О сложности перебора ключей в квантовой криптографии

С.Н.Молотков

Академия Криптографии Российской Федерации,

Лаборатория квантовых оптических технологий,

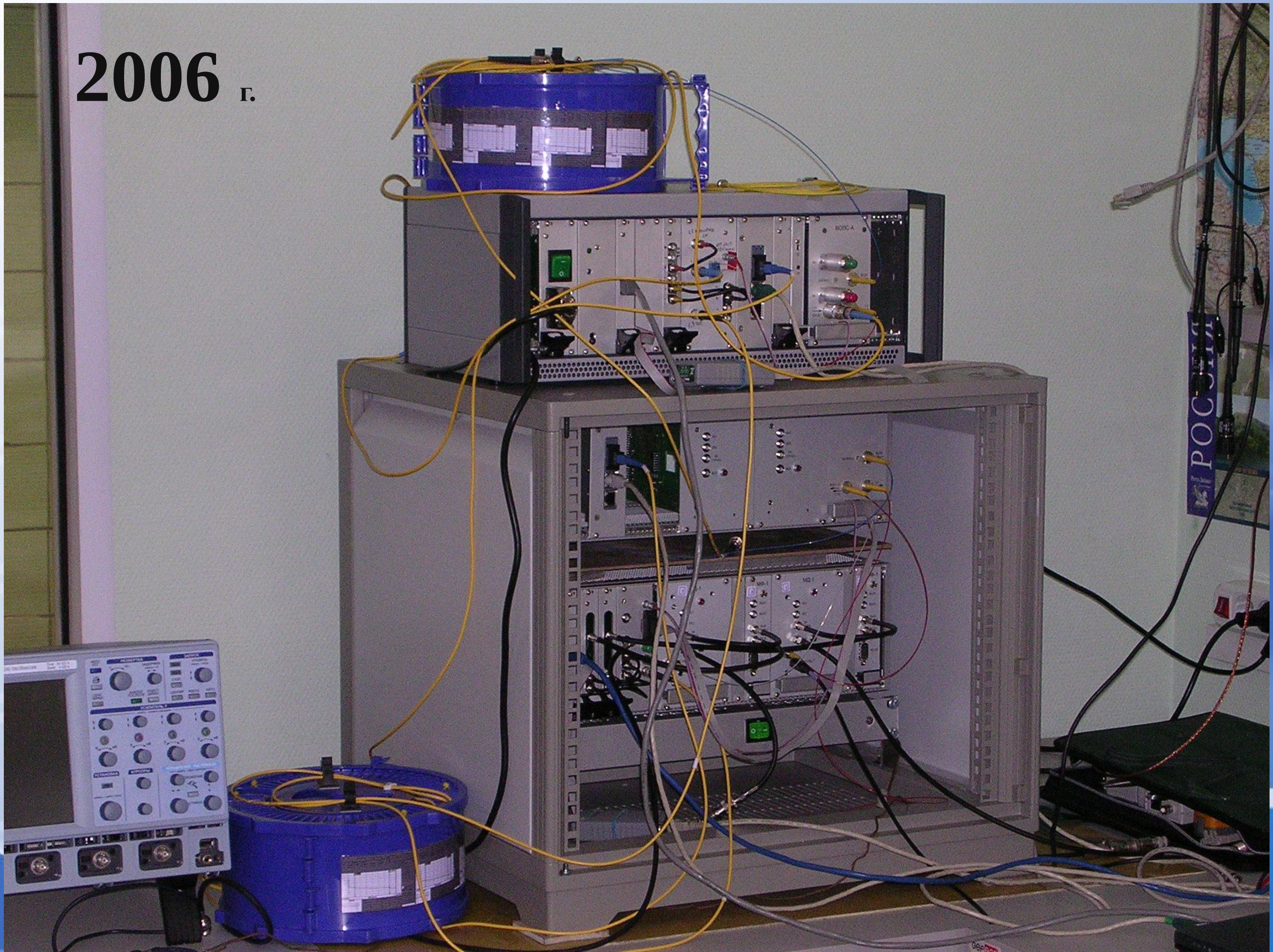
и Факультет ВМиК

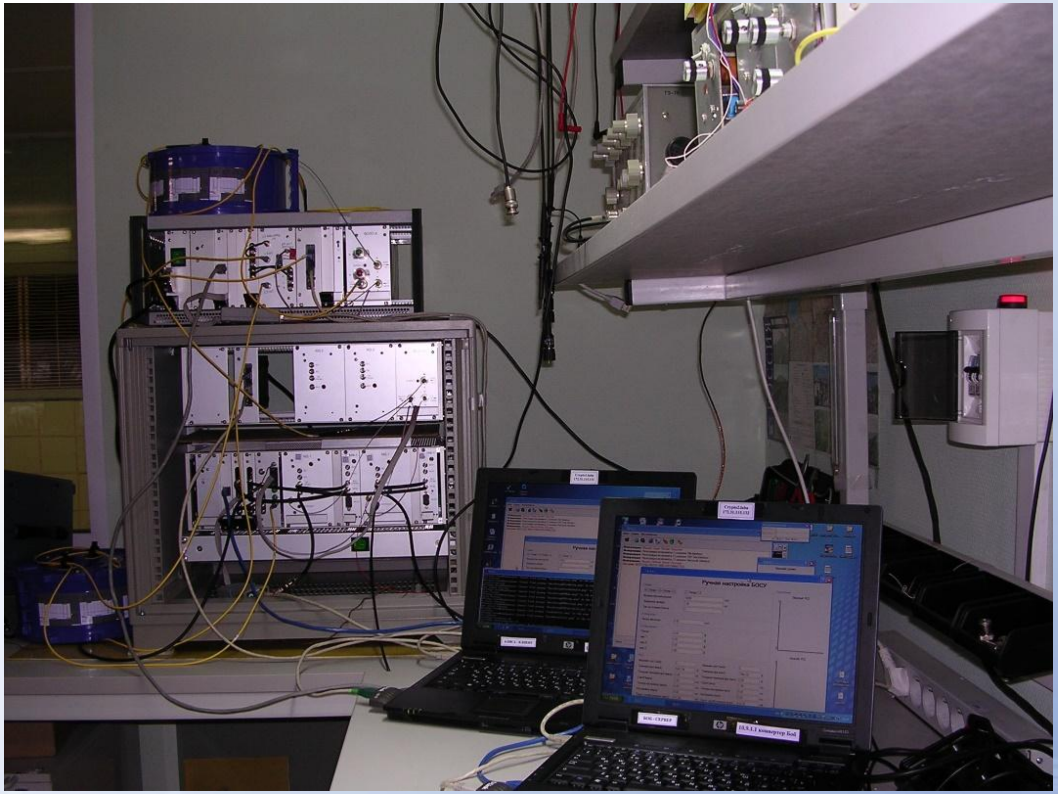
МГУ имени М.В.Ломоносова

QOT Лаборатория Квантовых Оптических Технологий

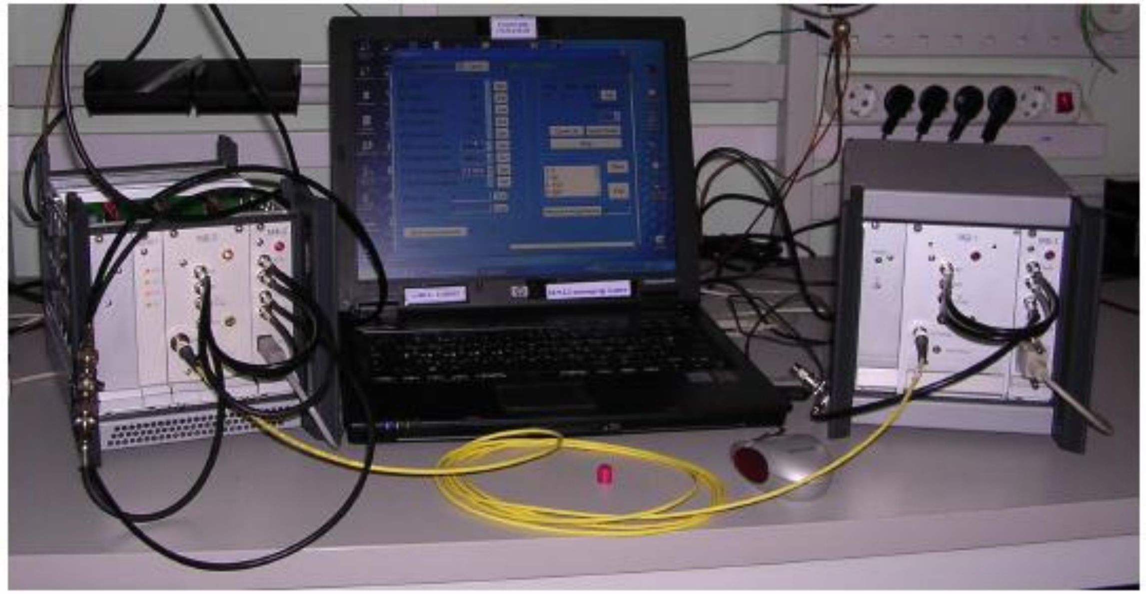
Цель квантового распределения ключей – создание сетевой полностью автоматизированной системы смены ключей без участия оператора (после запуска системы человек никогда не имеет доступа к ключам, используемым для шифрования)

