Квантовая криптография

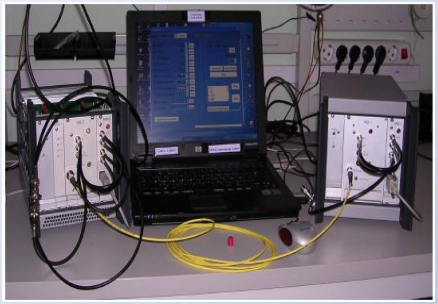
С.Н.Молотков

Кафедра суперкомпьютеров и квантовой информатики

ВМК, МГУ имени М.В.Ломоносова,

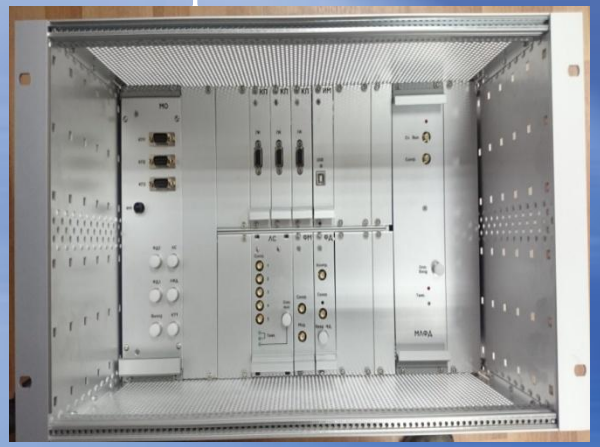
LOGO

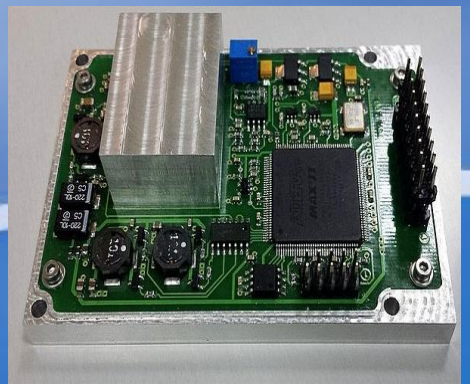
Лаборатория волоконной квантовой криптографии



Направления исследований:

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





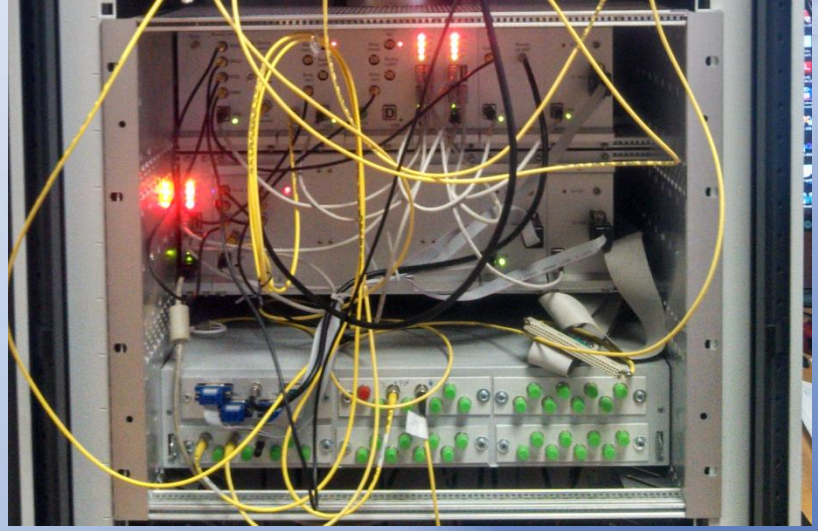
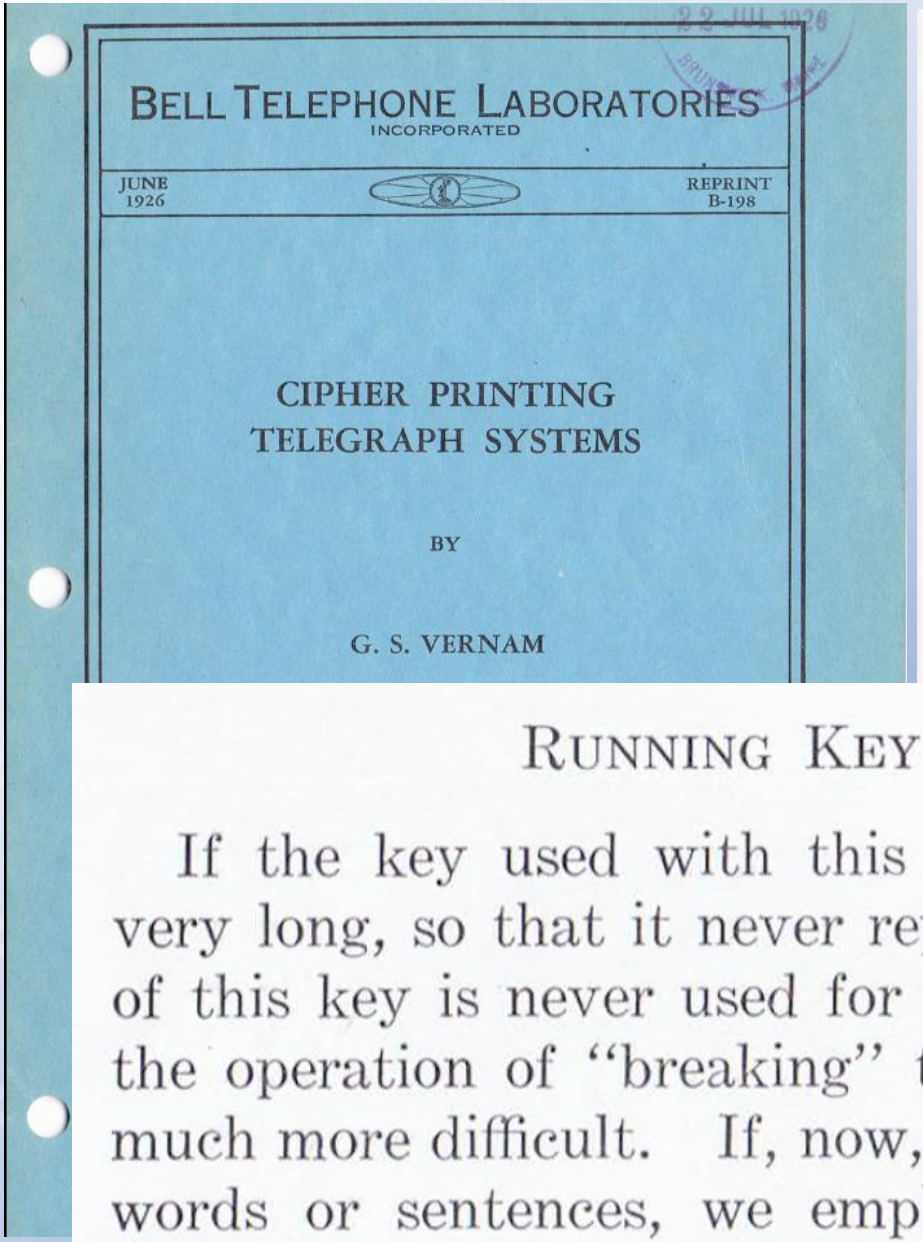



Схема сети квантового распределения ключей



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.

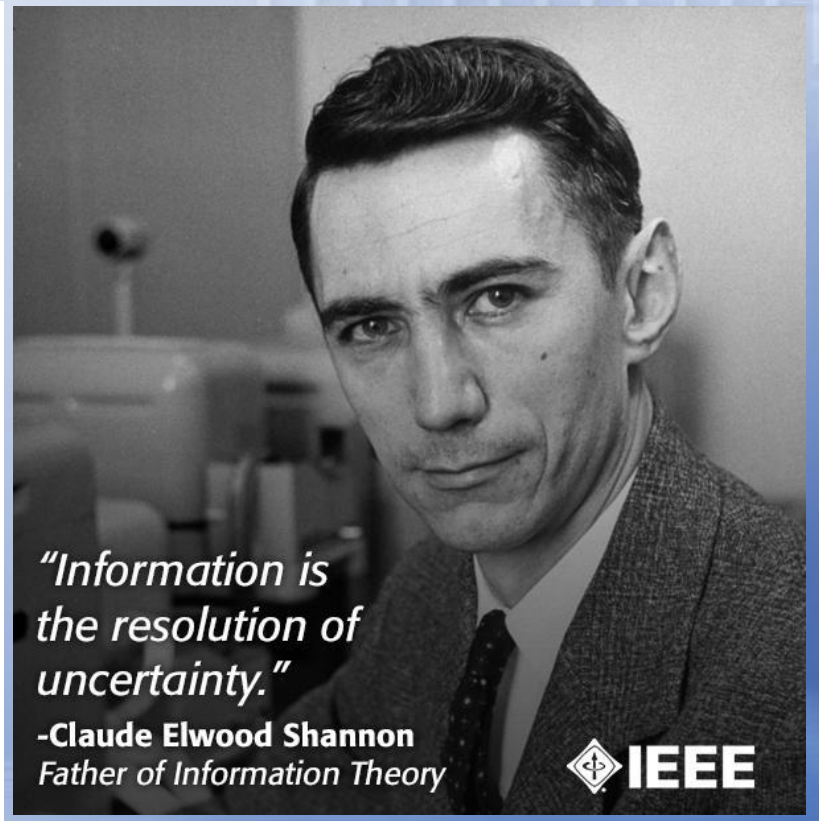
Communication Theory of Secrecy Systems*

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."

