SQUEEZING THE TIME

Miroslava Bondarenko,

Sergey Tikhonov

http://www.finteller.ru

http://itm.ranepa.ru/

RUSSIA

QUANTUM CRYPTOGRAPHY

Classic Approach, Crypto Channels, Key Distribution

- Basic task of cryptography is data **encryption** and **authenticating the sender**.
- **Sender** must **transform the message**, possibly **using** additional data called a **key**, to **provide the recipient** with the **ablility to determine** if the received **message** has been **changed**.
- The **classic approach** is to use **the same key for both encryption and decryption** of the message. The key must be known only to the sender and the recipient. Such systems are called **cryptosystems with a private key**.
- **Reliability** of encryption procedure is proved only for the **"one-time notebook" method**, proposed in 1917 by Gilbert Vernam.
- **Both participants of exchange should have a set of shared secret keys, each of which is used to encrypt only one message**. Keys are generated randomly and do not carry any information.
- In the encryption process **each character of the original message stacks with the corresponding key symbol** so that the key must be long enough and the message is short enough.
- In "precomputer" time, keys were stored in notebooks with detachable sheets (hence the name of the method). Each sheet of notebook was destroyed after use.
- In telecommunications systems there is secrecy problem during keys exchange: key must be delivered to the recipient in advance with strict confidentiality. So, **the keys allow confidential exchange of messages. But how to exchange the keys themselves with secrecy**

Symmetric encryption

- If a permanent private key is used, then the decryption of the message depends on the computing power of the system and the time.
- For example, in USA, Data Encryption Standard (DES), developed in 1977, was used for encryption. It is based on a 56-bit key allowing one to encode 64 bits of information.
- This standard was the base of the protection of banking transactions, passwords of Unix-systems and other secret data. But currently, there are data on the possibility of hacking such systems during 22 hours 15 min *, **

http://edition.cnn.com/TECH/computing/9901/21/descrack.idg/*

https://www.emc.com/emc-plus/rsa-labs/historical/des-challenge-iii.htm**

ASSYMMETRIC ENCRYPTION

- The public key encryption theory was created by Whitfield Diffie and Martin Hellman in 1976. Public-key cryptosystems are based on one-way functions: it is **easy to compute f (x) for some x**, but it is ***very difficult to calculate x knowing f (x)***.
- The first algorithm based on the Diffie-Hellman theory is RSA algorithm (proposed by Ron Rivest, Edi Shamir and Leonard Adleman in 1977).
- **RSA algorithm** is based on the **factorization of a prime number**.
- It is known the easiness of calculating the product of two primes. But the **inverse problem to expand number into prime factors is rather laborious**. Computation time exponentially increases with the number of bits in the original number.
- Although there are currently no quick algorithms for solving the **problem of factorization into prime numbers**, one can not say that they do not exist at all.
- Computing power is constantly increasing. So due to changes in architecture of computers the complexity of the problem does not mean its unsolvability*
- Now the only reliable method of encryption is the **"one-time notebook" method*.** Is it really reliable? Can we accelerate brute forcing?

*https://eden.dei.uc.pt/~sneves/pubs/2009-sn-msc.pdf**

FINTELLER LLC
http://www.finteller.ru

BRUTEFORCE ACCELERATION

GPU (graphic processing unit) AND BIG DATA

Big data solution (Hadoop)

resolved two huge, critical problems :

- Extending virtual data volumes beyond the bounds of single storage volumes without big difficulties
- New mechanism for running analytical and processing jobs in batches and in parallel using effective combination of new cloud-based methodologies and old data science methods that had been collecting dust since before the rise of dBASE.
- analytical and processing jobs could run in batches and in parallel due to new mechanism

An operator at the U.S. Army Tactical Operations Center from the U.S. Army, in the public domain.

Another technology is graphics processor-based acceleration.
Now it's possible for GPUs to run their own massively parallel tasks, at speeds that conventional, sequential, multi-core CPUs can't possibly approach, even in clusters

http://www.datacenterknowledge.com/archives/2016/11/17/gpu-acceleration-makes-kineticas-brute-force-database-brute/*

Quantum Computer Timeline

1960

Alexey I. Ekimov. Russian solid state physicist, worked in Vavilov State Optical Institute. Discovered semiconductor nanocrystals known as quantum dots.

ACM DL DIGITAL LIBRARY

Conjugate coding

Full Text: Pdf Buy this Article

Author: Stephen Wiesner Columbia University, New York, N.Y.

Published in:

· Newsletter
ACM SIGACT News - A special issue on cryptography Homepage archive
Volume 15 Issue 1, Winter-Spring 1983
Pages 78 - 78
ACM New York, NY, USA
table of contents doi>10.1145/1008908.1008920

1983 Article

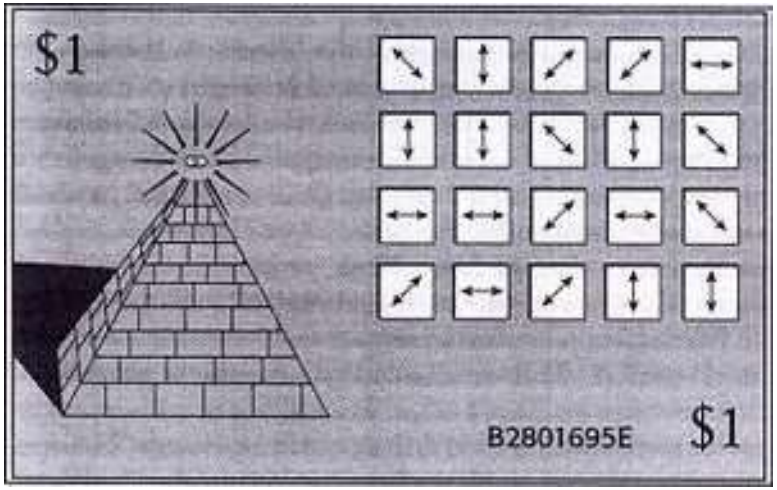
Bibliometrics

- Downloads (6 Weeks): 27
- Downloads (12 Months): 195
- Downloads (cumulative): 1,583
- Citation Count: 78

FINTELLER LLC
http://www.finteller.ru

Quantum Computer Timeline
1960-s

A quantum banknote, proposed by Stephen Wisner in 1969. Contains a pyramid with an eye, a serial number and 20 traps for photons, whose contents are a mystery. In each trap there is 1 photon with unknown polarization*



At the moment, the idea of quantum money is not realizable, so far no traps have been built for individual photons. But security specialists already offer protocols and attacks on them all the way

*https://en.wikipedia.org/wiki/Stephen_Wiesner

Quantum Computer Timeline
1973

- Alexander Holevo publishes a paper showing that n qubits cannot carry more than n classical bits of information (a result known as "Holevo's theorem" or "Holevo's bound " *)

https://en.wikipedia.org/wiki/Alexander_Holevo*

Alexander Holevo

Born	2 September 1943 Russian SFSR, Soviet Union
Nationality	Russian
Fields	Mathematician
Institutions	Steklov Mathematical Institute, Moscow State University, Moscow Institute of Physics and Technology
Alma mater	Moscow Institute of Physics and Technology
Known for	Holevo's theorem

Quantum Computer Timeline

1975

The statement of the quantum theory about the impossibility of creating an ideal copy of an arbitrary unknown quantum state.

