Information Security in the Post-Quantum Era

Aleksey Fedorov,
PhD in Physics,
Russian Quantum Center

RQC Russian Quantum Center

These trends are changing our world a lot

1. Internet of Things
2. Robots
3. Drones
4. Self-Driving Cars
5. 3D Printers
6. Next Gen Computing
7. Fintech
8. Big Data
9. Bitcoin
10. Wearables
11. Virtual Reality
12. Life Sciences
13. Safety, Security, Privacy
14. Space Exploration
15. Artificial Intelligence
16. Blockchain
17. Quantum Technologies

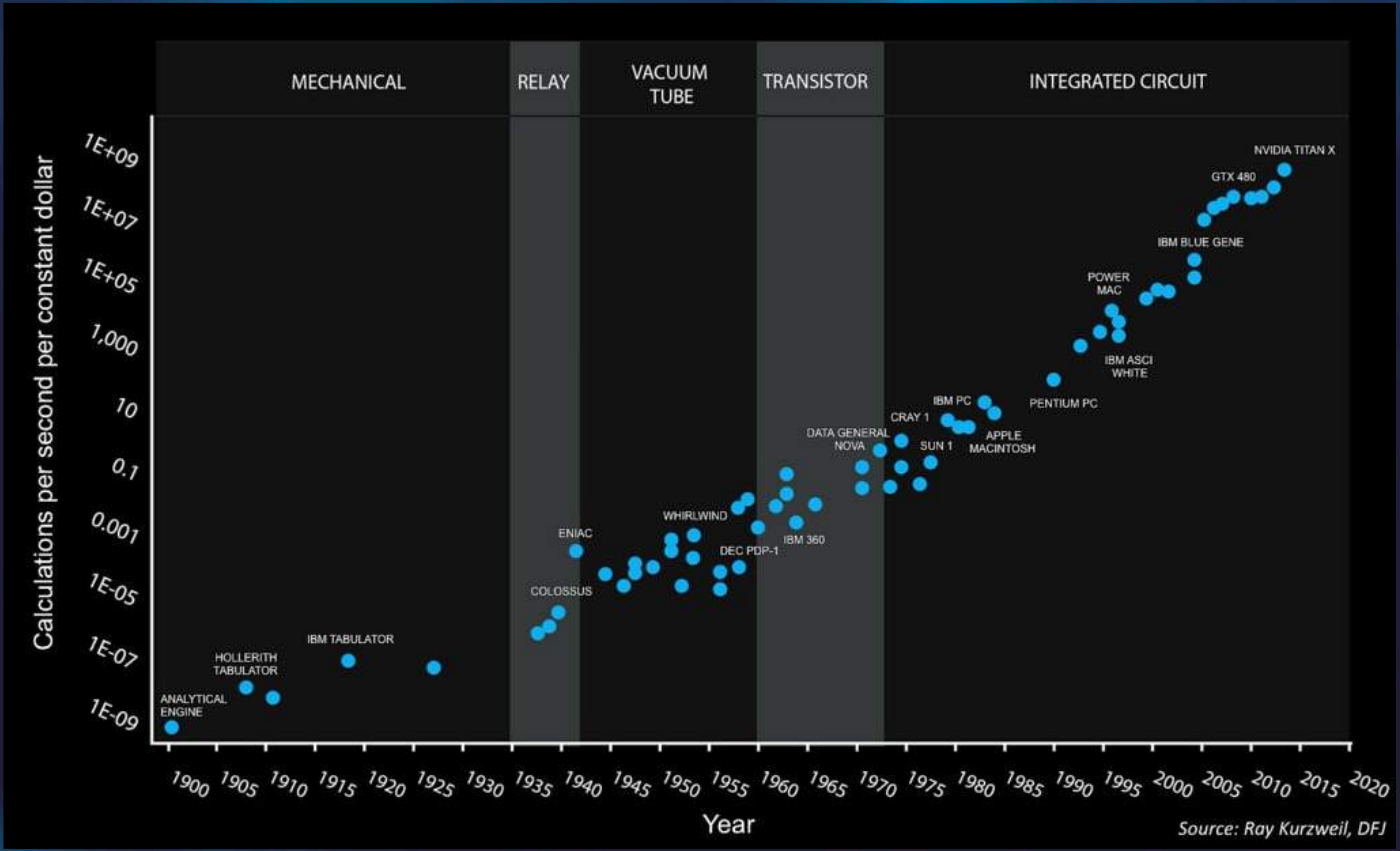
One thing is in common: …

These trends are changing our world a lot

1. Internet of Things
2. Robots
3. Drones
4. Self-Driving Cars
5. 3D Printers
6. Next Gen Computing
7. Fintech
8. Big Data
9. Bitcoin
10. Wearables
11. Virtual Reality
12. Life Sciences
13. Safety, Security, Privacy
14. Space Exploration
15. Artificial Intelligence
16. Blockchain
17. Quantum Technologies

