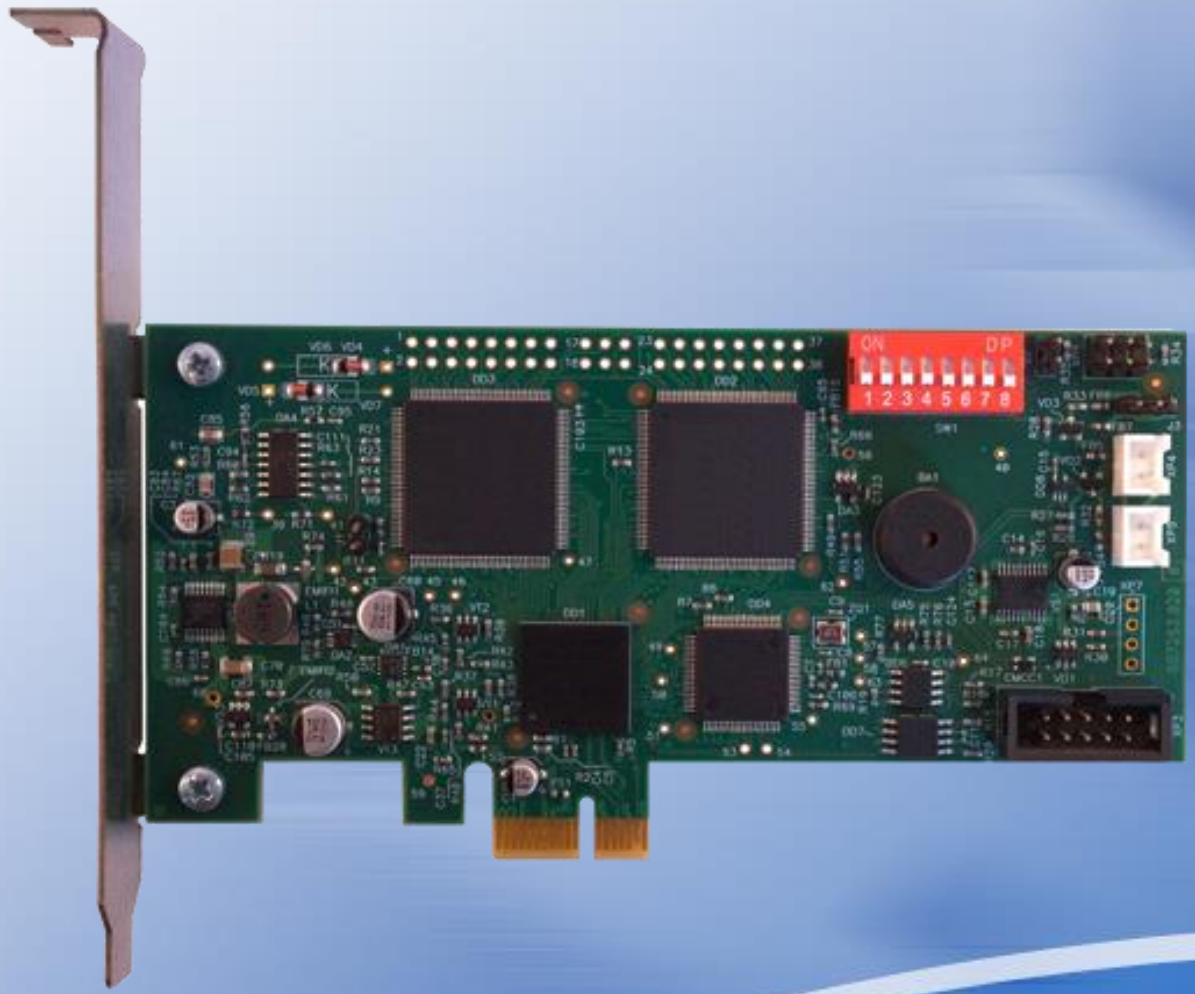
Часть II

1. Реализации систем квантовой криптографии. Обзор современного состояния.
2. Волоконно-оптические системы. Сравнение по доказуемой криптостойкости.
3. Системы для открытого пространства. Сравнение по доказуемой криптостойкости.
4. Сети с квантовым распределением ключей.
5. Реконфигурируемые сети с квантовым распределением ключей.
6. Где и что у кого есть?

Часть III.

1. Вопросы, которые требуется решить (интегрирование в имеющиеся шифр-средства, устойчивость относительно активного зондирования, инфраструктура, элементная база).

Современная плата шифратора, реализующая российский стандарт шифрования ГОСТ 28147-89 Р



Cold War Soviet Cryptanalysis

- Soviet Union was breaking codes and employed at least 100 cryptologists…

  [Source: Cryptologia, interviews by David Kahn with gen. Andreev=first head of FAPSI=Russian NSA]

Example: In 1967 GRU (Soviet Intelligence) was intercepting cryptograms from 115 countries, using 152 cryptosystems, and among these they broke 11 codes and "obtained" 7 other codes.

Часть I

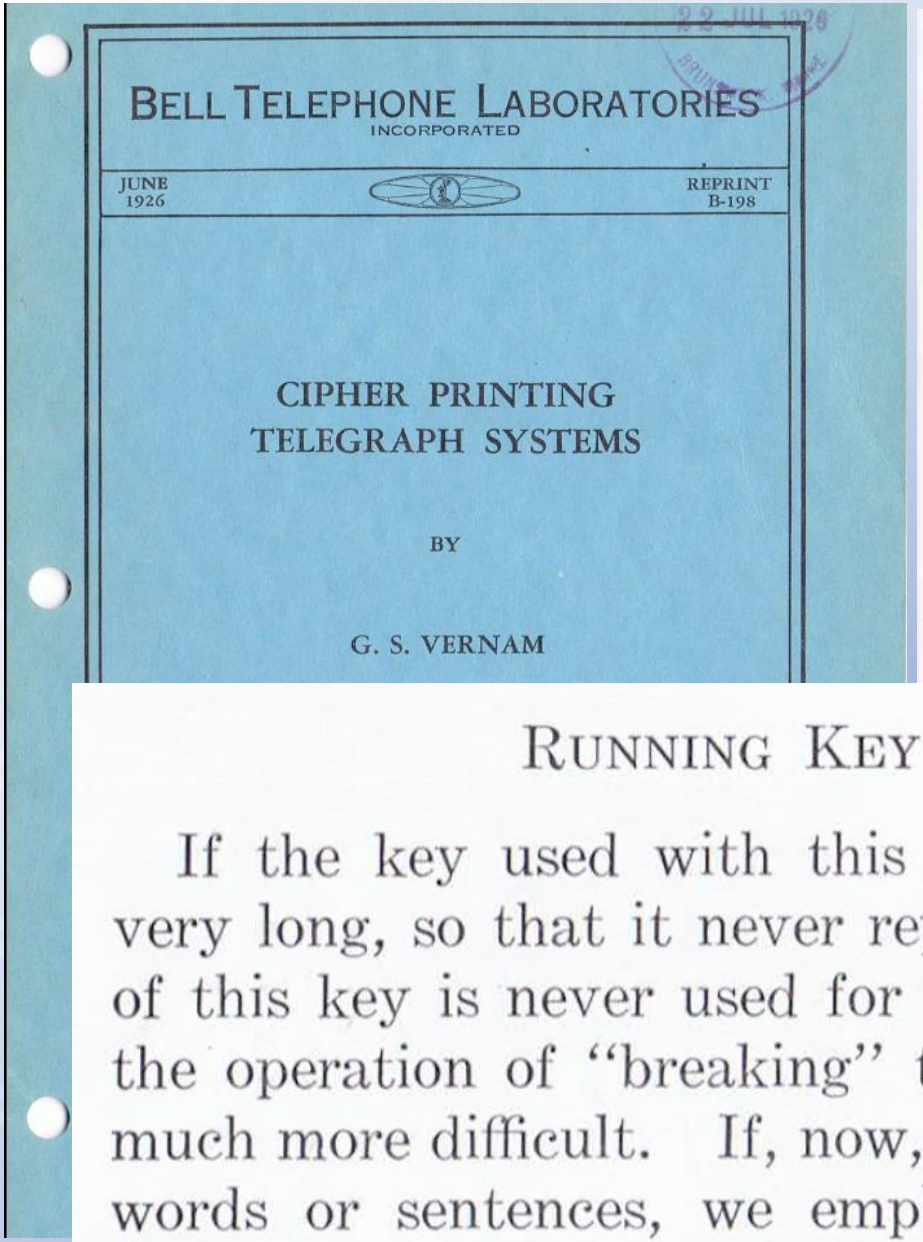
1. Зачем это нужно. Проблема распределения секретных ключей -- центральная проблема в криптографии.

Существуют ли абсолютно секретные (стойкие) системы шифрования? Ответ – ДА.

Шифрование с одноразовыми ключами.

В этом месте ошибались даже великие – Леонард Эйлер.

G.Vernam, В.А.Котельников, C.Shannon



CIPHER PRINTING TELEGRAPH SYSTEMS FOR SECRET WIRE AND RADIO TELEGRAPHIC COMMUNICATIONS

By G. S. Vernam[1]
Associate, A. I. E. E.

Synopsis.—*This paper describes a printing telegraph cipher system developed during the World War for the use of the Signal Corps, U. S. Army. This system is so designed that the messages are in secret form from the time they leave the sender until they are deciphered automatically at the office of the addressee. If copied while en route, the messages cannot be deciphered by an enemy, even though he has full knowledge of the methods and apparatus used. The operation of the equipment is described, as well as the method of using it for sending messages by wire, mail or radio.*

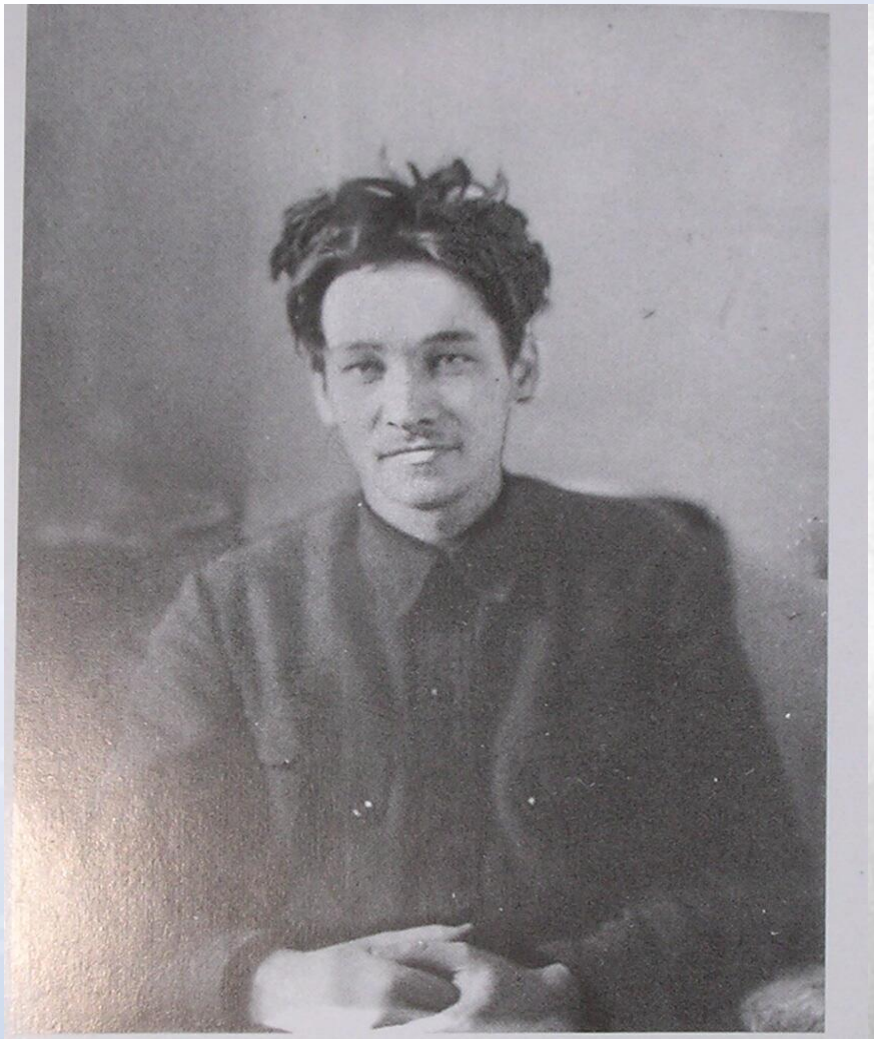
The paper also discusses the practical impossibility of preventing the copying of messages, as by wire tapping, and the relative advantages of various codes and ciphers as regards speed, accuracy and the secrecy of their messages.

Introduction

THE purpose of this paper is to discuss briefly certain methods for obtaining secrecy in connection with messages sent by wire or racio telegraphy, and to describe in particular printing telegraph cipher systems that were developed for this purpose during the World War

Running Key Ciphers

If the key used with this type of cipher is made very long, so that it never repeats and if any portion of this key is never used for more than one message, the operation of "breaking" the cipher becomes very much more difficult. If, now, instead of using English words or sentences, we employ a key composed of letters selected absolutely at random, a cipher system is produced which is absolutely unbreakable.



В.А. Котельников
Автор «теоремы Котельникова»
(1932 г.)

Владимир Александрович Котельников
(06.09.1908 – 11.02.2005)

Одноразовые ключи -- Отчет 19 июня 1941 г.

ОТКАЗ В ПУБЛИКАЦИИ СТАТЬИ В.А. КОТЕЛЬНИКОВА

Редакция журнала "ЭЛЕКТРИЧЕСТВО"

Орган Главэнергопрома и Главэнерго НКТП
и Энергетического института Академии Наук СССР.
Издание ОНТИ

Москва, Калужская, д. 67, Энергетический Институт Академии Наук СССР им. Г.М. Кржижановского
Адрес для корреспонденции: МОСКВА, Главный почтамт, почтовый ящик № 648
Тел. редакции: В 5-32-79
Тел. ответ. редактора: В 5-32-78

11. X. 1936

Тов. КОТЕЛЬНИКОВУ В.А.

Москва, ул. Горького, 17
Научно-Исследоват.
Ин-т Электросвязи.

Уваж. Тов!

Редакция журнала "Электричество" возвращает Вам статью "О пропускной способности эфира и проволоки в электросвязи", так как из-за перегруженности портфеля и узкого интереса данной статьи, учитывая профиль нашего журнала, использовать ее не сможем.

Приложение: Статья на 24 стр. и 4 рис.

Отв. Редактор журнала
"Электричество" _____ /Я.А. Климовицкий/

Зав. редакцией _____ /М.Г. Башкова/

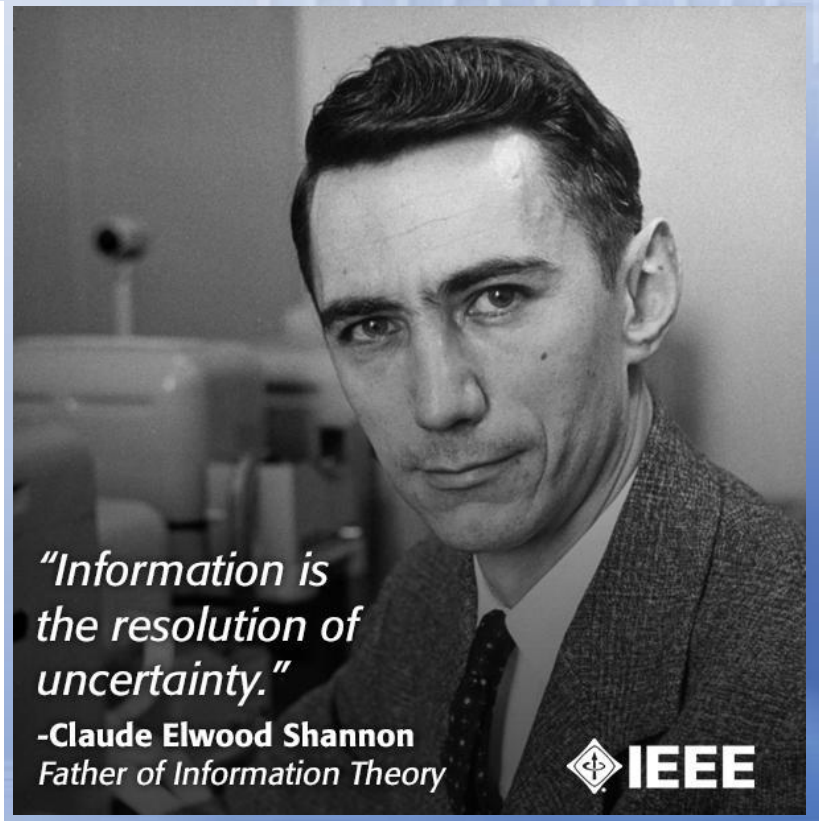
Communication Theory of Secrecy Systems*

By C. E. SHANNON

1 INTRODUCTION AND SUMMARY

The problems of cryptography and secrecy systems furnish an interesting application of communication theory[1]. In this paper a theory of secrecy systems is developed. The approach is on a theoretical level and is intended to complement the treatment found in standard works on cryptography[2]. There, a detailed study is made of the many standard types of codes and ciphers, and of the ways of breaking them. We will be more concerned with the general mathematical structure and properties of secrecy systems.

The treatment is limited in certain ways. First, there are three general types of secrecy system: (1) concealment systems, including such methods as invisible ink, concealing a message in an innocent text, or in a fake covering cryptogram, or other methods in which the existence of the message is concealed from the enemy; (2) privacy systems, for example speech inversion, in which special equipment is required to recover the message; (3) "true" secrecy systems where the meaning of the message is concealed by cipher, code, etc., although its existence is not hidden, and the enemy is assumed to have any special equipment necessary to intercept and record the transmitted signal. We consider only the third type—concealment system are



* The material in this paper appeared in a confidential report "A Mathematical Theory of Cryptography" dated Sept.1, 1946, which has now been declassified.

[1] Shannon, C. E., "A Mathematical Theory of Communication," Bell System Technical Journal, July 1948, p.379; Oct. 1948, p.623.

[2] See, for example, H. F. Gaines, "Elementary Cryptanalysis," or M. Givierge, "Cours de Cryptographie."

Секретный ключ

$$K \to \{0,1\}^n \qquad K_E \to \{0,1\}^n$$

$$P(K = k) = \frac{1}{2^n}$$

$$P(K = k \mid K_E = k_E) = \frac{1}{2^n}$$

$$I(K; K_E) = 0$$

Квантовая криптография

$$I(K; K_E) < 2^{-S} / \ln(2)$$

$$I(M;C) = H(C) - H(C|M) = 0$$

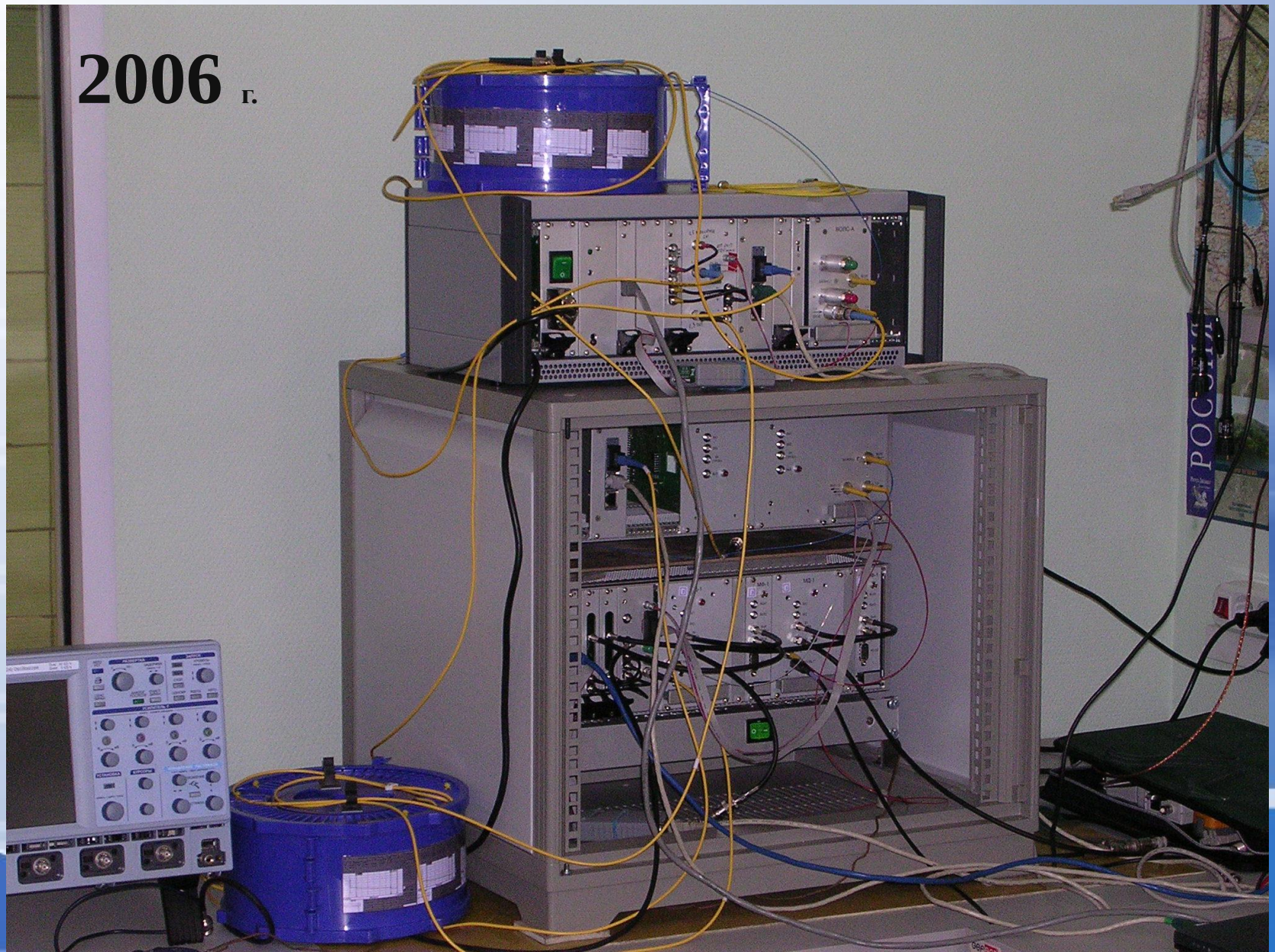
$$p(c|m) = p(c)$$

$$c = m \oplus k$$

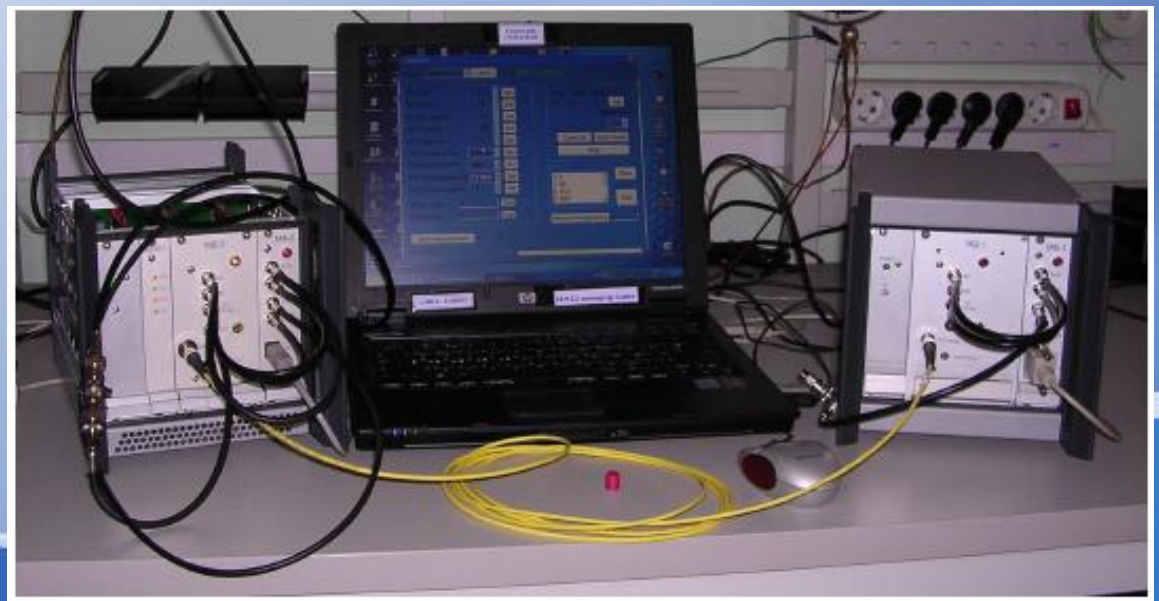
$$m = c \oplus k = (m \oplus k) \oplus k$$

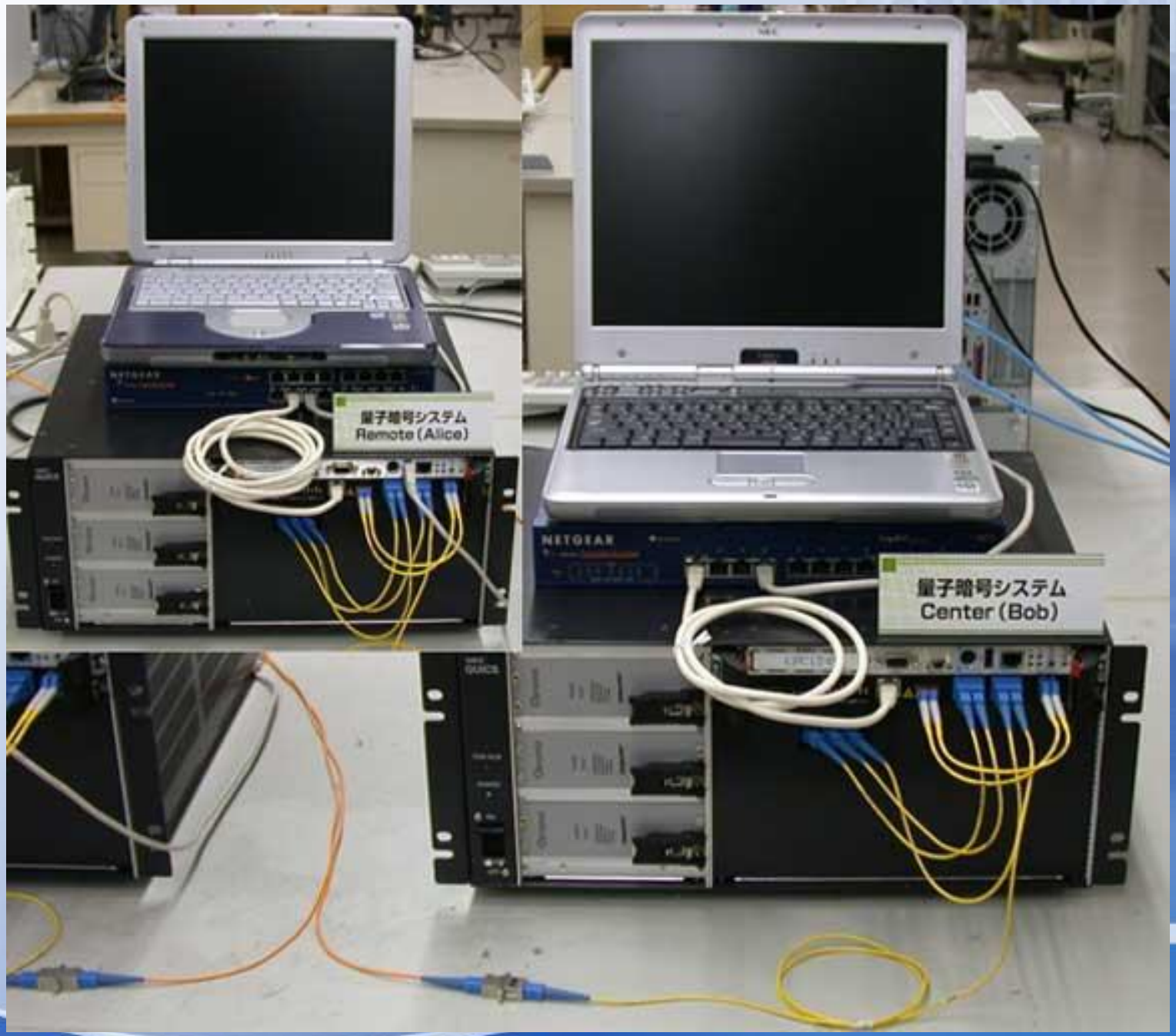
Цель квантового распределения ключей – создание сетевой полностью автоматизированной системы смены ключей без участия оператора (после запуска системы человек никогда не имеет доступа к ключам, используемым для шифрования)

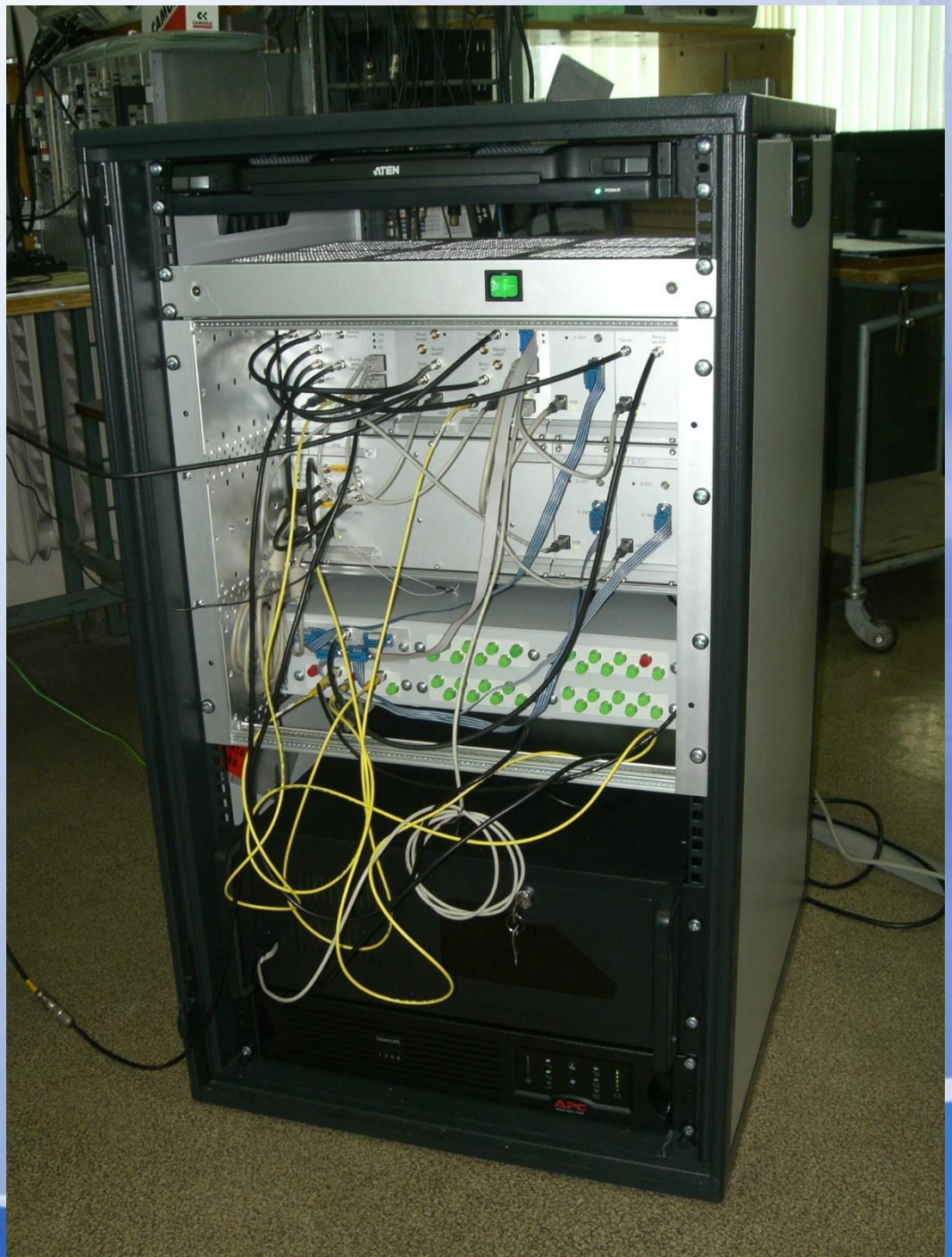
Как это выглядит сегодня и как может выглядеть в будущем.