Charles H. Bennett shows that computation can be done reversibly **

http://www.research.ibm.com:80/people/b/bennetc/**

FINTELLER LLC
http://www.finteller.ru

Quantum Computer Timeline

1976

- Polish mathematical physicist Roman Stanisław Ingarden publishes a seminal paper entitled "Quantum Information Theory" in Reports on Mathematical Physics, vol. 10, 43–72, 1976. (The paper was submitted in 1975.)
- It is one of the first attempts at creating
  - a quantum information theory,
  - showing that Shannon information theory cannot directly be generalized to the quantum case,
  - but rather that it is possible to construct a quantum information theory, which is a generalization of Shannon's theory, within the formalism of a generalized quantum mechanics of open systems and a generalized concept of observables (the so-called semi-observables).

QUANTUM CRYPTOGRAPHY 101*

- Whenever you perform an online transaction, such as a purchase or bank transfer, you trust your personal information with a secure encryption system.
- Such encryption is based on mathematical problems, hacking of which is problematic for modern computers. Therefore, your information is relatively safe
- But in future quantum computers will be able to decrypt many such coded messages. We need quantum-secure cryptographic tools.
- Fortunately quantum mechanics enables creating unbreakable codes resistant to any power of classic computing.
- Quantum mechanics states that the quantum system can not be observed without disturbance. So, the "key" material exchanged through a quantum link should have an indelible imprint of any attempt at eavesdropping. Keys with eavesdropping can be discarded. Therefore only secret keys are stored for use in non-destructive encryption protocols.
- Implementation case.
  - The Institute for Quantum Computing (IQC) is home to Alice,
  - a photon receiver in a Quantum Key Distribution (QKD) system.
  - Alice's counterpart, Bob, is housed in an office at Waterloo's Perimeter Institute for Theoretical Physics.
  - Alice and Bob receive entangled (highly correlated) photons emitted from a crystal excited by a laser.
  - By measuring the unique polarization of the photons, Alice and Bob receive random (but identical) "keys" which can be used to encode messages.

https://uwaterloo.ca/institute-for-quantum-computing/research/areas-research/quantum-cryptography*

Quantum Computer Timeline, 1980S

- **1980** **Paul Benioff** described quantum mechanical Hamiltonian models of computers, Yuri Manin proposed an idea of quantum computing
- **1981**
  - Richard Feynman
    - in his talk, famous lecture "There's Plenty of Room at the Bottom", the *First Conference on the Physics of Computation*(MIT, May 1981) observed impossibility of quantum system simulation evolution on classical computer in an efficient way.
    - proposed a basic model for a quantum computer that would be capable of such simulations
  - Paul Benioff's talk "Quantum mechanical Hamiltonian models of discrete processes that erase their own histories: application to Turing machines"at the conference, "Physics of Computation", MIT in May 1981.
  - Tommaso Toffoli introduced the reversible Toffoli gate, which, together with the NOT and XOR gates provides a universal set for classical computation.
- **1982**
  - Paul Benioff proposes the first recognisable theoretical framework for a quantum computer
  - William Wootters and Wojciech Zurek, and independently Dennis Dieks prove the no-cloning theorem.
- **1984, 1985**
  - Charles Bennett and Gilles Brassard employ Wiesner's conjugate coding for distribution of cryptographic keys.
  - David Deutsch, at the University of Oxford, described the first universal quantum computer. Just as a Universal Turing machine can simulate any other Turing machine efficiently, so the universal quantum computer is able to simulate any other quantum computer with at most a polynomial slowdown.
- **1989**
  - Bikas K. Chakrabarti & collaborators from Saha Institute of Nuclear Physics, Kolkata, proposed the idea that quantum fluctuations could help explore rough energy landscapes by escaping from local minima of glassy stems having tall but thin barriers by tunnelling instead of climbing over using thermal excitations, suggesting effectiveness of quantum annealing over classical simulated annealing

FINTELLER LLC
http://www.finteller.ru

Quantum Computer Timeline
1990-1995

- **1991 Artur Ekert** at the University of Oxford, invents entanglement based secure communication.
- **1993 Dan Simon, at Université de Montréal**, invented an oracle problem for which a quantum computer would be exponentially faster than a conventional computer. This algorithm introduced the main ideas which were then developed in Peter Shor's factorization algorithm.
- **1994 Peter Shor**, at AT&T's Bell Labs in New Jersey, **discovers an important algorithm**. Shor's algorithm could theoretically break many of the cryptosystems in use today. Its invention sparked a tremendous interest in quantum computers. First United States Government workshop on quantum computing is organized by NIST in Gaithersburg, Maryland, in autumn.
- **December 1994**, Ignacio Cirac, at University of Castilla-La Mancha at Ciudad Real, and Peter Zoller at the University of Innsbruck proposed an experimental realization of the controlled-NOT gate with trapped ions.
- **1995 First United States Department of Defense workshop on quantum computing and quantum cryptography** is organized by United States Army physicists Charles M. Bowden, Jonathan P. Dowling, and Henry O. Everitt; it takes place in February at the University of Arizona in Tucson. Peter Shor and Andrew Steane simultaneously proposed the first schemes for quantum error correction. Christopher Monroe and David Wineland at NIST (Boulder, Colorado) experimentally realize the first quantum logic gate – the C-NOT gate – with trapped ions, according to Cirac and Zoller's proposal
- 1996 Lov Grover, at Bell Labs, invented the quantum database search algorithm. The quadratic speedup is signifcant for factoring, discrete logs, or physics simulations. But the algorithm can be applied to a much wider variety of problems. Any problem that had to be solved by random, brute-force search, could now have a quadratic speedup. The United States Government, particularly in a joint partnership of the Army Research Office (now part of the Army Research Laboratory) and the National Security Agency, issues the first public call for research proposals in quantum information processing. David P. DiVincenzo, from IBM, proposed a list of minimal requirements for creating a quantum computer*