One thing is in common: data

120 Years of Moore's Law



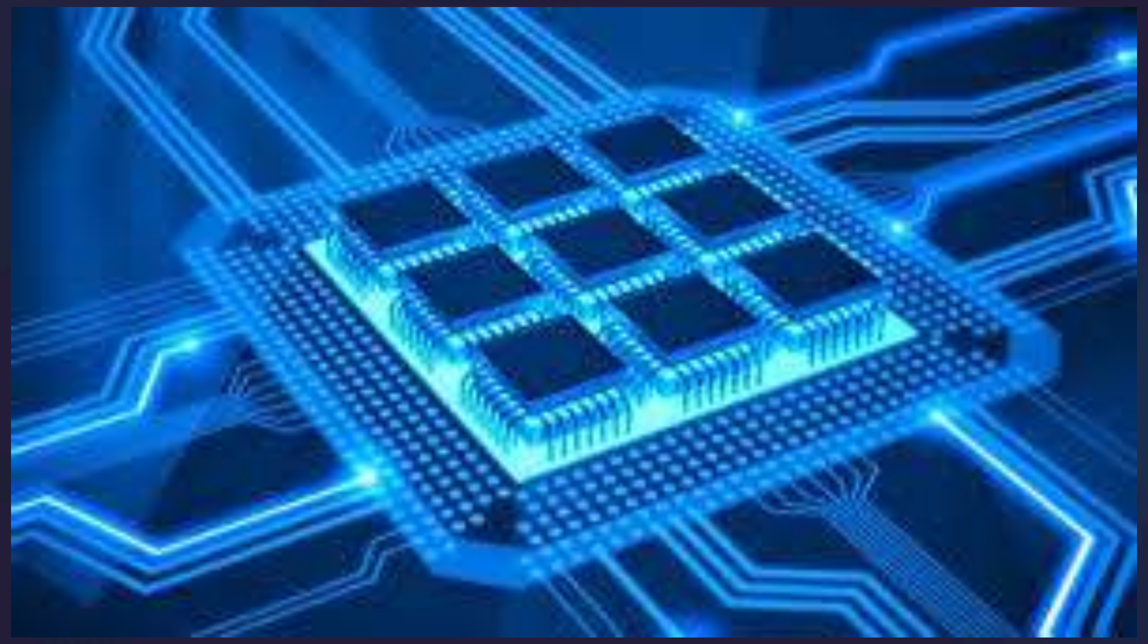
RQC | Russian Quantum Center

120 Years of Moore's Law

Second Quantum Revolution is Coming

First quantum revolution:
Collective quantum phenomena

Lasers



Transistors

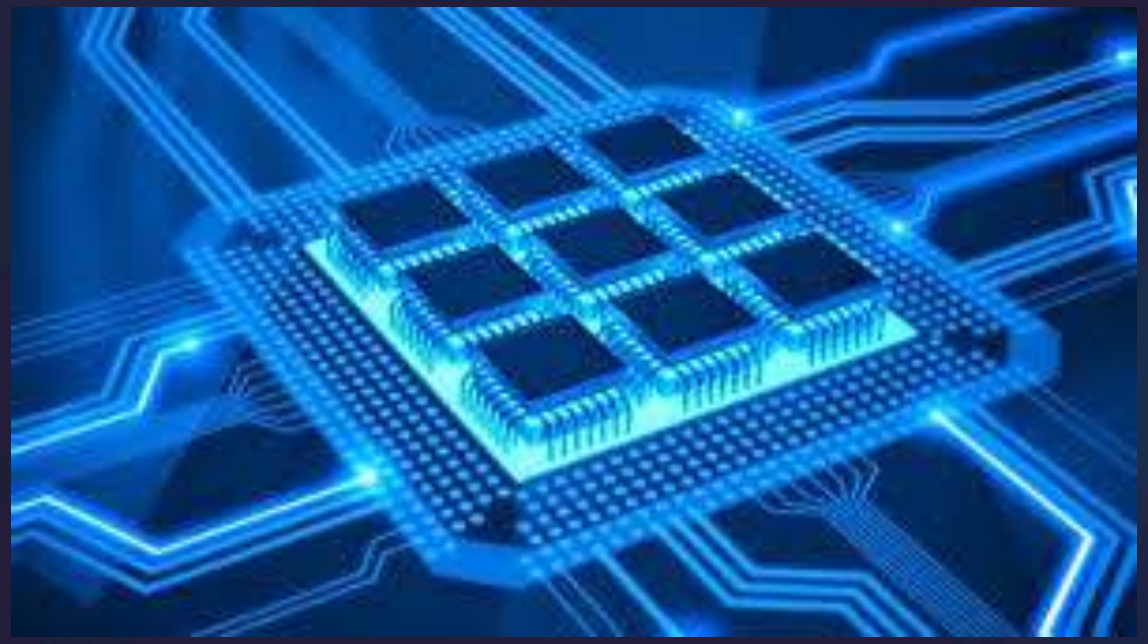
$3 Trillion Industry

Second Quantum Revolution is Coming

RQC Russian Quantum Center

First quantum revolution:
Collective quantum phenomena

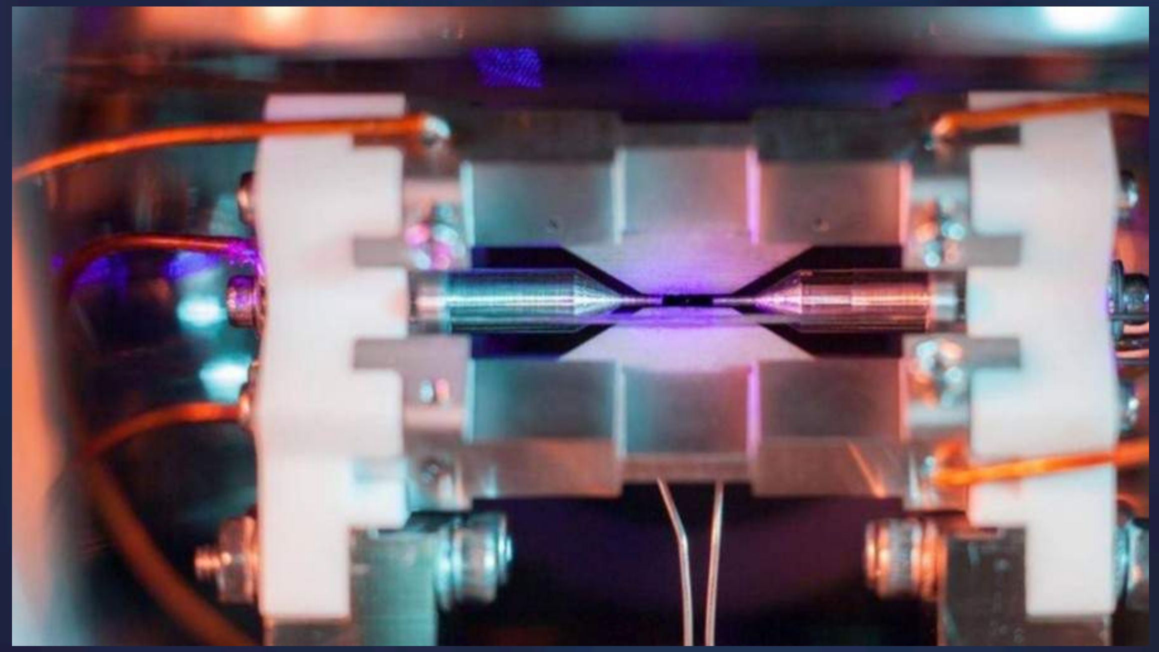
Lasers



Transistors

$3 Trillion Industry

Second quantum revolution:
Individual quantum systems



Single atoms, ions, electrons

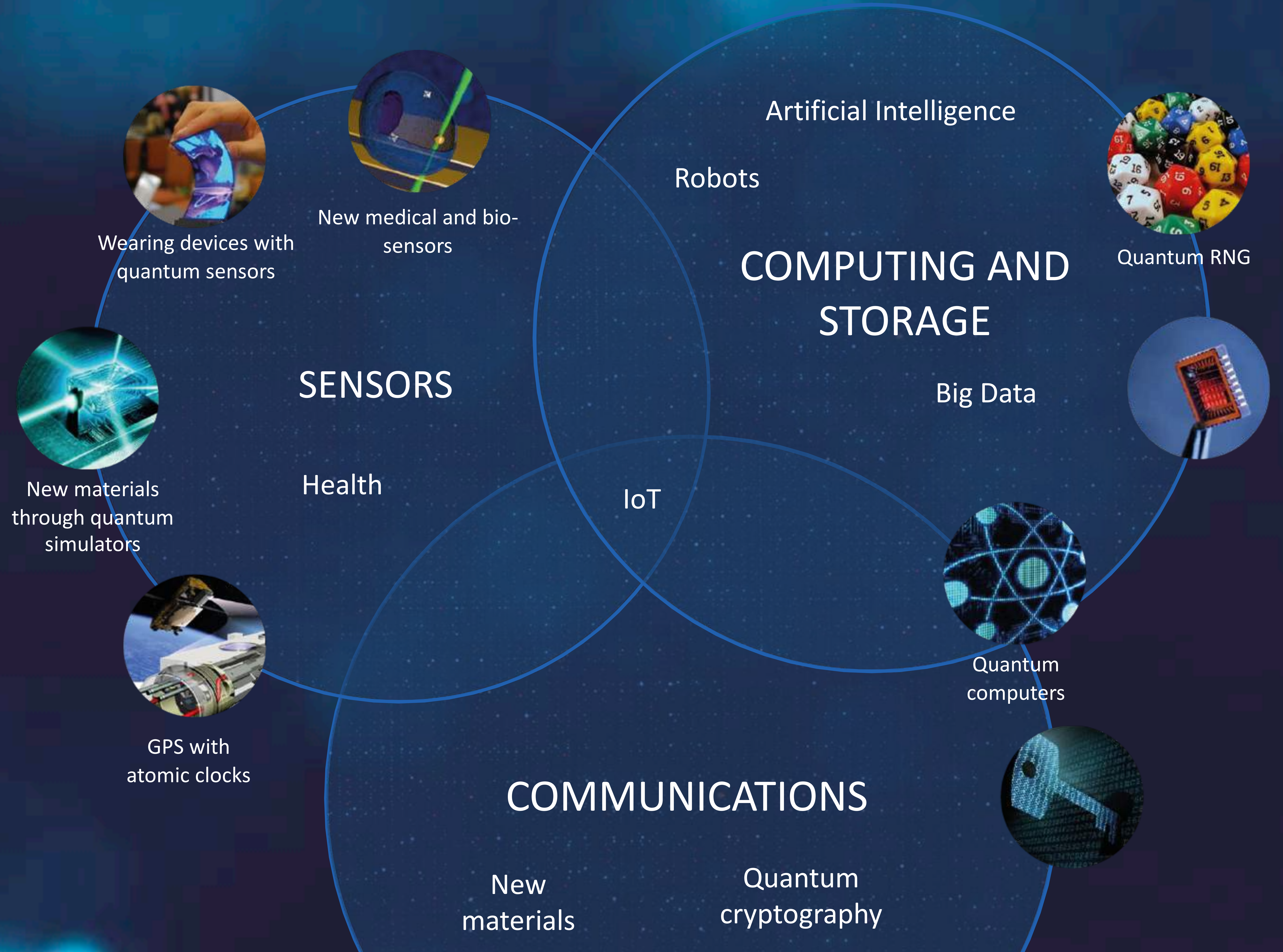
$10 Trillion Industry?

$100 Trillion Industry?

More?

