Квантовая криптография

С.Н.Молотков

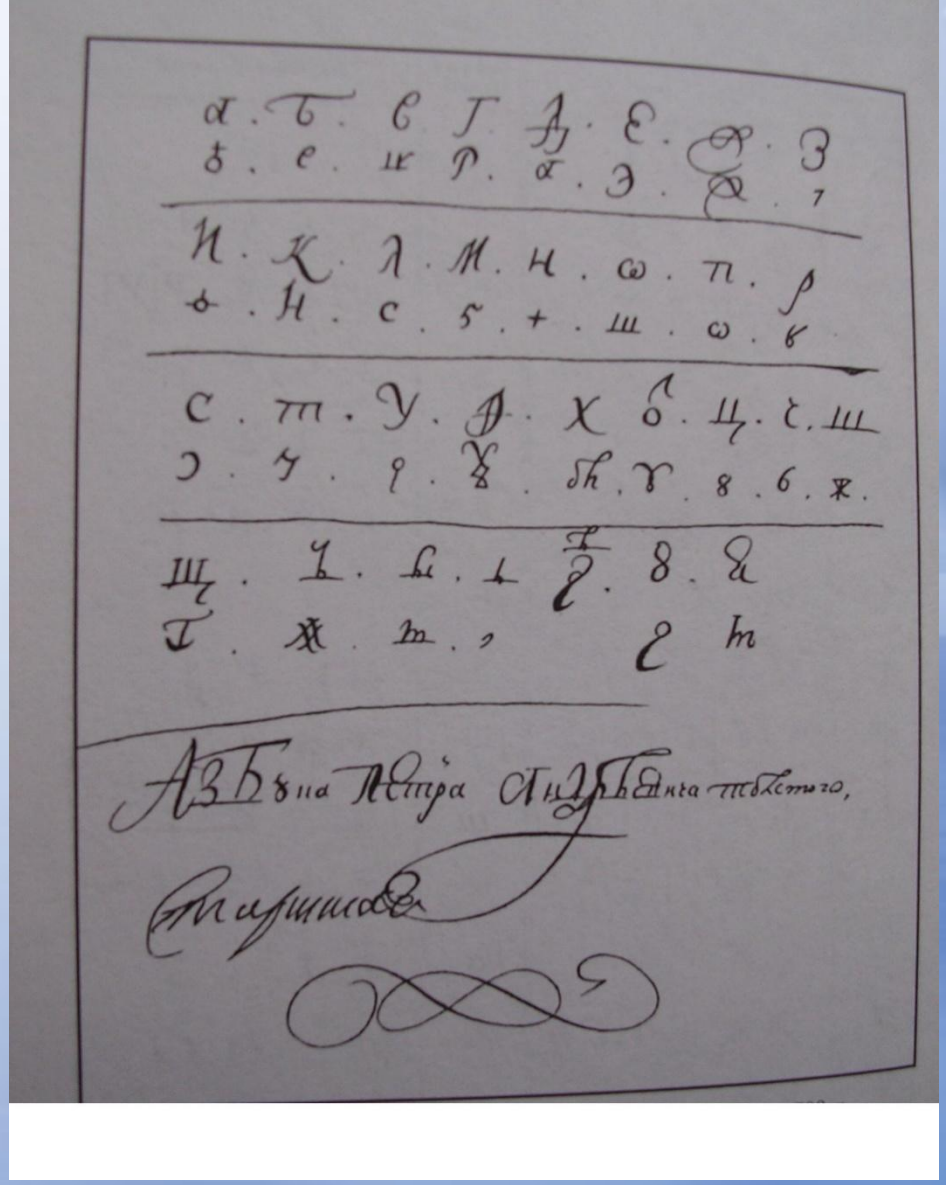
Кафедра суперкомпьютеров и квантовой информатики

ВМК, МГУ имени М.В.Ломоносова,

LOGO

Почти каждый изобретатель системы шифрования убежден в невозможности взлома своего детища.

Дэвид Кан



Шифр простой замены (“Цифирь”), написанная рукой Петра I (1700 год)

Копия.

Указъ Нашему Сенату.

Всемилостивѣйше пожаловали мы обрѣтающагося при Академии наукъ въ Сенатъ роты Ададурова въ Сенатские Секретари съ годовымъ жалованьемъ по тысячѣ по пятисотъ рублевъ его; и быть ему при собрании иностранныхъ словъ съ Академиею наукъ его обучениемъ; а помянутое ему опредѣленное жалованье получать ему изъ Сенатской Канторы, а нашему Сенату учинить исполнение по сему нашему указу.

Подлинной за подписаниемъ Ея Императорскаго Величества собственныя руки, –

Елисаветъ.

Марта 18 дня 1742 году.

Об определении в Коллегию иностранных дел бывшего при Академии наук профессора юстиц-рата Христиана Гольдбаха статским советником с жалованьем 1500 рублей, о выдаче недоданного ему в Академии наук жалованья и о выдаче ему вперед жалованья.

Россия 18 век
Христиан Гольдбах (1690-1764)
Франц Ульрих Теодор Эпинус (1724-1802)

20 век
1918 г. - один из самых замечательных трудов в области криптоанализа W.F.Friedman “The Index of Coincidence and its Applications in Cryptography”, Riverbank Labs. 1920.
1924 г. Патент на роторную шифровальную машину-- E.H.Hebern “Electronic Coding Machine”, US Patent, no/1,510,441 30 Sep.1924.

1920-1949 за одним исключением открытая литература умерла, исключение составила работа 1949 г. C.Shannon “The Communication Theory of Secrecy Systems”

Криптоанализ

- kryptós, **скрытый**
- analýein, **устранять, решать**

Term coined in 1920

by William F. Friedman.

- Born in Moldavia
- Chief cryptologist at NSA,1950s.

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.

Шифр Цезаря (58 – 51 д.н.э.)

ANYONE	KNOW	WHERE	I	CAN	GET	DECENT	PIZZA?
dqbrqh	nqrz	zkhuh	l	edq	jhw	ghfhqw	slccd?

$\mathcal{Z}_{26} = \{0, 1, \ldots, 25\}$ $k \in \mathcal{Z}_{26}$

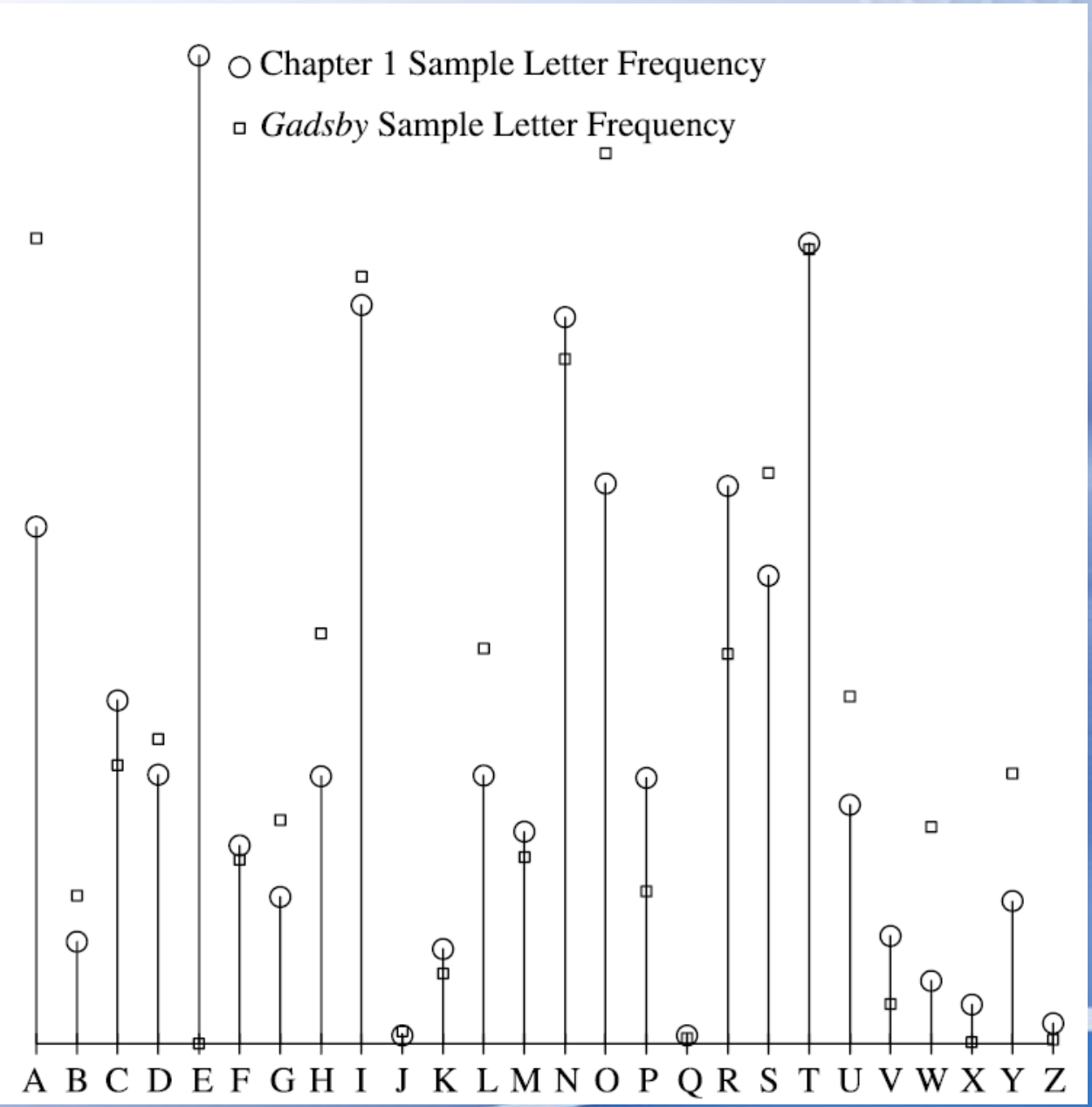
Подстановка Цезаря

$$\mathbf{C_k} : x \to y = \mathbf{C_k}(x) = (x + k) \text{ (modulo 26)}$$

Аффинный шифр Цезаря

$$\mathbf{A_{j,k}} : x \to y = \mathbf{A_{j,k}}(x) = (jx + k) \text{ (modulo 26)}$$

Не меняет частоту символов в шифре


Chapter 1 Sample Letter Frequency
Gadsby Sample Letter Frequency
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

Моноалфавитная подстановка

$$(x_0,\ x_1, \ldots, x_{n-1}) \rightarrow (y_0,\ y_1, \ldots, y_{n-1})$$

Общее правило подстановки

$$y_i = \theta(x_i)$$

Полиалфавитная подстановка

$$y_i = \theta_i(x_i), \qquad 0 \leq i < n$$

Бегущий ключ

$$\underline{k} = (k_0,\ k_1, \ldots, k_{n-1}), \qquad k_i \in \mathcal{Z}_{26}\ (0 \leq i < n)$$

$$\underline{x} = (x_0, x_1, \ldots, x_{n-1})$$

$$\underline{x} \rightarrow \underline{y} = (y_0, y_1, \ldots, y_{n-1}), \qquad y_i = C_{k_i}(x_i), \qquad 0 \leq i < n.$$

Porta's *Traicté des Chiffres* (1585)

Blaise de Vigenère 1523

A Treatise on Secret Writing

	Plaintext					
Key	A	B	C	...	Y	Z
0	a	b	c	...	y	z
1	b	c	d	...	z	a
2	c	d	e	...	a	b
	⋮	⋮	⋮	⋱	⋮	⋮
25	z	a	b	...	x	y

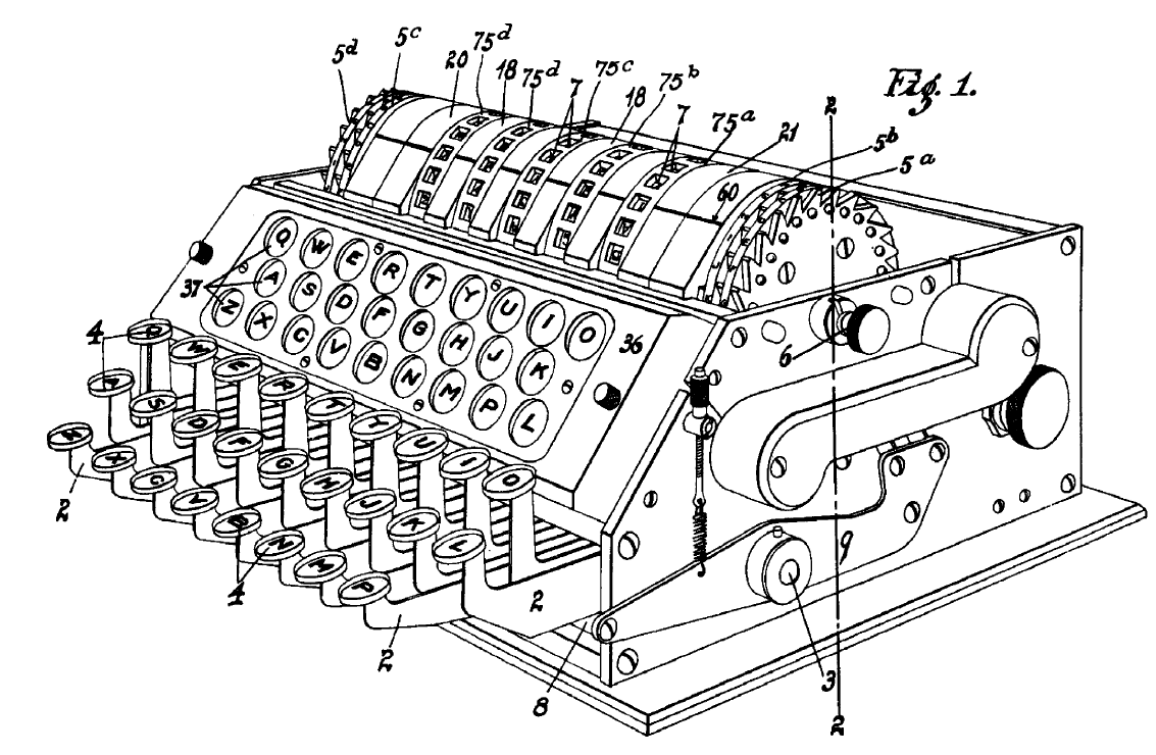
$x = \mathrm{B}$ $K = 2$ $y = \mathrm{d}$

$(k_0, k_1, \ldots, k_{r-1})$ $\underline{k} = (k_0, k_1, \ldots, k_{n-1}, \ldots)$

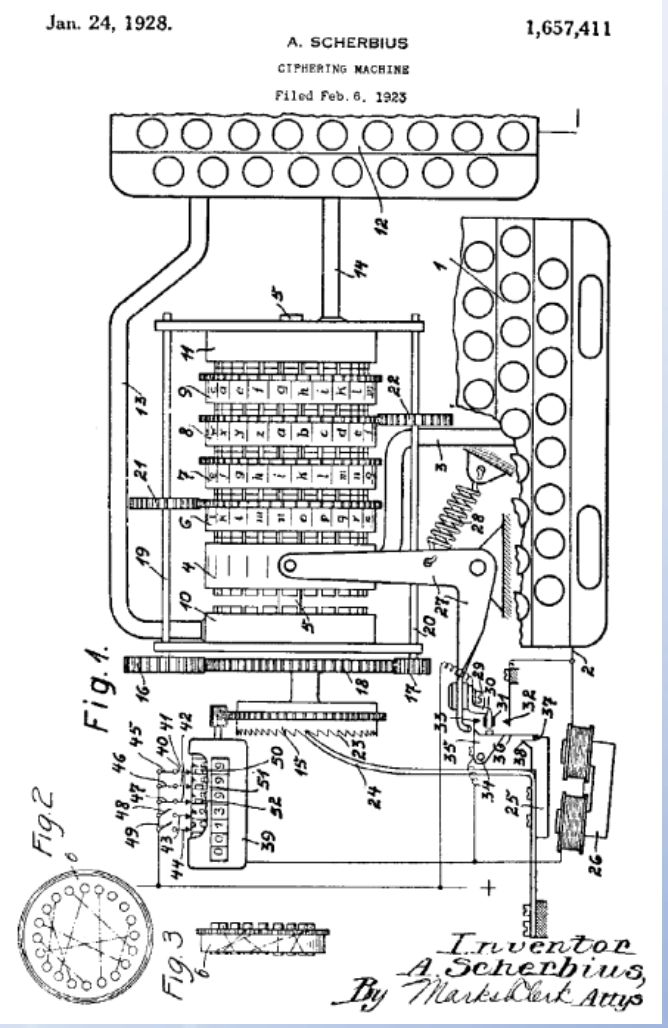
C	R	Y	P	T	O	G	R	A	P	H	Y
2	17	24	15	19	14	6	17	0	15	8	24

C	R	Y	P	T	O	G	R	A	P	H	Y	C	R	Y	P	T	O	G	R
2	17	24	15	19	14	6	17	0	15	8	24	2	17	24	15	19	14	6	17

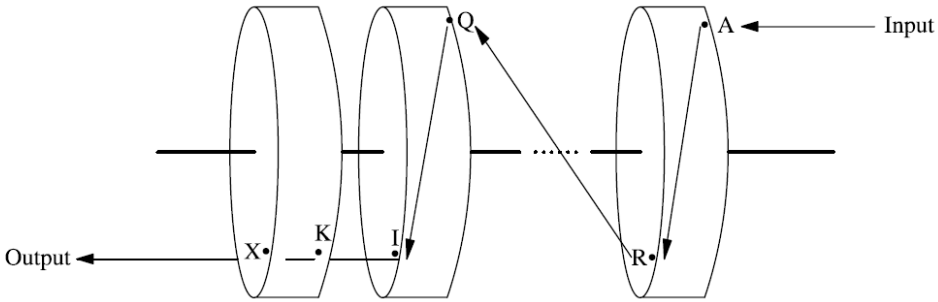
Эдвард Хеберн Арвид Дамм Артур Шербиус

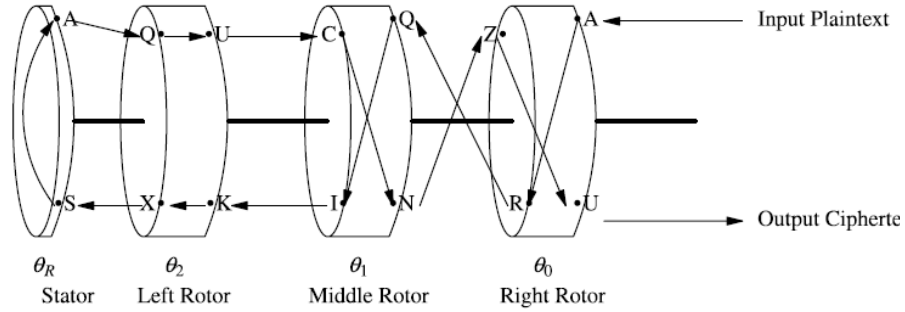


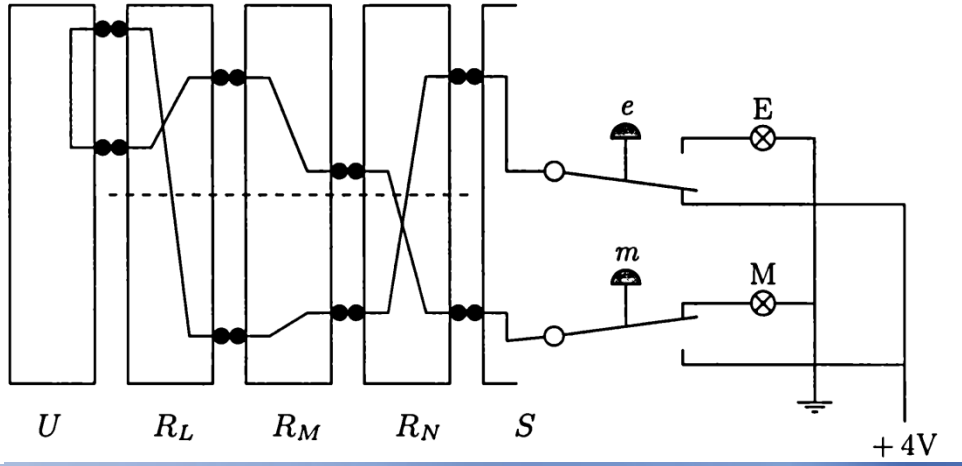
Edward Hebern's *Electric Code Machine* (U.S. Patent no: 1,673,072).



Patent no.	Year	Country	Patenter	Description
52,279	1919	Sweden	Arvid G. Damm	
1,484,477	1924	United States		Apparatus for enc/deciphering code expressions
1,502,889	1924	United States		Production of Ciphers
1,540,107	1925	United States		Apparatus for the production of cipher documents
10,700	1919	Holland	Hugo A. Koch	Geheimsschrijtmachine
1,533,252	1925	United States		Printing telegraph system
1,657,411	1928	United States	Arthur Scherbius	Ciphering machine
1,510,441	1924	United States	Edward H. Hebern	Electric code machine
1,861,857	1932	United States		Cryptographic machine







В ЭНИГМЕ I и в ЭНИГМЕ *Вермахта* «регулярное» перемещение роторов обеспечивалось благодаря наличию *одного* паза в *алфавитном кольце* каждого ротора. Самый «быстрый» ротор (крайний справа) R_N перемещался на одну позицию на каждом шаге шифрования. Каждый полный оборот его вызывает перемещение на одну позицию «среднего» ротора (центрального) R_M, полный оборот которого, в свою очередь, вызывает перемещение на одну позицию «медленного» (крайнего левого) ротора R_L. Фактически это означало регулярное, как в счетчике, вращение роторов («греческие» роторы β и γ, которые были введены позднее, не имели возможности перемещаться).

Начало криптоанализа Энигмы
Marian .Rajewski, Jerzy Rozycki, Henryzk Zygalsky 1932 - 1939.

Alan Turing, Gordon Welchman, начало 1939, 1940-1945

Fialka = Фиалка = Violet = M-125

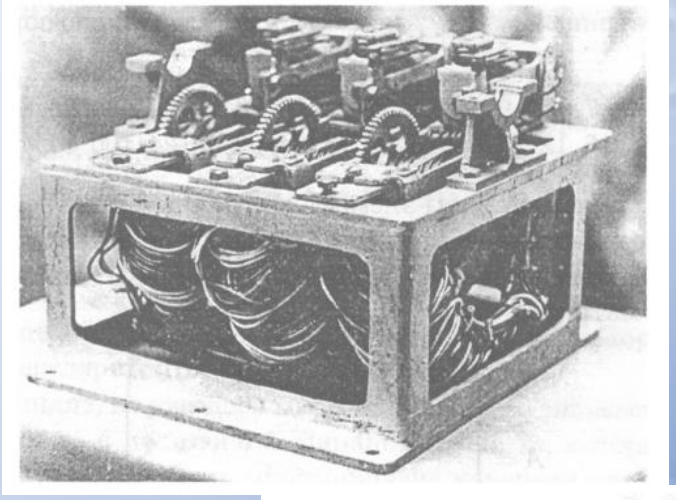
Around 1965.

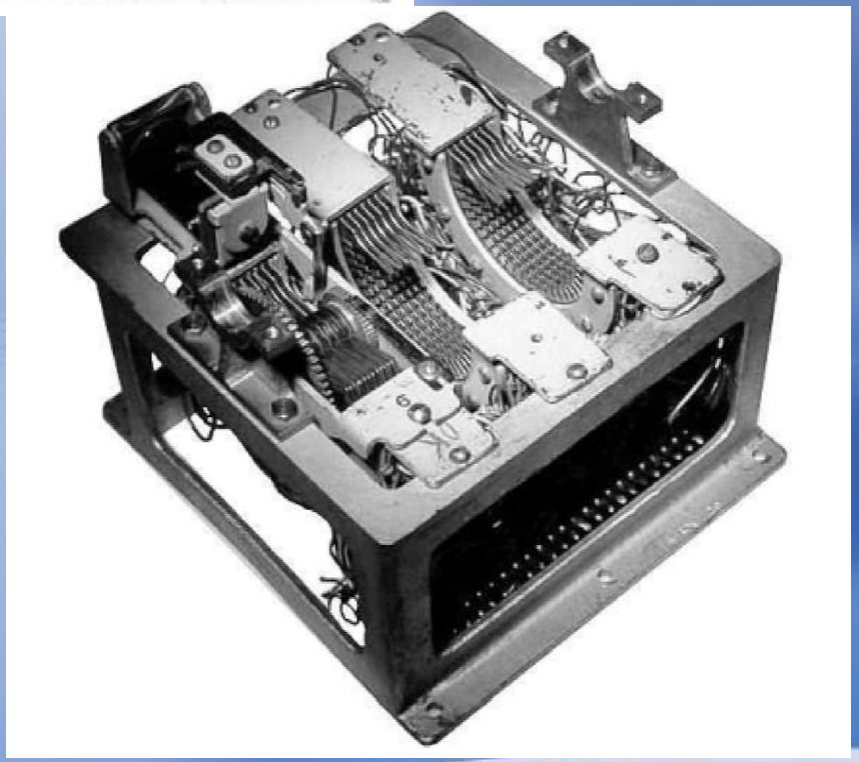
MUCH stronger than Enigma…

Used until 1987 in East Germany…

Was Fialka Broken?

- Israel have captured Fialka machines during the 6-day war in 1967 and … nothing more was disclosed.
- Austria would intercept and decrypt a fair proportion of Fialka traffic during the Cold War…
- In the 1970s the NSA would build a supercomputer to decrypt Fialka routinely





Японская шифровальная машина Purple

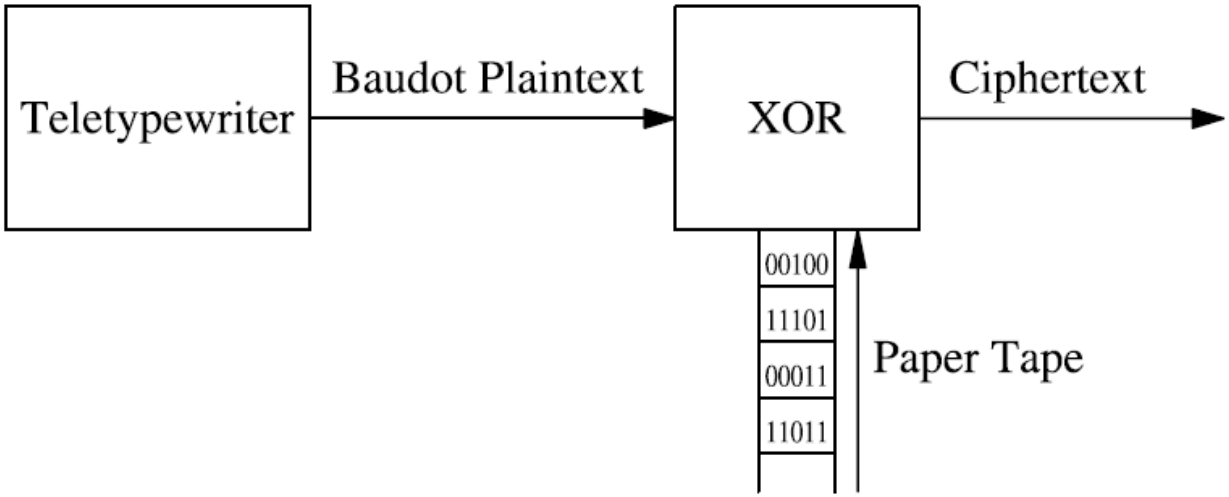
Гилберт Вернам -- инженер американской телефонной и телеграфной компании. В 1917 году разработал телетайп, чтобы он мог работать в режиме он-лайн шифрование/расшифрование. Открытый текст был впервые закодирован 0 и 1 с использованием кода Бодо, в котором каждый символ представлен 5-битовой последовательностью.

Шифрование в этой системе Вернама представляло собой переоткрый способ полиалфавитного шифрования Виженера. Ключ был написан на бумажной ленте как последовательность 0 и 1.

Открытый текст – последовательность 0 и 1 по коду Бодо, был зашифрован на периодическом ключе операцией XOR. Ключ представлял собой бумажную ленту с 0 и 1 и склеенными концами – петлю.

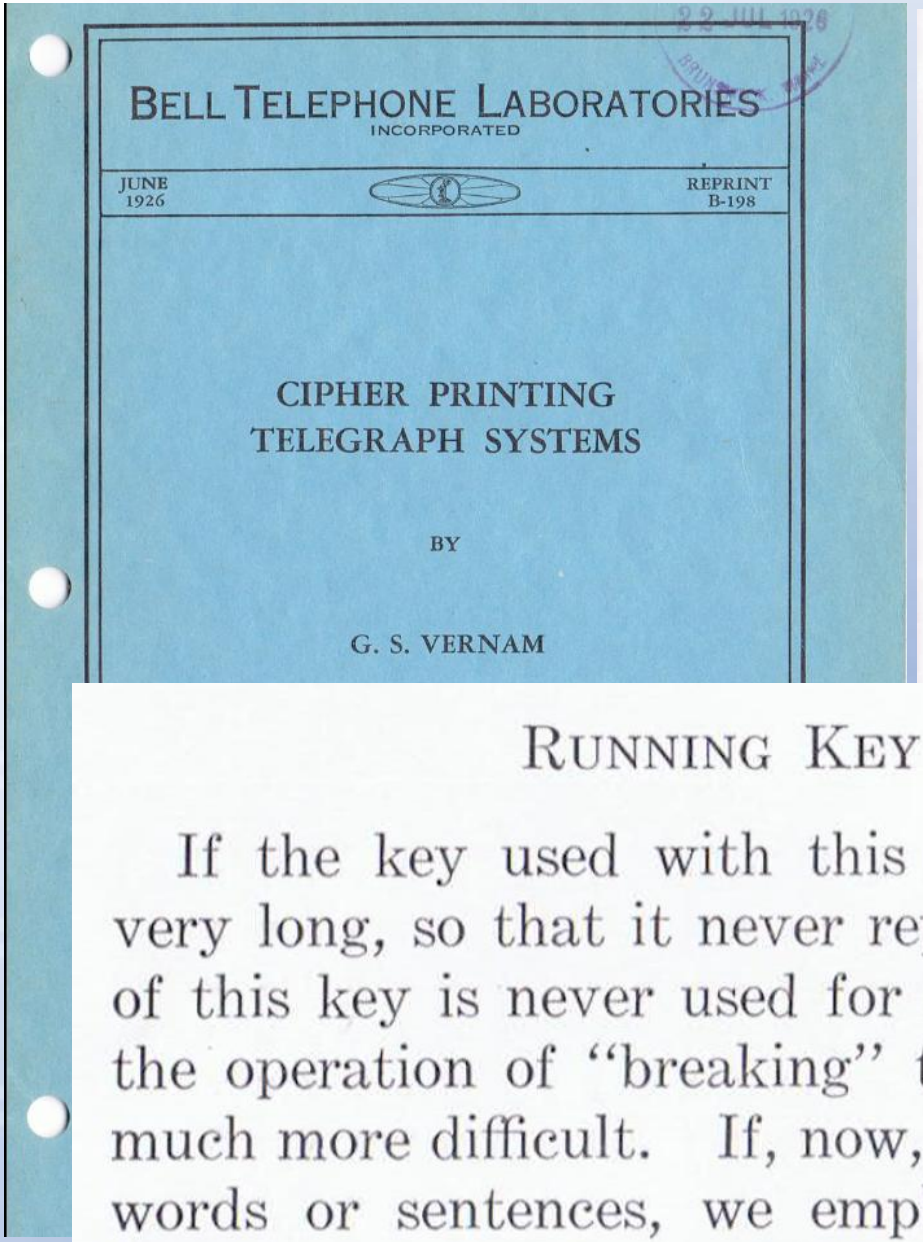
Baudot code

A	00011	B	11001	C	01110	D	01001
E	00001	F	01101	G	11010	H	10100
I	00110	J	01011	K	01111	L	10010
M	11100	N	01100	O	11000	P	10110
Q	10111	R	01010	S	00101	T	10000
U	00111	V	11110	W	11011	X	11101
Y	10101	Z	10001	LF	00010	CR	01000
↑	11111	↓	11011	SP	00100		00000
0	10110	1	10111	2	10011	3	00001
4	01010	5	10000	6	10101	7	00111
8	00110	9	11000	?	11001	$	01001
Bell	01011	!	01101	;	01110	&	11010
#	10100	(	01111	)	10010	.	11100
,	01100	/	11101	,	00101	;	11110



Доклад Вернама от компании AT&T для армии США об изобретении.
Майор Мауборн + Вернам -- Патент США 1,310,719, По-видимому, Майор Мауборн понял, что повторное использование ленты может сделать шифр Вернама уязвимым для криптоанализа.
В патенте Вернама и Мауборн описано обобщение полиалфавитного шифрования на случай бесконечной ленты – one-time tape (позднее one-time pad – одноразовый блокнот).