https://en.wikipedia.org/wiki/Timeline_of_quantum_computing*

FINTELLER LLC
http://www.finteller.ru

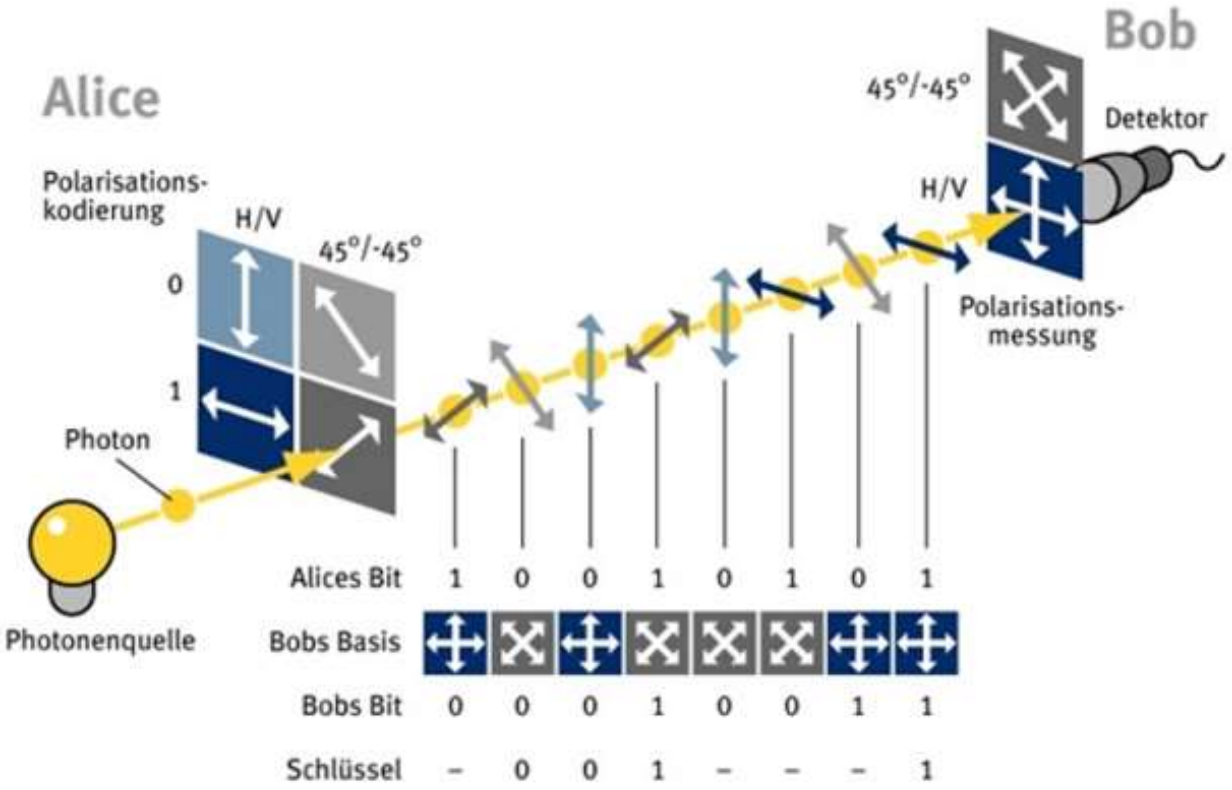
Quantum Computer Timeline
1995-2000

- 1997 David Cory, Amr Fahmy and Timothy Havel, and at the same time Neil Gershenfeld and Isaac L. Chuang at MIT published the first papers realising gates for quantum computers based on bulk spin resonance, or thermal ensembles. The technology is based on a nuclear magnetic resonance (NMR) machine, which is similar to the medical magnetic resonance imaging machine.
- Alexei Kitaev described the principles of topological quantum computation as a method for combating decoherence. Daniel Loss and David P. DiVincenzo proposed the Loss-DiVincenzo quantum computer, using as qubits the intrinsic spin-1/2 degree of freedom of individual electrons confined to quantum dots
- 1998 First experimental demonstration of a quantum algorithm. A working 2-qubit NMR quantum computer used to solve Deutsch's problem was demonstrated by Jonathan A. Jones and Michele Mosca at Oxford University and shortly after by Isaac L. Chuang at IBM's Almaden Research Center together with coworkers at Stanford University and MIT.
- First working 3-qubit NMR computer. First execution of Grover's algorithm on an NMR computer. Hidetoshi Nishimori & colleagues from Tokyo Institute of Technology showed that quantum annealing algorithm can perform better than classical simulated annealing.
- Daniel Gottesman and Emanuel Knill independently prove that a certain subclass of quantum computations can be efficiently emulated with classical resources.
- 1999 Samuel L. Braunstein and collaborators: showed that there was no mixed state quantum entanglement in any bulk NMR experiment. Pure state quantum entanglement is necessary for any quantum computational speedup, and thus this gave evidence that NMR computers would not yield benefit over classical computer. It was still an open question as to whether mixed state entanglement is necessary for quantum computational speedup
- Gabriel Aeppli, Thomas Felix Rosenbaum and colleagues demonstrated experimentally the basic concepts of quantum annealing in a condensed matter system*

https://en.wikipedia.org/wiki/Timeline_of_quantum_computing*


FINTELLER LLC
http://www.finteller.ru

The simplest algorithm for generating a private key (BB84), schema*



https://habrahabr.ru/post/315032/*

The simplest algorithm for generating a private key (BB84) explained

- Alice sends Bob a sequence of photon impulses. Each of the pulses is randomly polarized in directions: | - \ /. For example, Alice sends: - / \ | \ - |.
- For each photon, Bob randomly chooses the type of measurement: he changes either the rectilinear polarization (+) or the diagonal one (x) and tunes his detector in an arbitrary way to measure a series of either diagonally or orthogonally polarized pulses (you can not measure both at the same time)
- If Bob guessed the polarization, he would get the correct result (the same polarization as Alice sent), otherwise result is random.
- Bob and Alice set open channel to inform each other of the types of their polarizations (diagonal or orthogonal) and leave only the correctly measured polarizations.