Секретный ключ

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

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

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

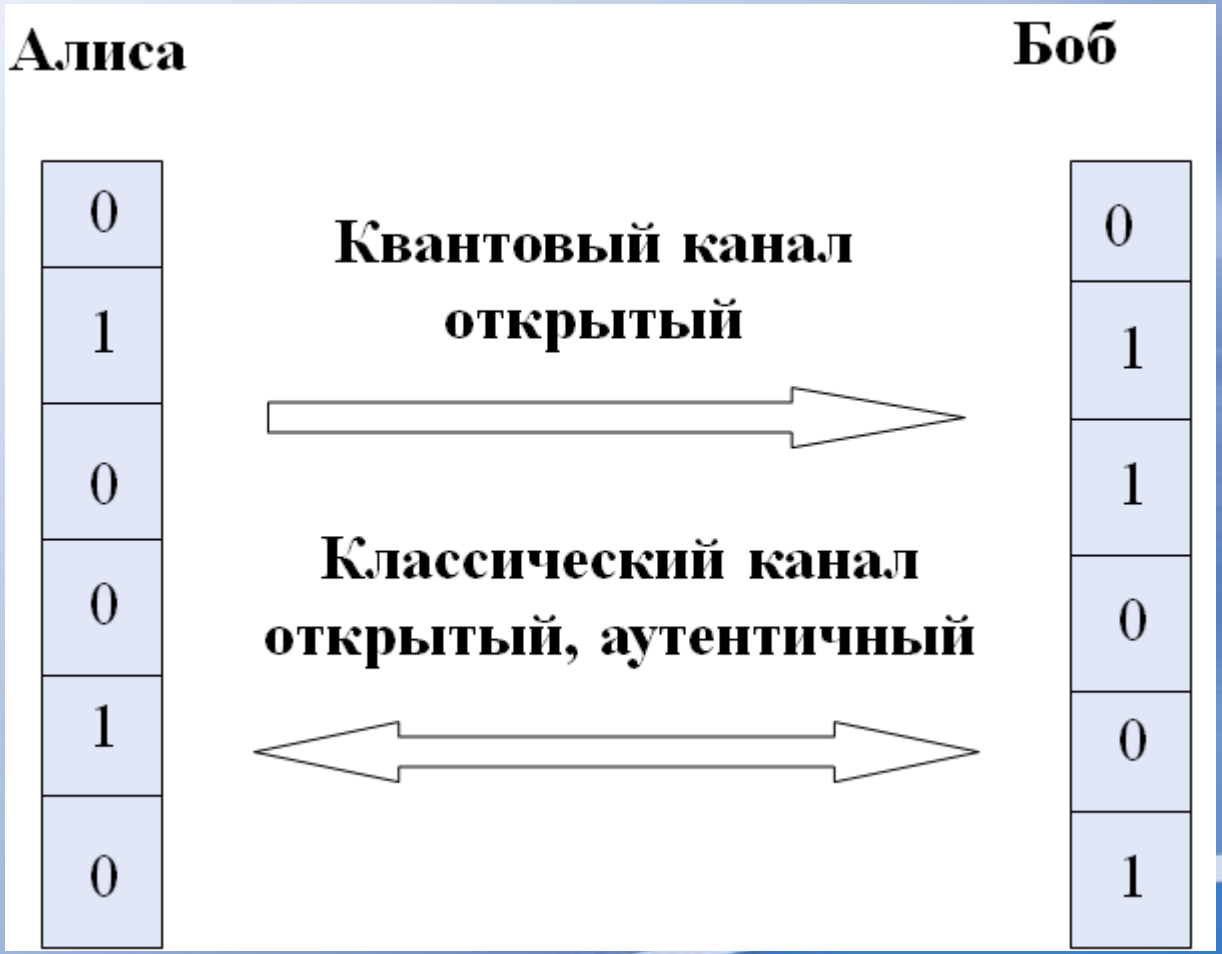
$$I(M;C) = H(C) - H(C|M) = 0$$

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

$$c = m \oplus k$$

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

Квантовая криптография = Квантовое распределение ключей = Согласование случайных последовательностей



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)

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.

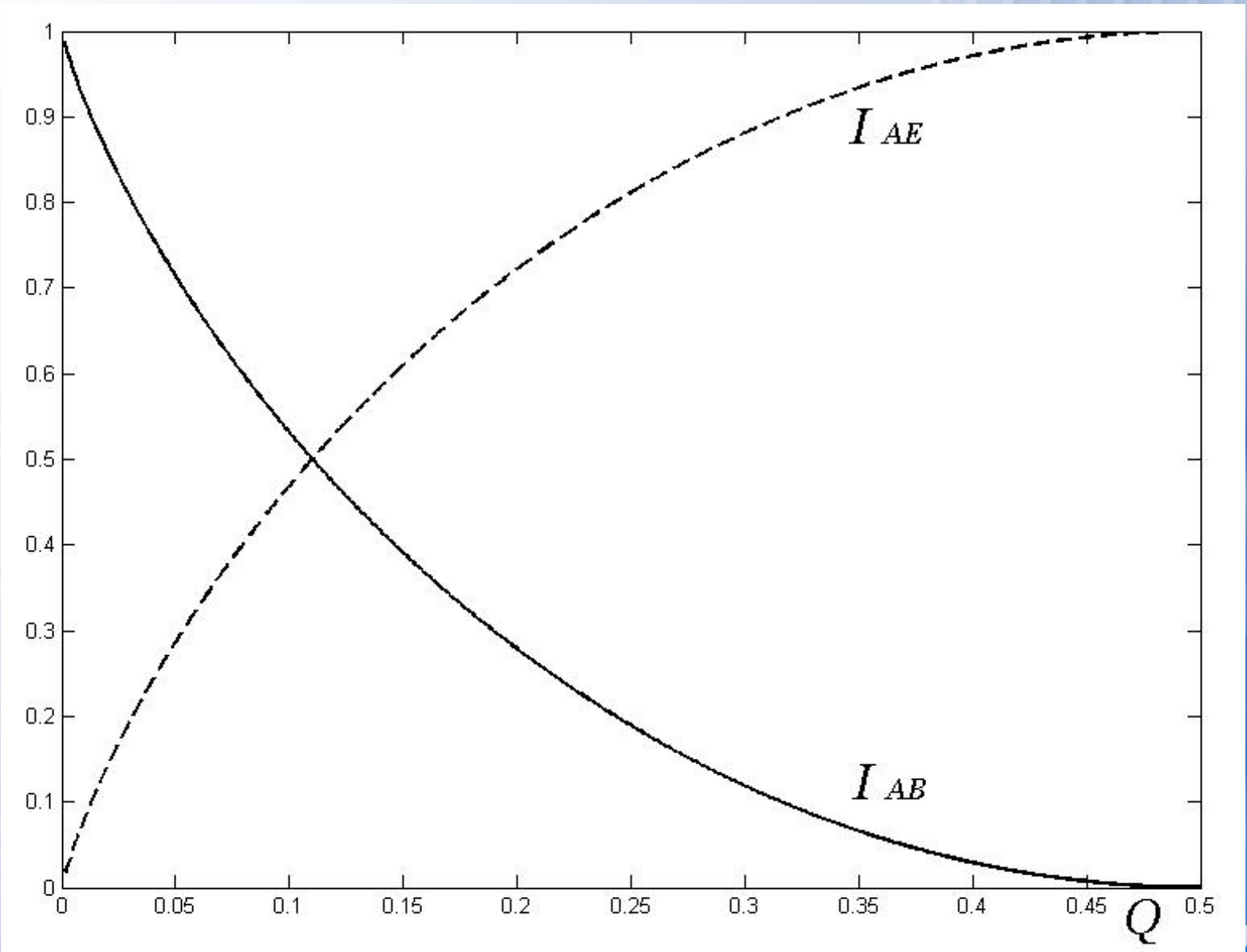
4) Сжатие очищенных ключей – усиление секретности универсальными хеш-функциями.

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.**


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

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.

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)

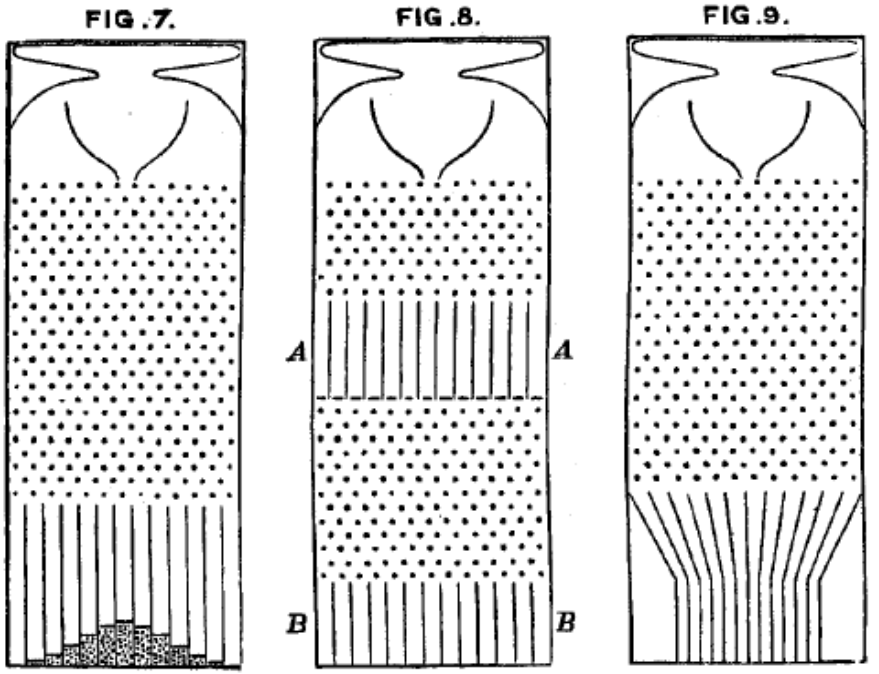
NATURAL INHERITANCE

BY

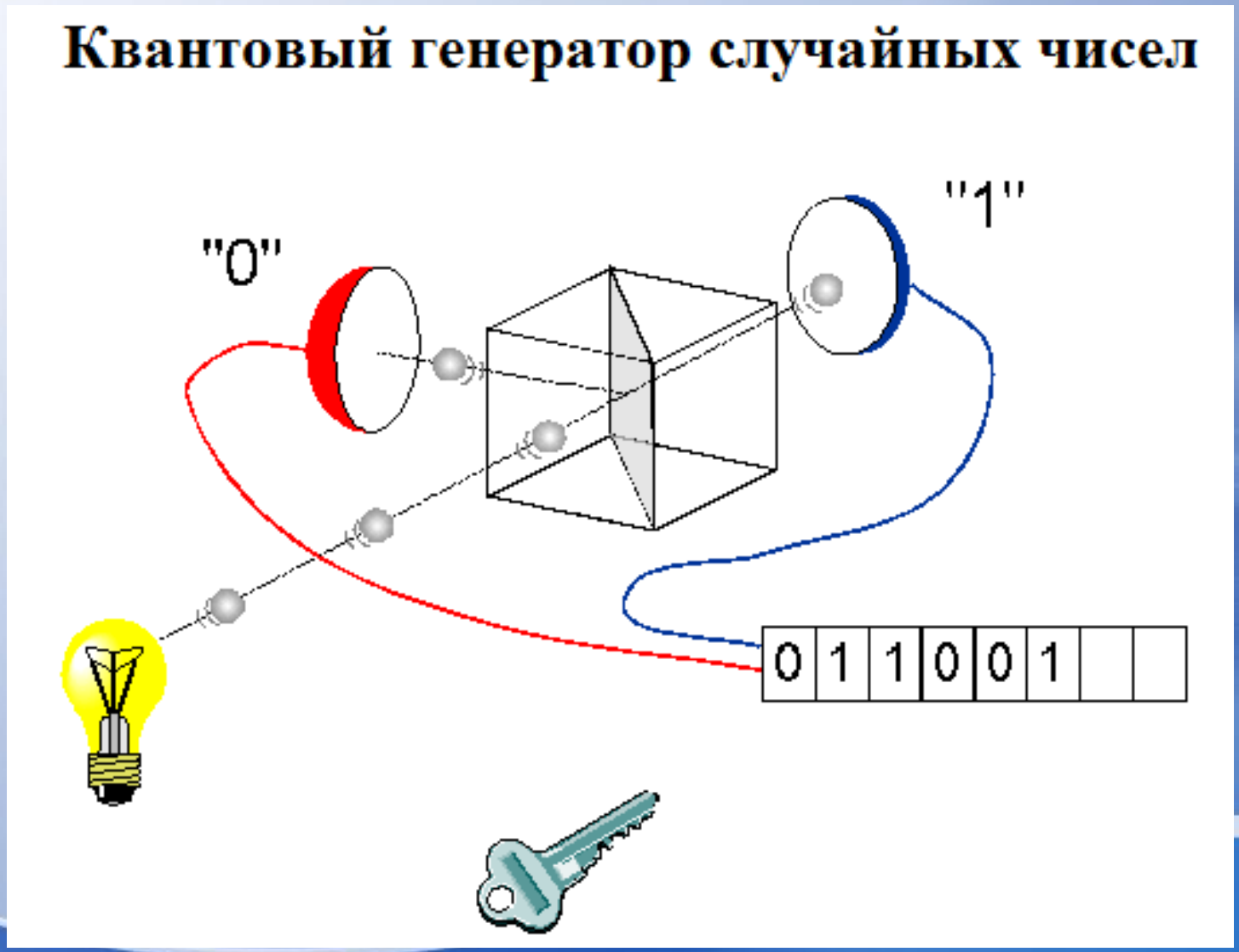
FRANCIS GALTON, F.R.S.