Vernam and Mauborgne



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.

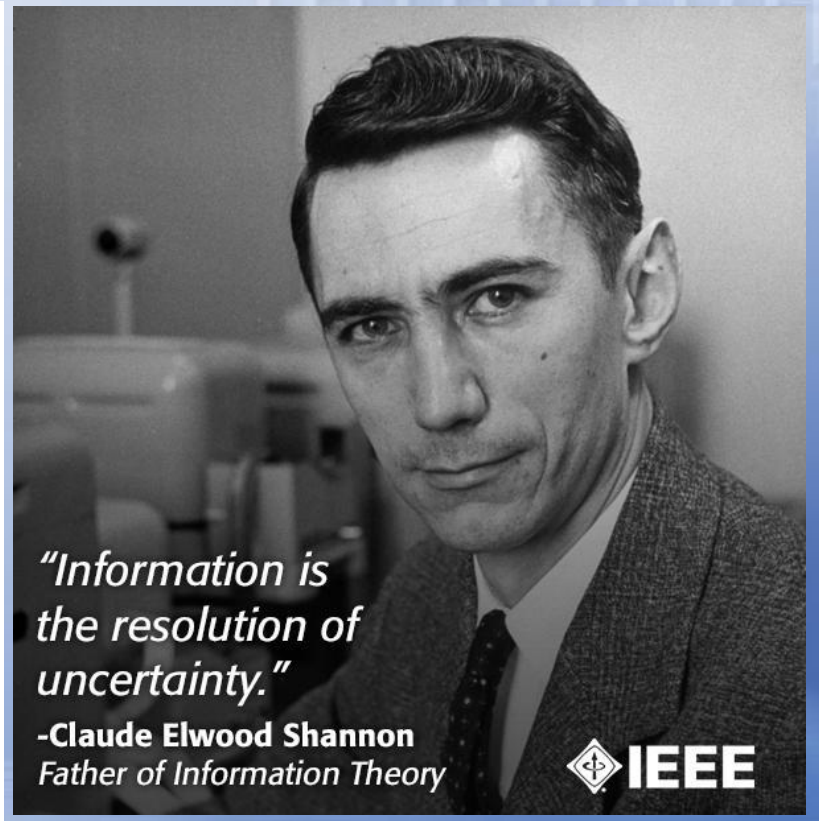
Communication Theory of Secrecy Systems*

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."

Одноразовый блокнот был найден в доме Рудольфа Ивановича Абеля, советского разведчика, арестованного в 1957 году в США. Одноразовый блокнот содержал 60 пятизначных групп случайных десятичных цифр.

В открытой литературе не рассказывается, как осуществлялась генерация случайны чисел.

20505	60476	04016	88622	36579	39249	67480	72479	66266	87127
92365	70390	04618	94915	08730	77472	67325	85635	01210	22288
99873	16471	56328	29731	35682	23798	46859	07234	10566	29350
03229	46862	90096	60275	61635	52187	94072	88348	20714	39363
49924	84439	53498	92235	92394	71287	36378	94819	19574	66292
98910	93264	32572	46231	58592	36289	98189	66859	23710	20413

Шифрование в два этапа
Кодовая таблица

Комбинация кодовой таблицы и шифрования в режиме одноразового блокнота

Phrase	Codeword
⋮	⋮
Contact	7652
⋮	⋮
endspell	1653
⋮	⋮
pay	6781
⋮	⋮
spell	5411
⋮	⋮

konheim delivered report about rockets

Teacher delivered report about grades

7394 2157 1139 3872 2216

73942 15711 39387 22216

16471 56328 29731 35682 23798 46659

Зачем это нужно?

Проблема распределения секретных ключей -- центральная проблема в криптографии.

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)

Секретный ключ

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

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

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

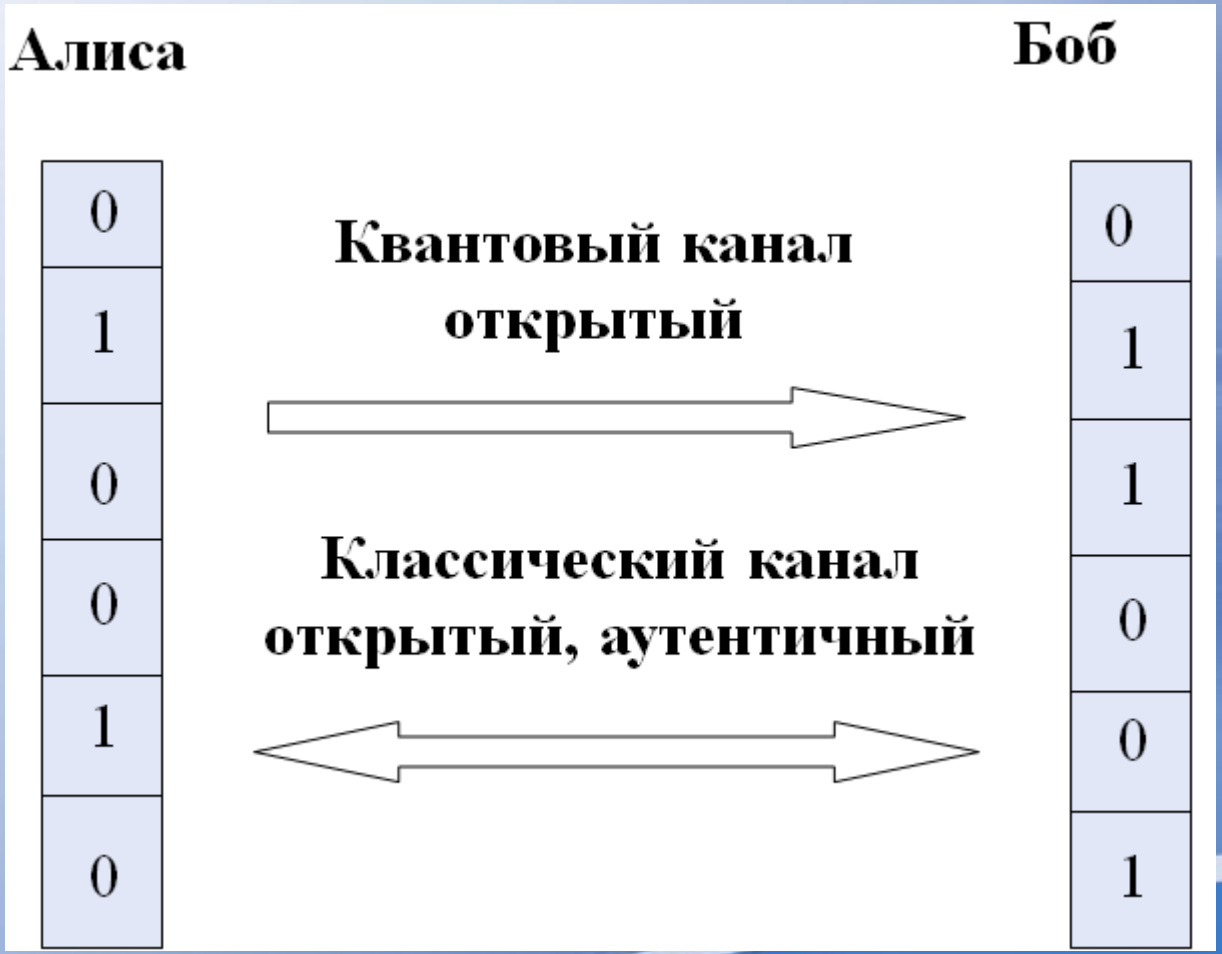
$$I(M;C) = H(C) - H(C|M) = 0$$

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

$$c = m \oplus k$$

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

Квантовая криптография = Квантовое распределение ключей = Согласование случайных последовательностей



Элементы систем квантовой криптографии:

1) Физический генератор (квантовый) истинно случайных последовательностей.

2) Протокол – набор действий, по которым 0 и 1 сопоставляются квантовые состояния. ЦЕНТРАЛЬНЫЙ МОМЕНТ – ДОКАЗАТЕЛЬСТВА СЕКРЕТНОСТИ КЛЮЧЕЙ.

3) Исправление ошибок в первичных ключах.

4) Сжатие очищенных ключей – усиление секретности универсальными хеш-функциями.

5) Конечный продукт работы любой системы квантовой криптографии – общий секретный ключ.

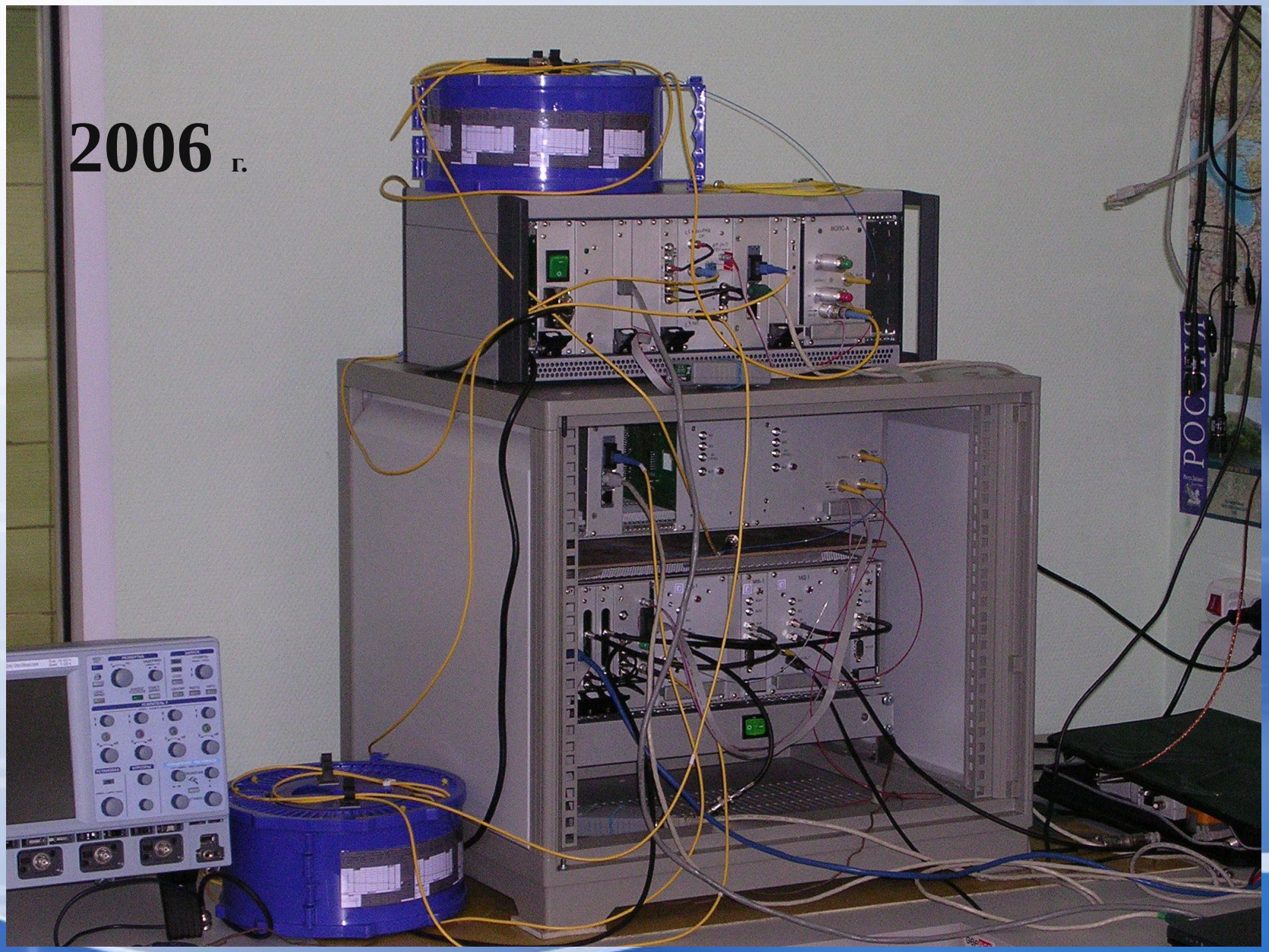
Как это работает – кратко общие принципы

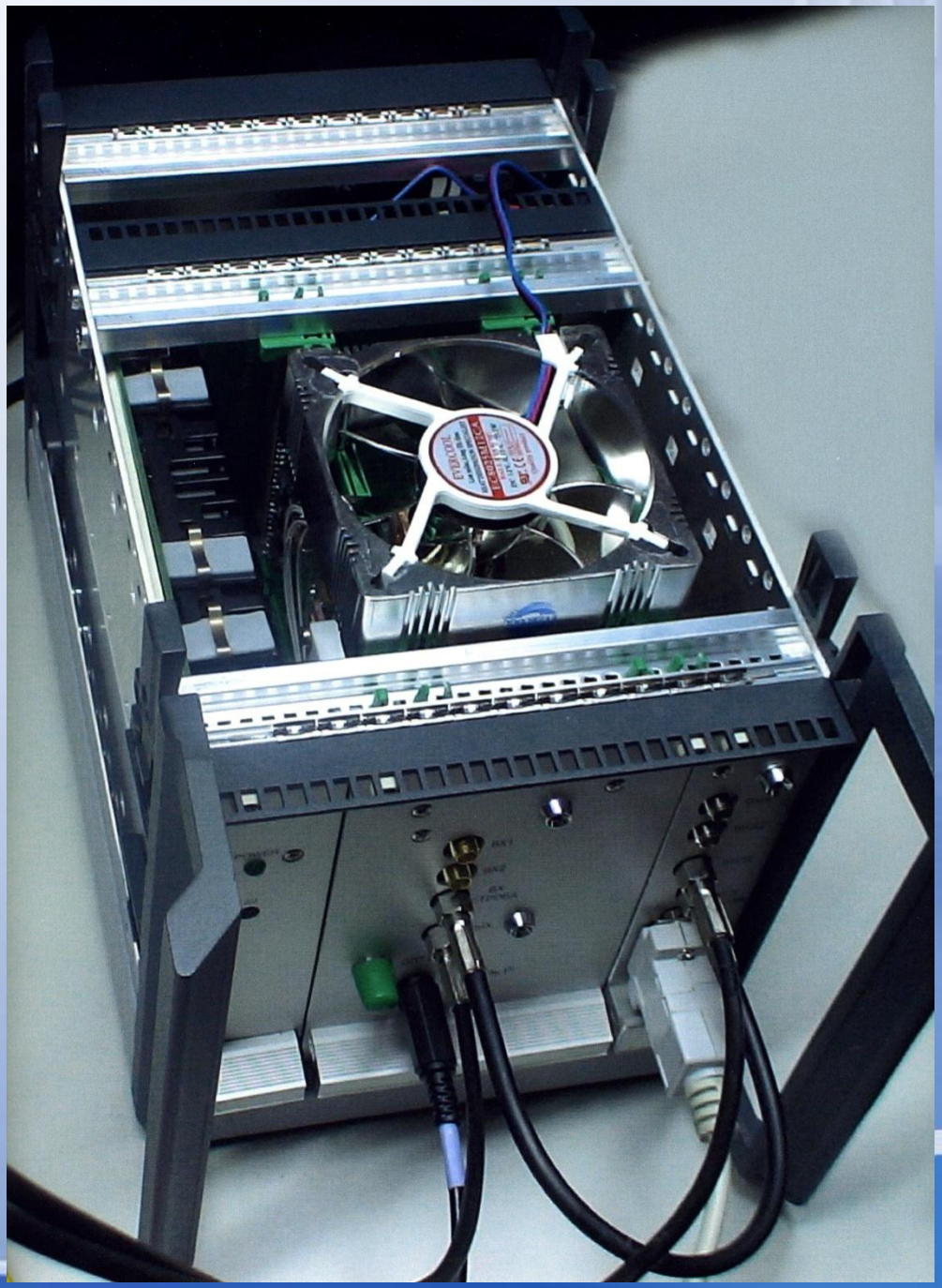
Фундаментальные запреты квантовой механики.

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.**

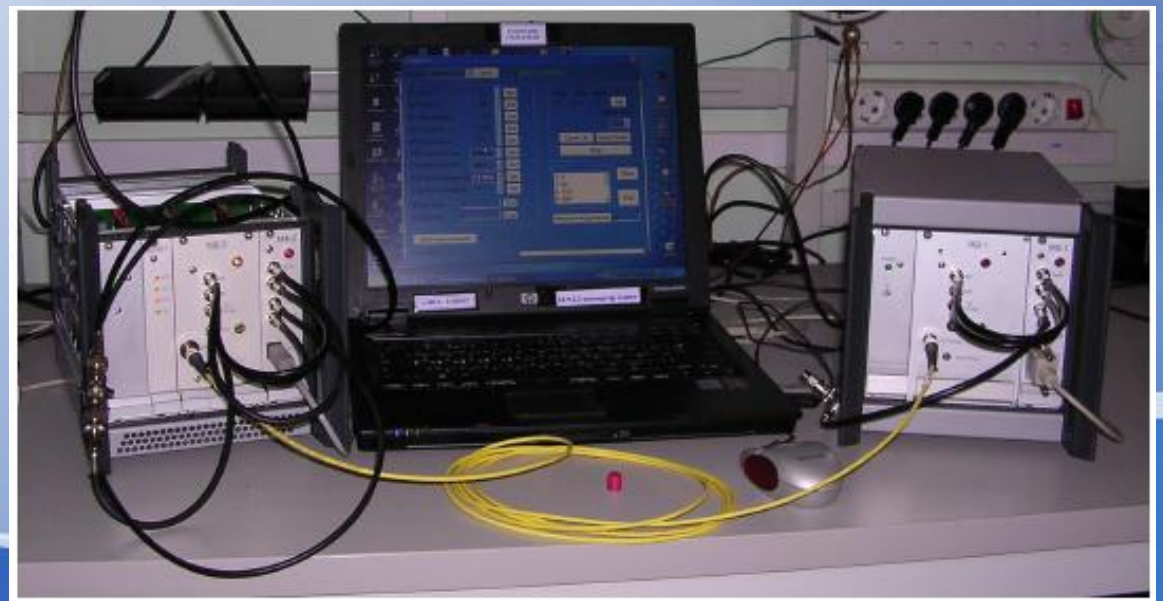
Цель квантового распределения ключей – создание сетевой полностью автоматизированной системы смены ключей без участия оператора (после запуска системы человек никогда не имеет доступа к ключам, используемым для шифрования)

2006 г.

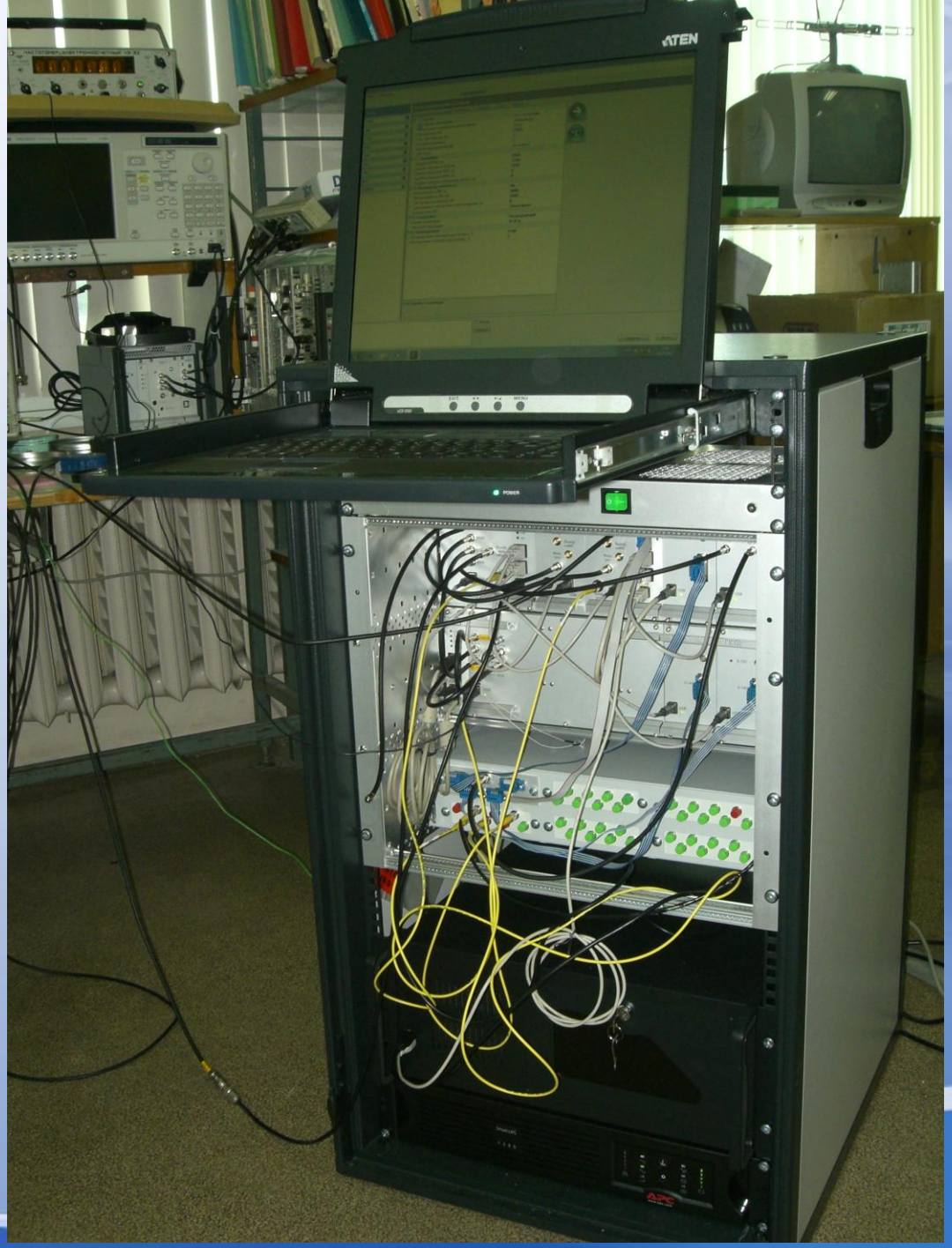




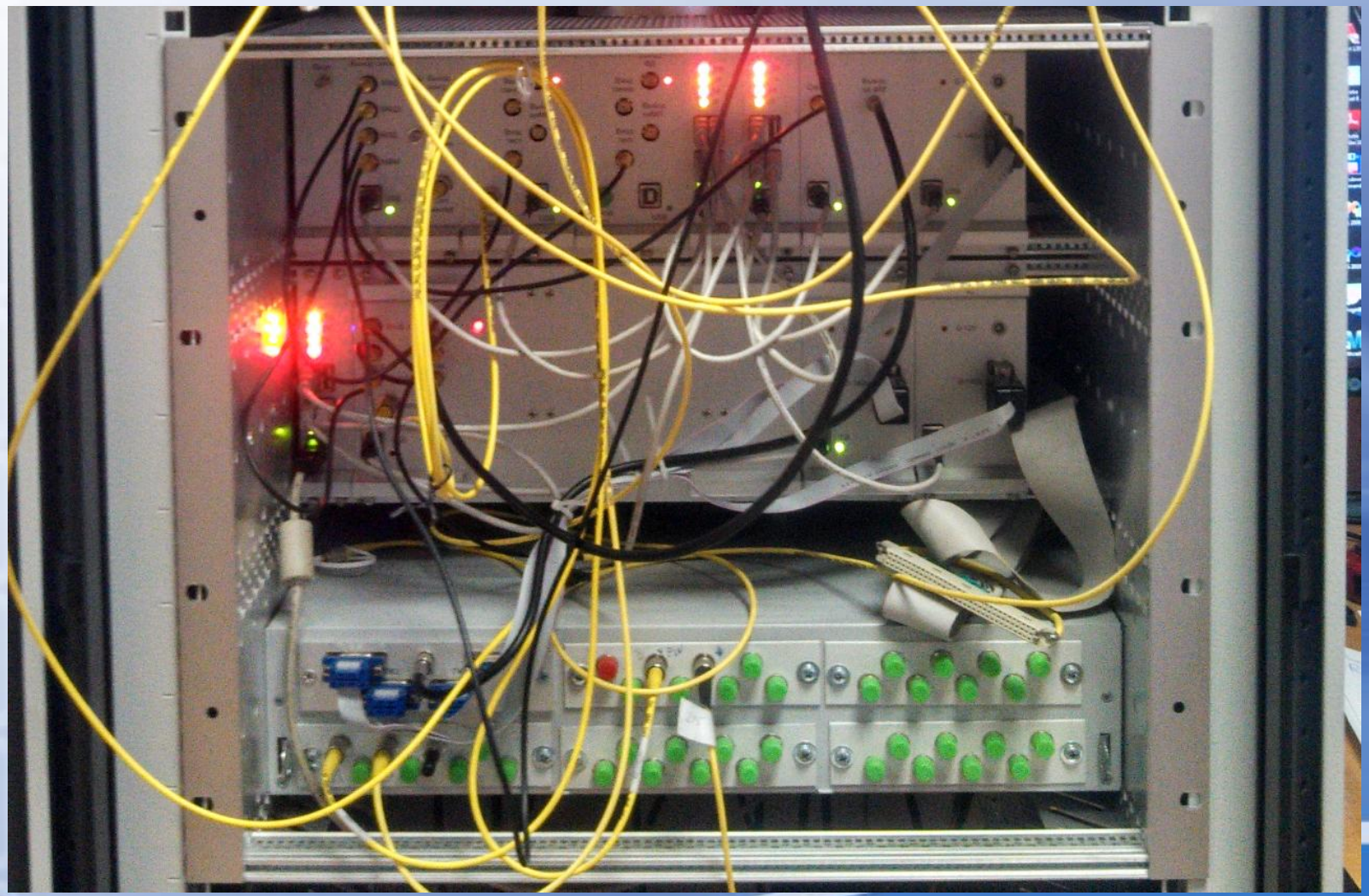

TRACO POWER
TEN 8-1611

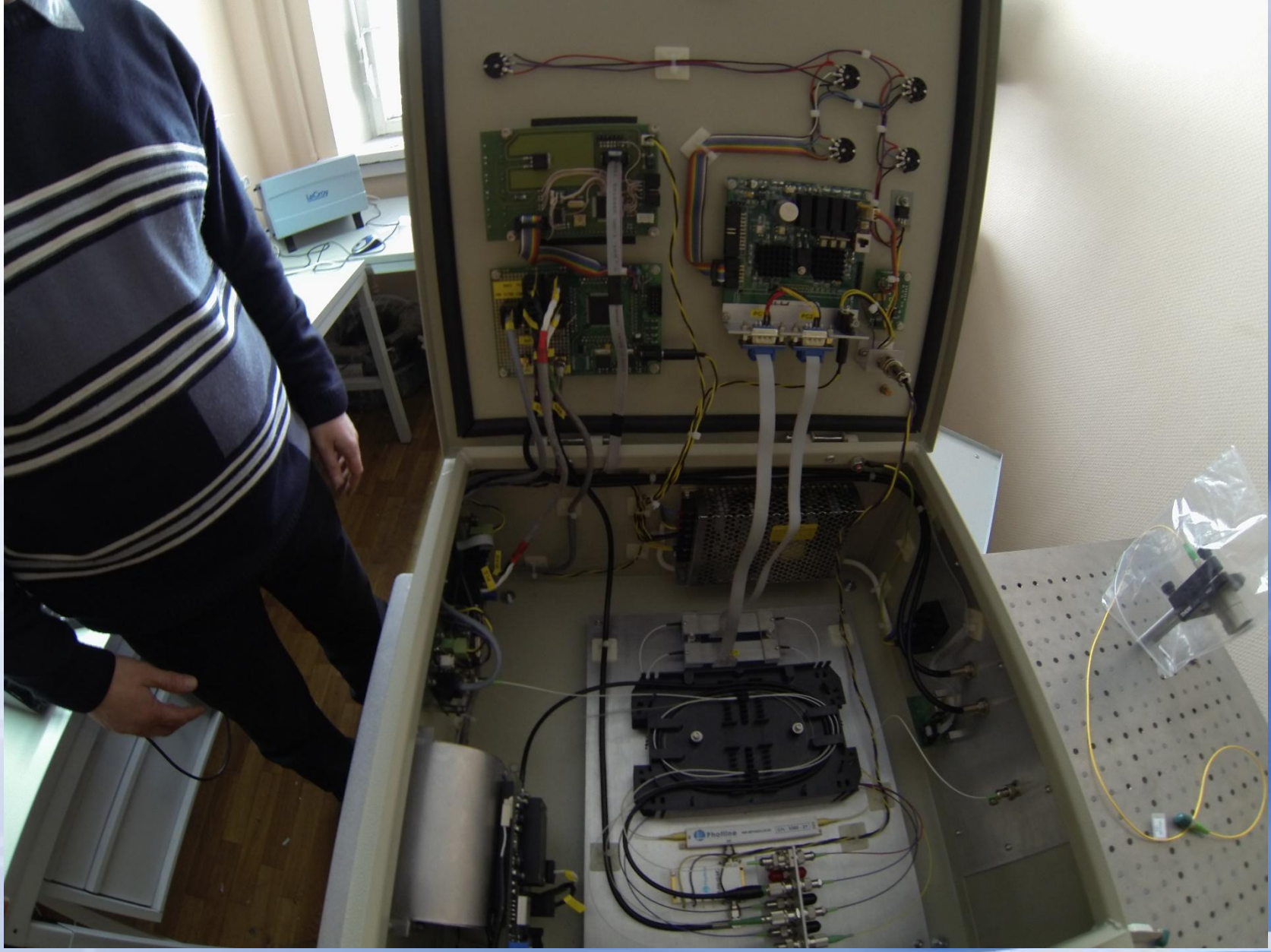


2011-2012 г.