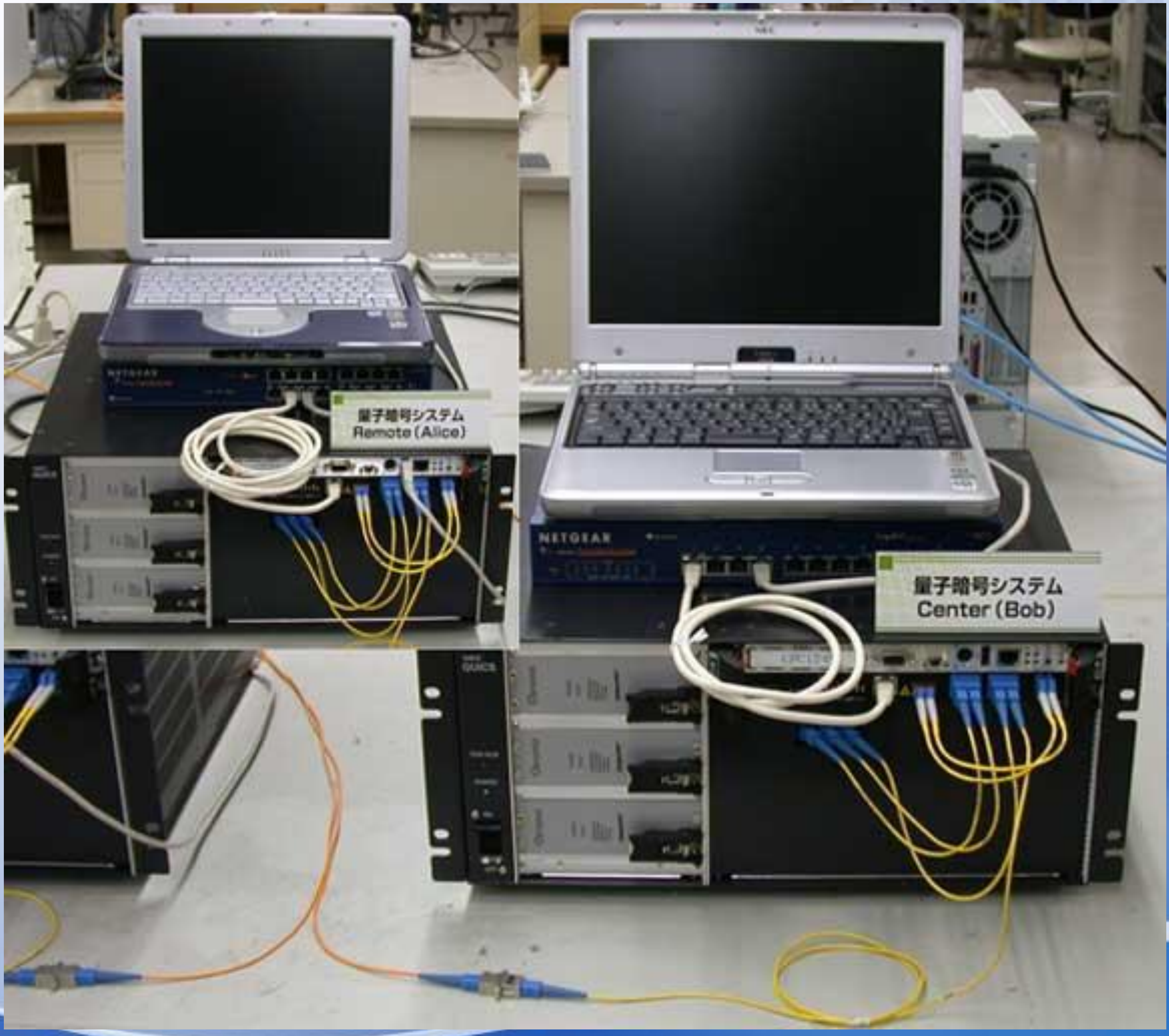
Как это выглядит сегодня и как может выглядеть в будущем.