ALICE		BOB		
Bit Value	φ_A	φ_B	$\varphi_A - \varphi_B$	Bit Value
0	0	0	0	0
0	0	$\pi/2$	$3\pi/2$	?
1	π	0	π	1
1	π	$\pi/2$	$\pi/2$	?
0	$\pi/2$	0	$\pi/2$	?
0	$\pi/2$	$\pi/2$	0	0
1	$3\pi/2$	0	$3\pi/2$	?
1	$3\pi/2$	$\pi/2$	π	1

- Suppose, in the example above, Bob guessed the polarization of the 2nd, 5th, 6th and 7th pulses. Then there remain: \\ - |.

According to the previously agreed conditions, these results turn into a sequence of bits (for example, 0 ° and 45 ° are taken as units, 90 ° and -45 ° for zero, in the above example we get 0010).

Bob and Alice can detect interception of the key message by checking the errors by checking the randomly selected bits from the message. Mismatches indicate the interception of the message, then the key changes, i.e. it is re-transmitted.
If there are no discrepancies, then the bits used for comparison are discarded, the key is accepted. With probability 1 – 2^k (where k is the number of compared bits), the channel was not listened.
If intruder can not only listen to the main channel Alice-> Bob, but also can falsify the work of the open channel Bob-> Alice, then the whole scheme collapses. (Man-In-The-Middle)

FINTELLER LLC
http://www.finteller.ru

Algorithm B92 for generating a private key

- The B92 protocol is one of the first protocols for quantum key distribution proposed in 1992 by Charles H. Bennett and based on the principle of uncertainty, unlike protocols such as E91.
- The carriers of information are 2-level systems, called qubits (quantum bits).
- An important feature of the protocol is the use of two non-orthogonal quantum states*

*Quantum computation and quantum information. — M.: MIR, 2006. — 824 c. — ISBN 5-03-003524-9.

FINTELLER LLC
http://www.finteller.ru

Quantum Computer Timeline
2000-2005

- First working 5-qubit NMR computer demonstrated at the Technical University of Munich.
- First execution of order finding (part of Shor's algorithm) at IBM's Almaden Research Center and Stanford University
- First working 7-qubit NMR computer demonstrated at the Los Alamos National Laboratory*
- Europe. 2004. Development of a Global Network for Secure Communication based on Quantum Cryptography

***Nuclear Magnetic Resonance Quantum Computing (NMRQC)**
http://web.physics.ucsb.edu/~msteffen/nmrqc.htm
** http://cordis.europa.eu/project/rcn/71407_en.html

FINTELLER LLC
http://www.finteller.ru

Quantum Computer Timeline 2005-2010

- 2006. Theory of macroscopic object entanglement, which has implications for the development of quantum repeaters*
- 2007. Breakthrough in applying spin-based electronics to silicon*
- D-Wave Systems claims to have produced a 128 qubit computer chip, though this claim has yet to be verified*

May 16, 2007 Scientific American *JR Minkel. "Spintronics Breaks the Silicon Barrier". Retrieved December 30, 2007**

December 19, 2008 *Next Big Future. "Dwave System's 128 qubit chip has been made". Retrieved December 20, 2008***

Quantum Computer Timeline
2010s

- D-Wave claims a quantum computation using 84 qubits*
- 1QB Information Technologies (1QBit) founded. World's first dedicated quantum computing software company**
- Documents leaked by Edward Snowden confirm the Penetrating Hard Targets project, by which **the National Security Agency seeks to develop a quantum computing capability for cryptography purposes*****

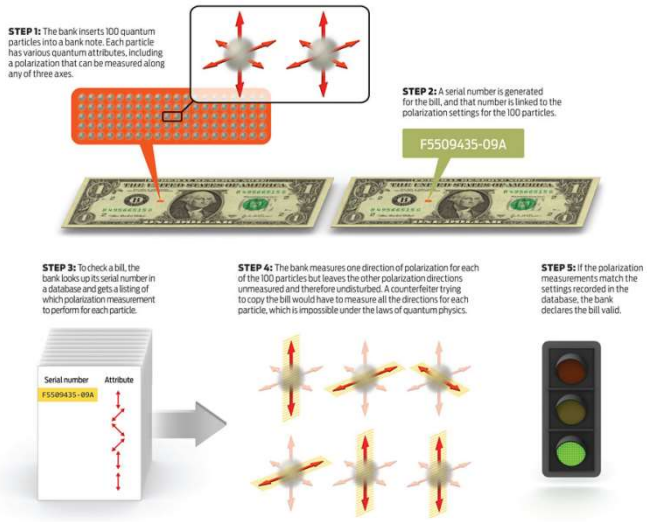
*Zhengbing Bian; Fabian Chudak; William G. Macready; Lane Clark; Frank Gaitan (2012). "Experimental determination of Ramsey numbers with quantum annealing". *Physical Review Letters*. **111** (13): 130505. arXiv:1201.1842 . Bibcode:2013PhRvL.111m0505B. doi:10.1103/PhysRevLett.111.130505. PMID 24116761

**http://1qbit.com/

***http://apps.washingtonpost.com/g/page/world/a-description-of-the-penetrating-hard-targets-project/691/

FINTELLER LLC
http://www.finteller.ru

Quantum anti-counterfeiting



- The bank database contains pairs "serial number - polarization of photons".
- If the bank checks the banknote =>bank knows which polarization each photon is
- Then bank can check banknote with one attempt.
- In the case of 100% matching, a genuine bill+. the bank fills the "spent photons" again.