2015





2015-2016

Free-Space Quantum Cryptography Using Multiphoton States: Secure Key Distribution to Satellites

S. N. Molotkov

Institute of Solid State Physics, Russian Academy of Sciences, Chernogolovka, Moscow oblast, 142432 Russia
Moscow State University, Moscow, 119899 Russia
e-mail: molotkov@issp.ac.ru

Received March 3, 2004

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

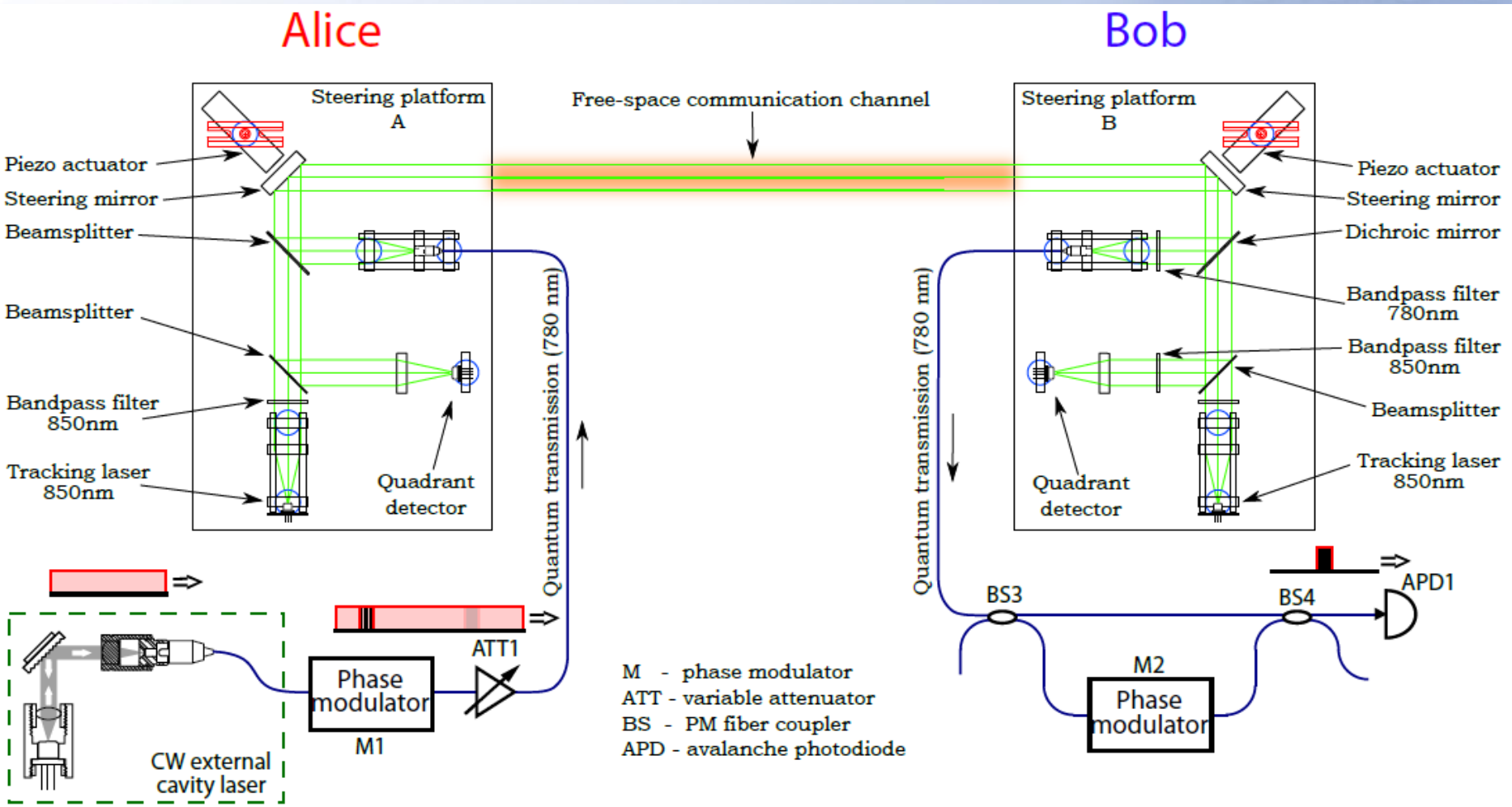
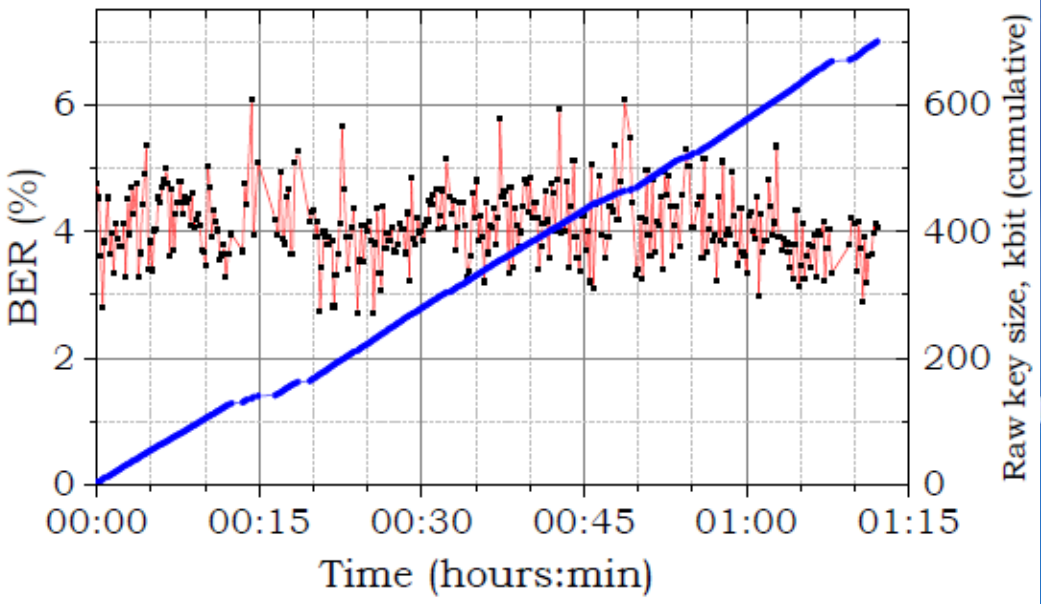


FIG. 1: Experimental setup including both the QKD part and the tracking system.

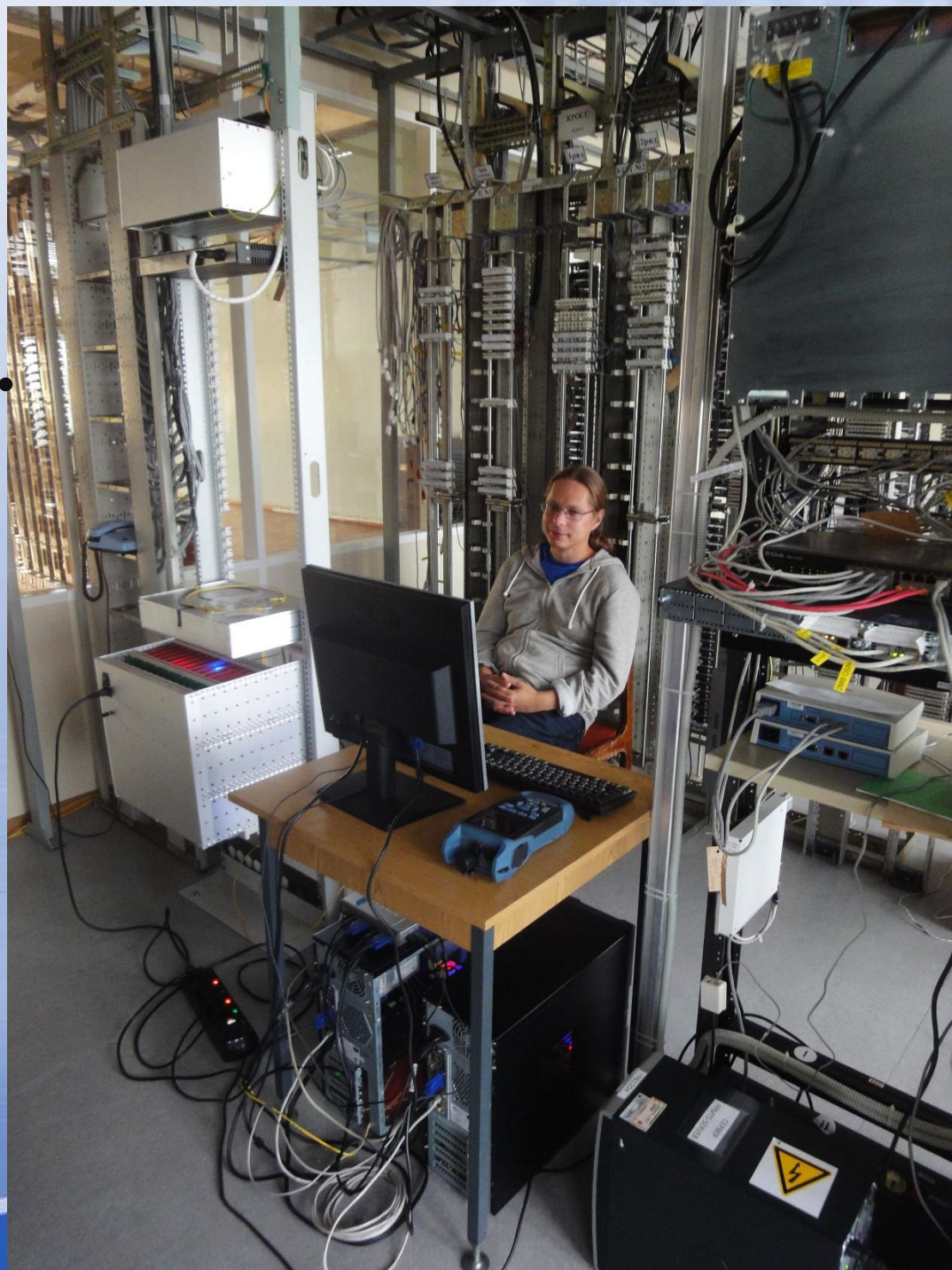
FIG. 3: Station Alice: a tripod v
tracking platform and a box with fi
all electronics.



2017-2018

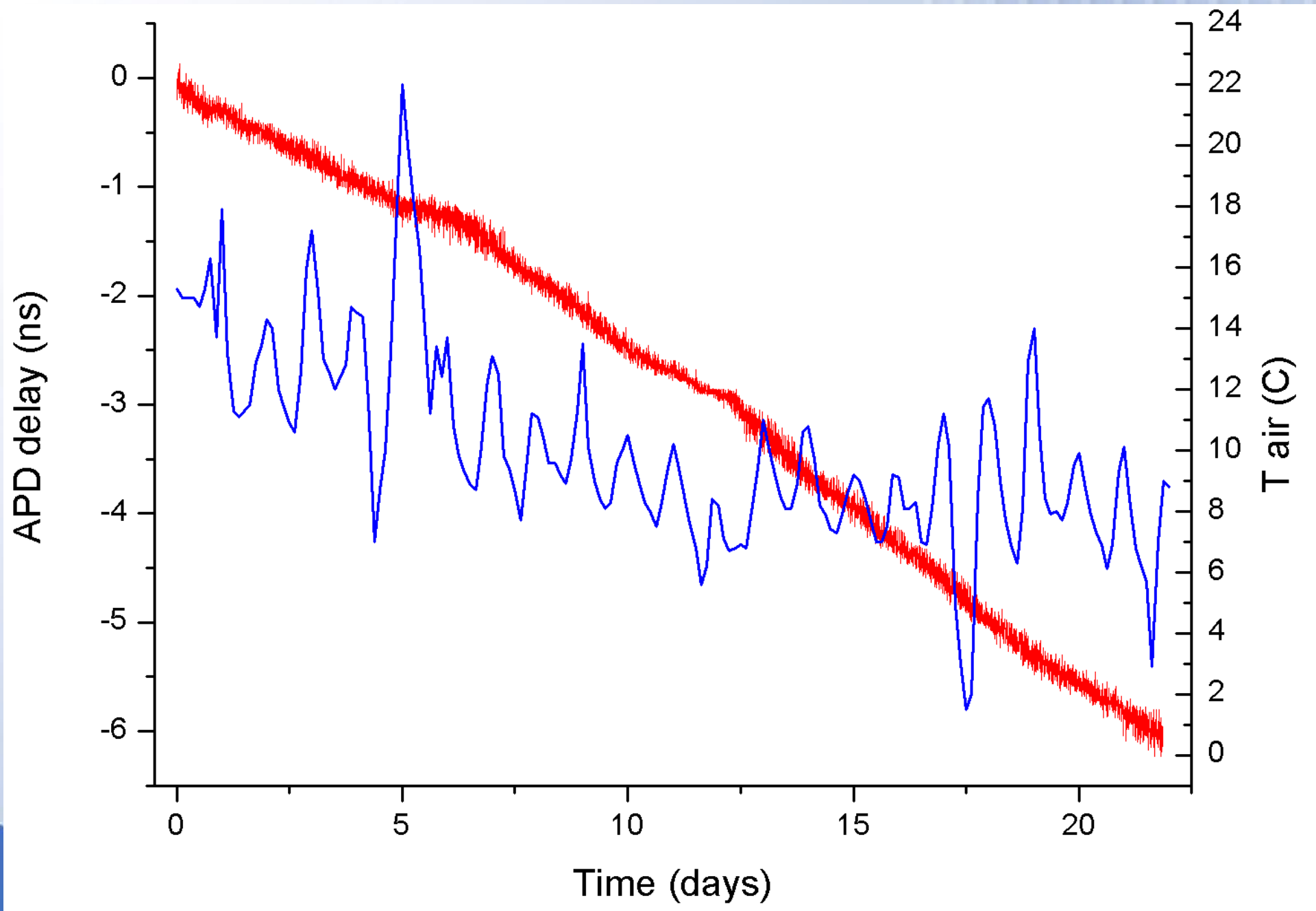

Схема сети квантового распределения ключей

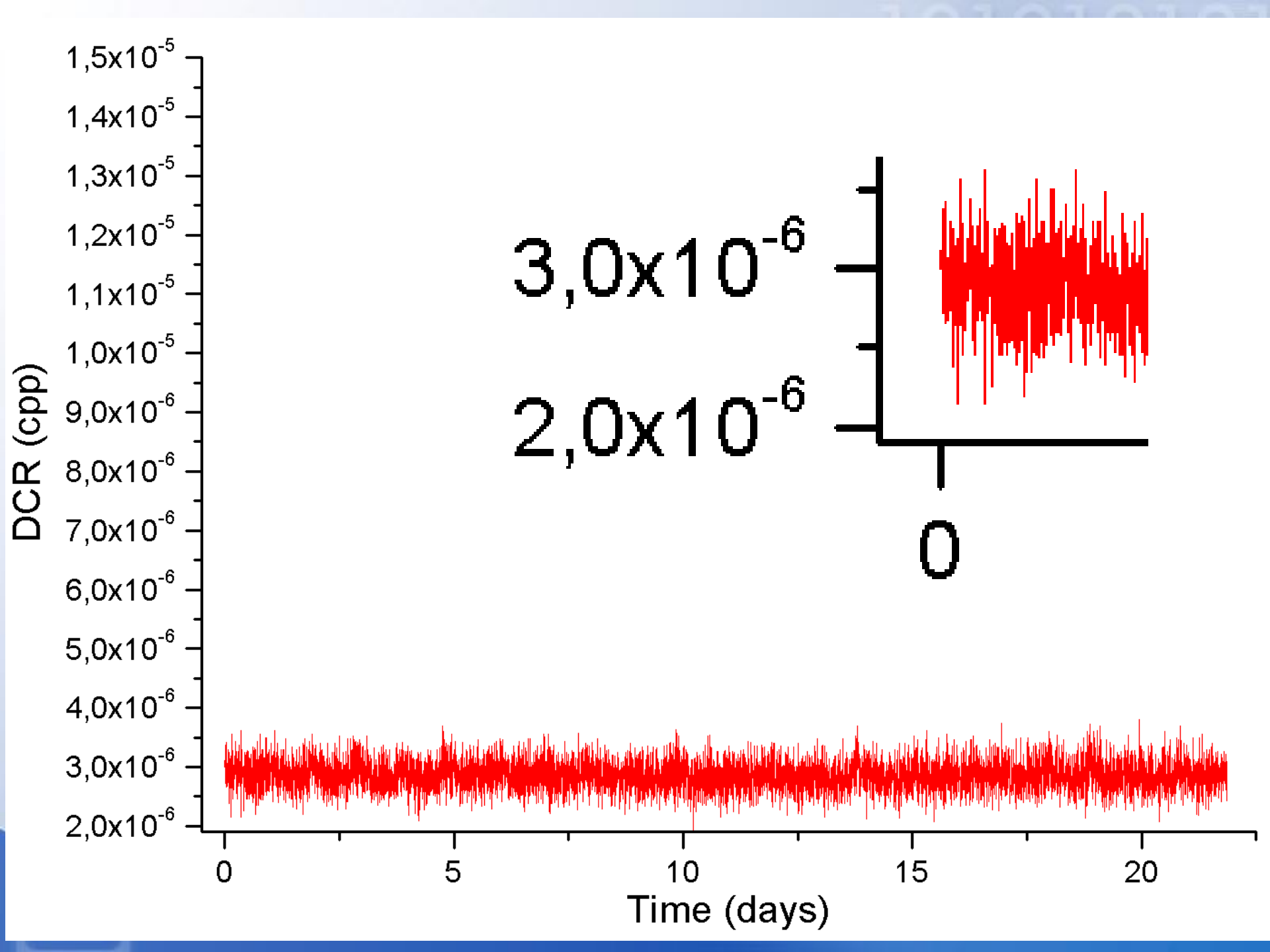
2017 -- Линия Ростелекома 32 км Ногинск-Павловский Посад. Непрерывная работа без сбоев в автоматическом режиме генерации ключей в течении месяца

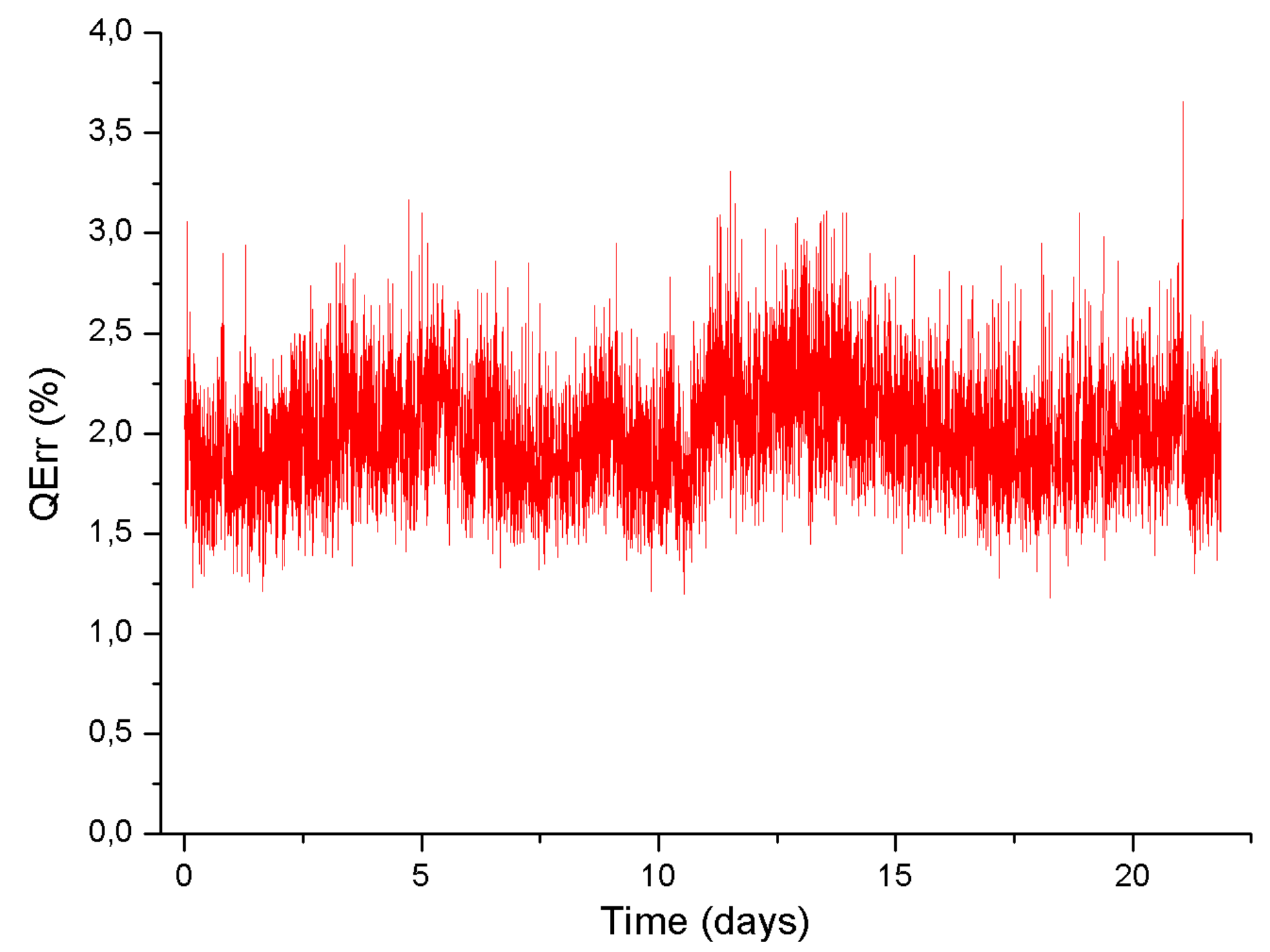


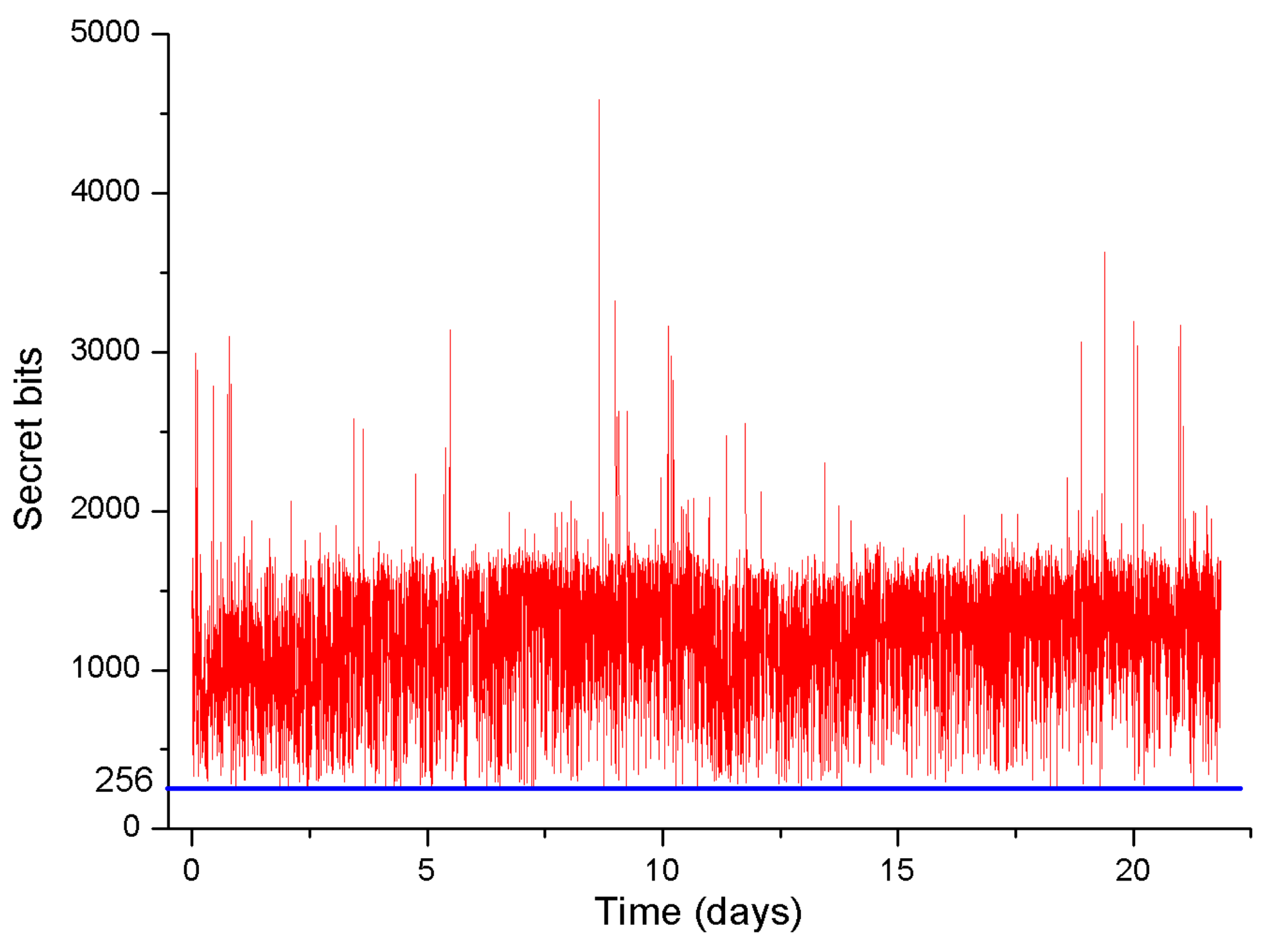
```
### 14:27:52 ################
*Series #1  (10000000 @ 3.20 kHz)*
### 14:28:27 ################
   APDcounts = 43334 (52453)   APDcounts efficiency = 4.33e-03 (5.25e-03)
   Counts@bases = 1741 (1925)   Counts@bases efficiency = 1.74e-04 (1.93e-04)    rawKey = 1741
              Secret bits efficiency = 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. ==================
_____________________________________________________________________________
```

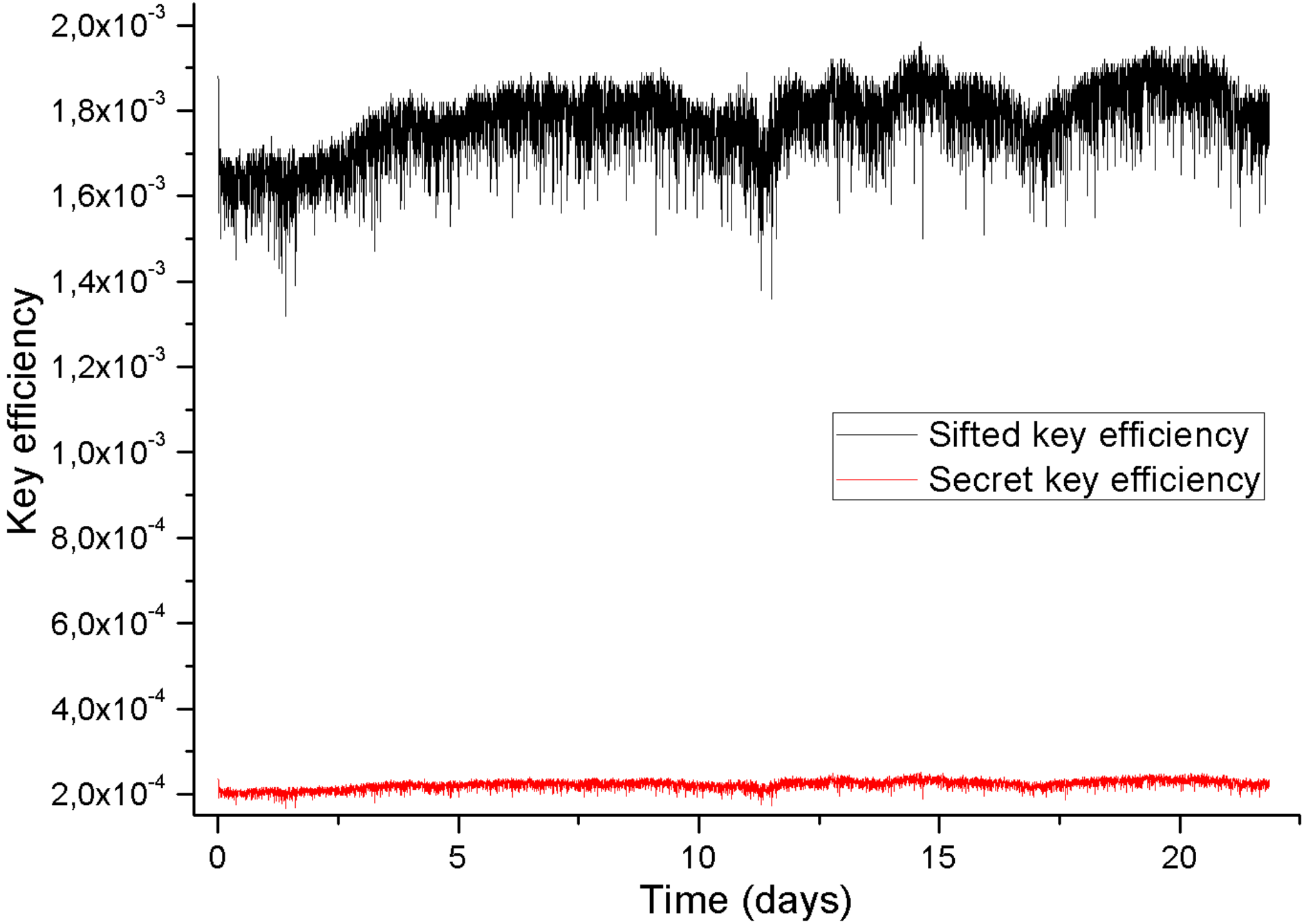
time(h)	ser	T(C)	DCR(cpp)	FCR(cpp)	dt(ns)	Vis-ty	Bal	V1	V2	V3	Smax	kHz	P@Bob	Ngiant	Eff@counts	Eff@bases	Err(%)	Real	Raw(b)	Estm(b)	Rate	Fails	Ns	t(min)	Raw	Estm	Err(%)	Pure(b)	Quant(b)	Secret	t(min)	key#
0.000	1	-50.0	1.70e-06	1.70e-05	+0.59	0.9930	0	57.5	18.5	44.0	37.4	10.0	15.80	0	1.12e-02	4.14e-04	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
2.140	1	-50.0	3.00e-06	1.48e-05	+1.50	0.9951	0	41.1	17.4	61.5	37.5	10.0	16.20	0	1.21e-02	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
2.215	1	-50.0	3.80e-06	1.96e-05	+1.50	0.9951	0	40.1	15.9	60.5	37.2	10.0	16.20	0	1.14e-02	4.44e-04	1.37	2.30	2170	893.8	662.1	0	1	1.4	2170	894	1.17	1376	14	1363	1.6	25
2.289	1	-50.0	2.90e-06	1.84e-05	+1.50	0.9951	1	38.1	18.4	61.5	37.4	10.0	16.20	0	1.12e-02	4.34e-04	1.40	1.37	2195	897.3	665.2	0	1	4.5	2195	897	1.88	1280	14	1266	4.8	26
2.363	1	-50.0	2.40e-06	1.78e-05	+1.50	0.9951	1	38.1	18.4	61.5	37.4	10.0	16.20	0	1.12e-02	4.34e-04	1.43	1.73	2256	920.3	682.5	0	1	4.5	2256	920	1.60	1376	14	1362	4.8	27
2.437	1	-50.0	2.90e-06	1.90e-05	+1.50	0.9951	0	38.1	18.4	61.5	37.4	10.0	16.20	0	1.12e-02	4.34e-04	1.66	2.02	2262	923.3	684.7	0	1	1.4	2262	923	1.93	1376	14	1362	1.7	28
2.511	1	-50.0	2.90e-06	1.90e-05	+1.50	0.9951	0	38.1	18.4	61.5	37.4	10.0	16.20	0	1.12e-02	4.34e-04	1.66	2.02	2262	923.3	684.7	0	1	1.4	2262	923	1.93	1376	14	1362	1.7	29
2.585	1	-50.0	2.90e-06	1.90e-05	+1.50	0.9951	0	38.1	18.4	61.5	37.4	10.0	16.20	0	1.12e-02	4.34e-04	1.66	2.02	2262	923.3	684.7	0	1	1.4	2262	923	1.93	1376	14	1362	1.7	30


APD delay (ns)
0
-1
-2
-3
-4
-5
-6
T air (C)
24
22
20
18
16
14
12
10
8
6
4
2
0
0
5
10
15
20
Time (days)


1,5x10-5
1,4x10-5
1,3x10-5
1,2x10-5
1,1x10-5
1,0x10-5
9,0x10-6
8,0x10-6
7,0x10-6
6,0x10-6
5,0x10-6
4,0x10-6
3,0x10-6
2,0x10-6
DCR (cpp)
3,0x10-6
2,0x10-6
0
0
5
10
15
20
Time (days)


4,0
3,5
3,0
2,5
2,0
1,5
1,0
0,5
0,0
QErr (%)
0
5
10
15
20
Time (days)


5000
4000
3000
2000
1000
256
0
Secret bits
0
5
10
15
20
Time (days)


2,0x10-3
1,8x10-3
1,6x10-3
1,4x10-3
1,2x10-3
1,0x10-3
8,0x10-4
6,0x10-4
4,0x10-4
2,0x10-4
Key efficiency
0
5
10
15
20
Time (days)
Sifted key efficiency
Secret key efficiency

Активная стабилизация оптической части в волоконной квантовой криптографии

К. А. Балыгин[+], *А. Н. Климов*[+*], *С. П. Кулик*[+], *С. Н. Молотков*[×∘∇1)]

[+] *Физический факультет МГУ им. Ломоносова, 119991 Москва, Россия*

[*] *Институт общей физики РАН им. Прохорова, 119991 Москва, Россия*

[×] *Институт физики твердого тела РАН, 142432 Черноголовка, Россия*

[∘] *Академия криптографии РФ, 121552 Москва, Россия*

[∇] *Факультет вычислительной математики и кибернетики, МГУ им. Ломоносова, 119991 Москва, Россия*

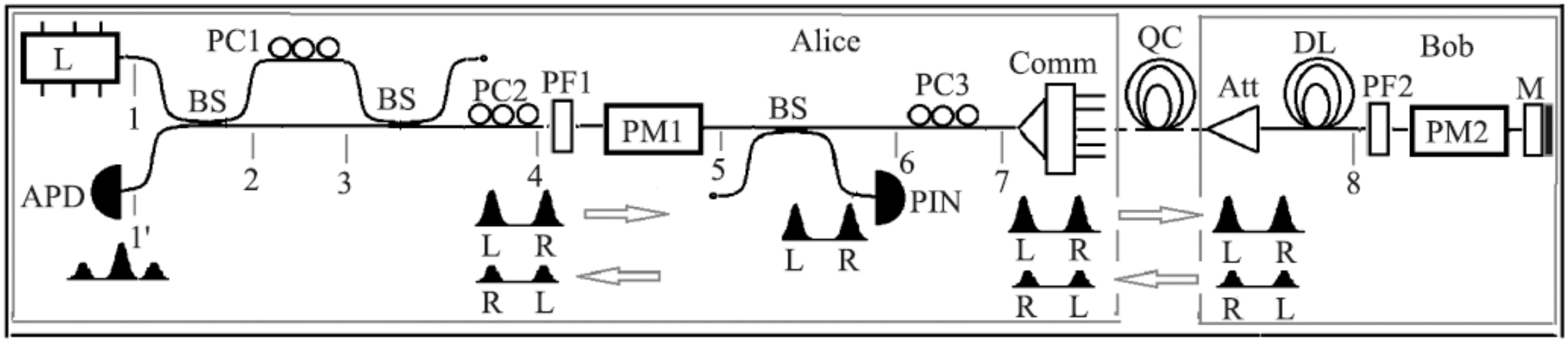


Рис. 1. Функциональная схема двухпроходной системы квантовой криптографии: L – лазер, BS – светоделители, PC1–PC3 – трехканальные контроллеры поляризации, PF1, PF2 – поляризационные фильтры, PM1, PM2 – фазовые модуляторы, APD – однофотонный лавинный детектор, PIN – классический фотодетектор, M – волоконное зеркало, Att – электронно-управляемый аттенюатор, QC – волоконная линия связи, DL – линия задержки, Comm – волоконный коммутатор для переключения между передающей станцией (Alice) и различными клиентами (Bob)

Управление распределенной интерференцией в в однопроходной системе квантовой криптографии

К.А.Балыгин[1], А.Н.Климов[1,2], С.П.Кулик[1], С.Н.Молотков[3,4,5]

[1] *Физический факультет МГУ имени М.В.Ломоносова, Москва, Россия*

[2] *Институт общей физики имени А.М.Прохорова РАН, Москва, Россия*

[3] *ИФТТ РАН, Черноголовка, Моск. обл., Россия*

[4] *Академия Криптографии Российской Федерации*

[5] *Факультет вычислительной математики и кибернетики МГУ имени М.В.Ломоносова, Москва, Россия*

Аннотация

Продемонстрировано управление интерференцией в двух разнесенных волоконных интерферометрах Маха-Цандера (МЦ) и поддержание видности на уровне близком к идеальной в однопроходной системе квантовой криптографии непосредственно в процессе распределения ключей при длине линии в 50 км. Показано, что отклонение видности от идеальной однозначно связано с регистрируемой разностью числа нулей и единиц в сыром (просеянном) ключе. Это позволяет осуществлять балансировку интерферометра только в квазиоднофотонном режиме без прерывания передачи ключей, используя разность числа нулей и единиц в сыром ключе, как сигнал ошибки. Предложенный подход сокращает время балансировки и, кроме того, не требует дополнительных обменов по открытому каналу связи.