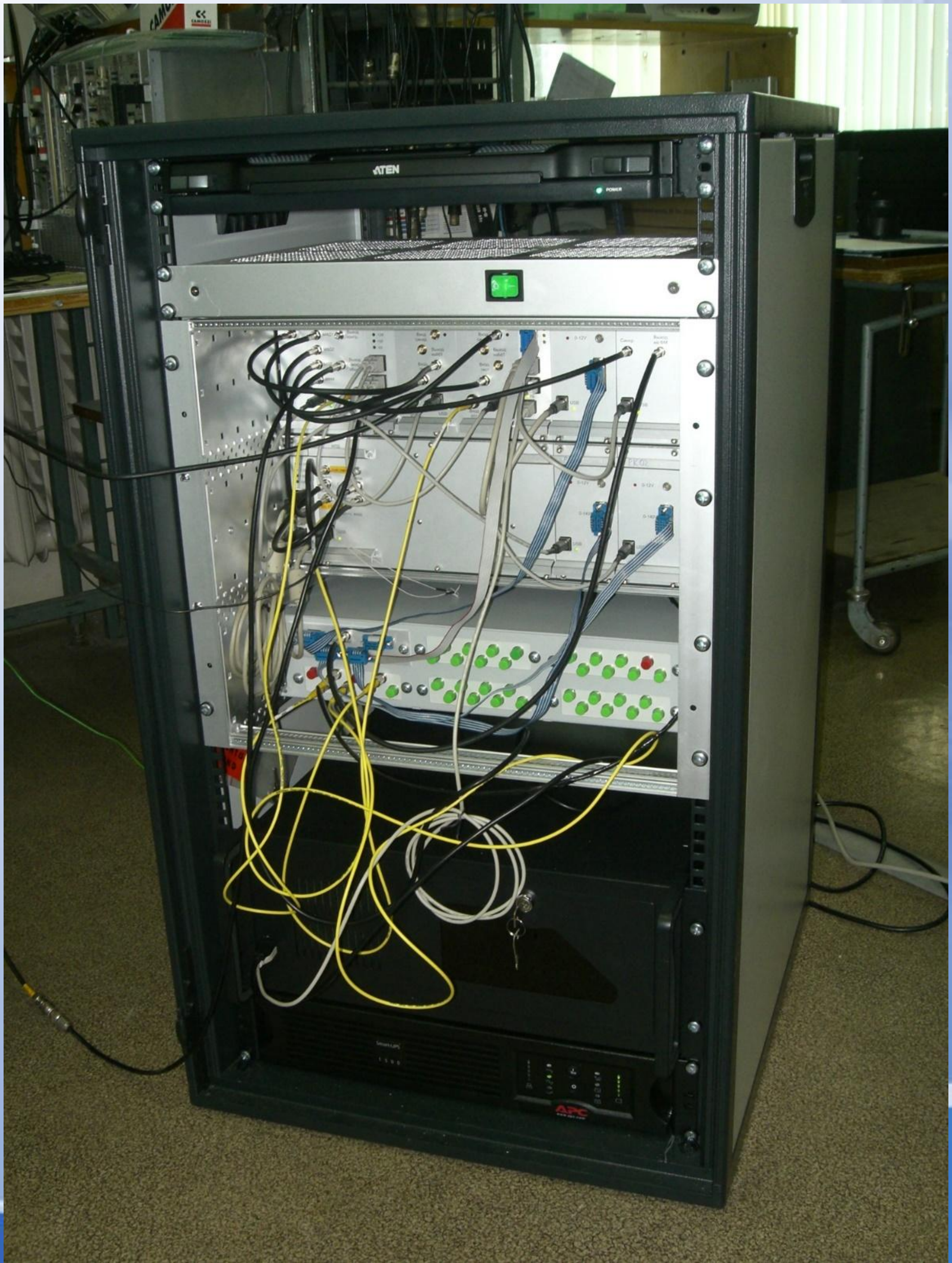


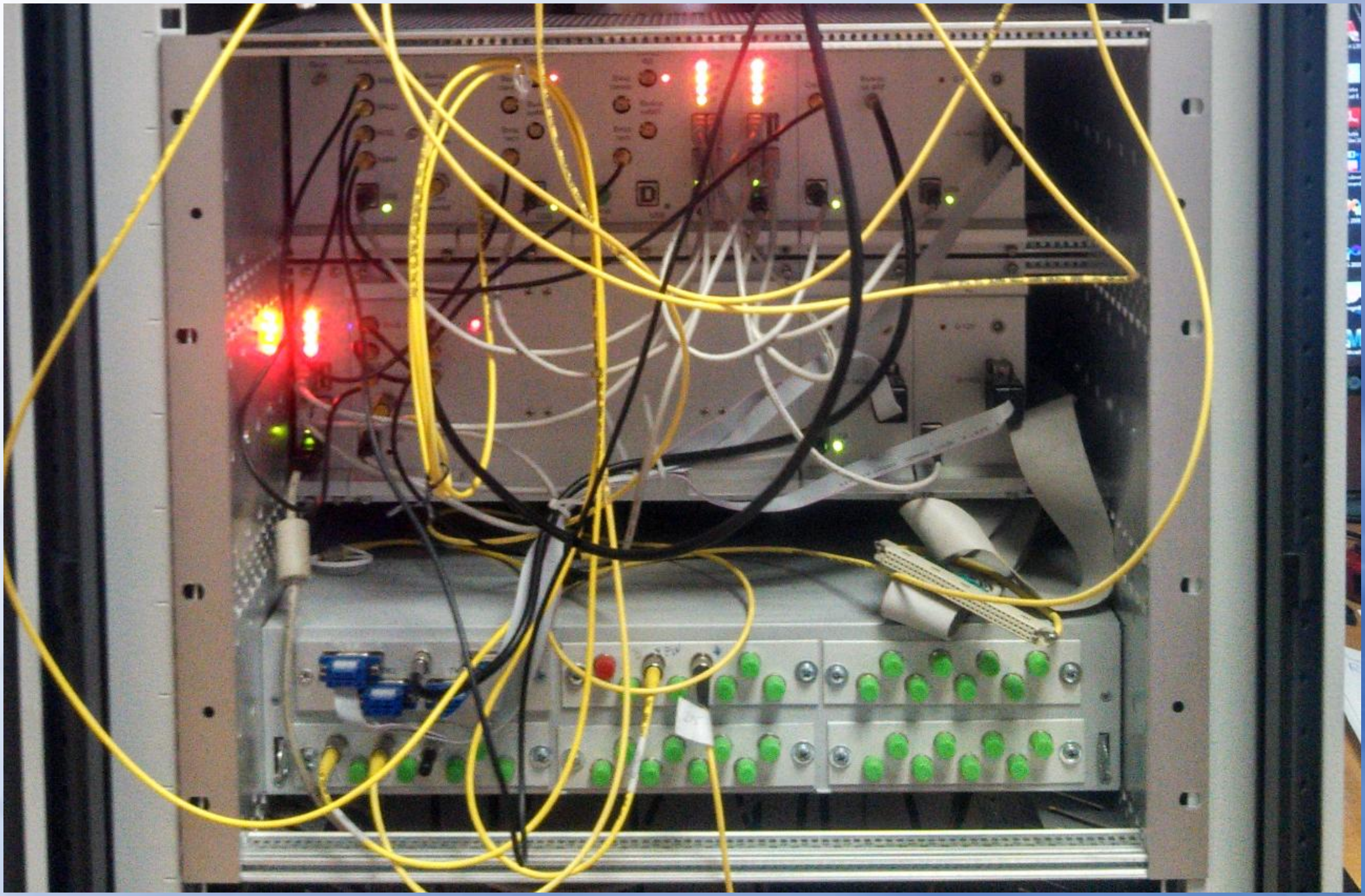

Ручная настройка БОСУ

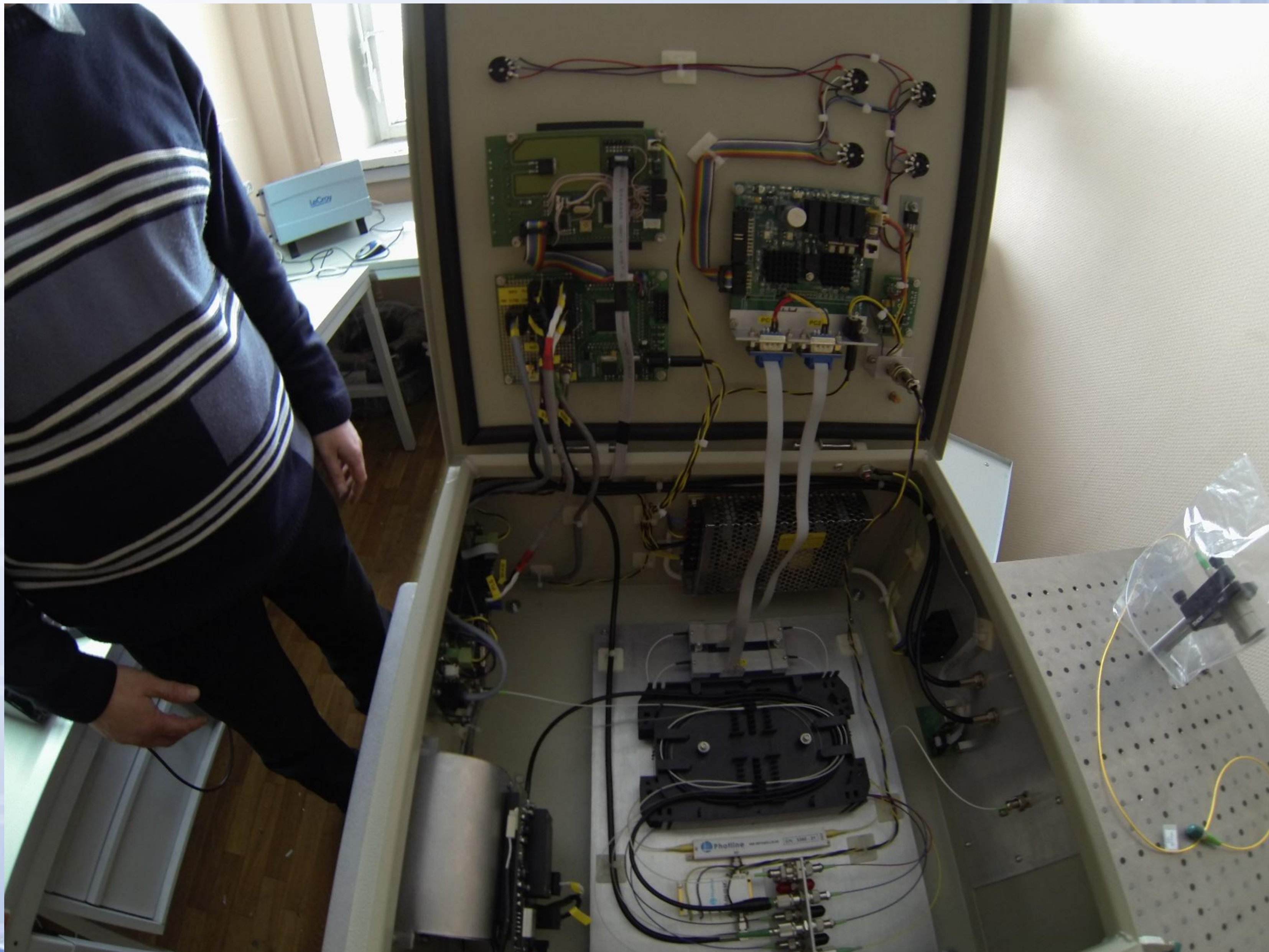

TRACO POWER
TRACO POWER




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

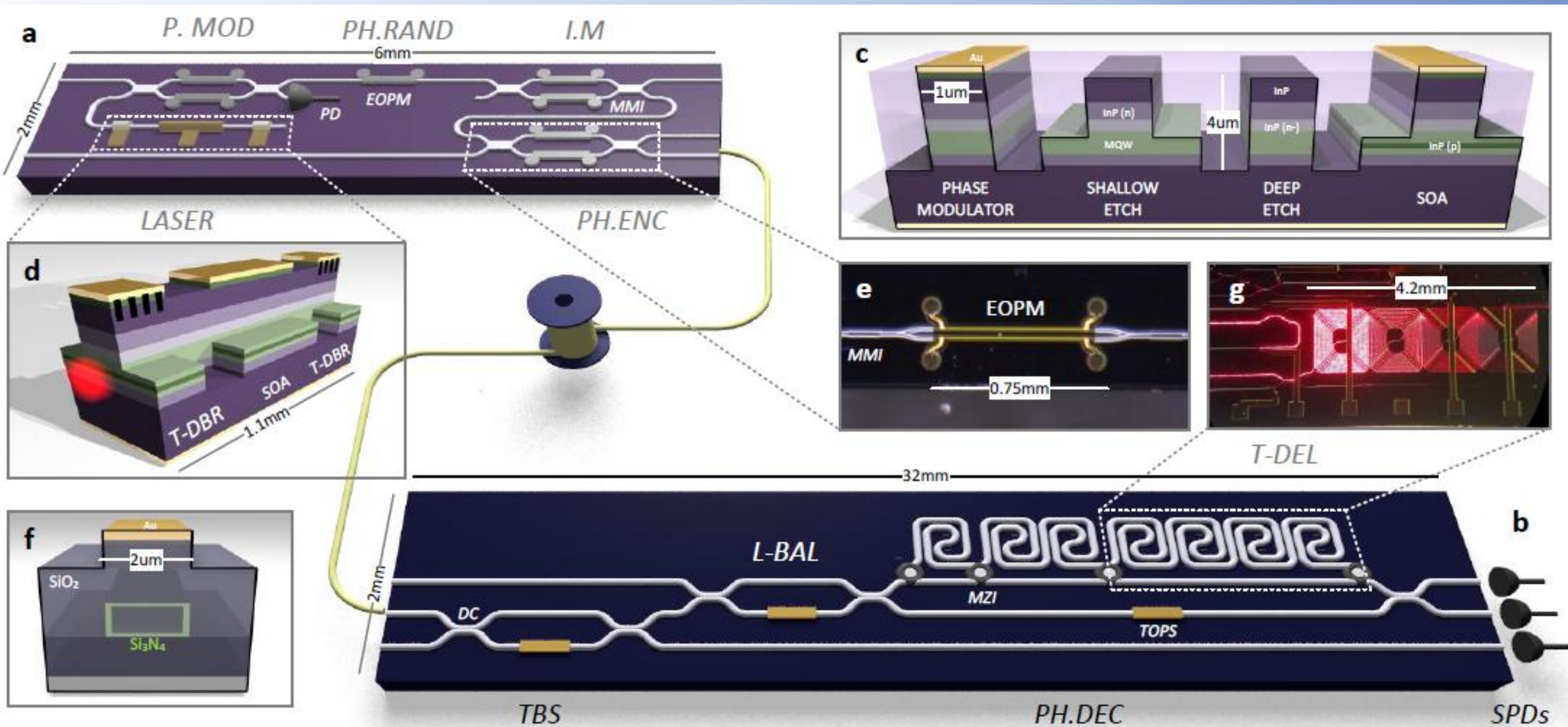

ATEN
APC




Photline

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,†]