Quantum Systems Are Strange…

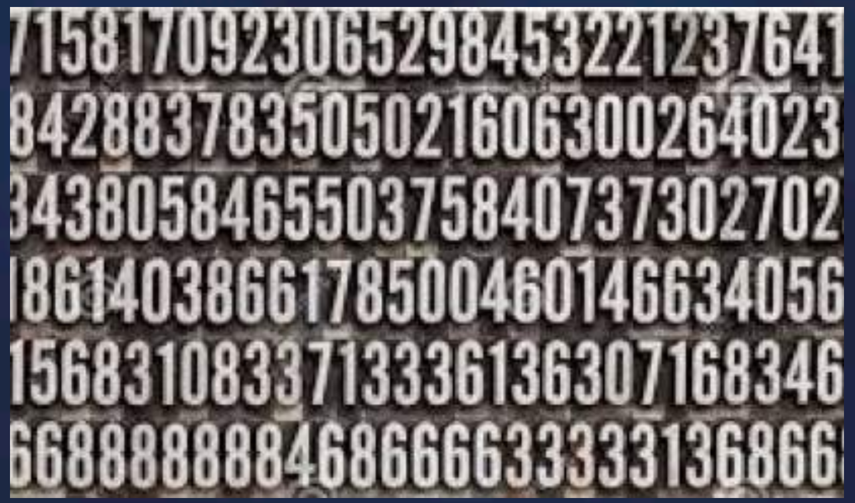
… But They Offer Remarkable Opportunities



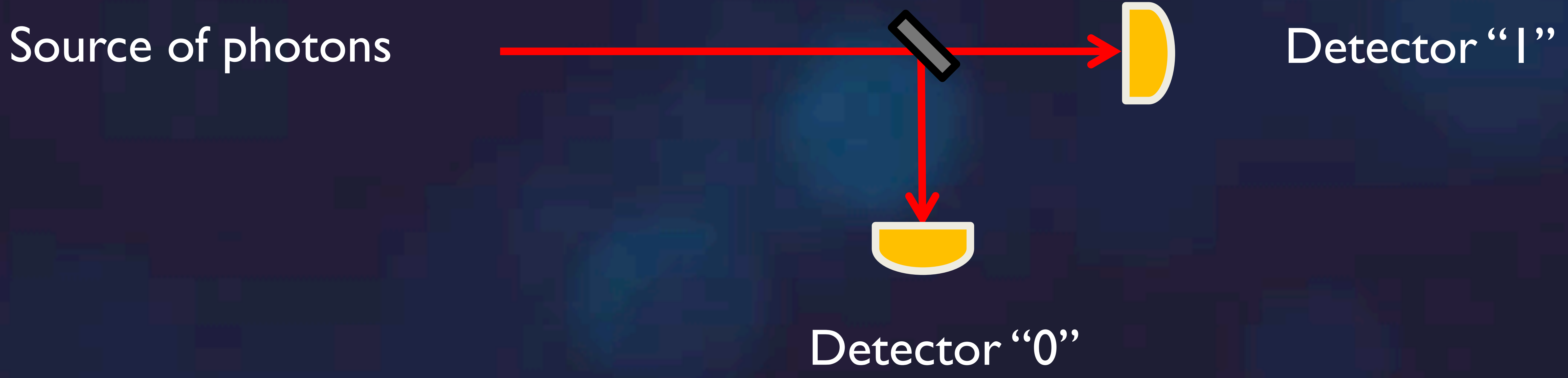
Simple Quantum Technology: Quantum Random Number Generator

RQC | Russian Quantum Center

- First-principles calculations (Monte-Carlo).
- Information security and cryptography.
- E-commerce.
- Lotteries and online casinos.



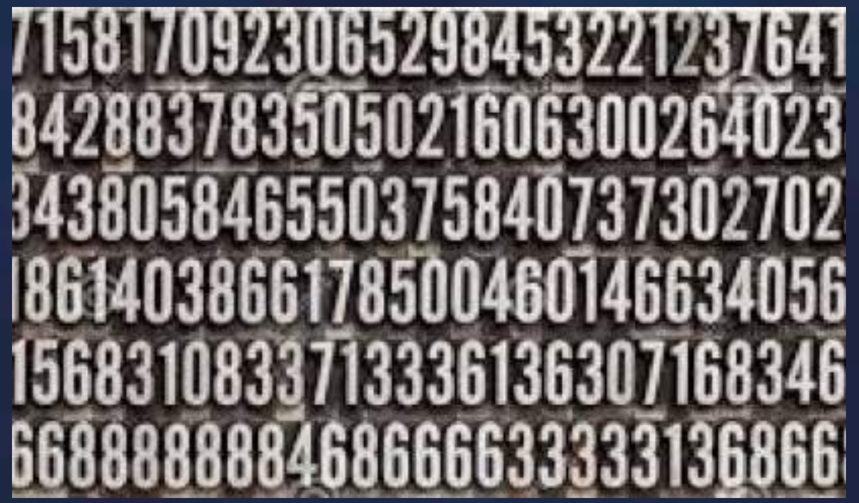
Simple Quantum Technology:
Quantum Random Number Generator



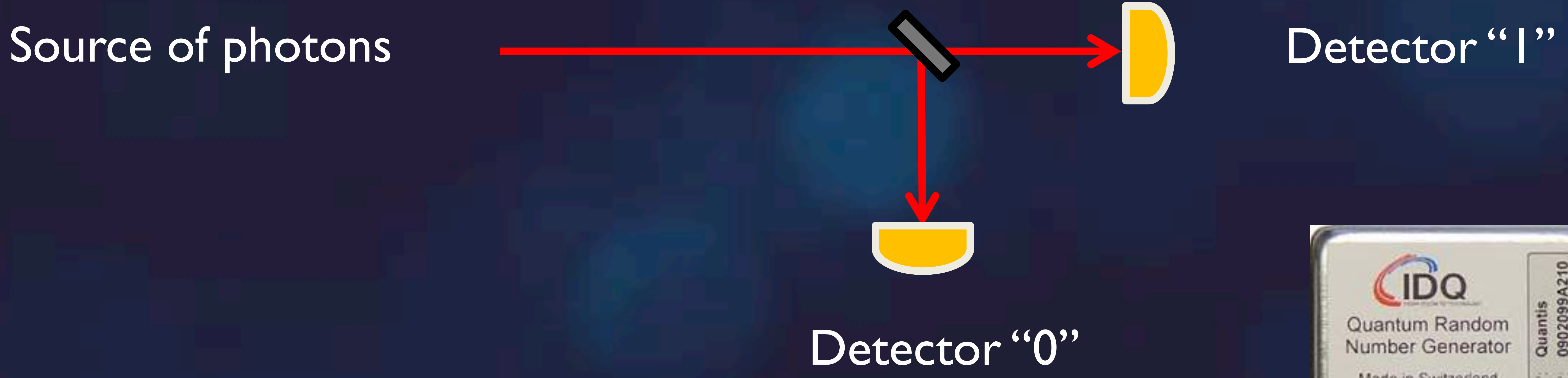
Simple Quantum Technology: Quantum Random Number Generator

Russian Quantum Center

- First-principles calculations (Monte-Carlo).
- Information security and cryptography.
- E-commerce.
- Lotteries and online casinos.



Simple Quantum Technology:
Quantum Random Number Generator



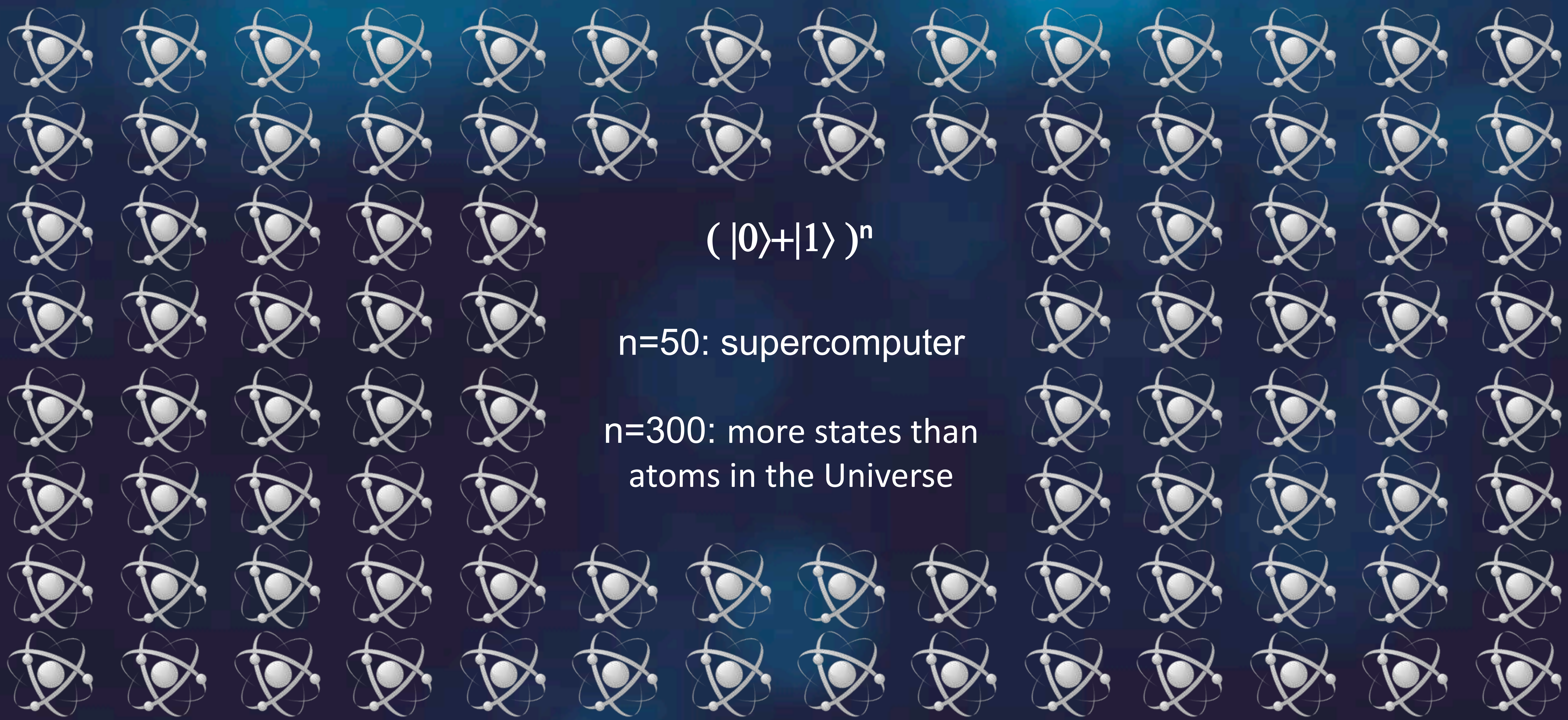
From Superposition to Quantum Information

$$|0\rangle + |1\rangle$$

From Superposition to Quantum Information

$$(|0\rangle+|1\rangle)^2=|00\rangle+|01\rangle+|10\rangle+|11\rangle$$

From Superposition to Quantum Information



$(|0\rangle + |1\rangle)^n$

n=50: supercomputer

n=300: more states than atoms in the Universe

Impossible to simulate using supercomputers!
Idea for a next generation of computers!