О противодействии атаке с яркими состояниями в двухпроходной системе квантовой криптографии

К. А. Балыгин[+], *А. Н. Климов*[+*], *А. В. Корольков*[×], *С. П. Кулик*[+], *С. Н. Молотков*[×∘∇1)]

[+] *Физический факультет, МГУ им. Ломоносова, 119991 Москва, Россия*

[*] *Институт общей физики РАН им. Прохорова, 119991 Москва, Россия*

[×] *Академия Криптографии Российской Федерации, 121552 Москва, Россия*

[∘] *Институт физики твердого тела РАН, 142432 Черноголовка, Россия*

[∇] *Факультет вычислительной математики и кибернетики МГУ им. Ломоносова, 119991 Москва, Россия*

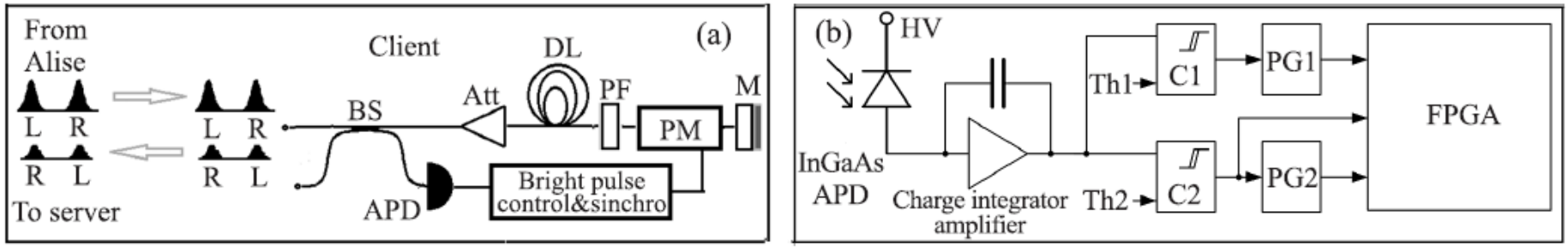


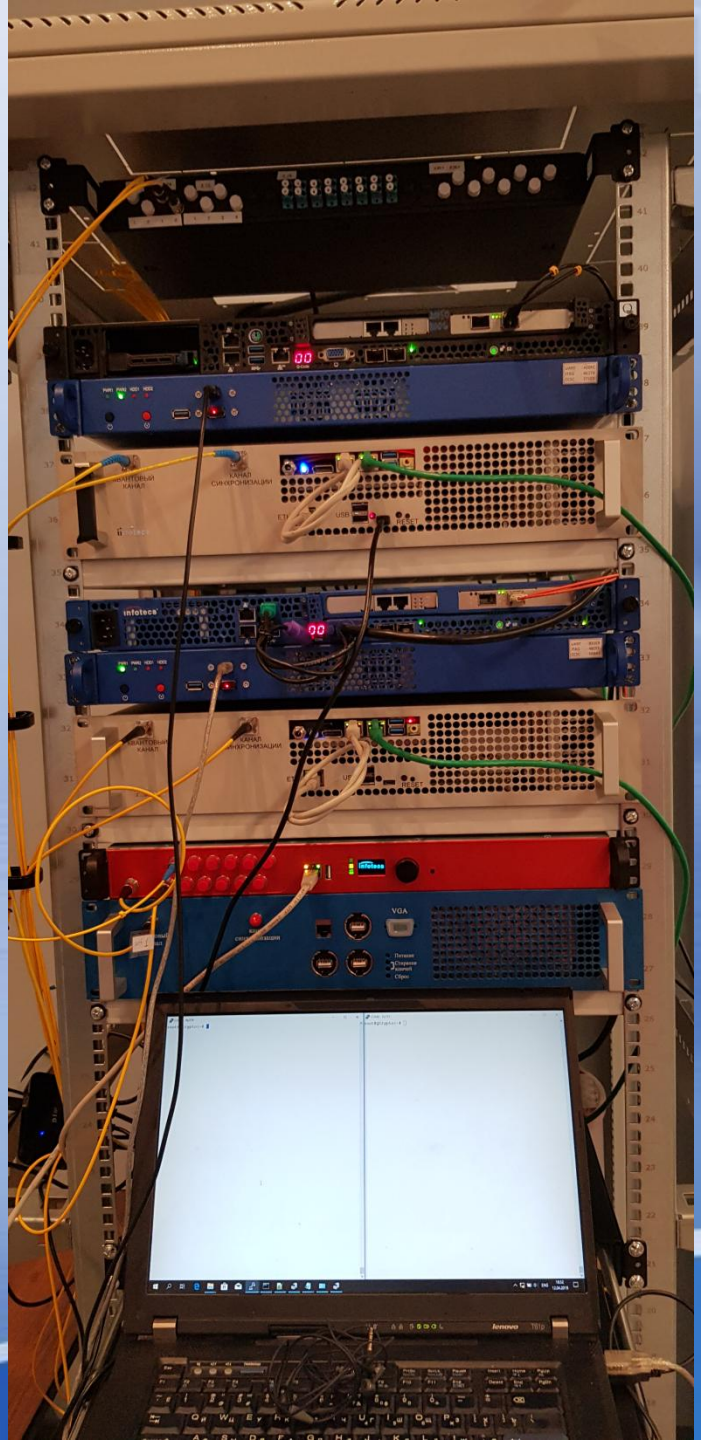
Рис. 1. (a) – Блок-схема клиента с контролем ярких импульсов: L(R) и R(L) – пара входных классических импульсов и ослабленных квазиоднофотонных, APD – лавинный фотодиод, BS – волоконный светоделитель, Att – медленный волоконный аттенюатор, DL – волоконная линия задержки, PF – поляризационный фильтр, PM – фазовый модулятор, M – волоконное зеркало. (b) – Блок-схема детектора входных импульсов у клиента: APD – лавинный фотодиод, HV – напряжение смещения, Charge Integrator Amplifier (CIA) – зарядово-чувствительный усилитель, Th1, 2 – независимо выставляемые пороги генерации синхроимпульсов и детектирования ярких импульсов, C1, 2 – компараторы, PG1, 2 – одновибраторы, FPGA – ПЛИС (Программируемая Логическая Интегральная Схема)

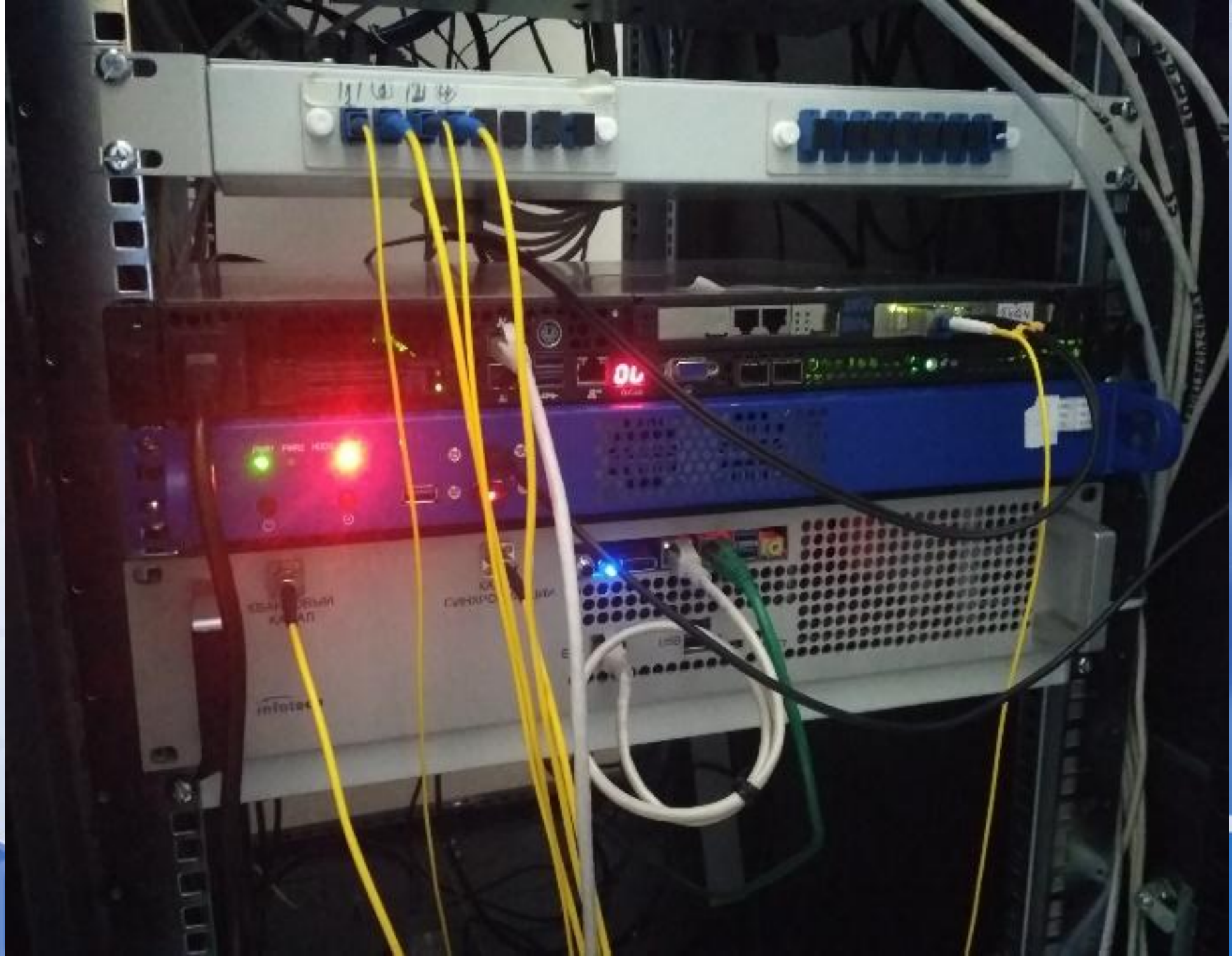
2019

Новое поколение интегрированных с классическими средствами шифрования систем квантовой криптографии -- единая замкнутая система

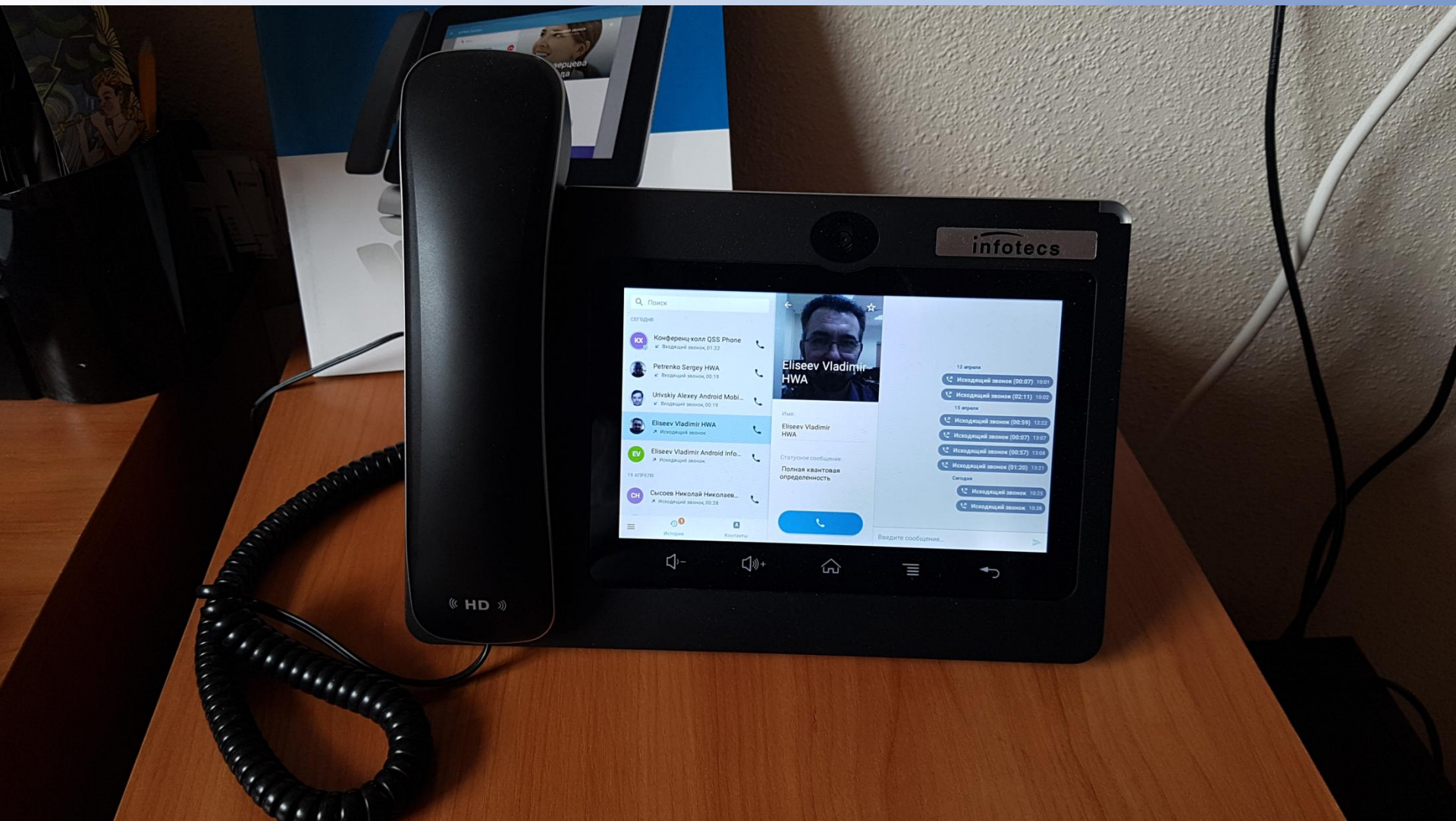
2019

Квантовая Криптография + 10G шифратор связь ЦОД – ЦОД

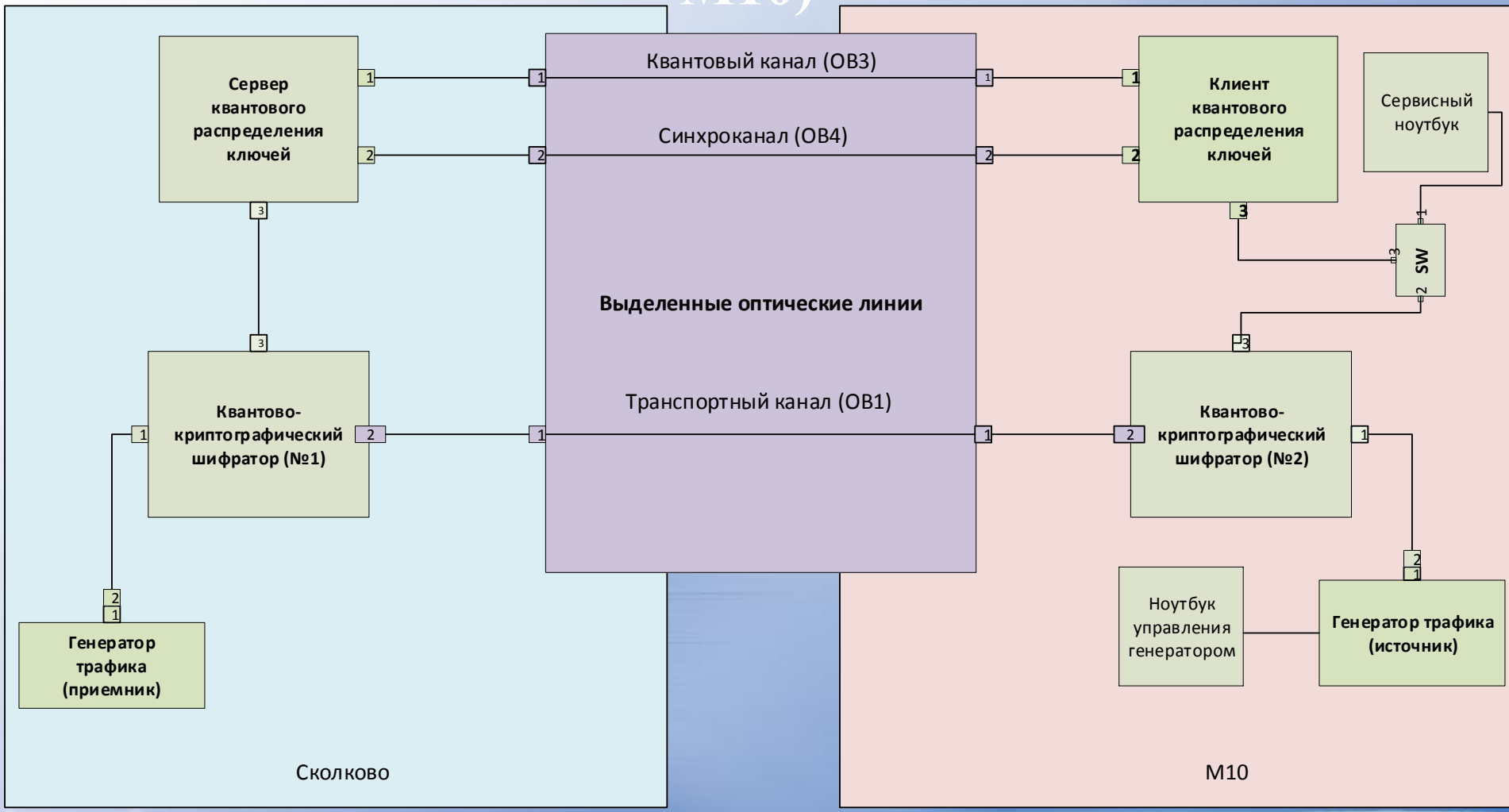




Квантовый телефон волоконная линия Инфотекс - МГУ

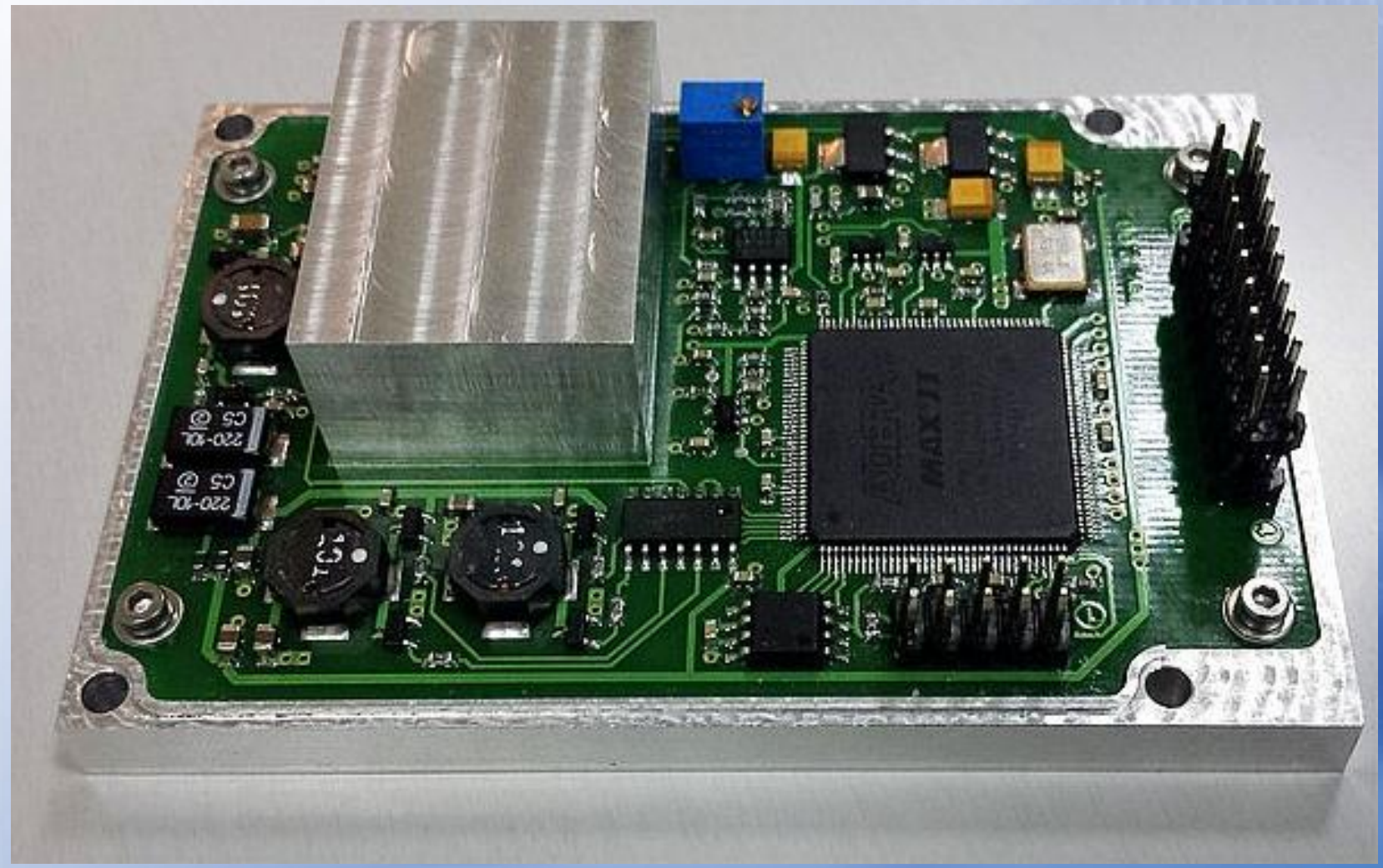


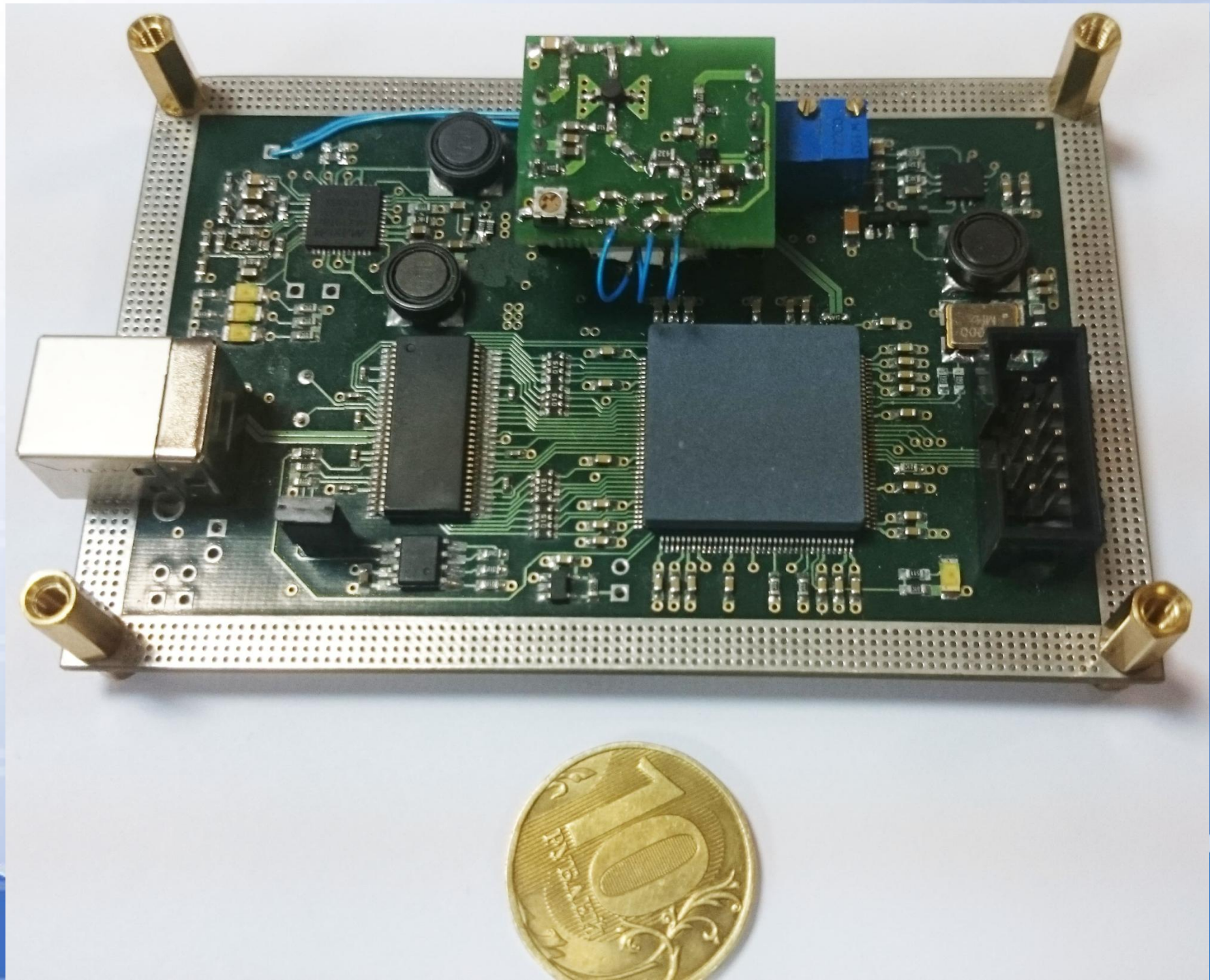
Испытаниях на площадках Ростелекома (Сколково и М10)

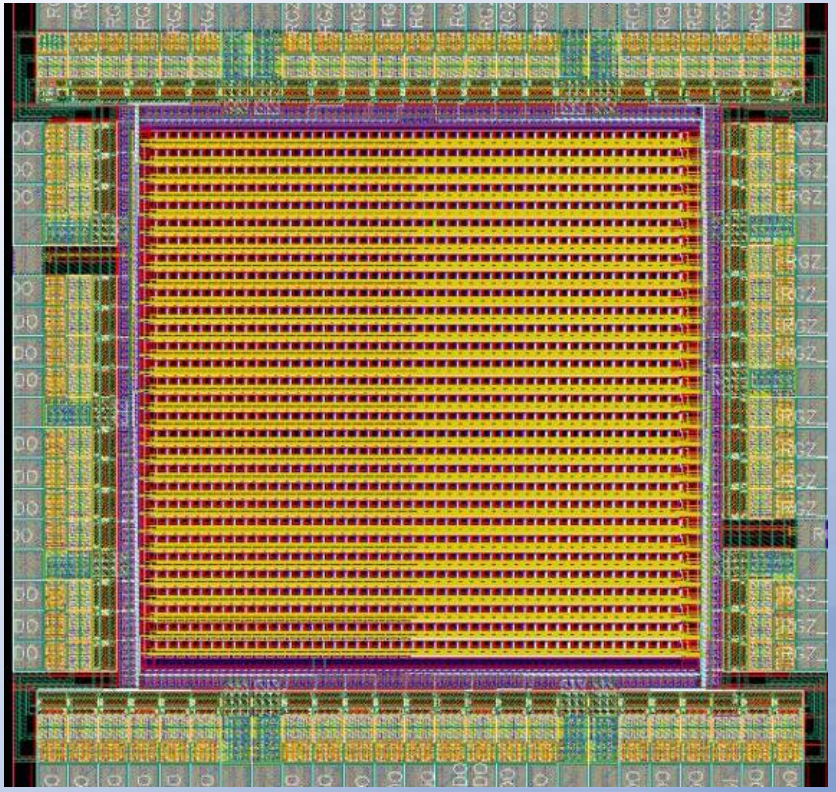


Наиболее широкое применение случайные числа находят в криптографии. Случайные последовательности используются для секретных ключей в системах симметричного шифрования, генерации паролей, PIN кодов для различных типов пластиковых карт, кодов аутентификации, вероятностных алгоритмов и систем квантового распределения ключей.

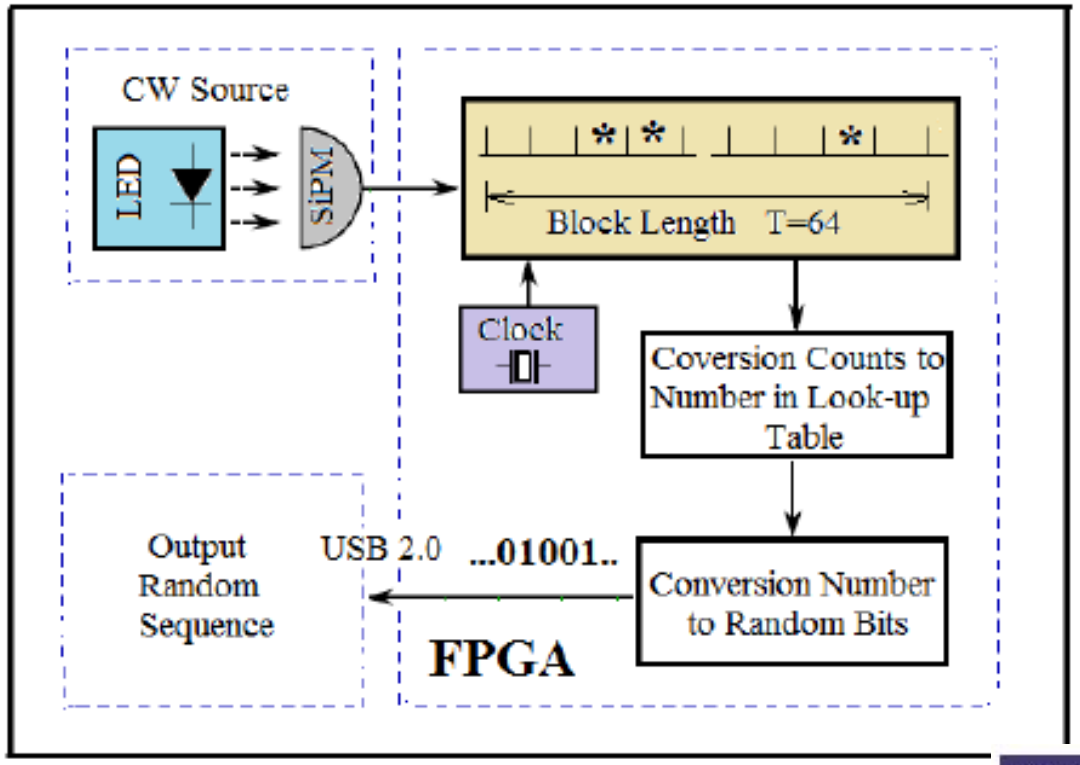
Практически для всех упомянутых применений требуются случайные числа, полученные исключительно с физических генераторов.