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.**

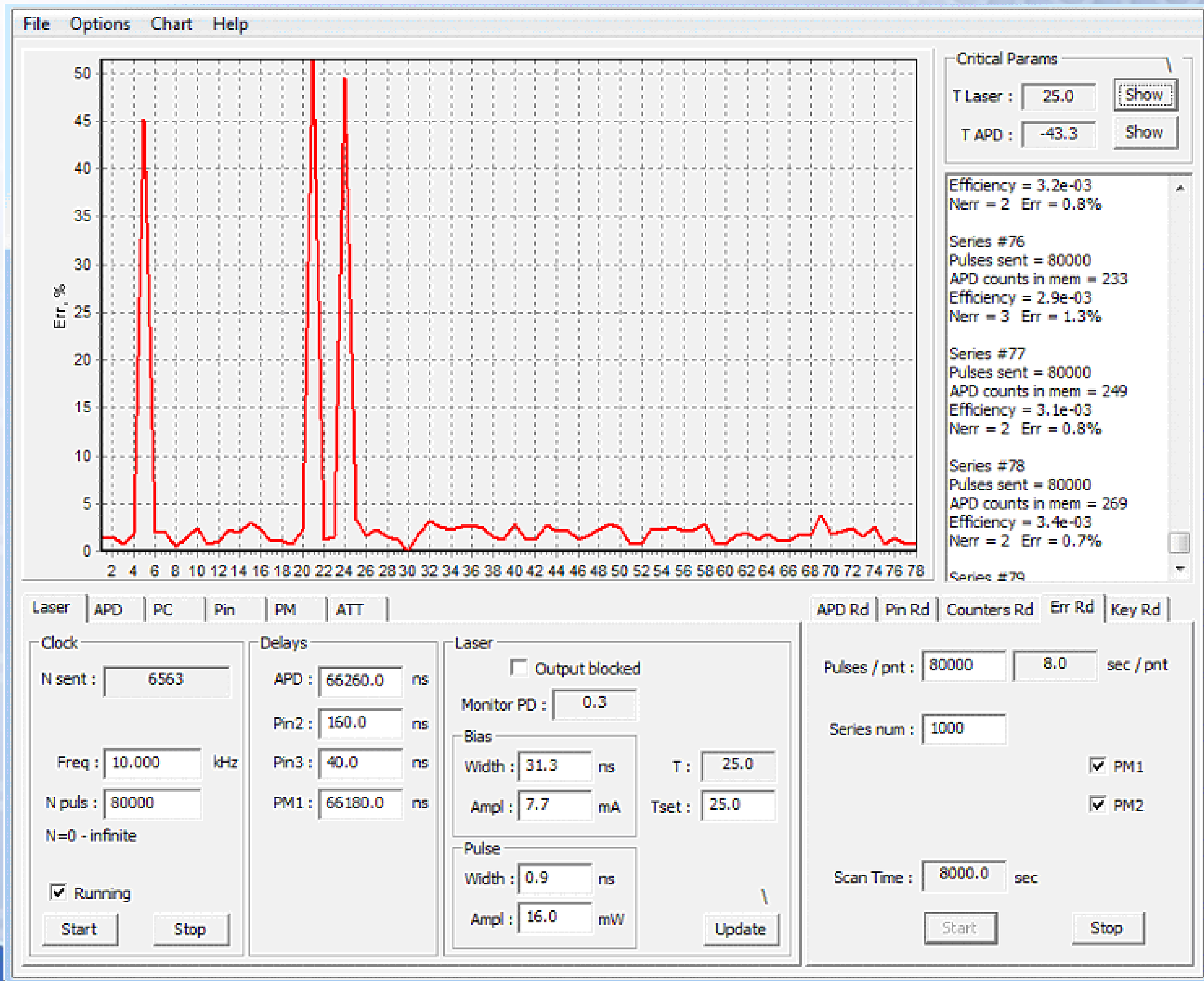
Следствия для распределения секретных ключей.

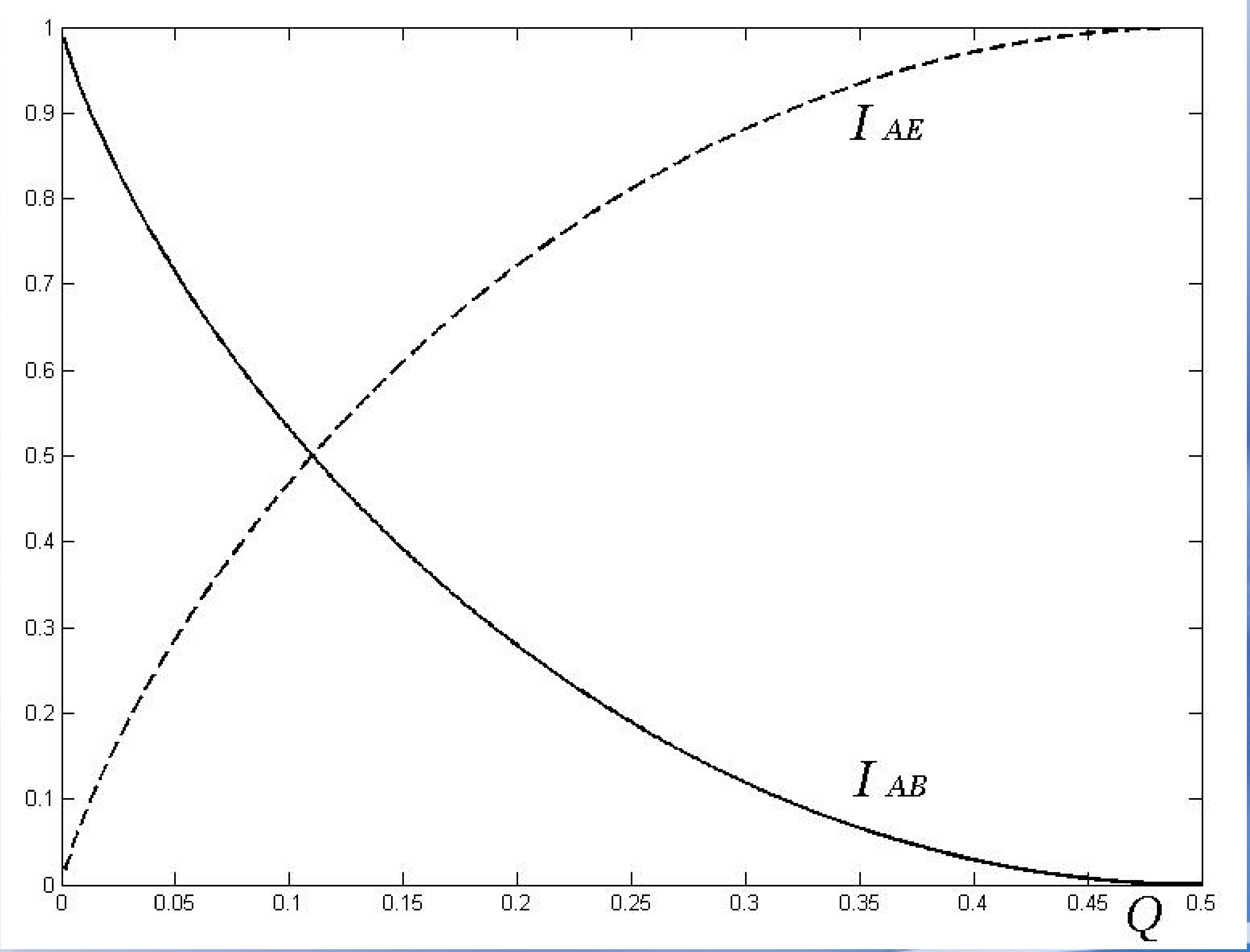
1) **Любое вторжение в канал связи приводит к возмущению квантовых состояний, которое детектируется – приводит к ошибке в первичных ключах.**
2) **Ошибка связана с верхней фундаментальной границей информации, которая уходит к подслушивателю при данной наблюдаемой вероятности ошибок на приемной стороне.**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

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

Любой протокол КРК содержит три стадии.

