Ассоциация РусКрипто

РусКрипто 2015

Ассоциация РусКрипто

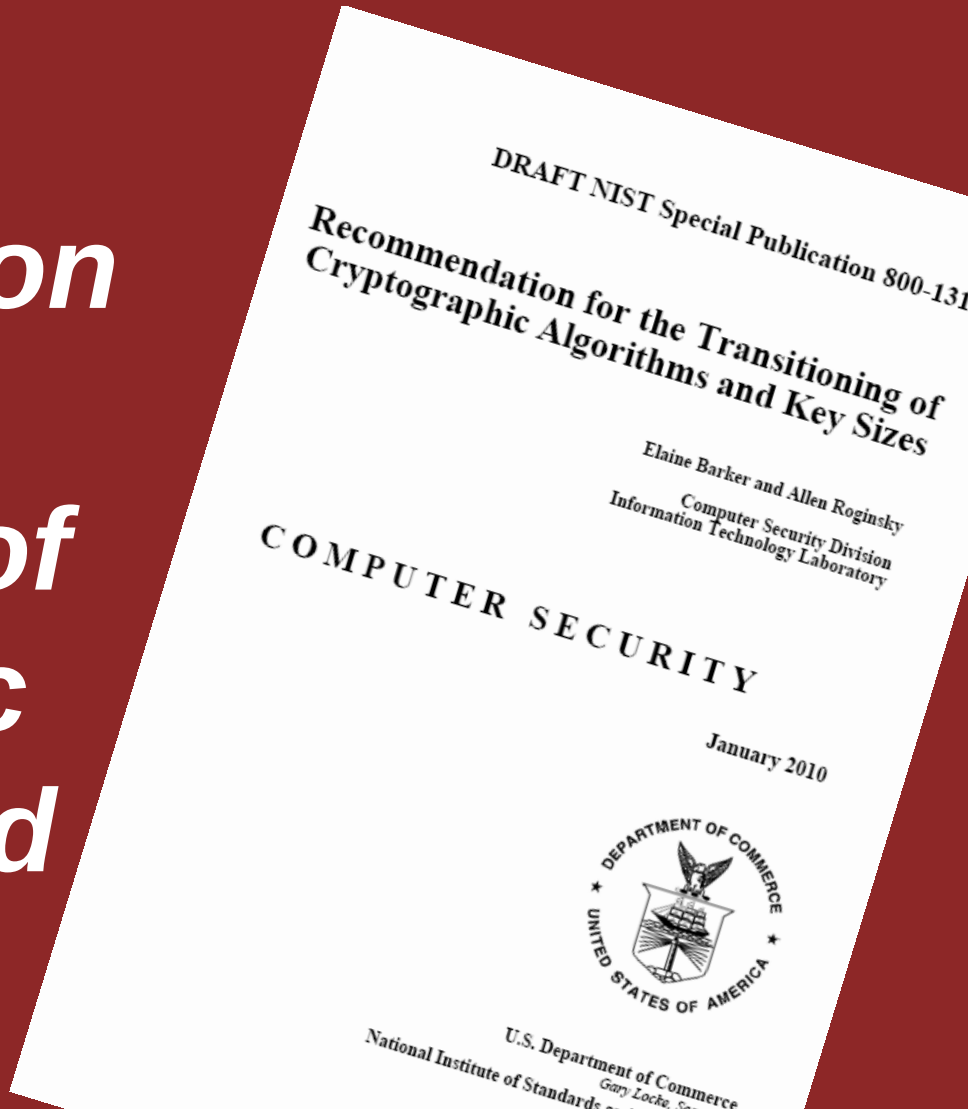
Вычислительные технологии и криптография

Ассоциация РусКрипто

Сравнительная стойкость криптоалгоритмов и сроки их действия

SP 800-131

Recommendation for the Transitioning of Cryptographic Algorithms and Key Sizes


DRAFT NIST Special Publication 800-131

Recommendation for the Transitioning of Cryptographic Algorithms and Key Sizes

Elaine Barker and Allen Roginsky

Computer Security Division
Information Technology Laboratory

COMPUTER SECURITY

January 2010

DEPARTMENT OF COMMERCE
UNITED STATES OF AMERICA

U.S. Department of Commerce

Ассоциация РусКрипто

Сравнительная стойкость криптоалгоритмов и сроки их действия

Bits of security	Symmetric key algorithms	FFC (DSA, D-H, MQV)	IFC (RSA)	ECC (ECDSA)
80 (до 2010 г.)	2TDEA, SKIPJACK,	$L = 1024$ $N = 160$	$k = 1024$	$f = 160\text{-}223$
112 (до 2030 г.)	3TDEA	$L = 2048$ $N = 224$	$k = 2048$	$f = 224\text{-}255$
128 (после 2030 г.)	AES-128	$L = 3072$ $N = 256$	$k = 3072$	$f = 256\text{-}383$
192	AES-192	$L = 7680$ $N = 384$	$k = 7680$	$f = 384\text{-}511$
256	AES-256	$L = 15360$ $N = 512$	$k = 15360$	$f = 512+$