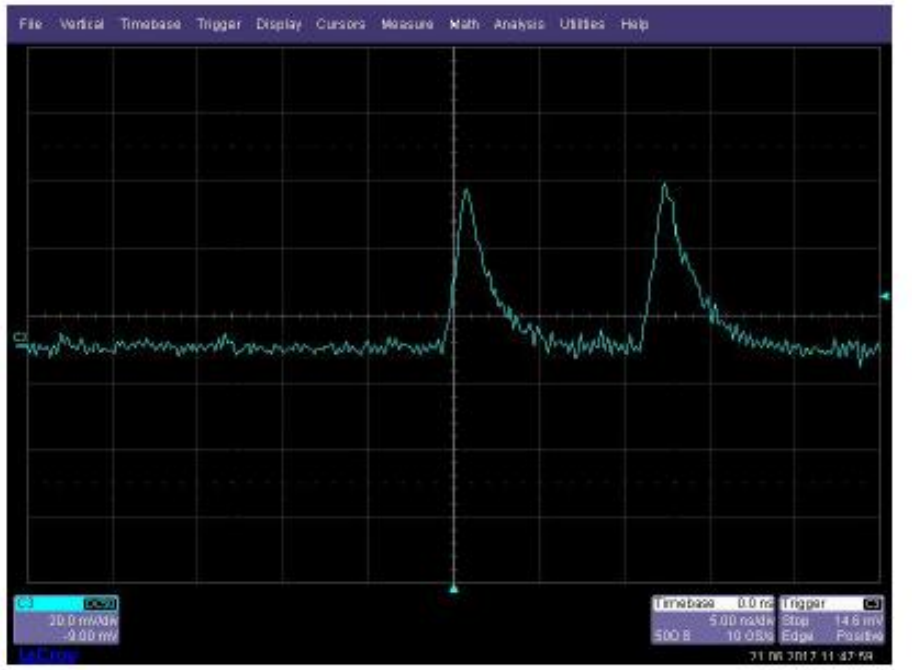

220-10L
C5
220-10L
C5





Оценка среднего числа фотонов на пиксел. Покажем, что генератор действительно работает в квантовом режиме. Оценим среднее число фотонов, падающих на SiPM. Реально наблюдаемой величиной является вероятность отсчета за один такт $P(*) = 0.207$. Данная вероятность равна $P(*) = \mu \cdot \eta \cdot N_{pic}$, μ – среднее число фотонов на один пиксел в SiPM за один такт, $\eta \approx 0.1$ – квантовая эффективность пиксела, $N_{pic} = 2880$ – число пикселей в матрице. В итоге получаем $\mu = \frac{P(*)}{\eta \cdot N_{pic}} \approx 0.7 \cdot 10^{-3}$ [(фотонов)/(в такт на пиксел)], т.е. приходится менее тысячной фотона на пиксел. Напомним, что для когеретного состояния с пуассоновской статистикой вероятность появления одного фотона $P(n = 1) = e^{-\mu}\mu \approx \mu$ ($\mu \ll 1$), соответственно, вероятность появления двух фотонов $P(n = 2) = e^{-\mu}\frac{\mu^2}{2} \approx 2.5 \cdot 10^{-7}$. Таким образом, реализован практически однофотонный режим.[2]


CW Source
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


File Vertical Timebase Trigger Display Cursors Measure Math Analysis Utilities Help

Истинно случайная битовая последовательность 0 и 1.

Pr(0)=Pr(1)=1/2,
Позиции некоррелированы.

Легко сформулировать на интуитивном уровне, но сложно найти истинную случайность, доказать это, и эффективно реализовать.

Information is inevitable physical

Rolf Landauer

the phrase can be continued

Randomness is also inevitable physical

Истинно случайная битовая последовательность 0 и 1.

Pr(0)=Pr(1)=1/2,
Позиции некоррелированы.

Легко сформулировать на интуитивном уровне, но сложно найти истинную случайность, доказать это, и эффективно реализовать.

Генераторы случайных чисел – математические -- некоторое рекурсивное преобразование

$$X(n+1)=F(X(n))=F(F(F\ldots(X(0))))$$

Дают псевдослучайную последовательность – зная затравочное X(0), знаем все.

Физические генераторы случайных чисел – измерение некоторого физического процесса (системы).

Классические генераторы – система “живет” по законам классической физики. Эволюция определяется начальными условиями -- также выдают псевдослучайные последовательности.

Квантовые генераторы -- измерение квантовой системы каждый раз приготовленной в одном и том же начальном состоянии дает принципиально непредсказуемый результат измерений.

Истинная случайность есть только в квантовой области.

Найти такой процесс, узнать сколько в нем истинной случайности и вытянуть из него эффективно истинно случайную последовательность 0 и 1.

Какой “линейкой” измерять случайность в физическом процессе.

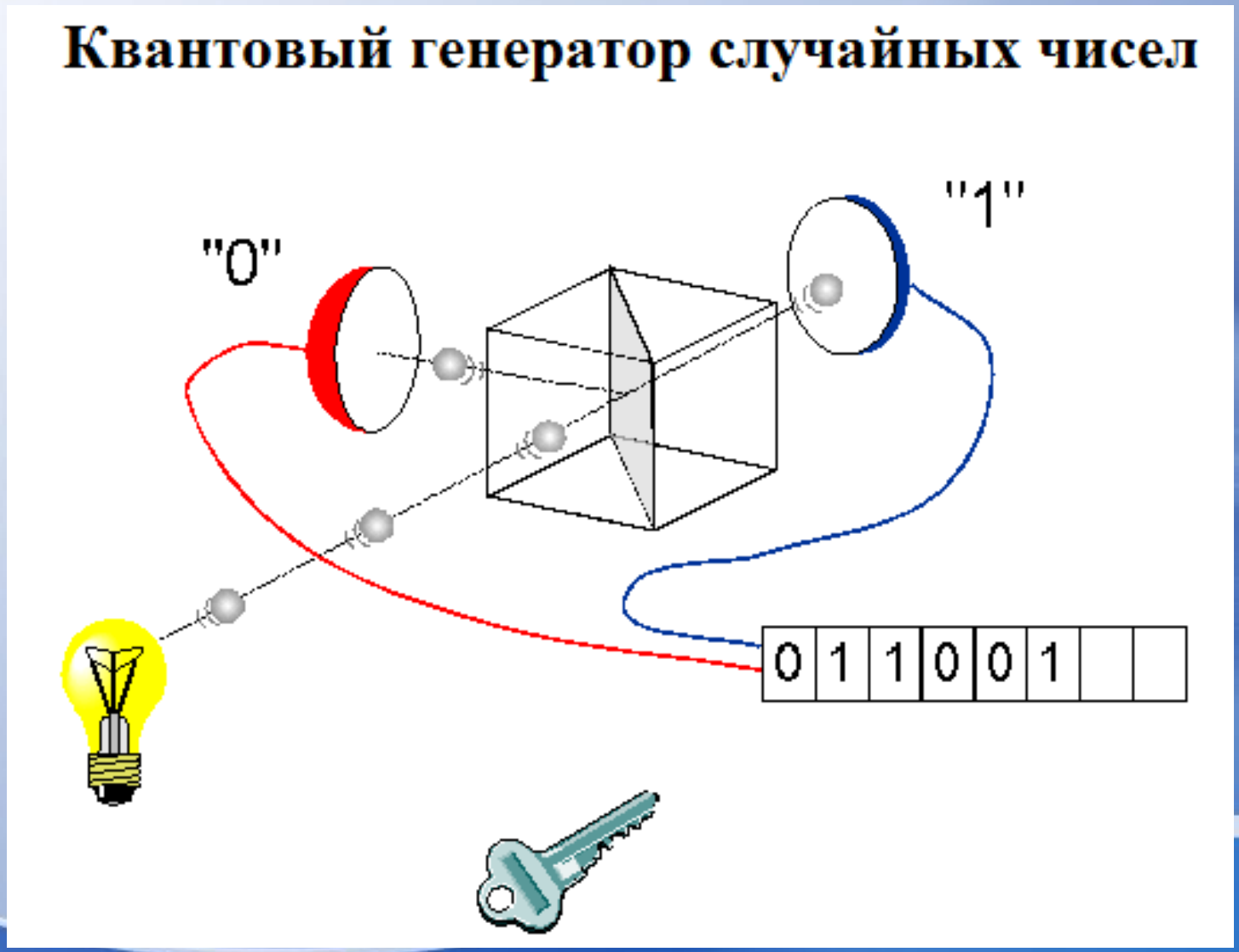
The absence of evidence is not evidence of absence.

Отсутствие доказательств вины не есть доказательство невиновности.

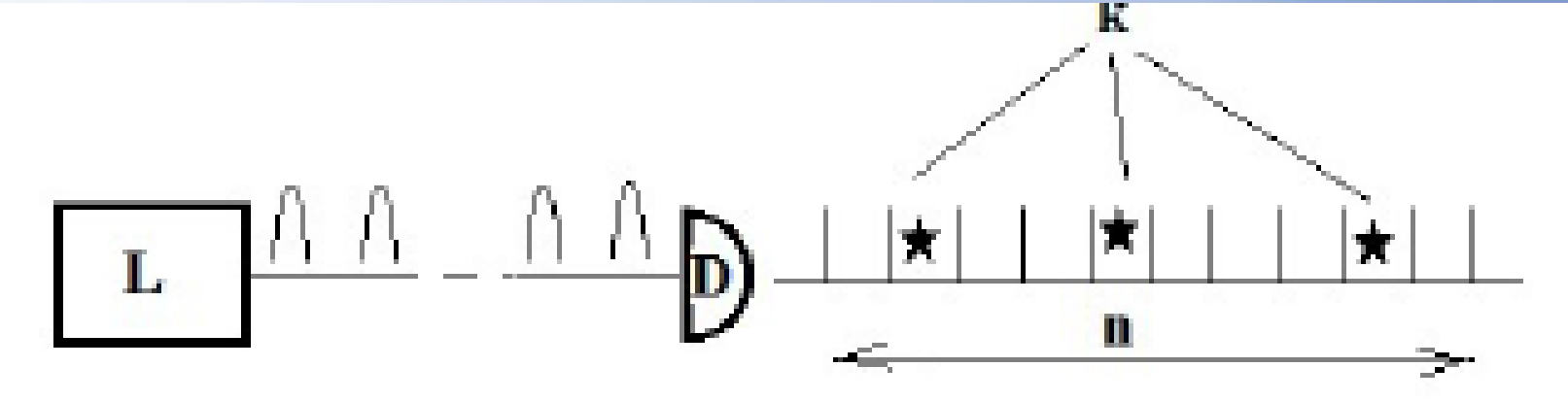
Доска Гальтона -- классический пример классической не случайности (псевдослучайности)

При реализации квантовых генераторов случайных чисел принципиально важно иметь математически доказуемый, экспериментально реализуемый и проверяемый процесс измерений над системой, из которого генерируется исходная случайная последовательность. Это позволяет быть уверенным, что происхождение случайности действительно имеет квантовую природу.

Необходимость квантового генератора случайных чисел.



Фотоэффект, Когерентное состояние, Статистика Пуассона



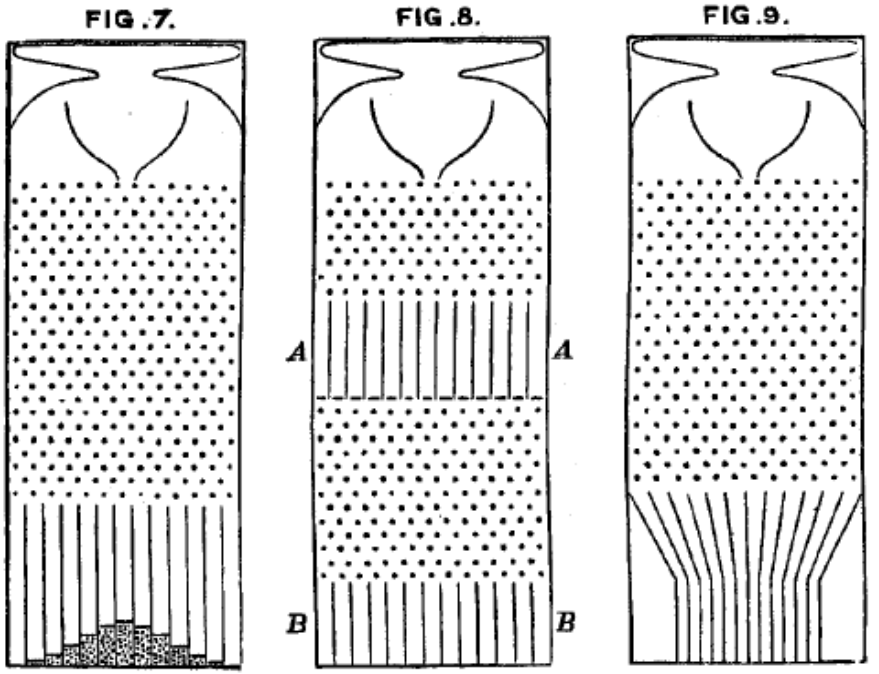
NATURAL INHERITANCE

BY

FRANCIS GALTON, F.R.S.

AUTHOR OF

"HEREDITARY GENIUS," "INQUIRIES INTO HUMAN FACULTY," ETC.



Various Techniques Used in Connection With Random Digits

By John von Neumann

pseudo-random. A simpler process suggested by Dr. Ulam is to use the mapping function $f(x)=4x(1-x)$. If one produces a sequence $\{x_i\}$ in this manner, x_{i+1} is completely determined by x_i, so that independence is lacking. It is, however, quite instructive to analyze the nature of randomness that exists in this sequence. One can, by an incomplete argumentation, apparently establish one kind, and then see that in reality a very different kind holds. First, let the relations $x_i=\sin^2 \pi\alpha_i$ define the sequence $\{\alpha_i\}$ (each modulo 1). Since $x_{i+1}=4x_i(1-x_i)$, one sees that $\alpha_{i+1}=2\alpha_i$ (modulo 1). The sequence $\{\alpha_i\}$ is thus obtained in binary representation by shifting the binary number $\alpha_1=\cdot\beta_1\beta_2\beta_3\beta_4\ \ldots$ as follows: $\alpha_2=\cdot\beta_2\beta_3\beta_4\ \ldots$, $\ldots$, $\alpha_i=\cdot\beta_i\beta_{i+1}\beta_{i+2}\ \ldots$, $\ldots$. It follows from the theorem of Borel about the randomness of the digits of real numbers that, for all numbers α_1 except those in a set of Lebesgue measure zero, the numbers α_i are uniformly distributed on the interval (0,1).

Метод фон Неймана,
Квантовые генераторы случайных чисел,
Арифметическое кодирование,
Треугольник Паскаля, числа Фибоначчи

00 10 01 11 10 00

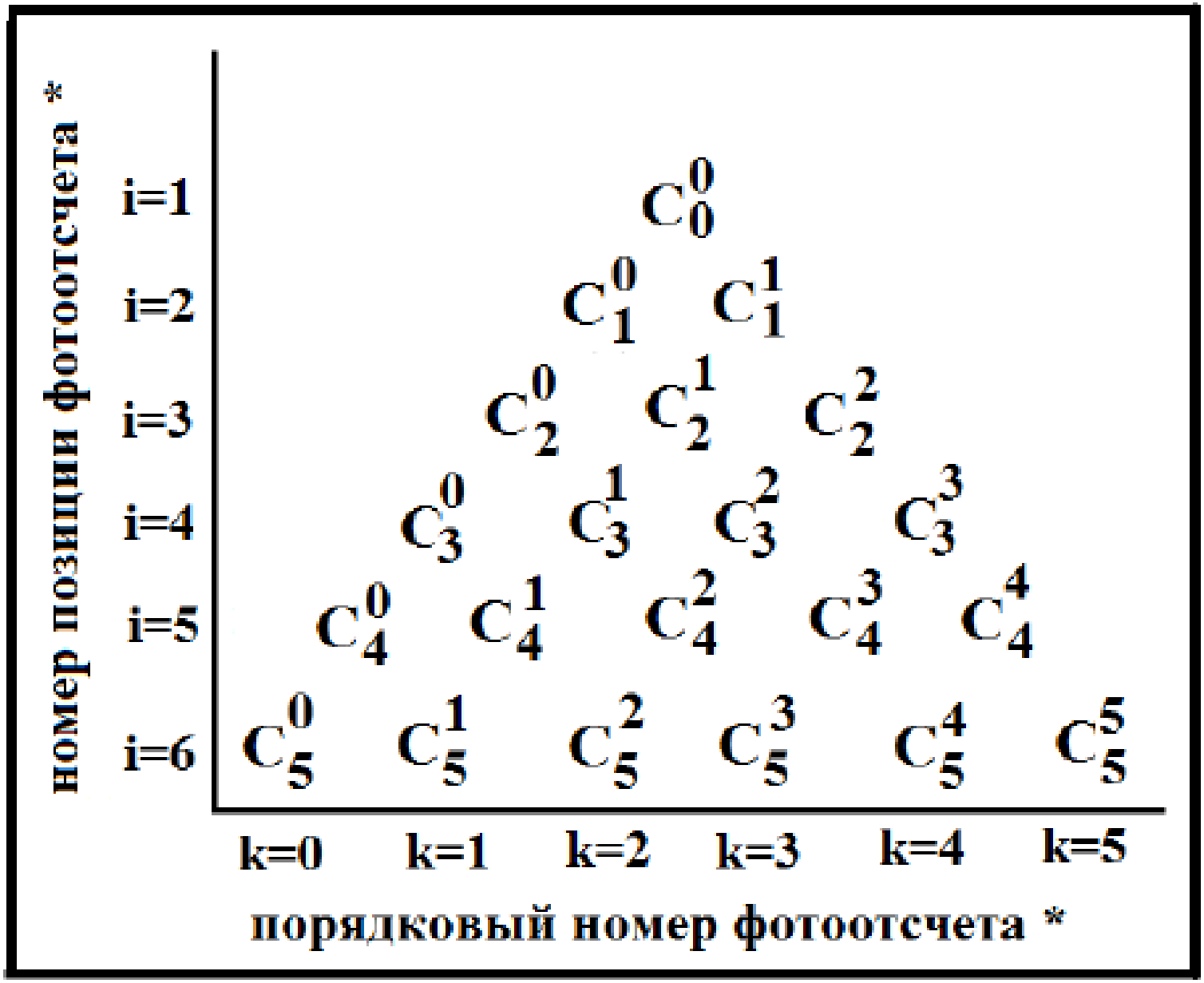
00 --
10 -- 0
01 -- 1
11 --

Арифметическое кодирование,
Треугольник Паскаля, числа Фибоначчи
64 такта

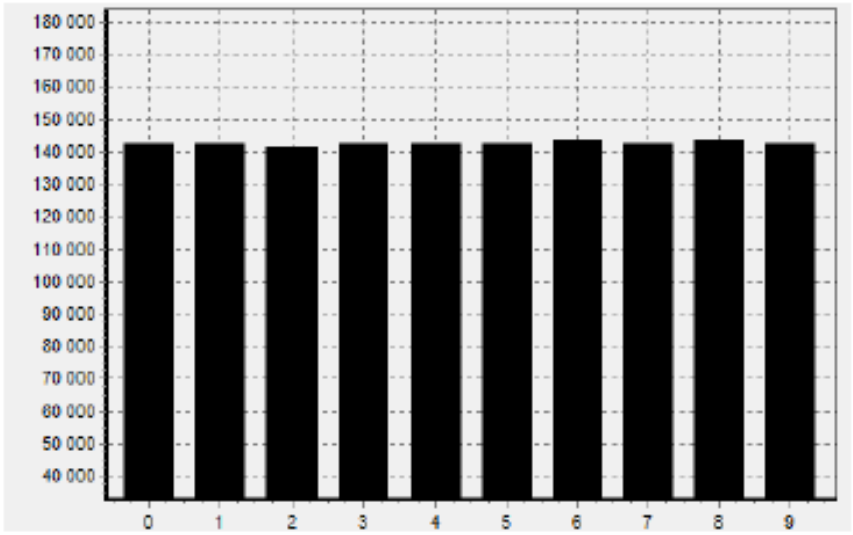
001001111000..010011100 ---- 00000..00 0 (64 бита адрес
…….....…… ---- 00000..01 номер 1
…… ----

Всего таких последовательностей $2^{64} - 10^{22}$

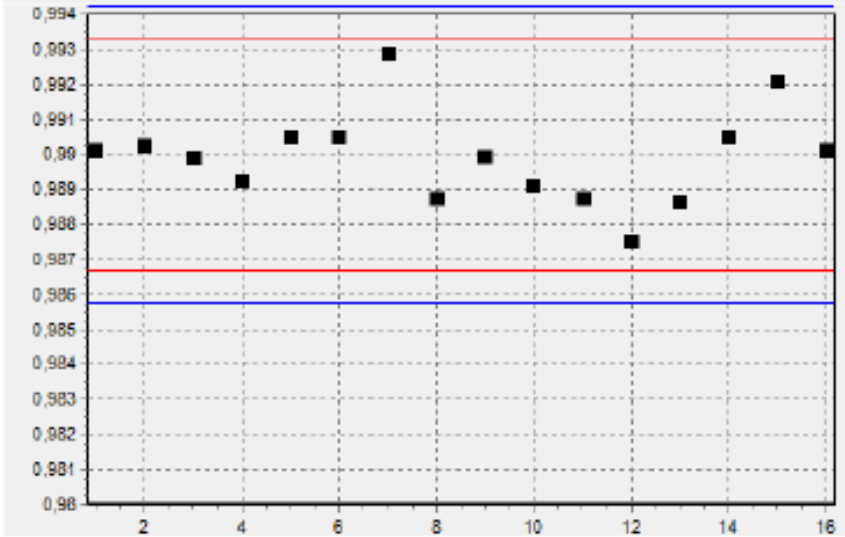
$10^{22} \rightarrow 10^{10}\ 10^{12}$


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 *

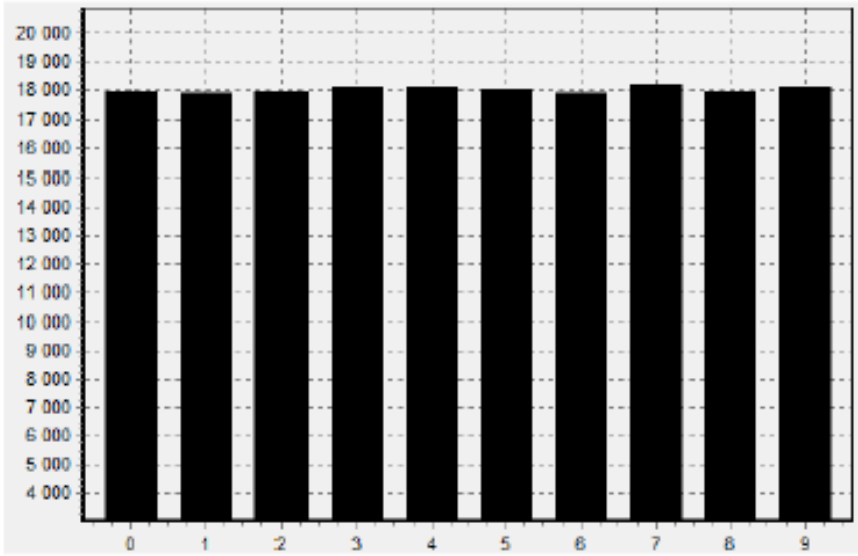
N	Название теста	доля послед. $M = 8000$ $L = 1 \cdot 10^6$	доля послед. $M = 1000$ $L = 2 \cdot 10^6$
1	Frequency Test	0.9901	0.9880
2	Block Frequency	0.9902	0.9886
3	Cumulative Sums	0.9899	0.9880
4	Cumulative Sums Reverse	0.9892	0, 9840
5	Runs	0.9905	0.9880
6	Longest Runs	0.9905	0.9886
7	Rank	0.9929	0.9910
8	FFT Fast Fourier Transform	0.9888	0.9879
9	Non Overlapping Template	0.9899	0.9893
10	Overlapping Template	0.9891	0.9867
11	Universal	0.9987	0.9880
12	Approximate Entropy	0.9874	0.9950
13	Random Excursions	0.9883	0.9914
14	Random Excursions Variant	0.9904	0.9915
15	Serial	0.9921	0.9860
16	Linear Complexity	0.9901	0.9880


180 000
170 000
160 000
150 000
140 000
130 000
120 000
110 000
100 000
90 000
80 000
70 000
60 000
50 000
40 000
0 1 2 3 4 5 6 7 8 9

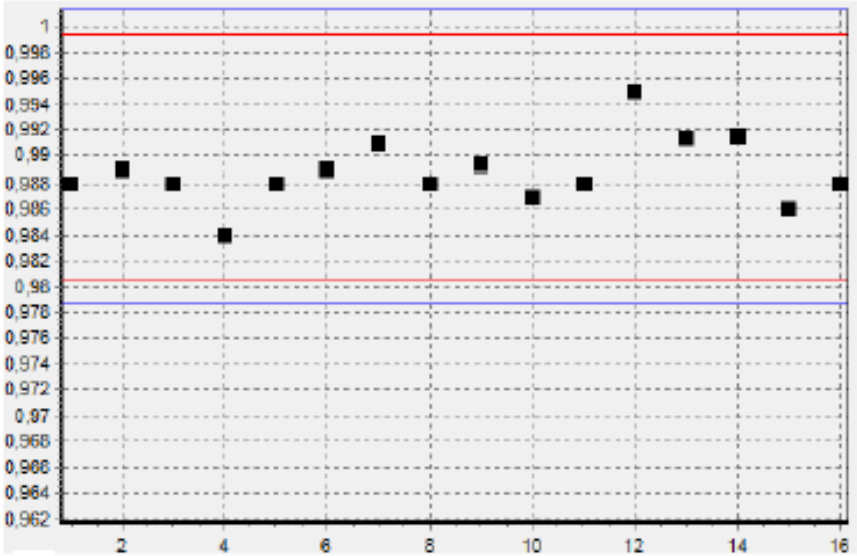
a)


0,994
0,993
0,992
0,991
0,99
0,989
0,988
0,987
0,986
0,985
0,984
0,983
0,982
0,981
0,98
2 4 6 8 10 12 14 16

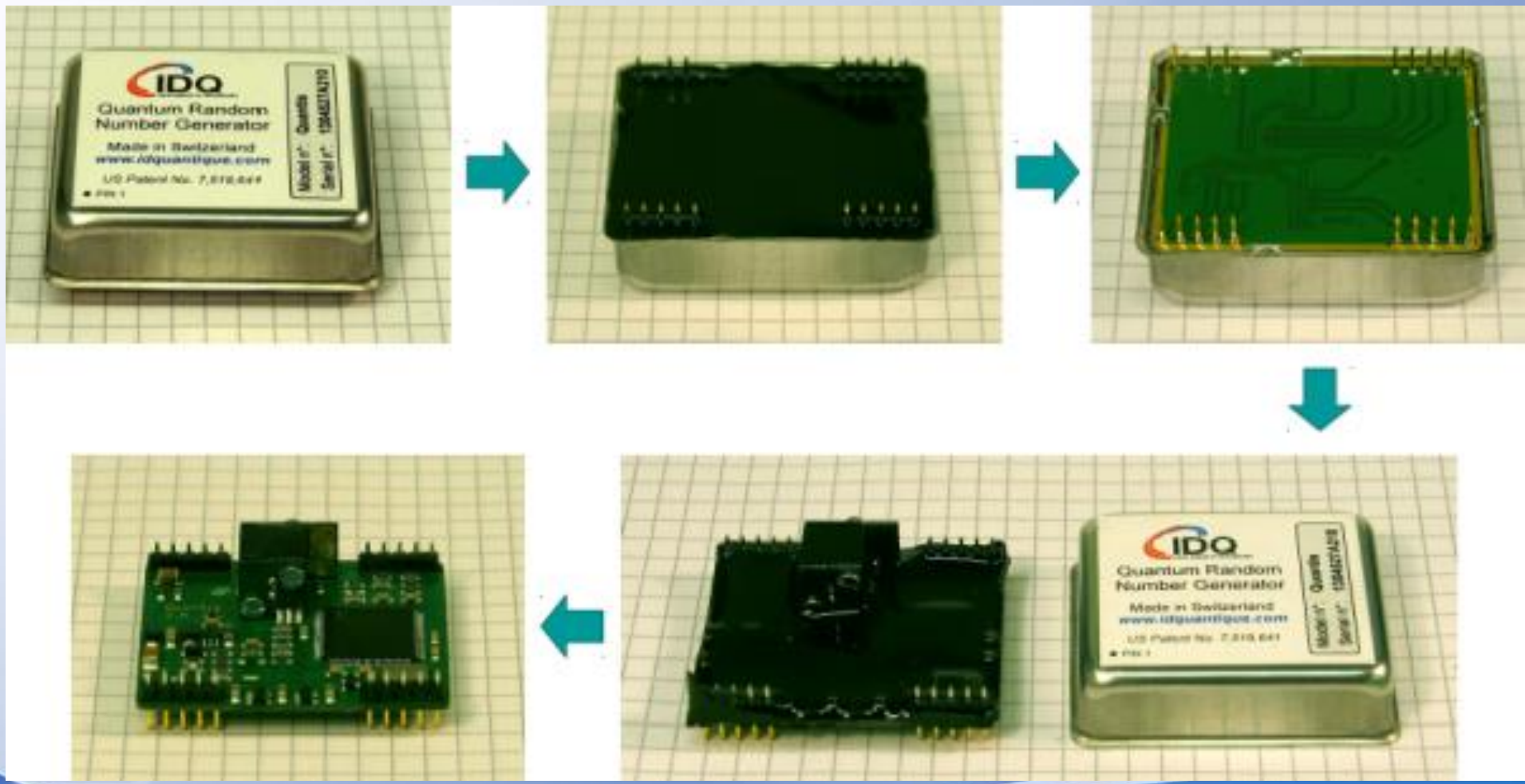
b)