AUTHOR OF

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



Необходимость квантового генератора случайных чисел.



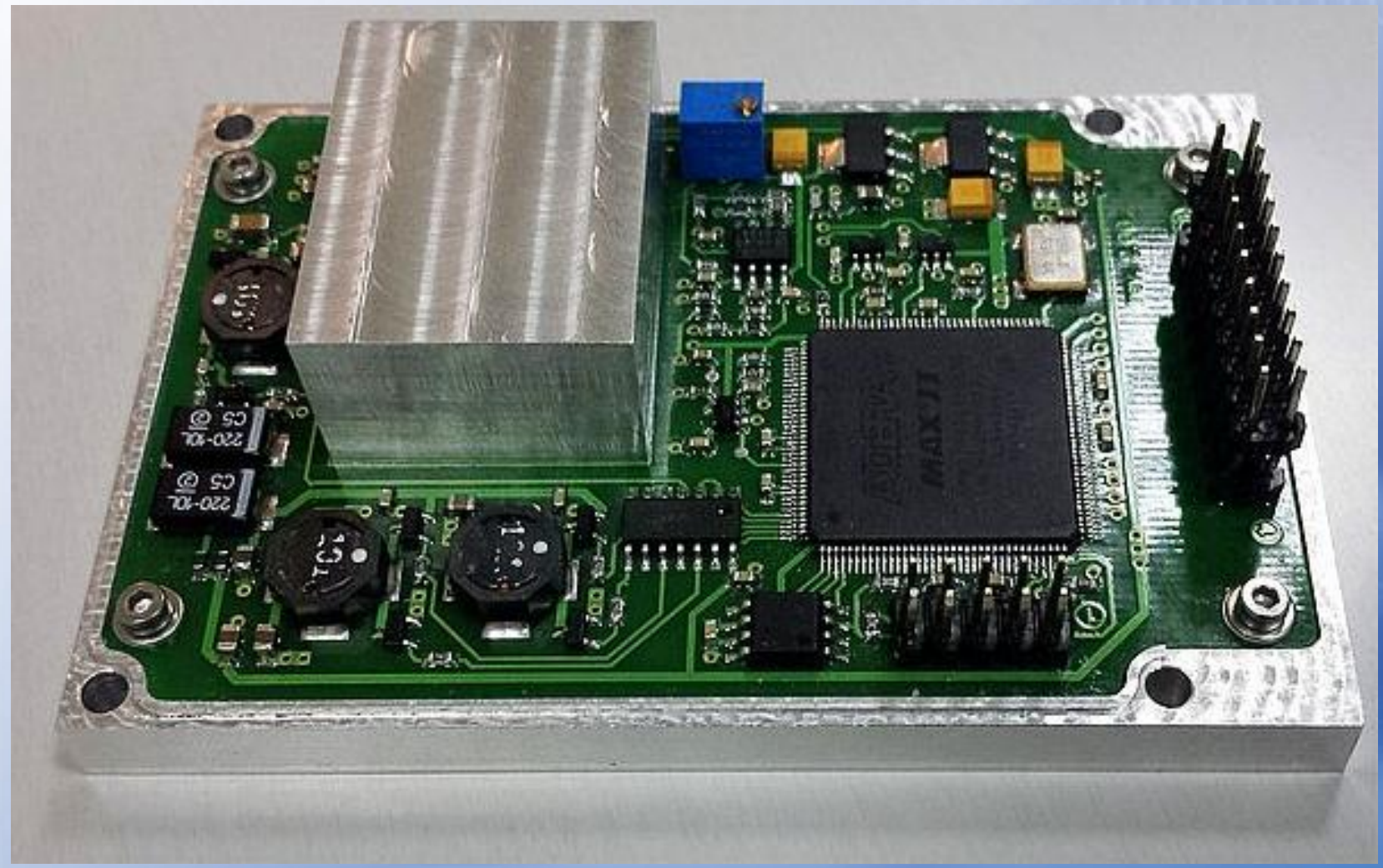

S = k log W
LVDWIG
BOLTZMANN
HENRIETTE
BOLTZMANN
BOLTZMANN
BOLTZMANN

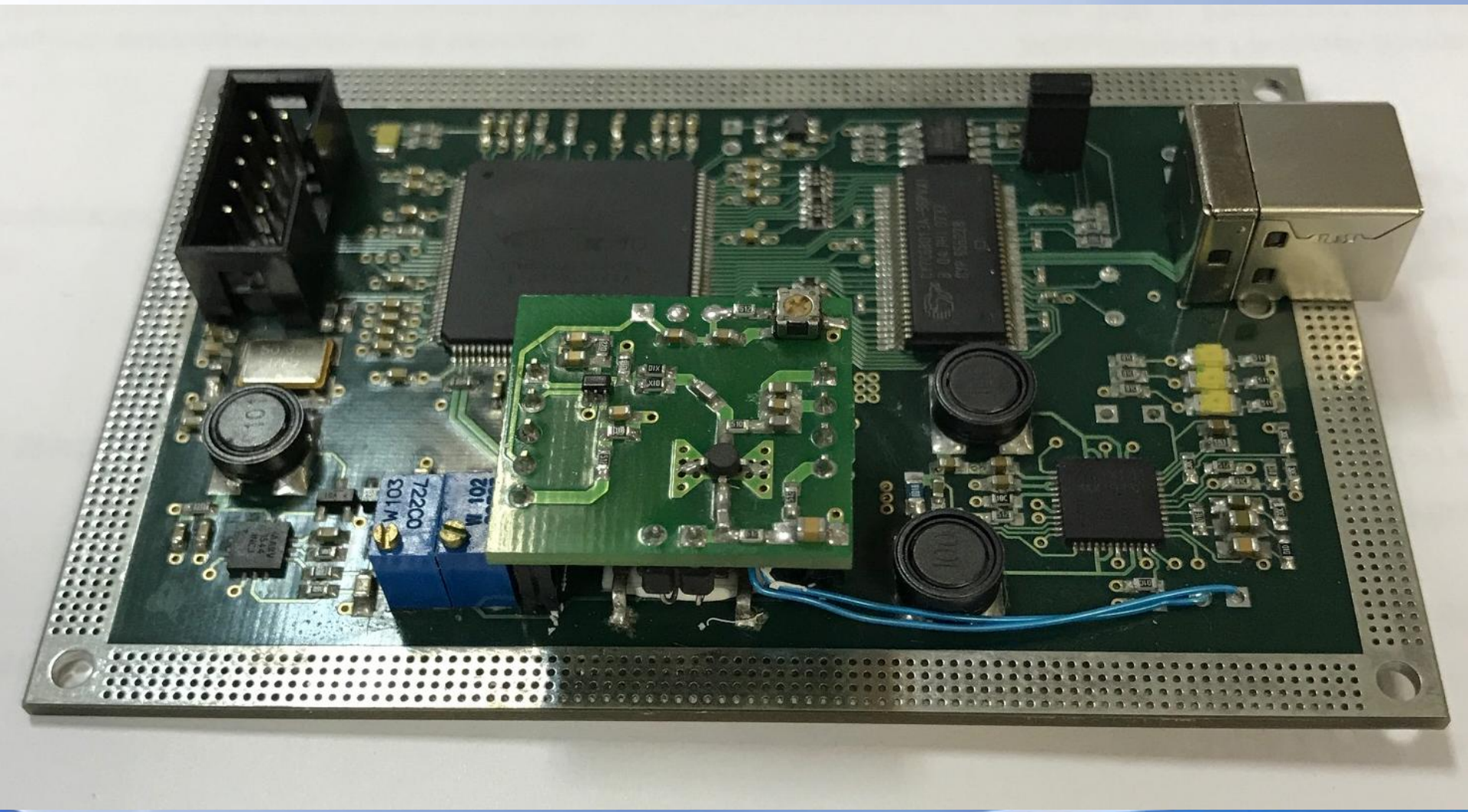
«Эта формула сохранит свою силу даже тогда, когда все памятники будут погребены под мусором тысячелетий».

При жизни Больцмана молекулярно-кинетическая теория газов встретила ожесточённую критику. Больцман понимал, что его труды почти никем не поняты. О некоторых работах он мог, по словам самого учёного, говорить только с Гельмгольцем, но тот был далеко от Вены — в Берлине.

Криптография,
Случайность,
Фотоэффект,
Когерентное состояние,
Статистический вес,
Статистика Пуассона,
Статистика Ферми-Дирака,
Энтропия Больцмана,
Энтропия Шеннона,
Метод фон Неймана,
Квантовые генераторы случайных чисел,
Арифметическое кодирование,
Треугольник Паскаля, числа Фибоначчи,
Тесты на случайность.

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.