Ассоциация РусКрипто

The Machine

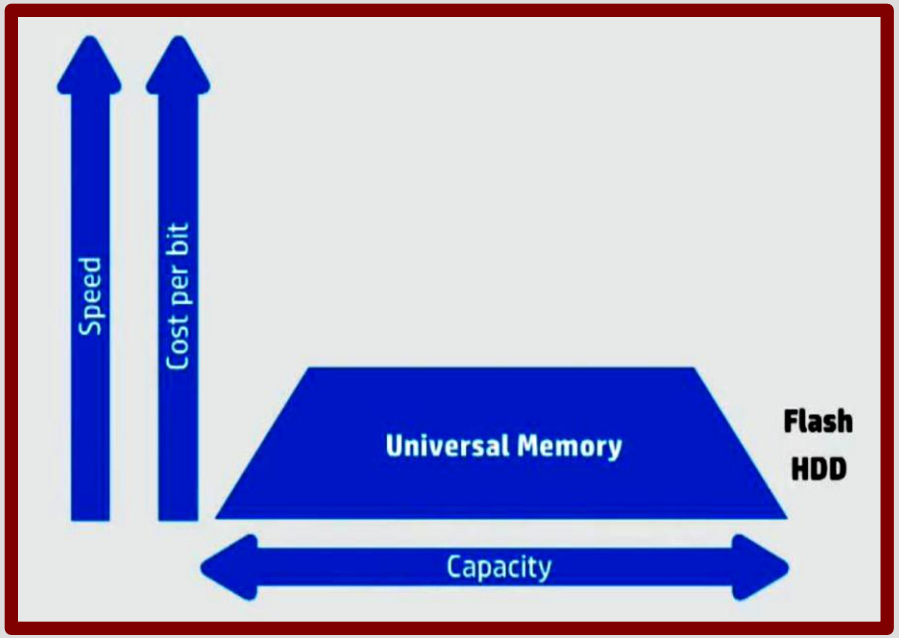
The Machine:
The future of technology

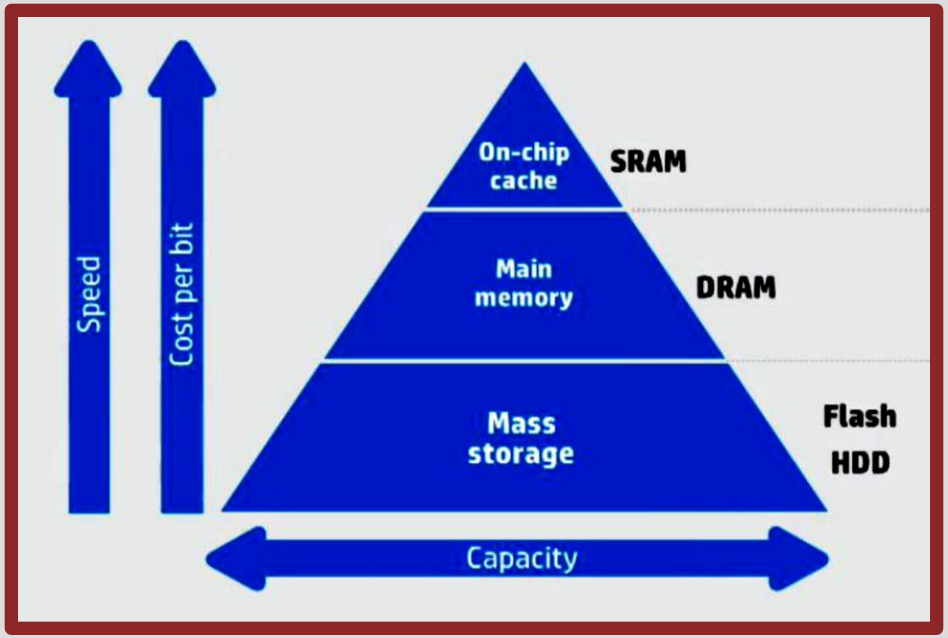
HP Labs

2014

Ассоциация РусКрипто

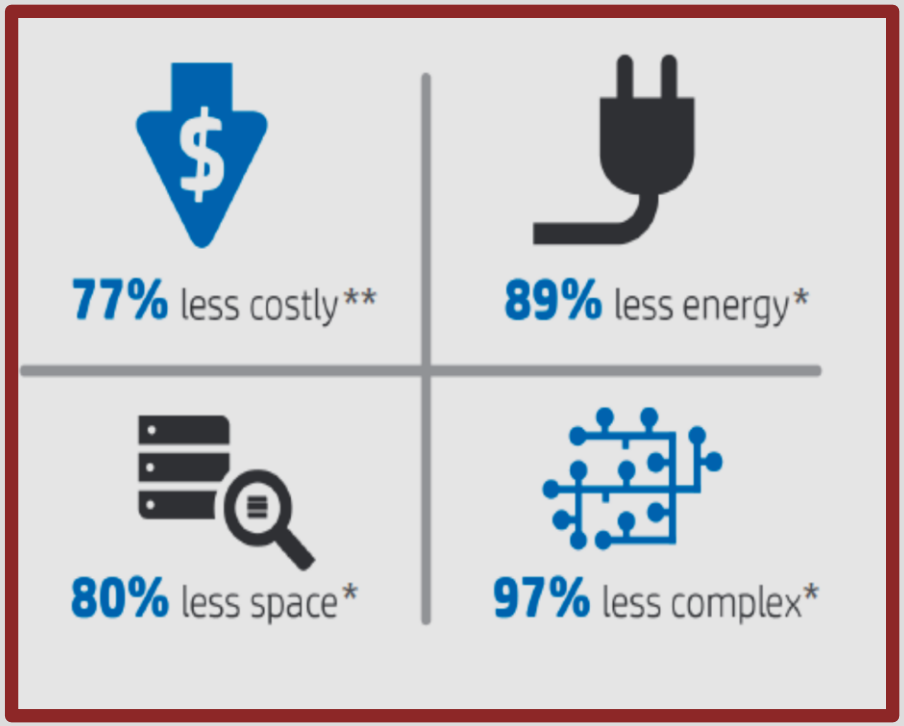
The Machine

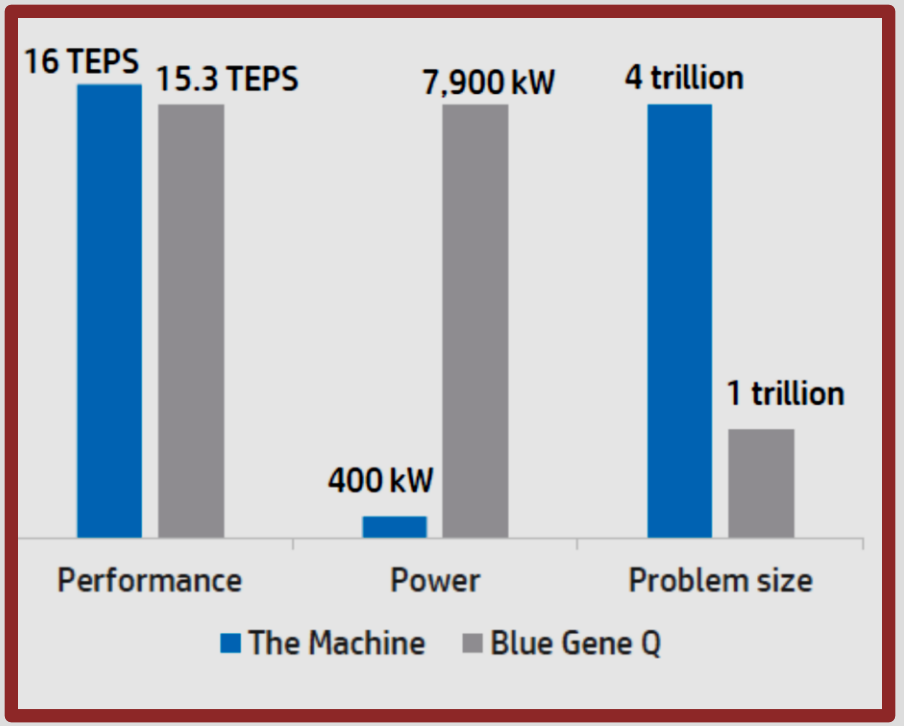




Ассоциация РусКрипто

The Machine





Ассоциация РусКрипто

Квантовый компьютер

Ассоциация РусКрипто

Квантовый компьютер

Агентство Национальной Безопасности строит квантовый компьютер.

Э.Сноуден

Ассоциация РусКрипто

Квантовый компьютер

Квантовая «угроза» криптографии

Ассоциация РусКрипто

Квантовый компьютер

- Квантовый компьютер — вычислительное устройство, использующее в своей работе законы квантовой механики.
- Способен реализовывать вычисления, недоступные в реальное время для классических компьютеров.

Ассоциация РусКрипто

Квантовый компьютер

- **Идея о квантовых вычислениях была высказана Ю.И. Маниным в 1980 году.**

Ю. И. Манин
Вычислимое и невычислимое. — М.: Сов. радио, 1980

Ассоциация РусКрипто

Квантовый компьютер

- **Первая модель квантового компьютера была предложена Р. Фейнманом в 1981 г.**

Feynman, R.P. *Simulating physics with computers* // International Journal of Theoretical Physics, v.21, №6 (1982), pp. 467 - 488

Ассоциация РусКрипто

Квантовый компьютер

- **Вскоре П. Бениофф описал теоретические основы построения такого компьютера.**

Benioff P. *Quantum Mechanical Hamiltonian Models of Turing Machines* // Journal of Statistical Physics, 29 (3) (1982) , pp. 515 - 546.

Ассоциация РусКрипто

Квантовый компьютер

- **Д. Дейч математически строго сформулировал понятие квантового вычисления.**

Deutsch D. *Quantum theory, the Church-Turing principle and the universal quantum computer.* Proc. Royal Society London Ser. A400, pp. 97-117 (1985)

Ассоциация РусКрипто

Физические реализации квантовых компьютеров

- Построение квантового компьютера в виде реального физического прибора является фундаментальной задачей физики XXI века.
- В настоящее время построены только ограниченные его варианты.
- Вопрос о масштабировании такого устройства — предмет интенсивно развивающейся области — *многочастичной квантовой механики*.