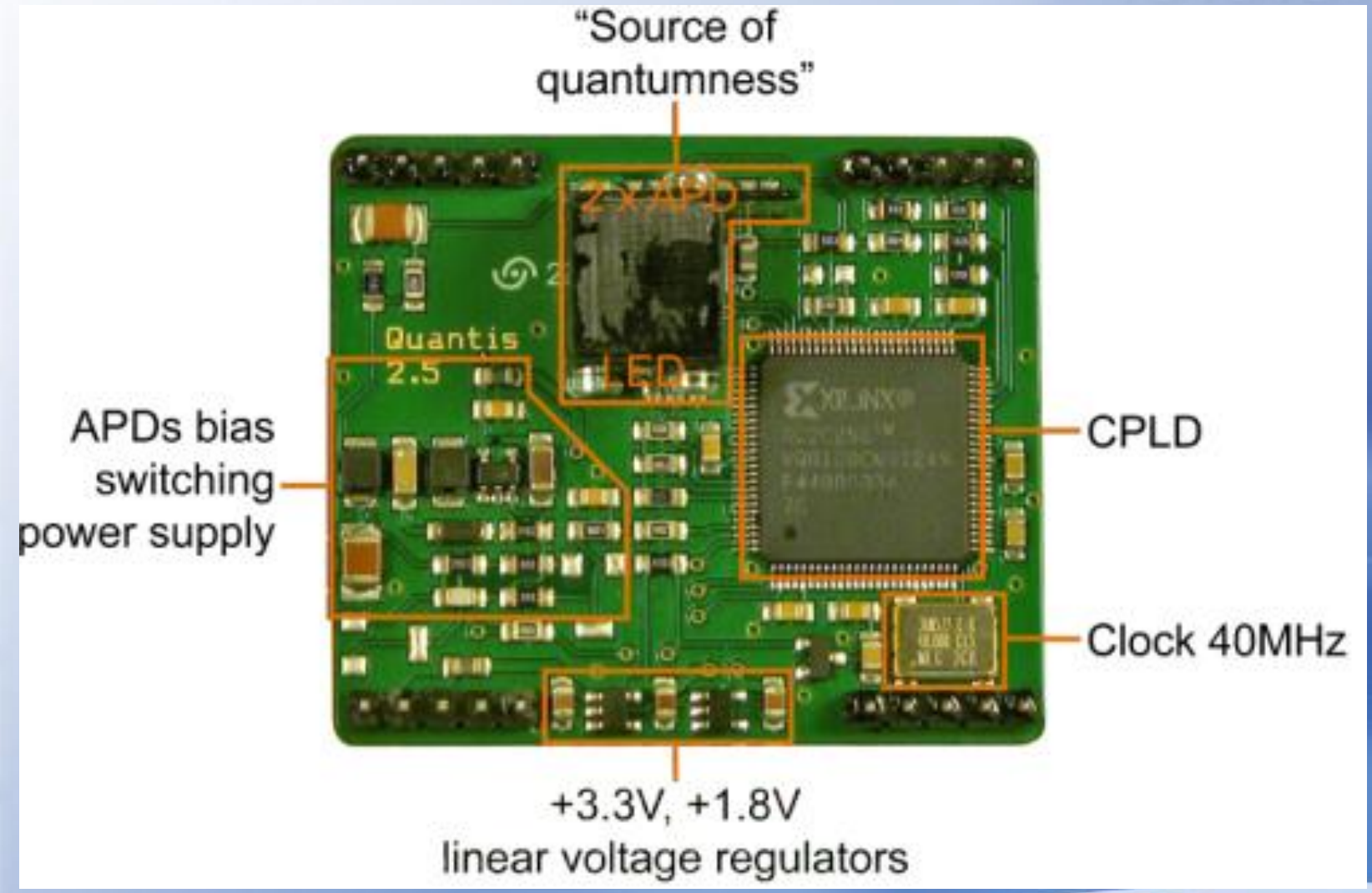

20 000
19 000
18 000
17 000
16 000
15 000
14 000
13 000
12 000
11 000
10 000
9 000
8 000
7 000
6 000
5 000
4 000
0 1 2 3 4 5 6 7 8 9

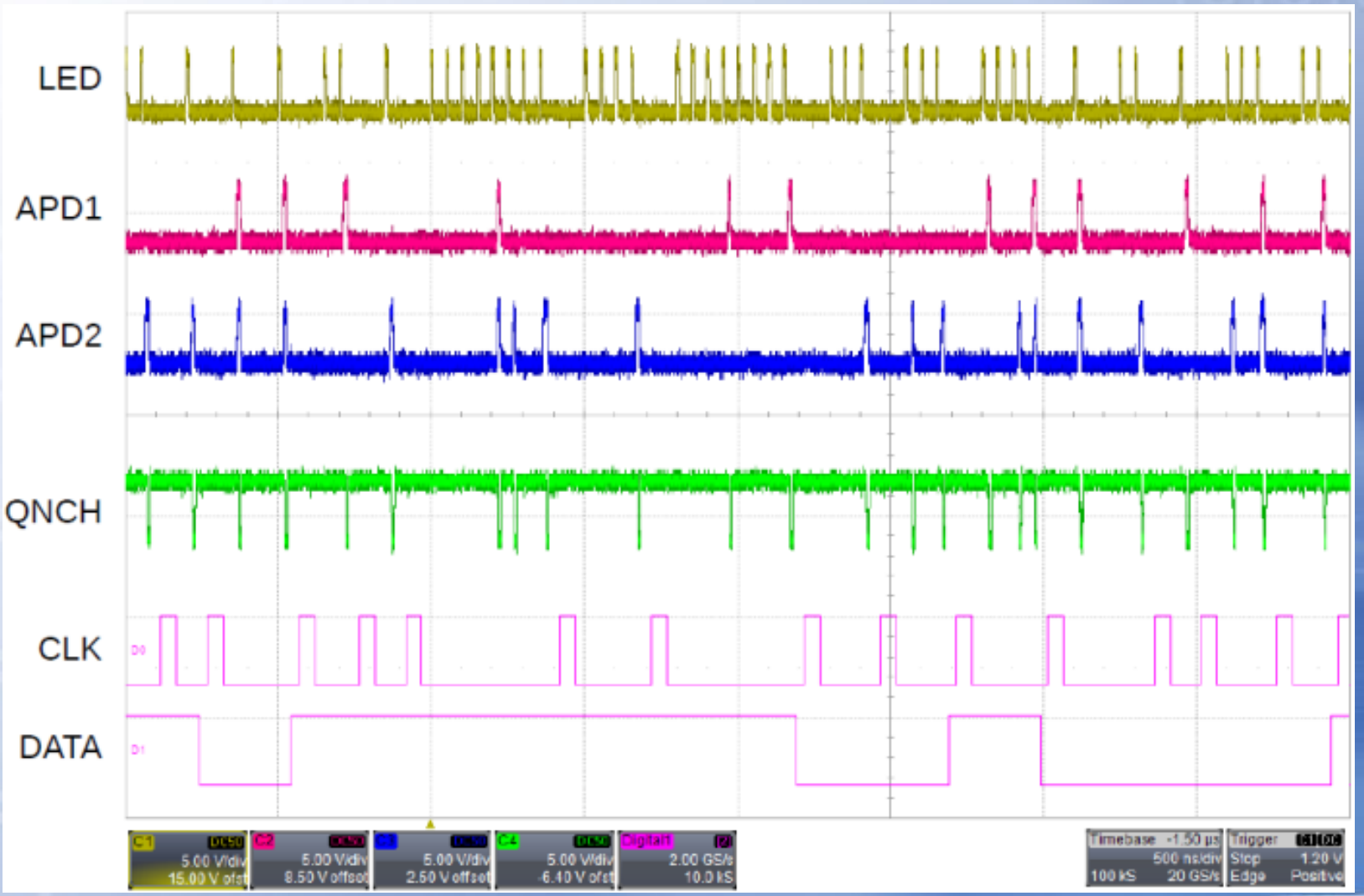
c)


1
0,998
0,996
0,994
0,992
0,99
0,988
0,986
0,984
0,982
0,98
0,978
0,976
0,974
0,972
0,97
0,968
0,966
0,964
0,962
2 4 6 8 10 12 14 16

d)


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"
2xAPD
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
C1 DC50
5.00 V/div
15.00 V offset
C2 DC50
5.00 V/div
8.50 V offset
C3 DC50
5.00 V/div
2.50 V offset
C4 DC50
5.00 V/div
-6.40 V offset
Digital1
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

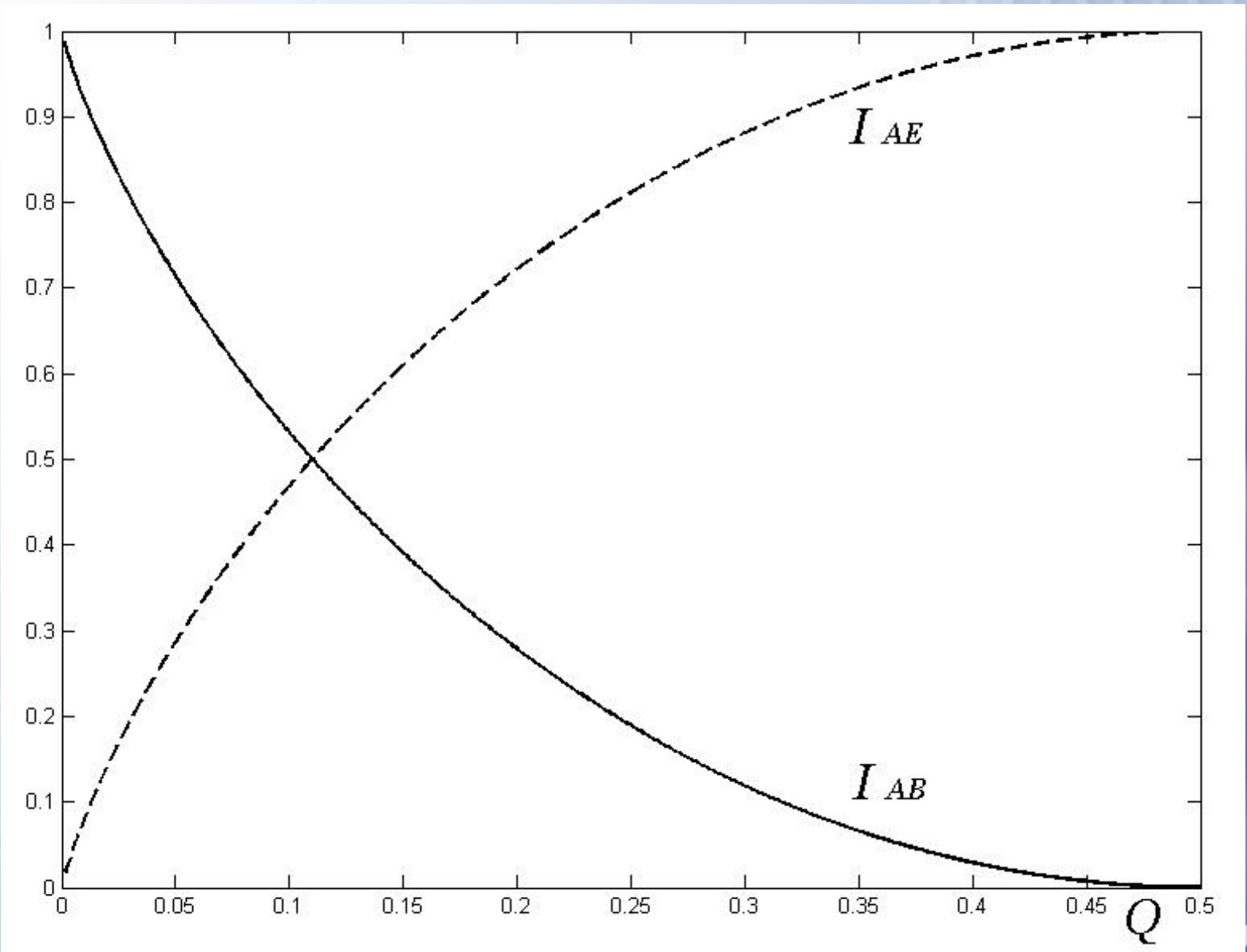
3. Как это работает – общие принципы

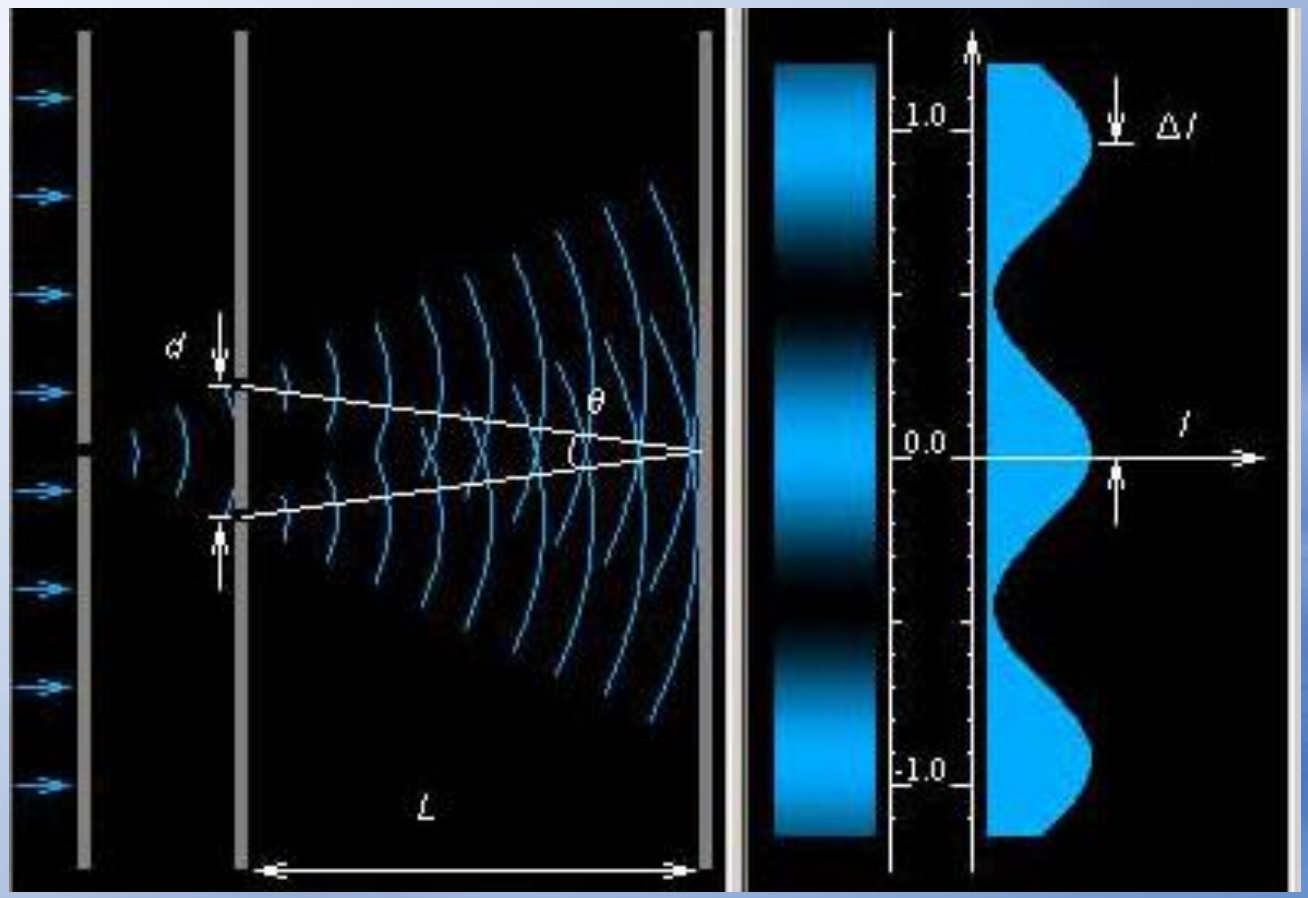
Фундаментальные запреты квантовой механики.

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.

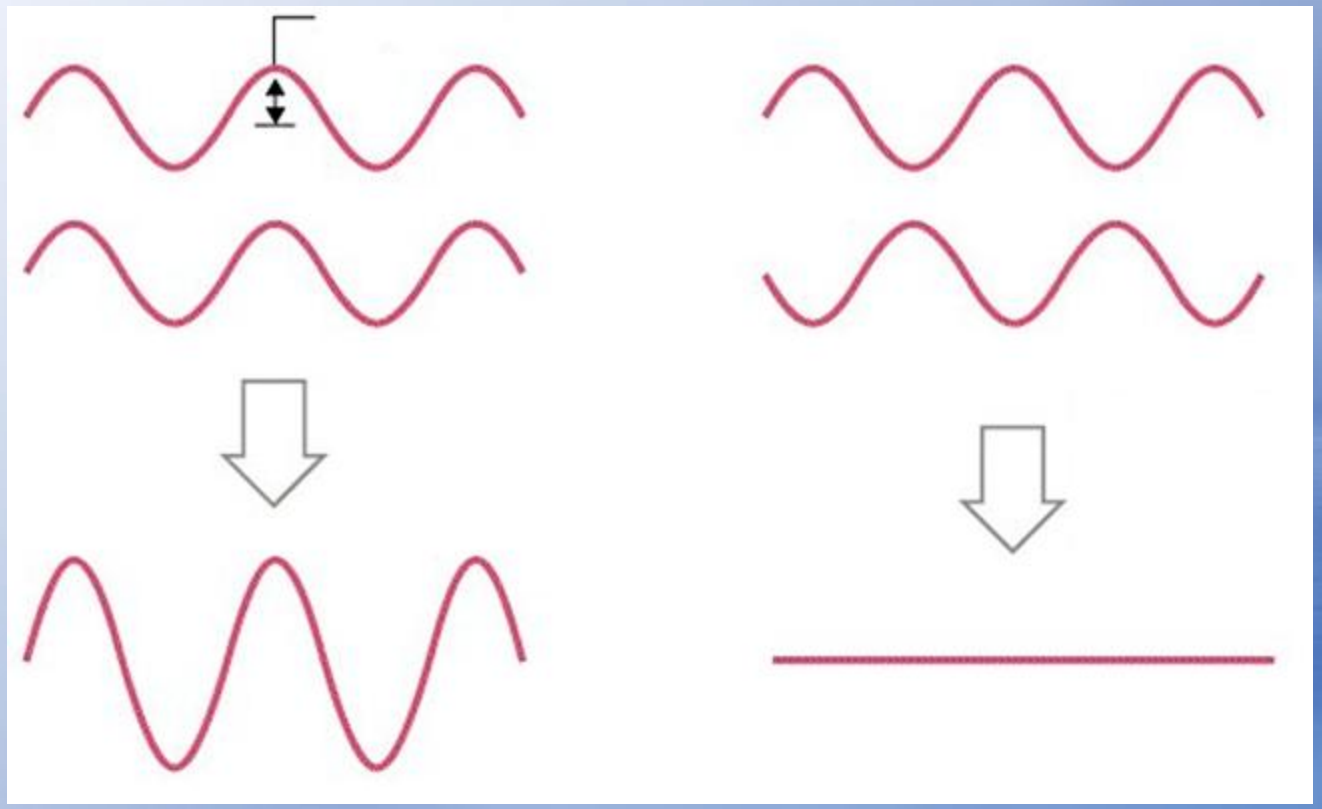
Следствия для распределения секретных ключей.

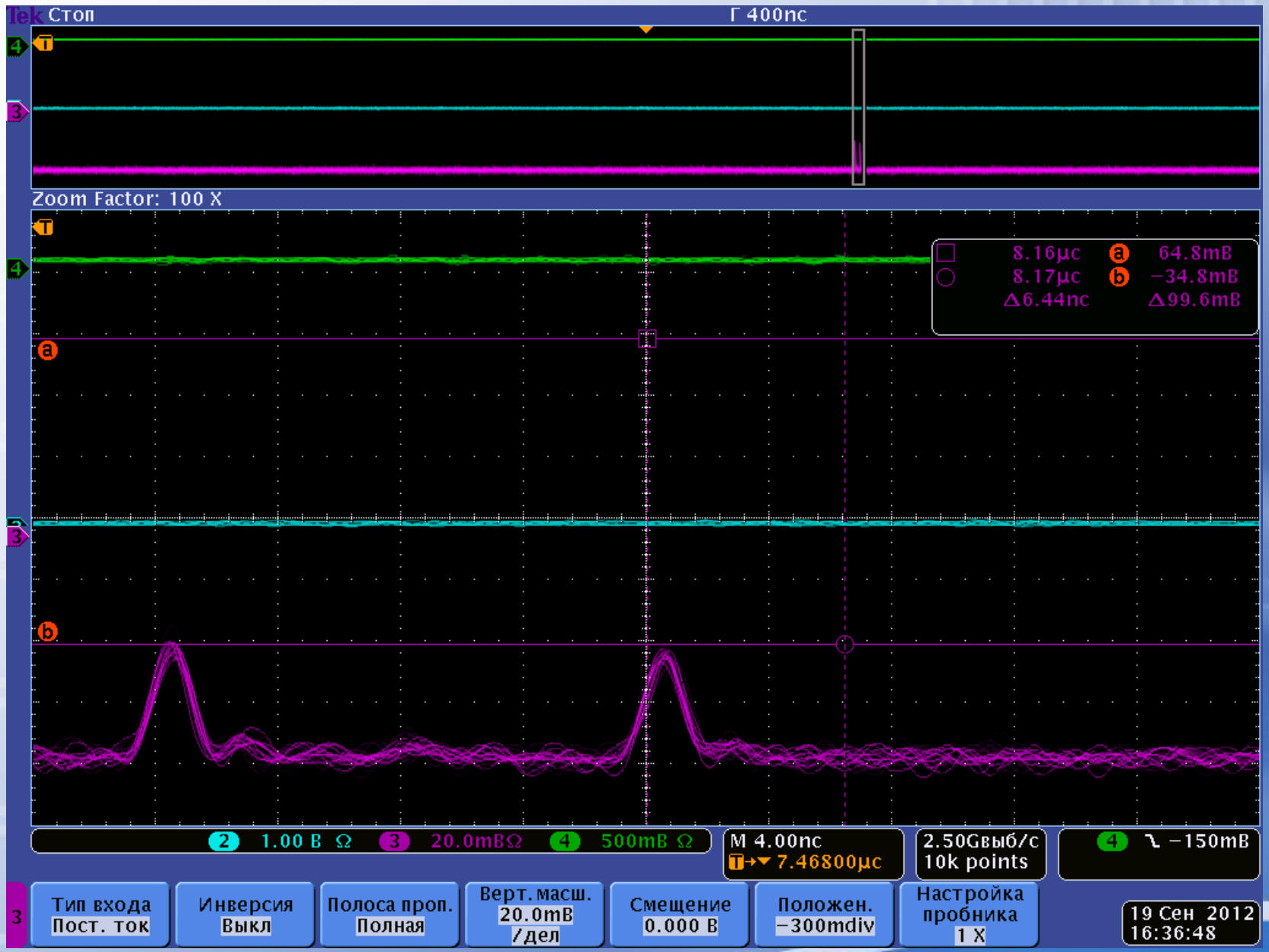
1) Любое вторжение в канал связи приводит к возмущению квантовых состояний, которое детектируется – приводит к ошибке в первичных ключах.
2) Ошибка связана с верхней фундаментальной границей информации, которая уходит к подслушивателю при данной наблюдаемой вероятности ошибок на приемной стороне.
3)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

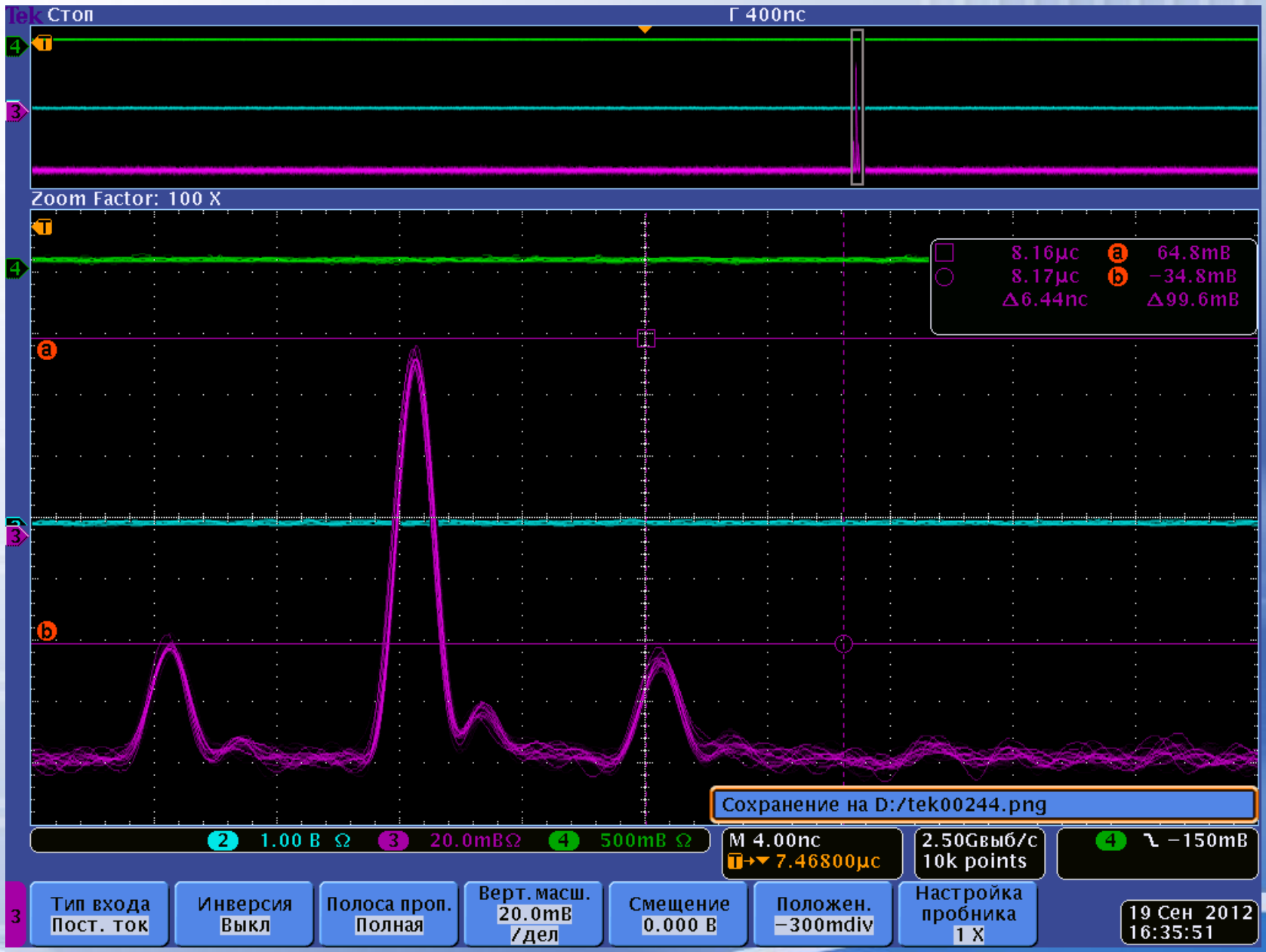

1
0.9
0.8
0.7
0.6
0.5
0.4
0.3
0.2
0.1
0
0
0.05
0.1
0.15
0.2
0.25
0.3
0.35
0.4
0.45
0.5
Q
I AE
I AB


d
θ
L
1.0
Δ I
0.0
I
-1.0

Фазовое кодирование



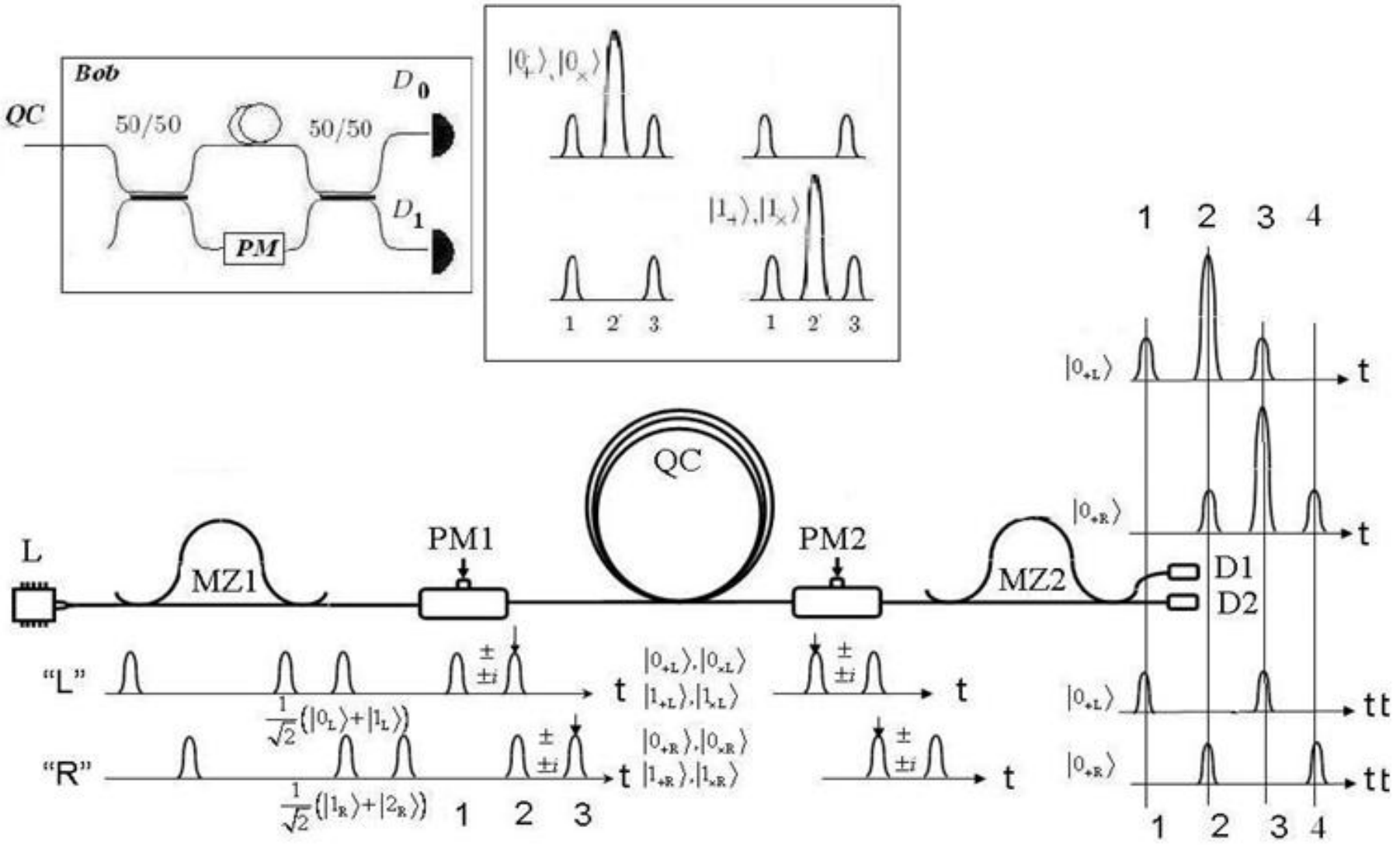

Tek Стоп
Г 400nc
Zoom Factor: 100 X
8.16µc
8.17µc
Δ6.44nc
a 64.8mB
b −34.8mB
Δ99.6mB
2 1.00 B Ω
3 20.0mBΩ
4 500mB Ω
M 4.00nc
T→▼ 7.46800µc
2.50Gвыб/с
10k points
4 ∖ −150mB
3
Тип входа
Пост. ток
Инверсия
Выкл
Полоса проп.
Полная
Верт. масш.
20.0mB
/дел
Смещение
0.000 B
Положен.
−300mdiv
Настройка
пробника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

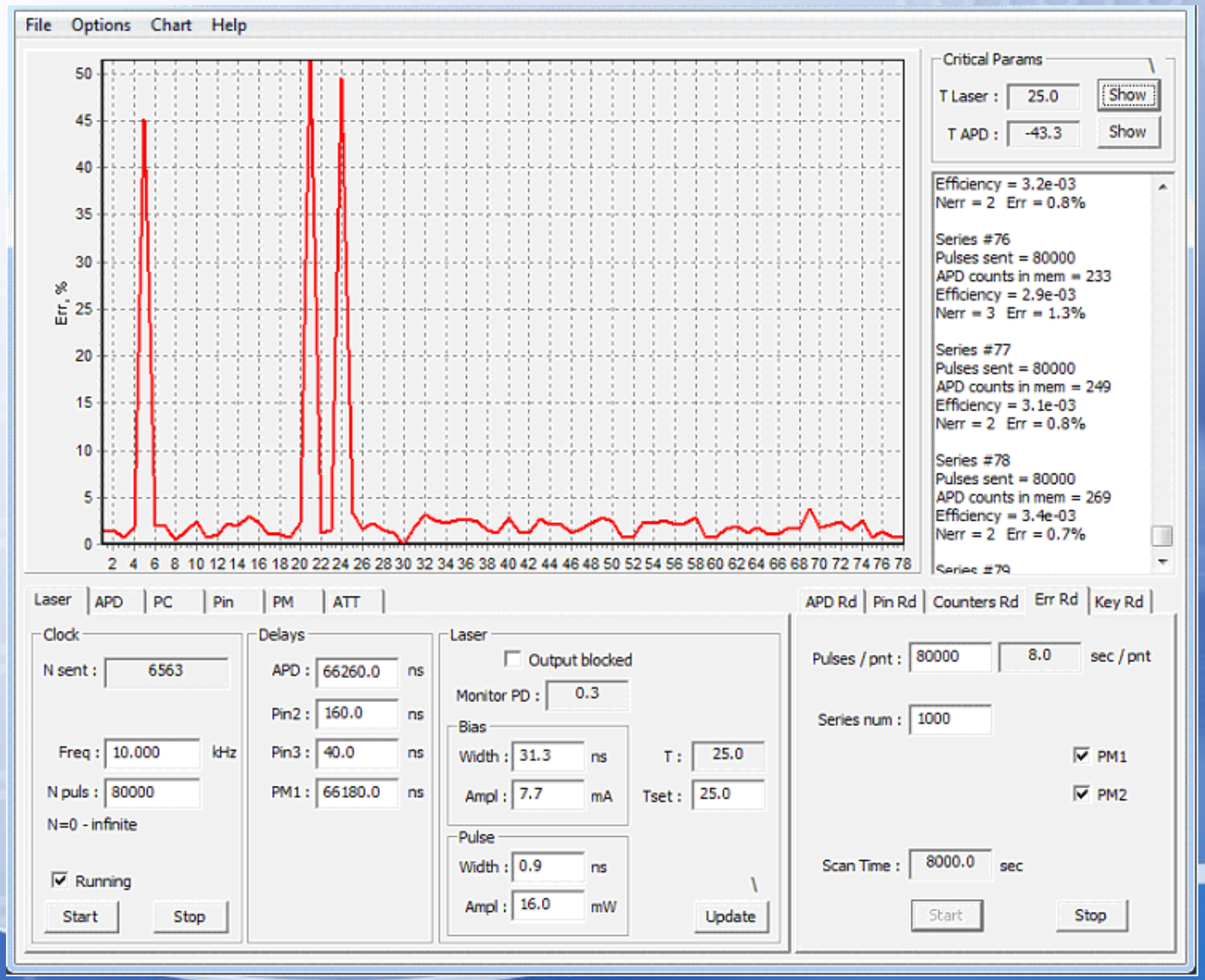

Tek Стоп
Г 400nc
Zoom Factor: 100 X
8.16µc a 64.8mB
8.17µc b −34.8mB
Δ6.44nc Δ99.6mB
Сохранение на D:/tek00244.png
2 1.00 B Ω 3 20.0mBΩ 4 500mB Ω
M 4.00nc
T→▼ 7.46800µc
2.50Gвыб/с
10k points
4 ∖ −150mB
Тип входа
Пост. ток
Инверсия
Выкл
Полоса проп.
Полная
Верт. масш.
20.0mB
/дел
Смещение
0.000 B
Положен.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

Фазово-временное кодирование

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

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




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
APD Rd
Pin Rd
Counters Rd
Err Rd
Key Rd
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
Pulses / pnt : 80000 8.0 sec / pnt
Series num : 1000
PM1
PM2
Scan Time : 8000.0 sec
Start
Stop

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.