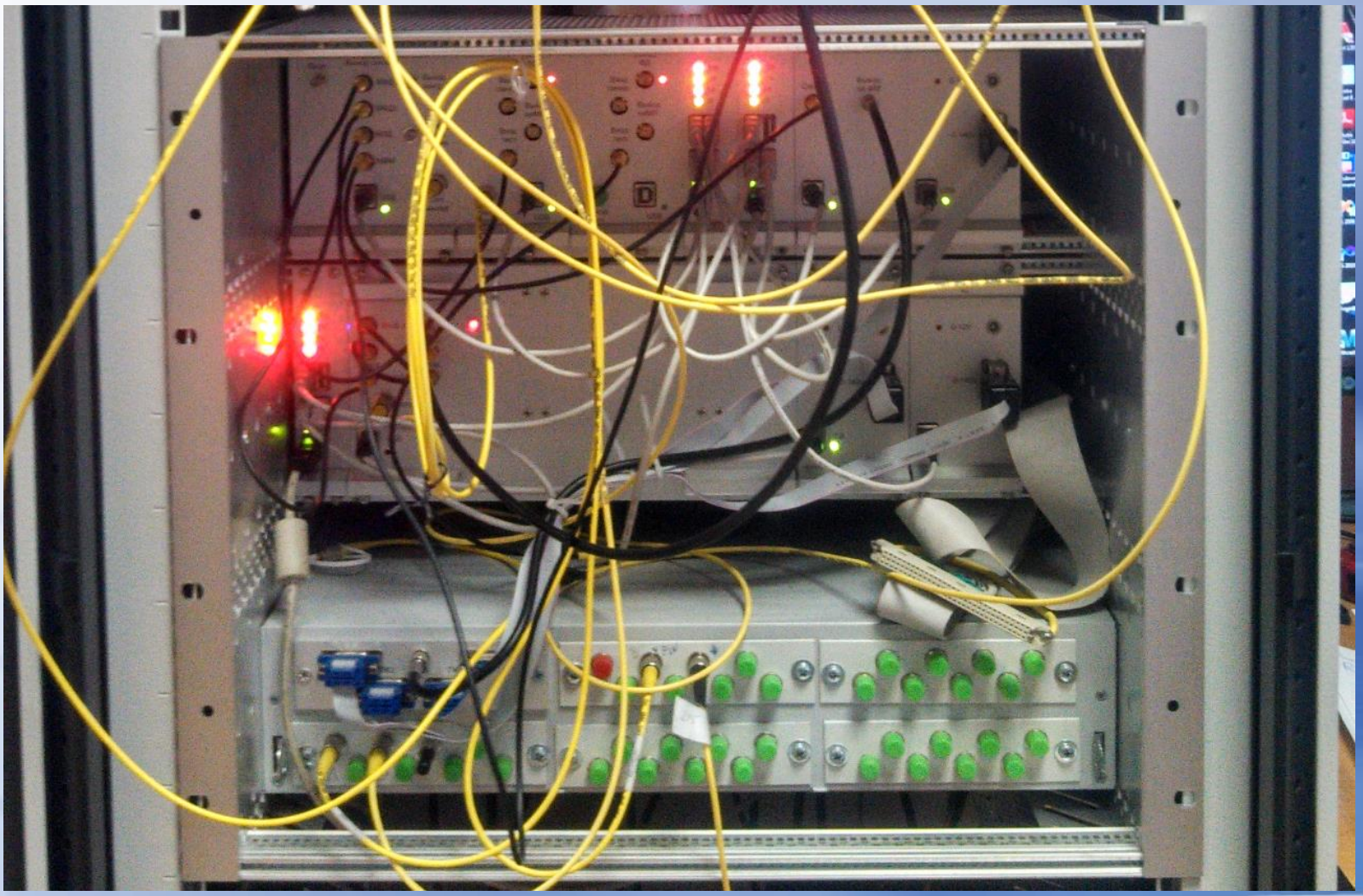


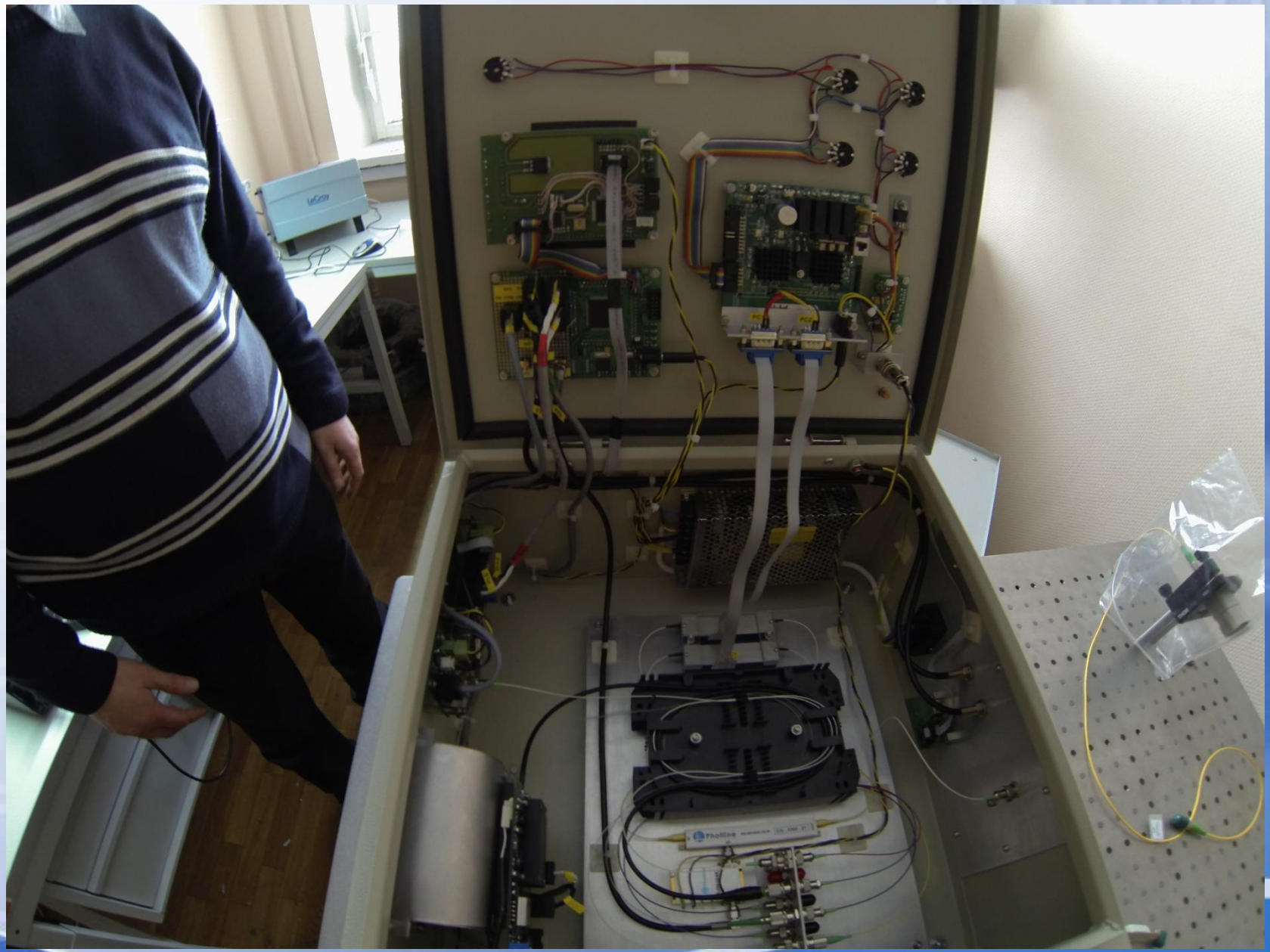

TRACO POWER
TEN 6WIR




量子暗号システム
Remote (Alice)
NETGEAR
量子暗号システム
Center (Bob)


ATEN
APC



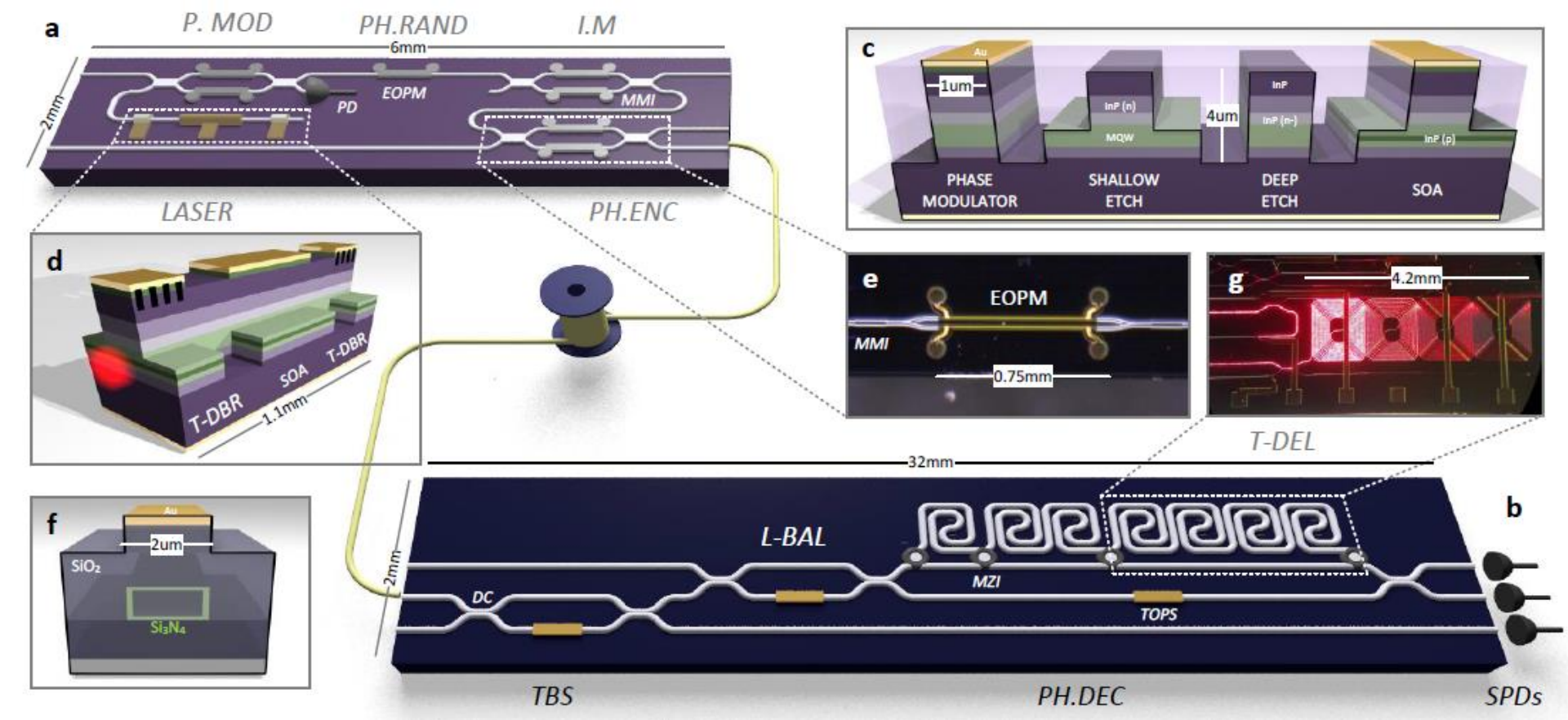


Как это будет выглядеть в будущем – контуры будущего уже явно просматриваются сегодня.

Качественный скачок в технологическом уровне -- переход на интегрально-оптическую платформу.

Chip-based Quantum Key Distribution

P. Sibson,[1,*] C. Erven,[1] M. Godfrey,[1] S. Miki,[2] T. Yamashita,[2] M. Fujiwara,[3] M. Sasaki,[3] H. Terai,[2] M. G. Tanner,[4] C. M. Natarajan,[4] R. H. Hadfield,[4] J. L. O'Brien,[1] and M. G. Thompson[1,†]



3. Как это работает – общие принципы

Фундаментальные запреты квантовой механики.

1) Неизвестное квантовое состояние нельзя скопировать (с вероятностью единица).
2) Любое измерение с целью отличить одно квантовое состояние от другого искажает состояние. Важно -- возмущение гарантируется для неортогональных квантовых состояний.

$$|\varphi_0\rangle \otimes |A\rangle \rightarrow |\varphi_0\rangle \otimes |\varphi_0\rangle \otimes |A_0\rangle$$

$$|\varphi_1\rangle \otimes |A\rangle \rightarrow |\varphi_1\rangle \otimes |\varphi_1\rangle \otimes |A_1\rangle$$

$$\langle \varphi_0 | \varphi_1 \rangle \neq 0$$

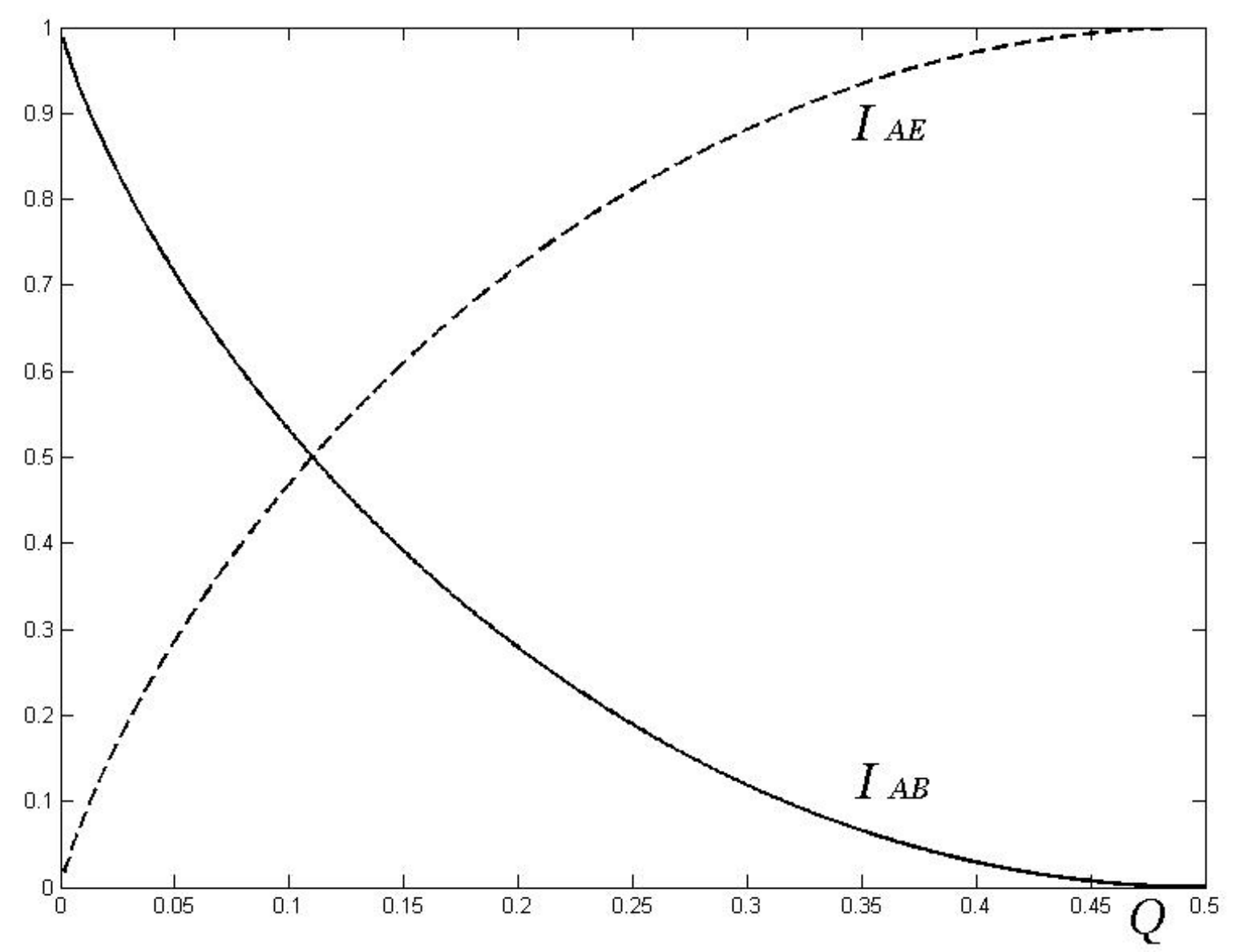
$$|\varphi_1\rangle \otimes |A\rangle \rightarrow U(|\varphi_1\rangle \otimes |A\rangle) = |\varphi_1\rangle \otimes |A_1\rangle$$

$$|\varphi_0\rangle \otimes |A\rangle \rightarrow U(|\varphi_0\rangle \otimes |A\rangle) = |\varphi_0\rangle \otimes |A_0\rangle$$

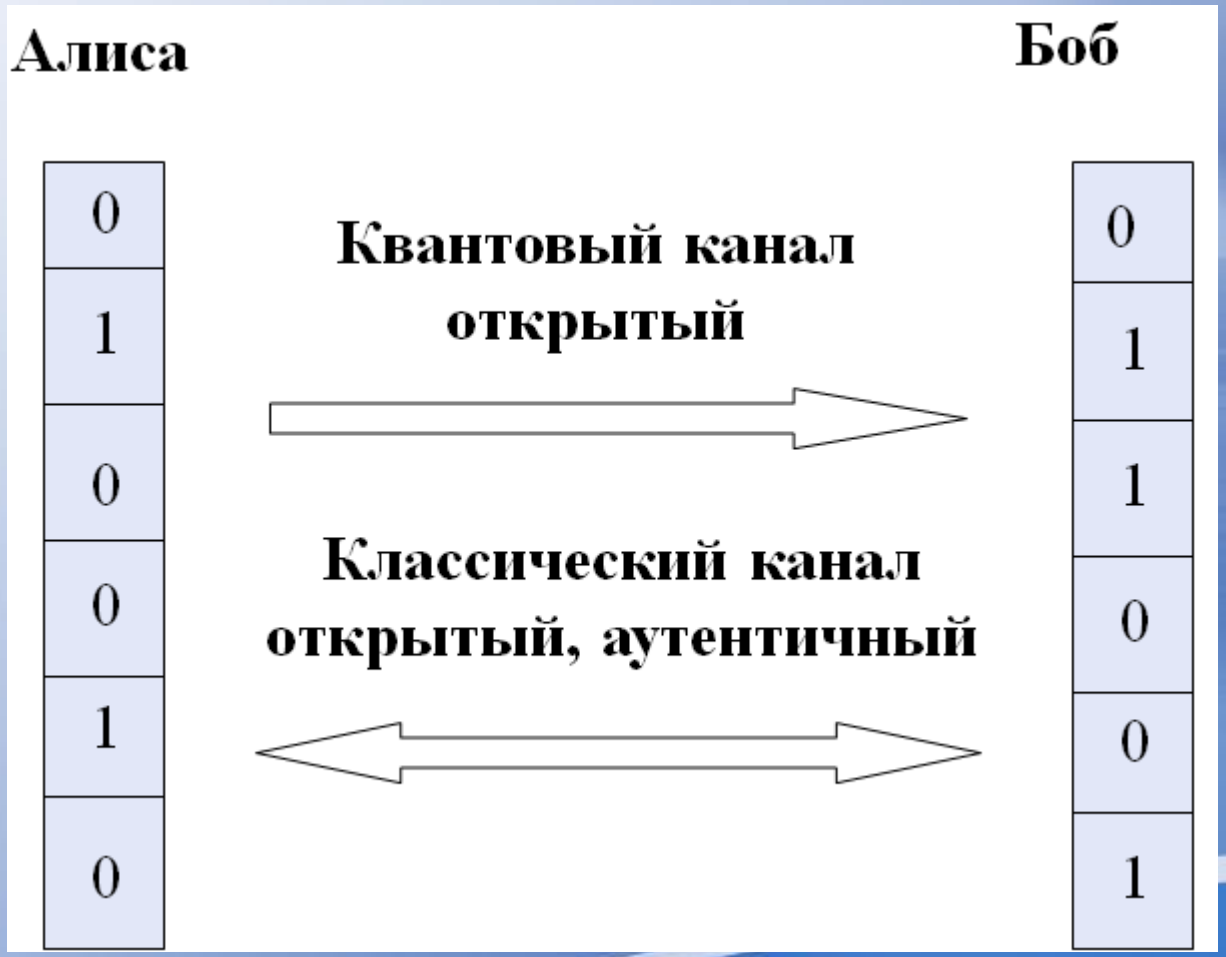
$$|A_0\rangle \neq |A_1\rangle$$

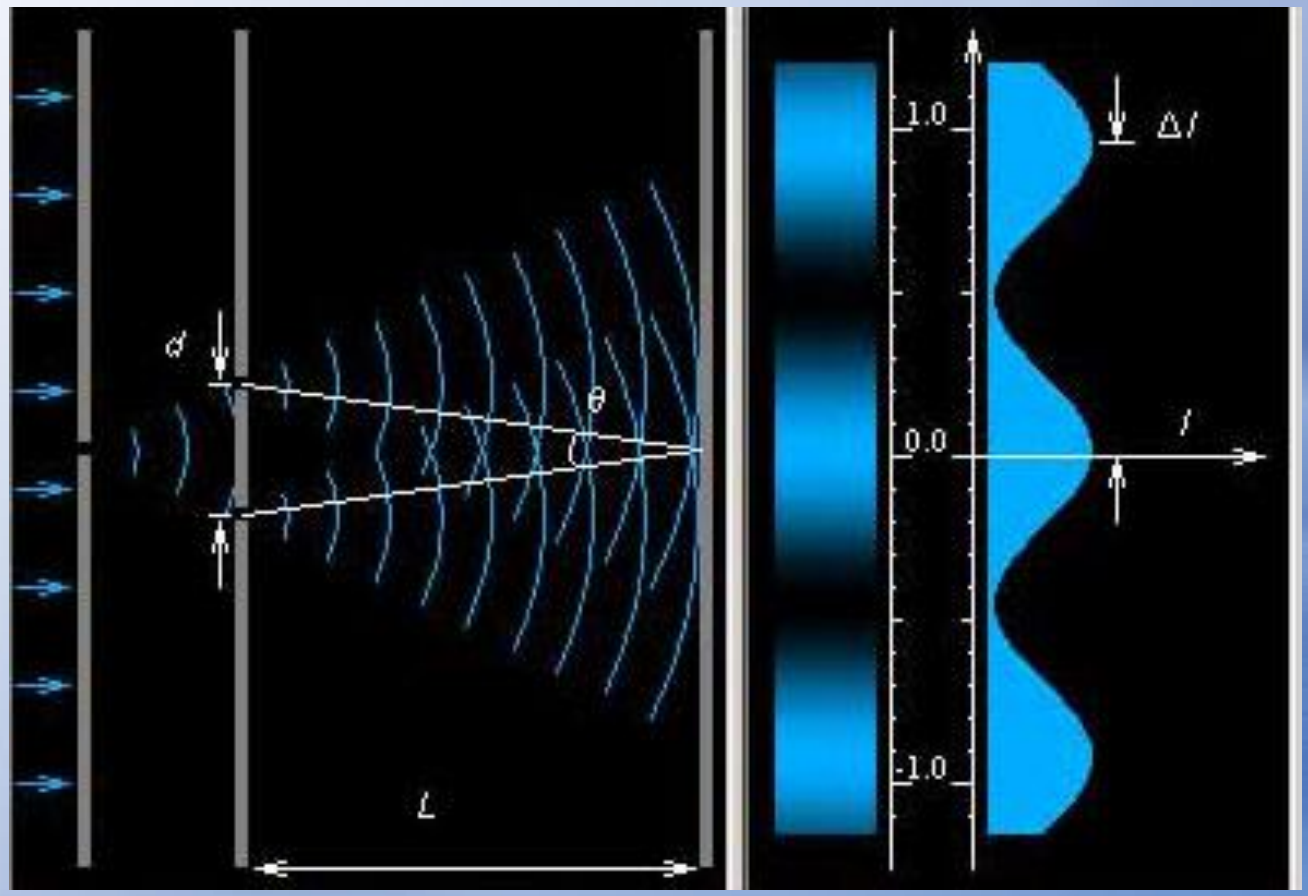
Следствия для распределения секретных ключей.

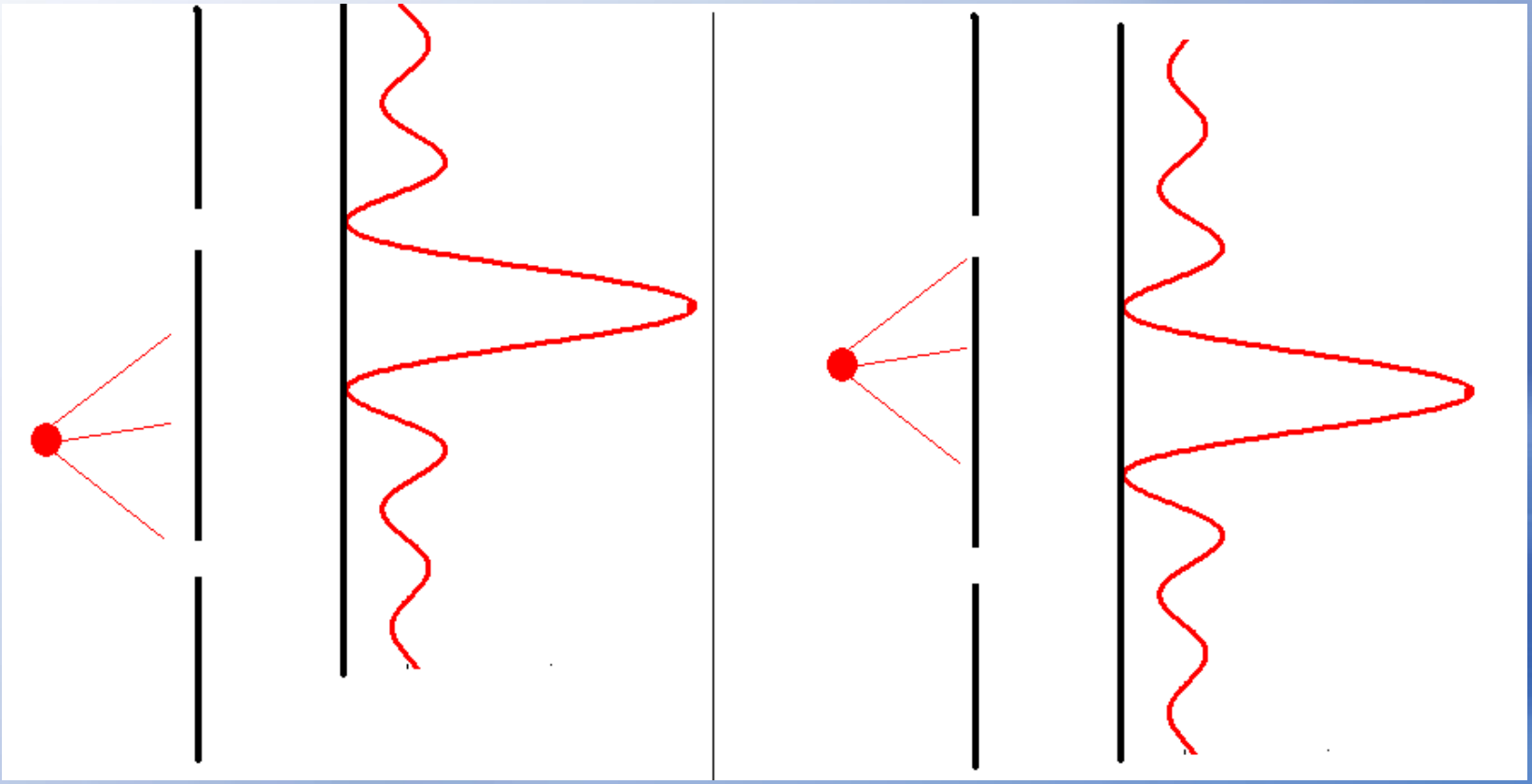
1) Любое вторжение в канал связи приводит к возмущению квантовых состояний, которое детектируется – приводит к ошибке в первичных ключах.
2) Ошибка связана с верхней фундаментальной границей информации, которая уходит к подслушивателю при данной наблюдаемой вероятности ошибок на приемной стороне.
3) Если вероятность ошибки меньше критической величины, то информация между передатчиком и приемником больше, чем между передатчиком и подслущивателем. Разность – секретный ключ.


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

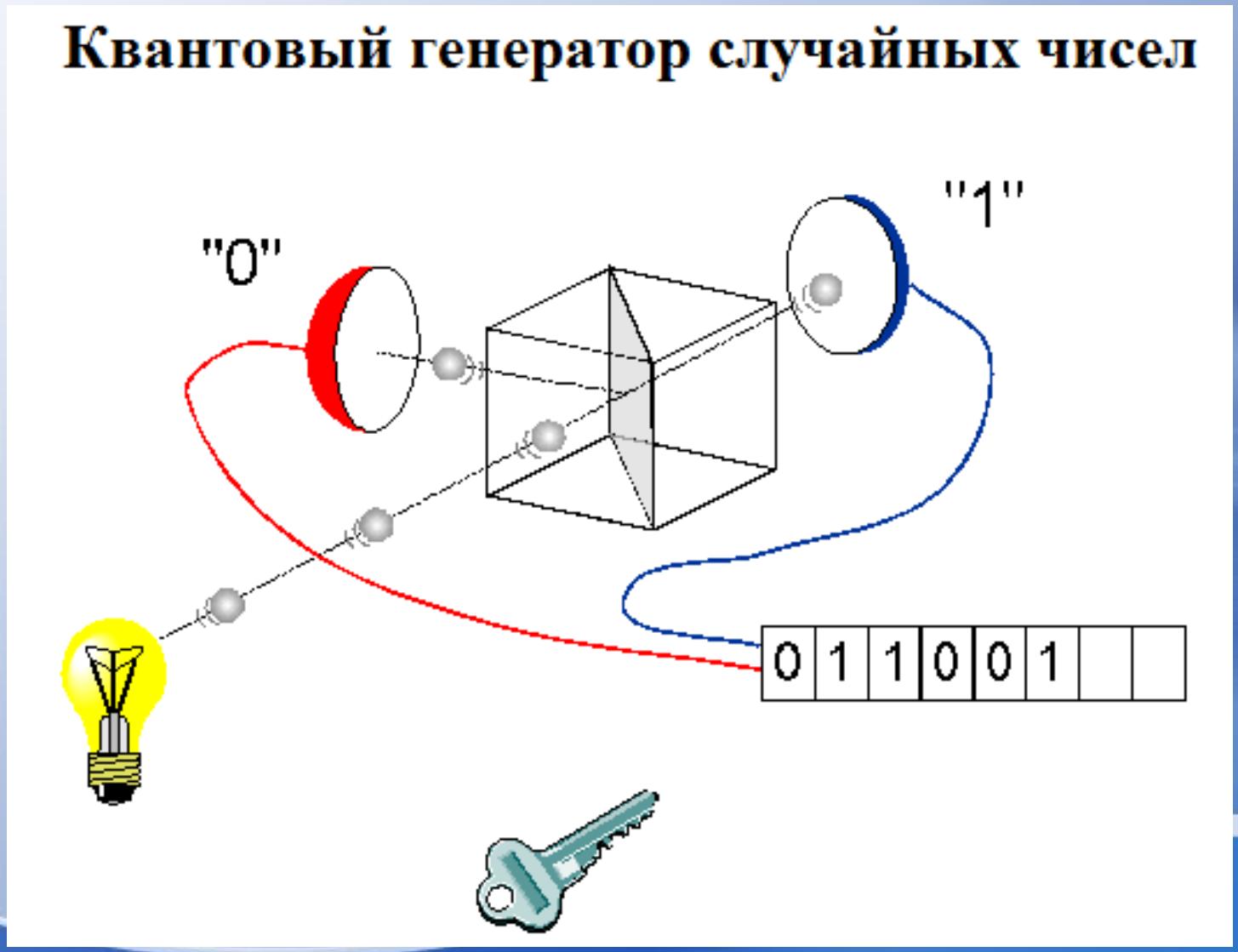
Квантовая криптография = Квантовое распределение ключей = Согласование случайных последовательностей




d
θ
L
1.0
Δl
0.0
l
-1.0



Необходимость квантового генератора случайных чисел.



Research Article | Vol. 32, No. 8 / August 2015 / Journal of the Optical Society of America B | 1743

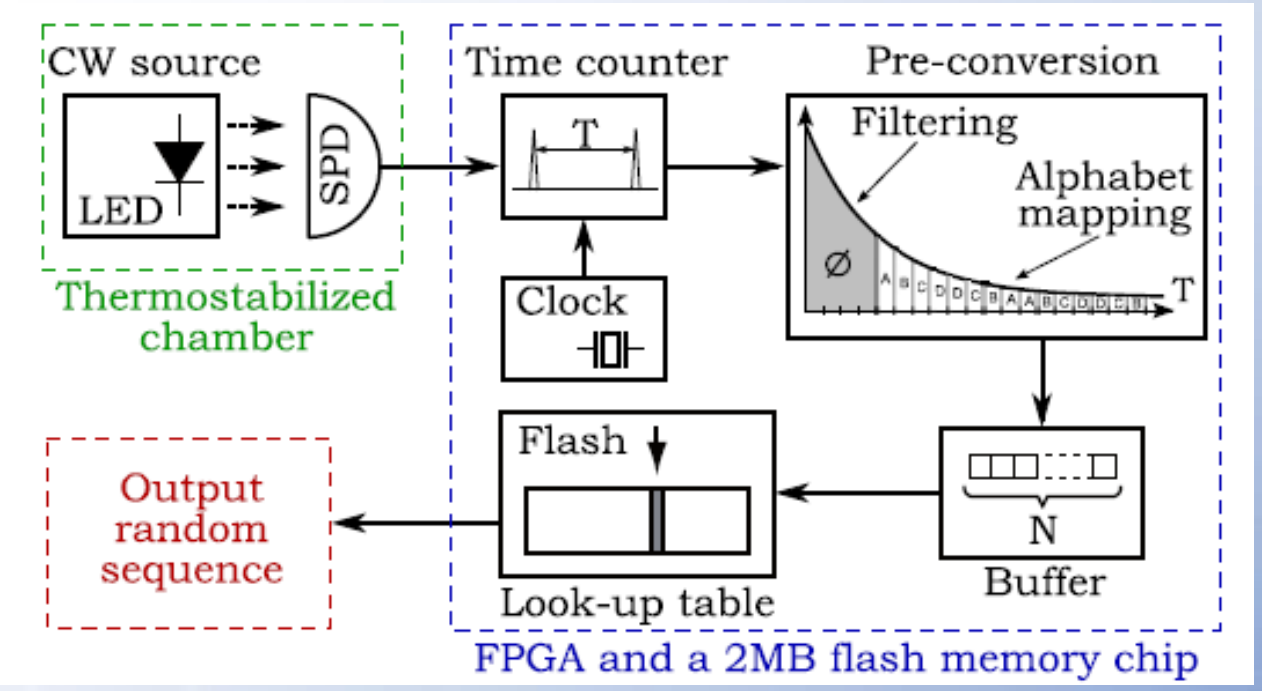
Journal of the Optical Society of America B

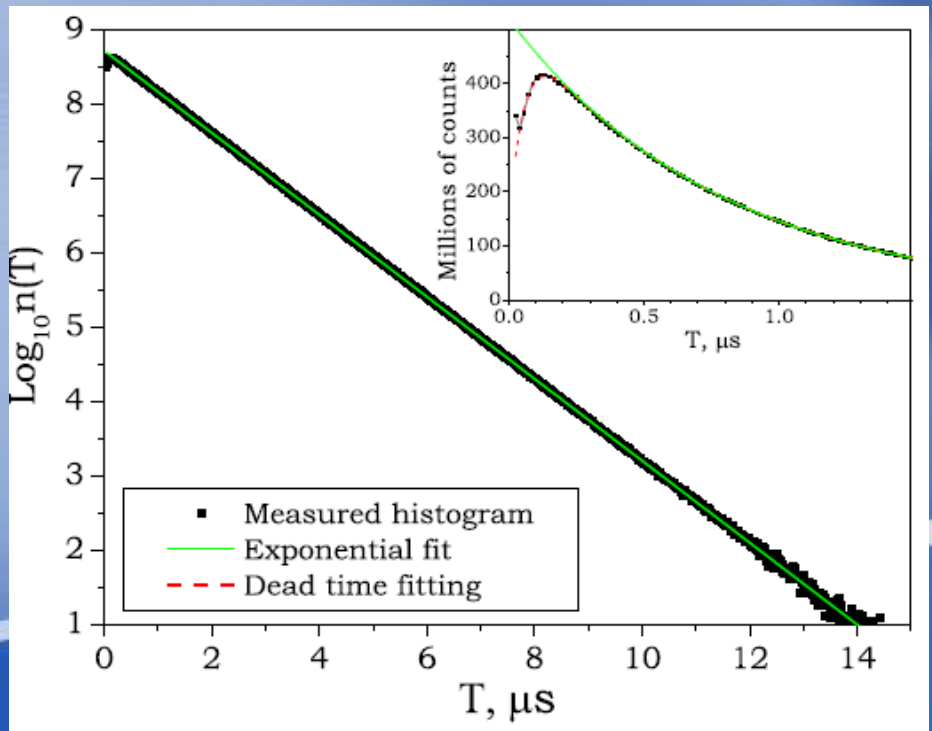
OPTICAL PHYSICS

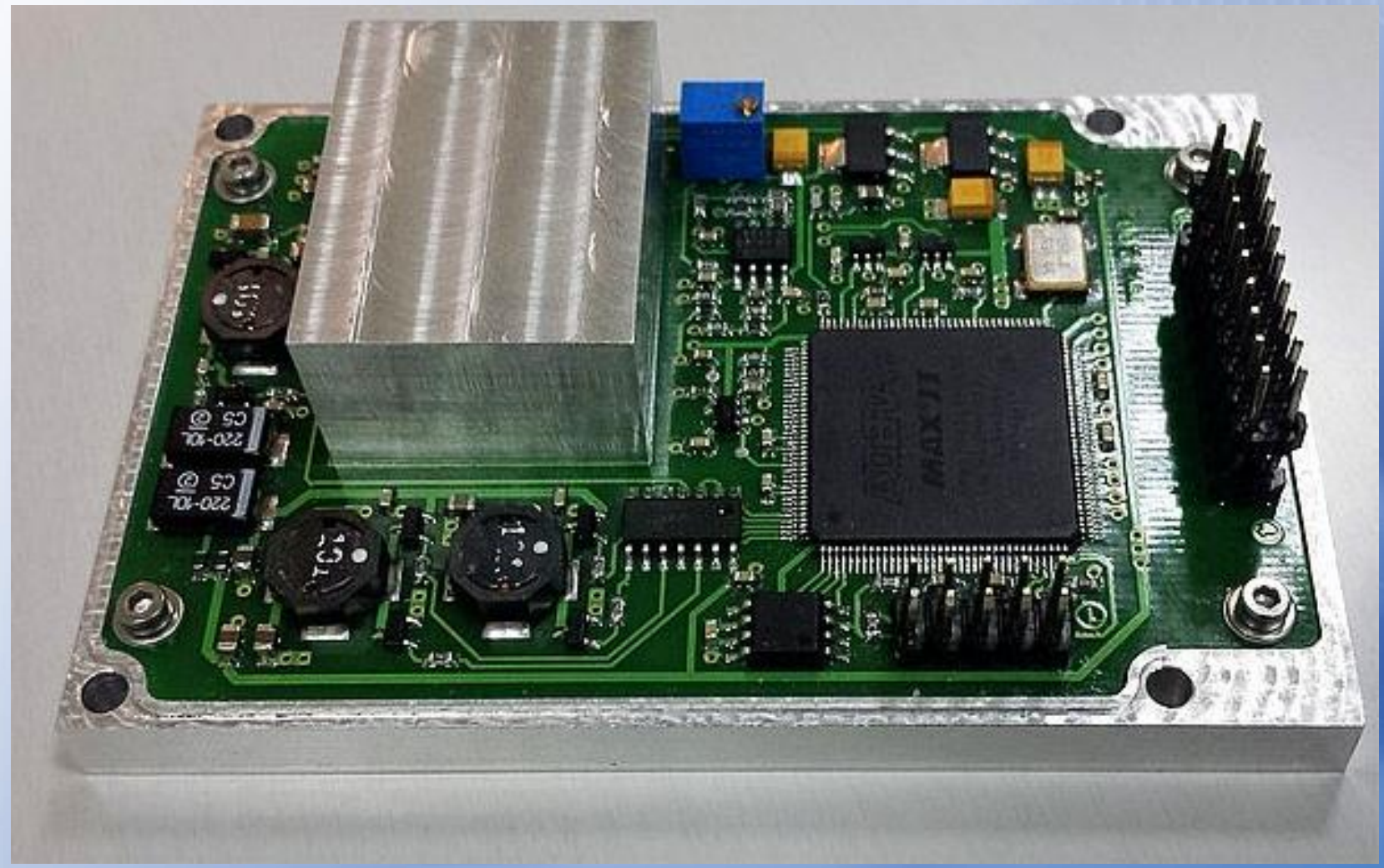
Minimalist design of a robust real-time quantum random number generator