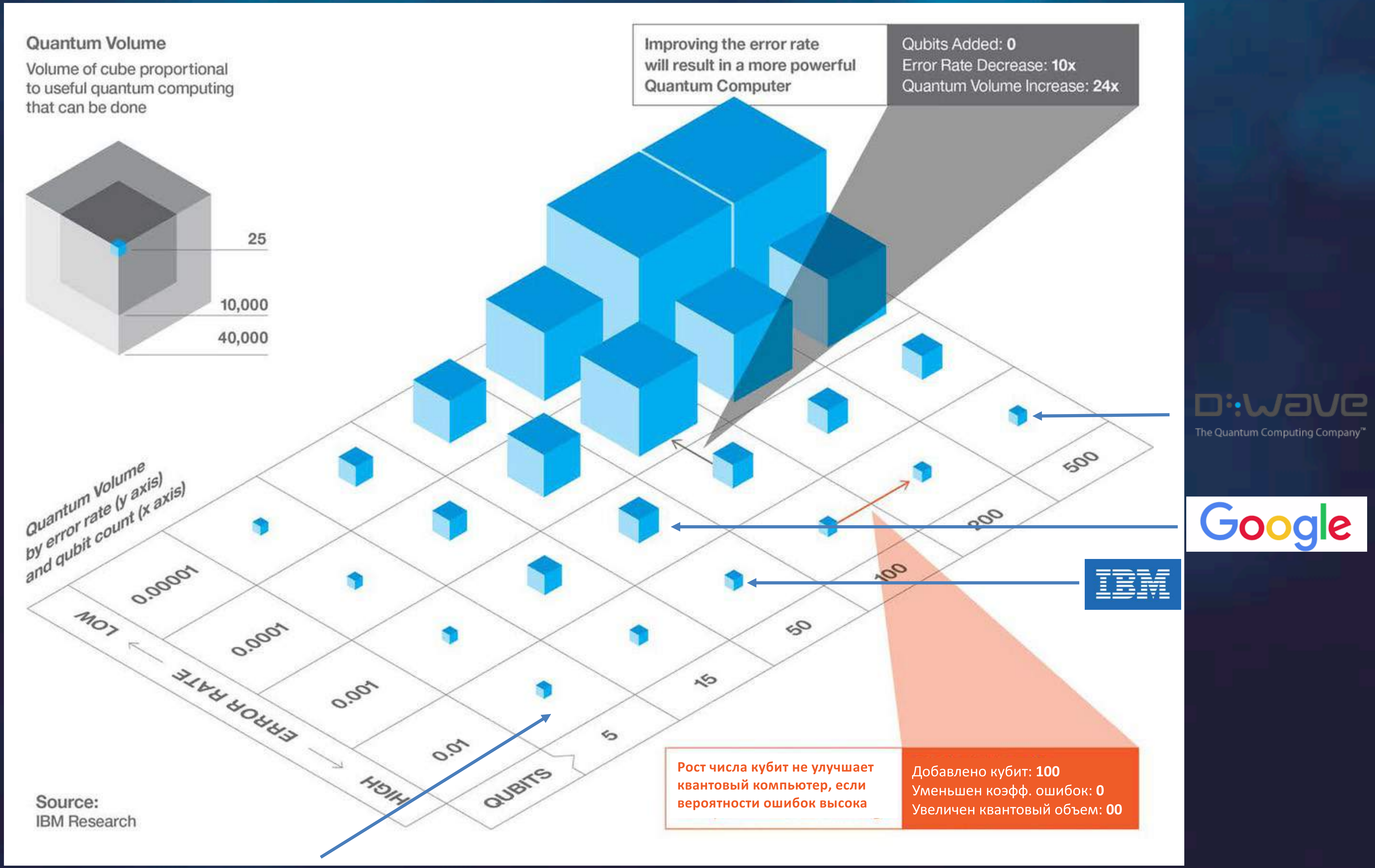
Simulation of quantum computers using classical ones

RQC Russian Quantum Center

Qubits	Memory	Time for one gate operation
10	16 kByte	microseconds on a watch
20	16 MByte	milliseconds on smartphone
30	16 GByte	seconds on laptop
40	16 TByte	minutes on supercomputer
50	16 PByte	hours on top supercomputer
60	16 EByte	long long time
80	size of visible universe	age of the universe

Source: Presentation by M. Troyer

Quantum Volume



Investments from Governments, HighTech and VC

RQC | Russian Quantum Center

- Governmental programs

USA	China	EU	UK	Canada	Australia	Singapore
$20+ bln	$10 bln	€2+1 bln	$400 mln	$100 mln	$75 mln	$44 mln

- Corporations

Google	intel	IBM	Microsoft	Alibaba Group 阿里巴巴集团
$100 mln	$50 mln	$100 mln	$100 mln	$150 mln