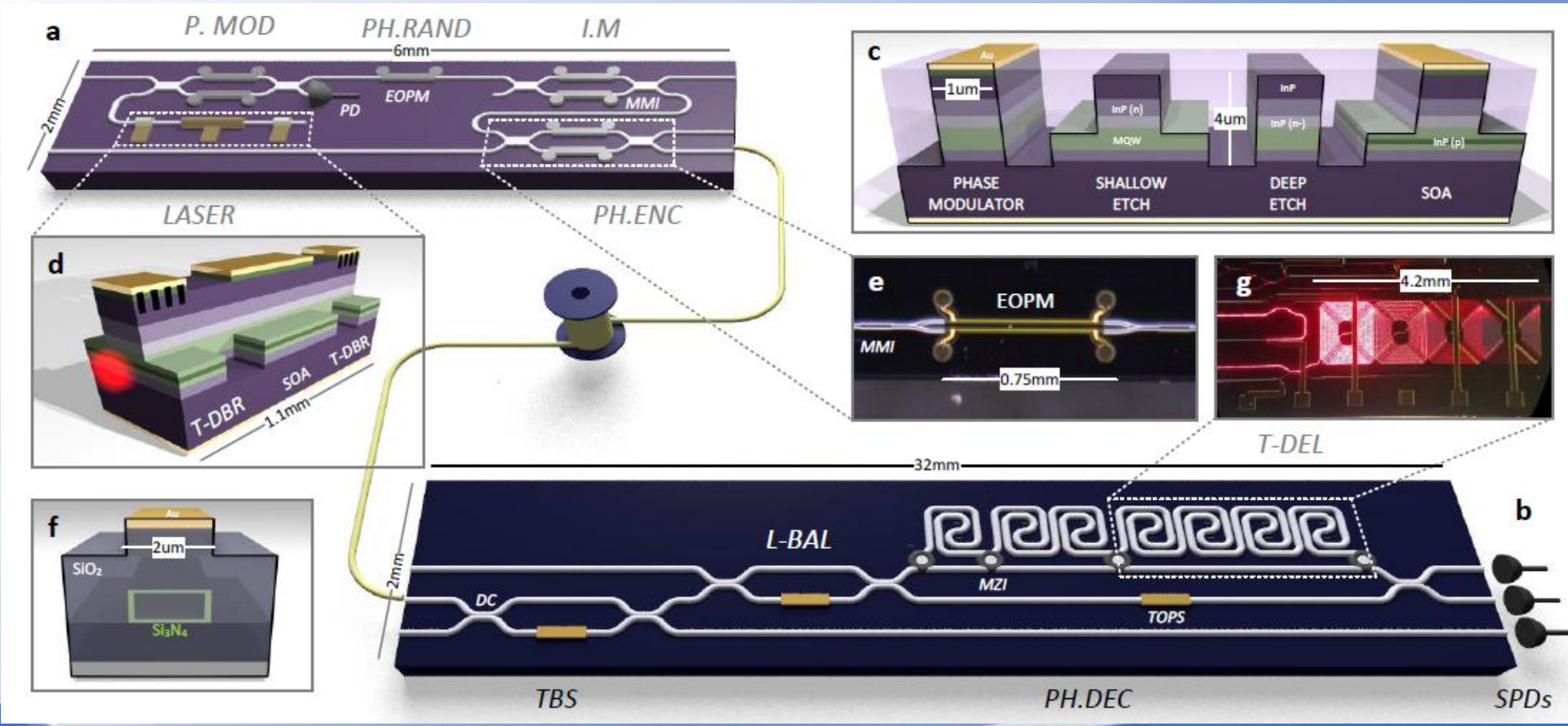
1) BB84.
2) B92.
3) SARG.
4) Decoy State.
5) Фазово-временной.
6) DPS – Differential Phase Shift.
7) COW – Coherent One Way.
8) CW – с непрерывными переменнымию
9) С реперным состоянием.
10) Релятивистская квантовая криптография.

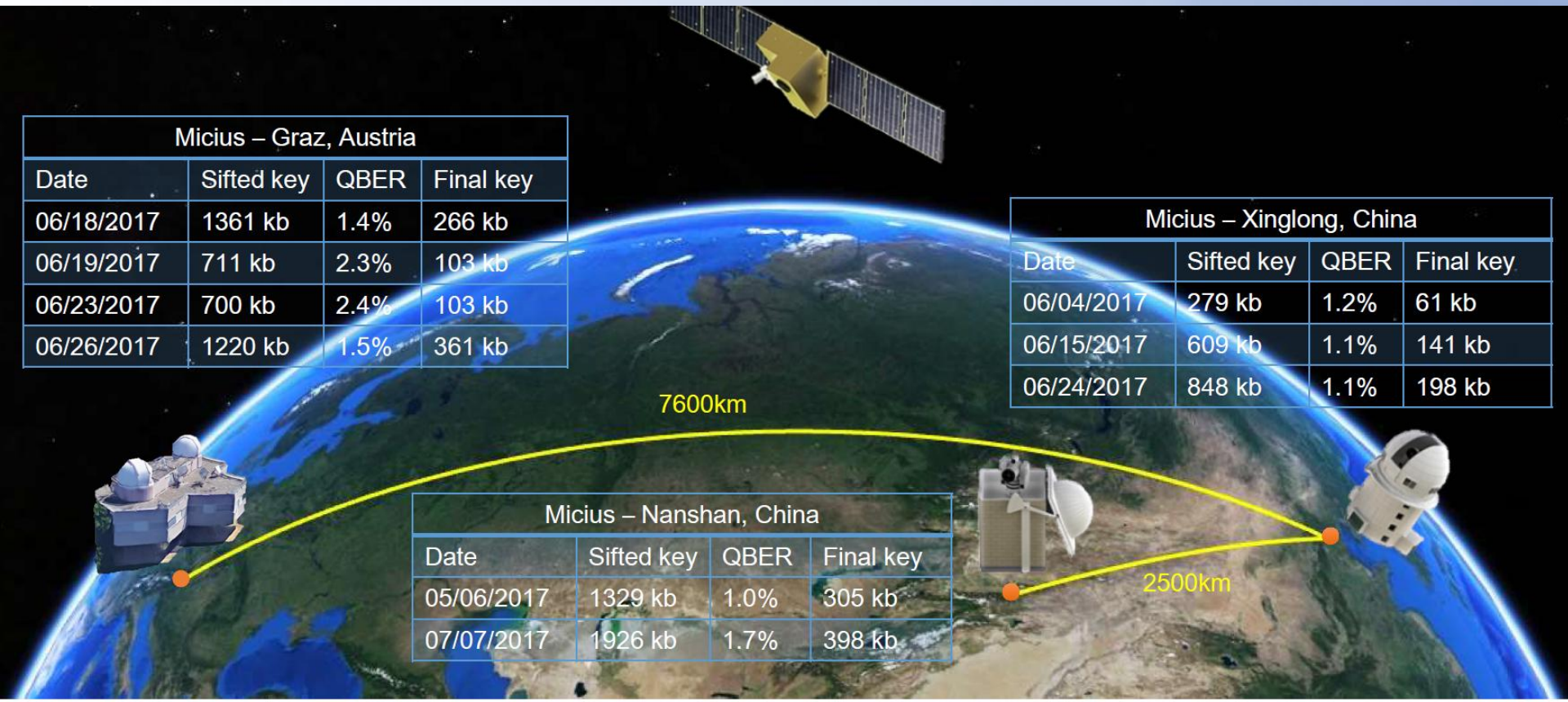
Как это будет выглядеть в будущем – контуры будущего уже явно просматриваются сегодня.

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,†]

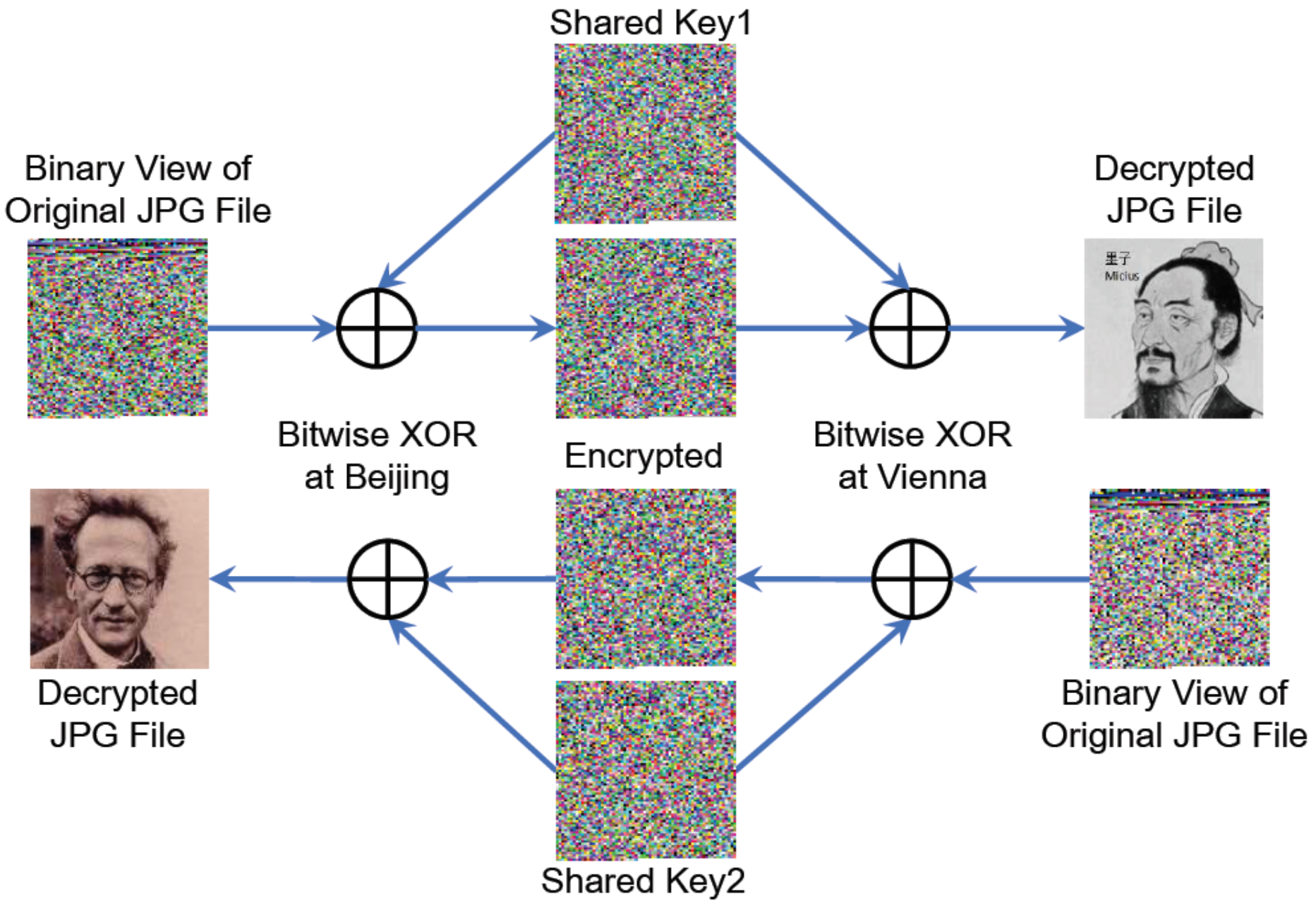




Micius – Graz, Austria			
Date	Sifted key	QBER	Final key
06/18/2017	1361 kb	1.4%	266 kb
06/19/2017	711 kb	2.3%	103 kb
06/23/2017	700 kb	2.4%	103 kb
06/26/2017	1220 kb	1.5%	361 kb

Micius – Xinglong, China			
Date	Sifted key	QBER	Final key
06/04/2017	279 kb	1.2%	61 kb
06/15/2017	609 kb	1.1%	141 kb
06/24/2017	848 kb	1.1%	198 kb

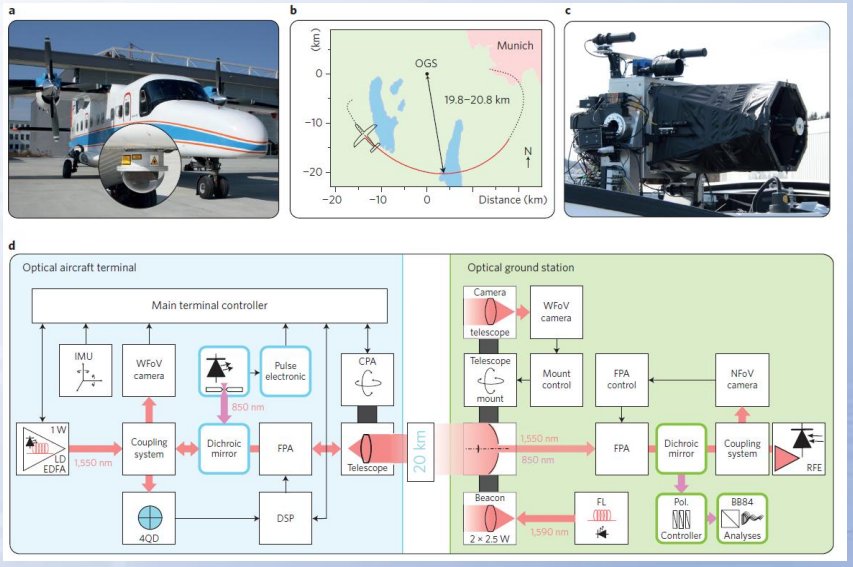
Micius – Nanshan, China			
Date	Sifted key	QBER	Final key
05/06/2017	1329 kb	1.0%	305 kb
07/07/2017	1926 kb	1.7%	398 kb

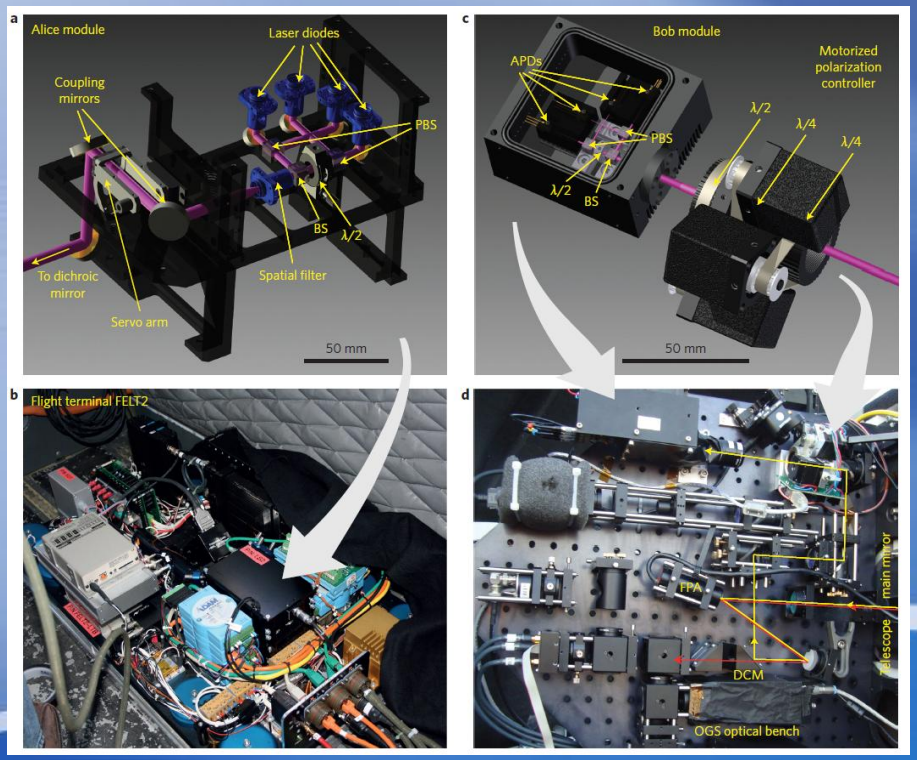

Shared Key1
Binary View of
Original JPG File
Decrypted
JPG File
里子
Micius
Bitwise XOR
at Beijing
Encrypted
Bitwise XOR
at Vienna
Decrypted
JPG File
Binary View of
Original JPG File
Shared Key2

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]





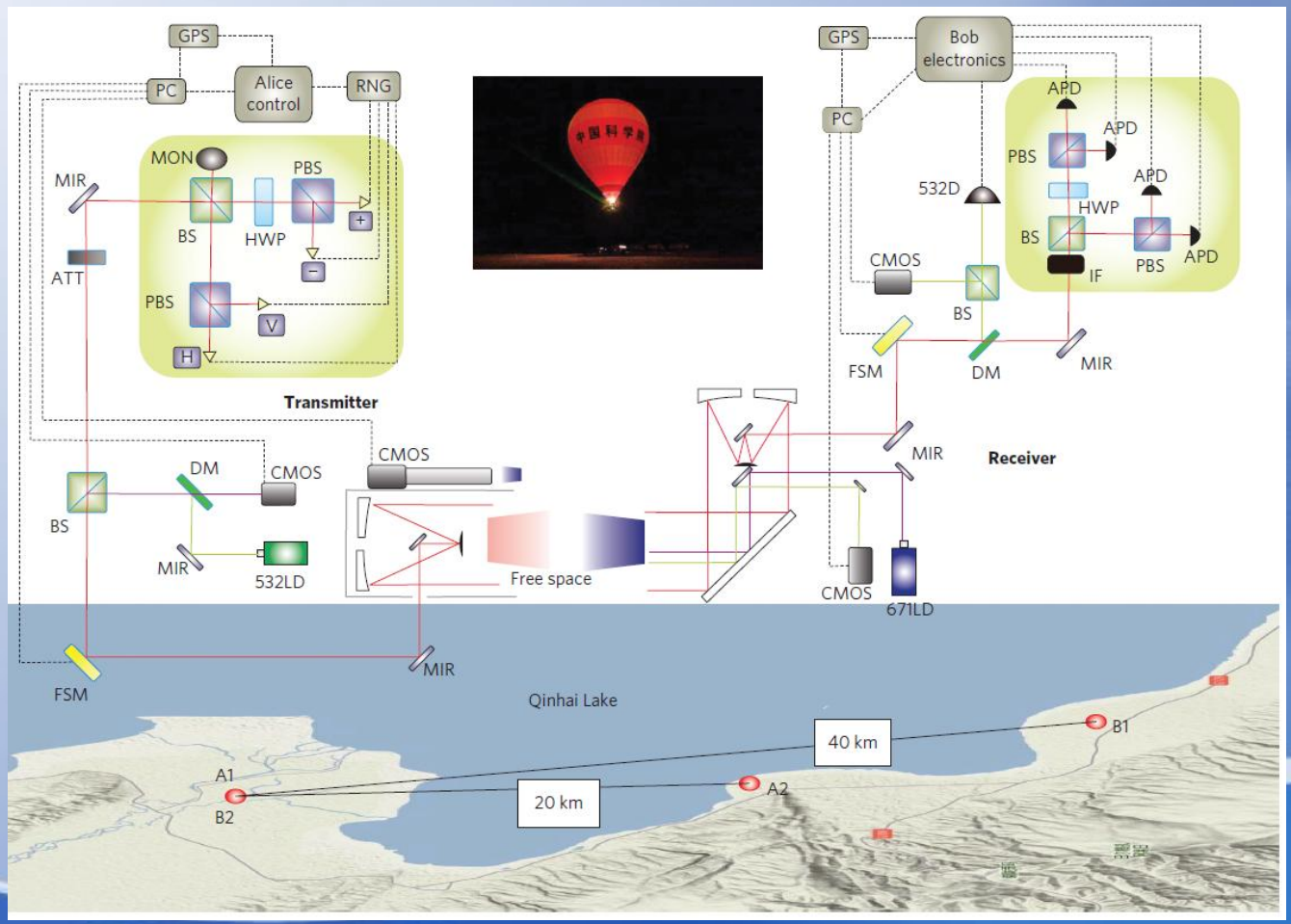
nature photonics

ARTICLES

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

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

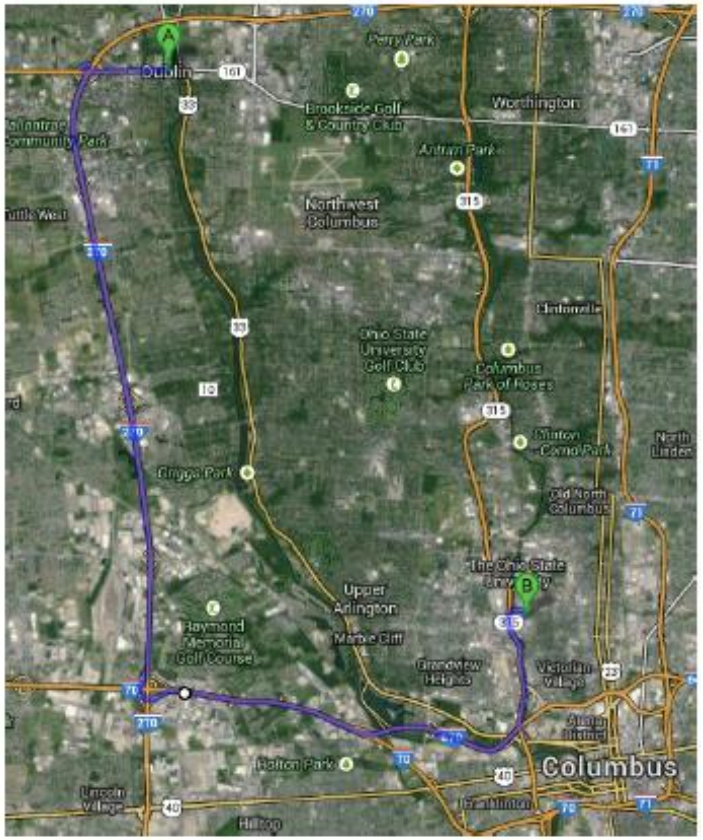
Jian-Yu Wang[1,2†], Bin Yang[1†], Sheng-Kai Liao[1,2], Liang Zhang[2], Qi Shen[1], Xiao-Fang Hu[1], Jin-Cai Wu[2], Shi-Ji Yang[2], Hao Jiang[2], Yan-Lin Tang[1], Bo Zhong[3], Hao Liang[1], Wei-Yue Liu[3], Yi-Hua Hu[2], Yong-Mei Huang[4], Bo Qi[4], Ji-Gang Ren[1], Ge-Sheng Pan[1], Juan Yin[1], Jian-Jun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



Enterprise: Corporate Data & IP

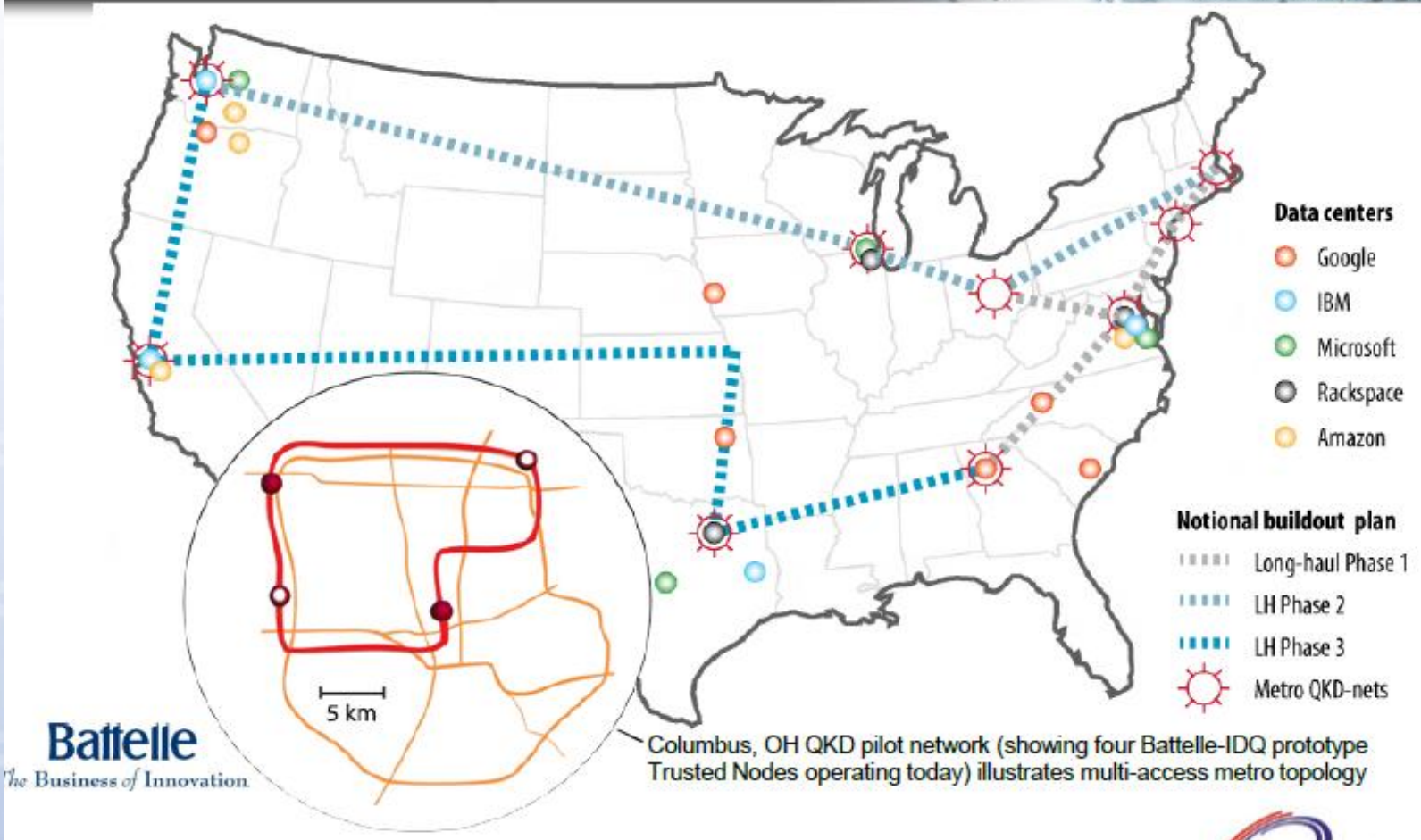
Battelle
The Business of Innovation

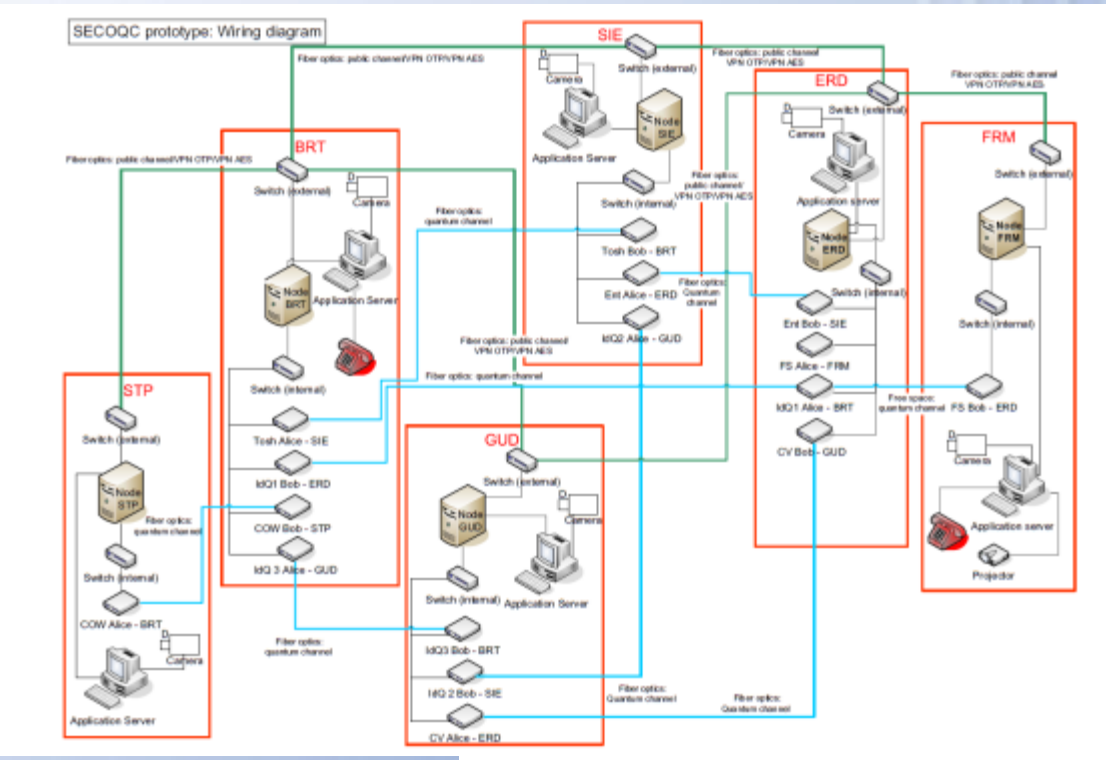
- Battelle USA
  - World's largest nonprofit R&D organization
  - Over 22,000 employees at more than 130 locations globally
- Requirement to protect mission critical corporate, financial information & intellectual property (designs, drawings, etc)
- IDQ's quantum cryptography used to secure critical 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

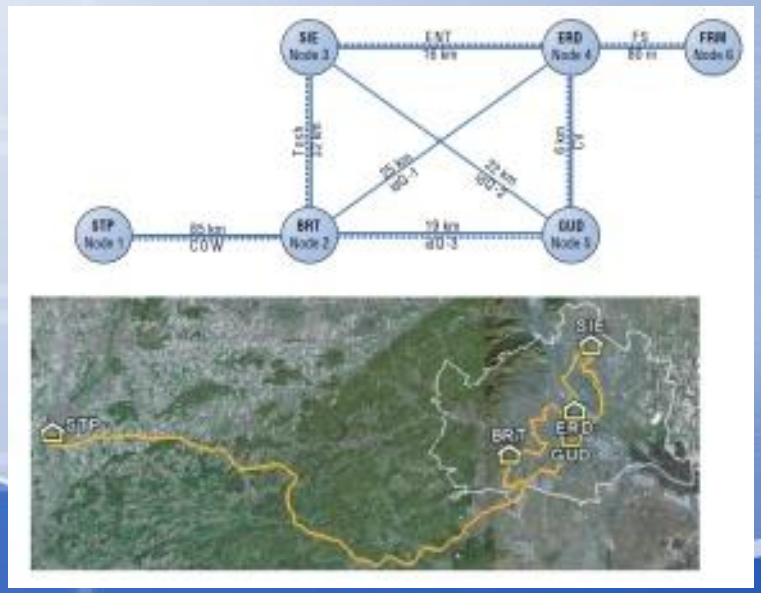


IDQ
FROM VISION TO TECHNOLOGY

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







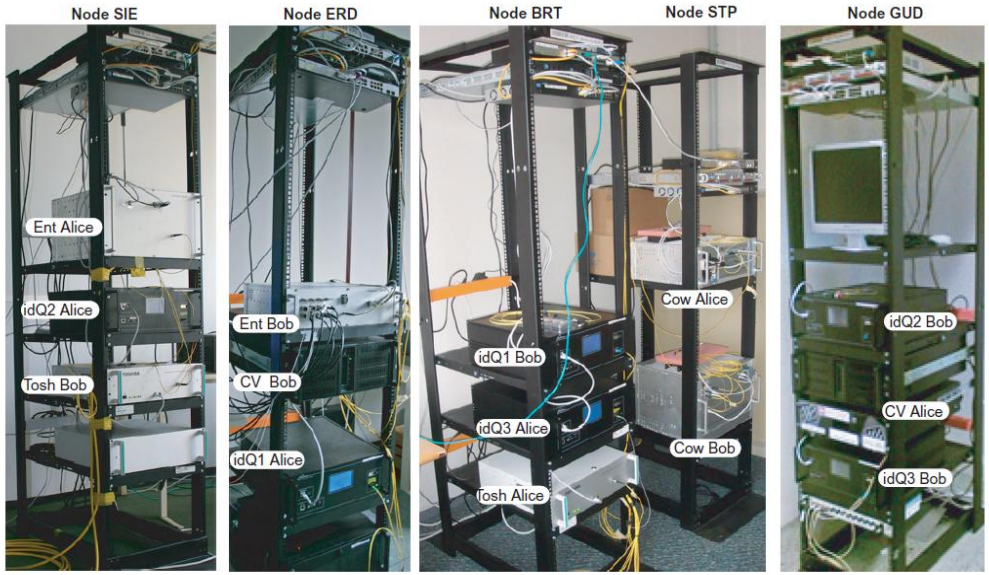


Figure 5. Photographs of the SECOQC network node racks.