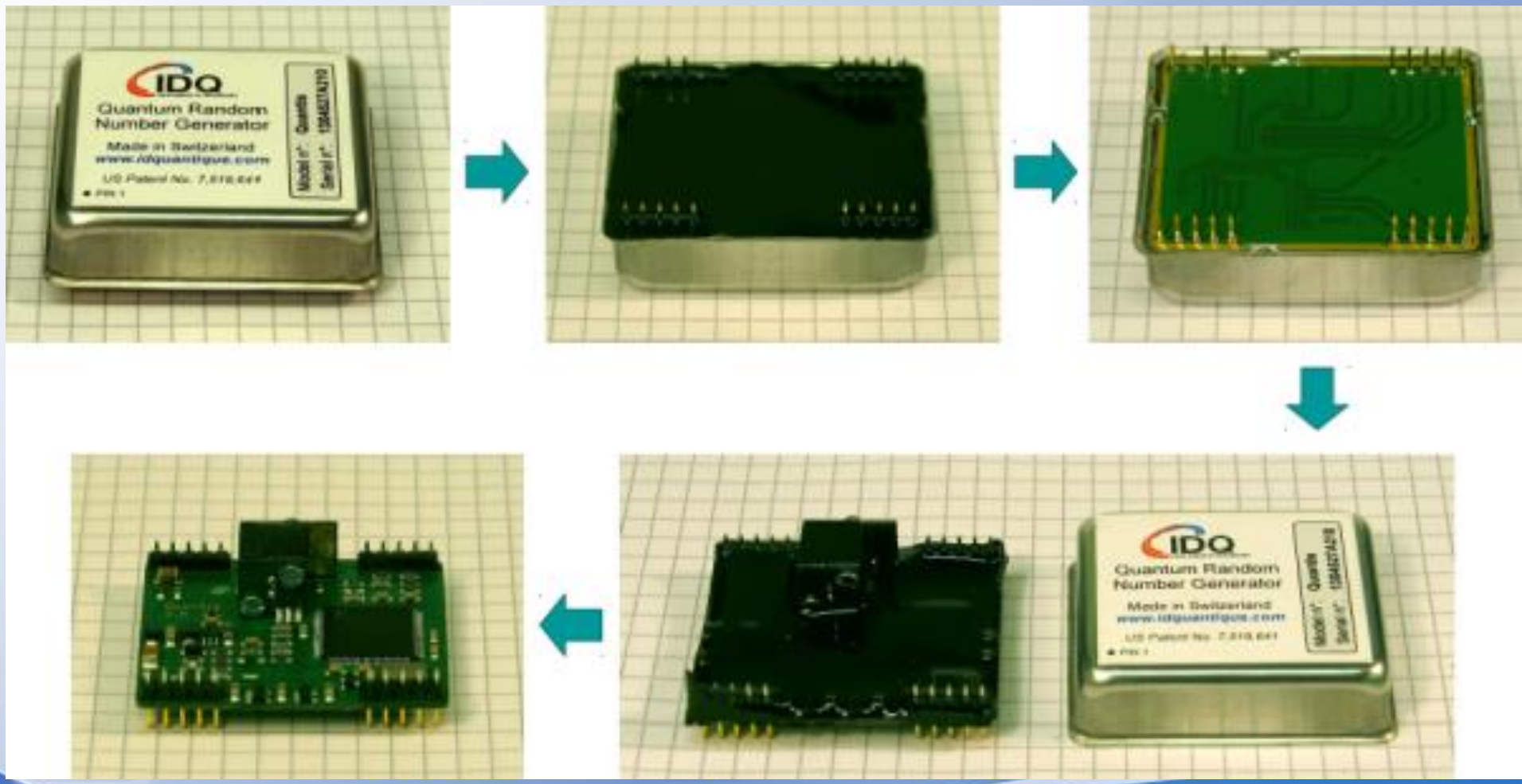
K. S. Kravtsov,[1,2,*] I. V. Radchenko,[1,2] S. P. Kulik,[1] and S. N. Molotkov[3,4,5]

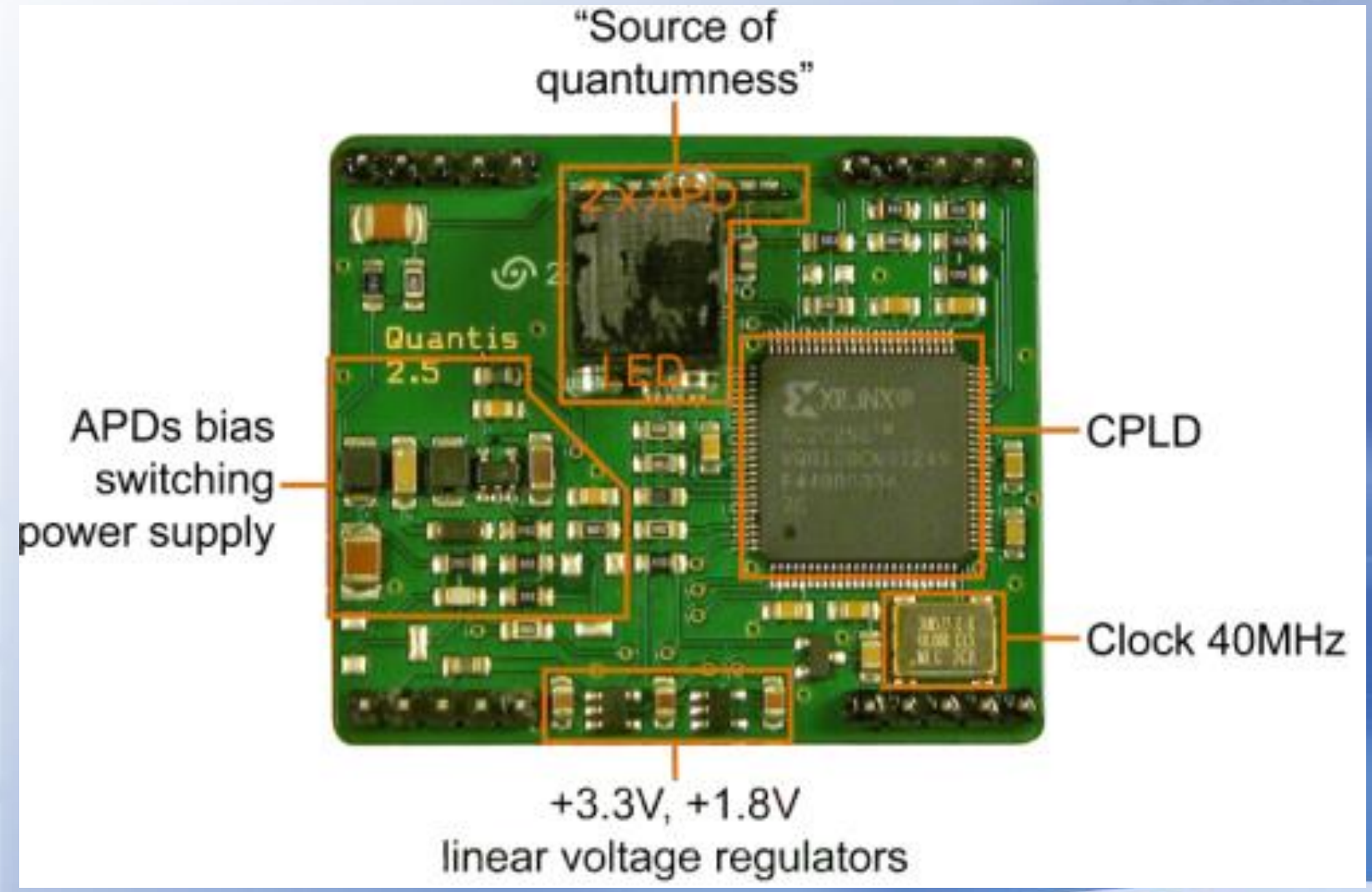
(4,0,0,0)	(3,1,0,0)	(2,2,0,0)	(2,1,1,0)	(1,1,1,1)
AAAA → ∅	BBBC → 00	AACC → 00	ABBD → 000 } 8	ABCD → 0000 } 16
	BBCB → 01	ACAC → 01	ABDB → 001	ABDC → 0001
	BCBB → 10	ACCA → 10	... ...	... ...
	CBBB → 11	CAAC → 11	BDAB → 111	CBDA → 1111
		CACA → 0	BDBA → 00	CDAB → 000 } 8
		CCAA → 1	DABB → 01	CDBA → 001
			DBAB → 10	... ...
			DBBA → 11	DCBA → 111

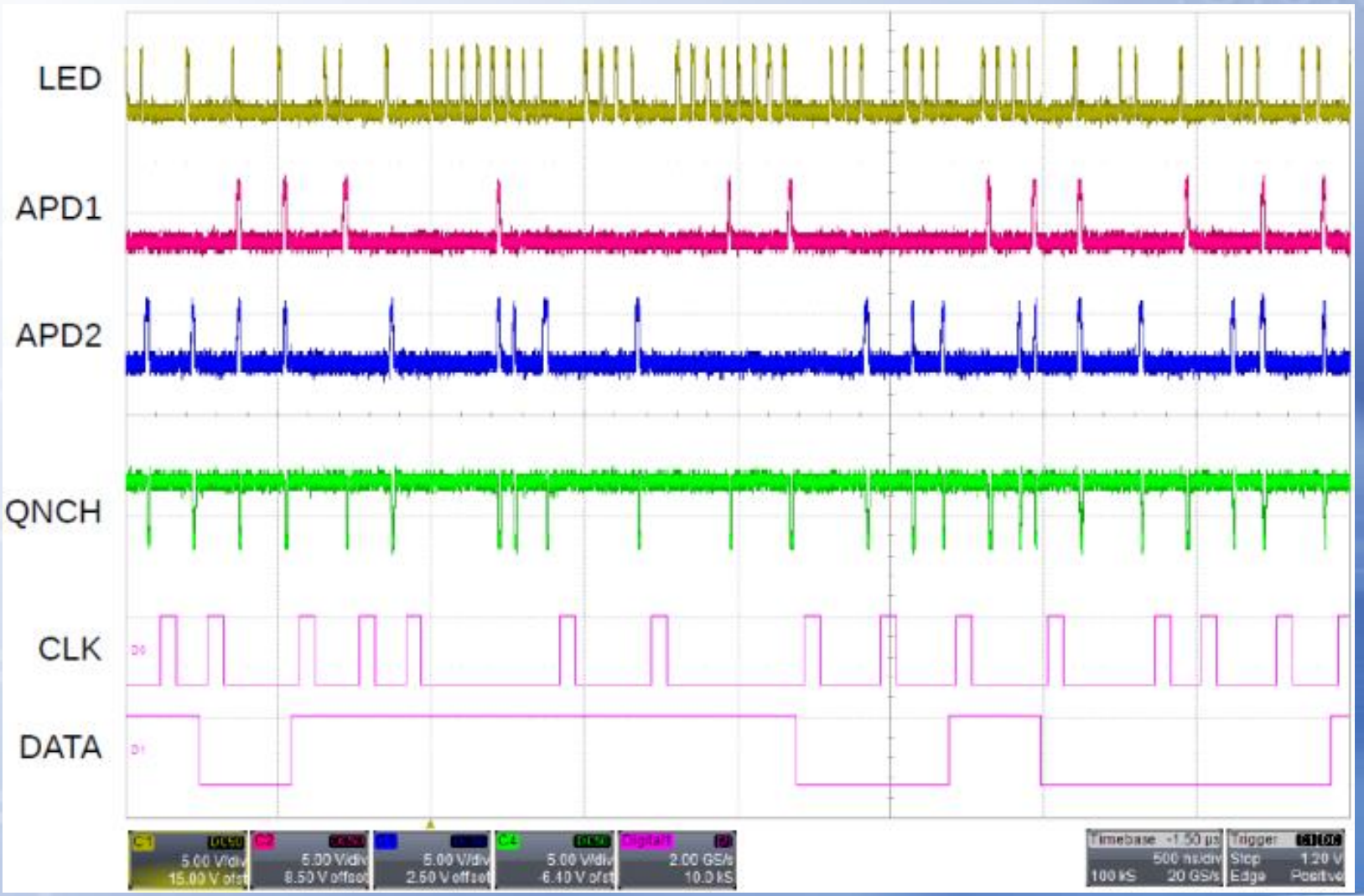

CW source
LED
SPD
Thermostabilized chamber
Time counter
T
Clock
Pre-conversion
Filtering
Alphabet mapping
Ø
T
Flash
Look-up table
N
Buffer
Output random sequence
FPGA and a 2MB flash memory chip


Log10n(T)
T, μs
Millions of counts
T, μs
Measured histogram
Exponential fit
Dead time fitting


220-10L
C5
220-10L
C5

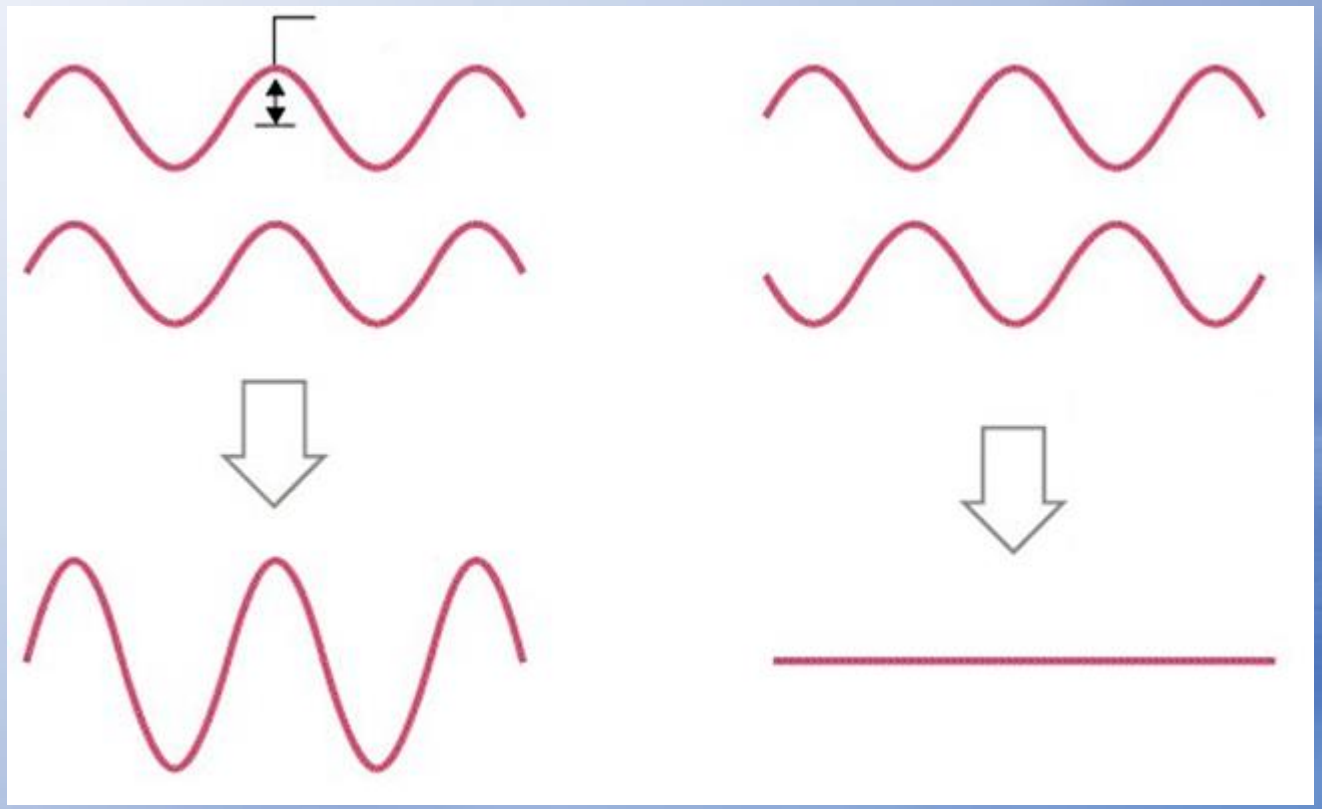

IDQ
Quantum Random
Number Generator
Made in Switzerland
www.idquantique.com
IDQ
Quantum Random
Number Generator
Made in Switzerland
www.idquantique.com


"Source of quantumness"
2x APD
LED
Quantis 2.5
APDs bias switching power supply
CPLD
Clock 40MHz
+3.3V, +1.8V linear voltage regulators


LED
APD1
APD2
QNCH
CLK
DATA
5.00 V/div
15.00 V offset
5.00 V/div
8.50 V offset
5.00 V/div
2.50 V offset
5.00 V/div
6.40 V offset
2.00 GS/s
10.0 kS
Timebase -1.50 µs
500 ns/div
100 kS
20 GS/s
Trigger
Stop
1.20 V
Edge
Positive

№	$N(x_n = 0)$	$N(x_n = 1)$	$\frac{N(0) - N(1)}{N(0) + N(1)}$	$N(x_n \hat{} x_{n-1} = 0)$	$N(x_n \hat{} x_{n-1} = 1)$	$\frac{N(\hat{}0) - N(\hat{}1)}{N(\hat{}0) + N(\hat{}1)}$
1	536'873'035	536'868'789	4.0e-6	536'698'339	537'043'484	-3.2e-4
2	536'882'563	536'859'261	2.2e-5	536'787'990	536'953'833	-1.5e-4
3	536'867'999	536'873'825	-5.4e-6	536'828'388	536'913'435	-7.9e-5
4	536'892'157	536'849'667	4.0e-5	536'666'863	537'074'960	-3.8e-4
5	536'869'215	536'872'609	-3.2e-6	536'839'365	536'902'458	-5.9e-5

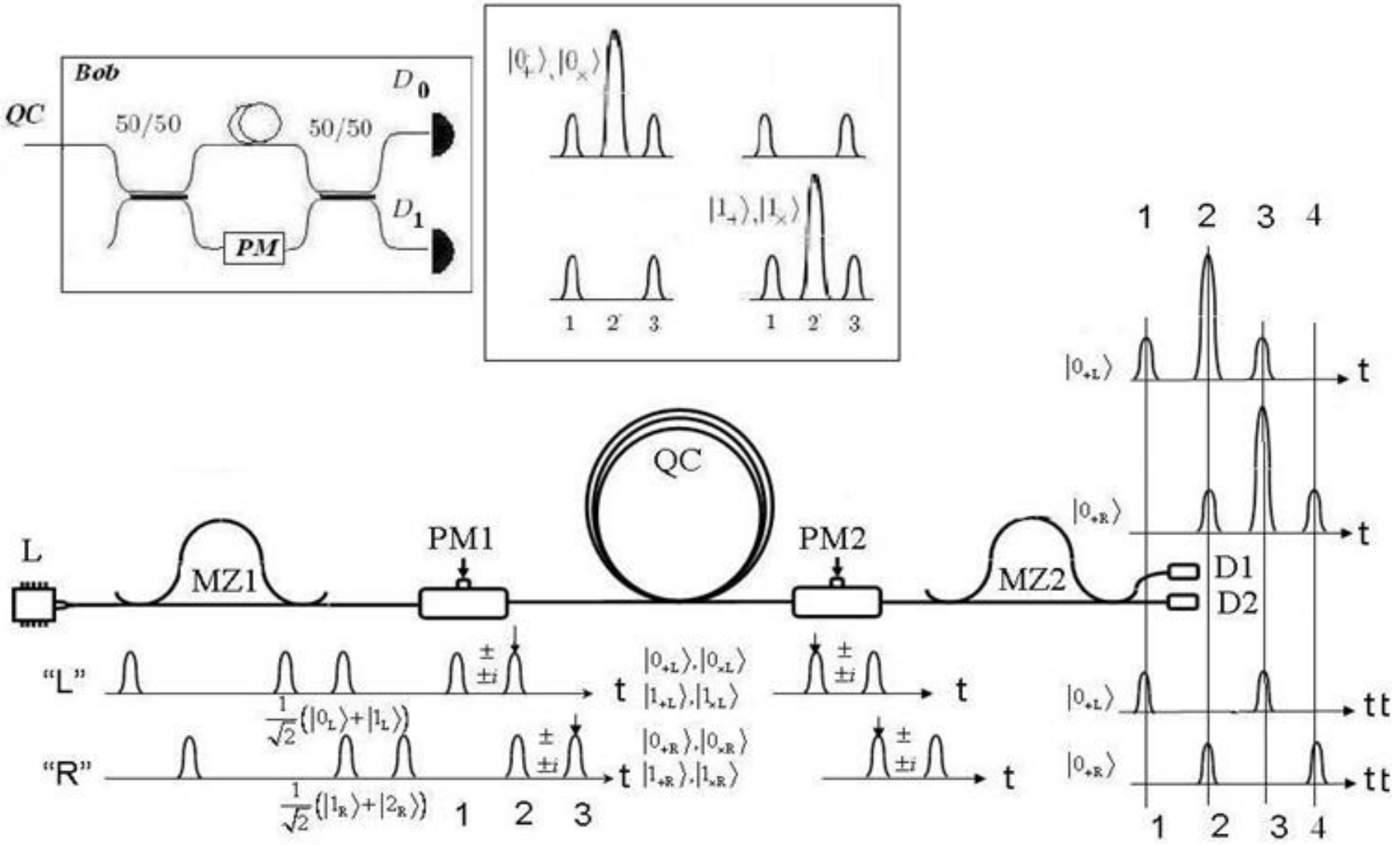
Фазовое кодирование

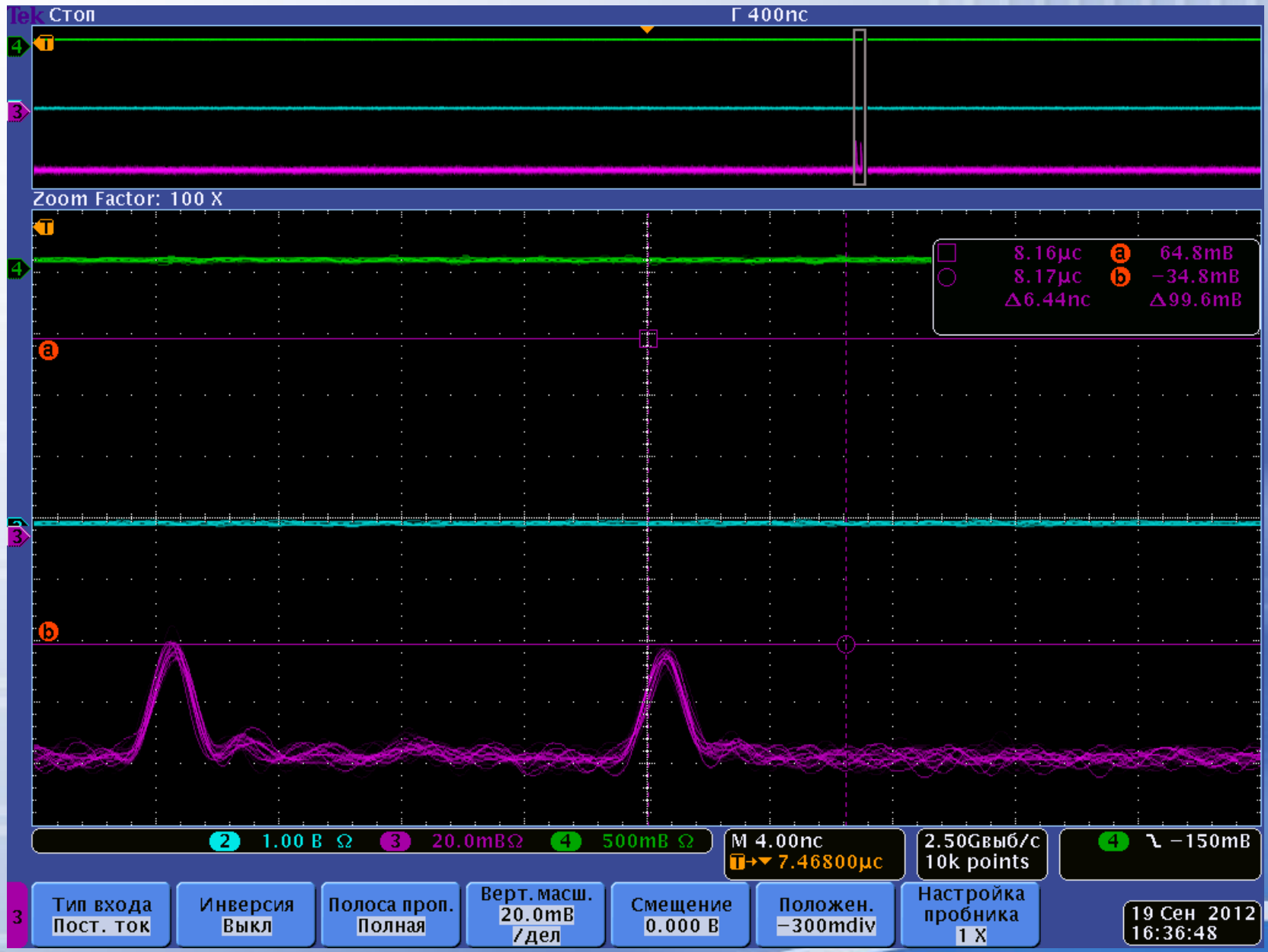


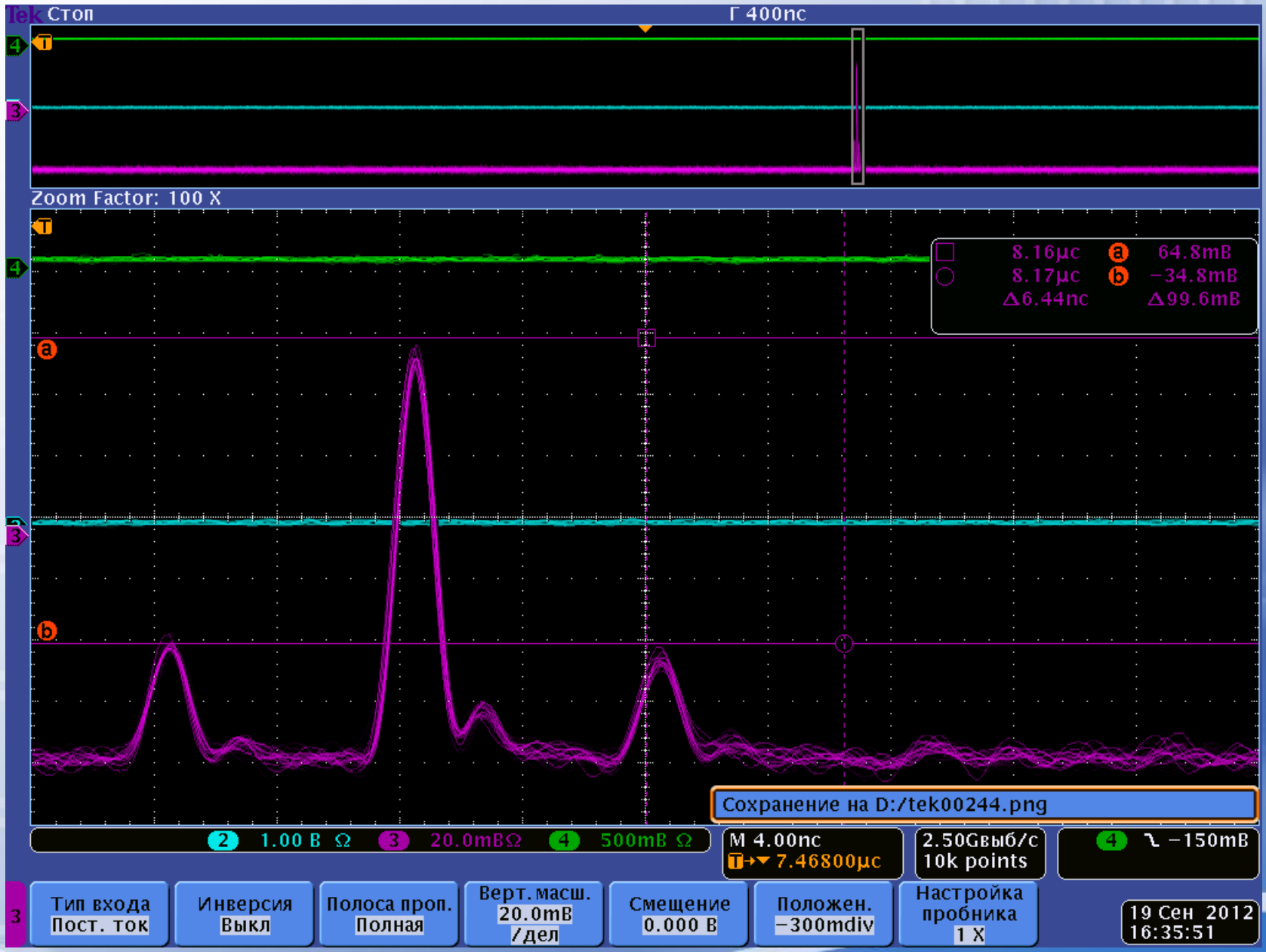
Фазово-временное кодирование

$$Q = \frac{1-V}{2}$$

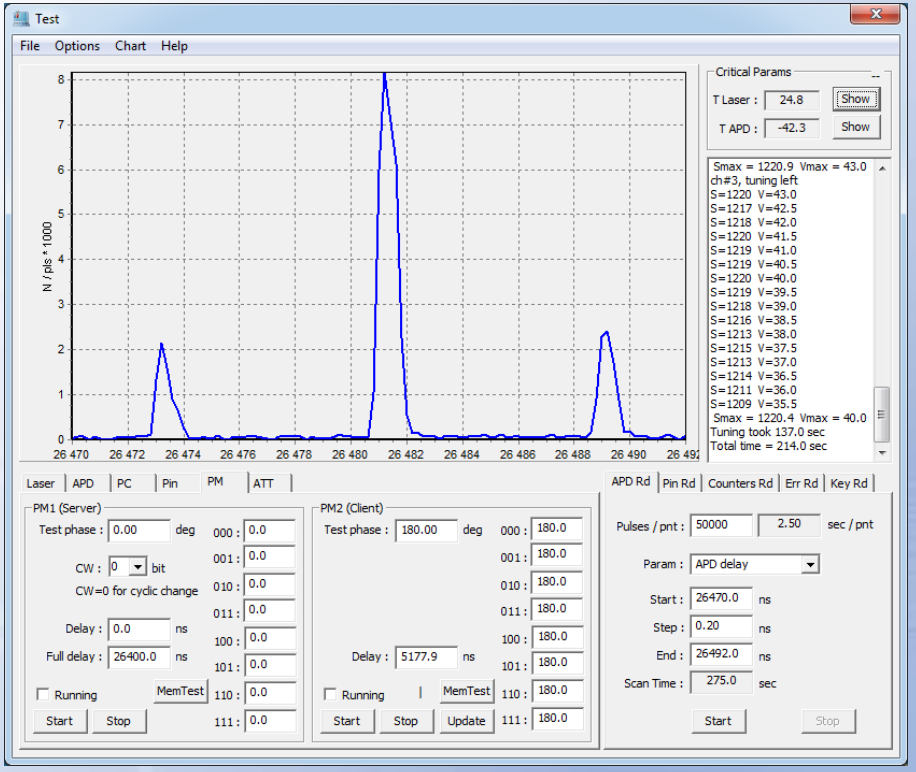
$$V = \frac{I_{D_1} - I_{D_2}}{I_{D_1} + I_{D_2}}$$

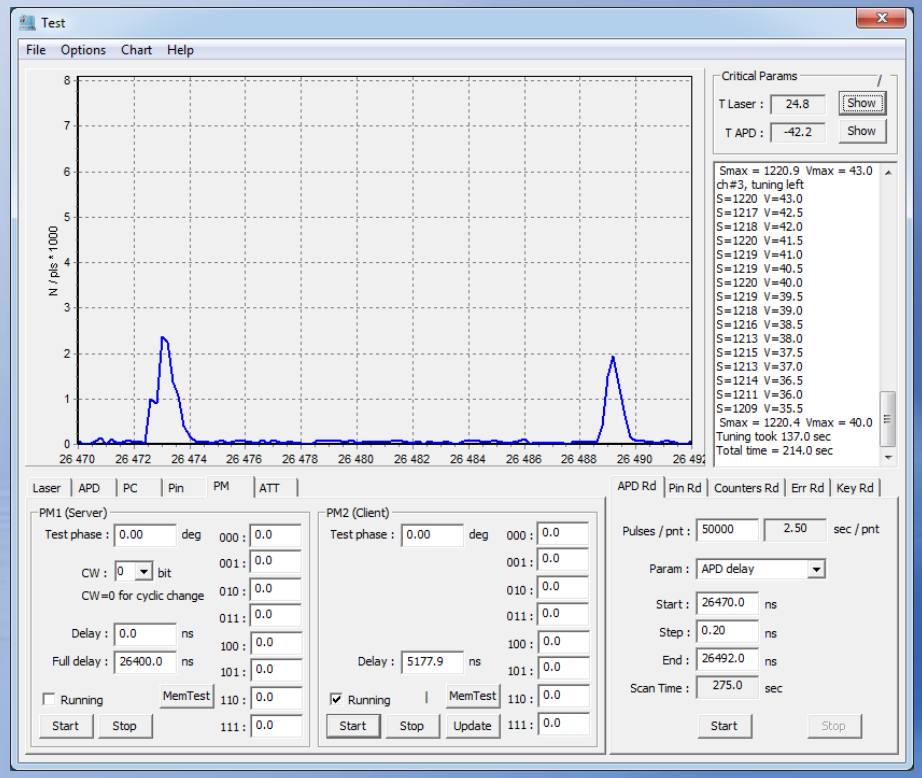


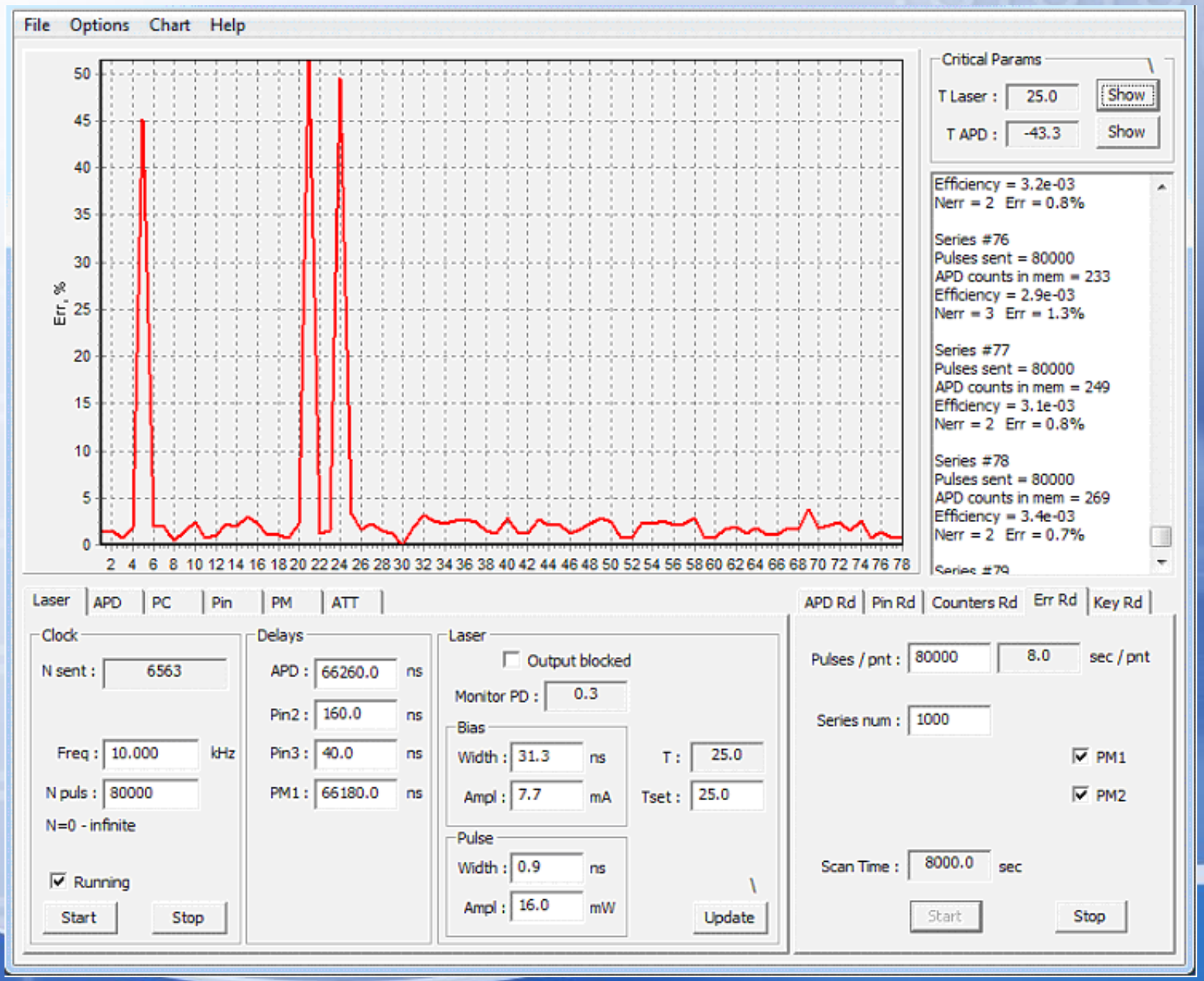

Tek Стоп
Г 400nc
Zoom Factor: 100 X
8.16µc
64.8mB
8.17µc
−34.8mB
Δ6.44nc
Δ99.6mB
2 1.00 В Ω
3 20.0mBΩ
4 500mB Ω
M 4.00nc
T→▼ 7.46800µc
2.50Gвыб/с
10k points
4 ∖ −150mB
3
Тип входа
Пост. ток
Инверсия
Выкл
Полоса проп.
Полная
Верт. масш.
20.0mB
/дел
Смещение
0.000 В
Положен.
−300mdiv
Настройка
пробника
1 X
19 Сен 2012
16:36:48


Tek Стоп
Г 400nc
Zoom Factor: 100 X
8.16µc a 64.8mB
8.17µc b −34.8mB
Δ6.44nc Δ99.6mB
Сохранение на D:/tek00244.png
2 1.00 В Ω 3 20.0mBΩ 4 500mB Ω
M 4.00nc
T→▼ 7.46800µc
2.50Gвыб/с
10k points
4 ∖ −150mB
Тип входа
Пост. ток
Инверсия
Выкл
Полоса проп.
Полная
Верт. масш.
20.0mB
/дел
Смещение
0.000 В
Положен.
−300mdiv
Настройка
пробника
1 X
19 Сен 2012
16:35:51

Пример однофотонной интерференции






File
Options
Chart
Help
Err, %
50
45
40
35
30
25
20
15
10
5
0
2 4 6 8 10 12 14 16 18 20 22 24 26 28 30 32 34 36 38 40 42 44 46 48 50 52 54 56 58 60 62 64 66 68 70 72 74 76 78
Critical Params
T Laser : 25.0
Show
T APD : -43.3
Show
Efficiency = 3.2e-03
Nerr = 2 Err = 0.8%
Series #76
Pulses sent = 80000
APD counts in mem = 233
Efficiency = 2.9e-03
Nerr = 3 Err = 1.3%
Series #77
Pulses sent = 80000
APD counts in mem = 249
Efficiency = 3.1e-03
Nerr = 2 Err = 0.8%
Series #78
Pulses sent = 80000
APD counts in mem = 269
Efficiency = 3.4e-03
Nerr = 2 Err = 0.7%
Laser
APD
PC
Pin
PM
ATT
Clock
N sent : 6563
Freq : 10.000 kHz
N puls : 80000
N=0 - infinite
Running
Start
Stop
Delays
APD : 66260.0 ns
Pin2 : 160.0 ns
Pin3 : 40.0 ns
PM1 : 66180.0 ns
Laser
Output blocked
Monitor PD : 0.3
Bias
Width : 31.3 ns
Ampl : 7.7 mA
T : 25.0
Tset : 25.0
Pulse
Width : 0.9 ns
Ampl : 16.0 mW
Update
APD Rd
Pin Rd
Counters Rd
Err Rd
Key Rd
Pulses / pnt : 80000 8.0 sec / pnt
Series num : 1000
PM1
PM2
Scan Time : 8000.0 sec
Start
Stop

Доказательства секретности ключей. Криптостойкость относительно любых атак, включая квантовую память и квантовый компьютер.