An attacker who wants duplicate a banknote needs

- either will fill out photons at random, which will then be found out,
- or need to count the state of photons.
- since each photon has "1 attempt is given", if the photon is "lost", the attacker does not possess complete information about this photon,
- if hacker "fakes a photon" a mistake is inevitable with a certain probability and the bank can determine this mistake.
- The number of traps for photons achieves the necessary error probability for the attacker
- The probability of successful copying does not exceed (5/6) n, where n is the number of photons on the banknote

Quantum cryptography 2017*

According to ISSA April 2017 web-conference*

Quantum Computer Timeline

Present days

- IBM Q http://research.ibm.com/ibm-q/
- Dwave https://www.dwavesys.com/quantum-computing/industries
- CERN announced interest in quantum computing http://cerncourier.com/cws/article/cern/68128
- Microsoft has big quantum computing plans http://www.pcworld.com/article/3190713/computers/microsofts-cool-quantum-computing-plan-embraces-cryogenic-memory.html

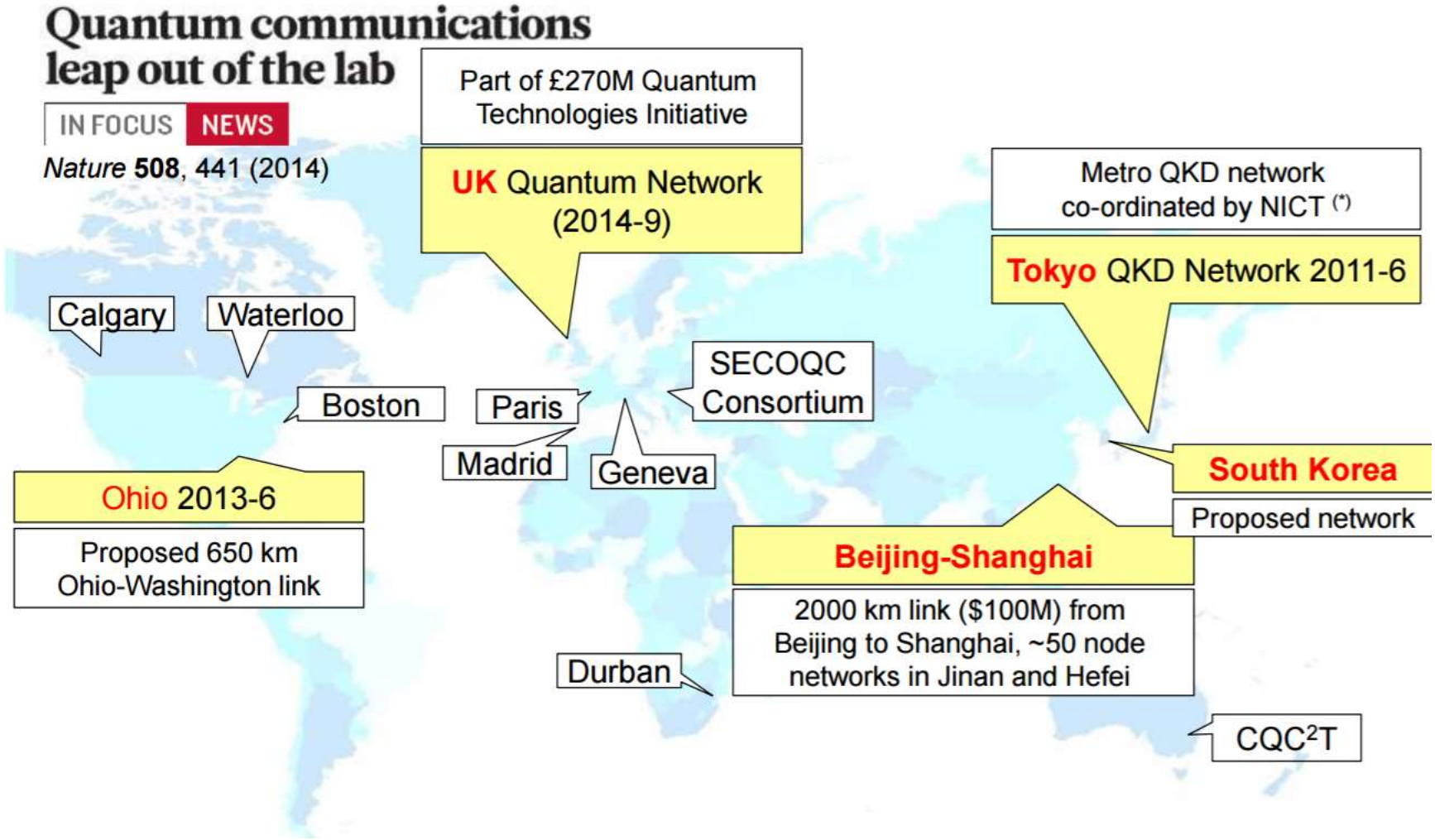
Quantum key distribution (QKD)*

- **Fundamental aspect of quantum mechanics**: the process of measuring a quantum system in general disturbs the system.
- QKD uses quantum mechanics to guarantee secure communication: enables two parties to produce a shared random secret key that can be used to encrypt and decrypt messages.
- By using quantum superpositions or quantum entanglement and transmitting information in quantum states, a communication system can be implemented that detects eavesdropping.
- An important and unique property of quantum key distribution is the ability of the two communicating users to detect the presence of any third party trying to gain knowledge of the key.
- Quantum key distribution is only used to produce and distribute a key, not to transmit any message data.
- The algorithm most commonly associated with QKD is the one-time pad, as it is provably secure when used with a secret, random key.
- In real-world situations, it is often also used with encryption using symmetric key algorithms like the Advanced Encryption Standard algorithm **

More formal description *

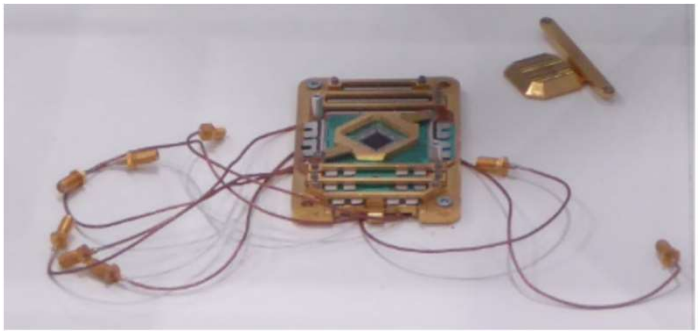
https://en.wikipedia.org/wiki/Quantum_key_distribution**