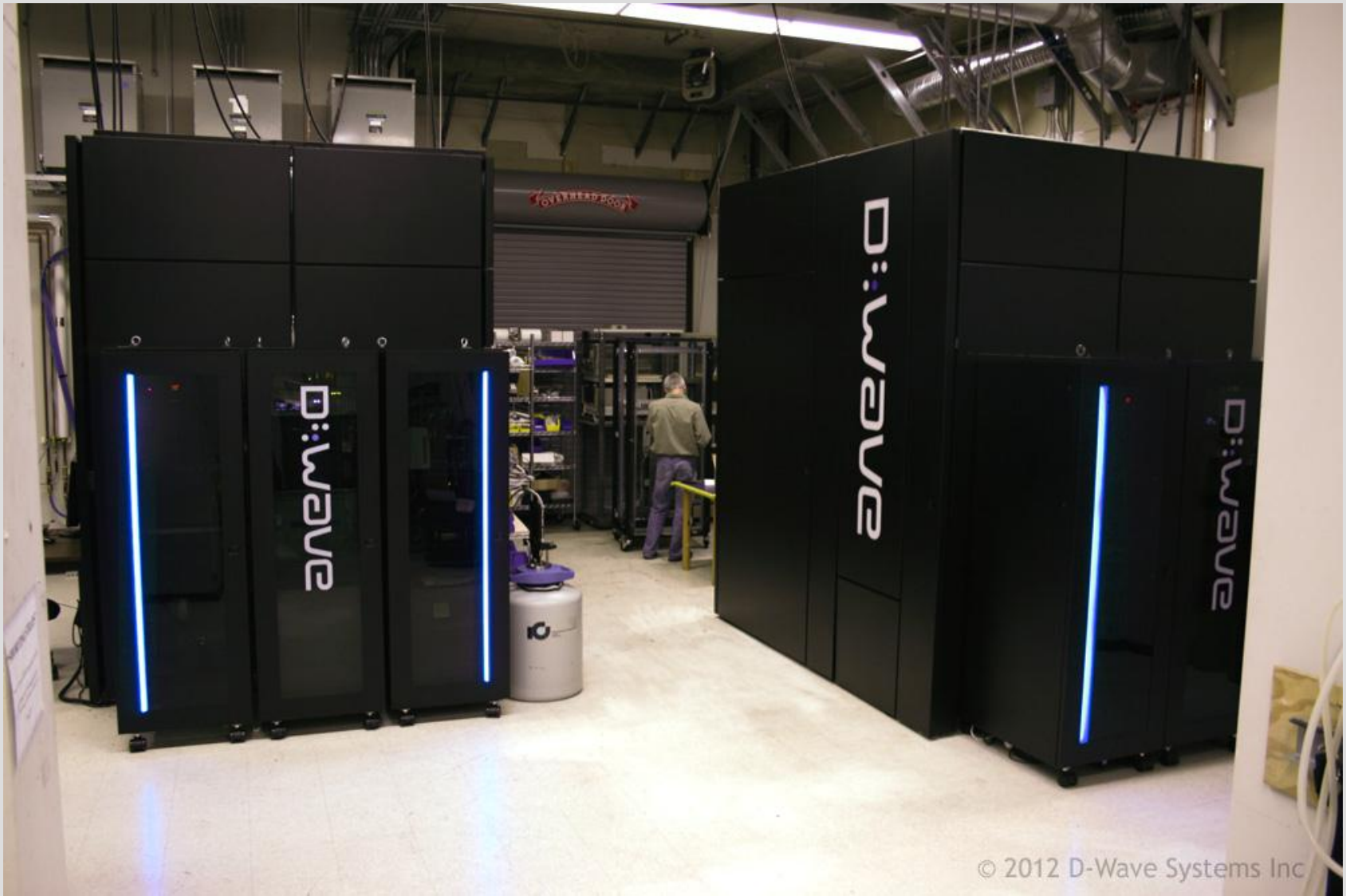
Ассоциация РусКрипто

Этапы развития квантового компьютера

- 1981 г. – предложена модель квантового компьютера и созданы теоретические основы построения
- 2000 г. – квантовый компьютер из 1 кубита
- 2001 г. – квантовый компьютер из 2 кубит
- 2003 г. – квантовый компьютер из 7 кубит
- 2005 г. – квантовый компьютер из 10 кубит

Ассоциация РусКрипто

Компьютеры D-Wave



Ассоциация РусКрипто

Компьютеры D-Wave

Канадская компания D-Wave Systems в феврале 2007 года заявила о создании образца квантового компьютера, состоящего из 16 кубит (устройство получило название *Orion*).

Ассоциация РусКрипто

Компьютеры D-Wave

В ноябре 2007 года компания *D-Wave* продемонстрировала работу образца 28-кубитного компьютера (устройство получило название *Leda*)

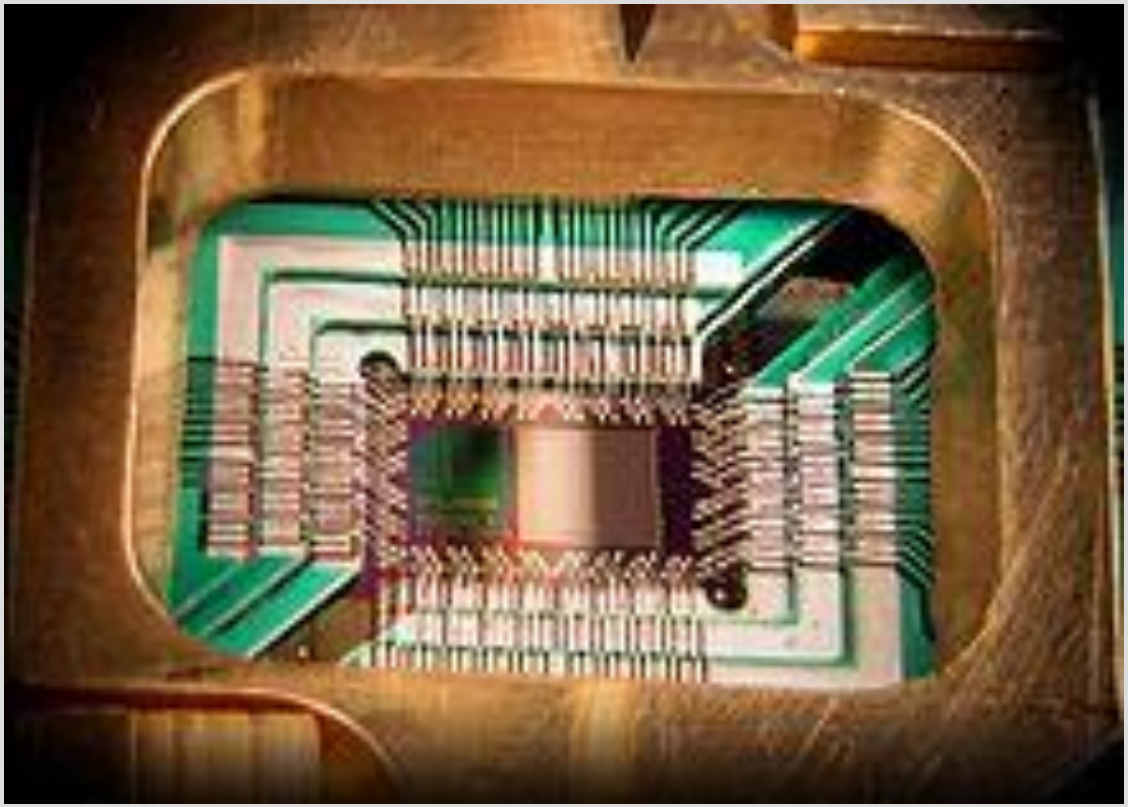
Ассоциация РусКрипто

Компьютеры D-Wave

11 мая 2011 г. представлен компьютер *D-Wave One*, созданный на базе 128-кубитного процессора.

Ассоциация РусКрипто

Компьютеры D-Wave



Photograph of a chip constructed by D-Wave Systems Inc., designed to operate as a 128-qubit superconducting adiabatic quantum optimization processor