- Venture: $150+ mln in the last three years

rigetti IONQ D-Wave The Quantum Computing Company™

RQC | Russian Quantum Center

Google

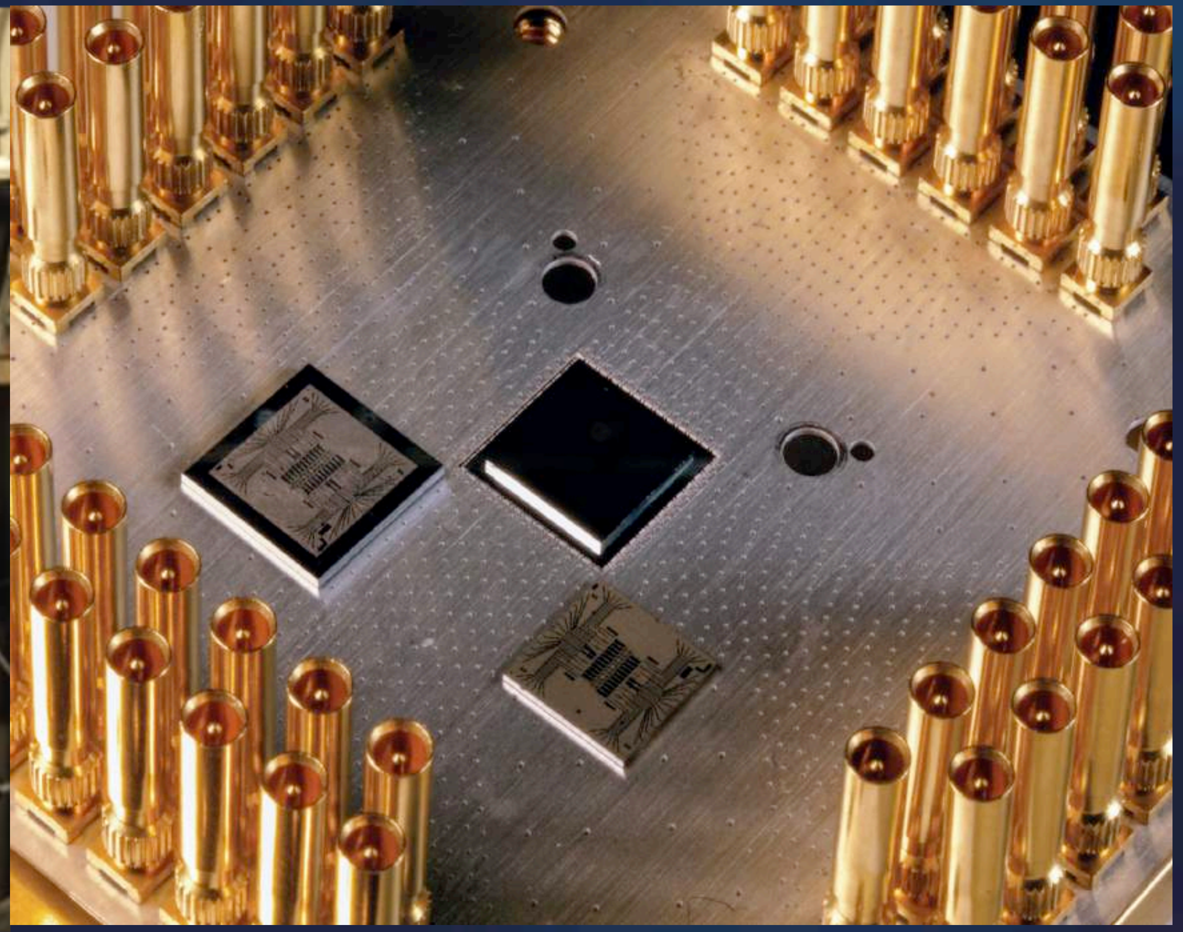
20 qubits

Universal
quantum computer

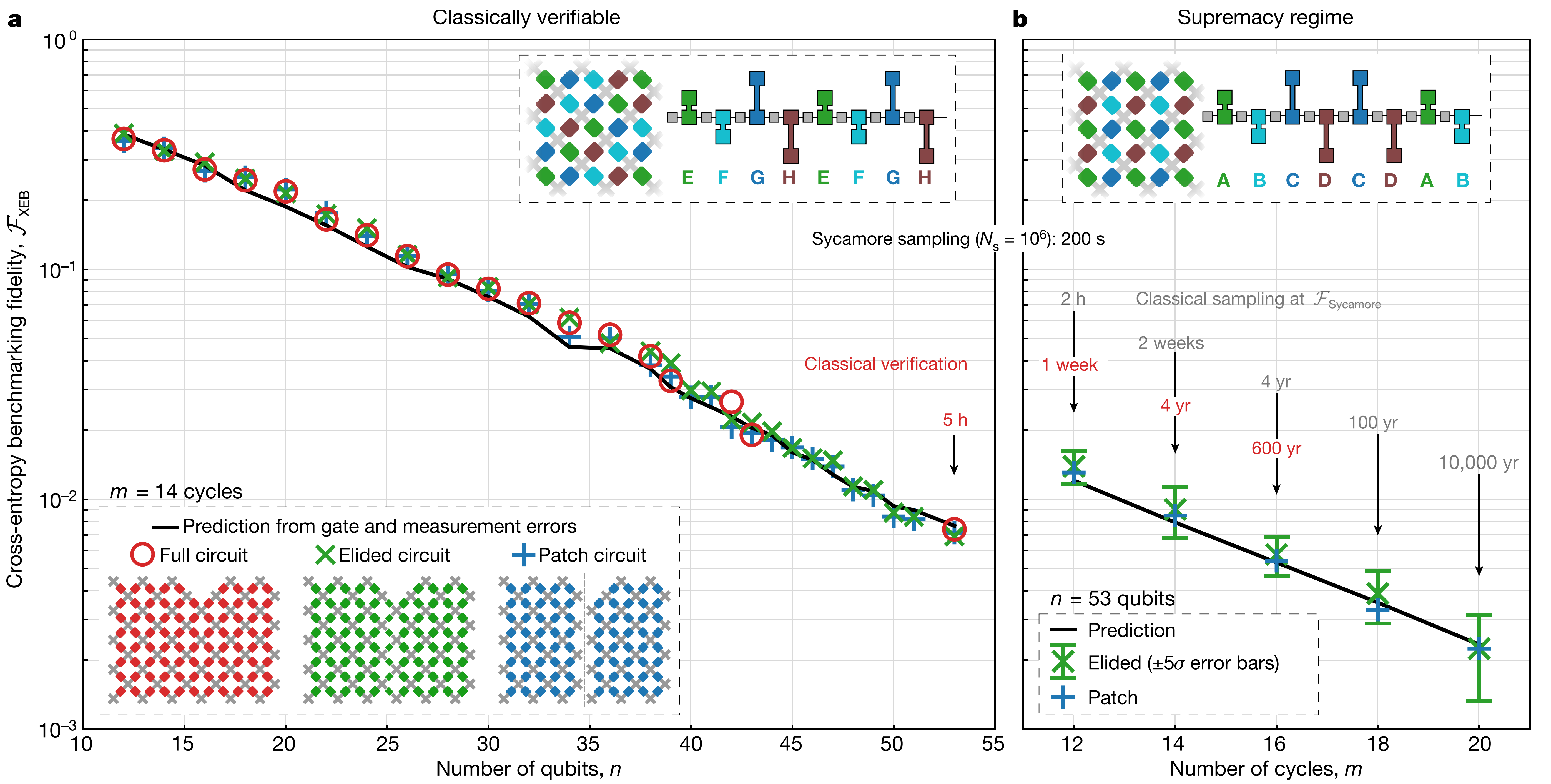
In 2018

72 qubits

John Martinis



Close to demonstrating quantum supremacy

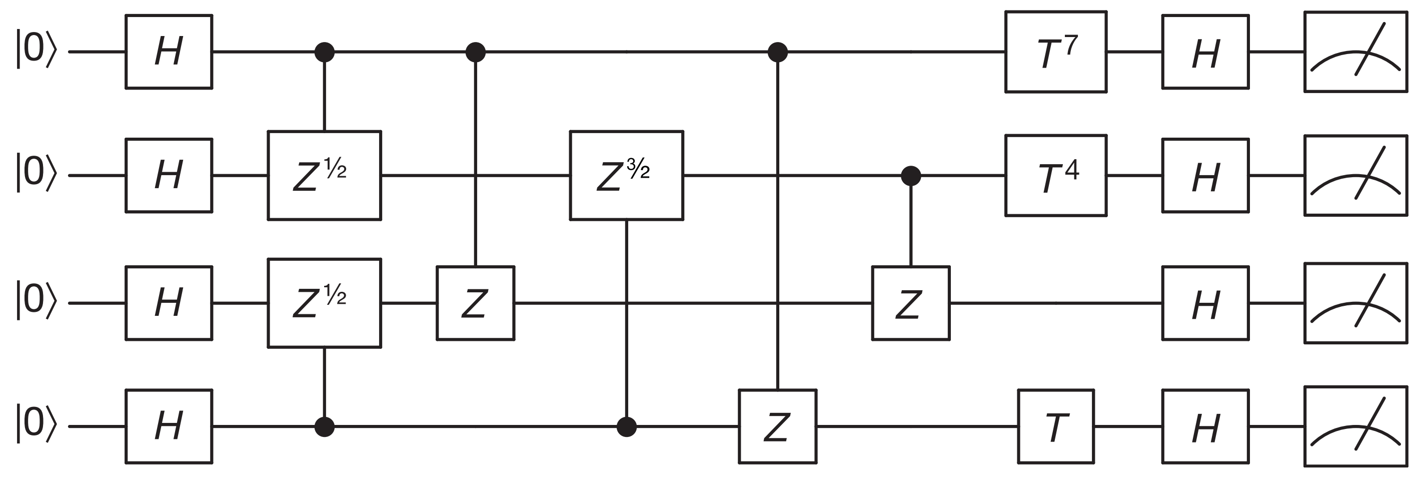


"Our Sycamore processor takes about 200 seconds to sample one instance of a quantum circuit a million times —our benchmarks currently indicate that the equivalent task for a state-of-the-art classical supercomputer would take approximately 10,000 years".