QKD Implementations

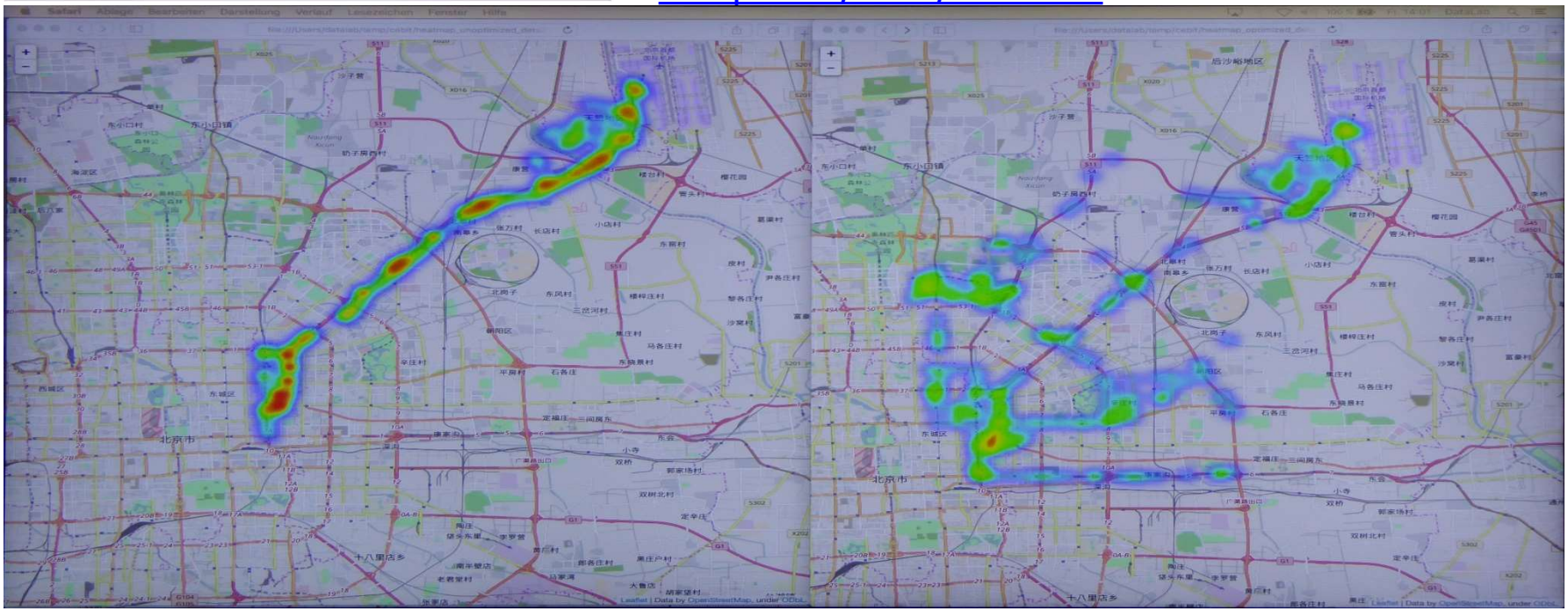


http://www.cambridgewireless.co.uk/Presentation/CWTEC16-Zhiliang_Yuan-Toshiba.pdf