220-10L
C5
220-10L
C5

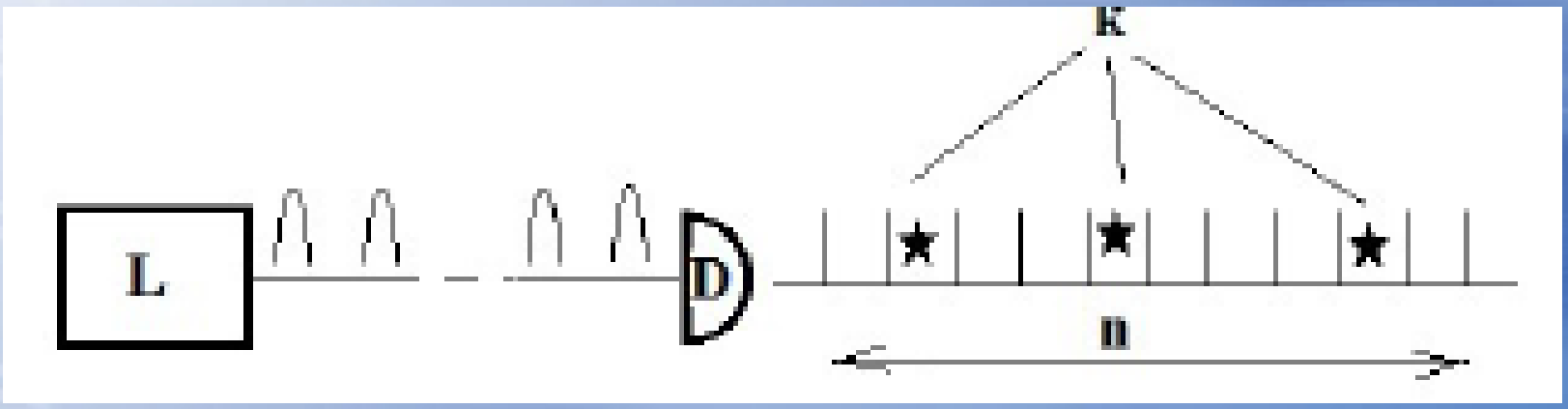

W103
72200
W102

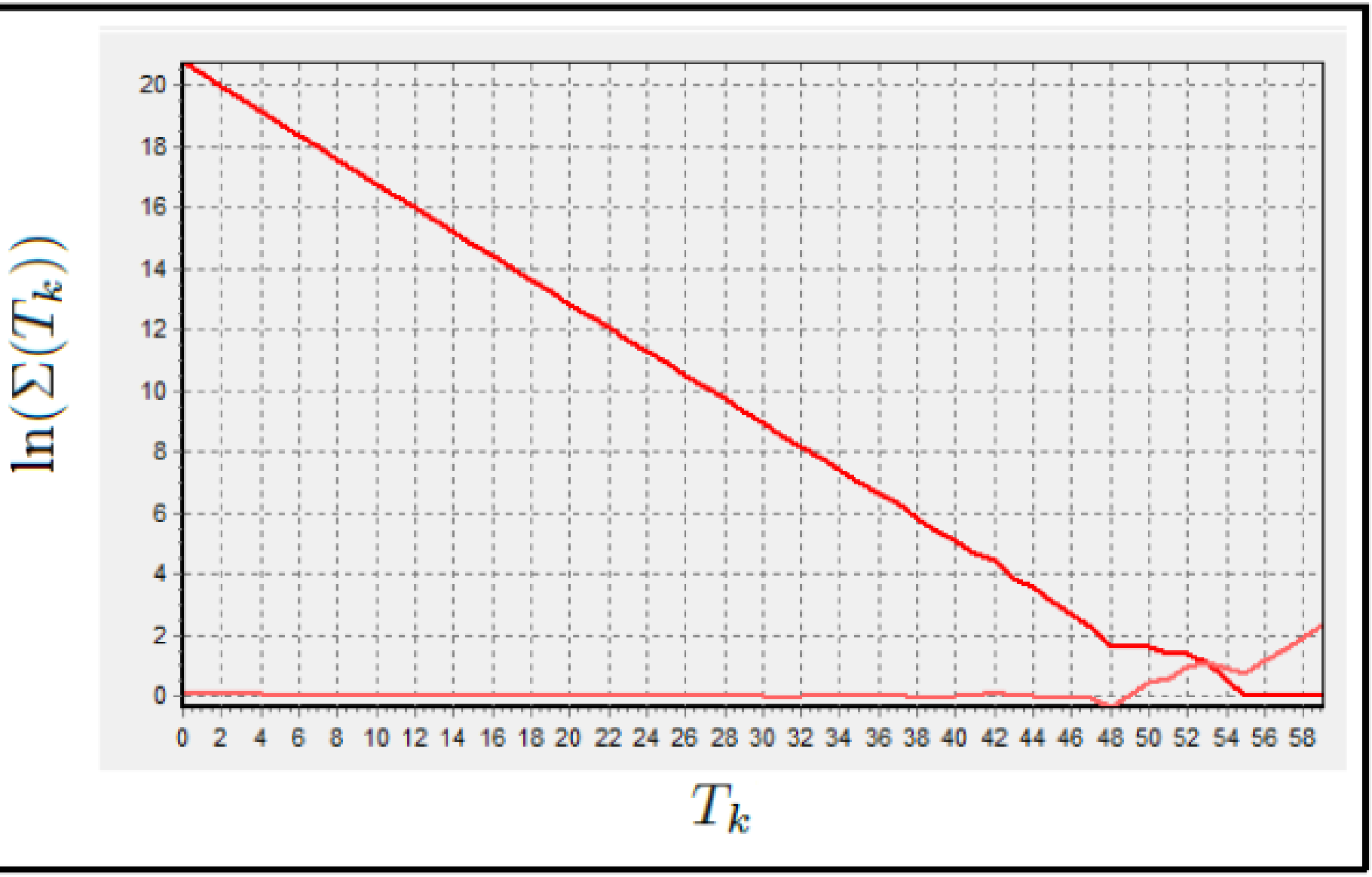
Фотоэффект, Когерентное состояние, Статистика Пуассона

$$P_T(m) = e^{-\mu T} \frac{(\mu T)^m}{m!}.$$

$$P(*) = 1 - e^{-\mu}$$

$$P(\sqcup) = e^{-\mu}$$

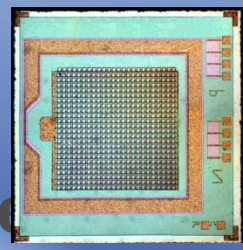



$\ln(\Sigma(T_k))$
20
18
16
14
12
10
8
6
4
2
0
0 2 4 6 8 10 12 14 16 18 20 22 24 26 28 30 32 34 36 38 40 42 44 46 48 50 52 54 56 58
T_k

How to achieve the experimentally ideal Poisson statistics of photocounts?

Use the smallest average number of photons in the quantum state –

$$\mu = P(*)/\eta N_{pic} \approx 2.94 \cdot 10^{-3}$$



Use specially designed SiPM instead single avalanche detector with “independents” pixels -- solves the problem of dead time and afterpulsing.

The probability of a photon getting into the same pixel is negligible (order 10^-6), which is several orders of magnitude less than for one detector.

SiPM is a physical heart of QRNG

Статистика Ферми-Дирака, Энтропия Больцмана, Энтропия Шеннона,

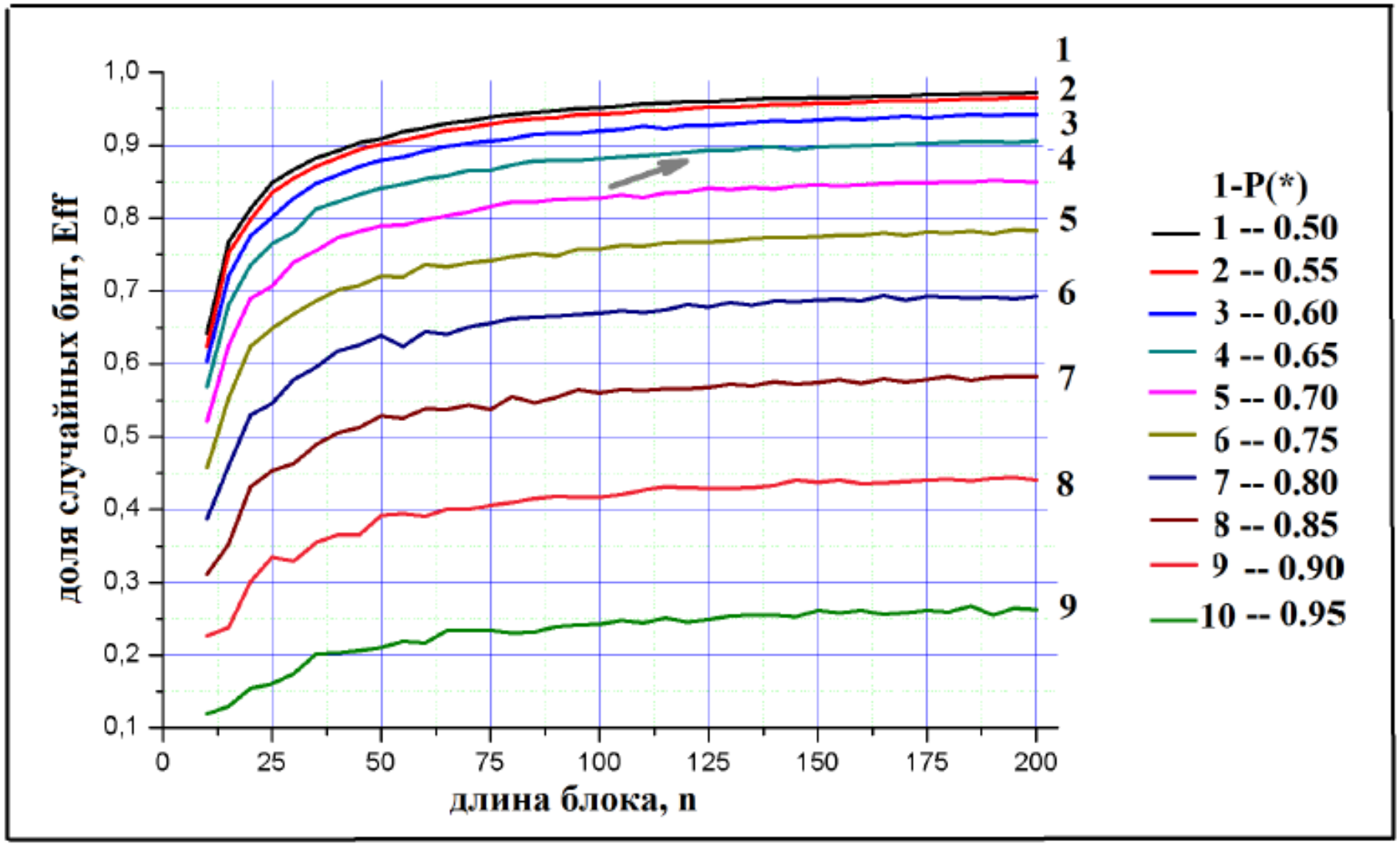
$$(1-p+p)^n = \sum_{k=0}^{n} C_n^k (1-p)^k p^{n-k}, \quad C_n^k = \frac{n!}{k!(n-k)!}.$$

$$P_n(k) = (1-p)^k p^{n-k}$$

$$\log(C_n^k)$$

$$H_n^{F-D}(p) = \sum_{k=0}^{n} P_n(k) C_n^k \log(C_n^k)$$

$$H_n^{Sh}(p) = -\sum_{k=0}^{n} C_n^k P_n(k) \log(P_n(k))$$


доля случайных бит, Eff
1,0
0,9
0,8
0,7
0,6
0,5
0,4
0,3
0,2
0,1
0
25
50
75
100
125
150
175
200
длина блока, n
1
2
3
4
5
6
7
8
9
1-P(*)
1 -- 0.50
2 -- 0.55
3 -- 0.60
4 -- 0.65
5 -- 0.70
6 -- 0.75
7 -- 0.80
8 -- 0.85
9 -- 0.90
10 -- 0.95

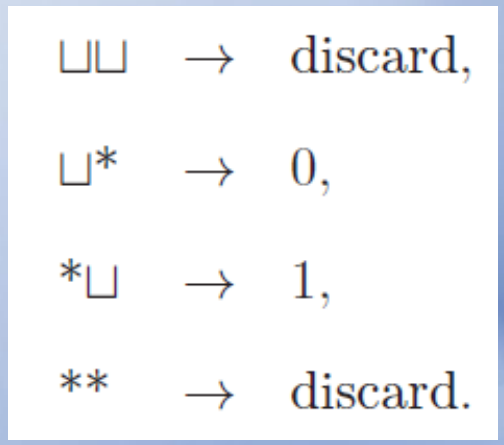
Various Techniques Used in Connection With Random Digits

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).

Enumeration of photocount sequences is “mathematical” heart of QRNG

Recall von Neumann method



von Neumann did not say these words, but the method in a hidden form contains something more important.

1) Divide all sequences of the same length into classes.

2) Each class includes equiprobable sequences - sequences with the same number of photocounts.

3) Enumerate all sequences in the class starting from zero.

4) Binary representation of the sequence number in the class is a random block 0 and 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 --

Разбиение на классы, число случайных бит в классе, как эффективно извлечь.

$$\log(C_n^k)$$

S=log(W), W –статистический вес

Логарифм от числа равновероятных состояний системы (статистического веса) есть число случайных бит.

Перенумеровать все равновероятные последовательности из данного класса.

Двоичное представление номера (грубо) есть случайный блок.

C_n^k – число способов разместить k частиц (*) по n ящикам (уровням), в каждом не более одной частицы – статистика Ферми-Дирака.

Логарифм от числа равновероятных состояний системы (статистического веса) есть число случайных бит.

Перенумеровать все равновероятные последовательности из данного класса.

Двоичное представление номера (грубо) есть случайный блок.