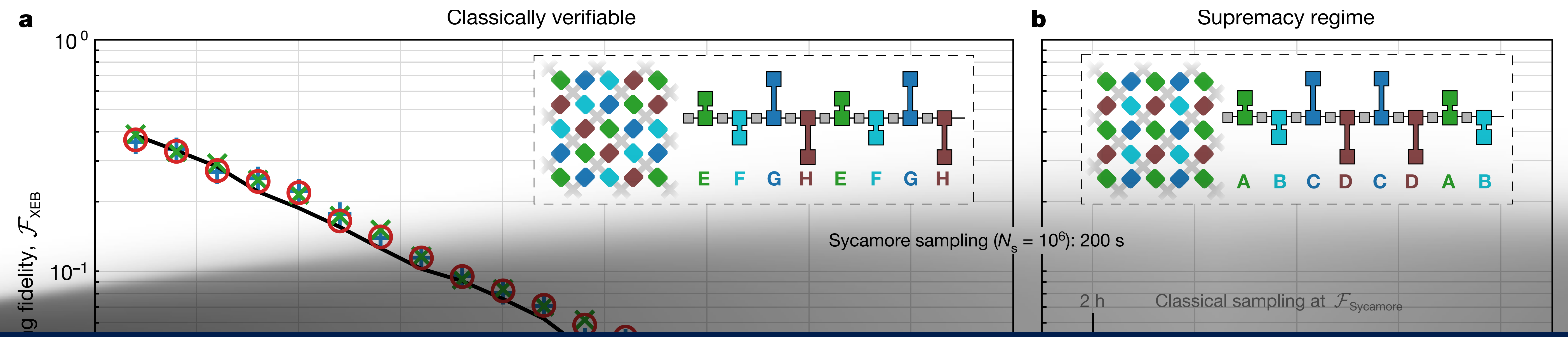
BOX 2

Random quantum circuits

Unlike boson sampling, some quantum-supremacy proposals remain within the standard quantum circuit model. In the model of commuting quantum circuits[10] known as IQP (instantaneous quantum polynomial-time), one considers circuits made up of gates that all commute, and in particular are all diagonal in the X basis; see Box 2 Figure below. Although these diagonal gates may act on the same qubit many times, as they all commute, in principle they could be applied simultaneously. The computational task is to sample from the distribution on measurement outcomes for a random circuit of this form, given a fixed input state. Such circuits are both potentially easier to implement than general quantum circuits and have appealing theoretical properties that make them simpler to analyse[11,18]. However, this very simplicity may make them easier to simulate classically too. Of course, one need not be restricted to commuting circuits to demonstrate supremacy. The quantum-AI group at Google has recently suggested an experiment based on superconducting qubits and non-commuting gates[12]. The proposal is to sample from the output distributions of random quantum circuits, of depth around 25, on a system of around 49 qubits arranged in a 2D square lattice structure (see Fig. 1). It has been suggested[12] that this should be hard to simulate, based on (a) the absence of any known simulation requiring less than a petabyte of storage, (b) IQP-style theoretical arguments[18] suggesting that larger versions of this system should be asymptotically hard to simulate, and (c) numerical evidence[12] that such circuits have properties that we would expect in hard-to-simulate distributions. If this experiment were successful, it would come very close to being out of reach of current classical simulation (or validation, for that matter) using current hardware and algorithms.



Box 2 Figure | Example of an IQP circuit. Between two columns of Hadamard gates (H) is a collection of diagonal gates (T and controlled-$\sqrt{Z}$). Although these diagonal gates may act on the same qubit many times they all commute, so in principle could be applied simultaneously.



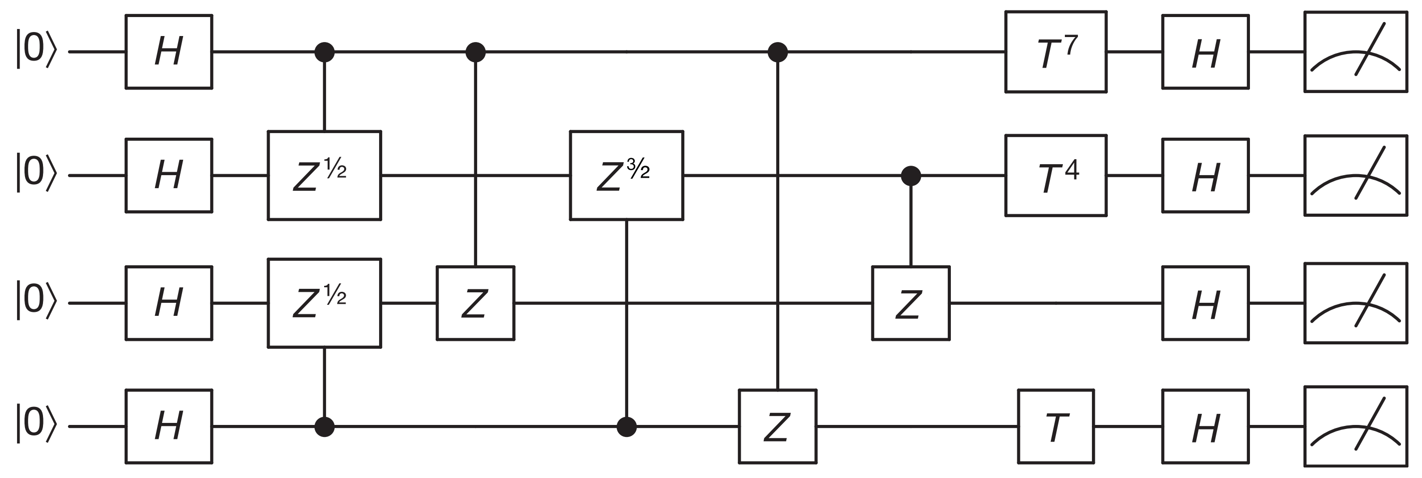
BOX 2
Random quantum circuits

Unlike boson sampling, some quantum-supremacy proposals remain within the standard quantum circuit model. In the model of commuting quantum circuits[10] known as IQP (instantaneous quantum polynomial-time), one considers circuits made up of gates that all commute, and in particular are all diagonal in the X basis; see Box 2 Figure below. Although these diagonal gates may act on the same qubit many times, as they all commute, in principle they could be applied simultaneously. The computational task is to sample from the distribution on

IBM: 10'000 years can be reduced to several days. Let us wait!

come very close to being out of reach of current classical simulation (or validation, for that matter) using current hardware and algorithms.

"Our Sycamore processor takes about 200 seconds to sample one instance of a quantum circuit a million times —our benchmarks currently indicate that the equivalent task for a state-of-the-art classical supercomputer would take approximately 10,000 years".



Box 2 Figure | Example of an IQP circuit. Between two columns of Hadamard gates (*H*) is a collection of diagonal gates (*T* and controlled-√*Z*). Although these diagonal gates may act on the same qubit many times they all commute, so in principle could be applied simultaneously.

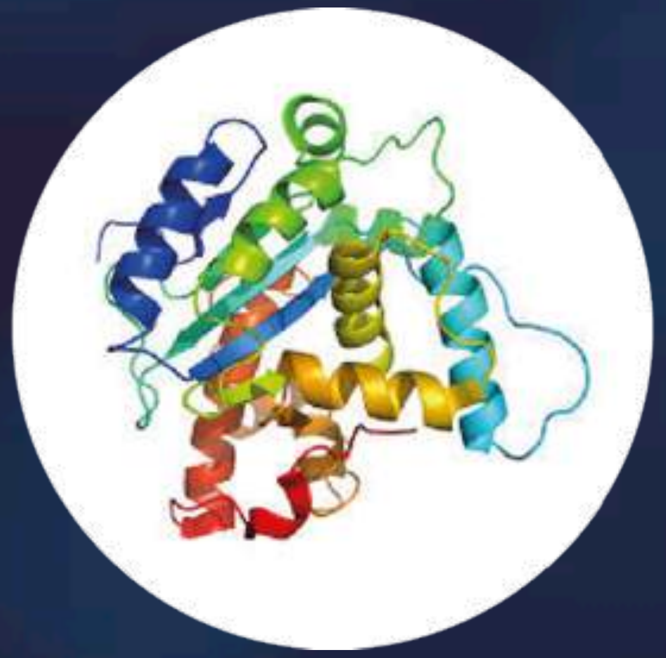
Why Do We Need Quantum Computers?

Why Do We Need Quantum Computers?