1) **Согласование базисов.**
2) **Коррекцию ошибок.**
3) **Сжатие очищенных ключей – усиление секретности.**


File Options Chart Help
50
45
40
35
30
25
20
15
10
5
0
Err, %
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



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
I_{AE}
I_{AB}
Q

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

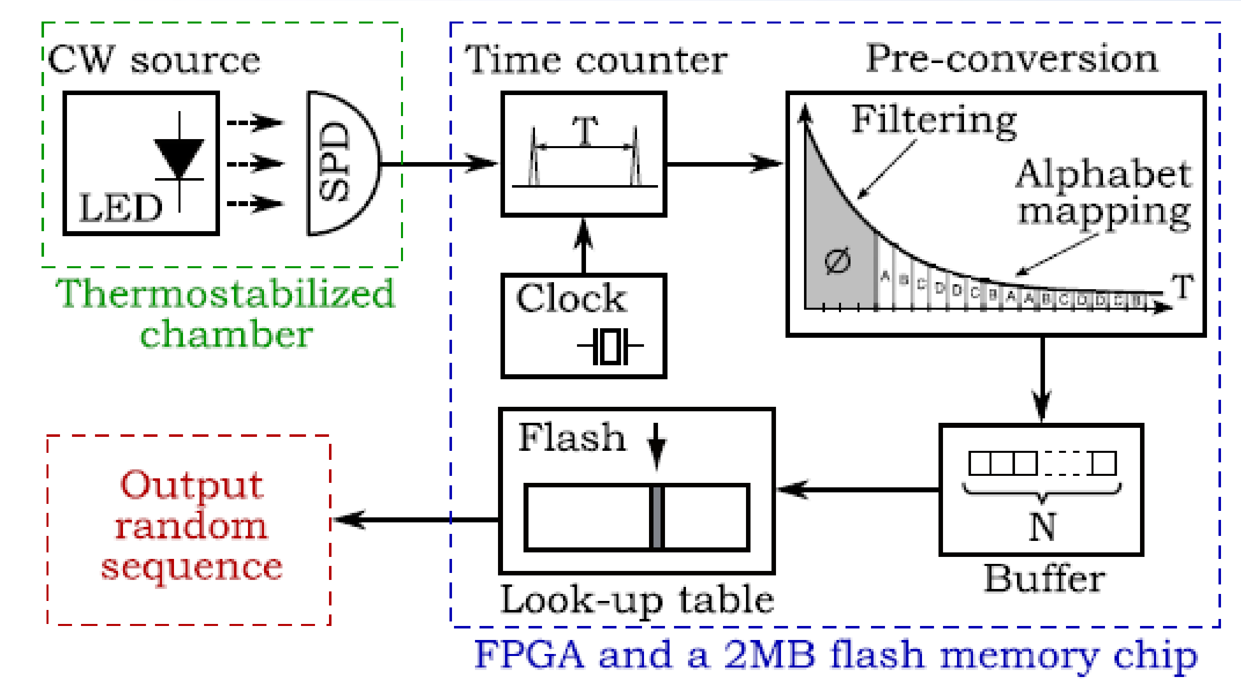
Journal of the Optical Society of America B

OPTICAL PHYSICS

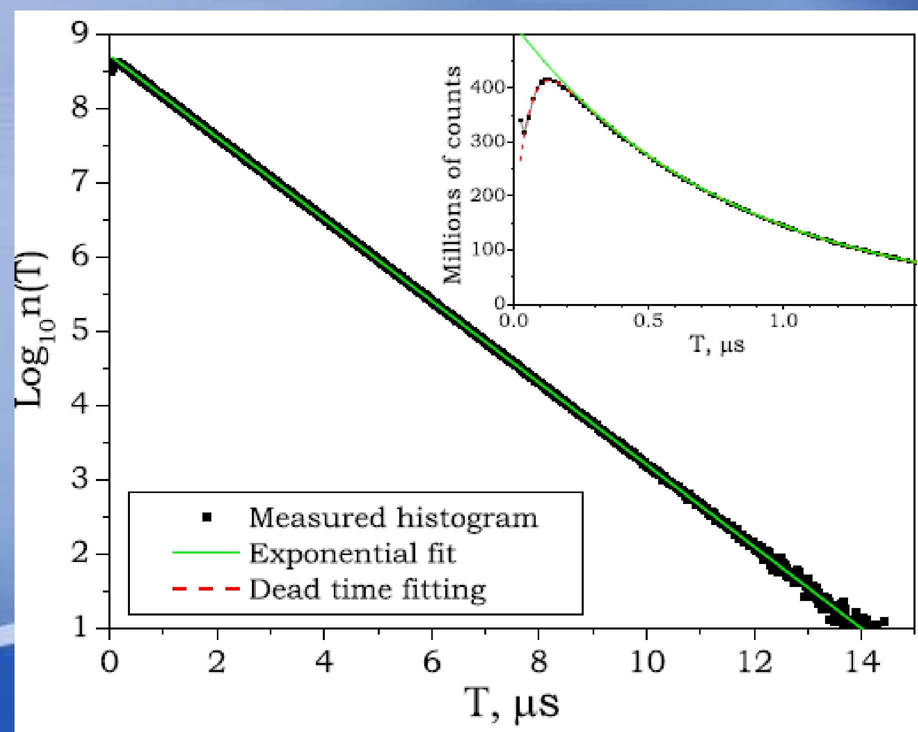
Minimalist design of a robust real-time quantum random number generator

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

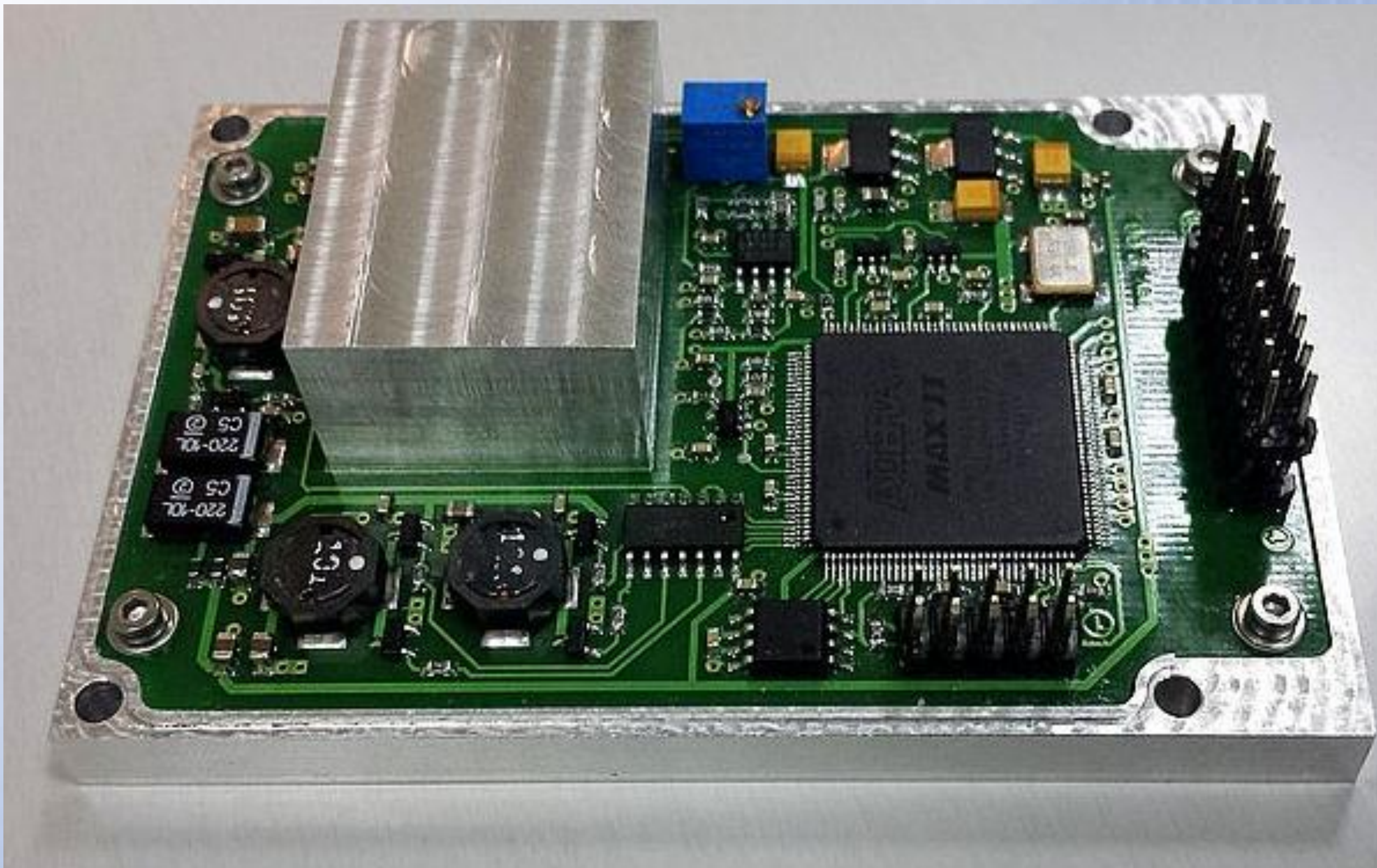
(4,0,0,0)	(3,1,0,0)	(2,2,0,0)	(2,1,1,0)	(1,1,1,1)
AAAA → ∅	BBBC → 00	AACC → 00	ABBD → 000	ABCD → 0000
	BBCB → 01	ACAC → 01	ABDB → 001 8	ABDC → 0001 16
	BCBB → 10	ACCA → 10	... ...	... ...
	CBBB → 11	CAAC → 11	BDAB → 111	CBDA → 1111
		CACA → 0	BDBA → 00	CDAB → 000
		CCAA → 1	DABB → 01	CDBA → 001 8
		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