Любой протокол КРК содержит три стадии.

1) **Согласование базисов.**
2) **Коррекцию ошибок.**
3) **Сжатие очищенных ключей – усилением секртености.**

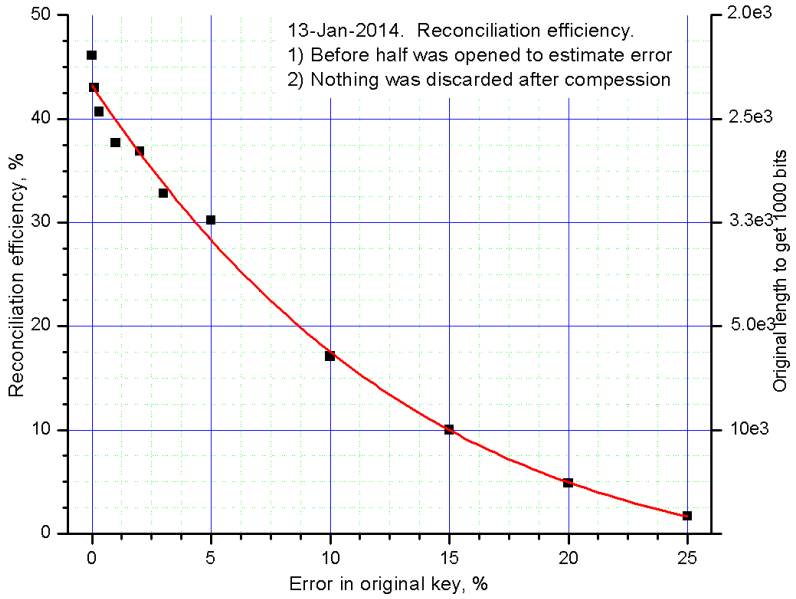
Коды Хэмминга с доп. проверкой на четность с сохранением конфиденциальности

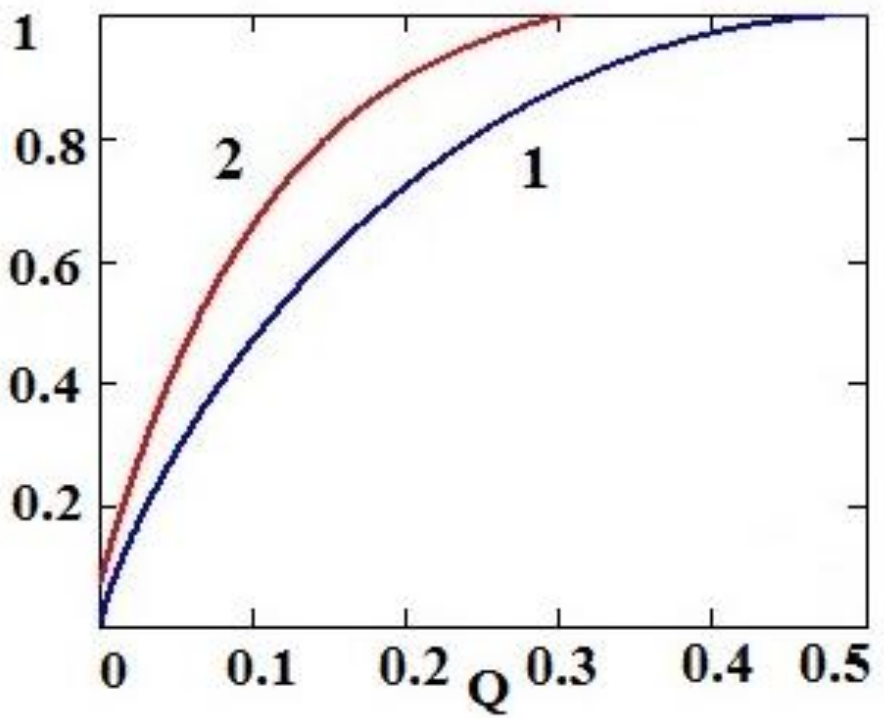
$$S_d = S_a \oplus S_b \neq \{0\}^m.$$

$$h^{(3)} = \begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}$$

$$h_{i,j}^{(m)} = \left\lfloor \frac{j}{2^{i-1}} \right\rfloor \pmod 2$$

$$S_i = \left(\sum_{j=1}^{N_h} X_j h_{i,j}^{(m)} \right) \pmod 2 \in \{0,1\}^m$$


13-Jan-2014. Reconciliation efficiency.
1) Before half was opened to estimate error
2) Nothing was discarded after compession
Reconciliation efficiency, %
Original length to get 1000 bits
Error in original key, %
0
10
20
30
40
50
5
15
25
2.0e3
2.5e3
3.3e3
5.0e3
10e3


1
0.8
0.6
0.4
0.2
0
0.1
0.2
0.3
0.4
0.5
Q
2
1

Секретность и корректность ключей.

$$\mathcal{X}_A = \{0,1\}^n \qquad \mathcal{X}_B = \{0,1\}^n.$$

Строка Боба содержит ошибки.

очищенный ключ $\mathcal{X} = \mathcal{X}_A$

$$\Pr(X_A \neq X_B) \leq 1/2^M = \varepsilon_{corr}$$

Сжатие очищенных ключей универсальными хэш-функциями второго порядка

$$\Pr_f[f(\hat{x}) = f(x)] \leq \frac{1}{|Z|} = 2^{-k}, \quad \hat{x} \neq x$$

Сжатие очищенных ключей

Функция сжатия g(X) - универсальная хэш-функция

g(X) - случайная функция (известна всем, в том числе и подслушивателю) .

1) x, a={0,1, ……..,0,0}

2) Реализация: x, a - элементы $GF(2^n)$, a - случайная строка бит длины n.

3) Умножение в GF(2) – r(x)=a*x(mod P(x)).

4) Взять отстаток r старших бит.

5) Ключ длины r.

Полиномы степени n<10 000.

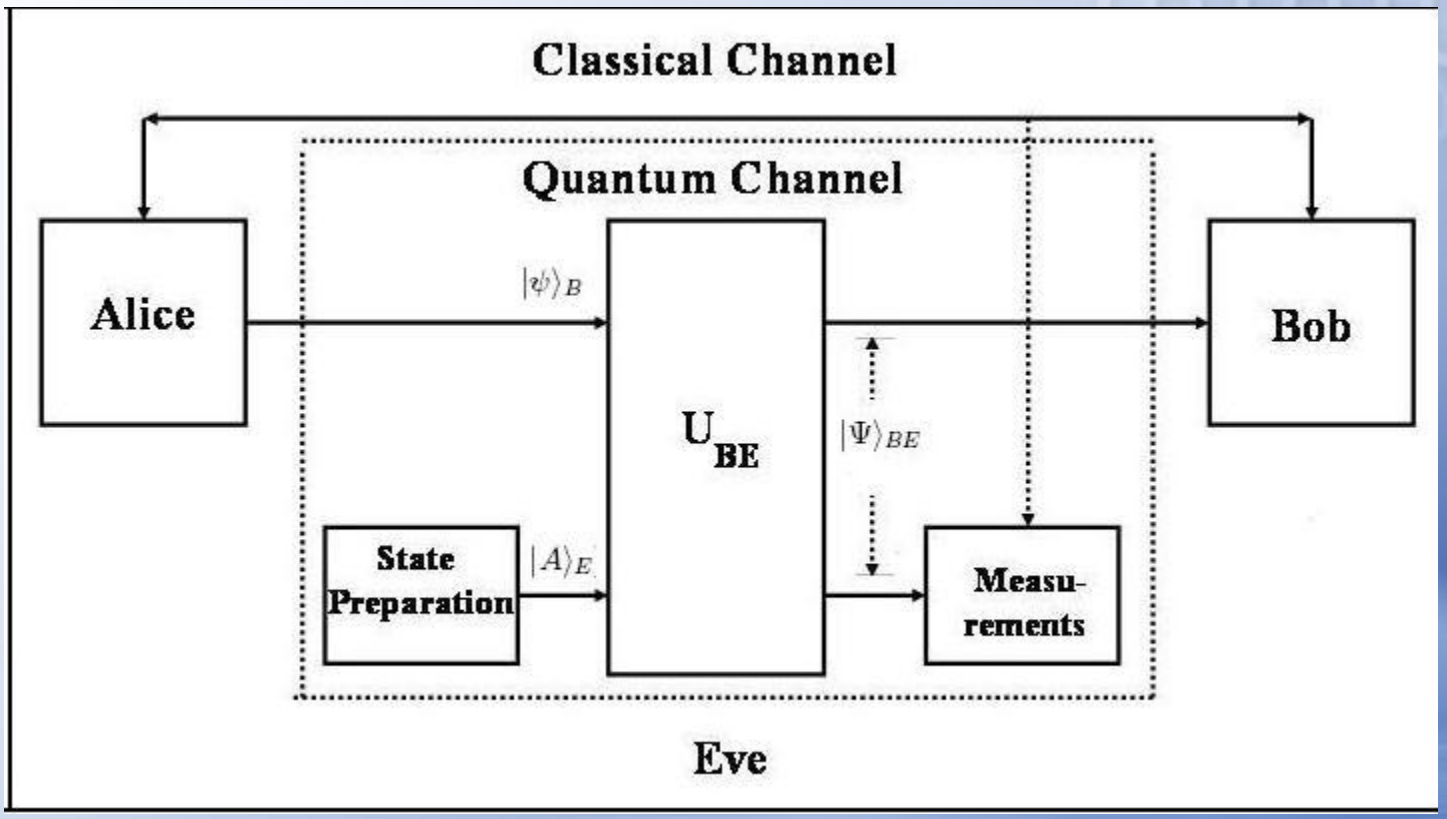
$$x^{9998}+x^{4013}+1$$

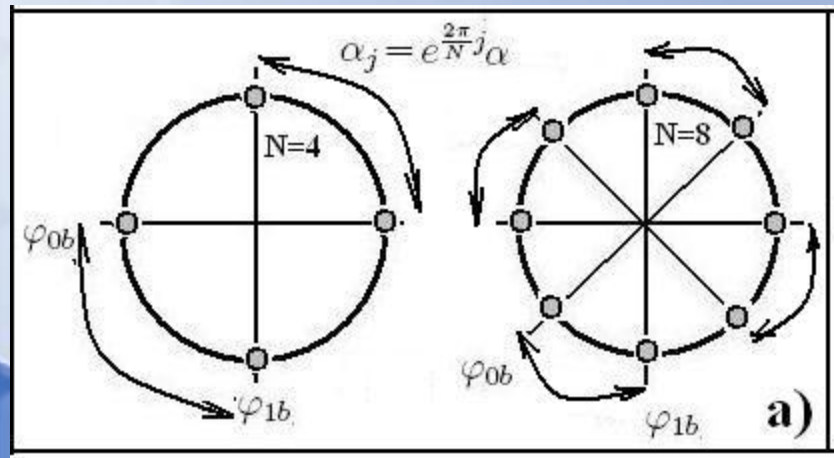
$$x^{9999}+x^{2951}+1$$

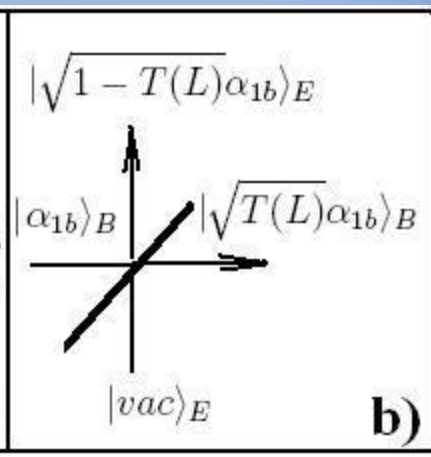
$$x^{10000}+x^{19}+x^{13}+x^{9}+1$$

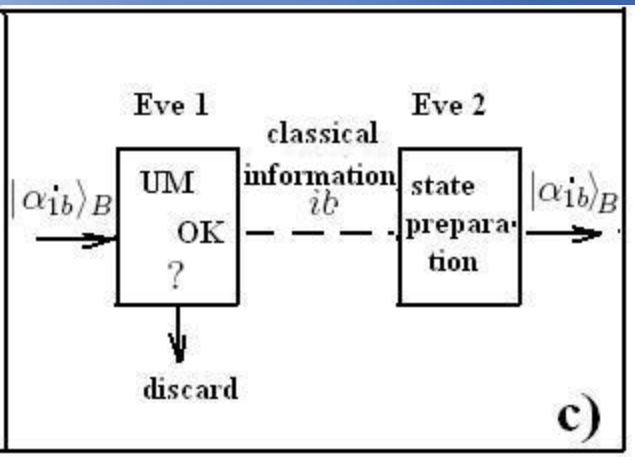
Протоколы и секретность.

1) BB84.
2) B92.
3) SARG.
4) Decoy State.
5) Фазово-временной.
6) DPS – Differential Phase Shift.
7) COW – Coherent One Way.
8) CW – с непрерывными переменнымию
9) С реперным состоянием.
10) Релятивистская квантовая криптография.


Classical Channel
Quantum Channel
Alice
Bob
$|\psi\rangle_B$
U_{BE}
$|\Psi\rangle_{BE}$
State Preparation
$|A\rangle_E$
Measu-rements
Eve


$\alpha_j = e^{\frac{2\pi}{N}j}\alpha$
N=4
N=8
φ_{0b}
φ_{1b}
φ_{0b}
φ_{1b}
a)


$|\sqrt{1-T(L)}\alpha_{1b}\rangle_E$
$|\alpha_{1b}\rangle_B$
$|\sqrt{T(L)}\alpha_{1b}\rangle_B$
$|vac\rangle_E$
b)


Eve 1
Eve 2
classical information
ib
$|\alpha_{ib}\rangle_B$
UM
OK
?
discard
state preparation
$|\alpha_{ib}\rangle_B$
c)

Качественное пояснение природы секретности.

$$|\psi\rangle_{ABE} \in H_A \otimes H_B \otimes H_E$$

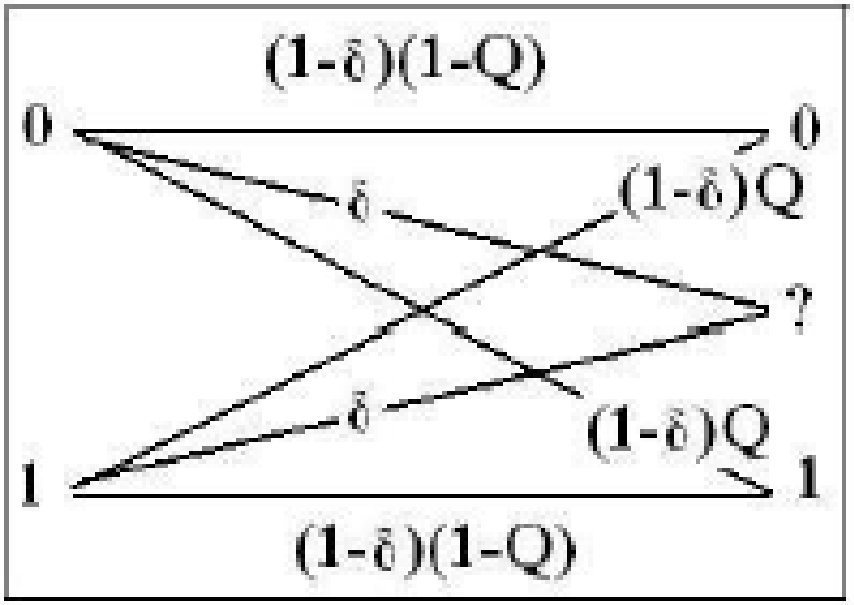
$$H(R_A \mid E) + H(L_A \mid B) \geq 2\log\frac{1}{c}$$

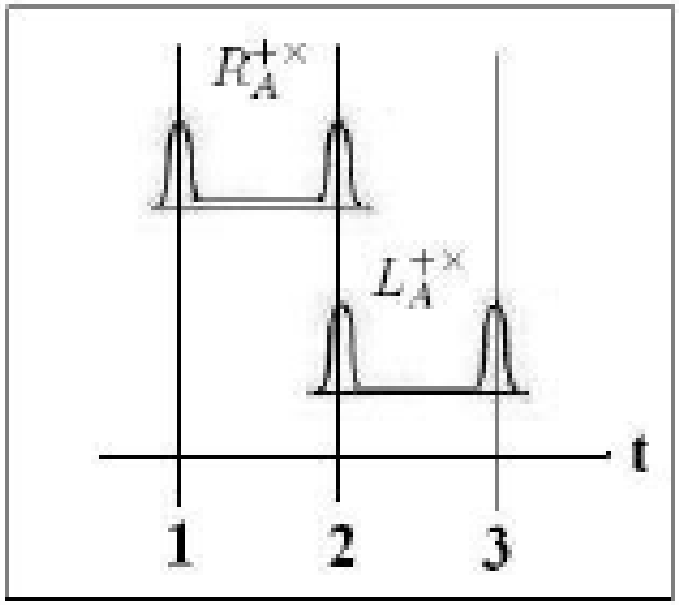
$$c = \max_{i,j} |_A\langle r_i | l_j \rangle_A|$$

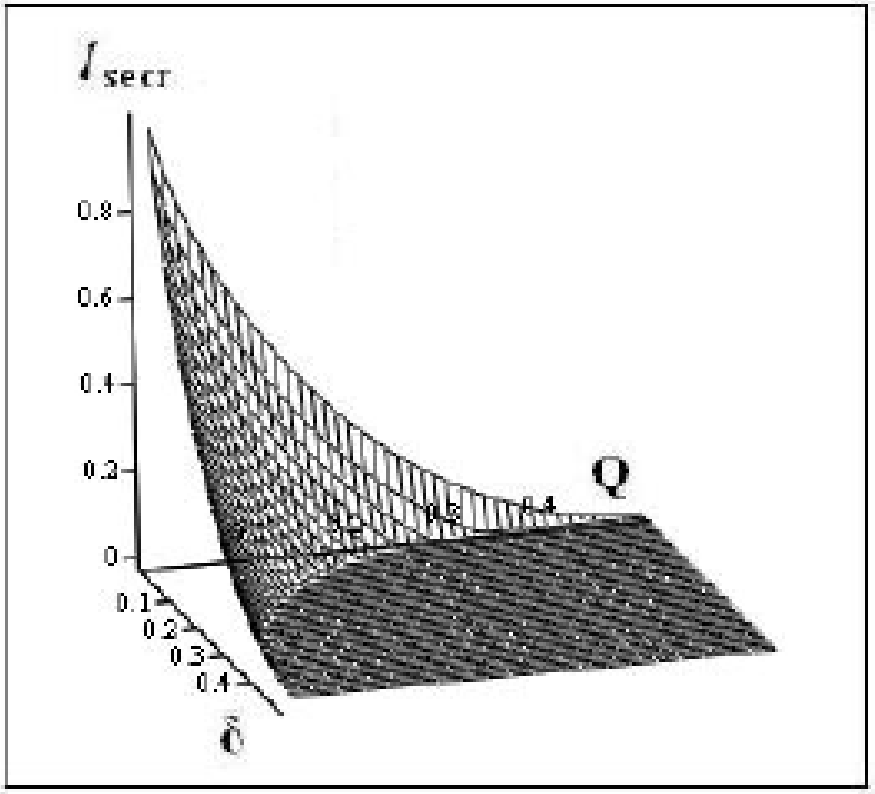
$$l_{\sec r} \leq H(R_A \mid E) - H(R_A \mid R_B)$$

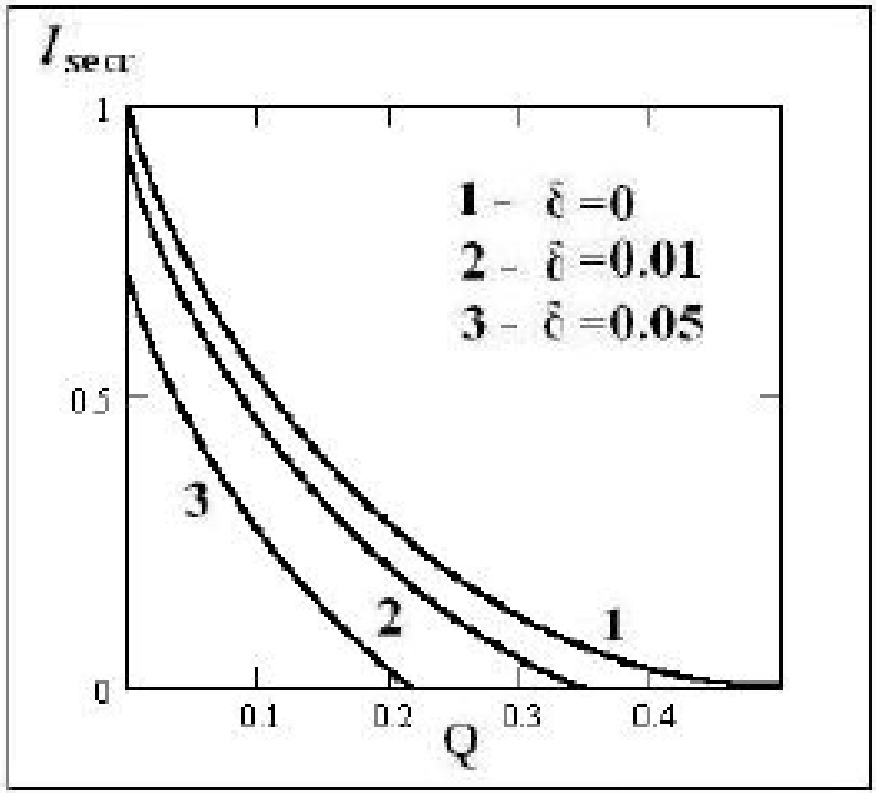
$$H(X_A|E) \geq 2\log\frac{1}{c} - H(X_A|Y_B)$$

$$l_{secr} \approx 2\log\frac{1}{c} - 2H(X_A|Y_B)$$

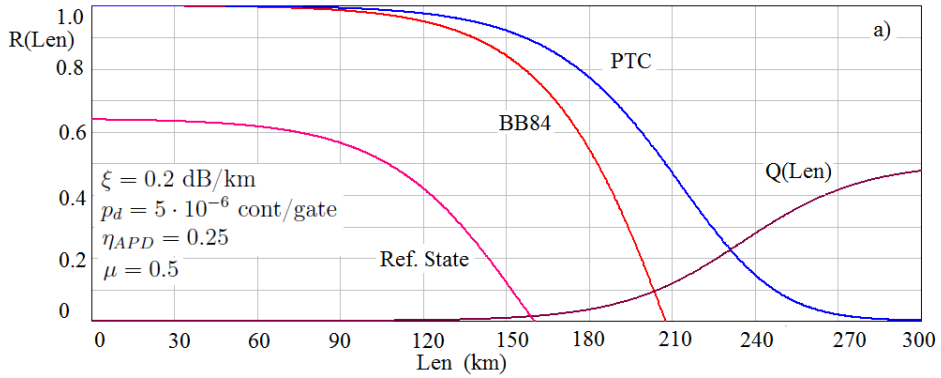


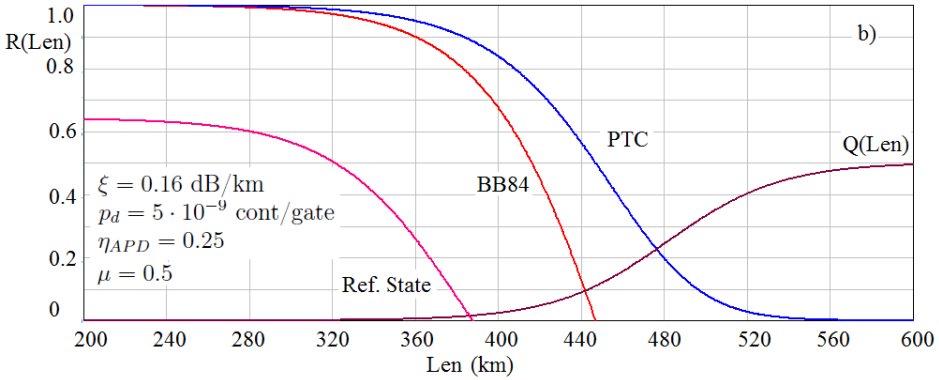


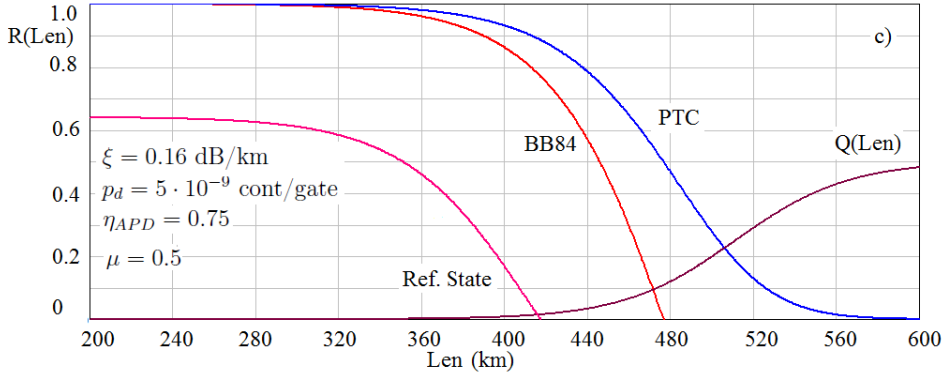

I_{secr}
0.8
0.6
0.4
0.2
0
0.1
0.2
0.3
0.4
δ
Q

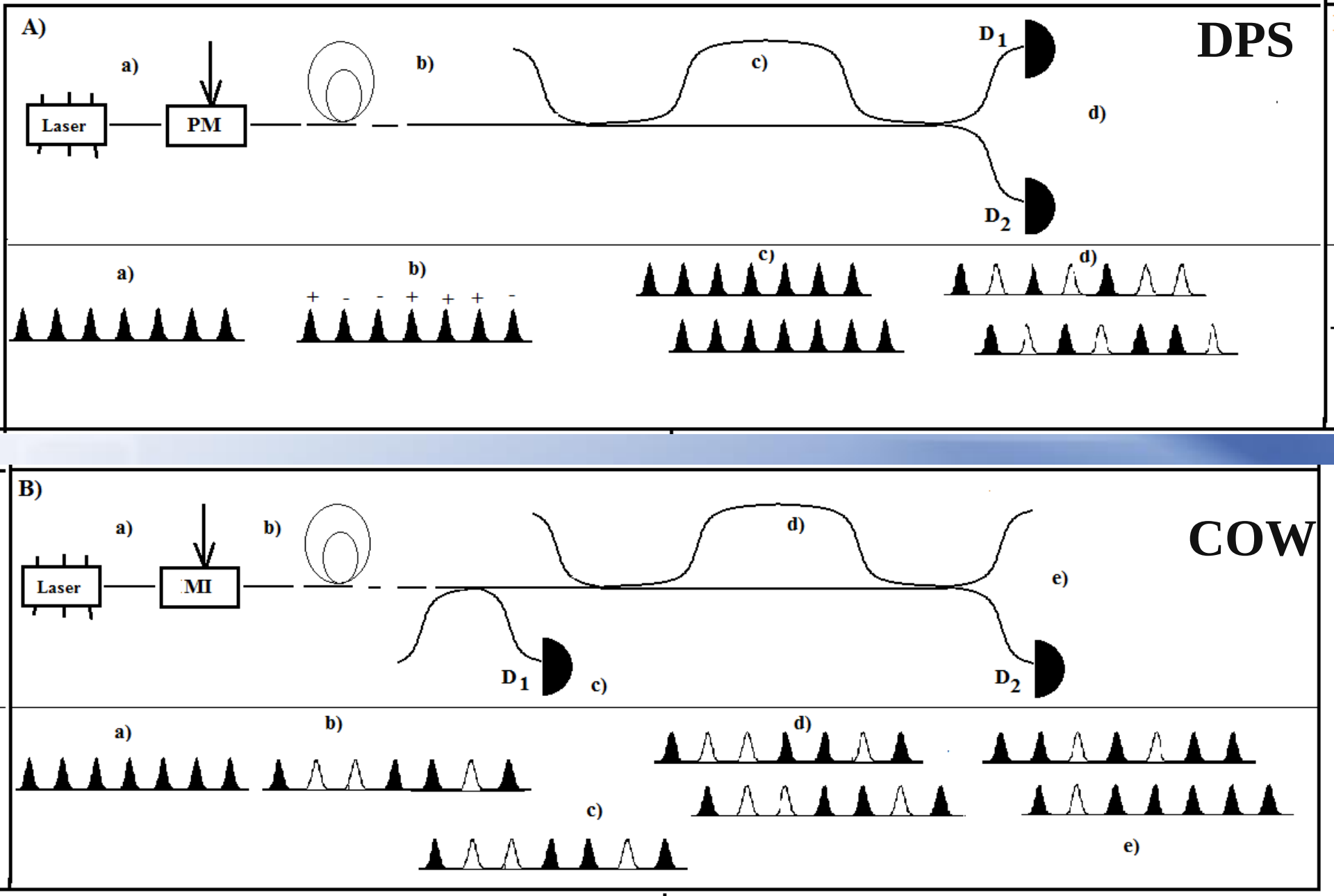

I_{secr}
1
0.5
0
0.1
0.2
0.3
0.4
Q
1 - δ =0
2 - δ =0.01
3 - δ =0.05
1
2
3

Какой протокол квантовой криптографии обеспечивает максимальную дальность в случае создания строго однофотонного источника?

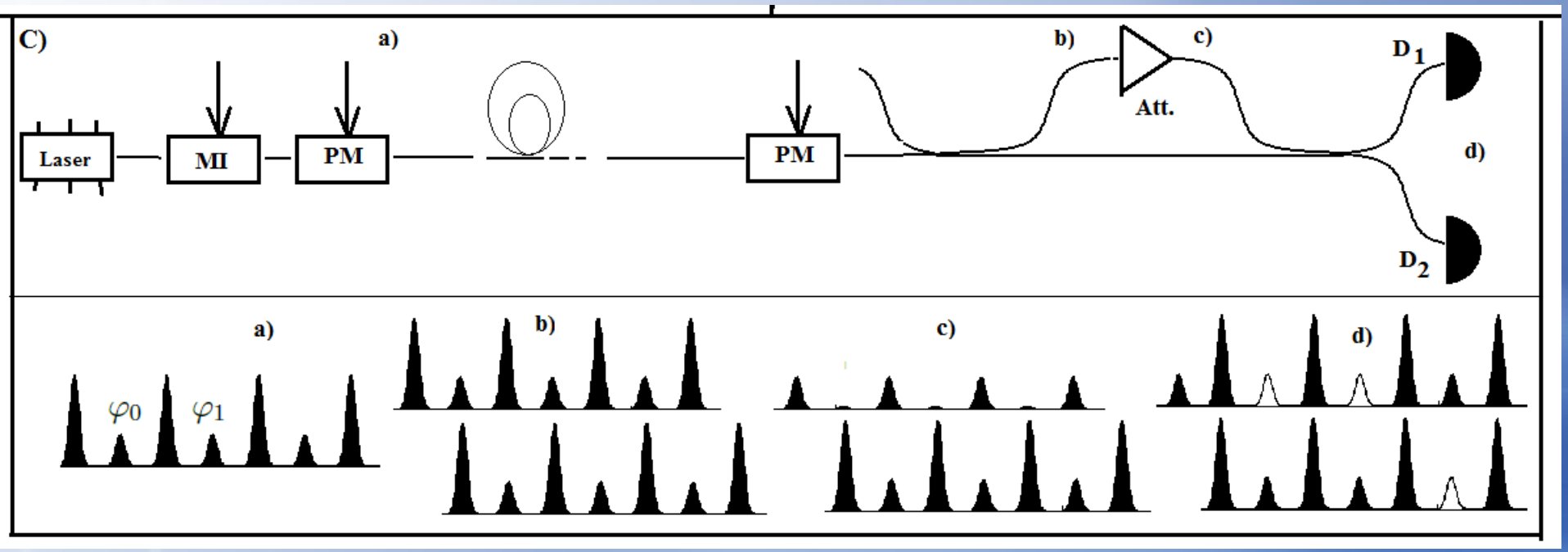




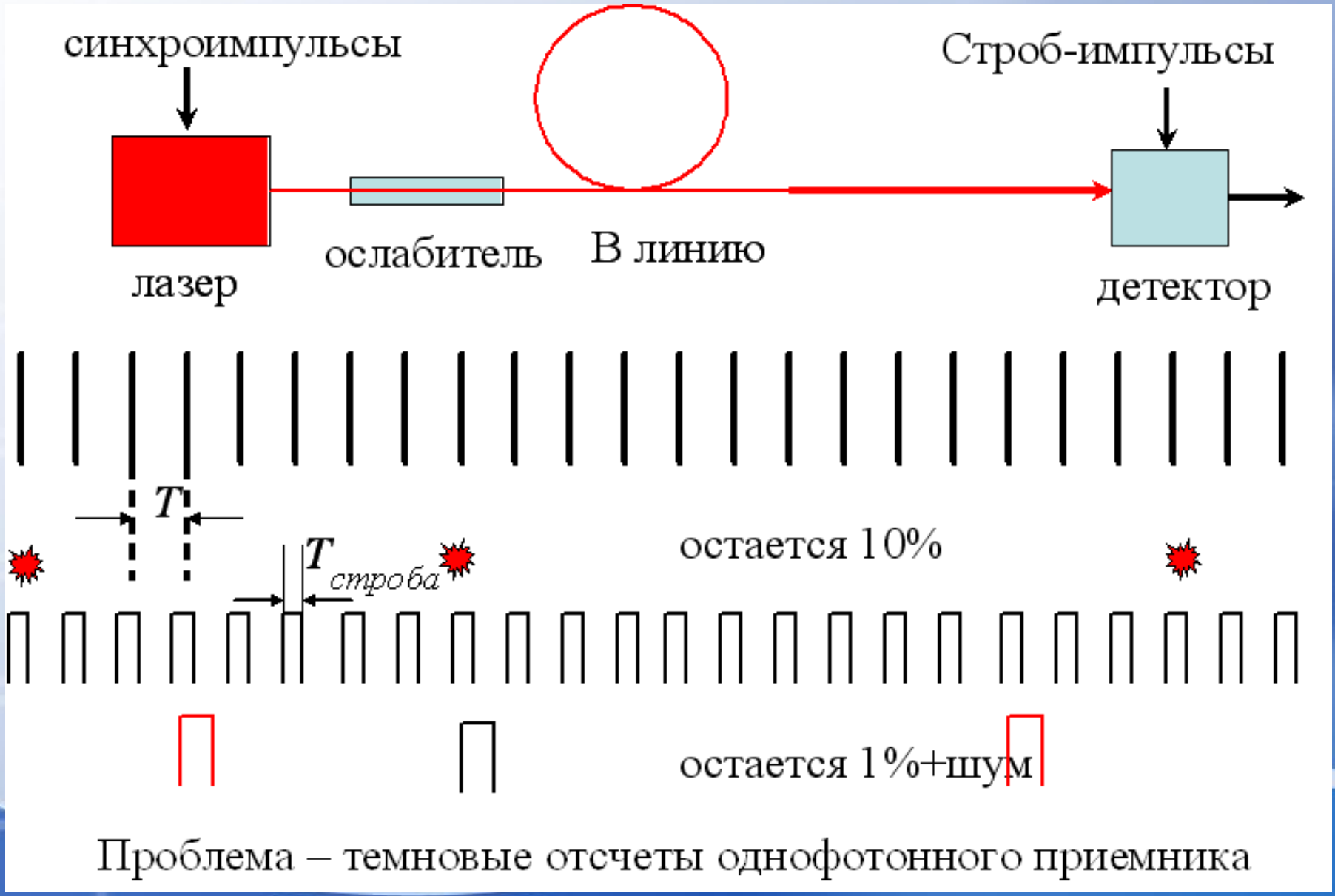



A)
DPS
a)
b)
c)
d)
Laser
PM
D1
D2
a)
b)
c)
d)
+ - - + + + -
B)
COW
a)
b)
d)
e)
Laser
MI
D1
c)
D2
a)
b)
d)
c)
e)

