Фестиваль науки в МГУ
28 октября 2006 г.

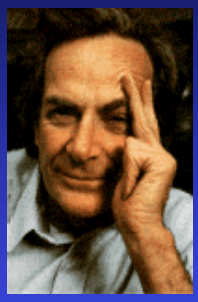
Квантовые компьютеры и квантовые вычисления: Мечты и реальность

Виктор Задков
Физический факультет, МГУ им. М.В.Ломоносова

Начало эры квантовых компьютеров

"There's plenty of room at the bottom."
— Richard Feynman[*)]

"…it seems that the laws of physics present no barrier to reducing the size of computers until bits are the size of atoms, and quantum behavior holds dominant sway."
— Richard Feynman[**)]

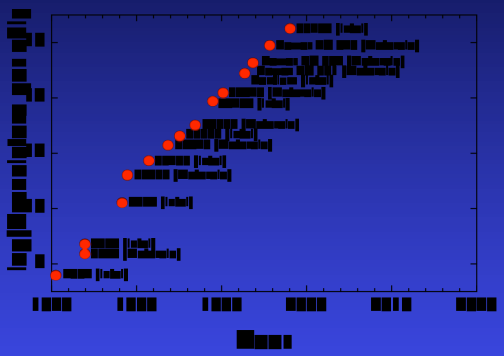


Richard P. Feynman

[*)] R.P.Feynman, "There's plenty of room at the bottom," *Engineering and Science*, vol. 23, pp.22-36 (1960).

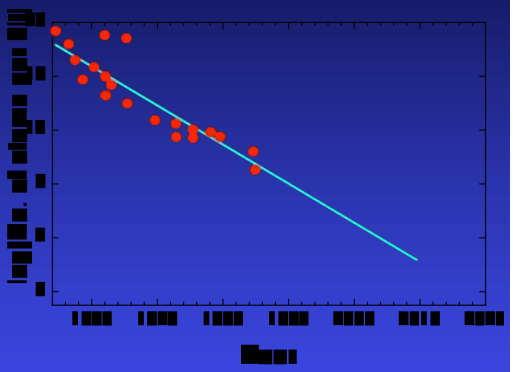
[**)] R.P.Feynman, "Quantum mechanical computers," *Optics News*, vol. 11, pp. 11-20 (1985).

Развитие технологий микроэлектроники



Logarithm of the number of transistors per chip as a function of calendar year and the processors that achieved these transistor densities.

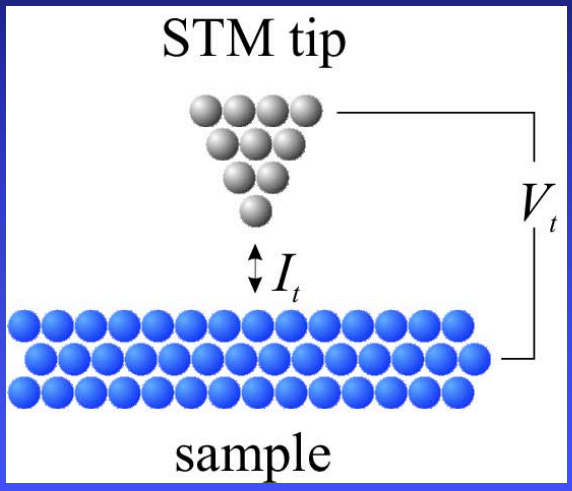
Adapted from: G.D.Hutcheson, J.D.Hutcheson, "Technology and economics in the semiconductor industry," Scientific American, January, pp.54–62 (1996)

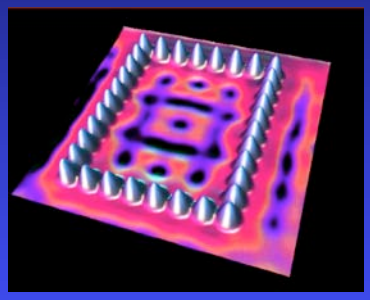


The number of atoms needed to represent one bit of information as a function of calendar year. Extrapolation of the trend suggests that the one-atom-per-bit level is reached in about the year 2020.