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



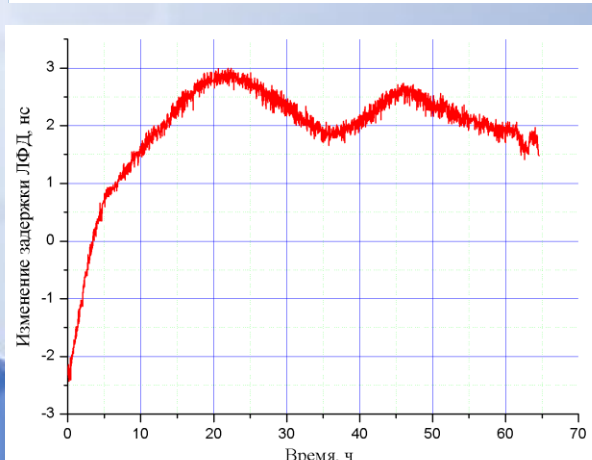
$Log_{10}n(T)$
T, μs
Millions of counts
T, μs
Measured histogram
Exponential fit
Dead time fitting

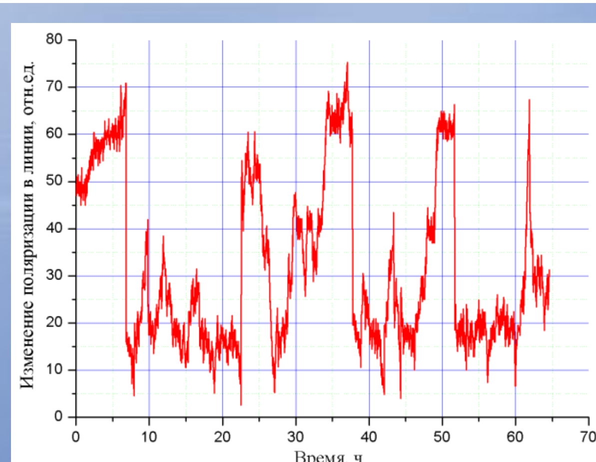

C5
220-10L
C5
220-10L
MAX II

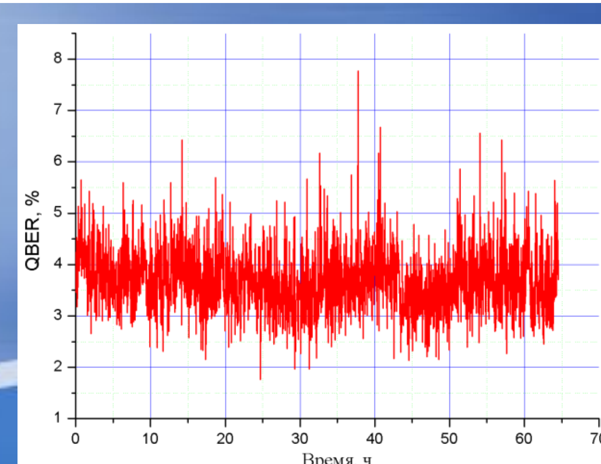
Работа ККС в автоматическом режиме.

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

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

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

time(h)	ser	T(C)	DCR(cpp)	FCR(cpp)	dt(ns)	Vis-ty	Bal	V1	V2	V3	Smax	kHz	P@Bob	Ngiant	Eff@counts	Eff@bases	Err(%)	Real	Raw(b)	Estm(b)	Rate	Fails	Ns	t(min)	Raw	Estm	Err(%)	Pure(b)	Quant(b)	Secret	t(min)	key#
0.000	1	-50.0	1.70e-06	1.70e-05	+0.59	0.9930	0	57.5	18.5	44.0	37.4	10.0	15.80	0	1.12e-02	4.14e-04	1.54	1.93	2071	823.4	595.2	0	1	1.4	2071	823	3.39	1024	14	1010	1.7	1
0.119	1	-50.0	2.80e-06	1.92e-05	+0.69	0.9945	0	56.0	21.0	47.0	36.9	10.0	16.20	0	1.10e-02	4.18e-04	1.72	2.34	2091	806.4	590.0	0	1	1.4	2091	806	1.91	1216	15	1201	1.7	2
0.194	1	-50.0	2.90e-06	2.34e-05	+0.73	0.9941	0	58.5	17.5	50.0	37.5	10.0	15.80	0	1.10e-02	4.27e-04	2.05	2.57	2136	788.2	569.8	0	1	1.4	2136	788	2.84	1120	16	1104	1.7	3
0.268	1	-50.0	2.90e-06	2.36e-05	+0.72	0.9952	0	59.0	21.5	51.0	37.1	10.0	16.20	0	1.00e-02	3.92e-04	2.24	3.06	1962	707.6	517.8	0	1	1.4	1962	708	3.25	984	16	968	1.6	4
0.342	1	-50.0	3.80e-06	2.32e-05	+0.75	0.9798	1	55.0	23.0	53.0	37.3	10.0	16.20	0	1.05e-02	4.03e-04	2.15	2.58	2013	733.4	165.4	0	1	4.4	2013	733	2.56	1088	16	1072	4.8	5
0.467	1	-50.0	4.00e-06	3.04e-05	+0.78	0.9934	1	51.0	21.5	52.5	37.1	10.0	16.20	0	1.05e-02	4.25e-04	2.66	2.59	2125	738.0	167.7	0	1	4.4	2125	738	3.06	1088	19	1070	4.7	6
0.591	1	-50.0	4.10e-06	1.70e-05	+0.77	0.9941	0	50.5	18.0	54.0	37.0	10.0	15.80	0	1.11e-02	4.28e-04	1.49	2.43	2138	858.1	627.9	0	1	1.4	2138	858	4.31	960	14	946	1.7	7
0.665	1	-50.0	3.00e-06	1.94e-05	+0.71	0.9913	0	52.0	17.0	52.0	37.4	10.0	16.20	0	1.16e-02	4.48e-04	1.62	1.56	2240	878.2	642.6	0	1	1.4	2240	878	2.29	1248	15	1233	1.7	8
0.739	1	-50.0	2.10e-06	2.10e-05	+0.86	0.9940	0	49.0	16.0	56.0	37.3	10.0	15.80	0	1.06e-02	4.05e-04	1.94	2.96	2026	757.2	554.1	0	1	1.4	2026	757	5.18	832	16	817	1.7	9
0.813	1	-50.0	2.50e-06	1.92e-05	+0.90	0.9962	0	49.0	17.0	56.0	37.4	10.0	16.20	0	1.07e-02	4.07e-04	1.77	2.45	2037	780.0	570.7	0	1	1.4	2037	780	3.84	960	15	945	Key stat tests failed!	
0.843	1	-50.0	2.90e-06	1.84e-05	+0.85	0.9919	0	48.0	14.5	54.0	37.2	10.0	15.80	0	1.15e-02	4.32e-04	1.60	2.13	2162	851.4	615.4	0	1	1.4	2162	851	1.75	1280	15	1266	1.7	10
0.917	1	-50.0	3.20e-06	2.06e-05	+0.89	0.9957	0	49.5	11.0	56.0	37.3	10.0	15.80	0	1.06e-02	4.08e-04	1.89	2.20	2041	768.0	561.9	0	1	1.4	2041	768	1.47	1248	15	1233	Key stat tests failed!	
0.946	1	-50.0	2.20e-06	1.72e-05	+0.89	0.9930	0	46.5	11.0	55.5	37.2	10.0	15.80	0	1.09e-02	4.14e-04	1.56	1.88	2072	821.2	600.9	0	1	1.4	2072	821	3.69	992	14	978	1.6	11
1.020	1	-50.0	1.80e-06	1.58e-05	+0.93	0.9946	0	49.0	13.0	56.5	37.4	10.0	15.40	0	1.15e-02	4.34e-04	1.37	1.89	2168	892.7	661.3	0	1	1.4	2168	893	3.82	1024	14	1011	1.7	12
1.094	1	-50.0	2.90e-06	1.66e-05	+1.03	0.9945	0	53.0	17.0	53.5	37.6	10.0	15.80	0	1.12e-02	4.42e-04	1.41	2.13	2210	902.1	660.0	0	1	1.4	2210	902	3.16	1120	14	1106	1.7	13
1.168	1	-50.0	2.60e-06	2.56e-05	+1.02	0.9941	0	55.0	13.5	52.5	37.2	10.0	15.80	0	1.16e-02	4.44e-04	2.15	1.44	2220	809.6	592.4	0	1	1.4	2220	810	4.67	960	17	943	1.7	14
1.242	1	-50.0	2.00e-06	2.90e-05	+1.11	0.9919	0	51.5	13.5	56.0	37.5	10.0	15.40	0	1.10e-02	4.09e-04	2.63	2.10	2046	711.7	527.2	0	1	1.4	2046	712	2.71	1088	18	1070	1.7	15
1.316	1	-50.0	2.90e-06	2.64e-05	+1.20	0.9978	1	48.5	17.5	55.0	37.6	10.0	16.20	0	1.15e-02	4.25e-04	2.31	1.98	2125	761.5	169.2	0	1	4.5	2125	761	3.93	992	17	975	4.8	16
1.442	1	-50.0	2.90e-06	1.36e-05	+1.24	0.9978	0	48.1	16.4	56.5	37.1	10.0	15.80	0	1.13e-02	4.27e-04	1.20	1.22	2136	916.7	670.8	0	1	1.4	2136	917	2.84	1120	13	1107	1.6	17
1.516	1	-50.0	2.20e-06	1.52e-05	+1.28	0.9935	0	49.1	11.9	59.0	37.3	10.0	16.20	0	1.08e-02	4.08e-04	1.40	2.15	2042	835.1	611.0	0	1	1.4	2042	835	1.26	1280	14	1267	1.7	18
1.635	1	-50.0	3.80e-06	1.40e-05	+1.27	0.9913	0	45.6	15.4	63.0	37.4	10.0	15.80	0	1.18e-02	4.41e-04	1.20	1.27	2205	947.4	693.2	0	1	1.4	2205	947	3.98	1024	13	1011	1.7	19
1.793	1	-50.0	3.60e-06	2.46e-05	+1.36	0.9925	1	44.1	11.9	62.0	37.3	10.0	16.20	0	1.12e-02	4.21e-04	2.18	1.57	2106	765.3	170.1	0	1	4.5	2106	765	0.92	1376	17	1360	4.8	20
1.918	1	-50.0	3.40e-06	2.00e-05	+1.45	0.9929	0	39.6	14.4	64.5	37.1	10.0	16.20	0	1.14e-02	4.44e-04	1.69	1.98	2219	860.5	629.6	0	1	1.4	2219	861	4.04	1024	15	1009	1.7	21
1.992	1	-50.0	3.70e-06	2.20e-05	+1.65	0.9935	0	36.6	12.4	63.0	36.9	10.0	16.20	0	9.48e-03	3.81e-04	2.16	3.21	1903	692.4	500.5	0	1	1.4	1903	692	2.97	984	16	969	1.7	22
2.066	1	-50.0	4.00e-06	1.34e-05	[illegible]	0.9951	0	39.6	16.4	62.5	37.3	10.0	15.80	0	1.12e-02	4.34e-04	1.16	1.43	2171	941.1	688.6	0	1	1.4	2171	941	3.26	1088	13	1075	1.7	23
[illegible]	1	-50.0	3.00e-06	[illegible]	[illegible]	[illegible]	0	41.1	17.4	61.5	37.5	10.0	[illegible]	0	[illegible]	4.63e-04	1.20	1.55	2317	994.1	718.6	0	1	1.4	2317	994	2.83	1216	14	1203	1.7	24
[illegible]	[illegible]	-50.0	3.80e-06	[illegible]	[illegible]	[illegible]	[illegible]	40.1	15.9	60.5	37.2	10.0	[illegible]	[illegible]	[illegible]	4.34e-04	1.37	2.30	2170	893.8	662.1	[illegible]	[illegible]	1.4	2170	894	1.17	1376	14	[illegible]	[illegible]	25
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	61.5	37.4	10.0	[illegible]	[illegible]	[illegible]	[illegible]	1.40	1.37	2195	897.3	[illegible]	[illegible]	[illegible]	[illegible]	2195	[illegible]	1.88	1280	14	[illegible]	[illegible]	26