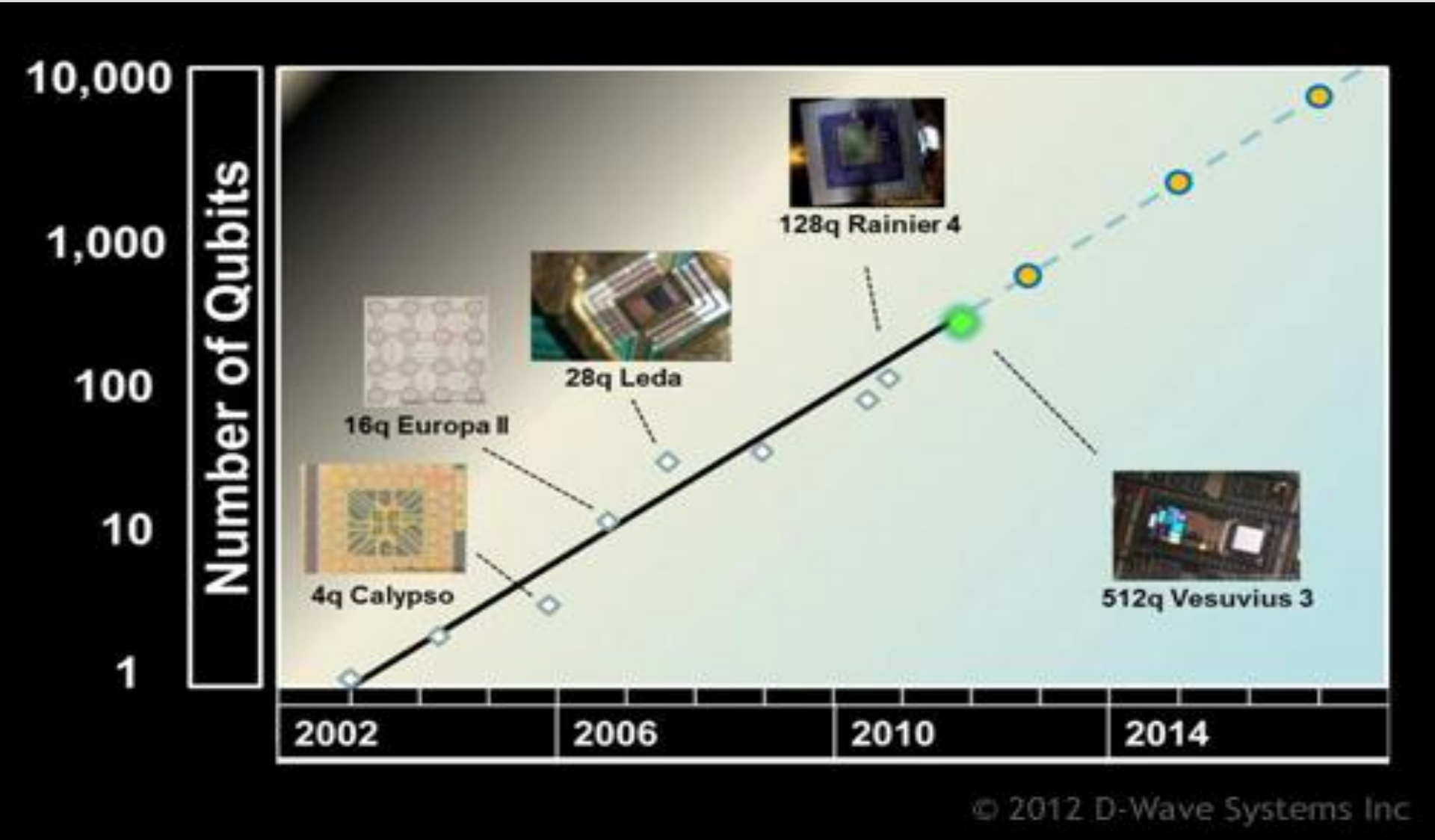
Ассоциация РусКрипто

Компьютеры D-Wave

В декабре 2012 года представлен новый процессор *Vesuvius*, который объединяет 512 кубитов.

Ассоциация РусКрипто

~~«Moore's Law»~~
«Rose's law»



Ассоциация РусКрипто

Компьютеры D-Wave

Ассоциация
РусКрипто

Квантовые алгоритмы и криптография

Ассоциация РусКрипто

Квантовый компьютер

Квантовая «угроза» криптографии

Ассоциация РусКрипто

Квантовые алгоритмы

- Квантовые вычисления позволяют решать лишь некоторые определенные проблемы, но очень эффективно.
- Беннетт: для любого классического вычисления существует квантовое той же эффективности.

Ассоциация РусКрипто

Квантовые алгоритмы

- В начале 90-х были открыты первые истинно квантовые алгоритмы, алгоритмы без классических аналогов, которые были доказано быстрее, чем любой классический алгоритм.

Ассоциация РусКрипто

Квантовые алгоритмы

- Алгоритм Саймона
- Алгоритм Залки — Визнера
- Алгоритм Дойча — Йожи
- Алгоритм Гровера
- Алгоритм Шора

Ассоциация РусКрипто

Квантовые алгоритмы

- **Алгоритм Гровера (квантовый перебор).**

Grover L.K. A fast quantum mechanical algorithm for database search // Proc. of 28th STOC, Philadelphia PA USA, 1996. – pp. 212-219.

Ассоциация РусКрипто

Нахождение ключа симметричной криптосистемы тотальным перебором

Классический компьютер

$$O(|K|) \sim 2^n$$

Квантовый компьютер

$$O\left(|K|^{1/2}\right) \sim 2^{n/2}$$

Ассоциация РусКрипто

Квантовые алгоритмы

Алгоритм Гровера

$$|K| = 2^n \Rightarrow \begin{cases} time = \frac{\pi}{4}\sqrt{2^n} \\ space = O(n) \end{cases}$$

$$O(|K|) \sim 2^n$$

$$O\left(|K|^{1/2}\right) \sim 2^{n/2}$$

Ассоциация РусКрипто

Квантовые алгоритмы

- **Алгоритм Шора**

Shor P.W. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on Quantum Computer, Proc. 35th Ann. Symp. on Foundations of Computer Science, Santa Fe, NM, Nov. 20-22, 1994, IEEE Computer Society Press, pp 124-134

Ассоциация РусКрипто

Квантовые алгоритмы

- **Алгоритм Шора позволяет разложить натуральное число N на простые множители за полиномиальное от $n = \log(N)$ время.**

$$n = \log N \Rightarrow O\left(n^2 \log n \log\log n\right)$$

Ассоциация РусКрипто

Задачи дискретного логарифмирования и факторизации

Классический компьютер

Квантовый компьютер

$$n = \log N$$

$$O\left(e^{cn^{1/2}\log^{1/2} n}\right)$$

$$O\left(e^{cn^{1/3}\log^{2/3} n}\right)$$

$$O\left(n^2 \log n \log\log n\right)$$

Ассоциация РусКрипто

Задачи дискретного логарифмирования и факторизации

Алгоритм квадратичного решета (QNS — quadratic number sieve)

$$O\left(e^{cn^{1/2}\log^{1/2}n}\right)$$

$$O\left(e^{cn^{1/3}\log^{2/3}n}\right)$$

Алгоритм решета числового поля (GNFS — general number field sieve)