Арифметическое кодирование,
Треугольник Паскаля, числа Фибоначчи
64 такта

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

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

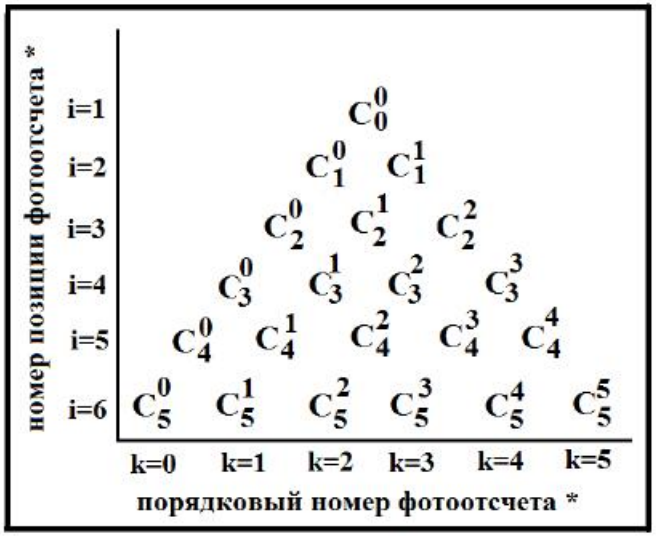
$10^{22} \rightarrow 10^{10}\ 10^{12}$

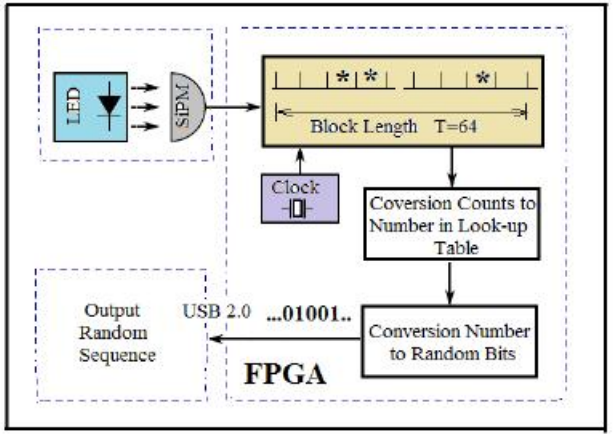
How to effectively enumerate?

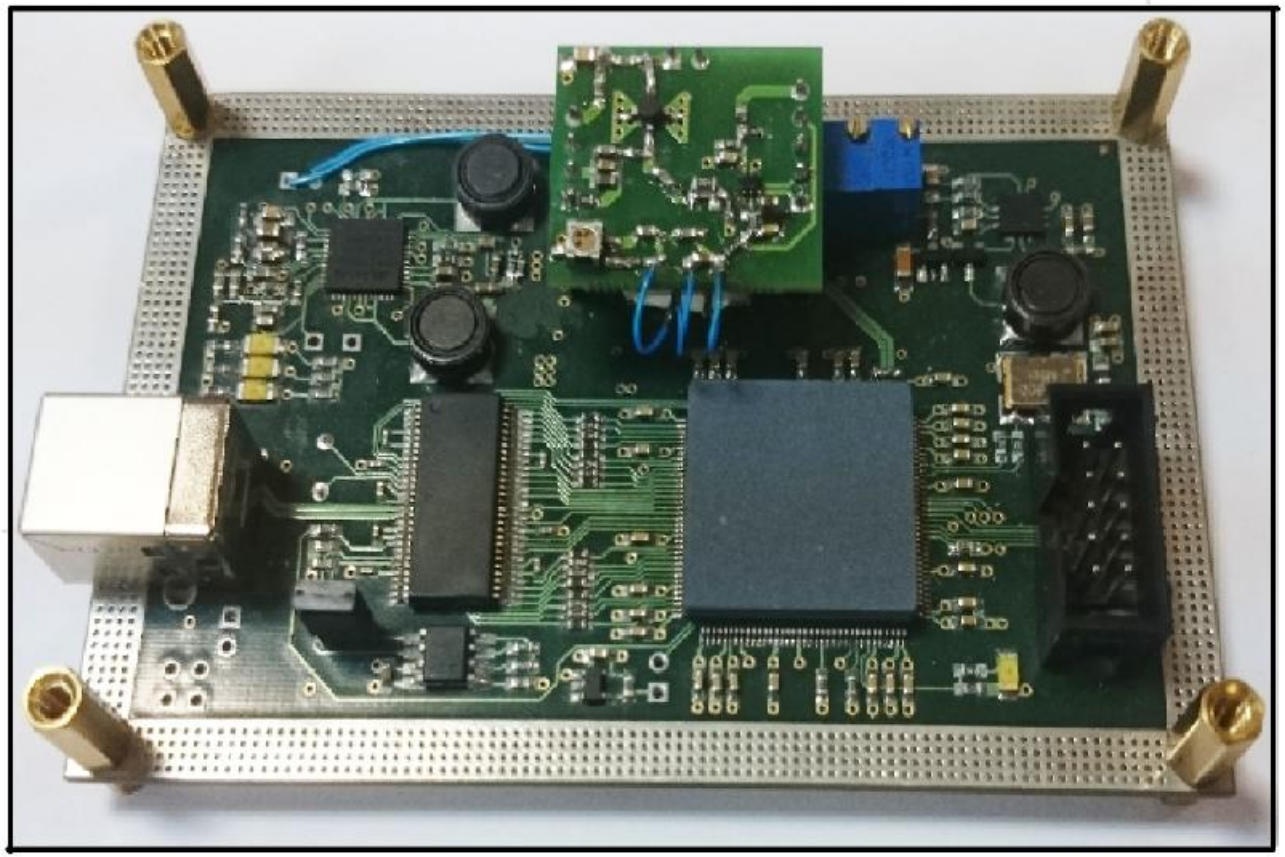
Use Pascal triangle and nice mapping between sequence of photocount $(i_1, i_2, \ldots, i_k)$ **and its number in class** $(0 \leq \mathrm{Num}(i_1, i_2, \ldots, i_k) \leq C_n^k - 1)$

numbering on the fly

$$\mathrm{Num}(i_1, i_2, \ldots, i_k) = C_{i_1-1}^1 + \\ + C_{i_2-1}^2 + \ldots + C_{i_k-1}^k, \quad C_j^l = 0, \quad j < l.$$


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


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



Extraction of a block of truly random bits from the sequence number

$$0 \leq \mathrm{Num} \leq N_k - 1$$

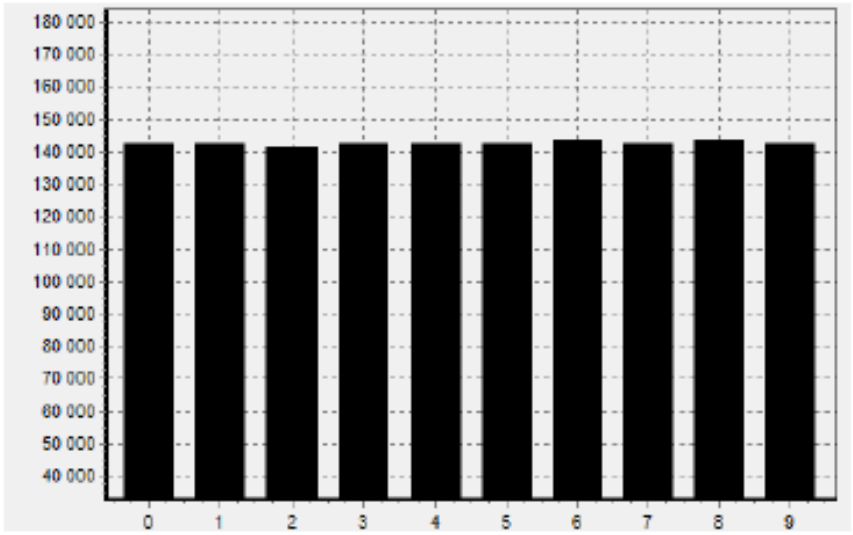
$$N_k = \sum_{i=0}^{i_{max}} 2^{k_i}$$

$$2^{k_0} + 2^{k_1} + \ldots + 2^{k_{i-1}} < \mathrm{Num} \leq$$

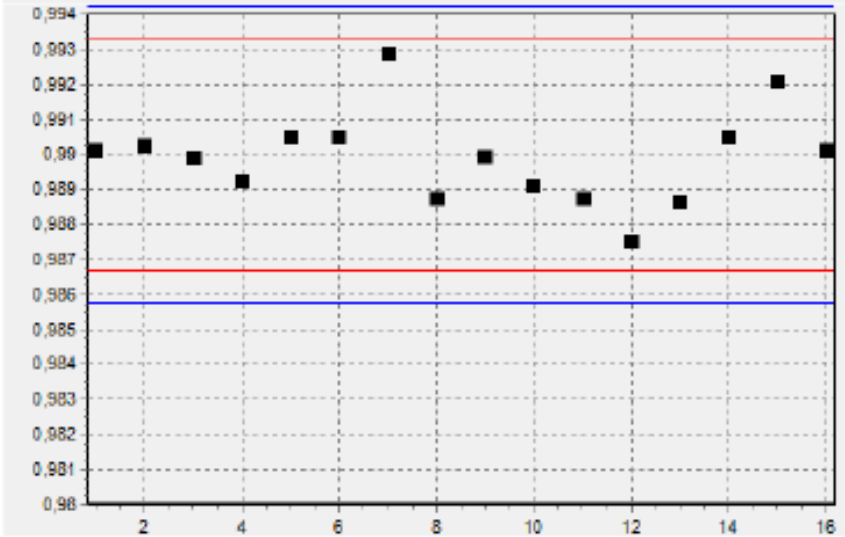
$$\leq 2^{k_0} + 2^{k_1} + \ldots + 2^{k_{i-1}} + 2^{k_i} - 1 \quad (i \leq i_{max})$$

k_i **least significant bits is random block**

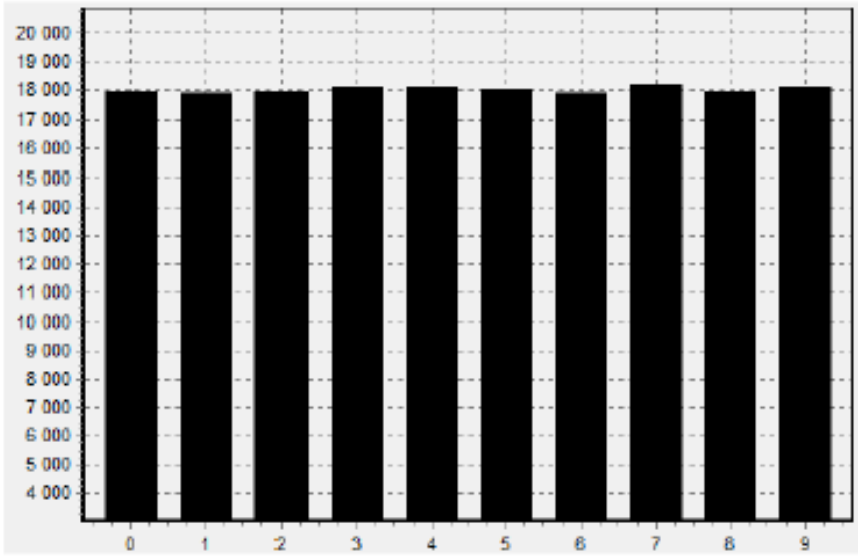
N	Название теста	доля послед. $M = 8000$ $L = 1 \cdot 10^6$	доля послед. $M = 1000$ $L = 2 \cdot 10^6$
1	Frequency Test	0.9901	0.9880
2	Block Frequency	0.9902	0.9886
3	Cumulative Sums	0.9899	0.9880
4	Cumulative Sums Reverse	0.9892	0, 9840
5	Runs	0.9905	0.9880
6	Longest Runs	0.9905	0.9886
7	Rank	0.9929	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