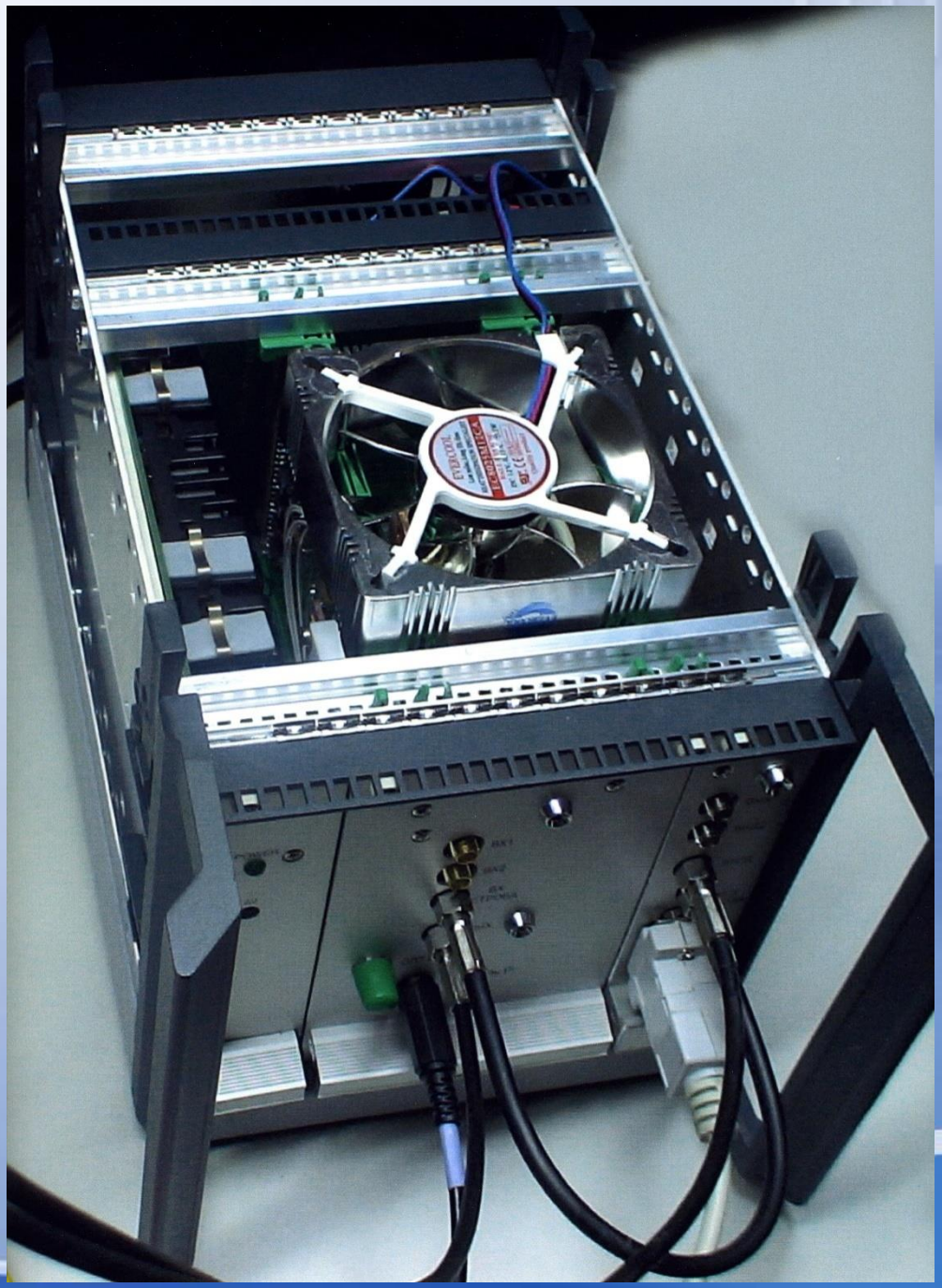
С реперным состоянием – строго доказуемая криптостойкость

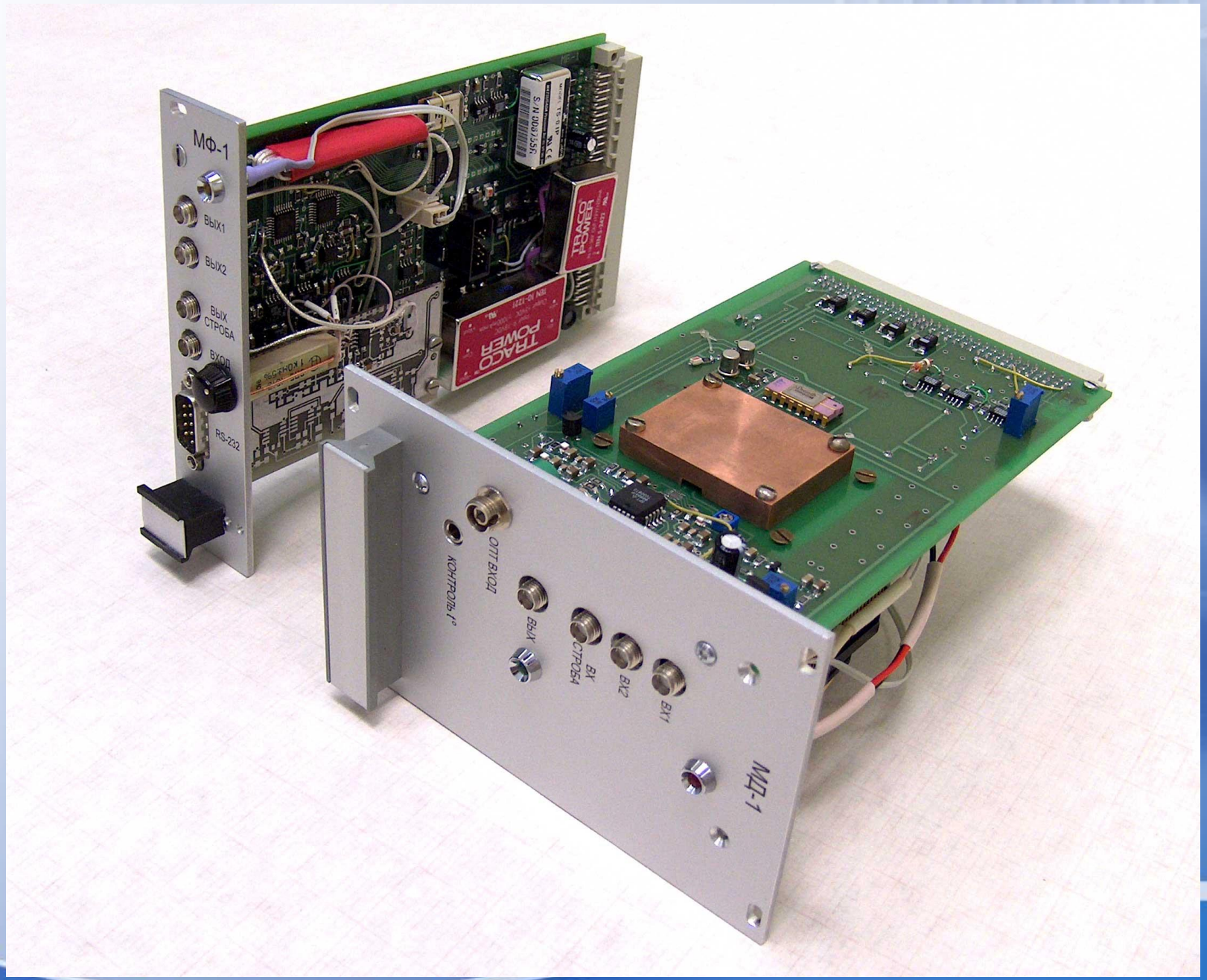


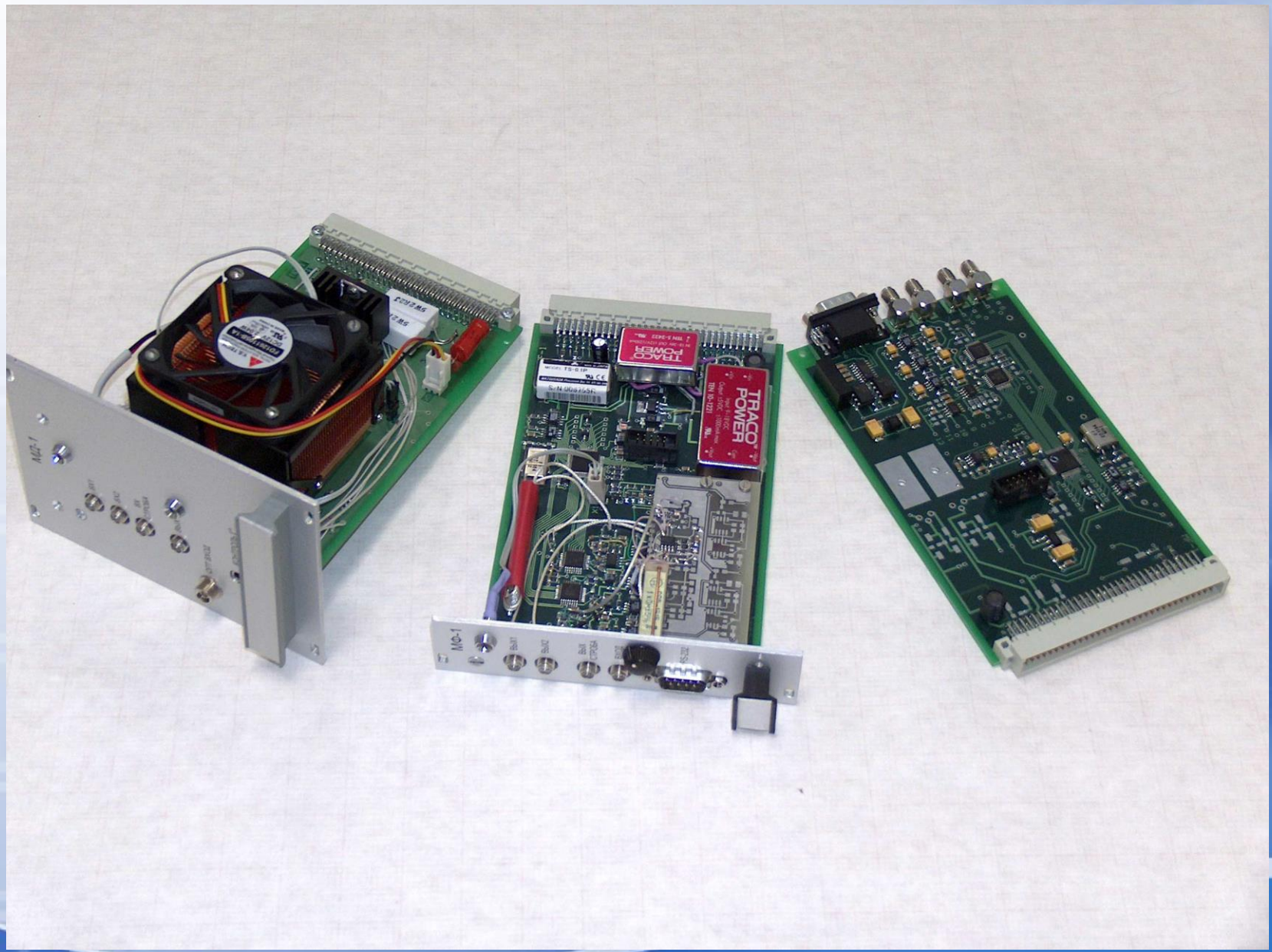
Детектирование одиночных фотонов



Проблема – темновые отсчеты однофотонного приемника

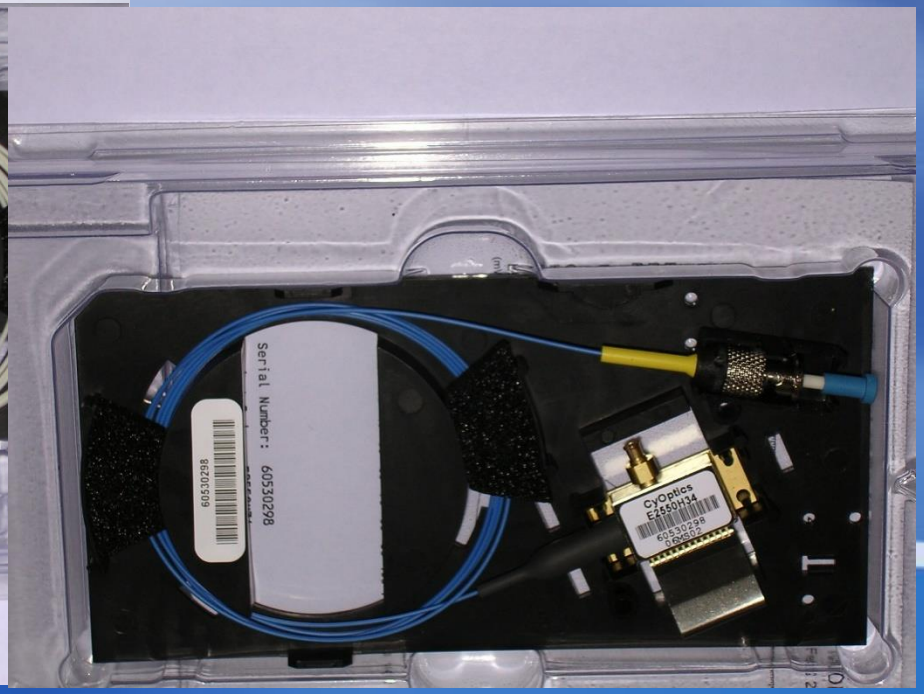


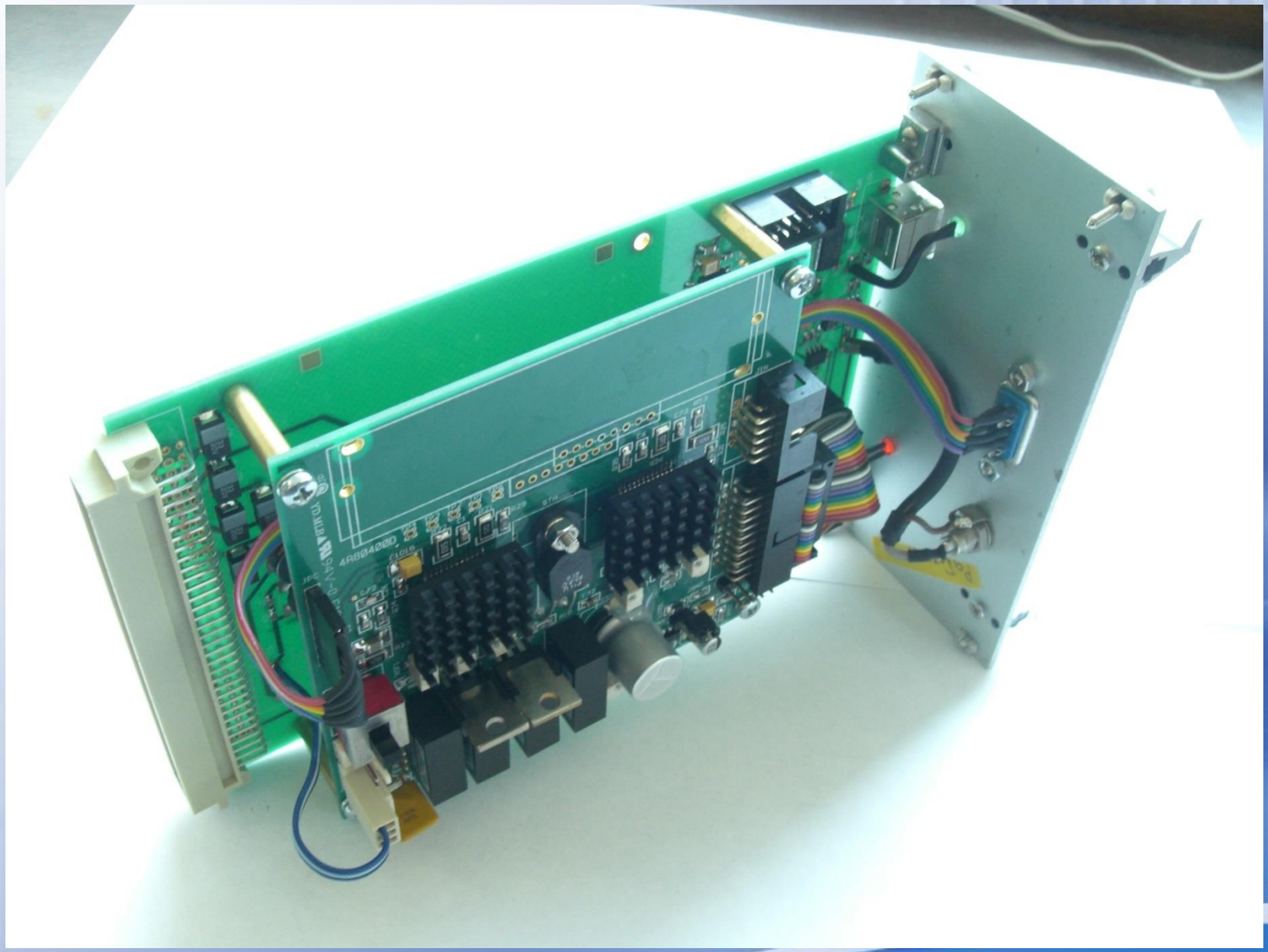

МФ-1
ВЫХ1
ВЫХ2
ВЫХ СТРОБА
ВХОД
RS-232
TRACO POWER
ОПТ.ВХОД
КОНТРОЛЬ 1"
ВЫХ
ВХ СТРОБ
ВХ2
ВХ1
МД-1

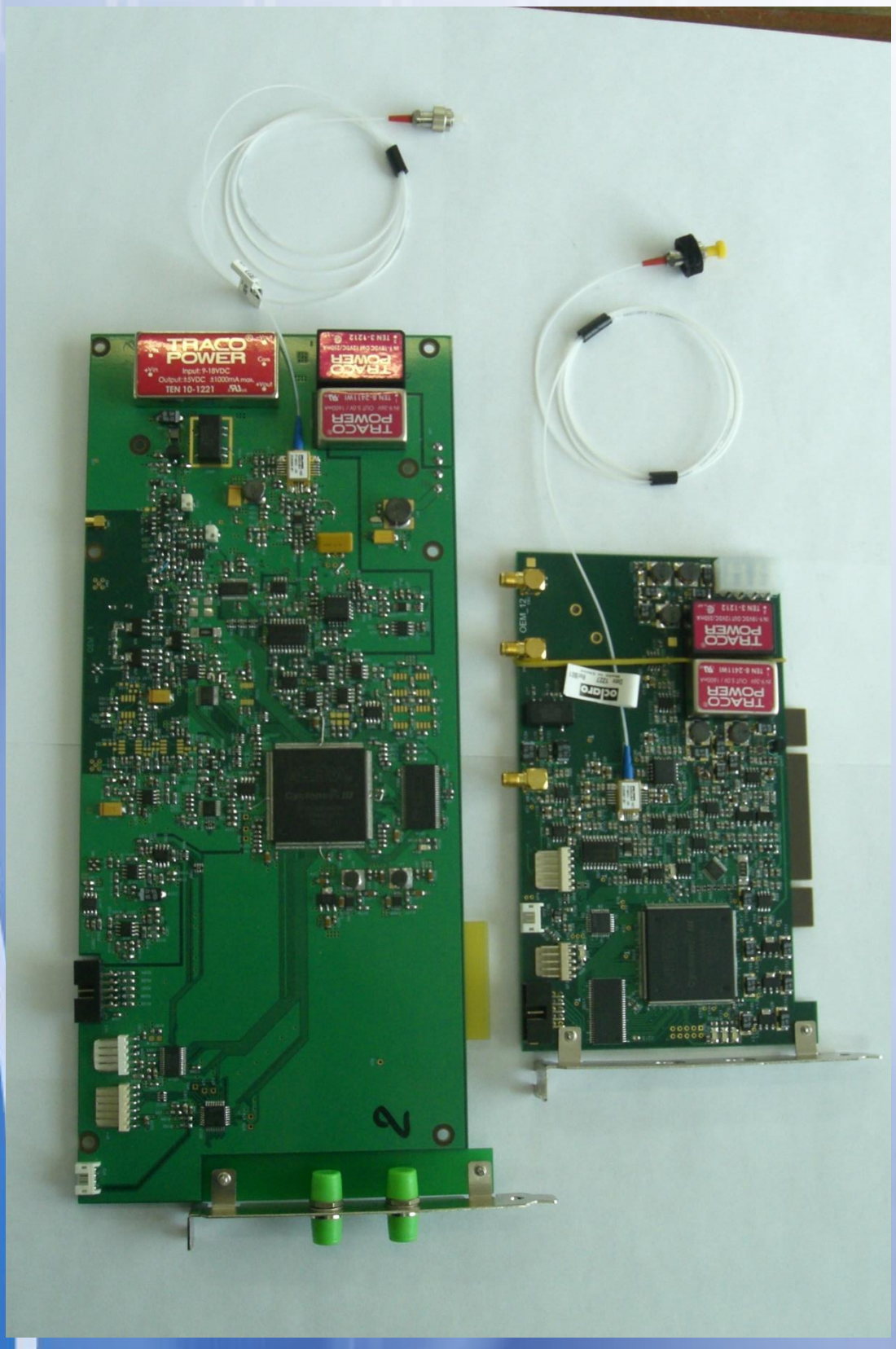

TRACO POWER
TRACO POWER

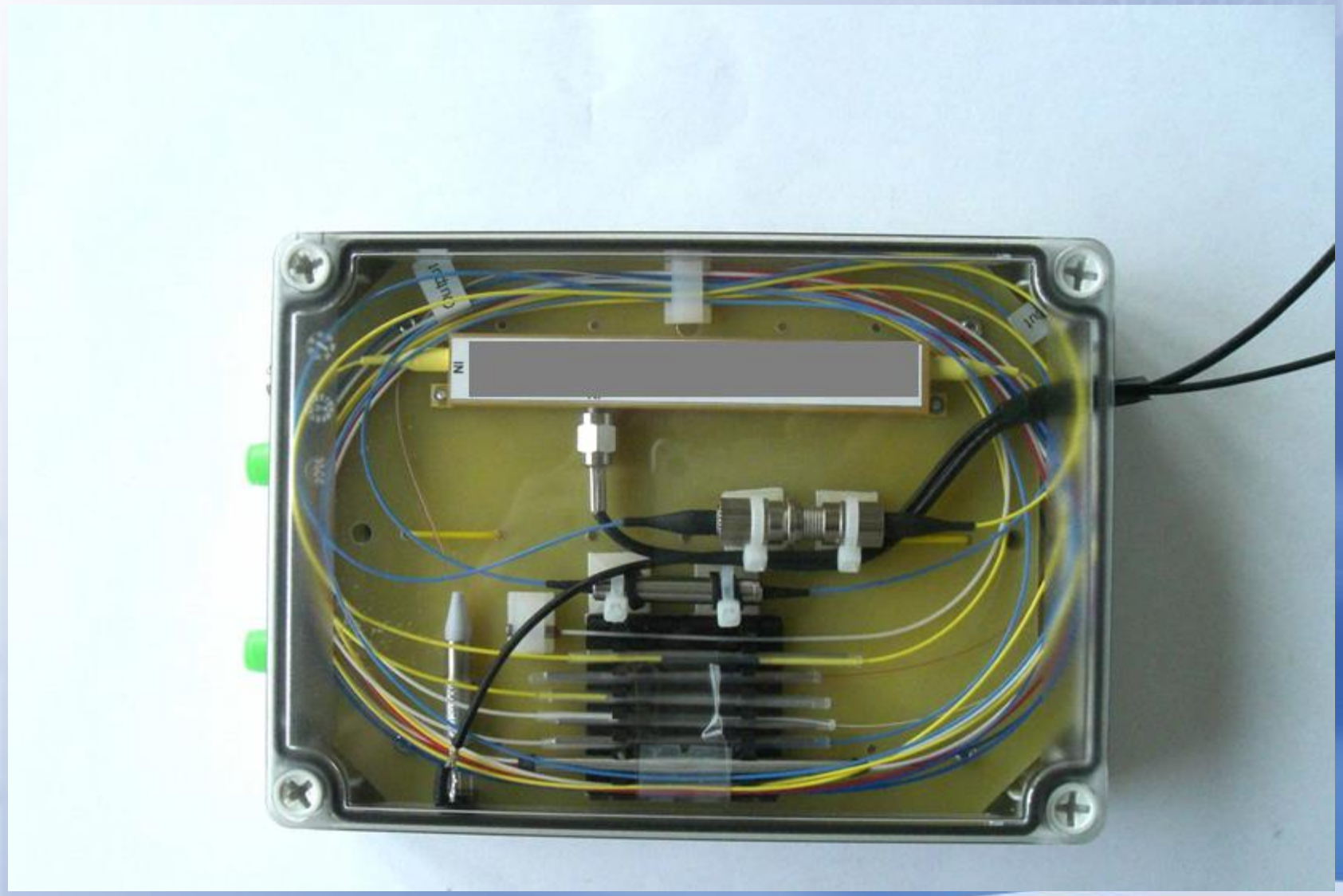

Посадочное место для лазера на 1.55 мкм
DSPLab 2006
Посадочное место для лазера на 1.3 мкм

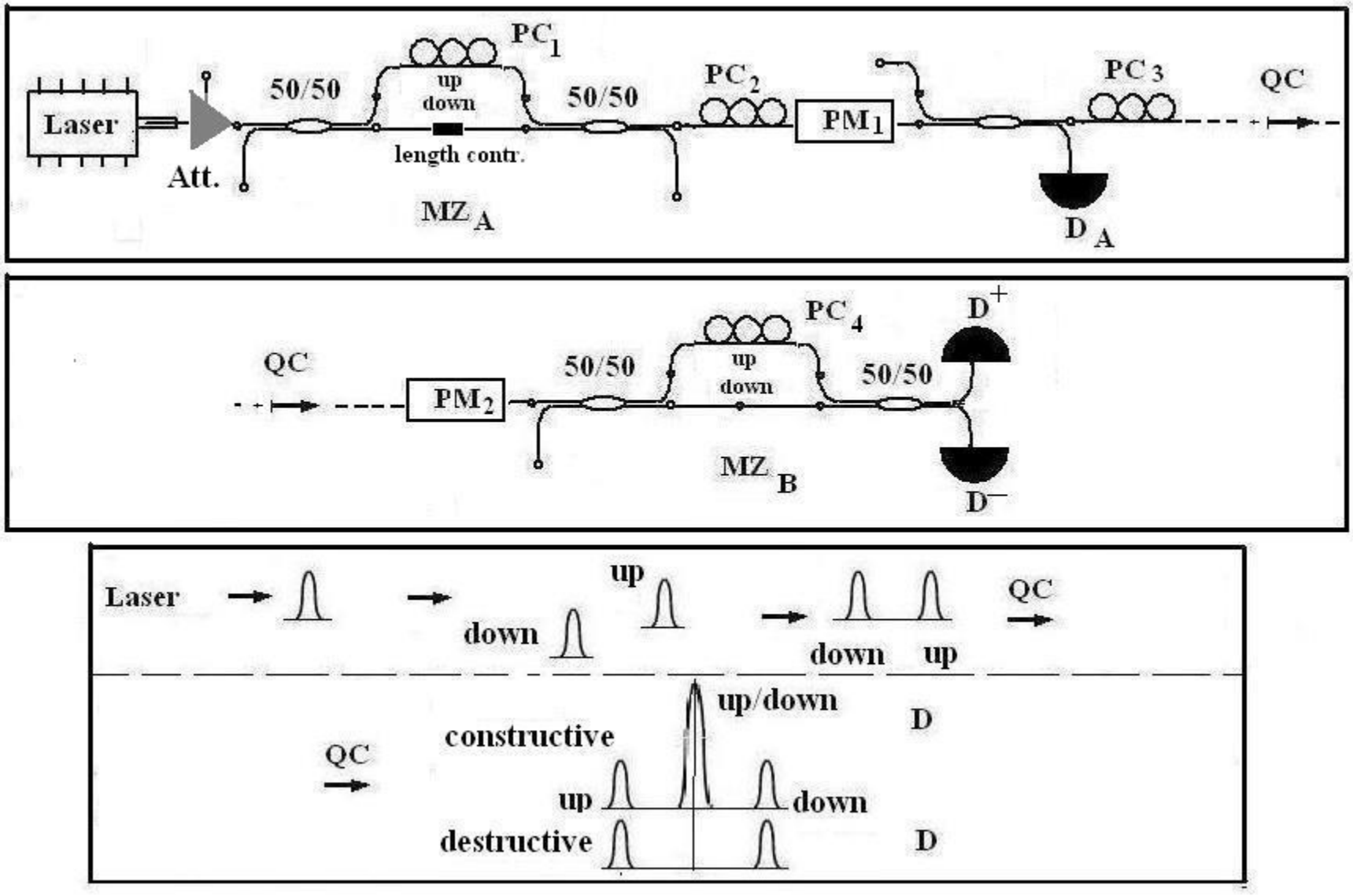

Serial Number: 55030140


Serial Number: 60530298
60530298
CyOptics
E2550H34
60530298

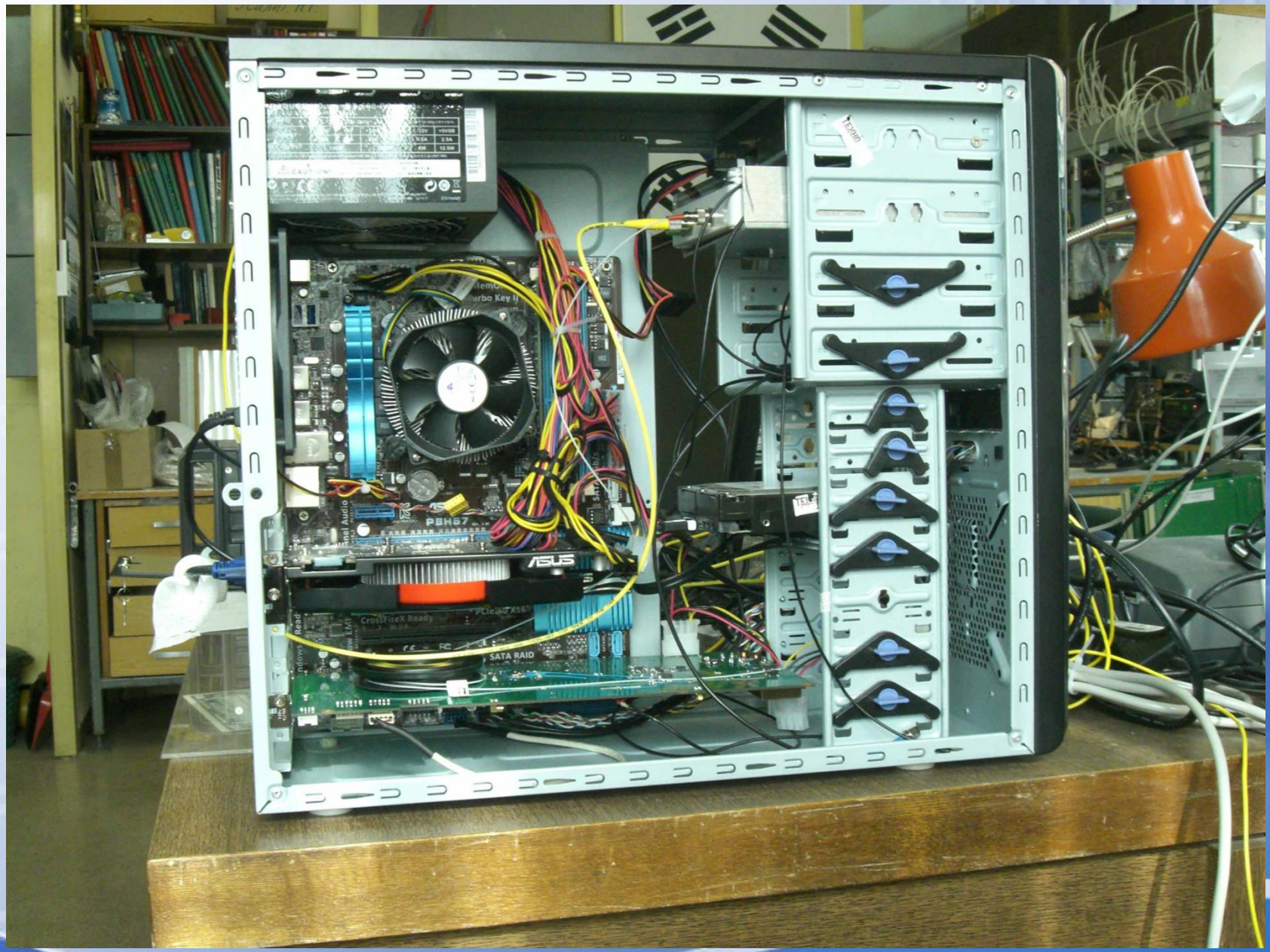


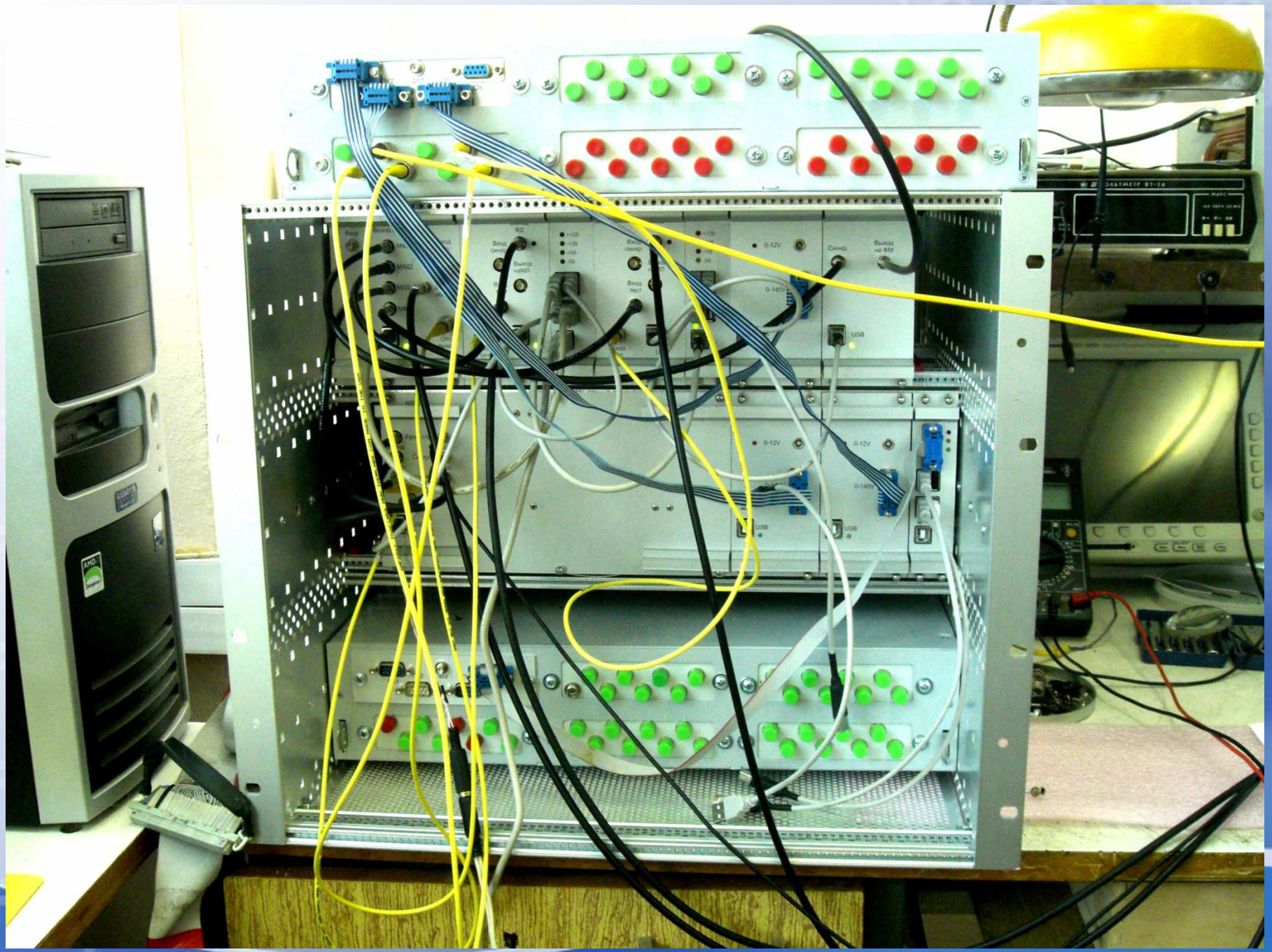

TRACO POWER
Input: 9-18VDC
Output: ±5VDC ±1000mA max.
TEN 10-1221
TRACO POWER
TRACO POWER
TRACO POWER
TRACO POWER
OEM_12

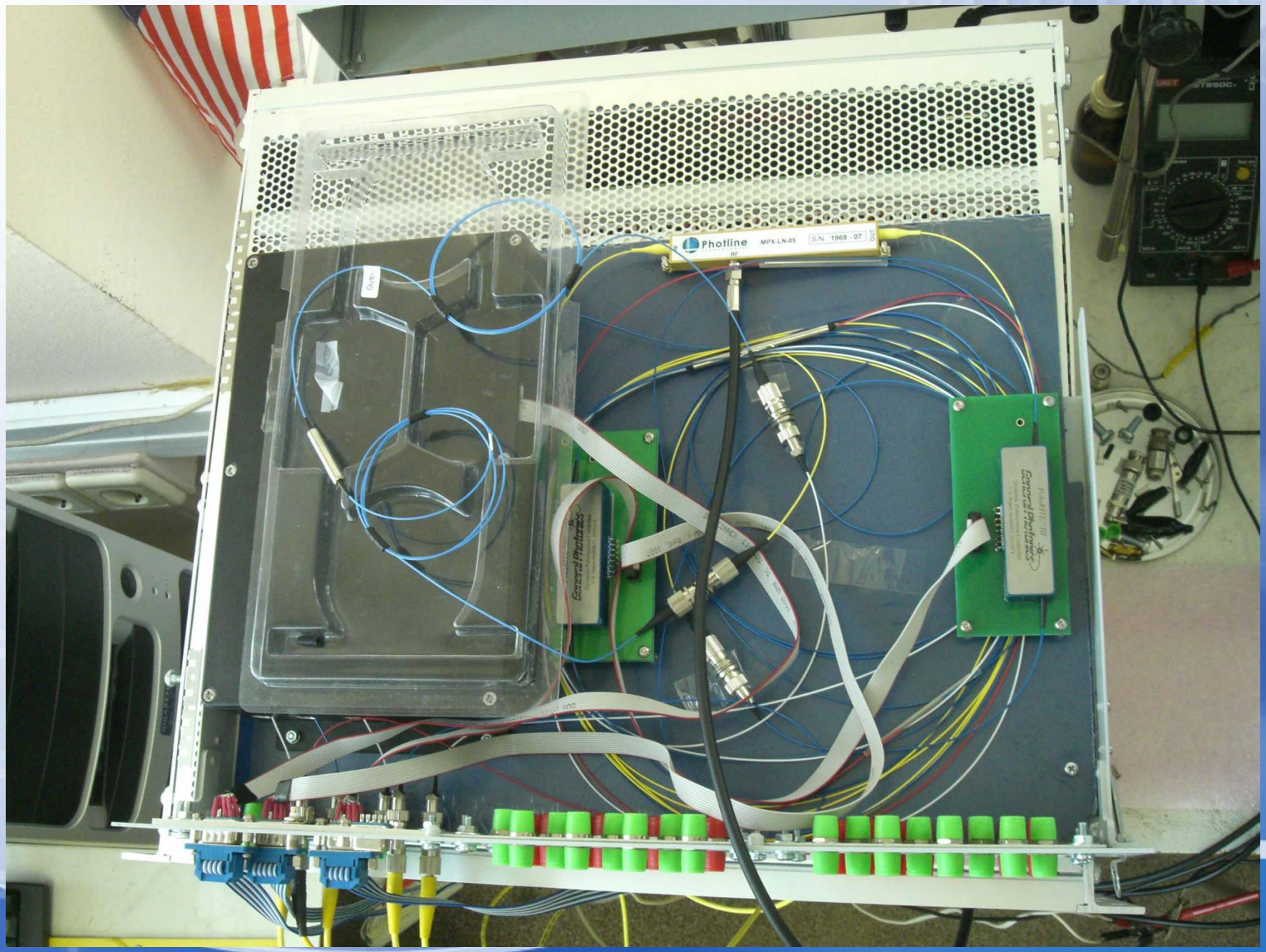



Laser
Att.
50/50
PC1
up
down
length contr.
50/50
MZA
PC2
PM1
PC3
QC
DA
QC
PM2
50/50
PC4
up
down
50/50
MZB
D+
D−
Laser
up
down
down
up
QC
up/down
D
constructive
QC
up
down
destructive
D