Ассоциация РусКрипто

Задачи дискретного логарифмирования и факторизации

Алгоритм Шора

Квантовый компьютер

$$O\left(n^2 \log n \log\log n\right)$$

$$O\left(e^{cn^{1/2}\log^{1/2} n}\right)$$

$$O\left(e^{cn^{1/3}\log^{2/3} n}\right)$$

Ассоциация РусКрипто

Задача дискретного логарифмирования в группе ЕС

Классический компьютер

Квантовый компьютер

$$n = \log N$$

$$O(N^{1/2}) = O\left(e^{n/2}\right)$$

$$O\left(n^2 \log n \log\log n\right)$$

Ассоциация РусКрипто

Сравнительная стойкость криптоалгоритмов и сроки их действия

Bits of security	Symmetric key algorithms	FFC (DSA, D-H, MQV)	IFC (RSA)	ECC (ECDSA)
80 (до 2010 г.)	2TDEA, SKIPJACK,	$L = 1024$ $N = 160$	$k = 1024$	$f = 160\text{-}223$
112 (до 2030 г.)	3TDEA	$L = 2048$ $N = 224$	$k = 2048$	$f = 224\text{-}255$
128 (после 2030 г.)	AES-128	$L = 3072$ $N = 256$	$k = 3072$	$f = 256\text{-}383$
192	AES-192	$L = 7680$ $N = 384$	$k = 7680$	$f = 384\text{-}511$
256	AES-256	$L = 15360$ $N = 512$	$k = 15360$	$f = 512+$

Ассоциация РусКрипто

Квантовые алгоритмы

Ресурсы для квантового решения задач факторизации и ECDLP

	Факторизация		ECDLP			кл. время
n	число кубитов	квант. время	n	число кубитов	квант. время	
512	1024	$0{,}54 \cdot 10^9$	110	700	$0{,}5 \cdot 10^9$	$6{,}4 \cdot 10^{16}$
1024	2048	$4{,}3 \cdot 10^9$	163	1000	$1{,}6 \cdot 10^9$	$3{,}0 \cdot 10^{24}$
2048	4096	$34 \cdot 10^9$	224	1300	$4{,}0 \cdot 10^9$	$9{,}2 \cdot 10^{33}$
3072	6114	$120 \cdot 10^9$	256	1500	$6{,}0 \cdot 10^9$	$6{,}0 \cdot 10^{38}$
15360	30720	$1{,}5 \cdot 10^{13}$	512	2800	$50 \cdot 10^9$	$2{,}1 \cdot 10^{77}$

Ассоциация РусКрипто

Квантовые алгоритмы

Ресурсы для квантового решения задачи поиска ключа симметричной криптосистемы

k	число кубитов	квантовое время	классическое время
56	56	$2{,}1 \cdot 10^{8}$	$7{,}2 \cdot 10^{16}$
80	80	$8{,}6 \cdot 10^{11}$	$1{,}2 \cdot 10^{24}$
112	112	$5{,}7 \cdot 10^{16}$	$5{,}2 \cdot 10^{33}$
128	128	$1{,}4 \cdot 10^{19}$	$3{,}4 \cdot 10^{38}$
168	168	$1{,}5 \cdot 10^{25}$	$3{,}7 \cdot 10^{50}$
256	256	$2{,}7 \cdot 10^{38}$	$1{,}2 \cdot 10^{77}$

Ассоциация РусКрипто

Квантовые алгоритмы

- Не для всякого алгоритма возможно «квантовое ускорение». Более того, возможность получения квантового ускорения для произвольного классического алгоритма является большой редкостью.

Ассоциация РусКрипто

Квантовая криптография

Квантовое «спасение» криптографии

Ассоциация РусКрипто

Квантовая криптография

- **Квантовая криптография зародилась в 1984 году**

Bennett C.H., Brassard G. Quantum Cryptography: Public Key Distribution and Coin Tossing // Proc.of IEEE Int. Conf. on Comput. Sys. and Sign. Proces., Bangalore, India, 1984. – pp. 175-179

Ассоциация РусКрипто

Квантовая криптография

- QKD – квантовое распределение ключей
- QSDC – квантовая защищенная прямая связь
- QSC – квантовой поточное шифрование
- QS – квантовая стеганография
- QKI – инфраструктура квантовых ключей
- QDC – квантовая цифровая подпись

Ассоциация РусКрипто

Квантовая криптография

- QKD – квантовое распределение ключей
- QSDC – квантовая защищенная прямая связь
- QSC – квантовой поточное шифрование
- QS – квантовая стеганография
- QKI – инфраструктура квантовых ключей
- QDC – квантовая цифровая подпись

Ассоциация РусКрипто

Квантовая криптография

- 1984 год – первый алгоритм квантового распределения ключей BB84 (C. Bennett, G. Brassard)
- 1989 год – первая работающая квантово-криптографическая схема (IBM). Расстояние – 32 см

Ассоциация РусКрипто

Квантовая криптография

- 1990-е годы – алгоритмы E91 и B92, достижение расстояний в 23 км и скоростей в единицы Кбит/с,
- 2000-е годы – алгоритмы SARG04, KMB09, COW, DPS, Decoy, достижение расстояний до 100 км и скоростей в сотни Кбит/с

Ассоциация РусКрипто

Коммерческие образцы систем QKD

- id 3100 Clavis2, id 5100 Cerberis (Швейцария)
- Quantum Link Encryptor (Австралия)
- MagiQ QPN 5505, MagiQ QPN 7505, MagiQ QPN 8505 (США)
- SQ Box (Франция)

Ассоциация РусКрипто

Коммерческие образцы систем QKD

Коммерческая система для квантового распределения ключей Cerberis швейцарской компании ID Quantique. Пара излучатель – приемник стоит около 97 тыс. долл.