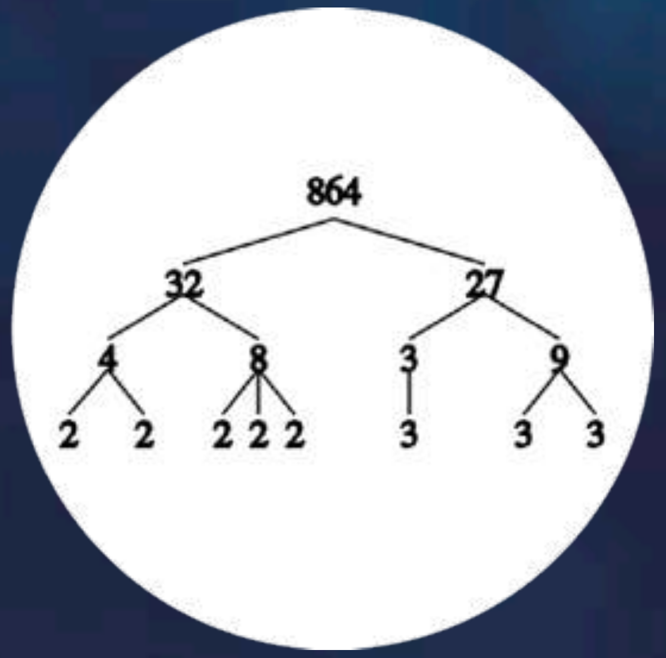
RQC Russian Quantum Center

Search and optimisation

Simulating complex systems



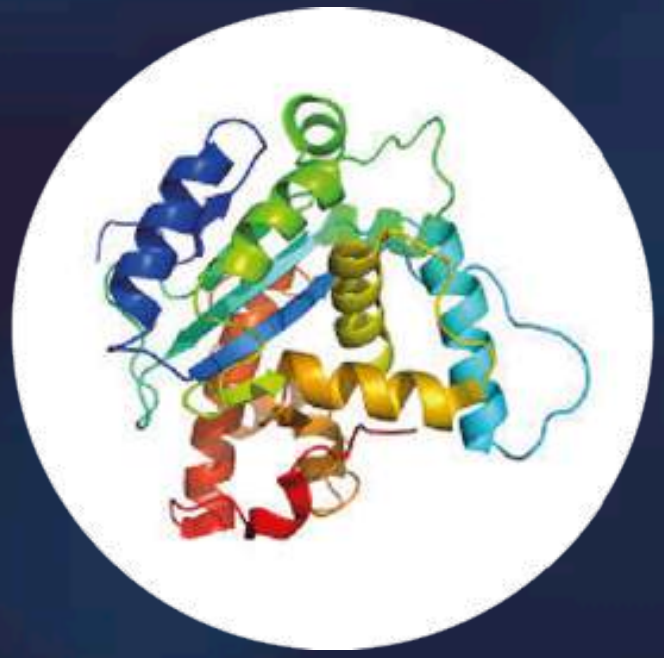
Factorization



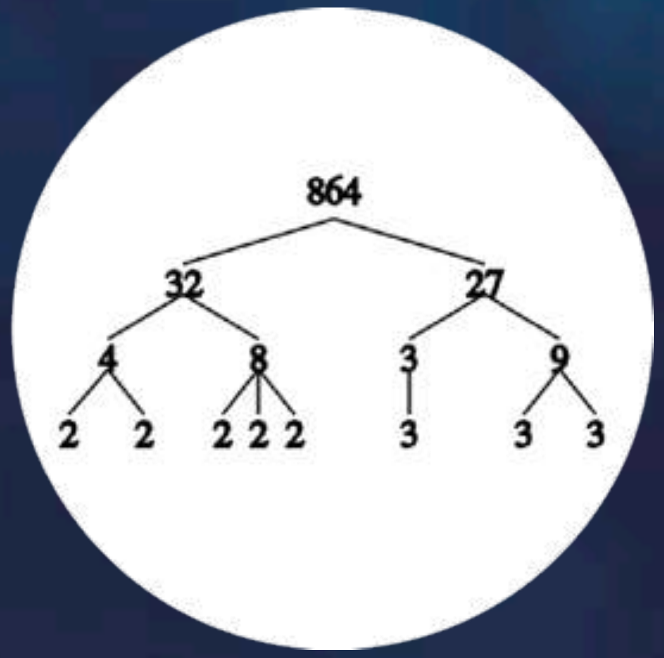
Why Do We Need Quantum Computers?

Search and optimisation

Simulating complex systems



Factorization



Bad news: Breaking popular public-key cryptography primitives:

Peter Shor has proposed an algorithm for factorization and discrete logarithms for polynomial time for a quantum computer.

Quantum Computers for Breaking Cryptosystems

- Modern asymmetric cryptography is based on the complexity of solving a certain class of mathematical problems, for example, factorization (factorization into prime factors).

- At the moment, an effective algorithm for solving such a problem is unknown, so an attacker needs a lot of time to crack a cryptographic key.

- In 1995, Peter Shore proposed an algorithm for factorization and discrete logarithms for polynomial time for a quantum computer.

- The number 15 was decomposed into multipliers 3 and 5 using a quantum computer using a computer with 7 qubits.

Quantum Computers for Breaking Cryptosystems

Estimation based on 10 ns gate time and 2N+3 logical qubits

RSA	cracked in	CPU years	Shor
453 bits	1999	10	1 hour
768 bits	2009	2000	5 hours
1024 bits		1000000	10 hours

Quantum computers for breaking cryptosystems

RQC Russian Quantum Center

1995:
Universal quantum computer
2N+1 logical qubits

Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer

Peter W. Shor (AT&T Research)

(Submitted on 30 Aug 1995 (v1), last revised 25 Jan 1996 (this version, v2))

2012:
Universal quantum computer
1’000’000’000 physical qubits
1.1 day

Surface codes: Towards practical large-scale quantum computation

Austin G. Fowler, Matteo Mariantoni, John M. Martinis, Andrew N. Cleland

(Submitted on 4 Aug 2012 (v1), last revised 27 Oct 2012 (this version, v2))

2018:
No universal quantum computer

Variational Quantum Factoring

Eric R. Anschuetz, Jonathan P. Olson, Alán Aspuru-Guzik, Yudong Cao

(Submitted on 27 Aug 2018)

2019:
Universal quantum computer
8’000’000 physical qubits
8 hours

How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits

Craig Gidney, Martin Ekerå

(Submitted on 23 May 2019)

Applying Grover's algorithm to AES: quantum resource estimates

Markus Grassl[1], Brandon Langenberg[2], Martin Roetteler[3] and Rainer Steinwandt[2]

[1] Universität Erlangen-Nürnberg & Max Planck Institute for the Science of Light

[2] Florida Atlantic University

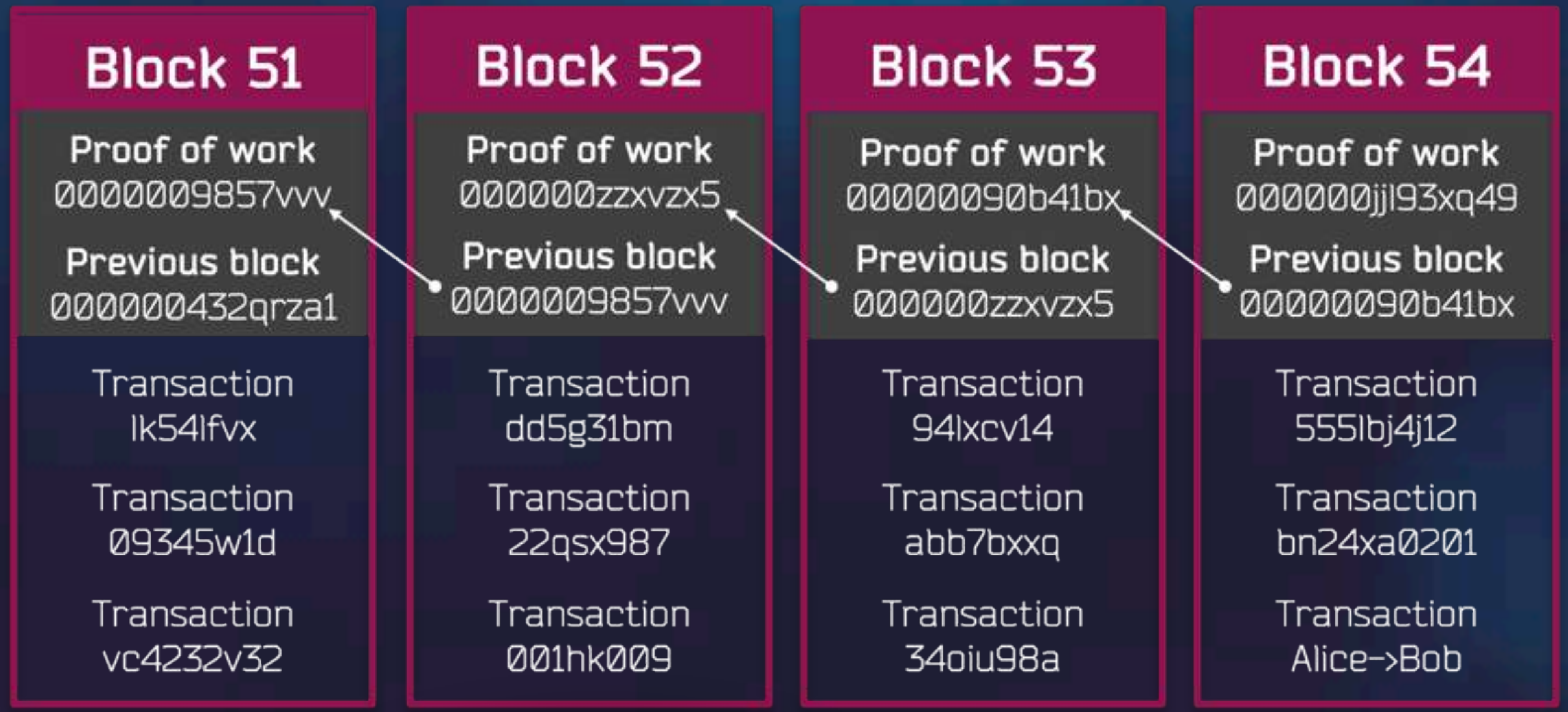
[3] Microsoft Research

February 24, 2016

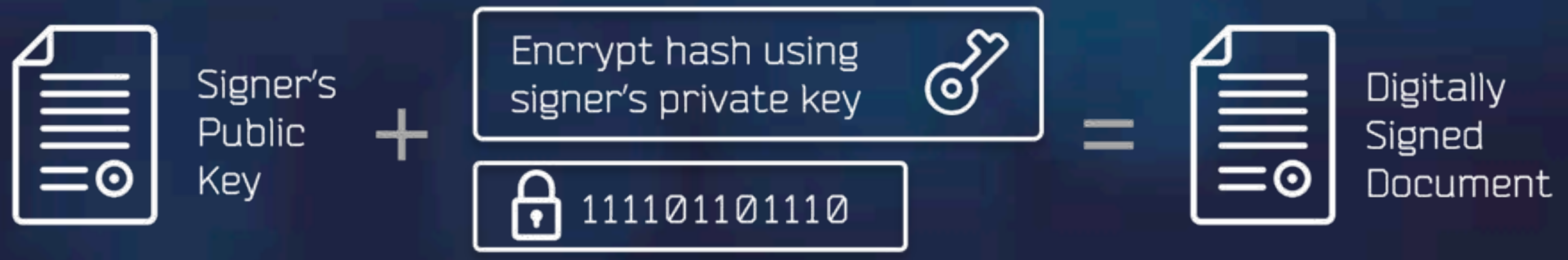
Impact on symmetric cryptography: Exhaustive search of a k-bit key in time $2^{k/2}$ with