MF-2
MØ-2-2


P8H67
ASUS
SATA RAID

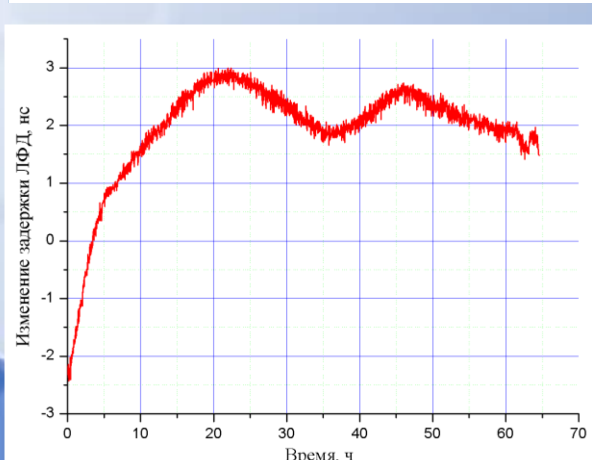


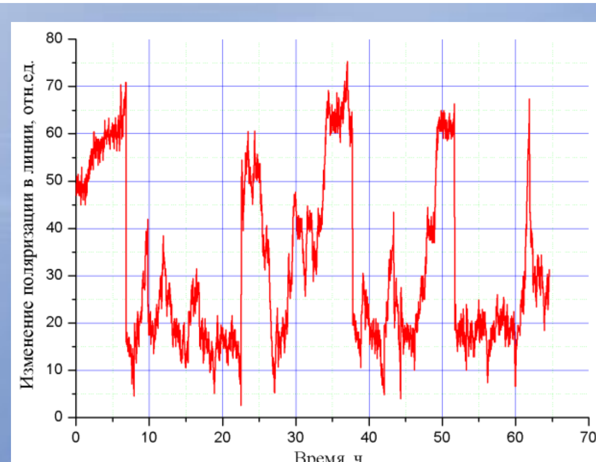

Photline
MPX-LN-05
S/N 1969 - 07
General Photonics

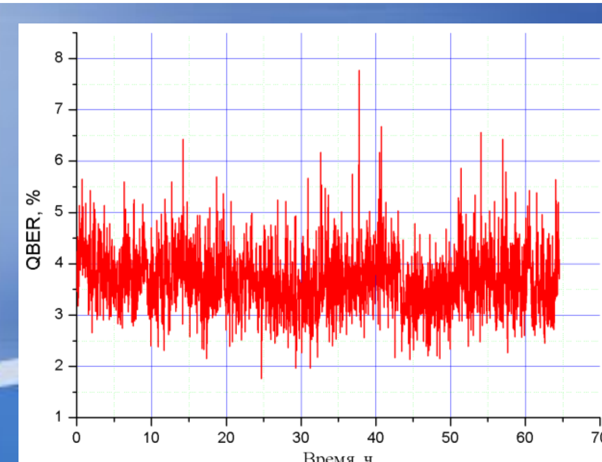
Работа ККС в автоматическом режиме.

```
### 14:27:52 ################
*Series #1  (10000000 @ 3.20 kHz)*
### 14:28:27 ################
   APDcounts = 43334 (52453)   APDcounts efficiency = 4.33e-03 (5.25e-03)
   Counts@bases = 1741 (1925)   Counts@bases efficiency = 1.74e-04 (1.93e-04)    rawKey = 1741
               Secret bits efficiency = 6.22e-05
   Key Estimation:
               errQ = 2.2%  Raw(1741)-Qerr(24.1)-ErrCorr(1094.9)=Secret(622.0)
   Averaged Key Estimation:
      errQ = 2.19% (real=4.48%)   Secret part = 6.22e-05

   Raw key = 1741,  Secret key = 622.04,     Rate = 268.51 bit/min
   Accepted series #1. Accumulated key: raw(1741) Qerr(24) ErrCorr(1095) Secret(622)
### 14:28:27 ################
1741 raw bits for 622 key have been successfully generated in 2.3 min!
Reconciliation start.
### 14:28:44 ################
   ErrQ = 4.1% (2.2%)  bits removed = 941 (1095)
### 14:28:44 ################
   Keys (800 bits) have been successfully reconciled in 17.1 sec!
   Quantum part to remove = 24 bits. 776 secret bits remain. Keys have truncated to 768 bits.
Key stat tests start.
   Key stat tests failed! Keys discarded.
========= Connection to Bob #1 :  OK. ==================
________________________________________________________________________________
*Pre-series checks*
      Temperature measurement
               Laser T = 25.0C,  APD T = -50.0C, OK!
      APD dark counts measurement
               Dark counts rate = 3.70e-06, OK.
      APD flare measurement
               Flare = 4.80e-06  Interference min = 9.40e-06  Aggregated min = 4.09e-03
      APD&PM1 delay adjust
               APD delay has changed from 269350.74 to 269350.89 ns. Smax = 28.1
               PM1 delay has changed from 269278.96 to 269279.08 ns.
      Interferometer balance check
               Smax = 28.1 Smin = 8.00e-02   Interference visibility = 0.9943
      PC3 balance for max with APD
               At beginning V1 = 17.0  V2 = 46.5  V3 = 8.0,  Smax = 27.8
               Balance took 9.0 sec
               Result: V1 = 19.5  V2 = 44.5  V3 = 7.5  Smax = 28.3
      Key Estimation:
               errQ = 1.8%  Raw(1925)-Qerr(23.6)-ErrCorr(1180.4)=Secret(721.3)
      Power at Bob check
               Power at Bob = 4.9e3 photons   Threshold set to 12.0e3 photons
      PM 1&2 Random sequence load
### 14:30:35 ################
*Series #1  (10000000 @ 3.20 kHz)*
### 14:31:09 ################
   APDcounts = 39673 (52453)   APDcounts efficiency = 3.97e-03 (5.25e-03)
   Counts@bases = 1546 (1925)   Counts@bases efficiency = 1.55e-04 (1.93e-04)    rawKey = 1546
               Secret bits efficiency = 5.46e-05
   Key Estimation:
               errQ = 2.3%  Raw(1546)-Qerr(23.5)-ErrCorr(976.8)=Secret(545.7)
   Averaged Key Estimation:
      errQ = 2.27% (real=5.50%)   Secret part = 5.46e-05

   Raw key = 1546,  Secret key = 545.66,     Rate = 235.54 bit/min
   Accepted series #1. Accumulated key: raw(1546) Qerr(24) ErrCorr(977) Secret(546)
### 14:31:09 ################
1546 raw bits for 546 key have been successfully generated in 2.3 min!
Reconciliation start.
### 14:31:27 ################
   ErrQ = 5.2% (2.3%)  bits removed = 914 (977)
### 14:31:27 ################
   Keys (632 bits) have been successfully reconciled in 18.0 sec!
   Quantum part to remove = 24 bits. 609 secret bits remain. Keys have truncated to 512 bits.
Key stat tests start.
   Stat tests succeeded! Keys were cooked in 2.6 min. Keys are ready to use.
========= Connection to Bob #2 :  OK. ==================
________________________________________________________________________________
```

time(h)	ser	T(C)	DCR(cpp)	FCR(cpp)	dt(ns)	Vis-ty	Bal	V1	V2	V3	Smax	kHz	P@Bob	Ngiant	Eff@counts	Eff@bases	Err(%)	Real	Raw(b)	Estm(b)	Rate	Fails	Ns	t(min)	Raw	Estm	Err(%)	Pure(b)	Quant(b)	Secret	t(min)	key#
0.000	1	-50.0	1.70e-06	1.70e-05	+0.59	0.9930	0	57.5	18.5	44.0	37.4	10.0	15.80	0	1.12e-02	4.14e-04	1.54	1.93	2071	823.4	595.2	0	1	1.4	2071	823	3.39	1024	14	1010	1.7	1
0.119	1	-50.0	2.80e-06	1.92e-05	+0.69	0.9945	0	56.0	21.0	47.0	36.9	10.0	16.20	0	1.10e-02	4.18e-04	1.72	2.34	2091	806.4	590.0	0	1	1.4	2091	806	1.91	1216	15	1201	1.7	2
0.194	1	-50.0	2.90e-06	2.34e-05	+0.73	0.9941	0	58.5	17.5	50.0	37.5	10.0	15.80	0	1.10e-02	4.27e-04	2.05	2.57	2136	788.2	569.8	0	1	1.4	2136	788	2.84	1120	16	1104	1.7	3
0.268	1	-50.0	2.90e-06	2.36e-05	+0.72	0.9952	0	59.0	21.5	51.0	37.1	10.0	16.20	0	1.00e-02	3.92e-04	2.24	3.06	1962	707.6	517.8	0	1	1.4	1962	708	3.25	984	16	968	1.6	4
0.342	1	-50.0	3.80e-06	2.32e-05	+0.75	0.9798	1	55.0	23.0	53.0	37.3	10.0	16.20	0	1.05e-02	4.03e-04	2.15	2.58	2013	733.4	165.4	0	1	4.4	2013	733	2.56	1088	16	1072	4.8	5
0.467	1	-50.0	4.00e-06	3.04e-05	+0.78	0.9934	1	51.0	21.5	52.5	37.1	10.0	16.20	0	1.05e-02	4.25e-04	2.66	2.59	2125	738.0	167.7	0	1	4.4	2125	738	3.06	1088	19	1070	4.7	6
0.591	1	-50.0	4.10e-06	1.70e-05	+0.77	0.9941	0	50.5	18.0	54.0	37.0	10.0	15.80	0	1.11e-02	4.28e-04	1.49	2.43	2138	858.1	627.9	0	1	1.4	2138	858	4.31	960	14	946	1.7	7
0.665	1	-50.0	3.00e-06	1.94e-05	+0.71	0.9913	0	52.0	17.0	52.0	37.4	10.0	16.20	0	1.16e-02	4.48e-04	1.62	1.56	2240	878.2	642.6	0	1	1.4	2240	878	2.29	1248	15	1233	1.7	8
0.739	1	-50.0	2.10e-06	2.10e-05	+0.86	0.9940	0	49.0	16.0	56.0	37.3	10.0	15.80	0	1.06e-02	4.05e-04	1.94	2.96	2026	757.2	554.1	0	1	1.4	2026	757	5.18	832	16	817	1.7	9
0.813	1	-50.0	2.50e-06	1.92e-05	+0.90	0.9962	0	49.0	17.0	56.0	37.4	10.0	16.20	0	1.07e-02	4.07e-04	1.77	2.45	2037	780.0	570.7	0	1	1.4	2037	780	3.84	960	15	945	Key stat tests failed!	
0.843	1	-50.0	2.90e-06	1.84e-05	+0.85	0.9919	0	48.0	14.5	54.0	37.2	10.0	15.80	0	1.15e-02	4.32e-04	1.60	2.13	2162	851.4	615.4	0	1	1.4	2162	851	1.75	1280	15	1266	1.7	10
0.917	1	-50.0	3.20e-06	2.06e-05	+0.89	0.9957	0	49.5	11.0	56.0	37.3	10.0	15.80	0	1.06e-02	4.08e-04	1.89	2.20	2041	768.0	561.9	0	1	1.4	2041	768	1.47	1248	15	1233	Key stat tests failed!	
0.946	1	-50.0	2.20e-06	1.72e-05	+0.89	0.9930	0	46.5	11.0	55.5	37.2	10.0	15.80	0	1.09e-02	4.14e-04	1.56	1.88	2072	821.2	600.9	0	1	1.4	2072	821	3.69	992	14	978	1.6	11
1.020	1	-50.0	1.80e-06	1.58e-05	+0.93	0.9946	0	49.0	13.0	56.5	37.4	10.0	15.40	0	1.15e-02	4.34e-04	1.37	1.89	2168	892.7	661.3	0	1	1.4	2168	893	3.82	1024	14	1011	1.7	12
1.094	1	-50.0	2.90e-06	1.66e-05	+1.03	0.9945	0	53.0	17.0	53.5	37.6	10.0	15.80	0	1.12e-02	4.42e-04	1.41	2.13	2210	902.1	660.0	0	1	1.4	2210	902	3.16	1120	14	1106	1.7	13
1.168	1	-50.0	2.60e-06	2.56e-05	+1.02	0.9941	0	55.0	13.5	52.5	37.2	10.0	15.80	0	1.16e-02	4.44e-04	2.15	1.44	2220	809.6	592.4	0	1	1.4	2220	810	4.67	960	17	943	1.7	14
1.242	1	-50.0	2.00e-06	2.90e-05	+1.11	0.9919	0	51.5	13.5	56.0	37.5	10.0	15.40	0	1.10e-02	4.09e-04	2.63	2.10	2046	711.7	527.2	0	1	1.4	2046	712	2.71	1088	18	1070	1.7	15
1.316	1	-50.0	2.90e-06	2.64e-05	+1.20	0.9978	1	48.5	17.5	55.0	37.6	10.0	16.20	0	1.15e-02	4.25e-04	2.31	1.98	2125	761.5	169.2	0	1	4.5	2125	761	3.93	992	17	975	4.8	16
1.442	1	-50.0	2.90e-06	1.36e-05	+1.24	0.9978	0	48.1	16.4	56.5	37.1	10.0	15.80	0	1.13e-02	4.27e-04	1.20	1.22	2136	916.7	670.8	0	1	1.4	2136	917	2.84	1120	13	1107	1.6	17
1.516	1	-50.0	2.20e-06	1.52e-05	+1.28	0.9935	0	49.1	11.9	59.0	37.3	10.0	16.20	0	1.08e-02	4.08e-04	1.40	2.15	2042	835.1	611.0	0	1	1.4	2042	835	1.26	1280	14	1267	1.7	18
1.635	1	-50.0	3.80e-06	1.40e-05	+1.27	0.9913	0	45.6	15.4	63.0	37.4	10.0	15.80	0	1.18e-02	4.41e-04	1.20	1.27	2205	947.4	693.2	0	1	1.4	2205	947	3.98	1024	13	1011	1.7	19
1.793	1	-50.0	3.60e-06	2.46e-05	+1.36	0.9925	1	44.1	11.9	62.0	37.3	10.0	16.20	0	1.12e-02	4.21e-04	2.18	1.57	2106	765.3	170.1	0	1	4.5	2106	765	0.92	1376	17	1360	4.8	20
1.918	1	-50.0	3.40e-06	2.00e-05	+1.45	0.9929	0	39.6	14.4	64.5	37.1	10.0	16.20	0	1.14e-02	4.44e-04	1.69	1.98	2219	860.5	629.6	0	1	1.4	2219	861	4.04	1024	15	1009	1.7	21
1.992	1	-50.0	3.70e-06	2.20e-05	+1.65	0.9935	0	36.6	12.4	63.0	36.9	10.0	16.20	0	9.48e-03	3.81e-04	2.16	3.21	1903	692.4	500.5	0	1	1.4	1903	692	2.97	984	16	969	1.7	22
2.066	1	-50.0	4.00e-06	1.34e-05	+1.54	0.9951	0	39.6	16.4	62.5	37.3	10.0	15.80	0	1.12e-02	4.34e-04	1.16	1.43	2171	941.1	688.6	0	1	1.4	2171	941	3.26	1088	13	1075	1.7	23
[illegible]	1	-50.0	3.00e-06	[illegible]	[illegible]	[illegible]	0	41.1	17.4	61.5	37.5	10.0	[illegible]	0	[illegible]	4.63e-04	1.20	1.55	2317	994.1	718.6	0	1	1.4	2317	994	2.83	1216	14	1203	1.7	24
[illegible]	[illegible]	-50.0	3.80e-06	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	15.9	60.5	37.2	10.0	[illegible]	[illegible]	[illegible]	[illegible]	1.37	2.30	2170	893.8	[illegible]	[illegible]	[illegible]	1.4	2170	894	1.17	1376	14	[illegible]	[illegible]	25
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	61.5	37.4	10.0	[illegible]	[illegible]	[illegible]	[illegible]	1.40	1.37	2195	897.3	[illegible]	[illegible]	[illegible]	[illegible]	2195	[illegible]	1.88	1280	14	[illegible]	[illegible]	26
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	2256	920.2	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	920	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	27
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	1.55	2282	925.3	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	1.93	[illegible]	14	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	1924	764.3	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]







Релятивистская квантовая криптография для открытого пространства

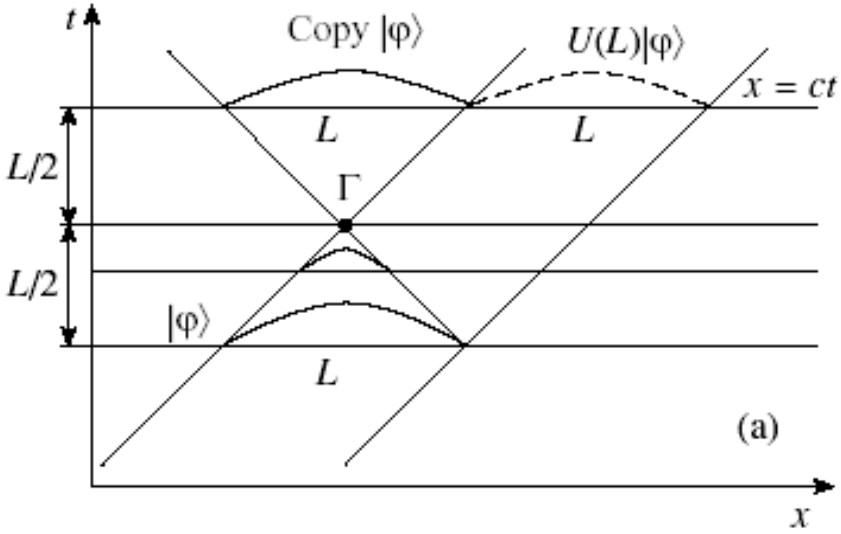
Проблемы с дальностью передачи ключей

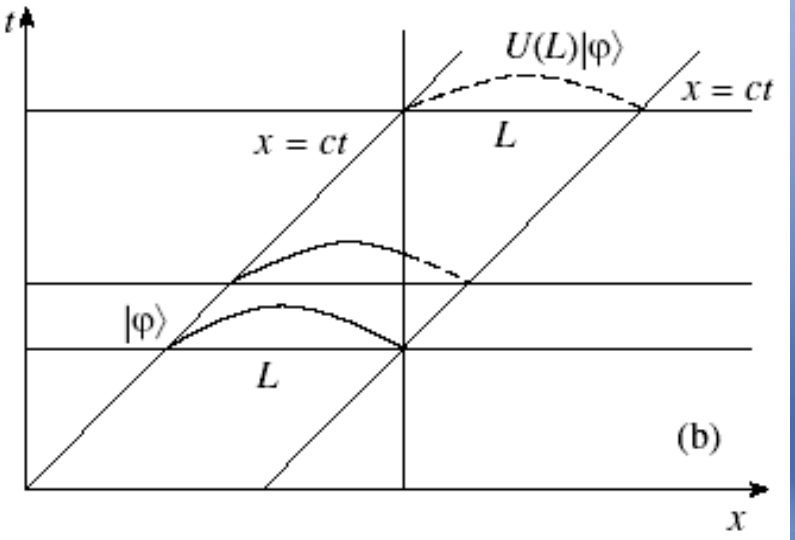
Для всех известных протоколов требуется знать потери в канале *a priori*.

Принципиальный вопрос.
Существуют ли протоколы гарантирующие секретность ключей при любых потерях (заранее неизвестных и меняющихся в течение работы протокола) и неоднофотонном источнике?

Фундаментальных ограничений только квантовой механики на измеримость квантовых состояний недостаточно.

Релятивистская квантовая криптография





$$|\varphi_0\rangle \longmapsto (U_L|\varphi_0\rangle) \otimes (U_L|\varphi_0\rangle),$$
$$|\varphi_1\rangle \longmapsto (U_L|\varphi_1\rangle) \otimes (U_L|\varphi_1\rangle),$$

$$|\varphi_0\rangle|A\rangle \longmapsto (U_L|\varphi_0\rangle) \otimes |A_0\rangle,$$
$$|\varphi_1\rangle \otimes |A\rangle \longmapsto (U_L|\varphi_1|) \otimes |A_1\rangle, \quad |A_0\rangle \neq |A_1\rangle.$$

IOP Publishing | Astro Ltd

Laser Physics Letters

Laser Phys. Lett. **11** (2014) 065203 (5pp)

doi:10.1088/1612-2011/11/6/065203

Letters

Relativistic quantum cryptography

I V Radchenko[1], K S Kravtsov[1], S P Kulik[2] and S N Molotkov[3,4,5]

[1] A.M. Prokhorov General Physics Institute RAS, Moscow, Russia
[2] Faculty of Physics, Moscow State University, Moscow, Russia
[3] Academy of Cryptography of Russian Federation, Moscow, Russia
[4] Institute of Solid State Physics, Chernogolovka, Moscow Rgn., Russia
[5] Faculty of Computational Mathematics and Cybernetics, Moscow State University, Moscow, Russia

A New Relativistic Orthogonal States Quantum Key Distribution Protocol

Jordan S. Cotler
Massachusetts Institute of Technology, Cambridge, Massachusetts 02139, USA

Peter W. Shor
Department of Mathematics, Center for Theoretical Physics and CSAIL, Massachusetts Institute of Technology, Cambridge, Massachusetts 02139, USA

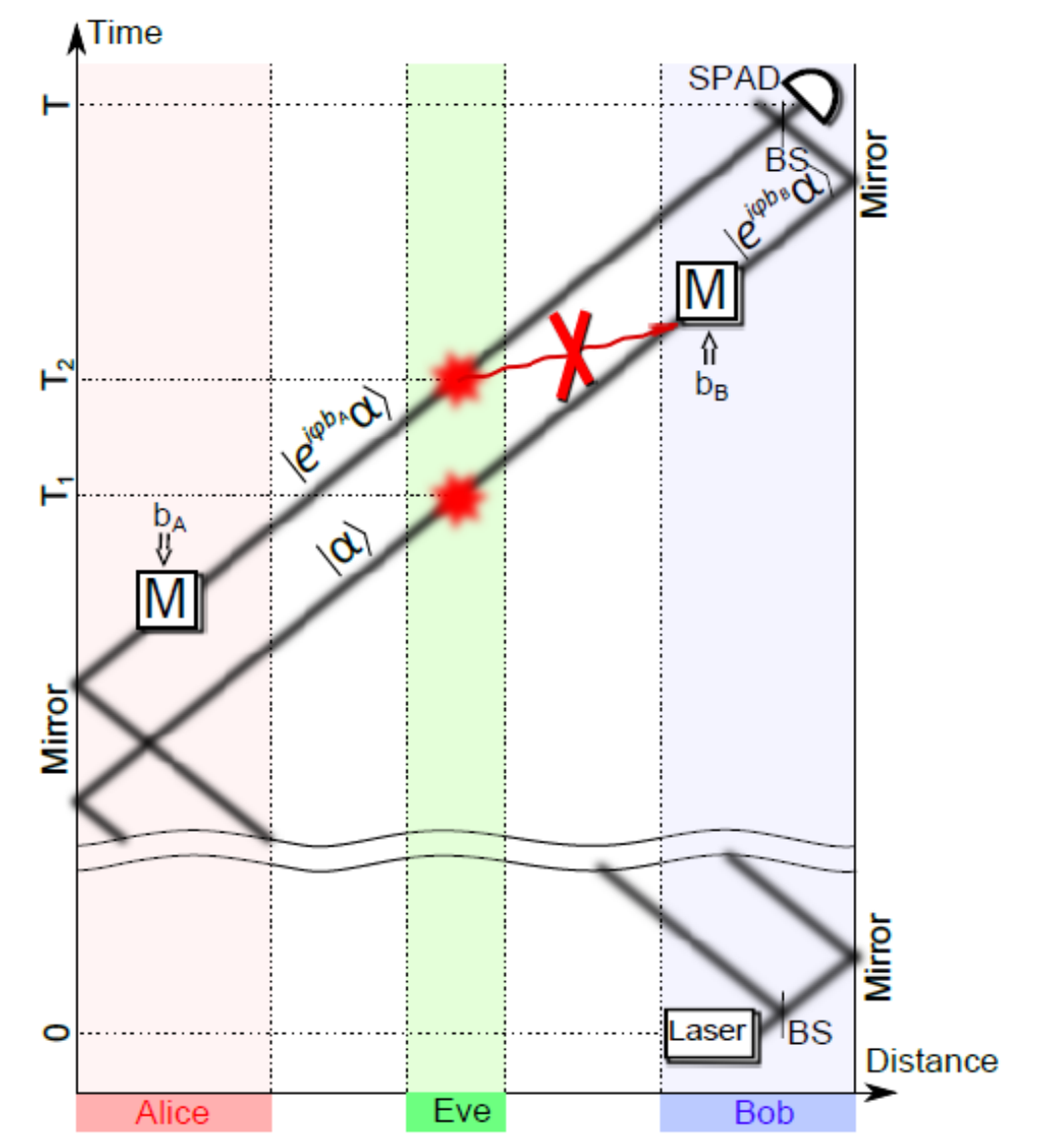
We introduce a new relativistic orthogonal states quantum key distribution protocol which leverages the properties of both quantum mechanics and special relativity to securely encode multiple bits onto the spatio-temporal modes of a single photon. If the protocol is implemented using a single photon source, it can have a key generation rate faster than the repetition rate of the source, enabling faster secure communication than is possible with existing protocols. Further, we provide a proof that the protocol is secure and give a method of implementing the protocol using line-of-sight and fiber optic channels.

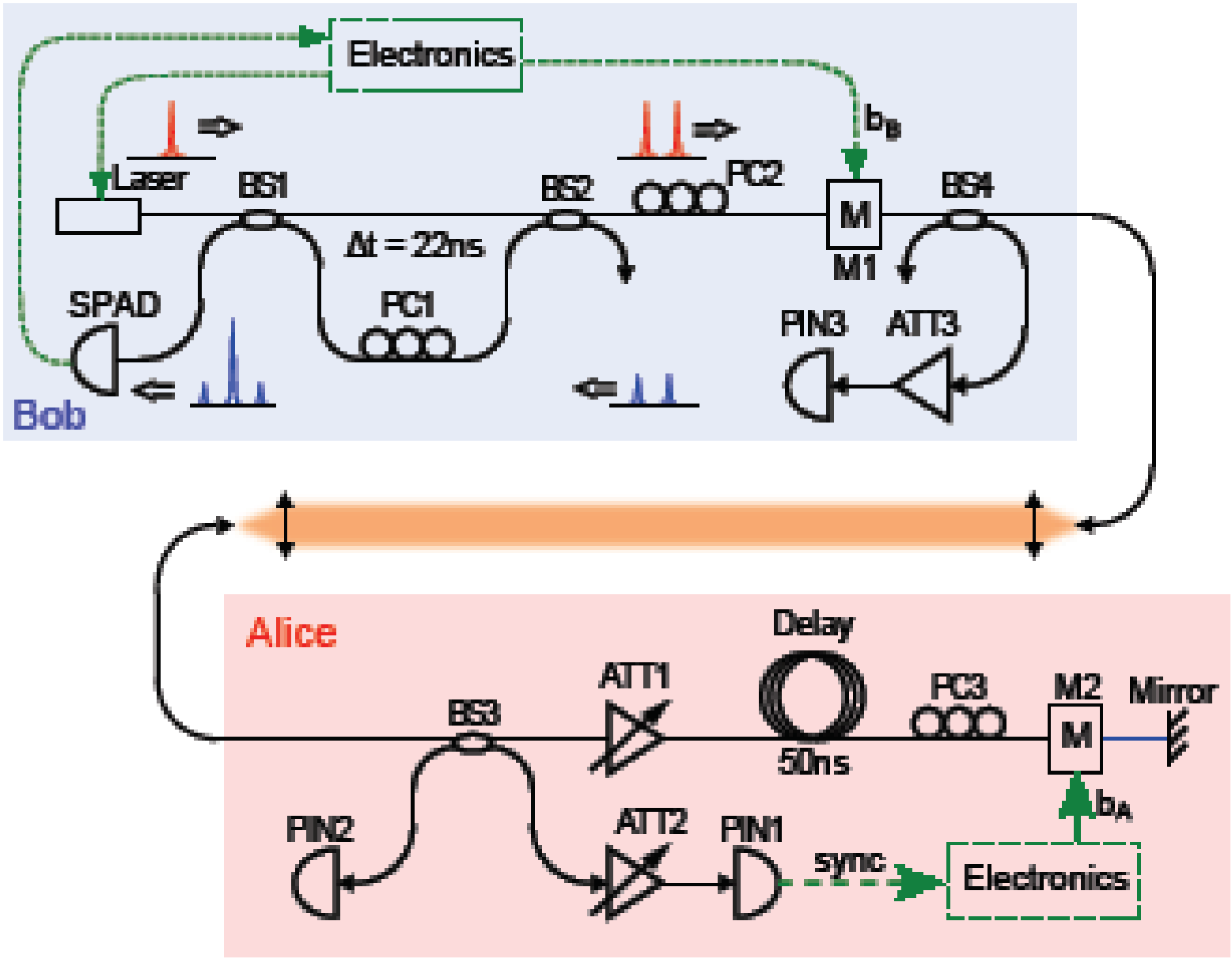
Keywords: Quantum Cryptography, Quantum Key Distribution, Secure Communications

I. INTRODUCTION

Cryptography underpins all secure communications, whether it is used for transferring credit card information

Релятивистский протокол




Electronics
Laser
BS1
BS2
PC2
M
BS4
M1
Δt = 22ns
SPAD
PC1
PIN3
ATT3
Bob
Alice
Delay
ATT1
BS3
PC3
M2
Mirror
50ns
PIN2
ATT2
PIN1
sync
Electronics

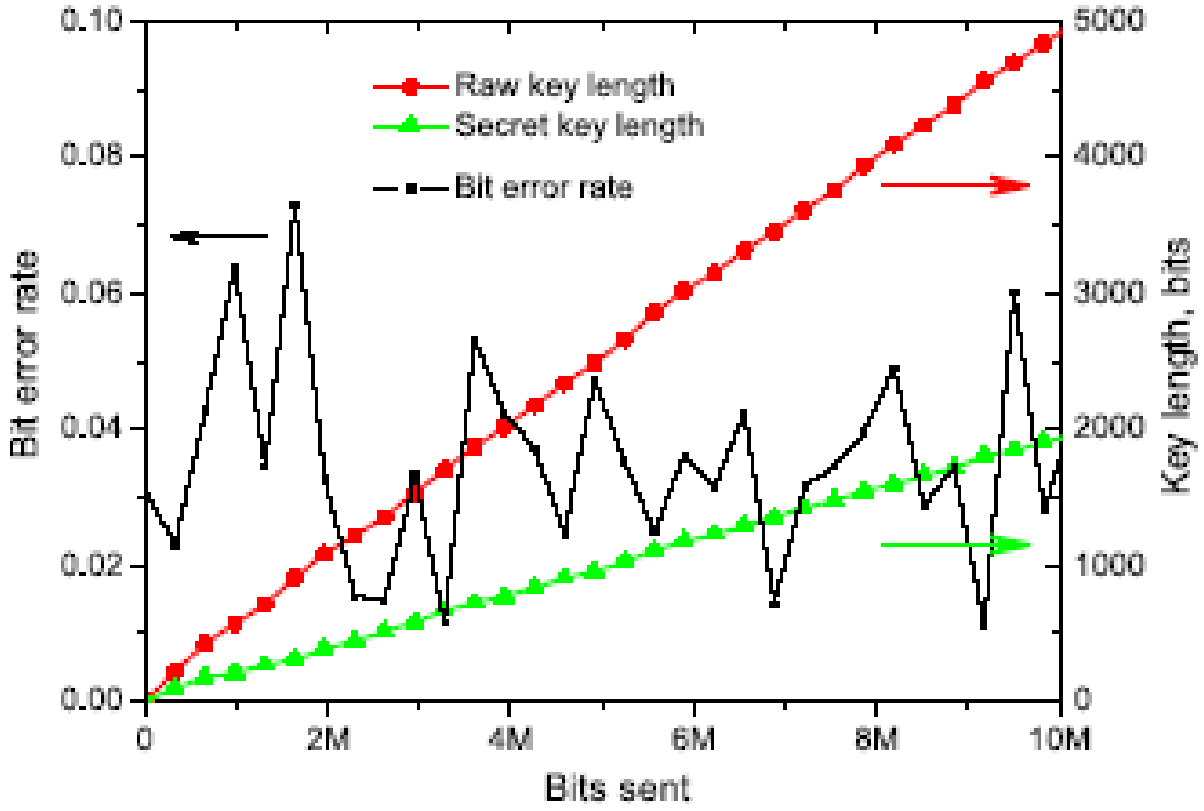


FIG. 4: **Experimentally measured bit error rate and the obtained key lengths.** During the run over 55 m long free space channel Alice was checking her observed timing sequence and compared it with that used by Bob. No timing errors were observed. Average number of photons per modulated pulse was kept at $\mu = 0.1$ and a depth of phase modulation was equal 130°. Detection of arriving photons was performed by Bob in a 4-ns time window, which is 5.5 times less than $\Delta t = 22$ ns, satisfying the requirements of the relativistic protocol.