Дальность ее действия не превышает 100 км, хотя исследователи из ID Quantique в экспери-ментах добились дальности передачи 250 км. Теоретический же максимум составляет 400 км.

Ассоциация РусКрипто

Сравнение QKD и PKI

QKD	PKI
Требует выделенного оборудования и линий связи	Может быть реализована программно, очень мобильна
Защищённость основана на фундаментальных физических законах и принципах	Требует увеличения длины ключей с ростом производительности компьютеров
Не подвержена проблемам с построением квантового компьютера	С построением квантового компьютера безопасность окажется под угрозой
Высокая стоимость	Низкая стоимость
Требуются только оптические каналы связи	Работает с любыми типами сетей

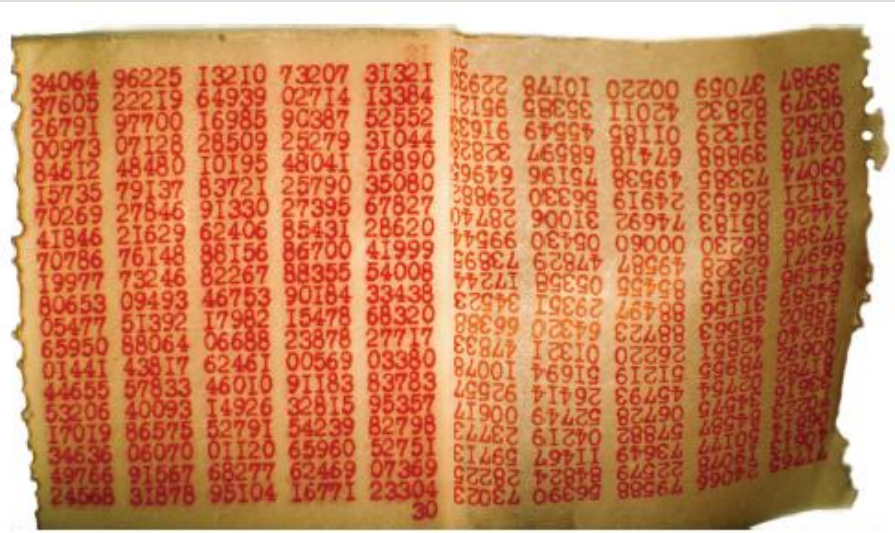
Ассоциация РусКрипто

Коммерческие образцы систем QKD

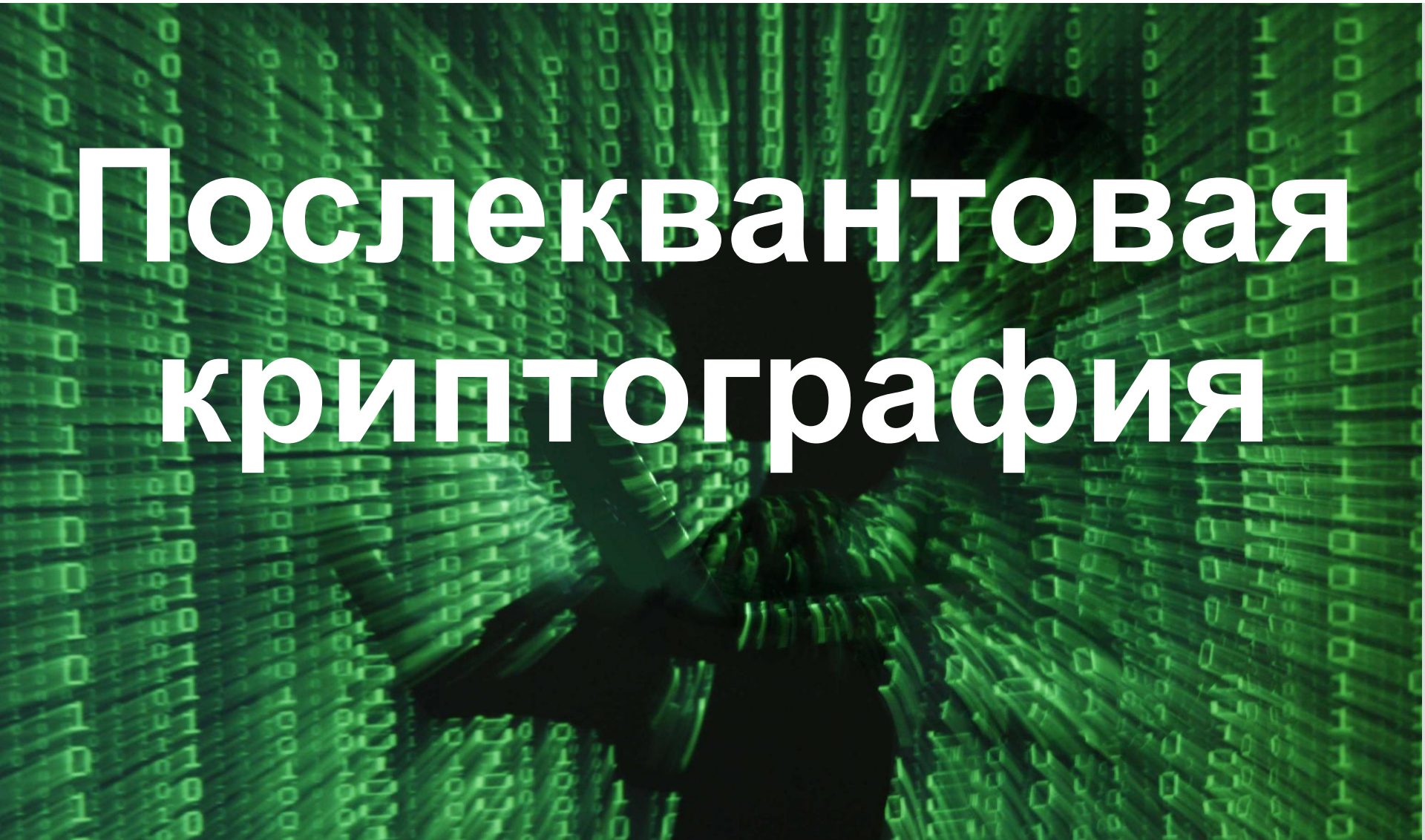
- **2009-2011 года – первые примеры успешных атак на системы квантового распределения ключей, *использующие технические недоработки* конкретных коммерческих реализаций**

Ассоциация РусКрипто

Коммерческие образцы систем QKD



Ассоциация
РусКрипто



Послеквантовая криптография

Ассоциация РусКрипто

Is cryptography dead?