Сжатие очищенных ключей универсальными хэш-функциями второго порядка

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

Сжатие очищенных ключей

Функция сжатия g(X) - универсальная хэш-функция

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

1) x, a={0,1, …….,0,0}

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

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

4) Взять отстаток r старших бит.

5) Ключ длины r.

Полиномы степени n<10 000.

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

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

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

Релятивистская квантовая криптография для открытого пространства

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

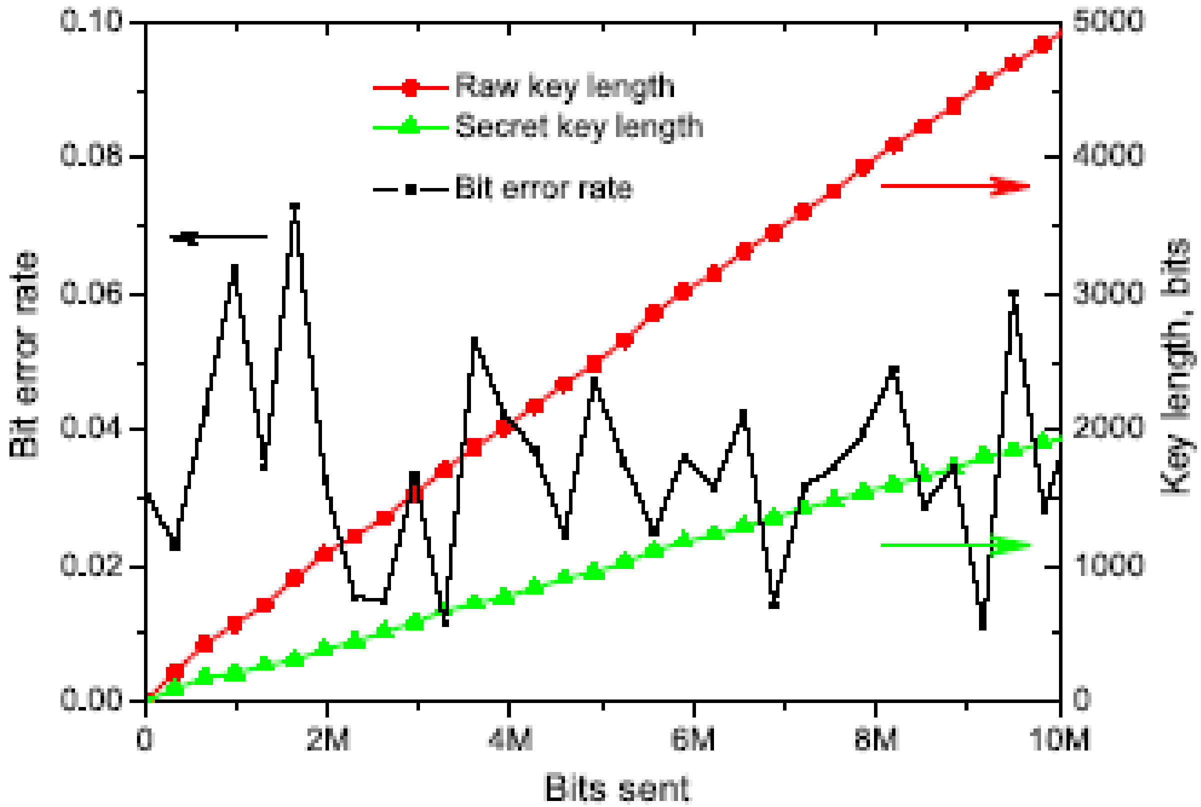


FIG. 4: **Experimentally measured bit error rate and the obtained key lengths.** During the run over 55 m long free space channel Alice was checking her observed timing sequence and compared it with that used by Bob. No timing errors were observed. Average number of photons per modulated pulse was kept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

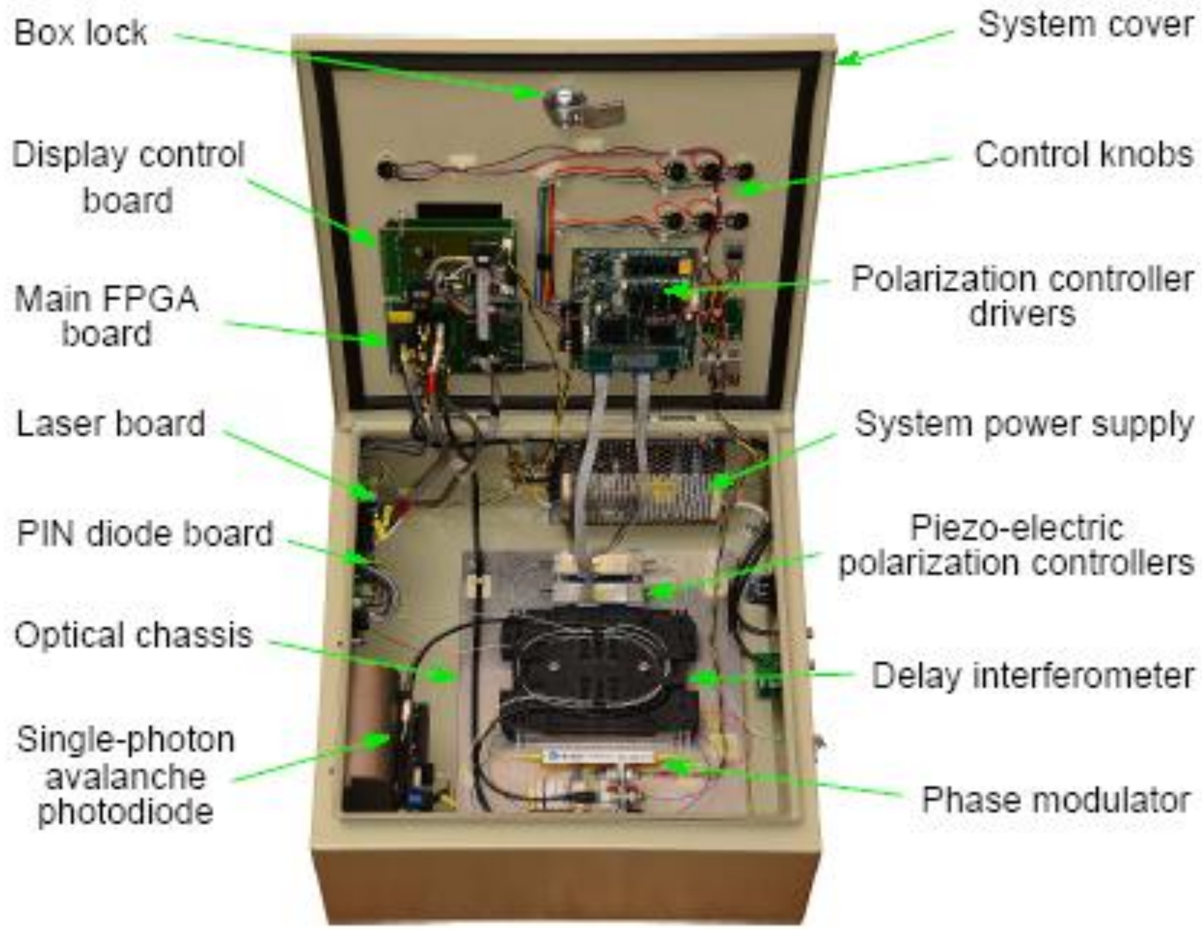


FIG. 6: **Hardware implementation of the Bob's station.** The station is packaged in a metal box with a cover, which has control knobs, buttons, and a small LCD display for visualization of the main operation parameters. It connects to a computer via a USB cable for transmission of the obtained raw keys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