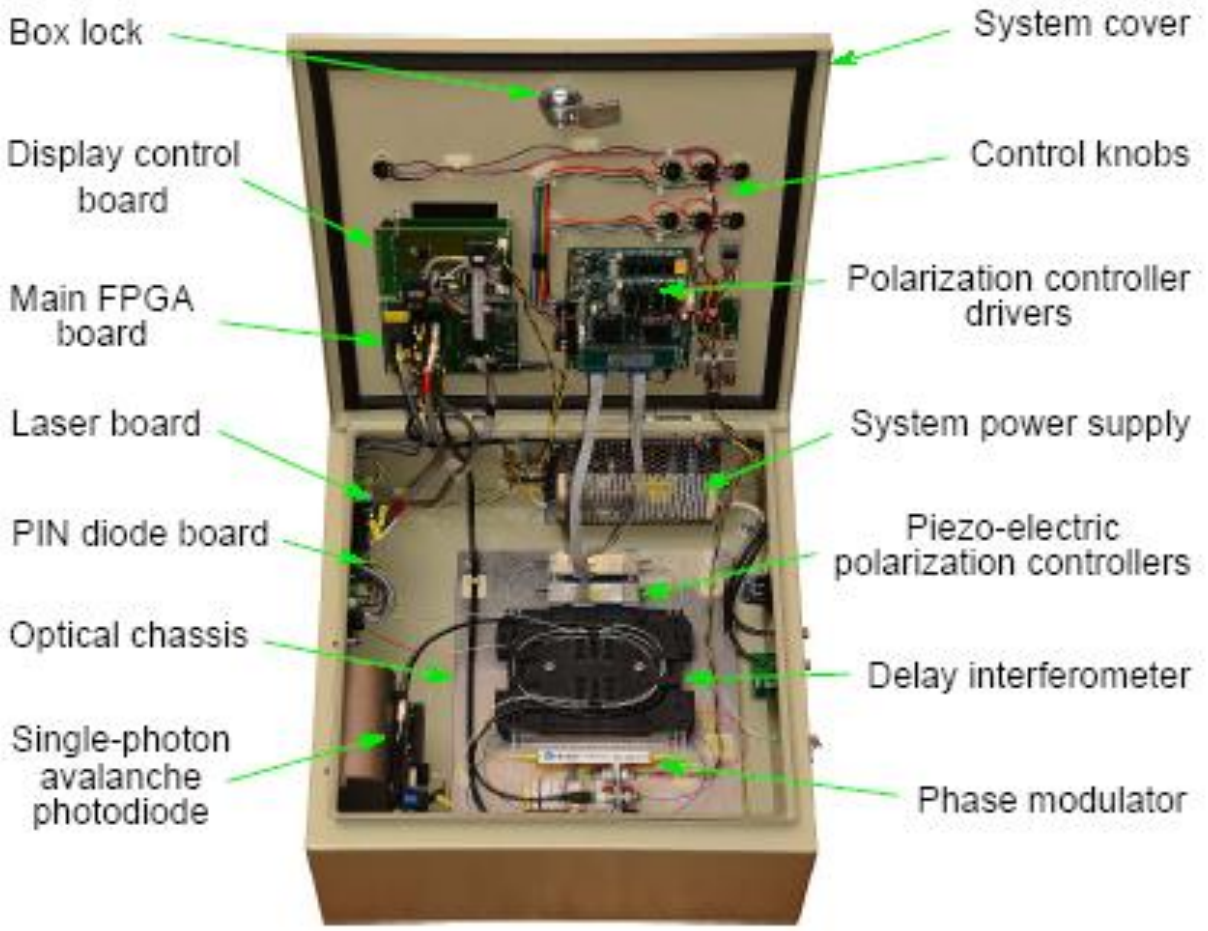
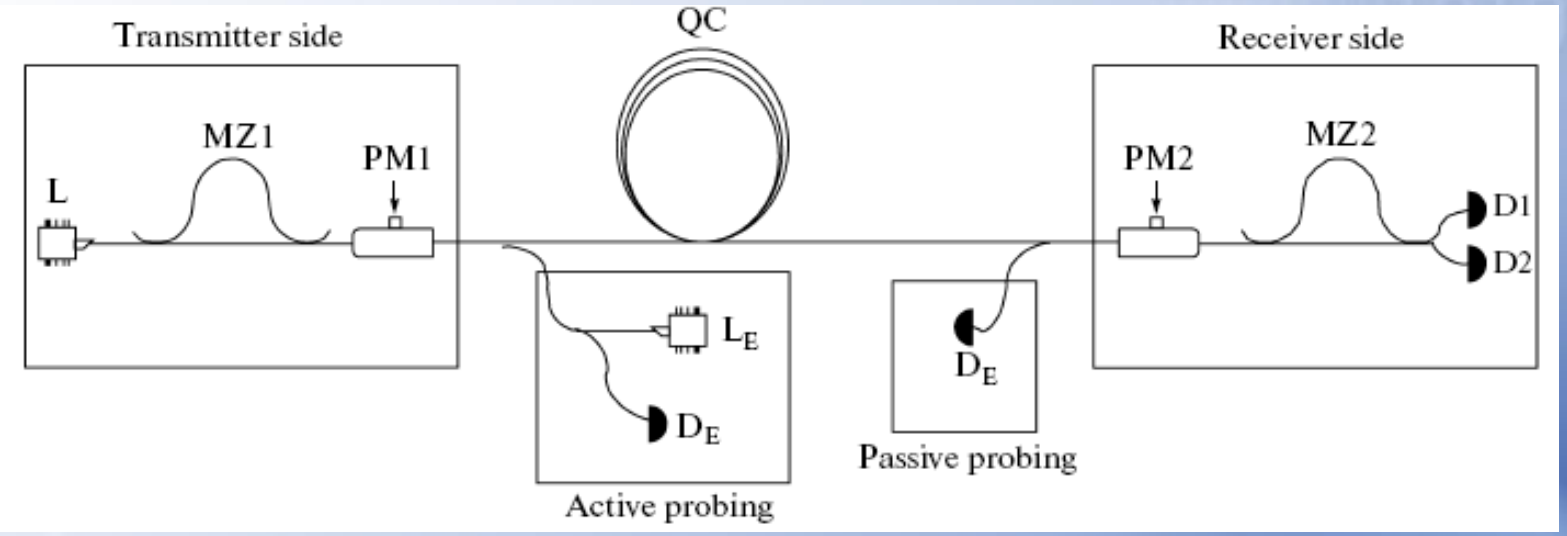
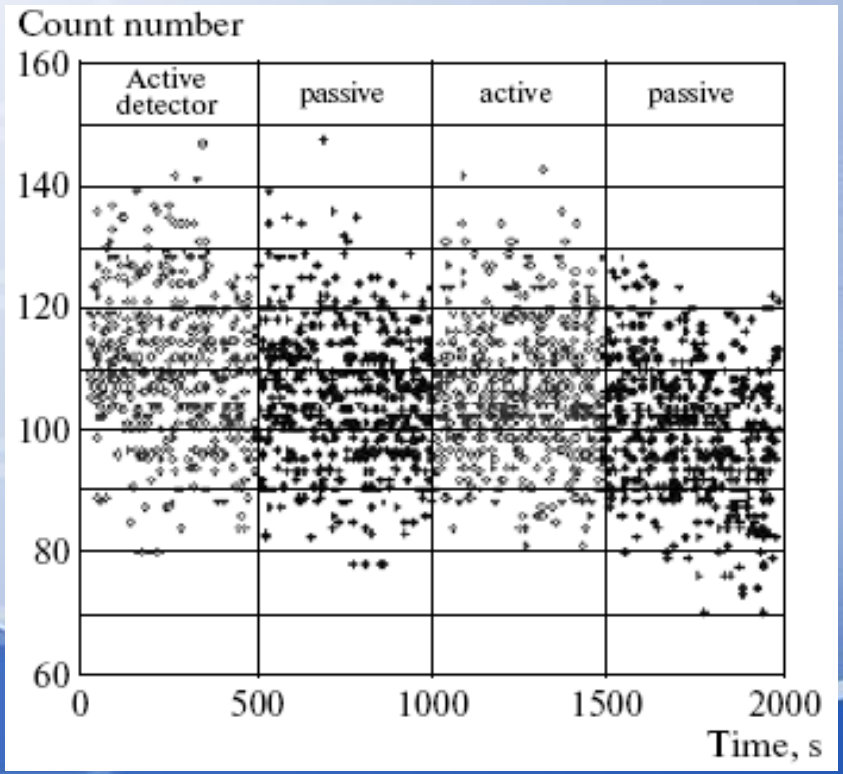


FIG. 6: **Hardware implementation of the Bob's station.** The station is packaged in a metal box with a cover, which has control knobs, buttons, and a small LCD display for visualization of the main operation parameters. It connects to a computer via a USB cable for transmission of the obtained raw keys as well as for exchange of control information.

Активное зондирование и побочные каналы

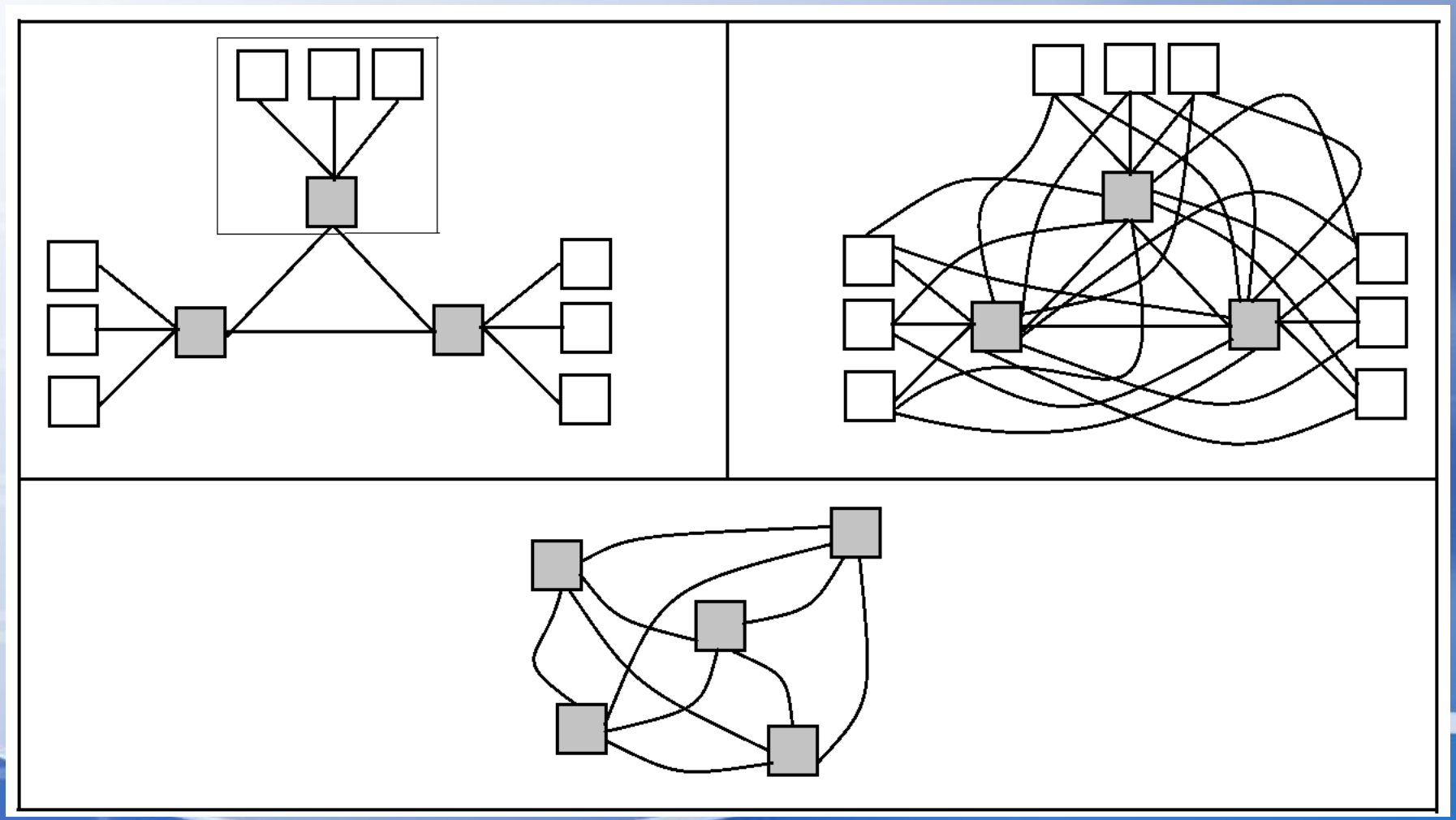


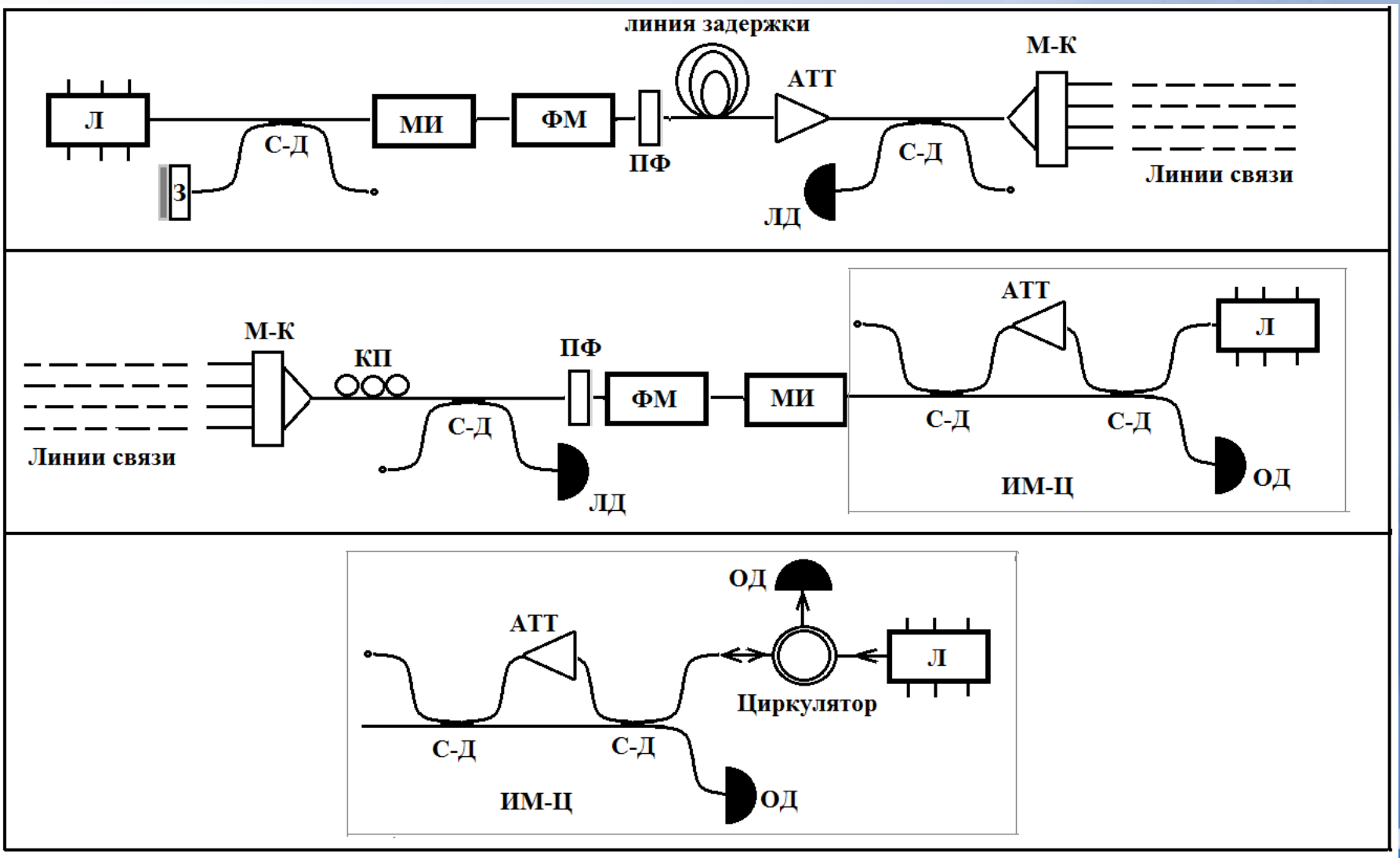


М.Т.Калашников

Все нужное просто.
Что сложно, то не нужно.

5. Реконфигурируемые сети с квантовым распределением ключей.




линия задержки
Л
З
С-Д
МИ
ФМ
ПФ
АТТ
М-К
ЛД
С-Д
Линии связи
Линии связи
М-К
КП
ПФ
ФМ
МИ
С-Д
ЛД
АТТ
Л
С-Д
С-Д
ОД
ИМ-Ц
ОД
АТТ
Л
Циркулятор
С-Д
С-Д
ИМ-Ц
ОД

6. Где и что у кого есть?

nature photonics

LETTERS

PUBLISHED ONLINE: 9 FEBRUARY 2015 | DOI: 10.1038/NPHOTON.2014.327

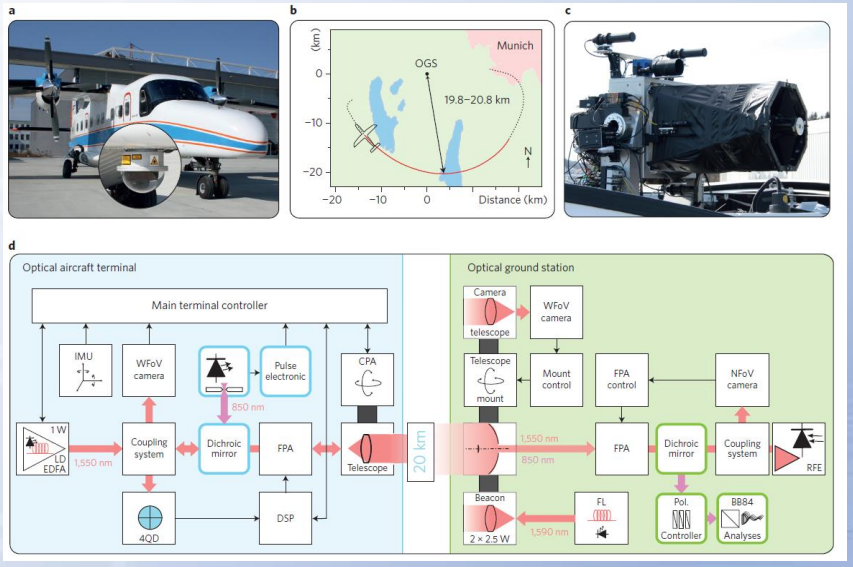
Provably secure and practical quantum key distribution over 307 km of optical fibre

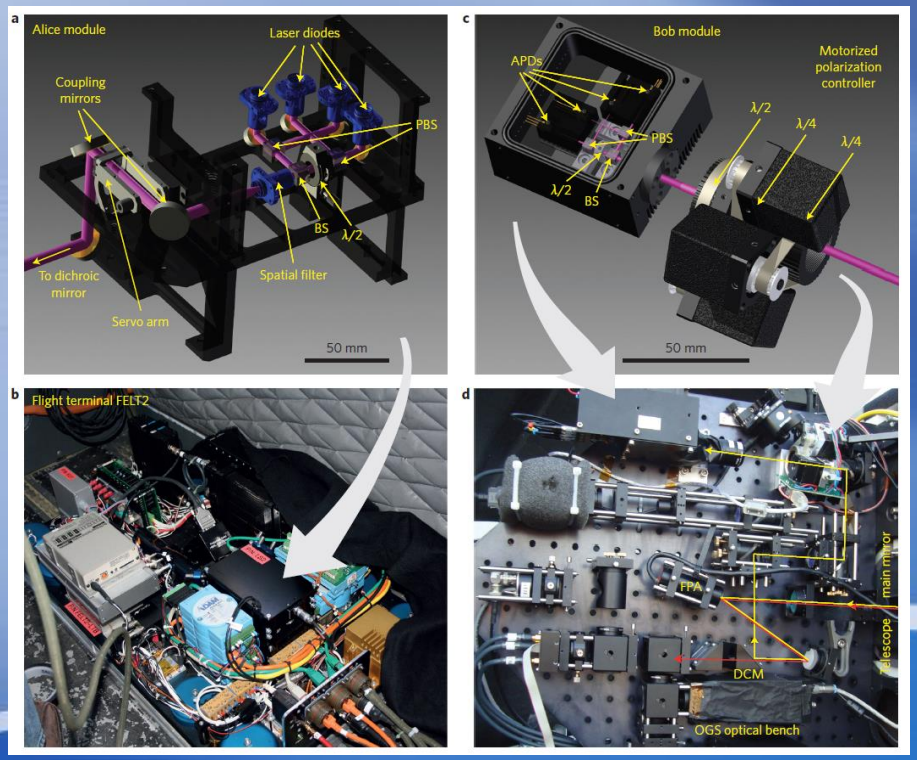
Boris Korzh[1]*, Charles Ci Wen Lim[1]*, Raphael Houlmann[1], Nicolas Gisin[1], Ming Jun Li[2], Daniel Nolan[2], Bruno Sanguinetti[1], Rob Thew[1] and Hugo Zbinden[1]

LETTERS
PUBLISHED ONLINE: 31 MARCH 2013 | DOI: 10.1038/NPHOTON.2013.46
nature photonics

Air-to-ground quantum communication

Sebastian Nauerth[1]*, Florian Moll[2], Markus Rau[1], Christian Fuchs[2], Joachim Horwath[2], Stefan Frick[1] and Harald Weinfurter[1,3]





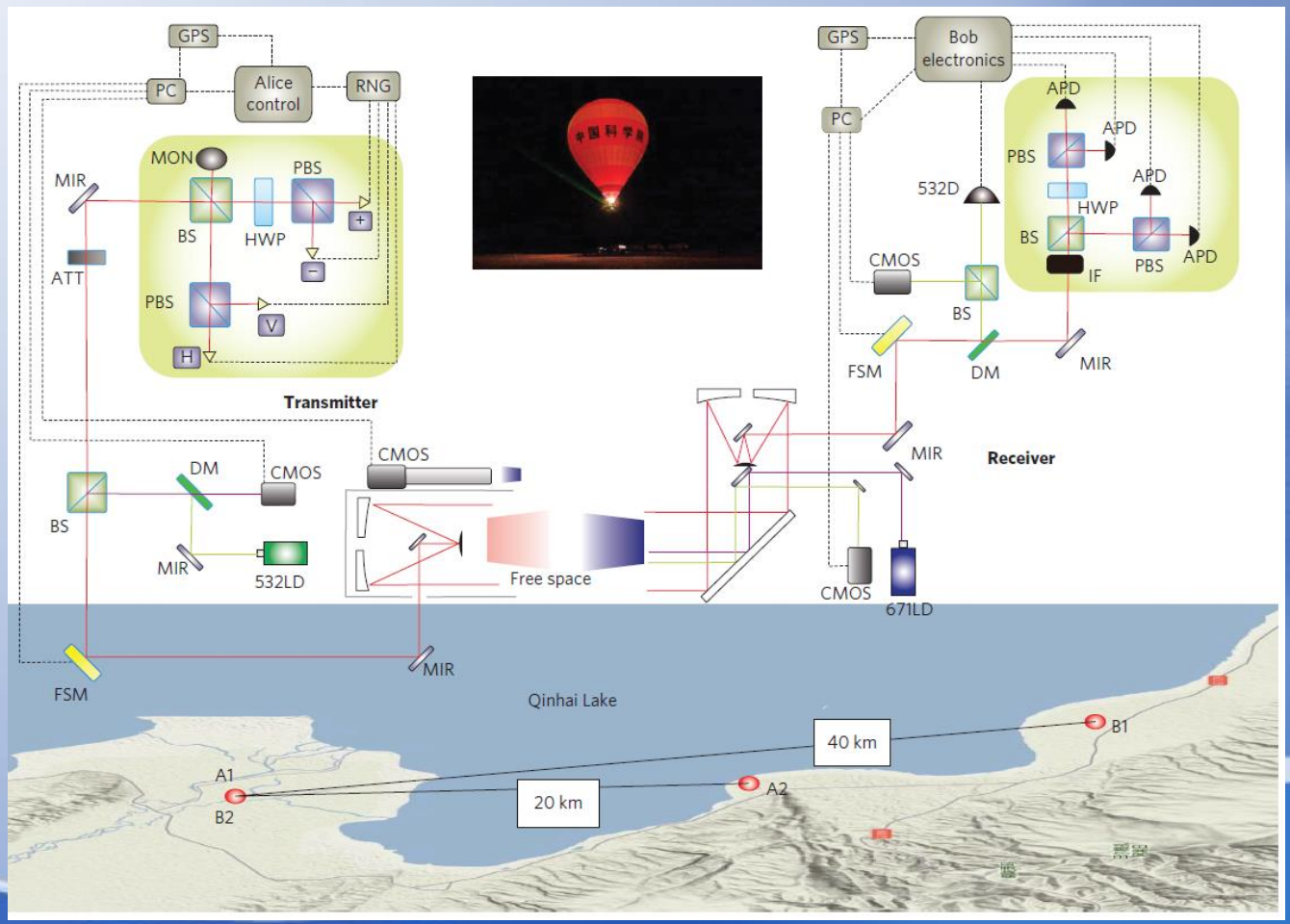
nature photonics

ARTICLES

PUBLISHED ONLINE: 21 APRIL 2013 | DOI: 10.1038/NPHOTON.2013.89

Direct and full-scale experimental verifications towards ground–satellite quantum key distribution

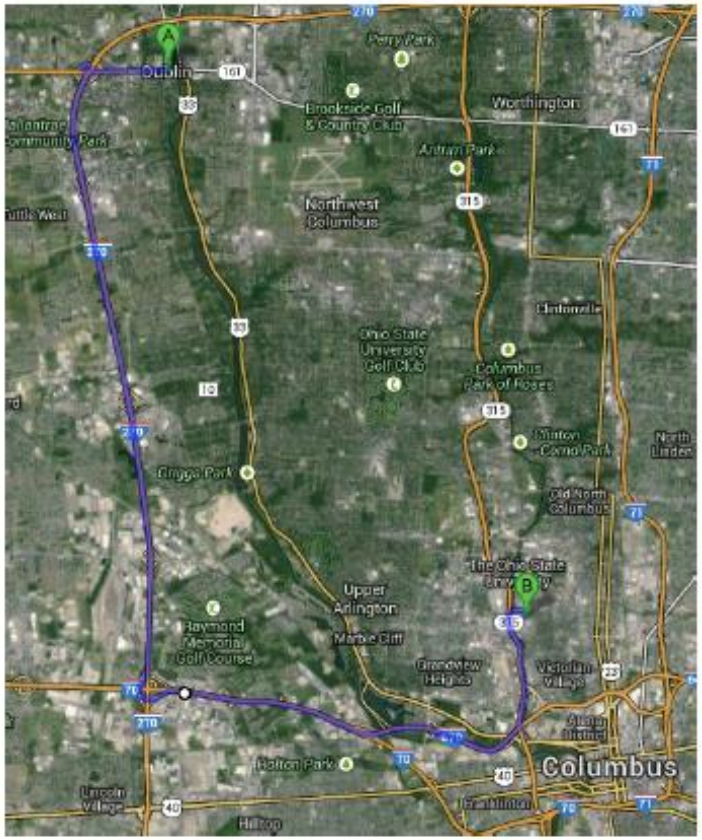
Jian-Yu Wang[1,2†], Bin Yang[1†], Sheng-Kai Liao[1,2], Liang Zhang[2], Qi Shen[1], Xiao-Fang Hu[1], Jin-Cai Wu[2], Shi-Ji Yang[2], Hao Jiang[2], Yan-Lin Tang[1], Bo Zhong[3], Hao Liang[1], Wei-Yue Liu[3], Yi-Hua Hu[2], Yong-Mei Huang[4], Bo Qi[4], Ji-Gang Ren[1], Ge-Sheng Pan[1], Juan Yin[1], Jian-Jun Jia[2], Yu-Ao Chen[1], Kai Chen[1], Cheng-Zhi Peng[1]* and Jian-Wei Pan[1]*



Enterprise: Corporate Data & IP

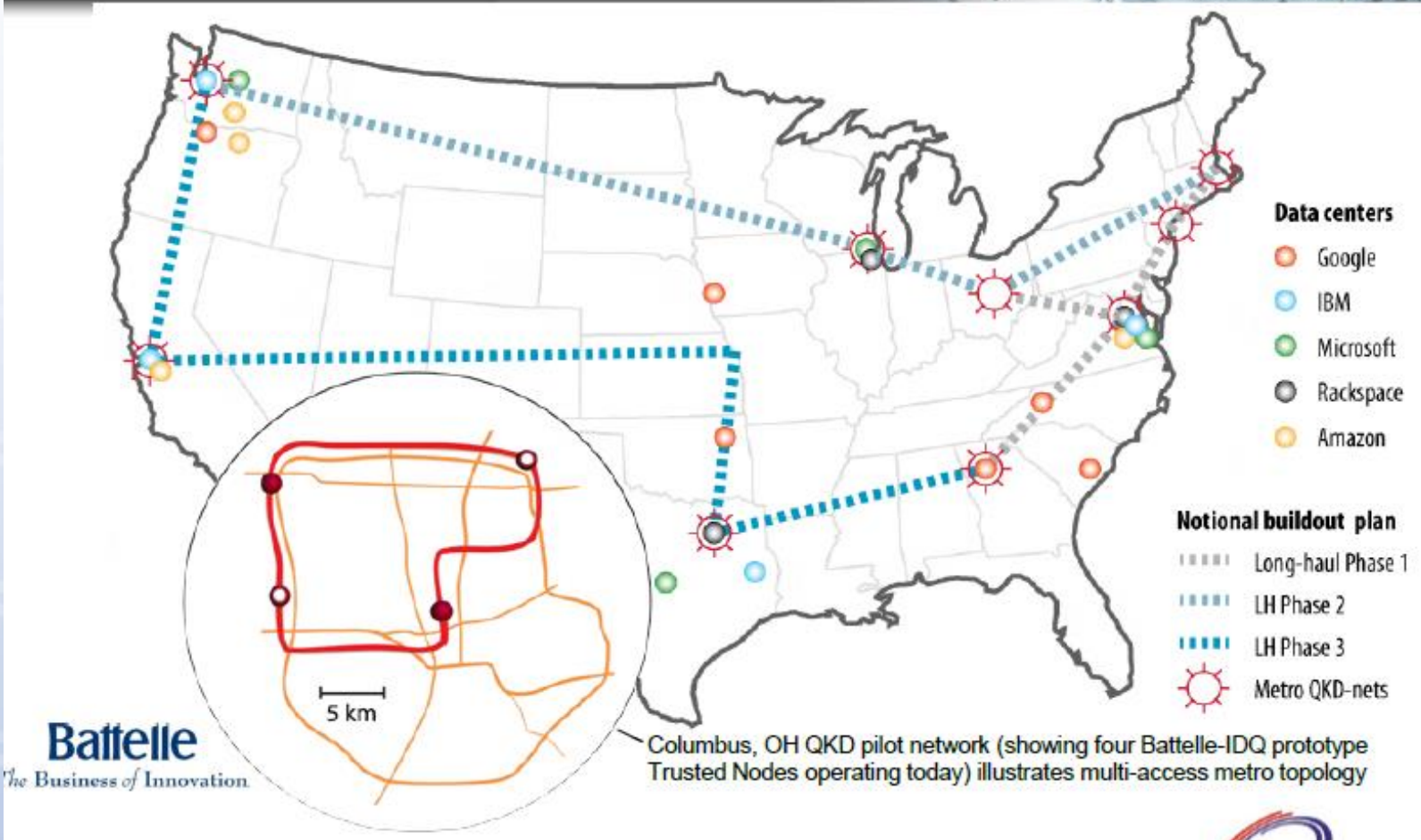
Battelle
The Business of Innovation

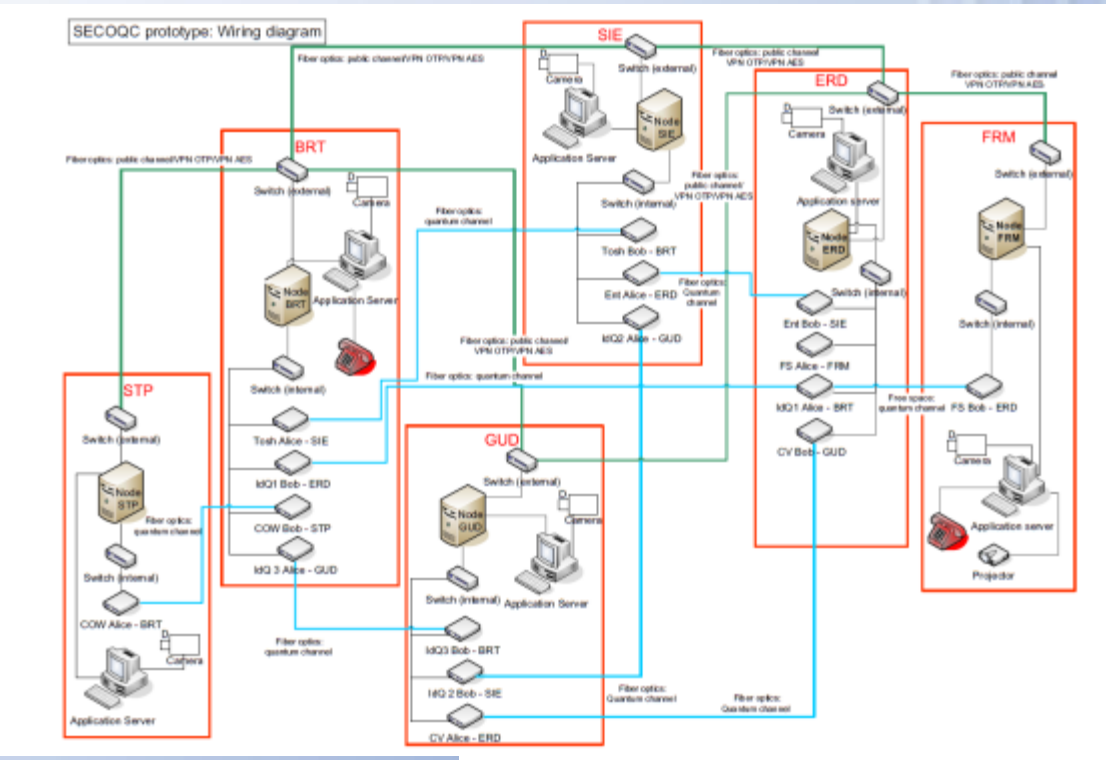
- Battelle USA
  - World's largest nonprofit R&D organization
  - Over 22,000 employees at more than 130 locations globally
- Requirement to protect mission critical corporate, financial information & intellectual property (designs, drawings, etc)
- IDQ's quantum cryptography used to secure critical links between headquarters in Columbus Ohio and satellite office in Dublin Ohio
- By 2015 will connect Battelle building in Washington DC with QKD-secured link
  - Working with IDQ to develop trusted nodes for increased distance of QKD

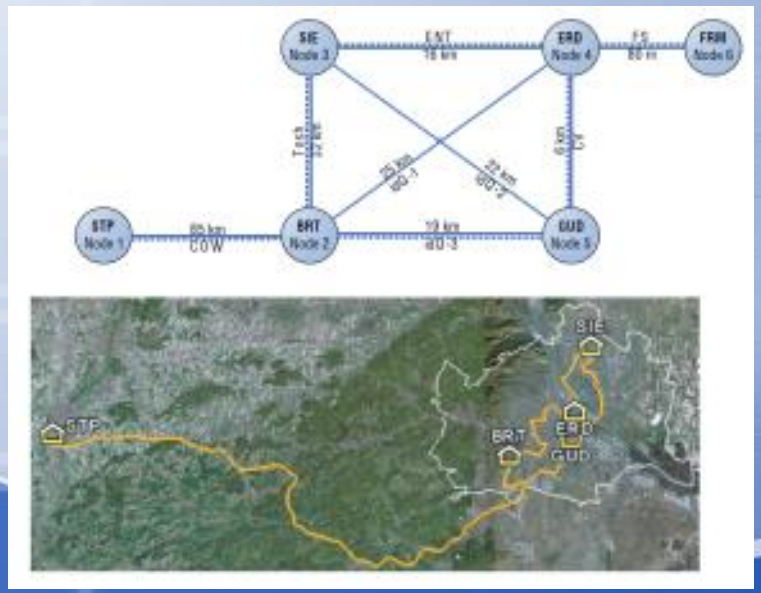


IDQ
FROM VISION TO TECHNOLOGY

2015: IDQ-Battelle quantum backbone for long-term inter-datacenter security







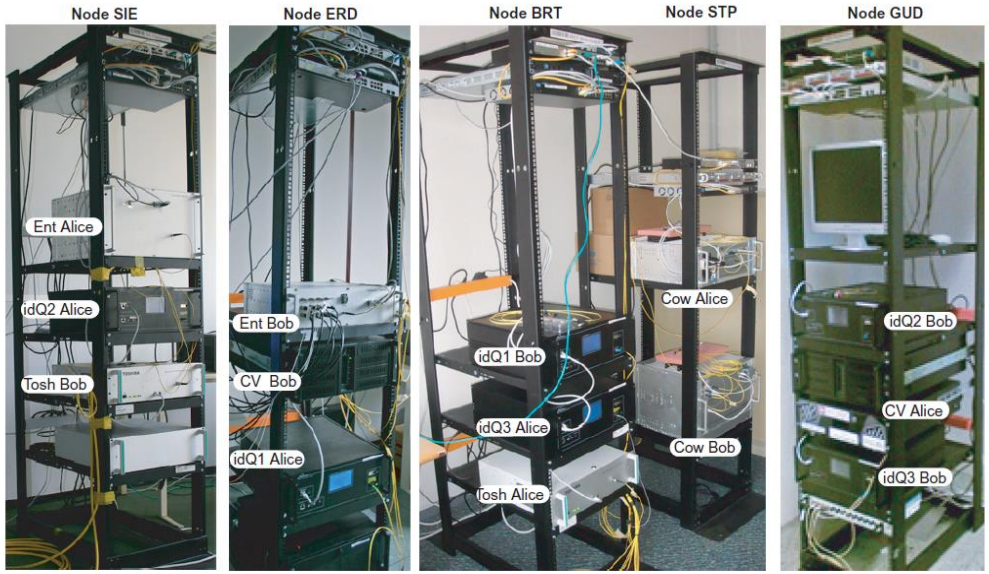


Figure 5. Photographs of the SECOQC network node racks.