Daniel J. Bernstein

Квантовая «угроза» криптографии

Ассоциация РусКрипто

Сравнительная стойкость криптоалгоритмов и сроки их действия

Bits of security	Symmetric key algorithms	FFC (DSA, D-H, MQV)	IFC (RSA)	ECC (ECDSA)
80 (до 2010 г.)	2TDEA, SKIPJACK,	$L = 1024$ $N = 160$	$k = 1024$	$f = 160\text{-}223$
112 (до 2030 г.)	3TDEA	$L = 2048$ $N = 224$	$k = 2048$	$f = 224\text{-}255$
128 (после 2030 г.)	AES-128	$L = 3072$ $N = 256$	$k = 3072$	$f = 256\text{-}383$
192	AES-192	$L = 7680$ $N = 384$	$k = 7680$	$f = 384\text{-}511$
256	AES-256	$L = 15360$ $N = 512$	$k = 15360$	$f = 512+$

Ассоциация РусКрипто

Квантовые алгоритмы

Ресурсы для квантового решения задач факторизации и ECDLP

	Факторизация		ECDLP			кл. время
n	число кубитов	квант. время	n	число кубитов	квант. время	
512	1024	$0{,}54 \cdot 10^9$	110	700	$0{,}5 \cdot 10^9$	$6{,}4 \cdot 10^{16}$
1024	2048	$4{,}3 \cdot 10^9$	163	1000	$1{,}6 \cdot 10^9$	$3{,}0 \cdot 10^{24}$
2048	4096	$34 \cdot 10^9$	224	1300	$4{,}0 \cdot 10^9$	$9{,}2 \cdot 10^{33}$
3072	6114	$120 \cdot 10^9$	256	1500	$6{,}0 \cdot 10^9$	$6{,}0 \cdot 10^{38}$
15360	30720	$1{,}5 \cdot 10^{13}$	512	2800	$50 \cdot 10^9$	$2{,}1 \cdot 10^{77}$

Ассоциация РусКрипто

«Квантово-устойчивые» криптоалгоритмы

- Существует несколько различных типов криптосистем с открытым ключом, устойчивых к квантовым вычислениям:

Ассоциация РусКрипто

«Квантово-устойчивые» криптоалгоритмы

- **Hash-based cryptography**
  - **Merkle signature scheme (MSS)** – 1979
  - **Lamport–Diffie one-time signature scheme (LD-OTS)** – 1979
  - **Winternitz one-time signature scheme (W-OTS)** – 1989

Ассоциация РусКрипто

«Квантово-устойчивые» криптоалгоритмы

- **Code-based cryptography**
  - **McEliece PKC** – 1978
  - **The Niederreiter variant** of encryption scheme – 1986
  - **Modifications** for the trapdoor of **McEliece's PKC**

Ассоциация РусКрипто

«Квантово-устойчивые» криптоалгоритмы

- **Lattice-based cryptography.**
  - **NTRU** is a ring-based cryptosystem proposed by Hoffstein, Pipher and Silverman 1998
  - **The LWE-based cryptosystem** presented by Regev – 2005

Ассоциация РусКрипто

«Квантово-устойчивые» криптоалгоритмы

- **Multivariate-quadratic-equations cryptography.**
  - **HFEv− public-key-signature system** (Patarin – 1996)
  - **Multivariate signature** (Ong, Schnorr, Shamir – 1984)
  - **PKC of Diffie and Fell** —1985

Ассоциация РусКрипто

Квантовые алгоритмы и симметричные криптосистемы

Ресурсы для квантового решения задачи поиска ключа симметричной криптосистемы

k	число кубитов	квантовое время	классическое время
56	56	$2{,}1 \cdot 10^{8}$	$7{,}2 \cdot 10^{16}$
80	80	$8{,}6 \cdot 10^{11}$	$1{,}2 \cdot 10^{24}$
112	112	$5{,}7 \cdot 10^{16}$	$5{,}2 \cdot 10^{33}$
128	128	$1{,}4 \cdot 10^{19}$	$3{,}4 \cdot 10^{38}$
168	168	$1{,}5 \cdot 10^{25}$	$3{,}7 \cdot 10^{50}$
256	256	$2{,}7 \cdot 10^{38}$	$1{,}2 \cdot 10^{77}$

April 2 – April 3, 2015

NIST Workshop On Cybersecurity in a Post-Quantum World

April 2 – April 3, 2015

Post-Quantum World

- How does the development of quantum computers affect the security of currently deployed public key algorithms?
- How would quantum computers affect other services which rely on public key infrastructure?
- Are there other concerns with the existing public key algorithms that would motivate the development of alternative cryptosystems?
- Are there other advanced computing technologies that could threaten the existing cryptosystems?

Ассоциация РусКрипто

Post-Quantum World

- How urgent is the need for post-quantum cryptography?
- What changes to applications and protocols could mitigate potential interoperability problems?
- What guidance should NIST provide with respect to post-quantum cryptography?

Post-Quantum World

- What are desirable properties of post-quantum cryptosystems with regard to security, performance, ease of implementation, and interoperability?
- What are desirable properties of post-quantum cryptosystems with regard to particular applications, such as encryption, digital signatures, key exchange, and message authentication?

Post-Quantum Cryptography

- What are the strengths and weaknesses of the different post-quantum cryptosystems that have been proposed? How can one gain confidence in the security of these cryptosystems against quantum and classical attacks?
- Are there ways to estimate the real-world performance of a quantum algorithm, without running it on a quantum computer?
- Which of these cryptosystems are mature, and which ones require further development?

Ассоциация РусКрипто

Послеквантовая криптография