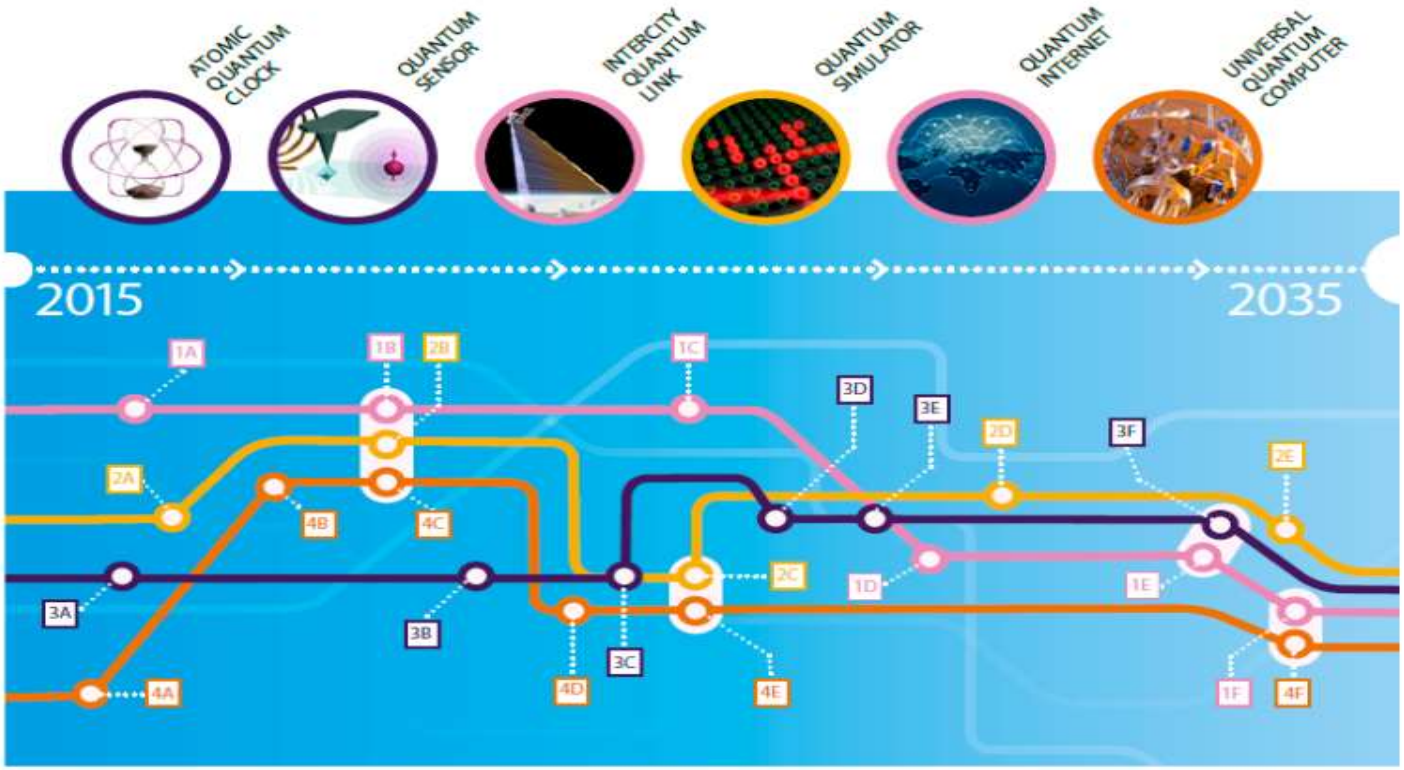
Quantum Computer, 2017, CeBIT

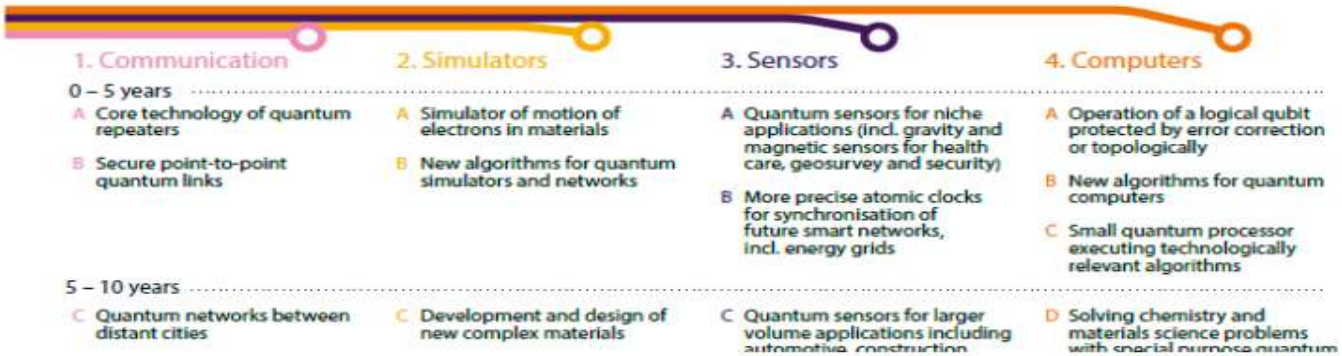


Volkswagen announced the usefullness of a quantum computer for transport task
https://www.volkswagen-media-services.com/en/detailpage/-/detail/Digital-pioneering-work-Volkswagen-uses-quantum-computers/view/4708404



Quantum Technologies Timeline





https://gilkalai.wordpress.com/2017/04/03/the-race-to-quantum-technologies-and-quantum-computers-useful-links

PostQuantum Risk Management. Practice. What is necessary the first?

Check and update the certificates.

Focus on hardware modules that provide cryptography logic.

Statistics show that about 34% of devices have not been updated and may become obsolete

Post Quantum Risk Management. Develop a post quantum strategy

- Wait for regulator approved algorithms
- Ask your Product Managers and Technology Vendors about their roadmaps plans
- Implement or seek “Hybrid Approach”.
- For example, (**FIPS 140-2 or AES-256**) and **post quantum crypto** can coexist now

How secure will our current crypto algorithms be?

ISSA

Algorithm	Key Length	Security level (Conventional Computer)	Security level (Quantum Computer)
RSA-1024	1024 bits	80 bits	~0 bits
RSA-2048	2048 bits	112 bits	~0 bits
ECC-256	256 bits	128 bits	~0 bits
ECC-384	384 bits	192 bits	~0 bits
AES-128	128 bits	128 bits	~64 bits
AES-256	256 bits	256 bits	~128 bits

According to April 2017 materials of ISSA web-conference

THE BENEFIT OF QUANTUM COMPUTERS

Full-fledged fault-tolerant quantum computer

- can solve many problems previously thought to be intractable
- optimizing/designing materials, drugs, chemical processes, etc
- computational mathematics (including breaking current public-key cryptography)
- Non fault-tolerant quantum devices
  - not a known threat to cryptography
  - probably they can capture some of the power of quantum computation and bypass some/all cost of fault tolerance
  - probably they can solve useful problems better than conventional devices

Postquantum cryptography. The biggest public companies

Google/IBM/Microsoft and others: the race for building quantum computers.

- The Race to Sell True Quantum Computers Begins Before They Really Exist, (Wired) Mainly on Google and IBM. IBM Inches Ahead of Google in Race for Quantum Computing Power, MIT Technology Review. Commercialize quantum technologies in five years (Nature)
- IBM: IBM's quantum cloud computer goes commercial (Nature) IBM moves from a 5-qubit quantum computer to 50-qubit commercial quantum computer in the near future. Also IBM's first commercial quantum computer paves way to overhaul of molecular simulations (chemistry world); IBM Building First Universal Quantum Computers for Business and Science (IBM Press Release); and a PC World article.
- Google: Researchers Report Milestone in Developing Quantum Computer (NYT); Quantum computing is poised to transform our lives. Meet the man leading Google's charge (Wired, and interview with John Martinis)
- Microsoft: Microsoft Makes Bet Quantum Computing Is Next Breakthrough (NYT) ; Inside Microsoft's quest for a topological quantum computer (Nature) Microsoft doubles down on quantum computing bet. Microsoft approach is based on topological quantum computing.

https://gilkalai.wordpress.com/2017/04/03/the-race-to-quantum-technologies-and-quantum-computers-useful-links/

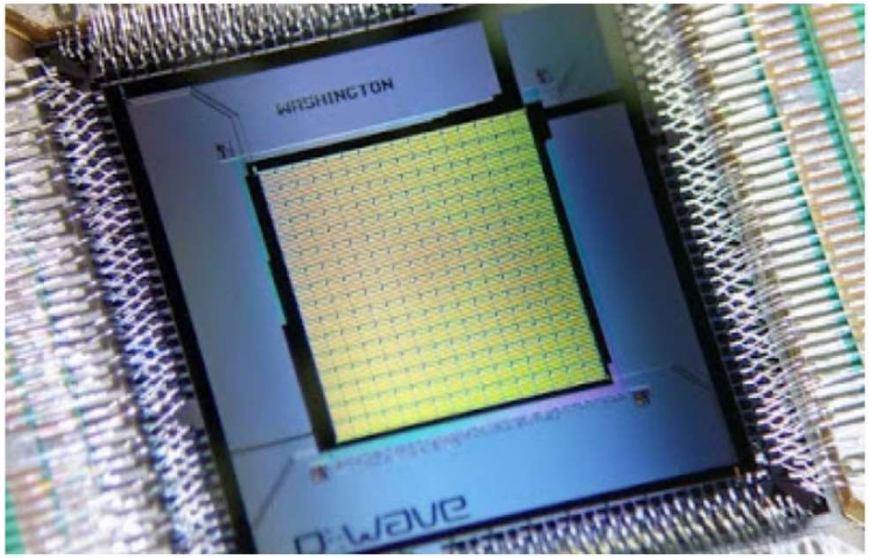
Postquantum cryptography. NIST,IBM, Dwave, Google, IBM