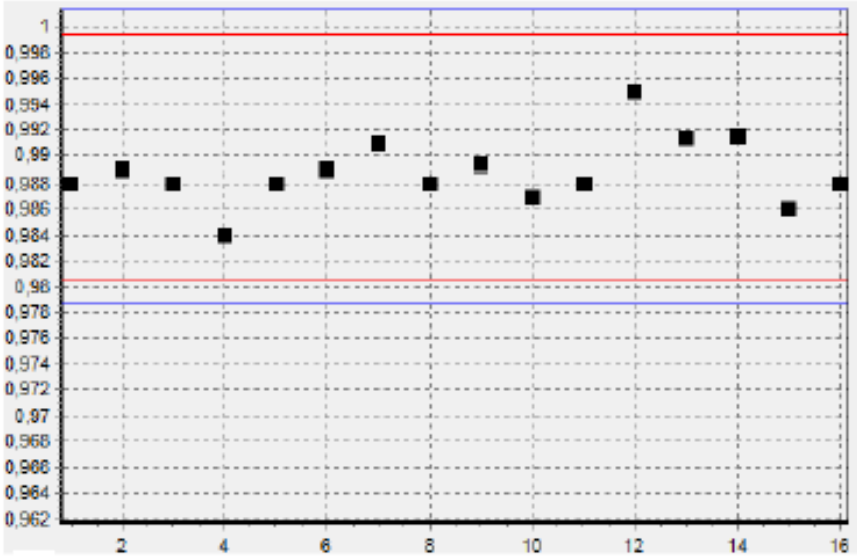
a)


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)

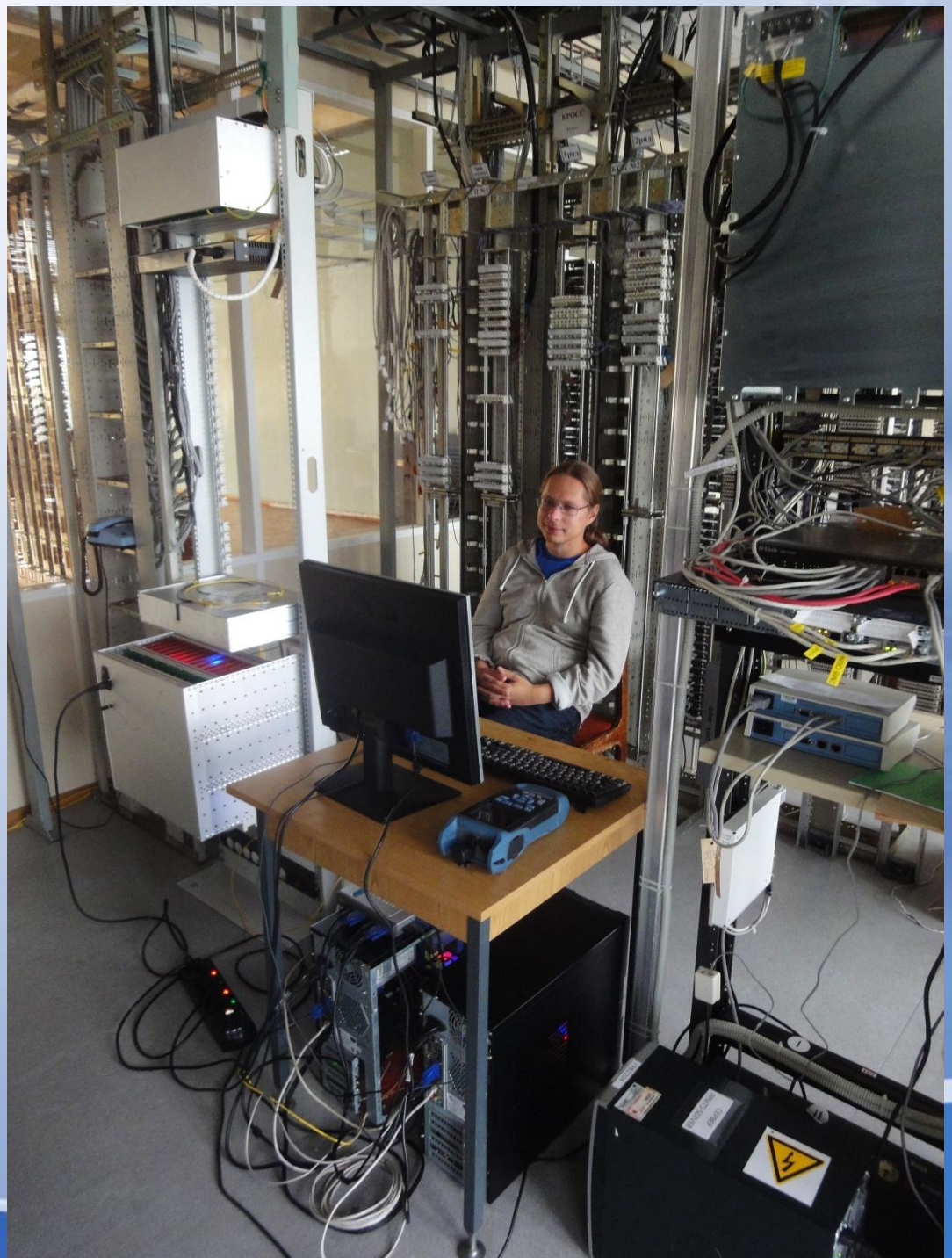

20 000
19 000
18 000
17 000
16 000
15 000
14 000
13 000
12 000
11 000
10 000
9 000
8 000
7 000
6 000
5 000
4 000
0 1 2 3 4 5 6 7 8 9

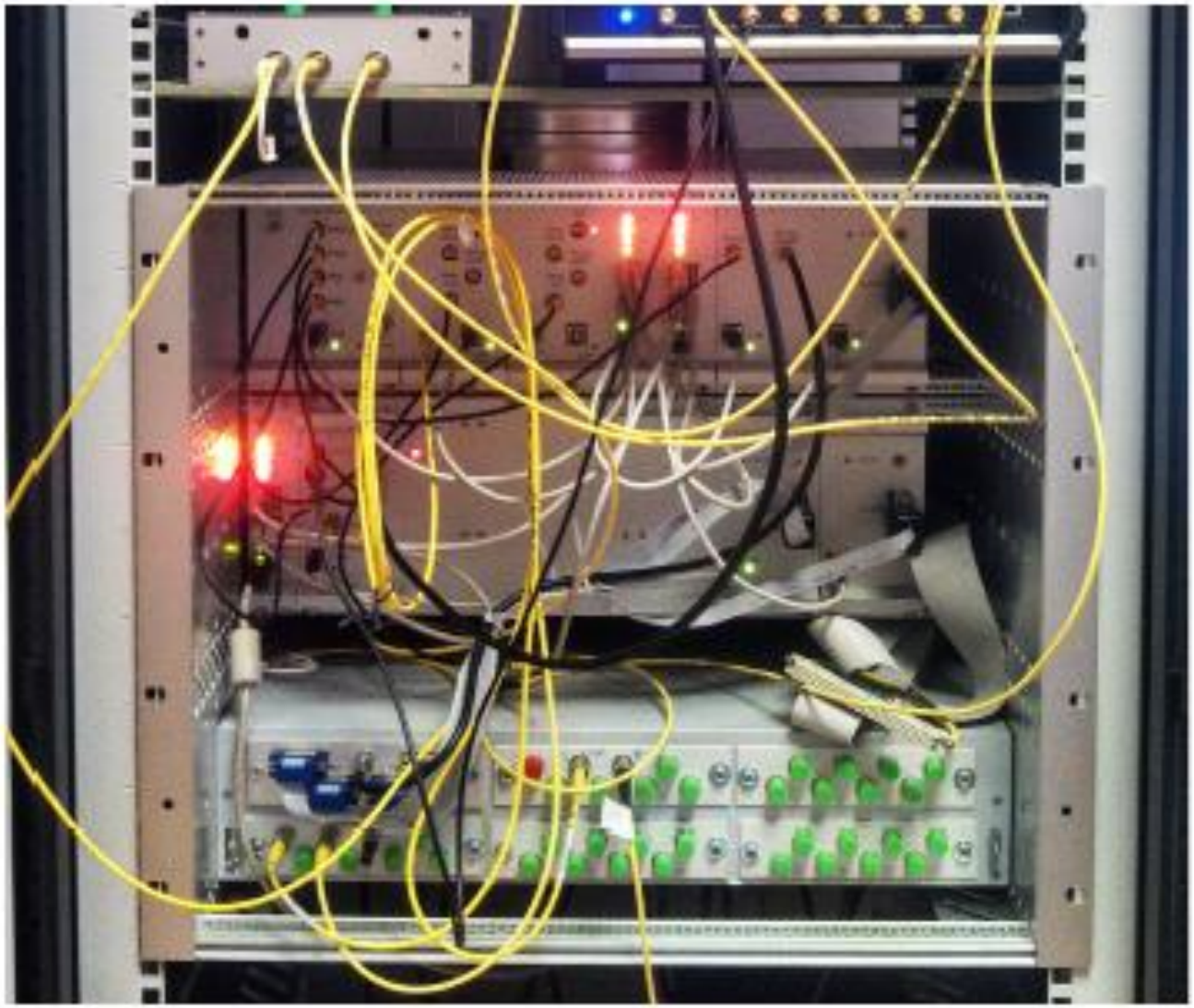
c)

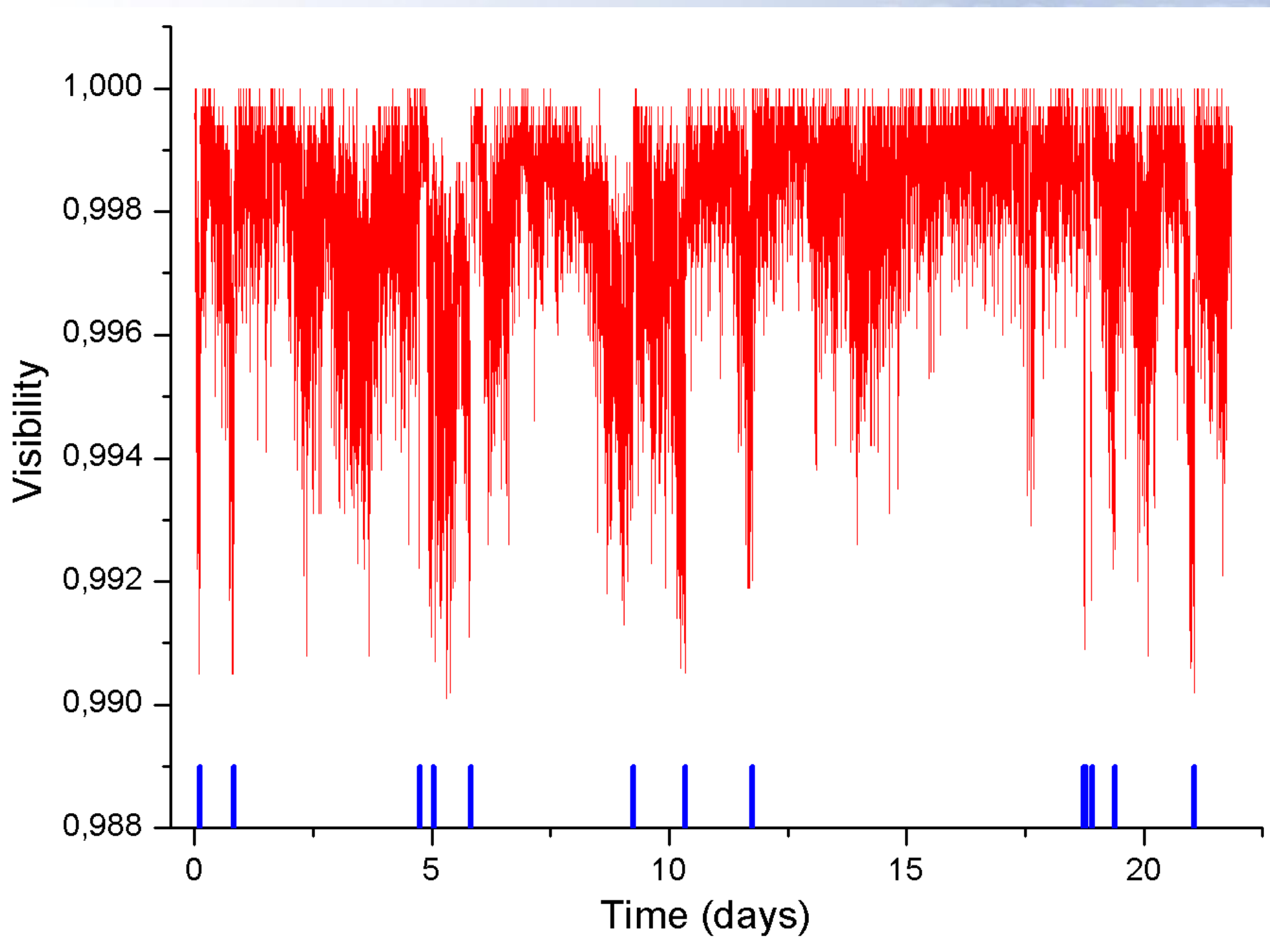

1
0,998
0,996
0,994
0,992
0,99
0,988
0,986
0,984
0,982
0,98
0,978
0,976
0,974
0,972
0,97
0,968
0,966
0,964
0,962
2 4 6 8 10 12 14 16