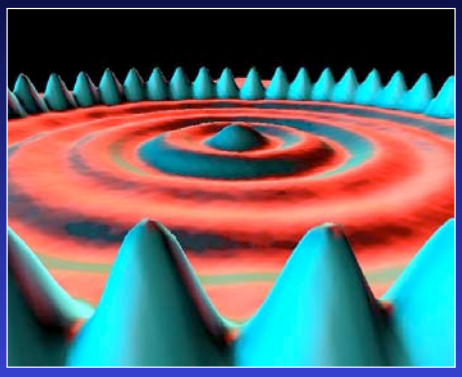
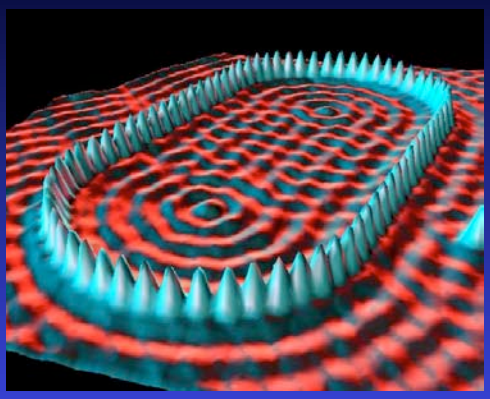
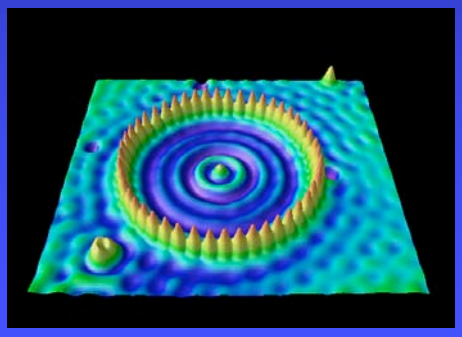
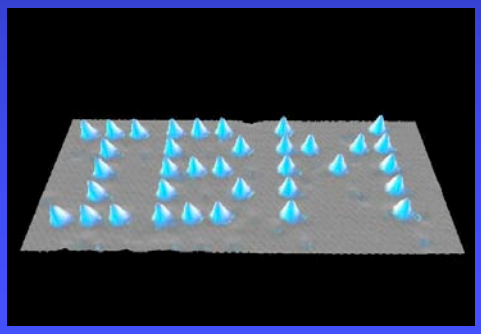
Adapted from: R.W.Keyes, "Miniaturization of electronics and its limits," IBM Journal of Research and Development, vol. 32, January, pp. 24–28 (1988).

Сканирующая туннельная микроскопия (СТМ)





STM/STS image

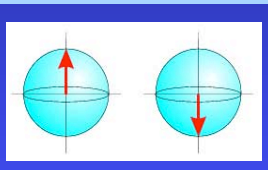
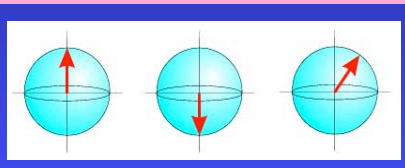
Биты и кубиты

Классический бит

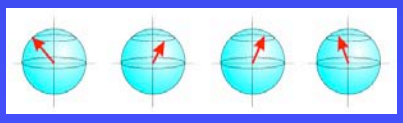
Принимает только два состояния
“0” и “1”

Квантовый бит (qubit*)

$|\Psi\rangle = a|0\rangle + b|1\rangle$
принимает два “классических” состояния:
“0”: $|\Psi\rangle_0 = 1|0\rangle + 0|1\rangle = |0\rangle$
“1”: $|\Psi\rangle_1 = 0|0\rangle + 1|1\rangle = |1\rangle$
и все состояния “между ними”

Фазы векторов являются исключительно важными для эффектов квантовой интерференции



*)This term was coined by Schumacher (Phys. Rev. A51, 2738 (1995)

Классические логические элементы

NOT

a	NOT a
0	1
1	0

AND

a	b	a AND b
0	0	0
0	1	0
1	0	0
1	1	1

OR

a	b	a OR b
0	0	0
0	1	1
1	0	1
1	1	1

Reversible OR

a	b	a	a OR b
0	0	0	0
0	1	0	1
1	0	1	1
1	1	1	1

- Фундаментальный набор элементов (NOT, AND, and OR)
- Эти элементы (кроме NOT) являются логически необратимыми
- Необратимые элементы генерируют энергию при работе
- Необратимые элементы можно сконвертировать в обратимые