- Others: Scientists are close to building a quantum computer that can beat a conventional one, Science, Chris Monroe and the Startup ionQ, and various other groups and methods. Quantum Computing on Cusp, EE Times, Yale's group and Quantum Circuits. Quantum hanky-panky (Seth Lloyd, Edge); Its much bigger than it looks (David Deutsch, Edge);
- NIST: National Institute of Standards and Technology, quantum divisions. Super *quantum* simulator 'entangles' hundreds of ions (Science daily) *Quantum computers* may have higher 'speed limits' than thought (Phys.org.) A thought experiment by Stephen Jordan.
- D-wave. D-wave is building large scale quantum computers with (rather noisy) superconducting qubits, and implement specific optimization algorithms. *D-Wave* quantum computers: The smart person's guide . Quantum computer learns to 'see' trees Science Magazine. An article in Quanta Magazine.
- List of companies involved in quantum computers. A few webpages: 1Qbit ; D-wave ; Quantum circuits (Yale group) ; Rigetti ; Monroe's blog; Station Q (Microsoft); Google; IBM-Q;

Postquantum cryptography. Error correcting. Supermacy

Quantum Error-Correcting

- The key for large scale universal quantum computers is quantum error-correcting codes.
- IBM to develop hardware to wipe out errors in quantum computing (New Scientists)
- Error fix for long-lived qubits brings quantum computers nearer (New Scientist)
- Physicists show that real-time error correction in quantum … (Phys.Org, reporting in South Africa)
- New Yale-developed device lengthens the life of quantum information (Yale news)



Quantum supremacy

- A convincing demonstration of computational complexity supremacy is expected by researchers in the near future.
- Main approaches are using quantum circuits with around 50 qubits or via demonstration of BosonSampling with 20-30 bosons *

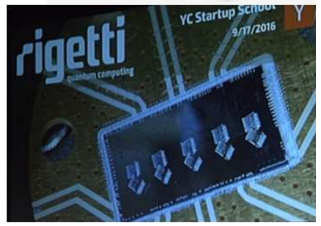
https://www.nextbigfuture.com/2016/10/race-to-quantum-computing-supremacy.html *

Can the Race to Quantum Computing Supremacy get definitive results in 2018?

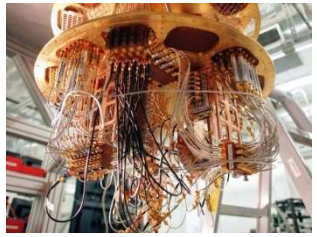
- Quantum computing Supremacy = quantum computers perform computational tasks beyond the capabilities of classical (regular) computers for a significant range of important problems.
- Some proposed technical metrics using cross entropy.
- Critical question: whether quantum devices without error correction can perform a well-defined computational task beyond the capabilities of state-of-the-art classical computers, achieving so-called quantum supremacy.
- Natural task for benchmarking quantum computers is the task of sampling from the output distributions of (pseudo-) random quantum circuits.
- Crucially, sampling this distribution to require direct numerical simulation of the circuit, with computational cost exponential in the number of qubits – typical requirement is typical of chaotic systems.

Can the Race to Quantum Computing Supremacy get definitive results in 2018 (continued)?

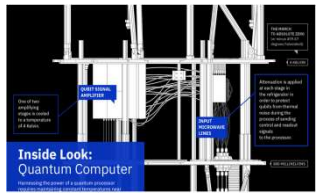
- While chaotic states are extremely sensitive to errors, quantum supremacy can be achieved in the near-term with approximately fifty superconducting qubits.
- Cross entropy can be a useful benchmark of quantum circuits which approximates the circuit fidelity
- **Dwave** Systems https://www.dwavesys.com/ annunce it has a 2000 qubit system superconducting quantum annealing system. Dwave's next chip will revamp their design. Dwave will likely try to address aspects of qubit coherence time and perhaps error correction to match the competing chips from Rigetti, Google and IBM.



- **Rigetti** http://rigetti.com/ computing currently testing a three-qubit chip made with alumnium circuits on a silicon wafer. The design due next year should have 40 qbit.Rigetti says that's possible thanks to design software his company has created that reduces the number of prototypes that will need to be built on the way to a final design. Versions with 100 or more qubits would be able to improve on ordinary computers when it comes to chemistry simulations and machine learning. Chad Rigetti was Technical Lead for 3-D quantum computing at IBM Research. He has been building prototype quantum processors for 12+ years. At Yale, he developed the first all-microwave control methods for superconducting qubits, and at IBM built qubits with world-record performance.



- **Google** by the end of this year plans to launch a 49-qubit quantum computer. John Martinis leads the quantum computing research group at the University of California, Santa Barbara . Google's project estimates that Martinis's group can make a quantum annealer with 100 qubits by the end of 2017. The coherence time of Martinis/Google's qubits, or the length of time they can maintain a superposition, is tens of microseconds—about 10,000 times the figure for those on D-Wave's chip.
- **IBM** Shows Off a Quantum Computing Chip. IBM's new chip is the first to integrate the basic devices needed to build a quantum computer, known as qubits, into a 2-D grid. Researchers think one of the best routes to making a practical quantum computer would involve creating grids of hundreds or thousands of qubits working together. The circuits of IBM's chip are made from metals that become superconducting when cooled to extremely low temperatures. The chip operates at only a fraction of a degree above absolute zero.



Quantum cryptography

INSTITUTE FOR QUANTUM COMPUTING

- The Institute for Quantum Computing (IQC) is home to Alice, a photon receiver in a Quantum Key Distribution (QKD) system.
- Bob, is housed in an office at Waterloo's Perimeter Institute for Theoretical Physics
- Alice and Bob receive entangled (highly correlated) photons emitted from a crystal excited by a laser

- By measuring the unique polarization of the photons, Alice and Bob receive random (but identical) "keys" which can be used to encode messages.
- IQC researcher Norbert Lütkenhaus is a leading international authority on the security of practical quantum key distribution systems. Thomas Jennewein is a world leader in quantum communication and quantum cryptography in free space. IQC's newest research assistant professor, Vadim Makarov, is a "quantum hacker" whose research focuses on finding the vulnerabilities in hardware implementations of QKD, and recommending solutions. He plays the part of "Eve," the eavesdropper, in communications between Alice and Bob. IQC researchers including Richard Cleve, Raymond Laflamme, Debbie Leung, Michele Mosca and Ashwin Nayak have worked on these and other facets of quantum cryptography, such as quantum fingerprints, quantum money and quantum private channels.

FINTELLER LLC
http://www.finteller.ru