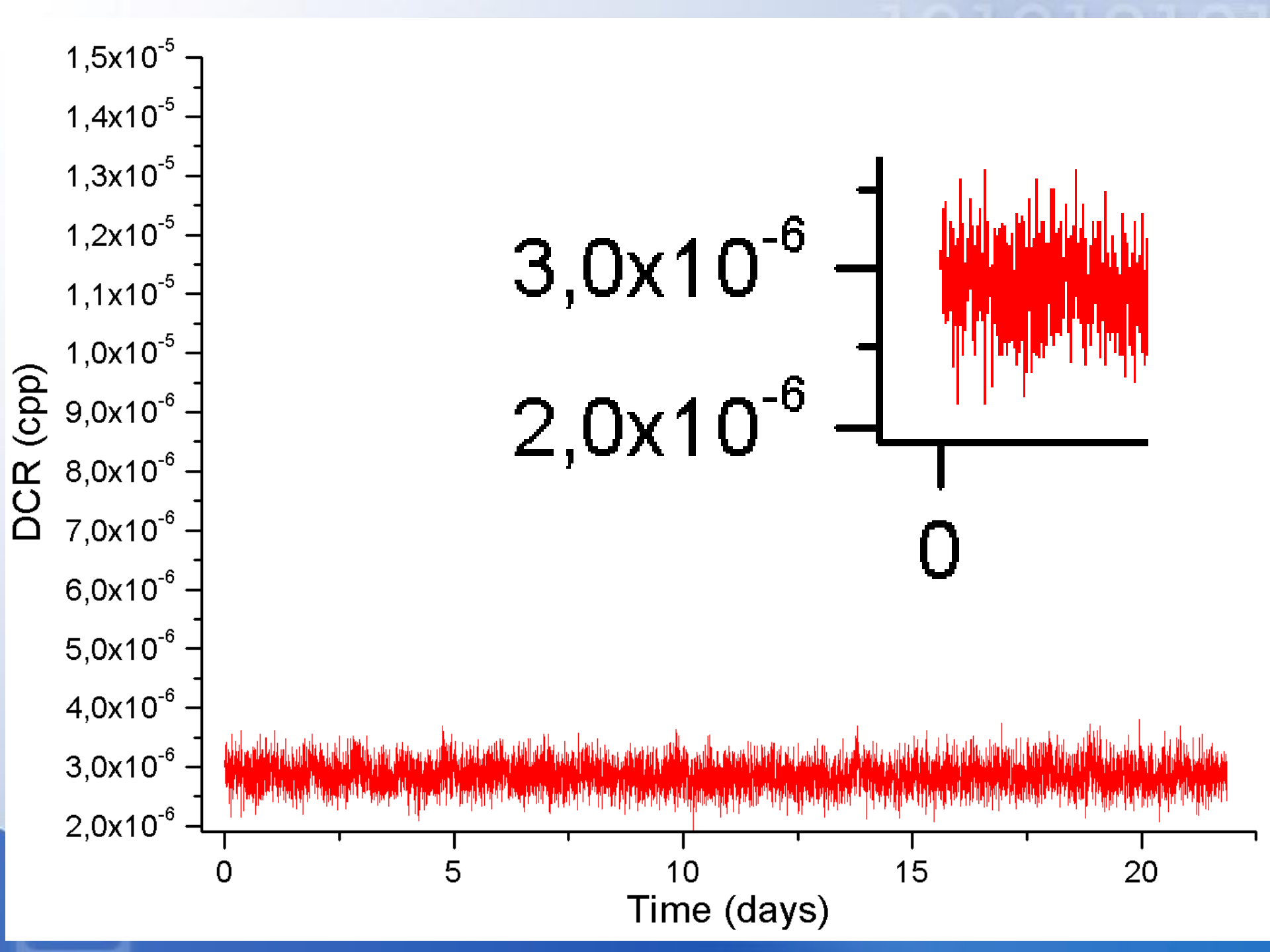
d)

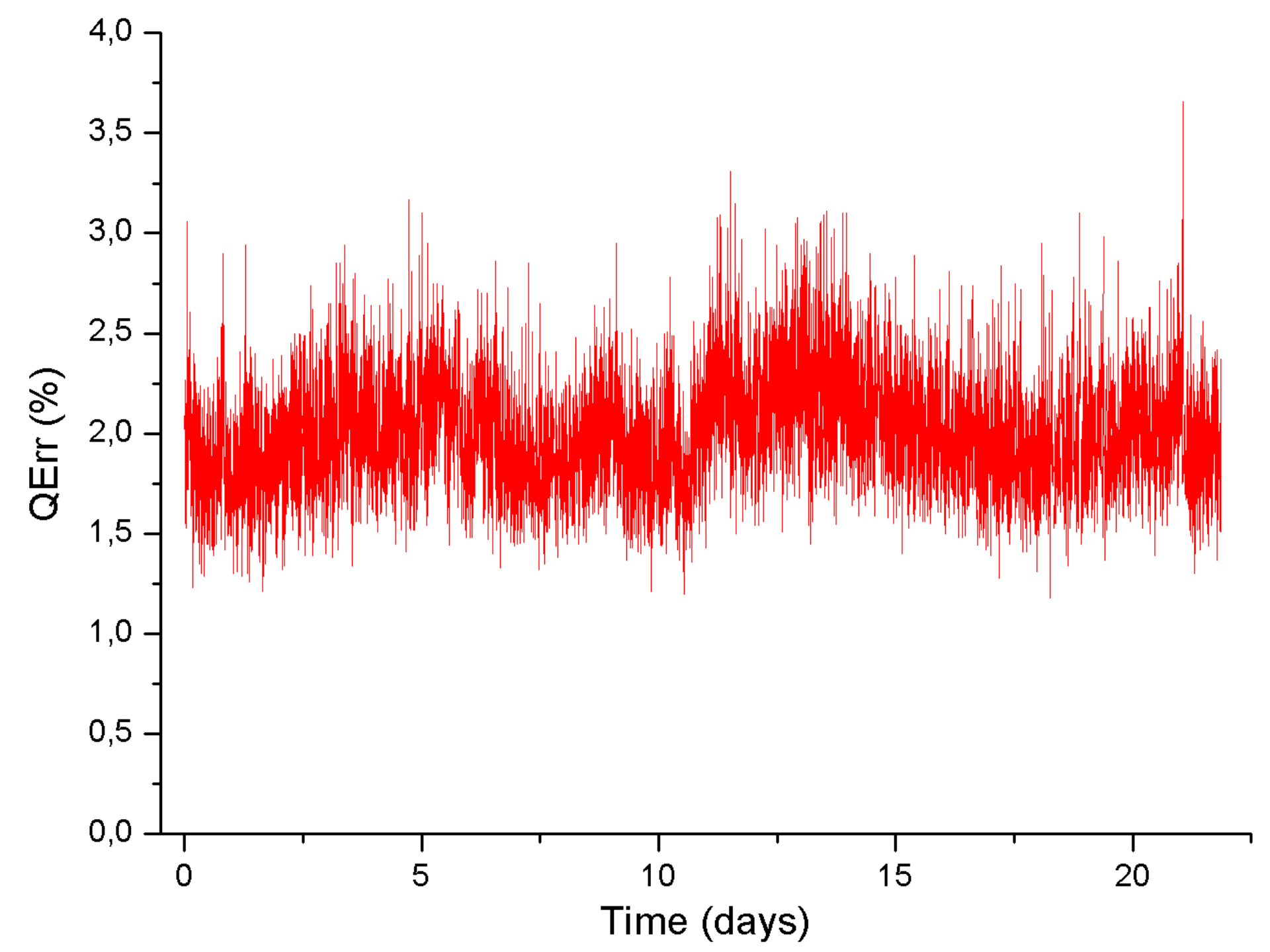
Работа ККС в автоматическом режиме.