Квантовые логические элементы

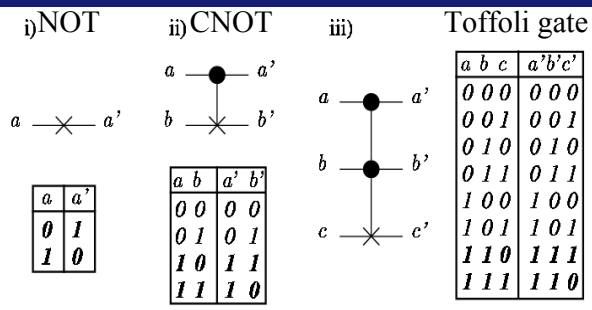


FIG. 5. Truth tables and graphical representations of the elementary quantum gates used for the construction of more complicated quantum networks. The control qubits are graphically represented by a dot, the target qubits by a cross. i) NOT operation. ii) Control–NOT. This gate can be seen as a "copy operation" in the sense that a target qubit (b) initially in the state 0 will be after the action of the gate in the same state as the control qubit. iii) Toffoli gate. This gate can also be seen as a Control–control–NOT: the target bit (c) undergoes a NOT operation only when the two controls (a and b) are in state 1.

Квантовое вычислительное устройство (процессор) строится из простейших квантовых логических элементов, работающих синхронно по времени

Source: V.Vedral, M.B.Plenio, Progr. Quant. Electron., vol. 22, pp. 1–40 (1998)

Простое квантовое вычислительное устройство

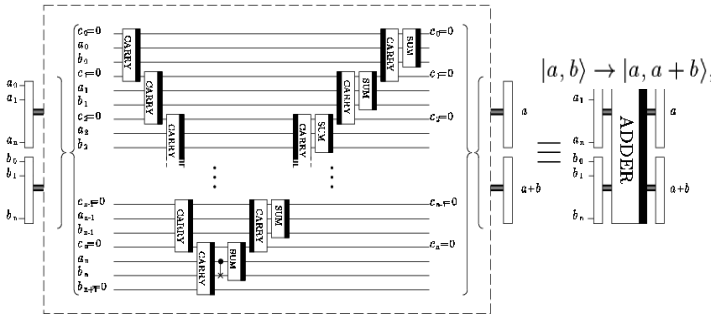
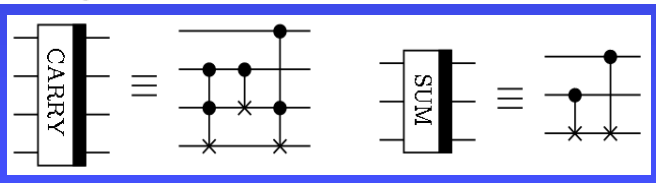


FIG. 6. Plain adder network. In a first step, all the carries are calculated until the last carry gives the most significant digit of the result. Then all these operations apart from the last one are undone in reverse order, and the sum of the digits is performed correspondingly. Note the position of a thick black bar on the right or left hand side of basic carry and sum networks. A network with a bar on the left side represents the reversed sequence of elementary gates embedded in the same network with the bar on the right side.

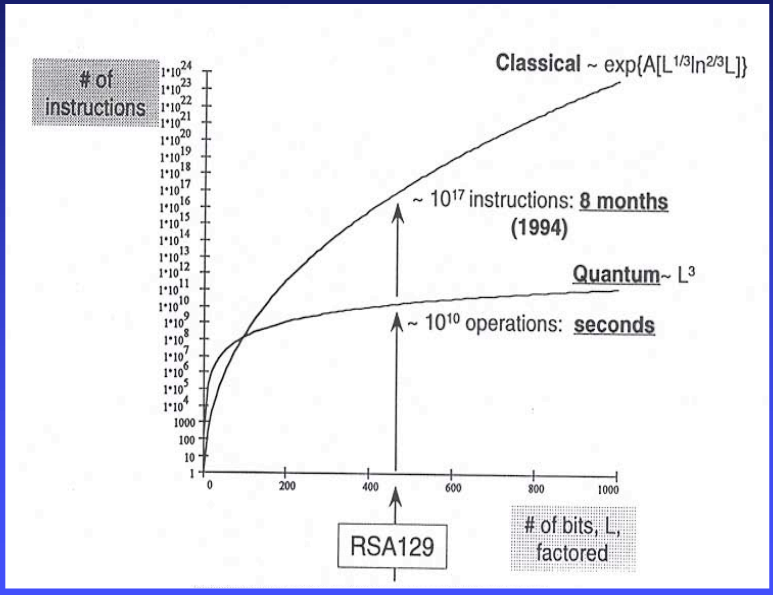


Source: V.Vedral, M.B.Plenio, Progr. Quant. Electron., vol. 22, pp. 1–40 (1998)