Tokyo QKD Network

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

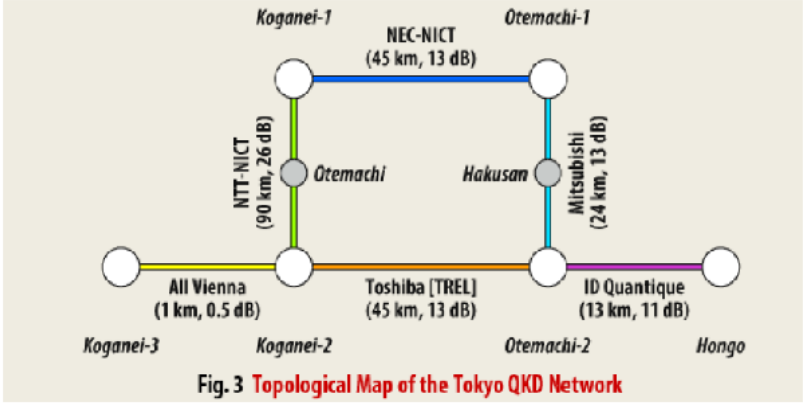


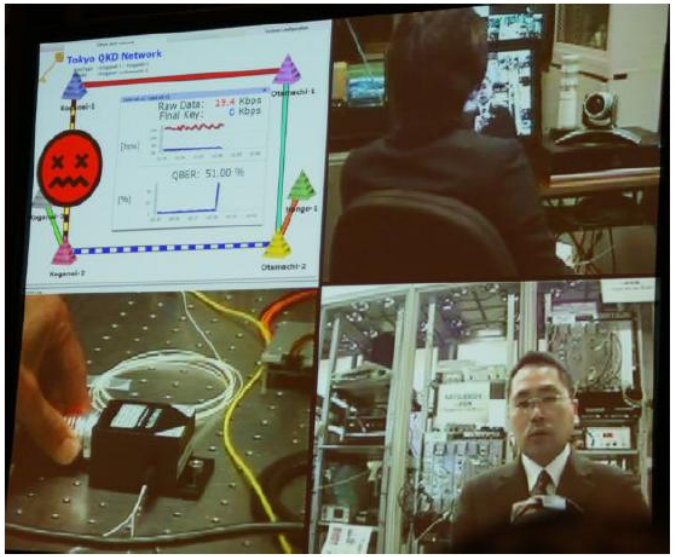
Fig. 3 Topological Map of the Tokyo QKD Network

Network Layout

- Make use of JGN2plus
- Star network

Fig. 1 Network Layout of the Tokyo QKD Network

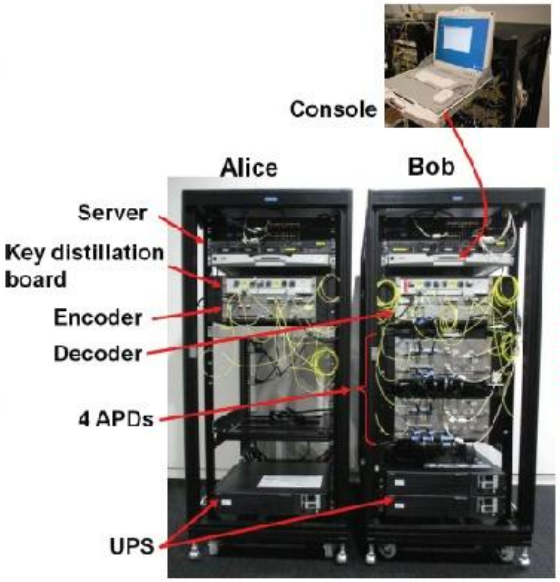
Secure Video Conference

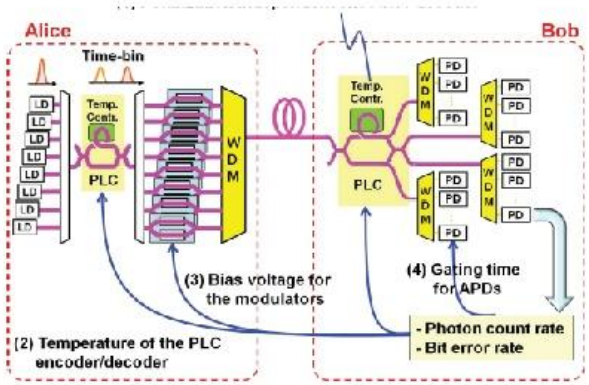


Alice


NICT

Bob


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


Alice
Bob
Time-bin
LD
Temp. Contr.
PLC
WDM
PD
(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

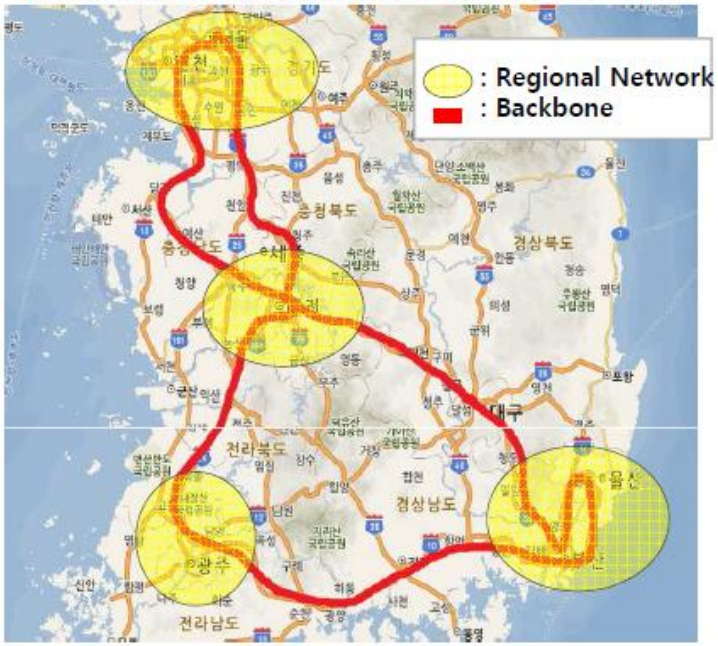
[Quantum R&D Testbed(~'15)]

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

[Quantum Backbone(~'17)]

- Seoul-Southern Gyeonggi-Sejong-Daejeon

[National Administrative Network ~'20)]



- Tentative the number of nodes

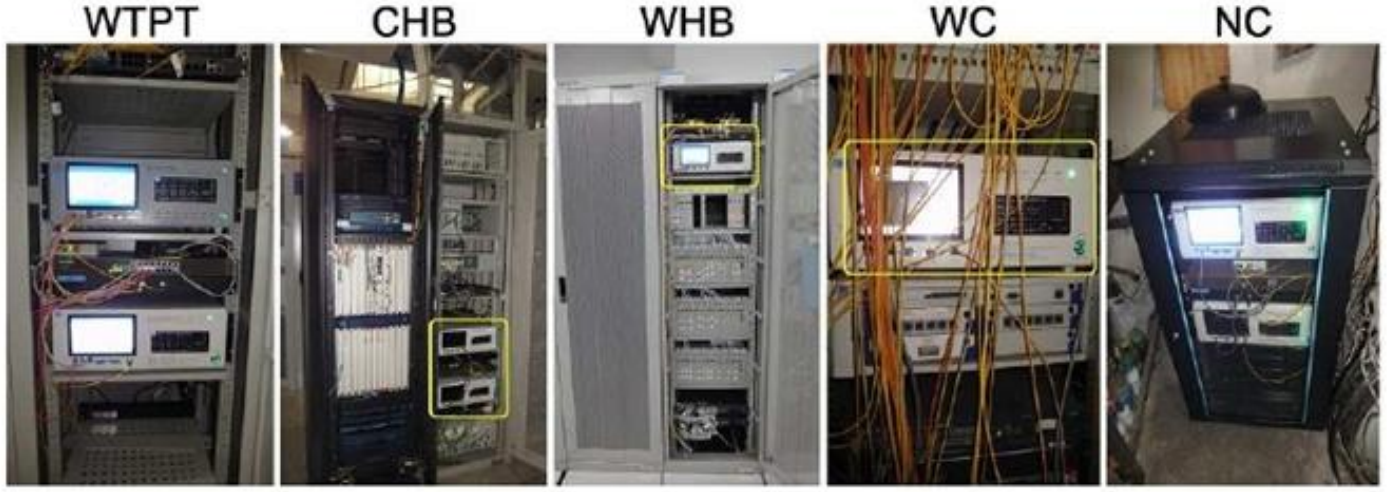
Category	# of node	비고
Public Administration	347	National wide office
Prosecutor & Police Office	2,264	National wide office
Post Office	3,562	National wide office

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

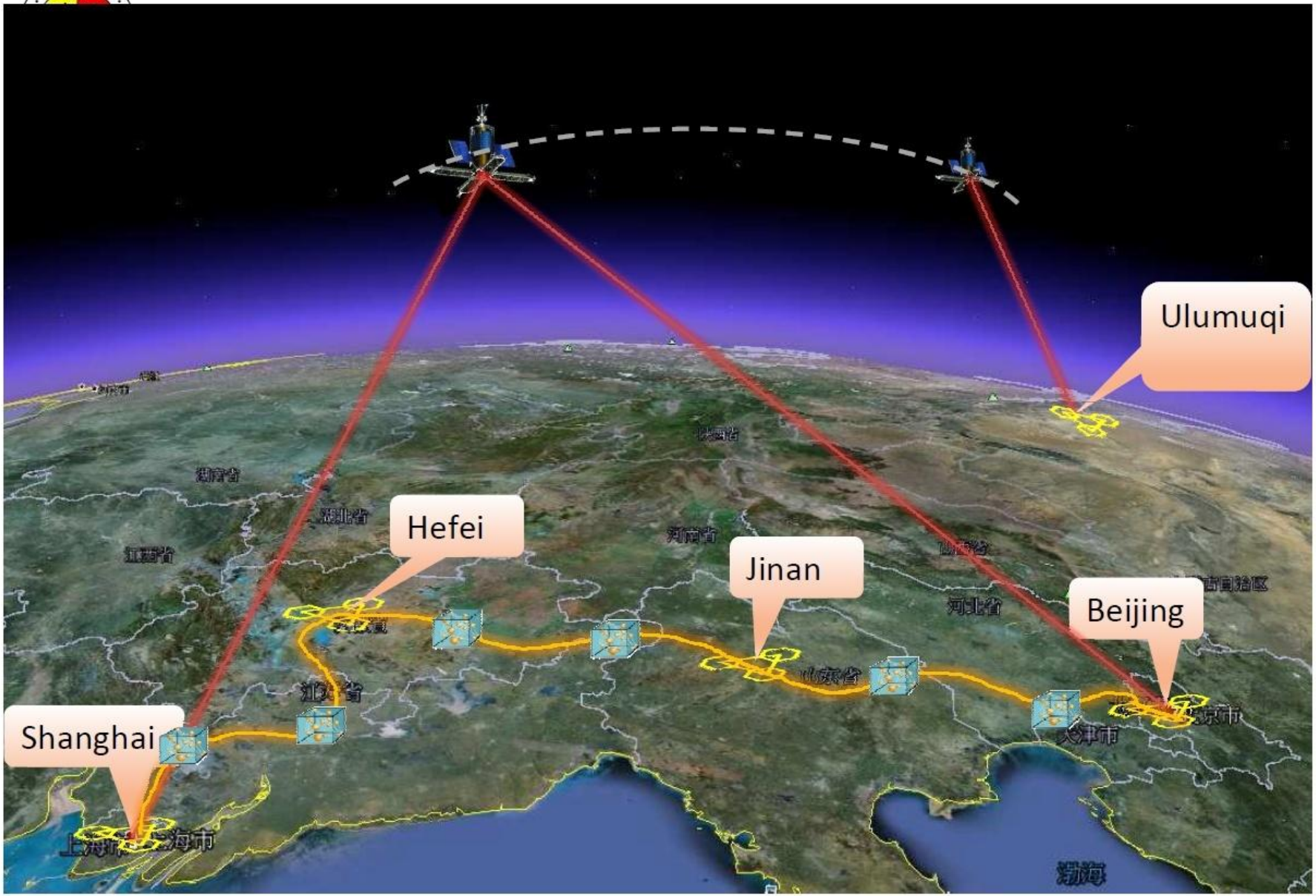
Chinese Trusted node Quantum network

- 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.

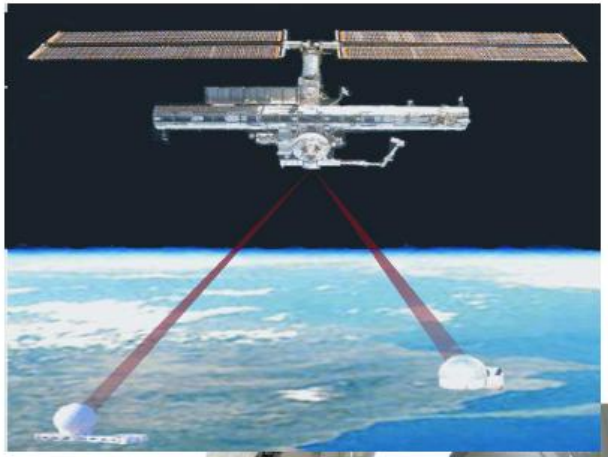


Chinese Trusted node Quantum network



Proposals for quantum communication in space

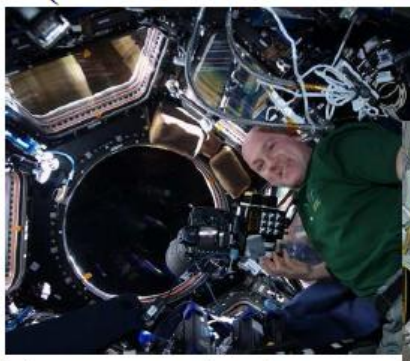
Dual-downlink
(ROM R&D 47 M€)

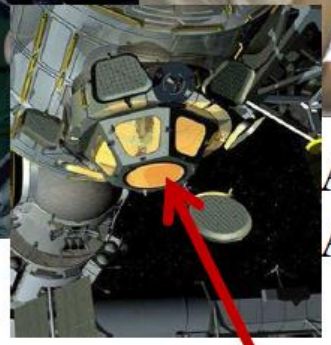


Simultaneous optical downlink: 1400 km separation.

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

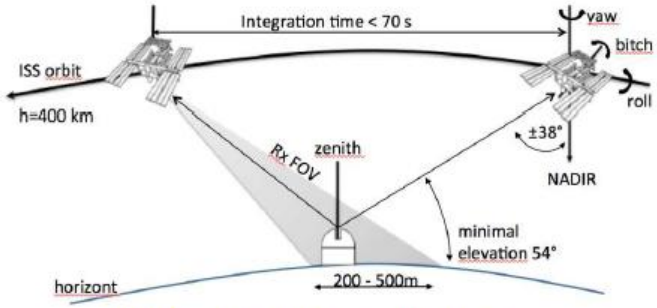
Single-uplink
(ROM R&D 1 M€)





Astronaut: A. Kuipers

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

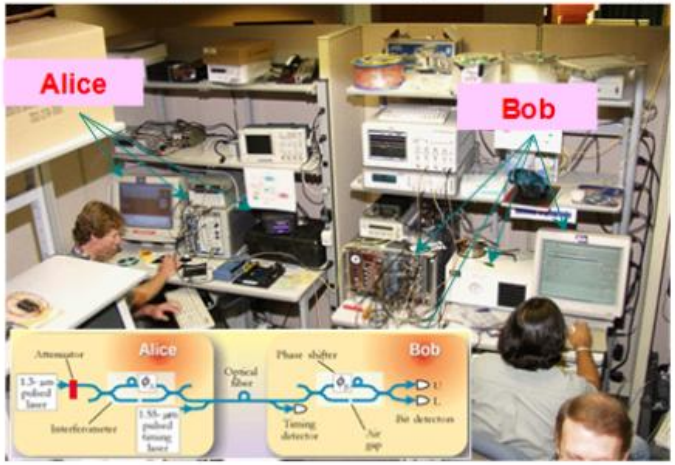


T. Scheidl, E. Wille, and R. Ursin, New Journal of Physics, 15, 043008 (2013)

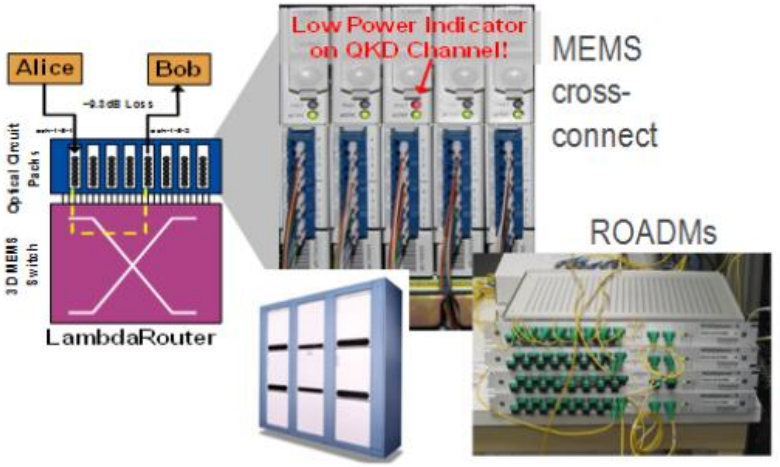
Rupert.Ursin@oeaw.ac.at - Institute for Quantum Optics and Quantum Information, Austrian Academy of Sciences

Telcordia Experience: Quantum Networks

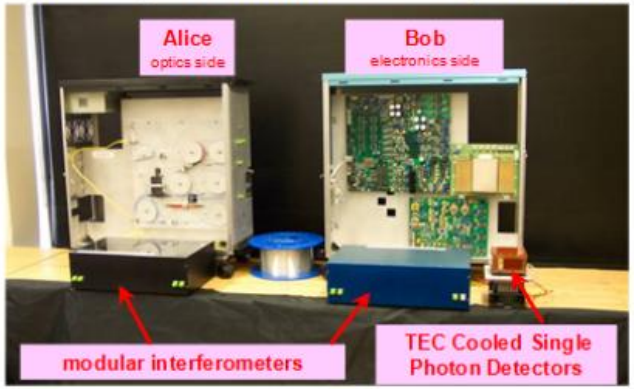
LANL 2nd generation fiber QKD system (F2)



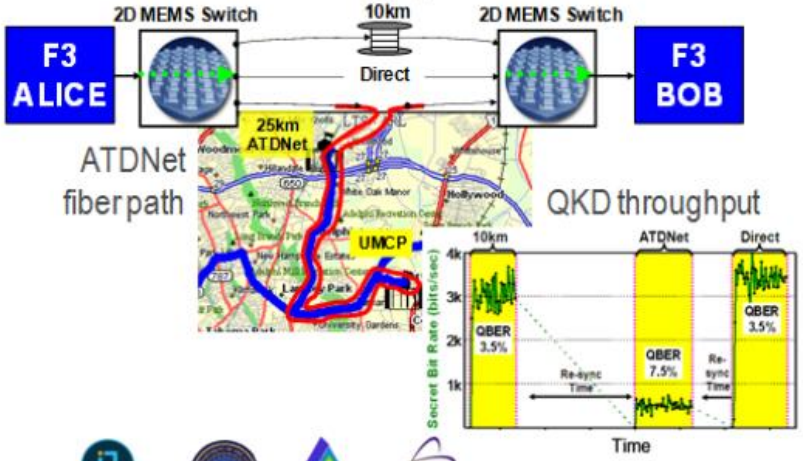
QKD Transmission through all-optical switches



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 LTS Los Alamos NATIONAL LABORATORY Telcordia

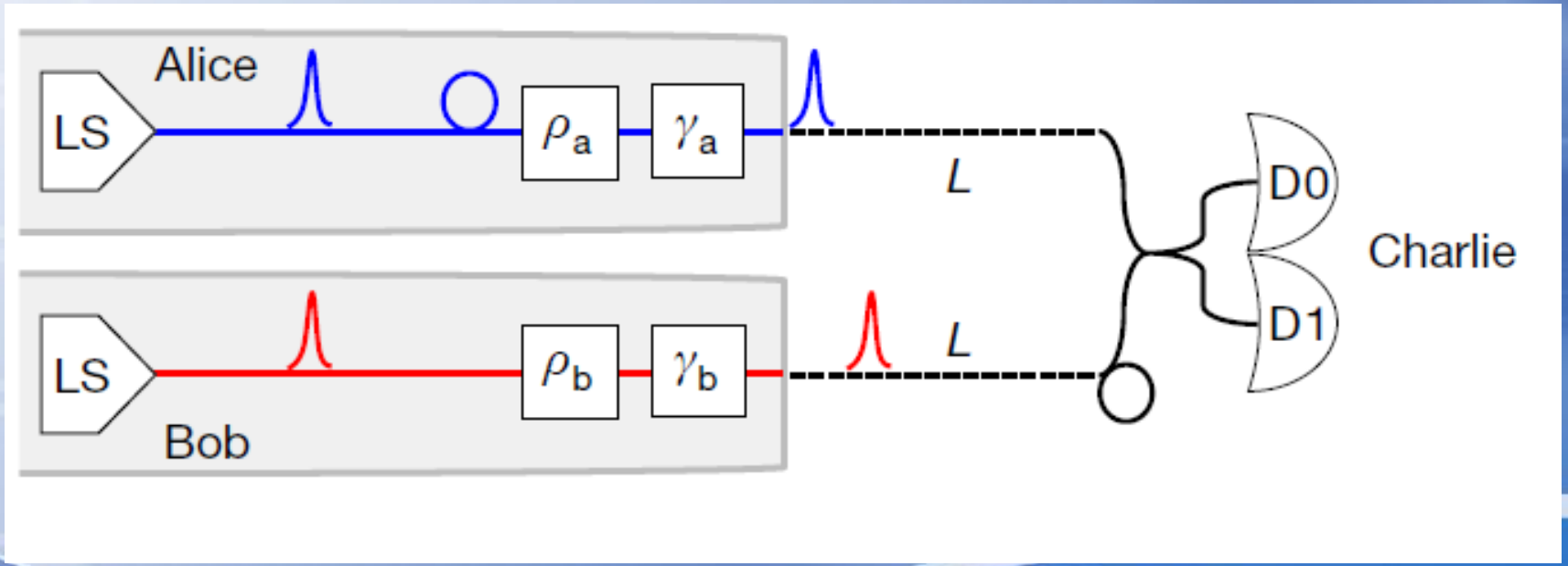
Передача ключей через НЕДОВЕРЕННЫЕ узлы

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

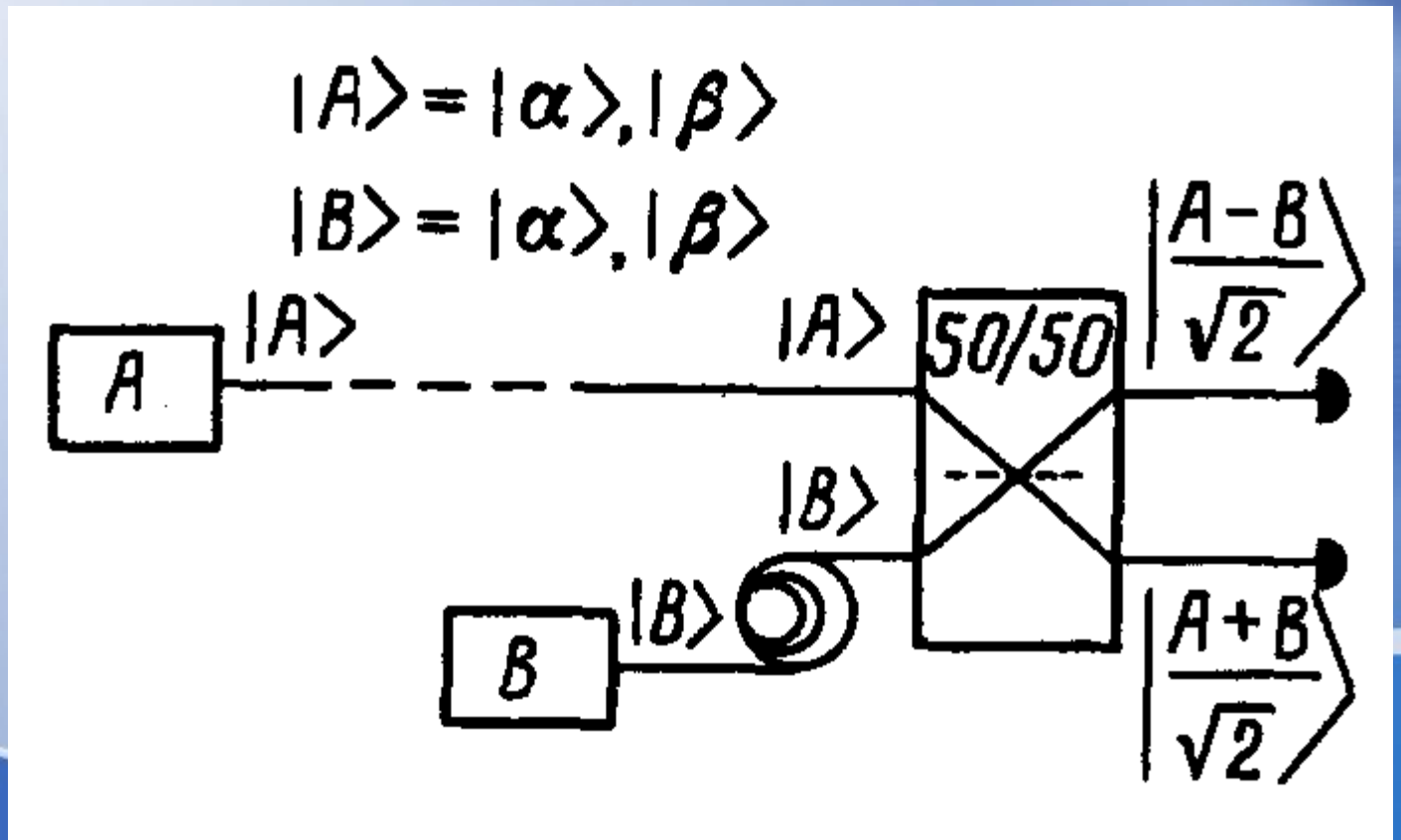
КВАНТОВАЯ КРИПТОГРАФИЯ НА КОГЕРЕНТНЫХ СОСТОЯНИЯХ НА ОСНОВЕ КВАНТОВОГО КОМПАРАТОРА

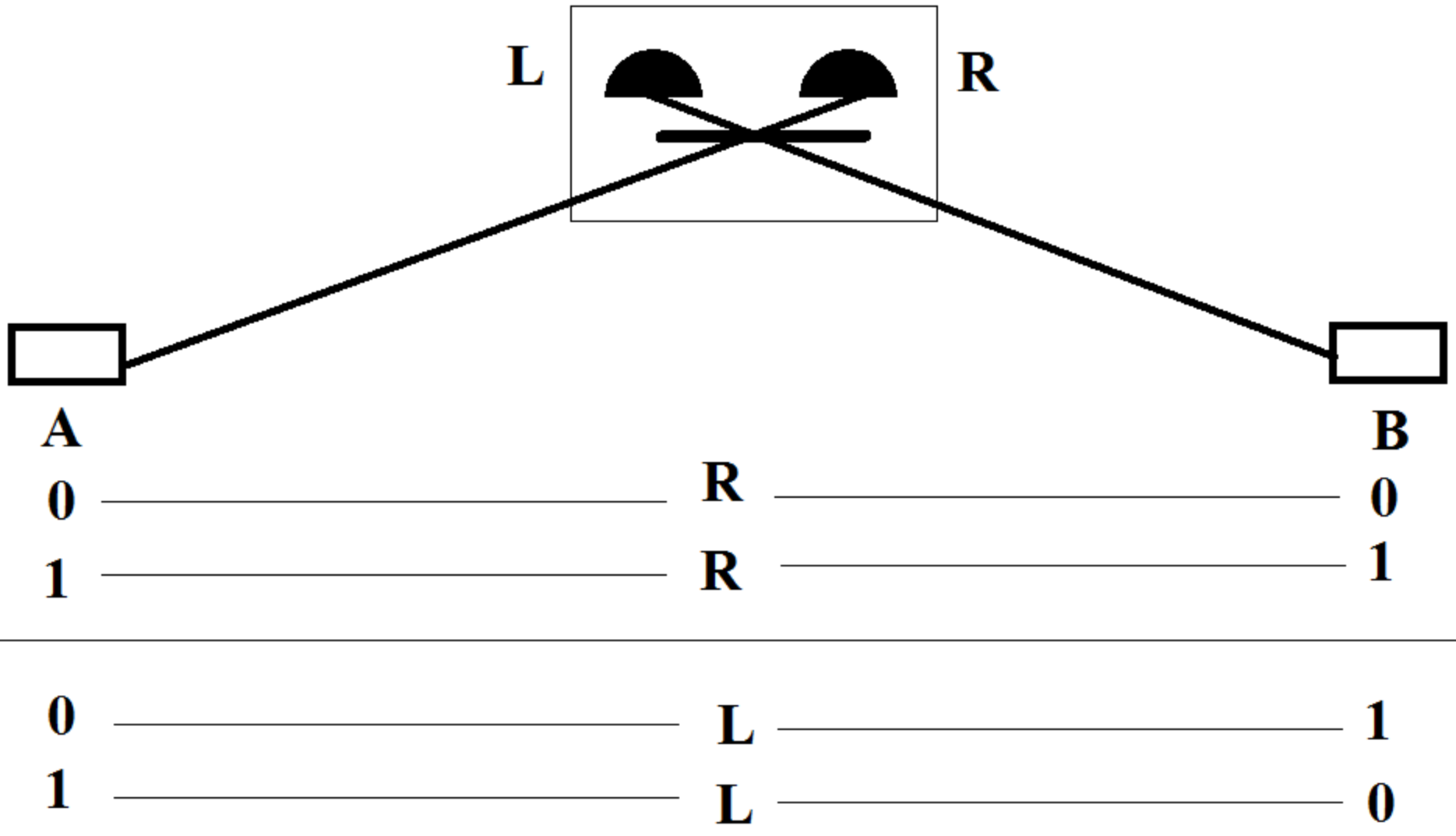
С.Н.Молотков

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

СПАСИБО ЗА ВНИМАНИЕ.