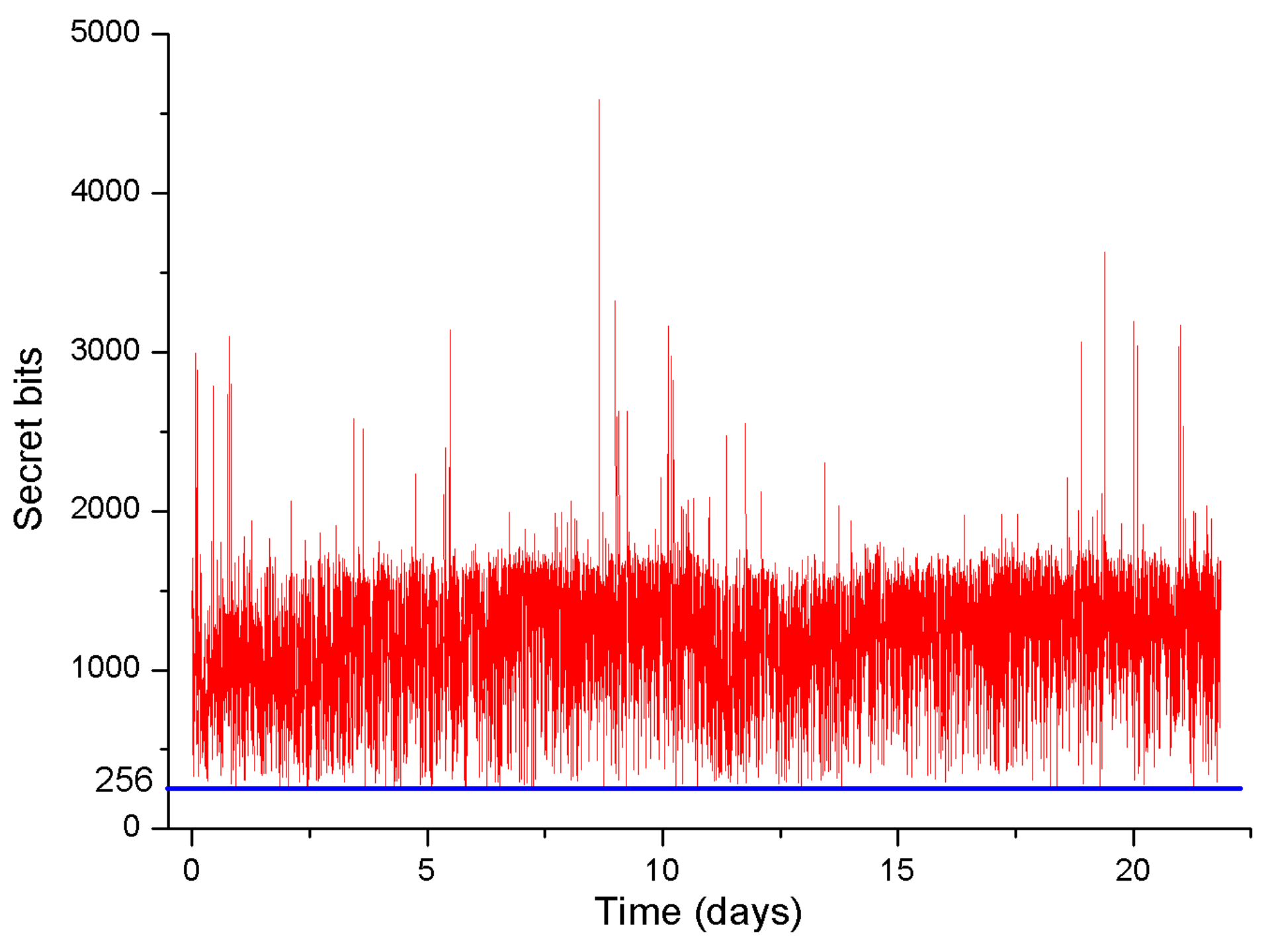


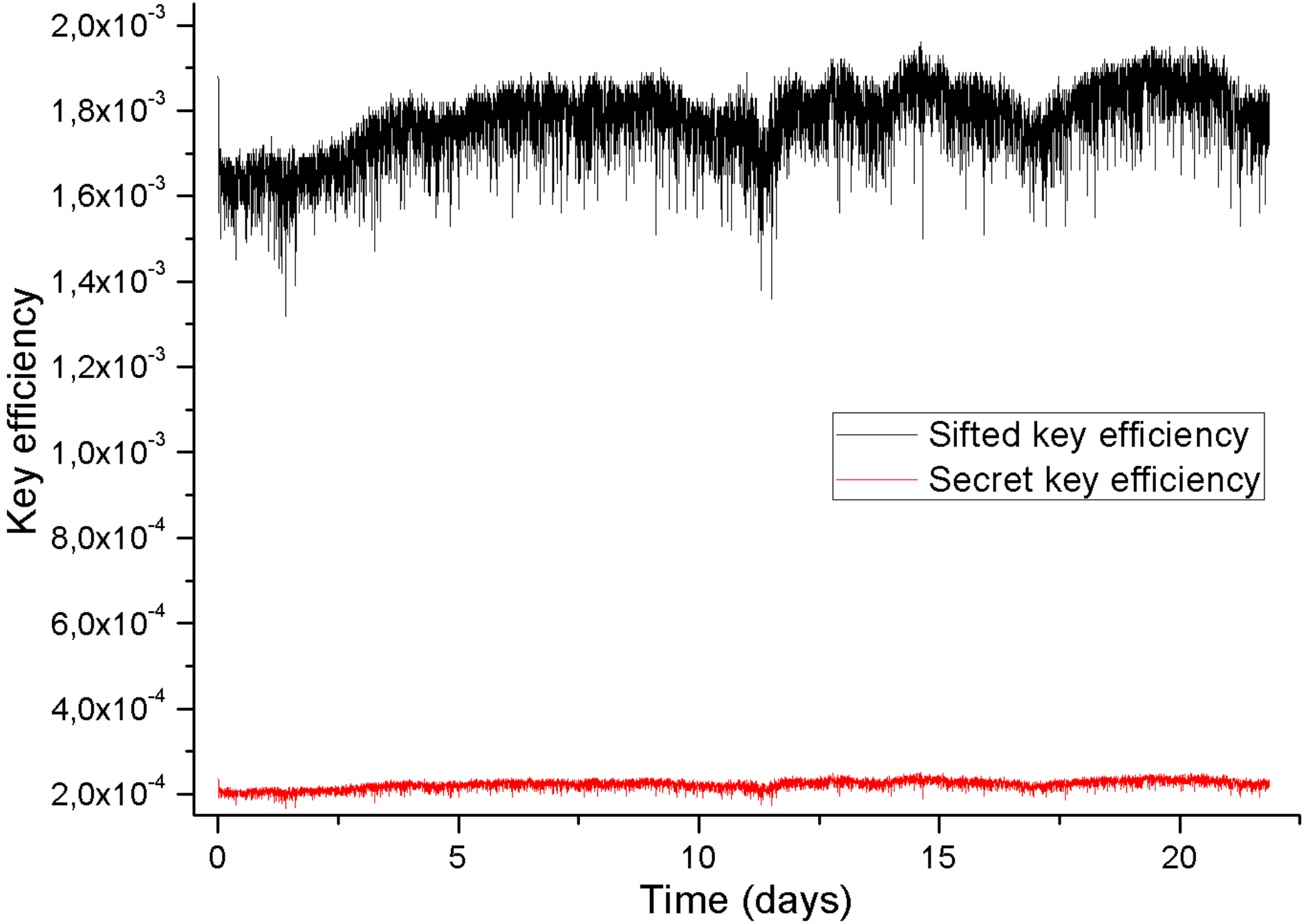



1,000
0,998
0,996
0,994
0,992
0,990
0,988
Visibility
0
5
10
15
20
Time (days)


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

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

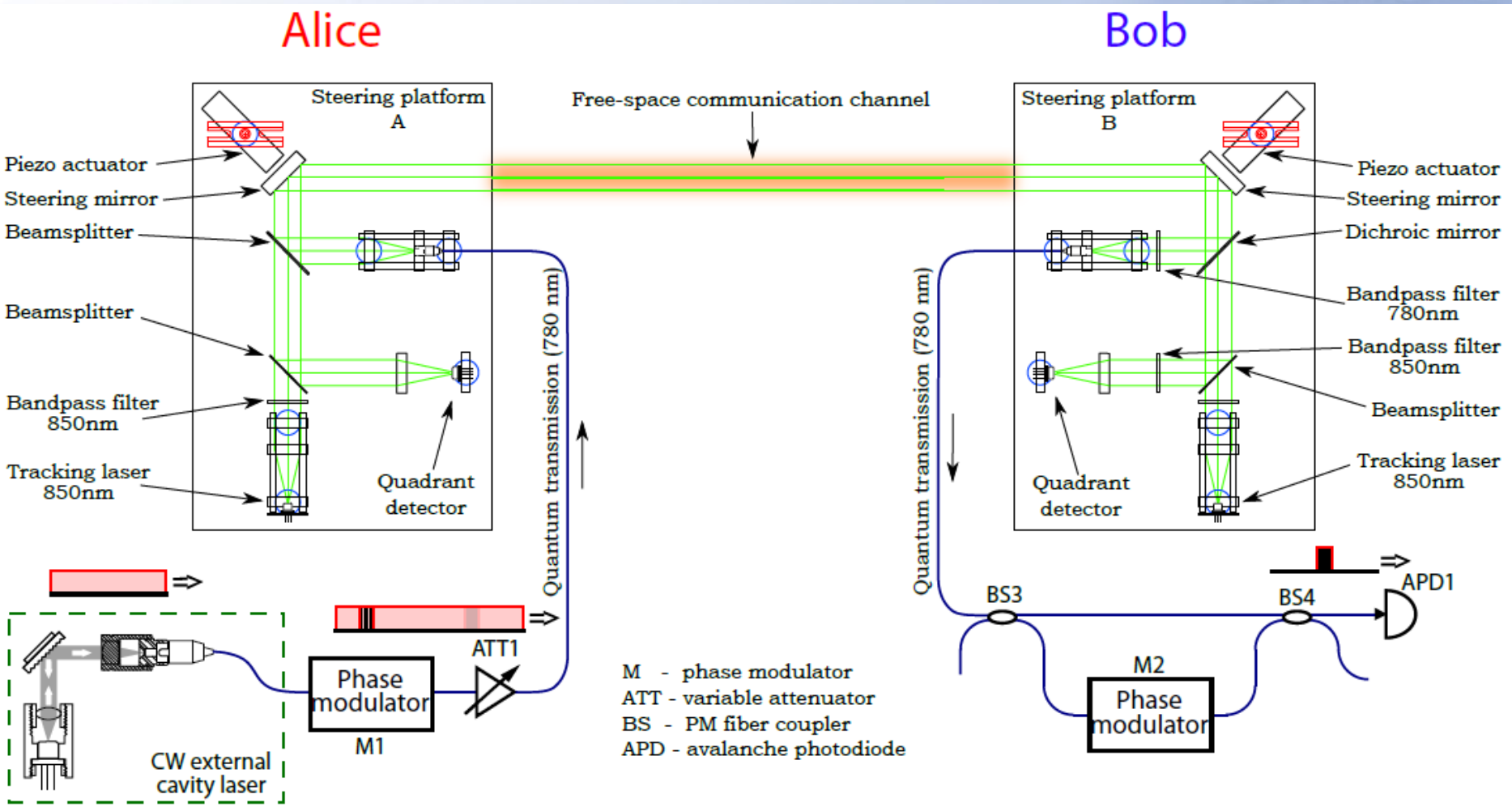
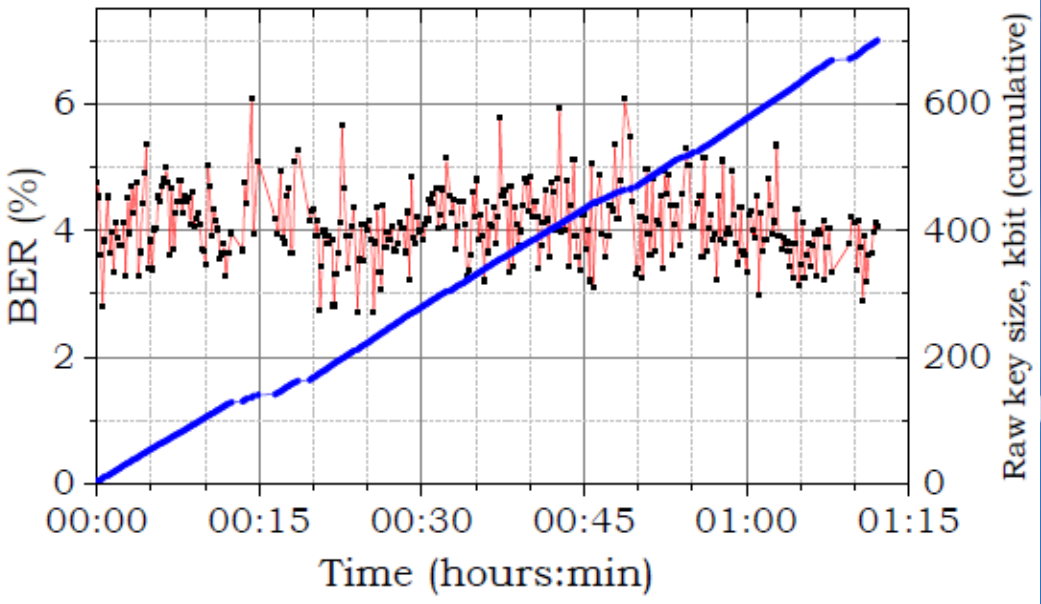


FIG. 1: Experimental setup including both the QKD part and the tracking system.

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



СПАСИБО ЗА ВНИМАНИЕ.