Ключевое преимущество квантовых компьютеров

- Фундаментальная работа Deutsch (1985)
  - Квантовые компьютеры могут естественным образом выполнять (вычислять) динамику суперпозиции квантовых состояний вплоть до конечного измерения
- Такой “квантовый параллелизм” может потенциально служить основой алгоритмов, которые работают существенно быстрее любых самых быстрых классических алгоритмов

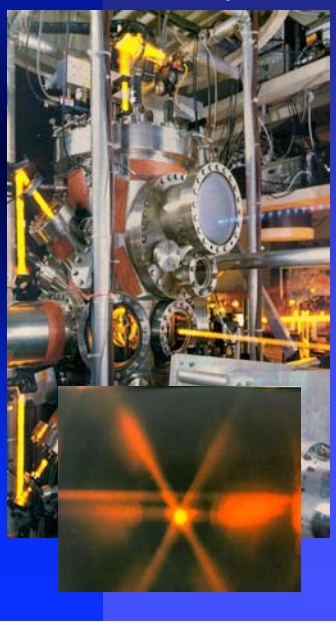
КК взламывает секретные коды быстрее любых классических ЭВМ



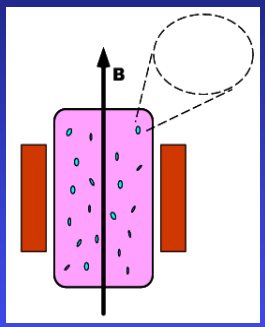
Используется алгоритм Шора (Shor) для факторизации целых чисел

Экспериментальные прототипы квантовых компьютеров

Atoms-based QC

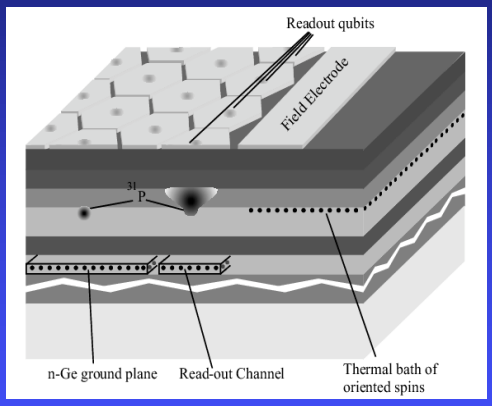


NMR-based QC

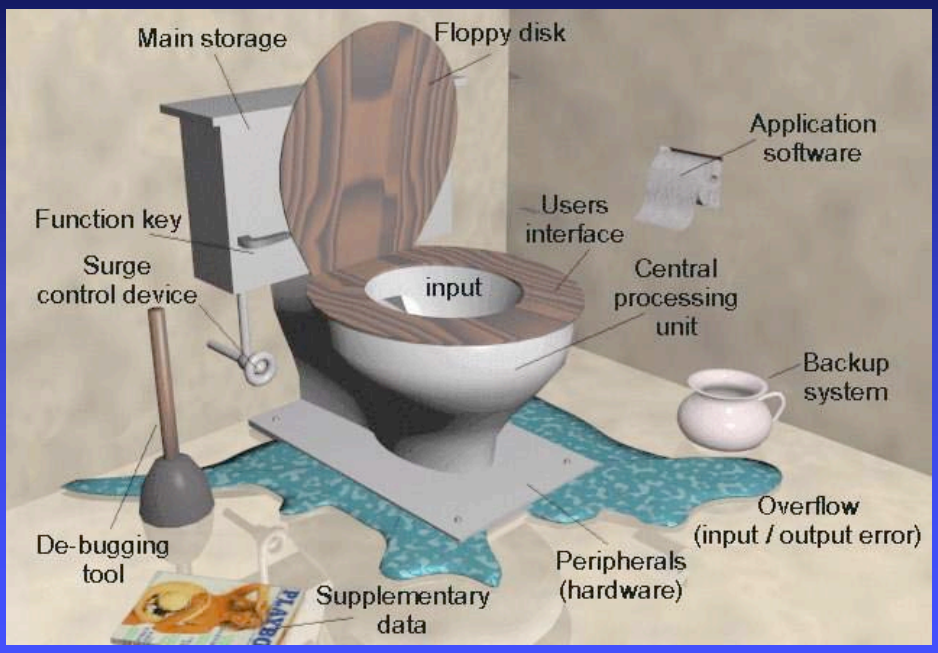


Qubit is implemented as the spin state of one of the nuclei in the atoms comprising each molecule of the sample