Tokyo QKD Network

- NEC, Mitsubishi Electric, NTT, NICT, Toshiba Research Europe Ltd. (UK), ID Quantique (Switzerland) All Vienna (Austria)

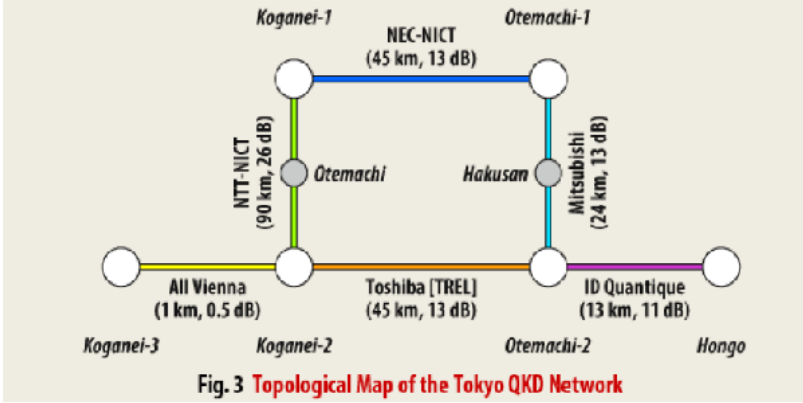


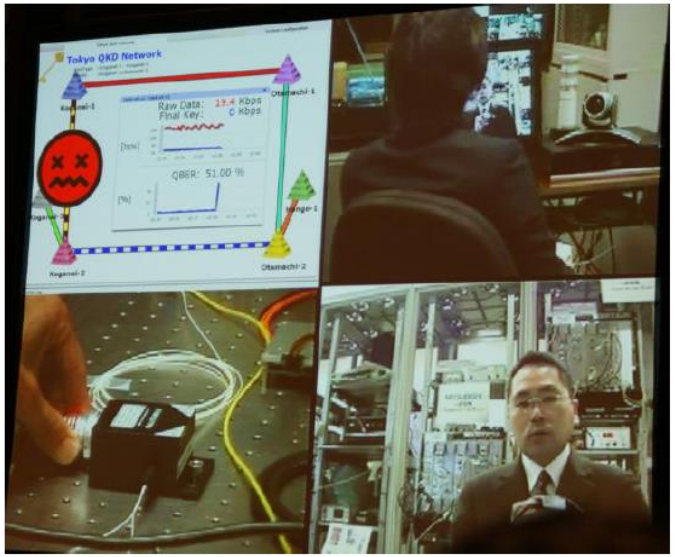
Fig. 3 Topological Map of the Tokyo QKD Network

Network Layout

- Make use of JGN2plus
- Star network

Fig. 1 Network Layout of the Tokyo QKD Network

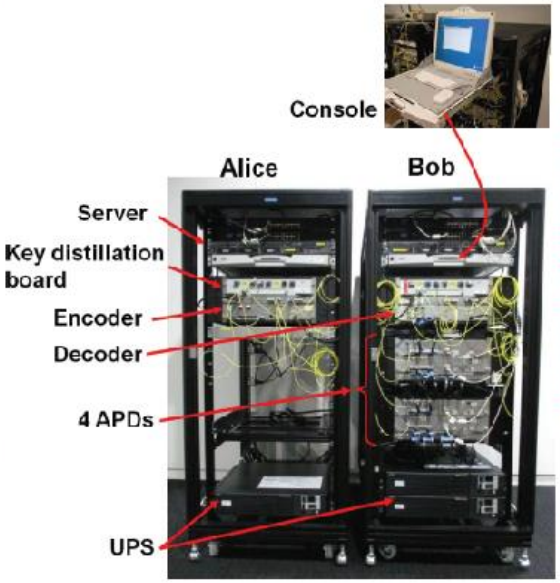
Secure Video Conference

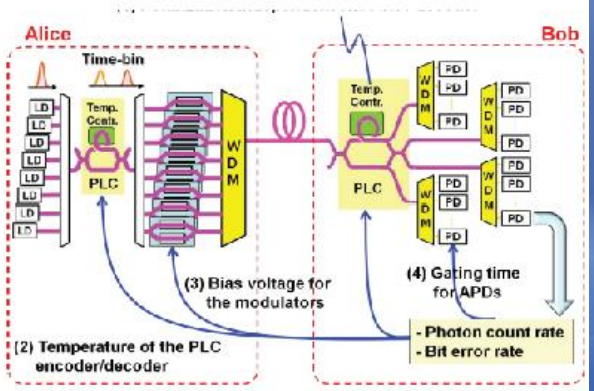


Alice


NICT

Bob


Console
Alice
Bob
Server
Key distillation board
Encoder
Decoder
4 APDs
UPS


Alice
Bob
Time-bin
Temp. Contr.
PLC
WDM
PD
LD
(3) Bias voltage for the modulators
(4) Gating time for APDs
(2) Temperature of the PLC encoder/decoder
- Photon count rate
- Bit error rate

Korean government plan

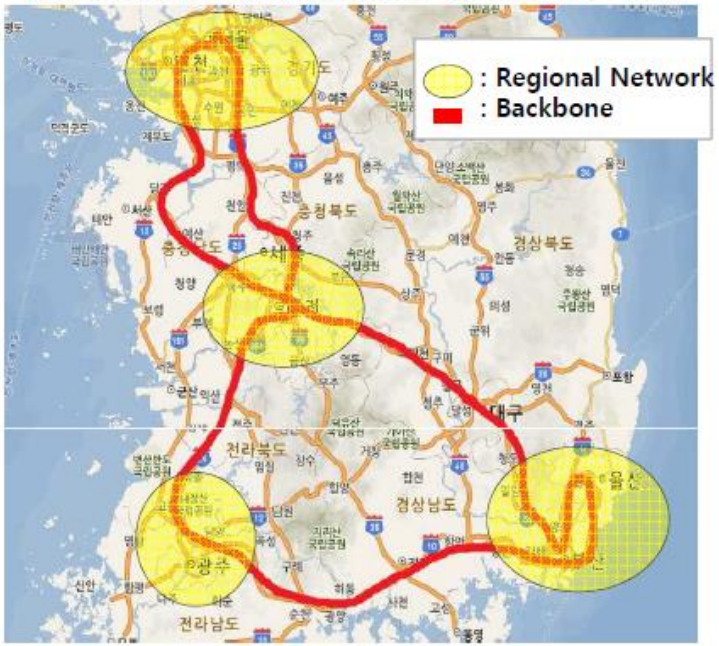
[Quantum R&D Testbed(~'15)]

- SKT(Bundang) – KIST(Suwon) – NSTR(Seoul)

[Quantum Backbone(~'17)]

- Seoul-Southern Gyeonggi-Sejong-Daejeon

[National Administrative Network ~'20)]



- Tentative the number of nodes

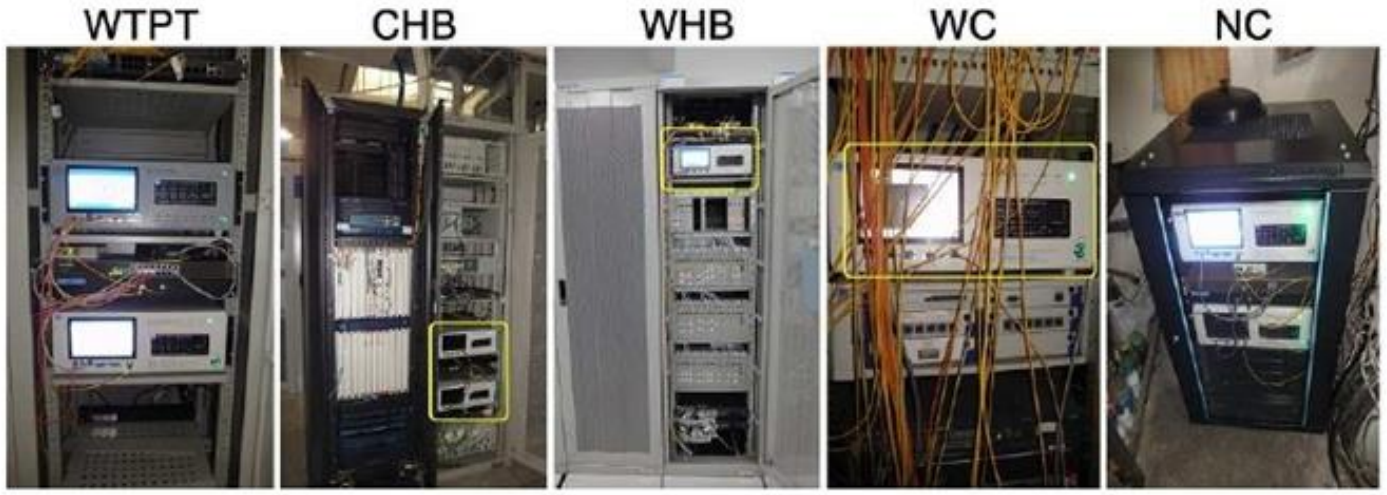
Category	# of node	비고
Public Administration	347	National wide office
Prosecutor & Police Office	2,264	National wide office
Post Office	3,562	National wide office

- Extend to defense and financial institute
  - Defense comm.: 516 nodes
  - Financial Institute(1tier) 8275 nodes(incl. branches)

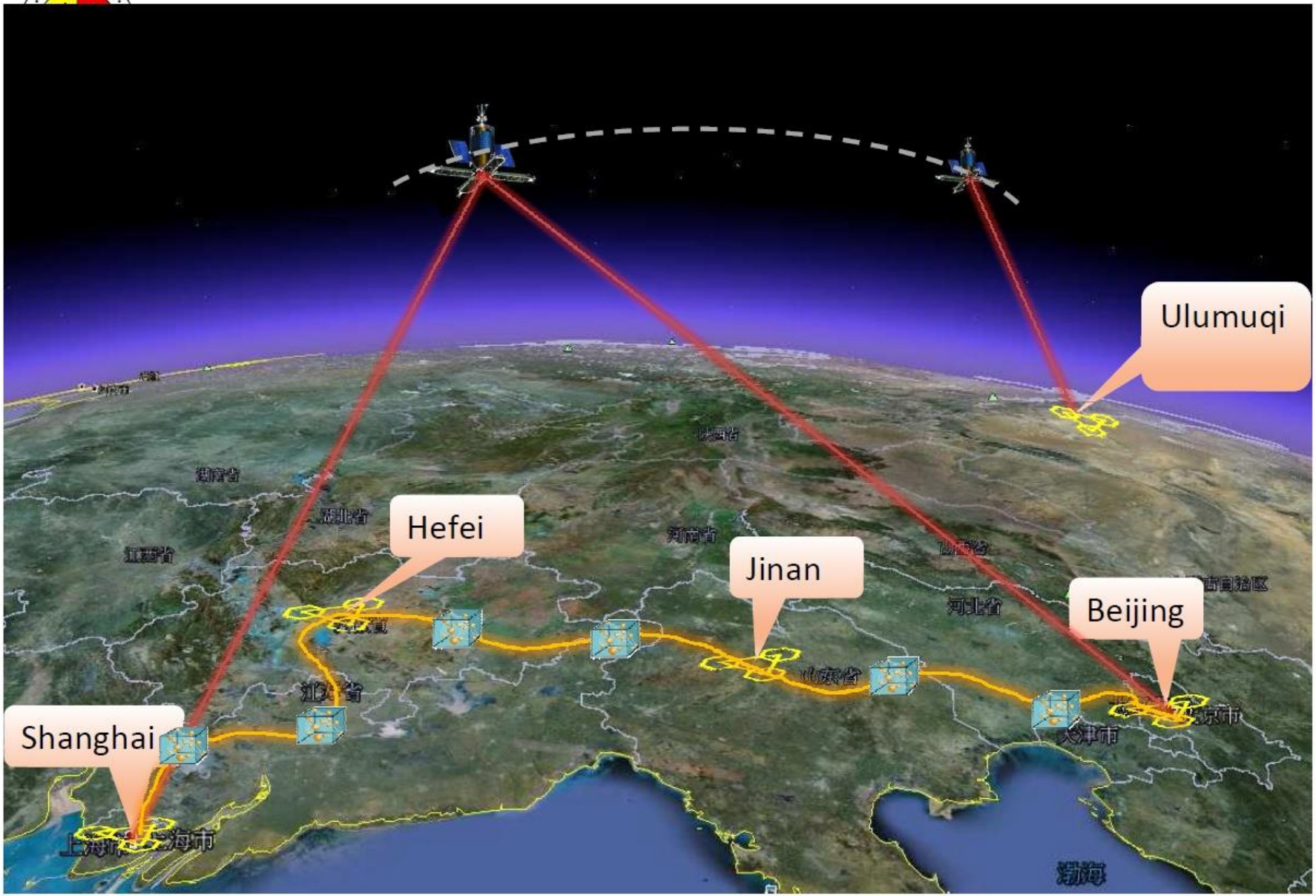
Chinese Trusted node Quantum network

- Total Length 2000 km
- 2013.6-2016.12
- 32 trustable relay nodes
  31 fiber links
- Metropolitan networks
  Existing: Hefei, Jinan
  New: Beijing, Shanghai
- Total Investment: 560 M RMB. Half by NDRC, Half by Local government
- Customer: China Industrial & Commercial Bank; Xinhua News Agency; CBRC

. Geographic distribution of the Hefei-Chaohu-Wuhu wide area QKD network, which connects three cities – Hefei, Chaohu, and Wuhu.

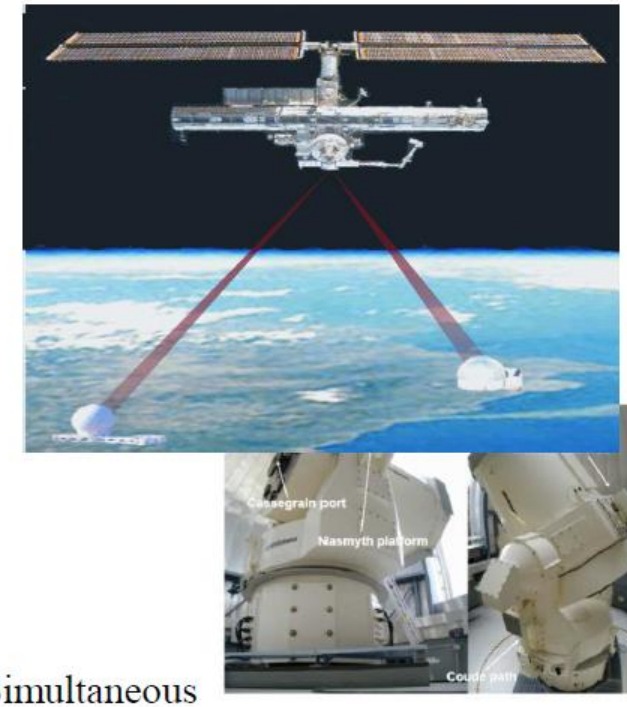


Chinese Trusted node Quantum network



Proposals for quantum communication in space

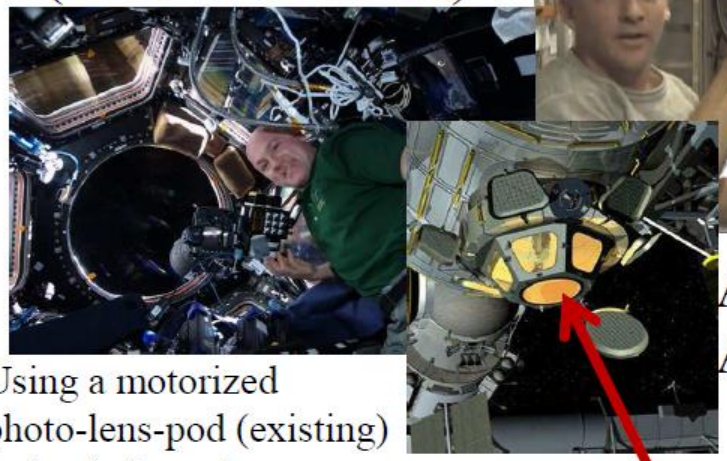
Dual-downlink
(ROM R&D 47 M€)



Simultaneous optical downlink: 1400 km separation.

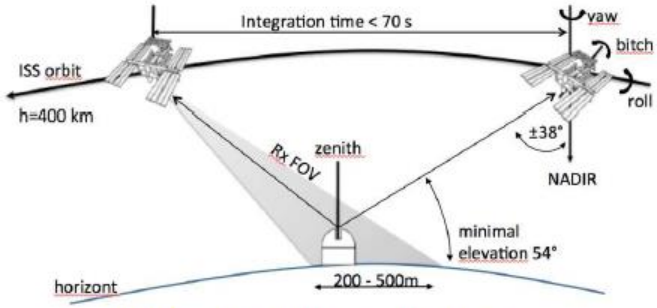
R. Ursin et al., Europhysics News, 26-29, 40–40 (3) (2009)

Single-uplink
(ROM R&D 1 M€)



Using a motorized photo-lens-pod (existing) and a dedicated quantum detector as "camera".

Astronaut: A. Kuipers

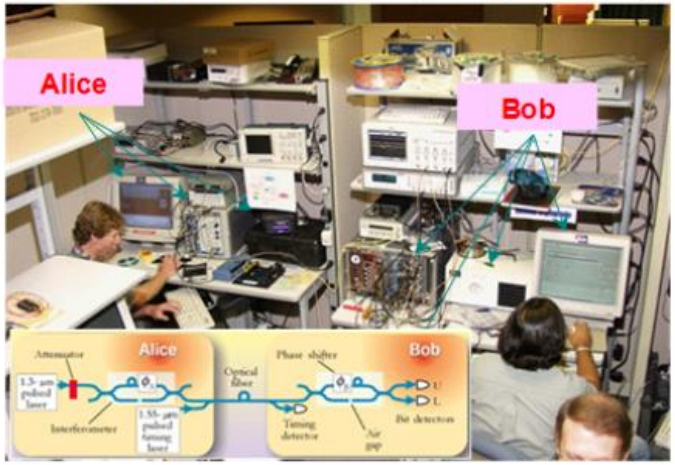


T. Scheidl, E. Wille, and R. Ursin, New Journal of Physics, 15, 043008 (2013)

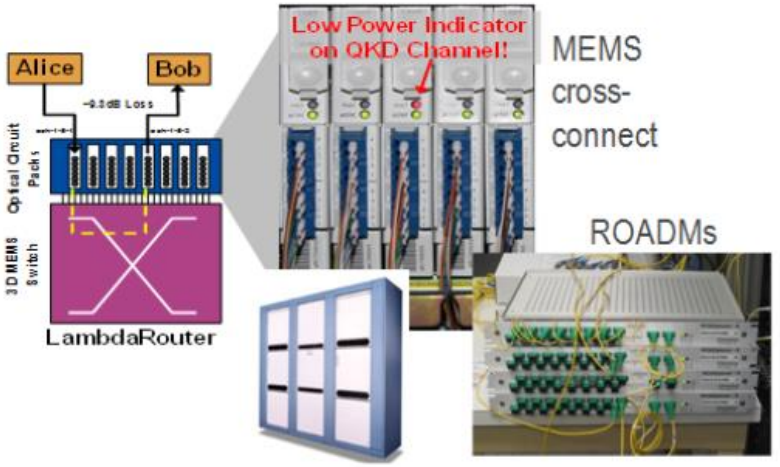
Rupert.Ursin@oeaw.ac.at - Institute for Quantum Optics and Quantum Information, Austrian Academy of Sciences

Telcordia Experience: Quantum Networks

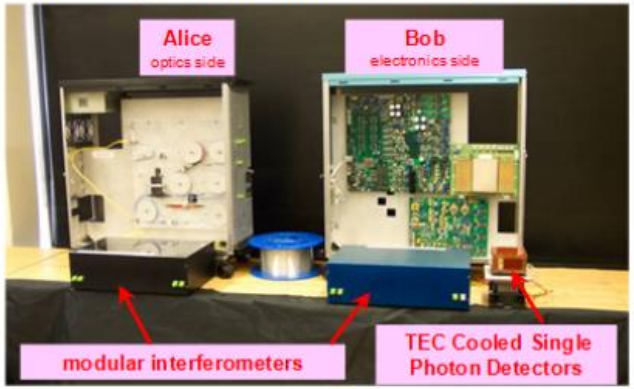
LANL 2nd generation fiber QKD system (F2)



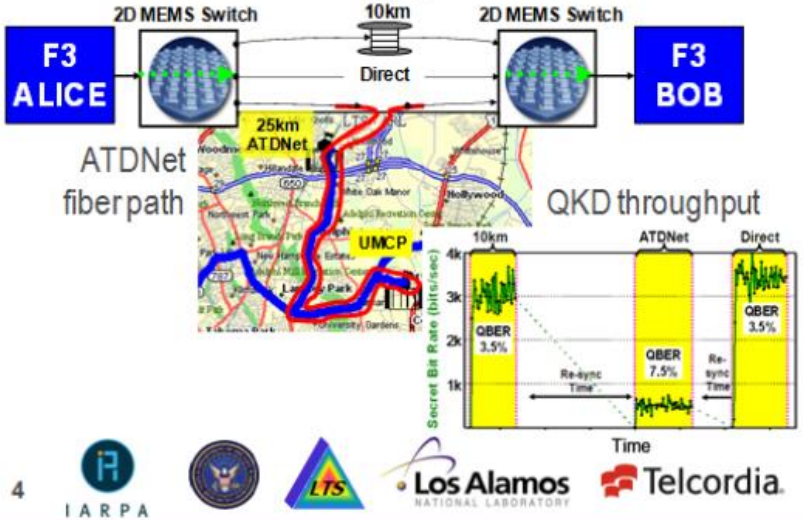
QKD Transmission through all-optical switches



LANL 3rd generation fiber QKD system (F3)



QKD Transmission through optical switches and ATDNet

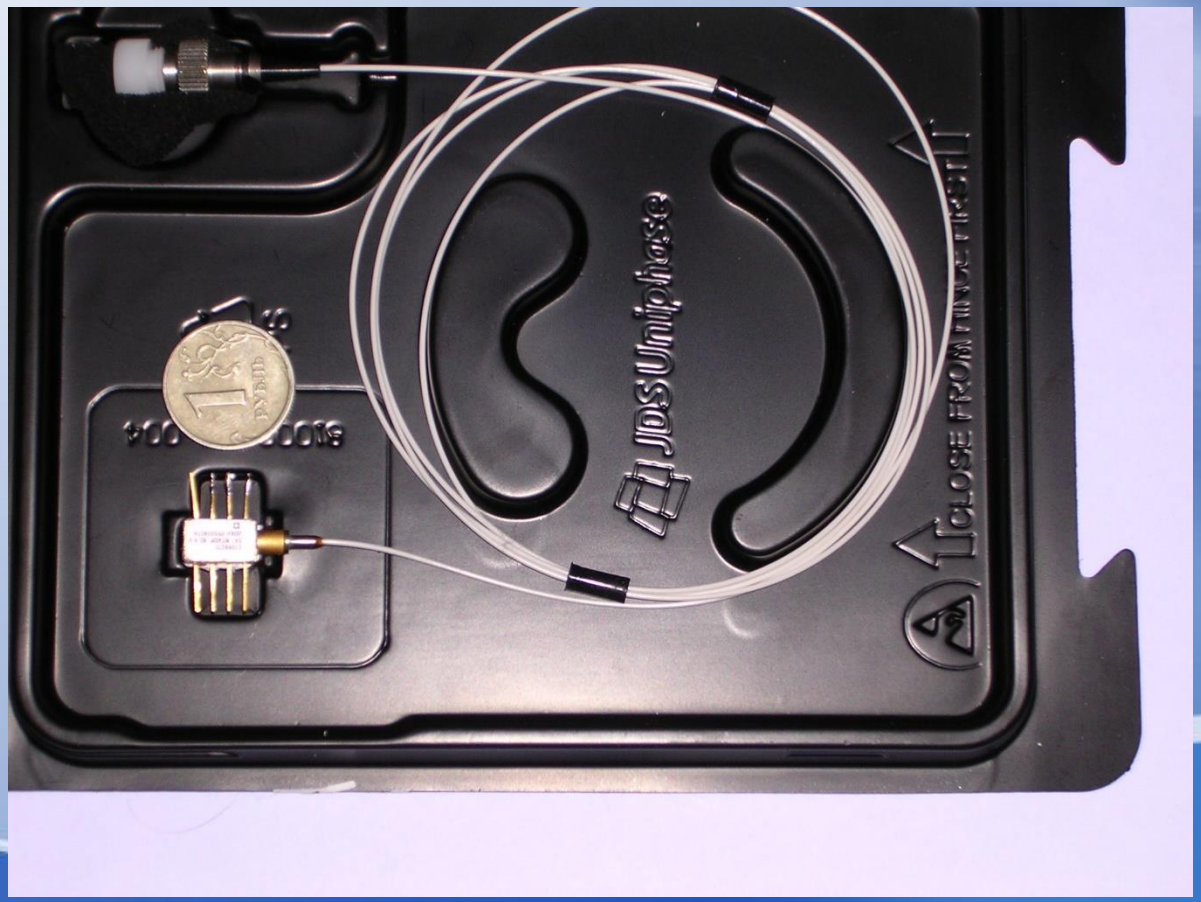


Ref: R. J. Hughes and T.E. Chapuran, "Introduction to Quantum Cryptography", *Optical Fiber Communications (OFC) Short Course*, Los Angeles, CA, 2011

IARPA Los Alamos NATIONAL LABORATORY Telcordia

Часть III.

1. Вопросы, которые требуется решить (интегрирование в имеющиеся шифр-средства, устойчивость относительно активного зондирования, инфраструктура, элементная база).



Hacking commercial quantum cryptography systems by tailored bright illumination

Lars Lydersen,[1,2,a)] Carlos Wiechers,[3,4,5] Christoffer Wittmann,[3,4] Dominique Elser,[3,4] Johannes Skaar,[1,2] and Vadim Makarov[1]

[1)] *Department of Electronics and Telecommunications, Norwegian University of Science and Technology, NO-7491 Trondheim, Norway*

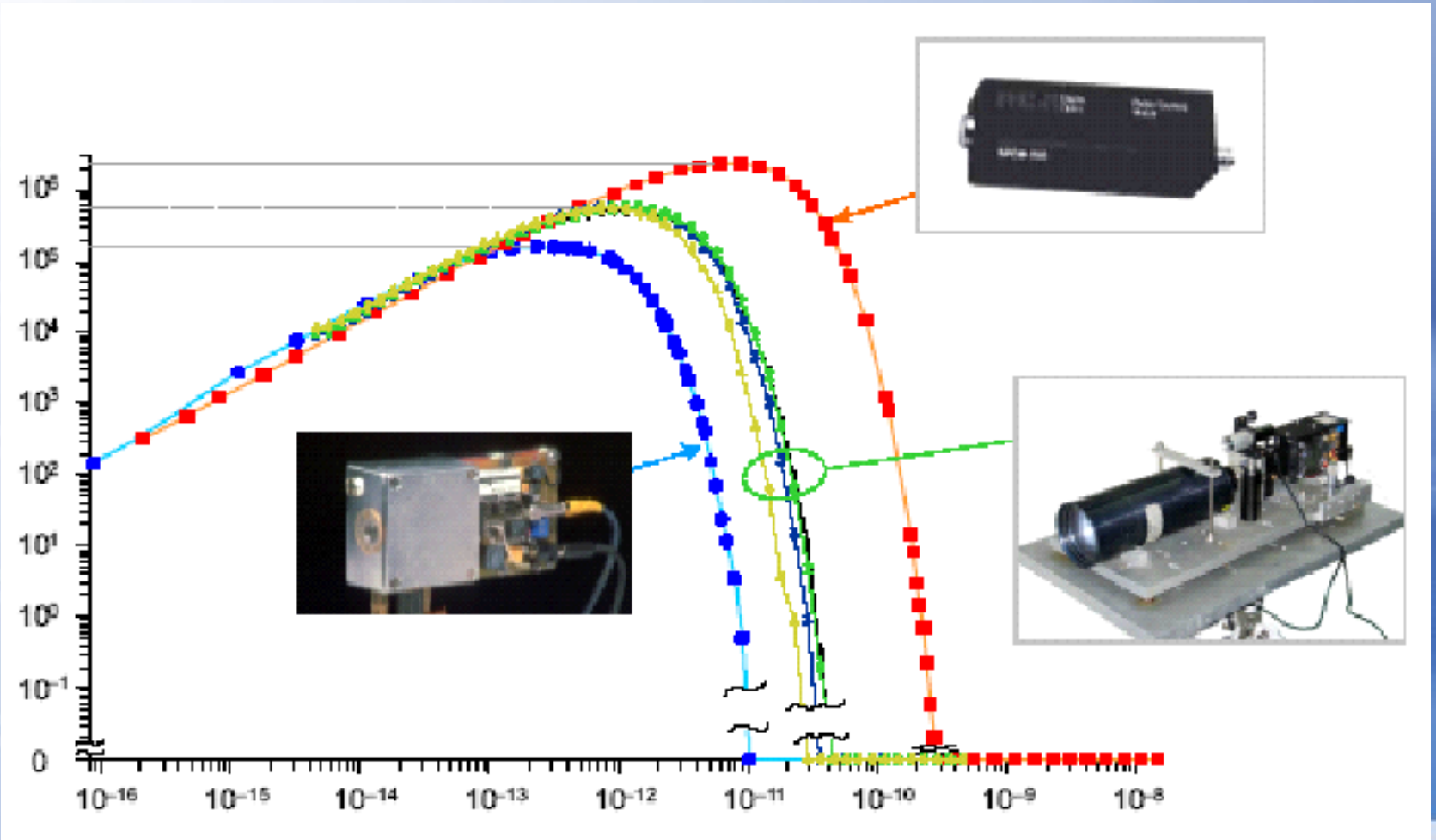
[2)] *University Graduate Center, NO-2027 Kjeller, Norway*

[3)] *Max Planck Institute for the Science of Light, Günther-Scharowsky-Str. 1/Bau 24, 91058 Erlangen, Germany*

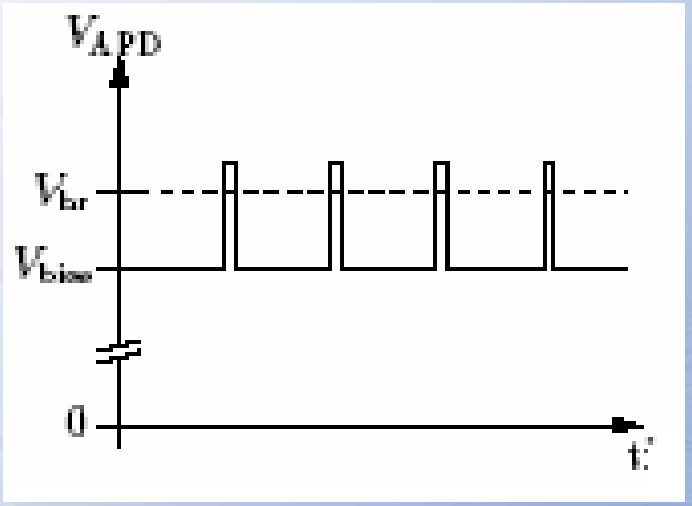
[4)] *Institut für Optik, Information und Photonik, University of Erlangen-Nuremberg, Staudtstraße 7/B2, 91058, Erlangen, Germany*

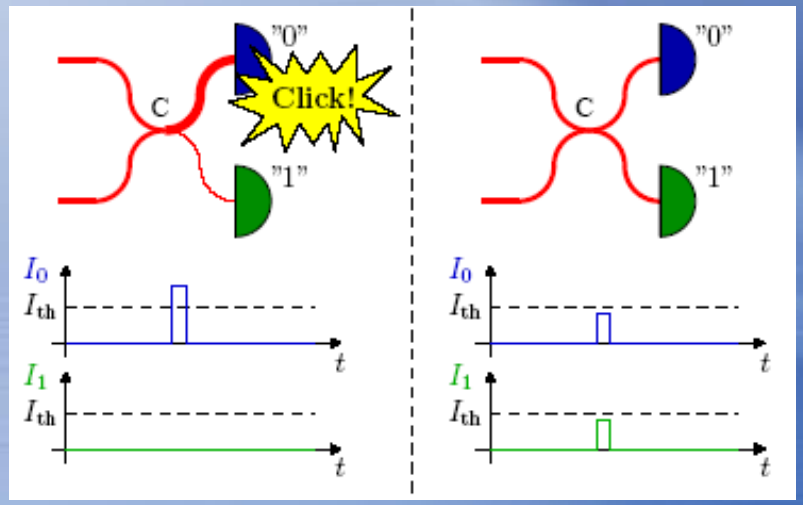
[5)] *Departamento de Física, Universidad de Guanajuato, Lomas del Bosque 103, Fraccionamiento Lomas del Campestre, 37150, León, Guanajuato, México*

Эффект ослепления

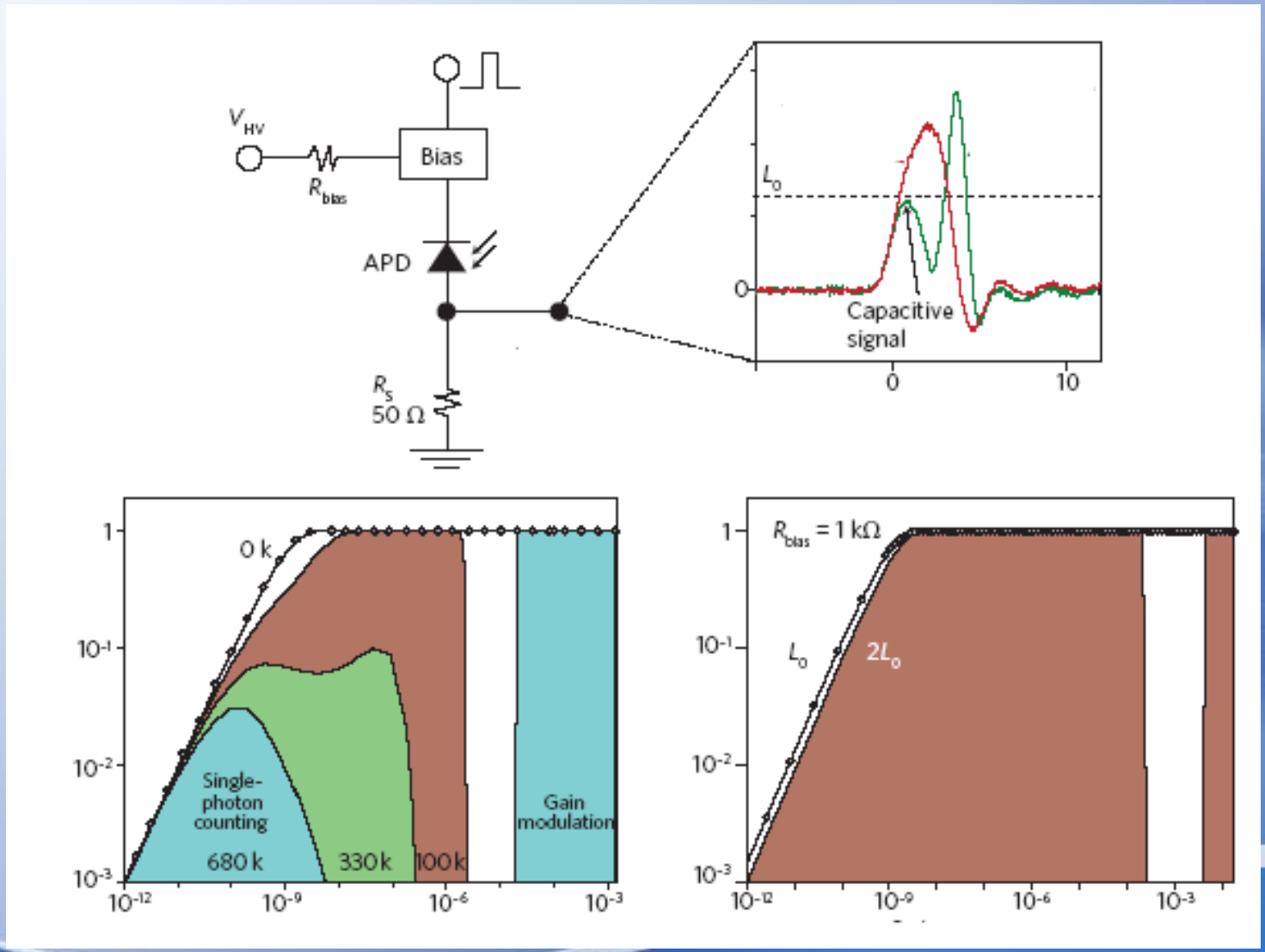


2.2 Атака на ключ посредством перевода лавинных фотодетекторов в классический режим фотодетектирования





Avoiding the blinding attack in QKD



ЖЭТФ, 2012, том 141, вып. 3, стр. 1–20

ОБ УЯЗВИМОСТИ БАЗОВЫХ ПРОТОКОЛОВ КВАНТОВОГО РАСПРЕДЕЛЕНИЯ КЛЮЧЕЙ И О ТРЕХ ПРОТОКОЛАХ, УСТОЙЧИВЫХ К АТАКЕ С «ОСЛЕПЛЕНИЕМ» ЛАВИННЫХ ФОТОДЕТЕКТОРОВ

С. Н. Молотков[*]

СПАСИБО ЗА ВНИМАНИЕ.