О сложности перебора ключей в квантовой криптографии

Пусть в результате работы системы квантовой криптографии получен ε-секретный ключ, про который гарантируется, что $\frac{1}{2}||\rho_{XE} - \rho_U \otimes \rho_E||_1 < \varepsilon$. Вопрос: насколько ε-секретный ключ уменьшит число шагов (трудоемкость) перебора, в смысле, обсужденном ниже, по сравнению с идеальными ключами?

Что гарантирует квантовая криптография?

$$\rho_{XE} = \sum_{x \in X} P_X(x)|x\rangle\langle x| \otimes \rho_E^x$$

$$|x\rangle = |x_1\rangle \otimes |x_1\rangle \otimes \ldots |x_k\rangle, \quad |X| = 2^k$$

$$X = \{0,1\}^k$$

$$I_E = \sum_{y \in Y} \mathcal{M}_y, \quad y \in Y = \{0,1\}^k$$

$$P_{X|Y}(X = x|y) = \mathrm{Tr}\{\mathcal{M}_y \rho_E^x\}$$

$$P_{X|Y}(X = x|x) = \mathrm{Tr}\{\mathcal{M}_x \rho_E^x\}, \quad y = x.$$

$$P_{guess}(X|E) = \max_{\{\mathcal{M}_x\}} \sum_{x \in X} P_X(x) \mathrm{Tr}\{\mathcal{M}_x \rho_E^x\} =$$

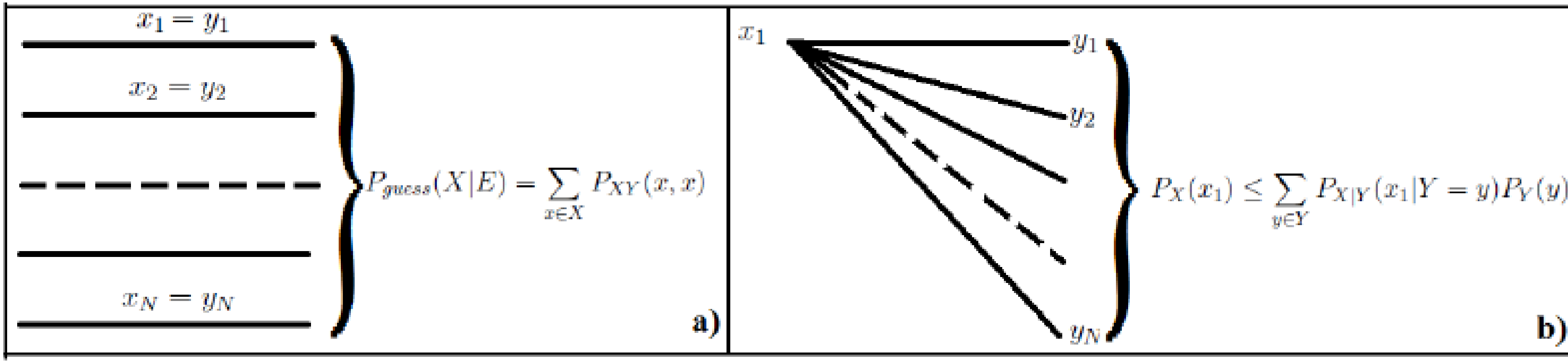
$$\sum_{x \in X} P_X(x) P_{X|Y}(X = x|x) = \sum_{x \in X} P_{XY}(x, x)$$

Квантовая криптография гарантирует

$$P_{guess}(X|E) = \sum_{x \in X} P_{XY}(x, x) \leq$$

$$\frac{1}{|X|} + \frac{1}{2} ||\rho_{XE} - \rho_U \otimes \rho_E||_1 = \frac{1}{2^k} + \varepsilon$$

$$\rho_U = \frac{1}{|X|} \sum_{x \in X} |x\rangle\langle x|, \quad \rho_E = \sum_{x \in X} P_X(x) \rho_E^x$$



$x_1 = y_1$
$x_2 = y_2$
$x_N = y_N$
$P_{guess}(X|E) = \sum_{x \in X} P_{XY}(x, x)$
a)
x_1
y_1
y_2
y_N
$P_X(x_1) \leq \sum_{y \in Y} P_{X|Y}(x_1|Y = y) P_Y(y)$
b)

следовое расстояние ($||\rho||_1 = \mathrm{Tr}\{|\rho|\} = \mathrm{Tr}\{\sqrt{\rho \cdot \rho^*}\}$)

Трудоемкость по перебору ключей (Guess Work)

$$G(X) = \sum_{i=1}^{N} i \cdot P_X(x_i)$$

$$G_U(X) = \sum_{i=1}^{N} i \cdot P_U(x_i) = \frac{N+1}{2}.$$

$$\frac{N+1}{2} - N||P_X - P_U||_1 \leq G(X) \leq \frac{N+1}{2} - \frac{N}{2}||P_X - P_U||_1$$

$$G(X|Y=y)=\sum_{i=1}^{N} i\cdot P_{X|Y}(x_i|Y=y)$$

$$G(X|Y=y)=\frac{N+1}{2}-\sum_{i=1}^{N} Q_i(X|Y=y)$$

$$Q_i(X|Y=y)=\sum_{j=1}^{i}\left(P_{X|Y}(x_j|Y=y)-P_U(x_j)\right)$$

$$G(X|Y) = \sum_{y\in Y} P_Y(y) G(X|Y=y) = \sum_{y\in Y} P_Y(y) \left(\frac{N+1}{2} - \sum_{i=1}^{N} Q_i(X|Y=y) \right) =$$

$$\frac{N+1}{2} - \sum_{i=1}^{N} \sum_{j=1}^{i} \left(\sum_{y\in Y} P_{X,Y}(x_j, y) - P_U(x_j) \right) = \frac{N+1}{2} - \sum_{i=1}^{N} \sum_{j=1}^{i} \left(P_X(x_j) - P_U(x_j) \right) =$$

$$= \frac{N+1}{2} - \sum_{i=1}^{N} Q_i(X), \quad Q_i(X) = \sum_{j=1}^{i} \left(P_X(x_j) - P_U(x_j) \right).$$

$$||P_X - P_U|| = Q_{max}(X) = \max_i Q_i(X) = \sum_{j=1, P_X(x_j) > P_U(x_j)}^{i} \left(P_X(x_j) - P_U(x_j) \right)$$

$$||P_X - P_U|| = \frac{1}{2} ||P_X - P_U||_1 = \frac{1}{2} \sum_{j=1}^{N} |P_X(x_j) - P_U(x_j)|$$

$$\frac{1}{2}||P_X - P_U||_1 \leq \frac{1}{2}||\rho_{XE} - \rho_U \otimes \rho_E||_1 \leq \varepsilon$$

$$\rho_X = \mathrm{Tr}_E\{\rho_{XE}\} = \sum_{x \in X} P_x(x)|x\rangle\langle x|$$

$$\rho_U = \mathrm{Tr}_E\{\rho_U \otimes \rho_E\} = \sum_{x \in X} P_U(x)|x\rangle\langle x|, \quad P_U(x) = \frac{1}{|X|}$$

$$G(X|Y) \geq \frac{N+1}{2} - \sum_{i=1}^{N} max_i\, Q_i(X) =$$

$$\frac{N+1}{2} - N||P_X - P_U||_1 \geq \frac{N(1-2\varepsilon)}{2} + \frac{1}{2}$$

$$\frac{N(1-2\varepsilon)}{2}+\frac{1}{2}\le G(X|Y)\le\frac{N(1-\varepsilon)}{2}+\frac{1}{2},\quad N=|X|=2^k$$

Связь между трудоемкостью перебора и максимальной вероятностью угадывания за один шаг

$$P_X(x_1)\le\sum_{y\in Y}P_{X|Y}(x_1|Y=y)P_Y(y)$$

$$=1-\frac{2}{N}(G(X|Y)-1)\le\frac{1}{N}+2\varepsilon$$

СПАСИБО ЗА ВНИМАНИЕ.