Solid-state based QC



Устройство компьютера на “бытовом уровне”



Квантовая криптография

Современная криптография основана на:

Теория сложности

Ключ является публичным

С помощью этого ключа можно вычислить декодирующий ключ, однако при помощи очень сложного алгоритма

Секретность не доказана

Пример:

127 x 229 = 29083

Теория информации

Ключ является секретным

Только два партнера знают ключ!

В этом случае секретность доказана (теорема Шеннона)

Пример:

Message:	011001001
Key:	110100110
Coded message:	101101111

Квантовая криптография: замечательная идея

- Квантовая механика утверждает, что любые квантовые измерения изменяют состояние измеряемой системы
  - Квантовыми носителями информации являются одиночные фотоны
  - Если Ева попытается подслушать «квантовый канал данных", она будет вынуждена проводить измерения на индивидуальных фотонах.
  - Однако, квантовая механика утверждает, что каждое измерение возмущает квантовую систему.
  - Поэтому «чтение/подслушивание" информации в квантовом канале третьим лицом (Ева) изменяет корреляции между данными Алисы и Боба.
  - Таким образом, Алиса и Боб могут определить наличие подслушивания информации в квантовом канале путем сравнения (по публичному каналу) части их квантового сигнала.

Квантовая криптография: замечательная идея (продолж.)

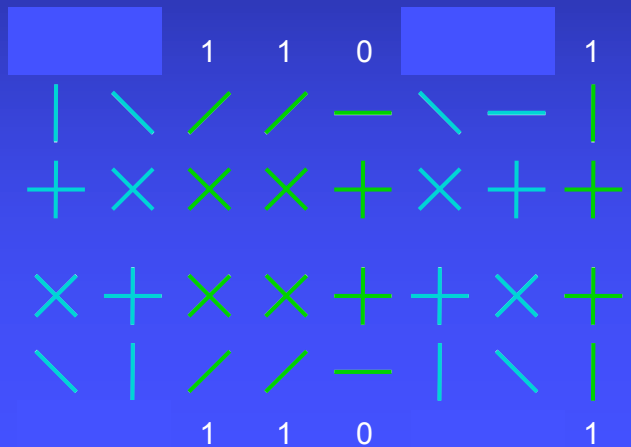
- Квантовый канал не используется для передачи самих данных, передается только ключ для декодирования информации.
- Если ключ был украден (подслушан), Алиса и Боб просто игнорируют его (при этом информация не теряется).
- Если переданный ключ успешно прошел проверку, он может быть использован для декодирования данных.
- Конфиденциальность ключа проверяется до передачи данных.
- Надежность квантовой криптографии основана на природе квантовой физики и гарантируется ее законами.

Протокол передачи квантового ключа (QKD)

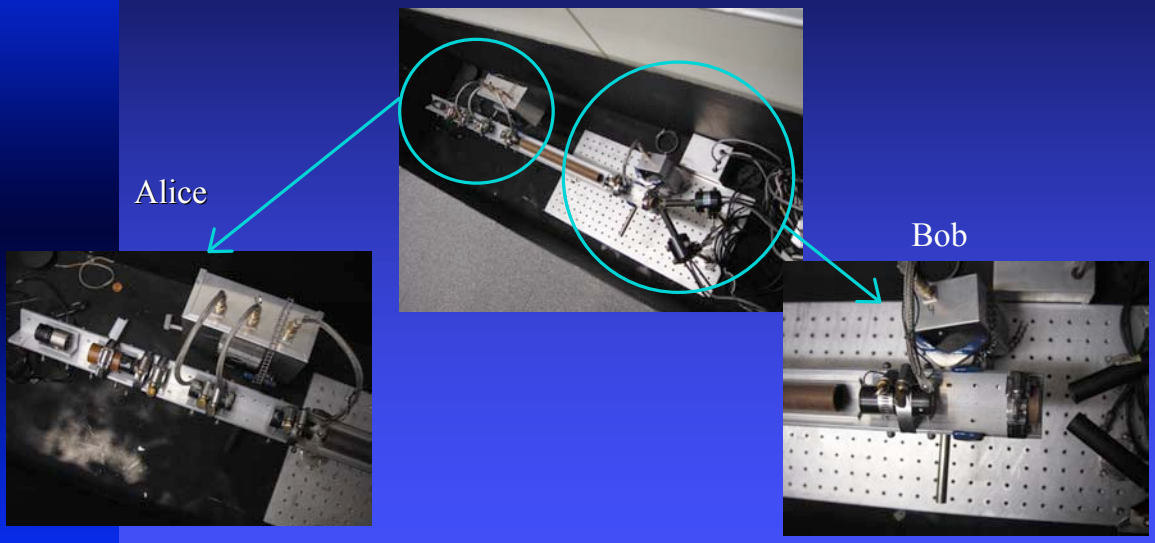
1) Передача сырого ключа
   - Алиса кодирует каждый бит информации случайной буквой и передает ее Бобу
   - Боб измеряет полученную букву в случайном базисе
2) Согласование базисов (формирование просеянного ключа)
   - Боб сообщает Алисе базис, который он использовал при измерениях
   - Алиса отбирает только те сообщения, в которых был использован этот базис

Alice

Bob



Экспериментальная реализация протокола QKD



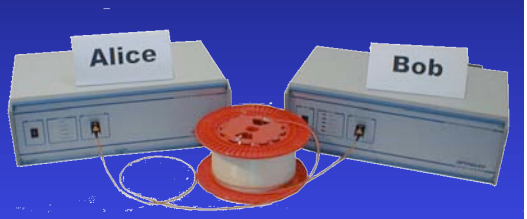
Ch. H. Bennett and G. Brassard, "The Dawn of a New Era for Quantum Cryptography: The Experimental Prototype Is Working!," Sigact News 20, No. 4, 78 – 82 (Fall 1989).

Коммерческое производство систем квантовой криптографии

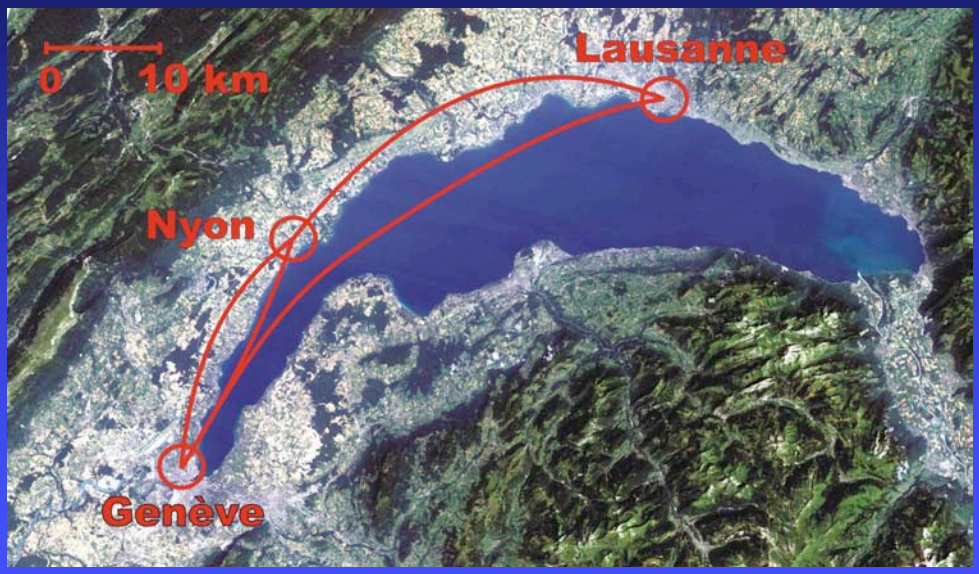
- Компания основана в 2001 г. как spin-off от университета г. Женевы
- Продукция
  - Системы для квантовой криптографии (на оптическом волокне)
  - Генератор случайных чисел
  - Детектор одиночных фотонов (1.3 мкм и 1.55 мкм)
- Контактная информация:

email: info@idquantique.com

web: http://www.idquantique.com



Реализация протокола квантовой криптографии на расстоянии 67 км



RMP 74, 145-195, 2002, Quant-ph/0101098

Спасибо за внимание!