Quantum Security of Blockchains

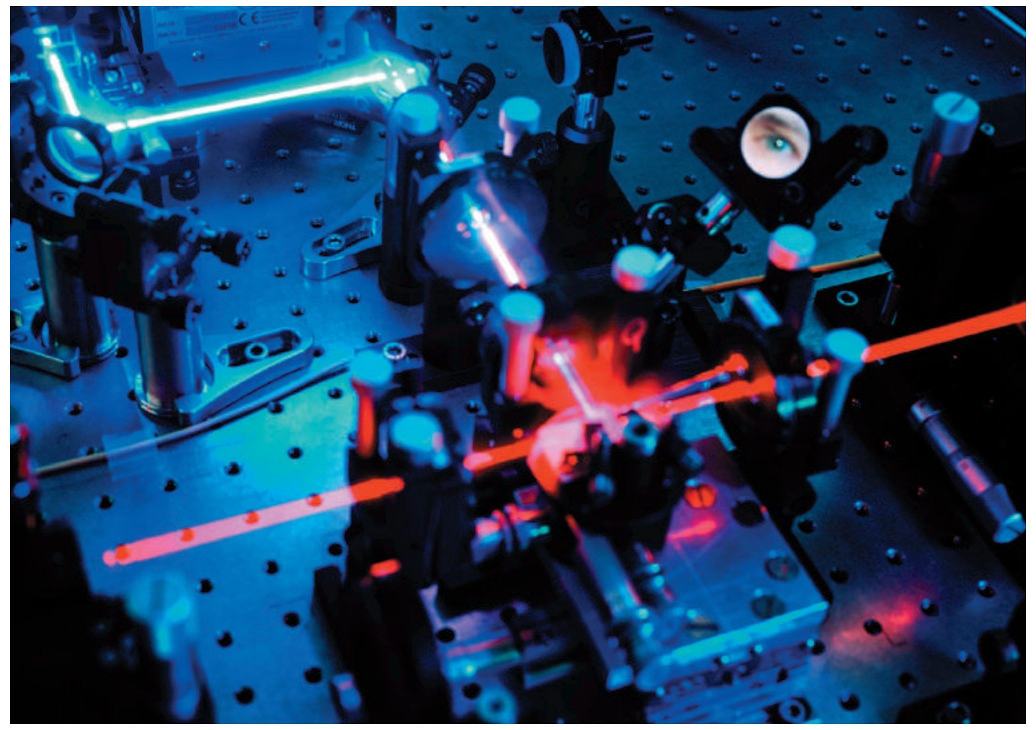
RQC | Russian Quantum Center



Digital signatures – Quantum-unsafe



Hash functions – Believed to be quantum-safe...?

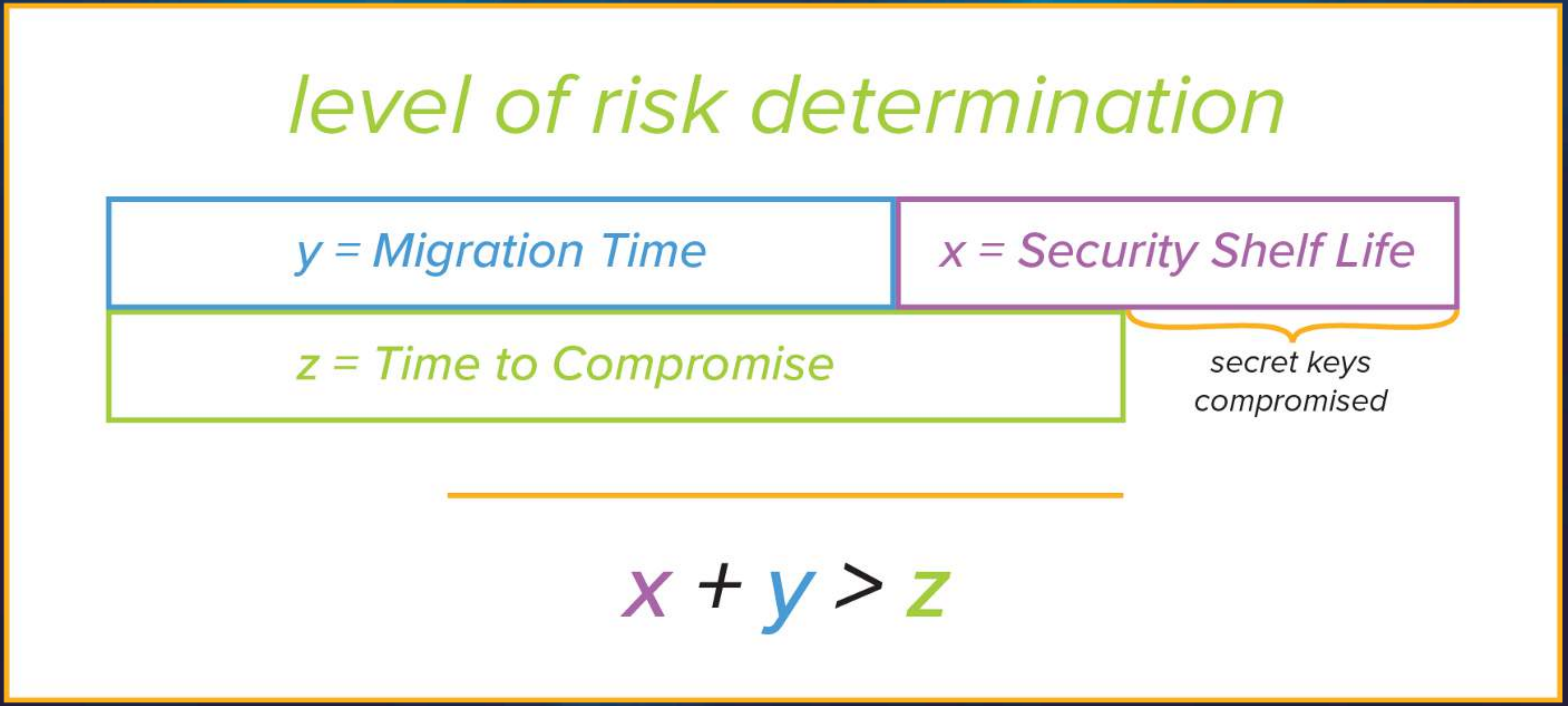


Quantum cryptography equipment, which uses the principle of entanglement to encode data that only the sender and receiver can access.

Quantum computers put blockchain security at risk

Bitcoin and other cryptocurrencies will founder unless they integrate quantum technologies, warn **Aleksey K. Fedorov**, **Evgeniy O. Kiktenko** and **Alexander I. Lvovsky**.

Mosca Theorem



Post-quantum cryptography is cryptography under the assumption that the attacker has a large quantum computer

Long-range Post-Quantum Security Plan


Deloitte.
University Press

Signals for Strategists

From fantasy to reality

Quantum computing is coming to the marketplace

By David Schatsky and Ramya Kunnath Puliyakodil

Introduction: A new way to solve computationally intensive problems

GRANTED, quantum computing is hard to explain. But that hasn't stopped the fantastical technology from attracting billions of dollars of R&D investment, catching the eye of venture capital firms, and spurring research programs at big tech companies and enterprises. Some companies are getting a head start on applying quantum technology to computationally intensive problems in finance, risk management, cybersecurity, materials science, energy, and logistics.

Signals

- In the last three years, venture capital investors have placed $147 million with quantum computing startups; governments globally have provided $2.2 billion in support to researchers[1]
- Some of the world's leading tech companies have active quantum computing programs
- Financial services, aerospace and defense, and public sector organizations are researching quantum computing applications
- Quantum computer maker D-Wave Systems announced the general availability of its next-

1

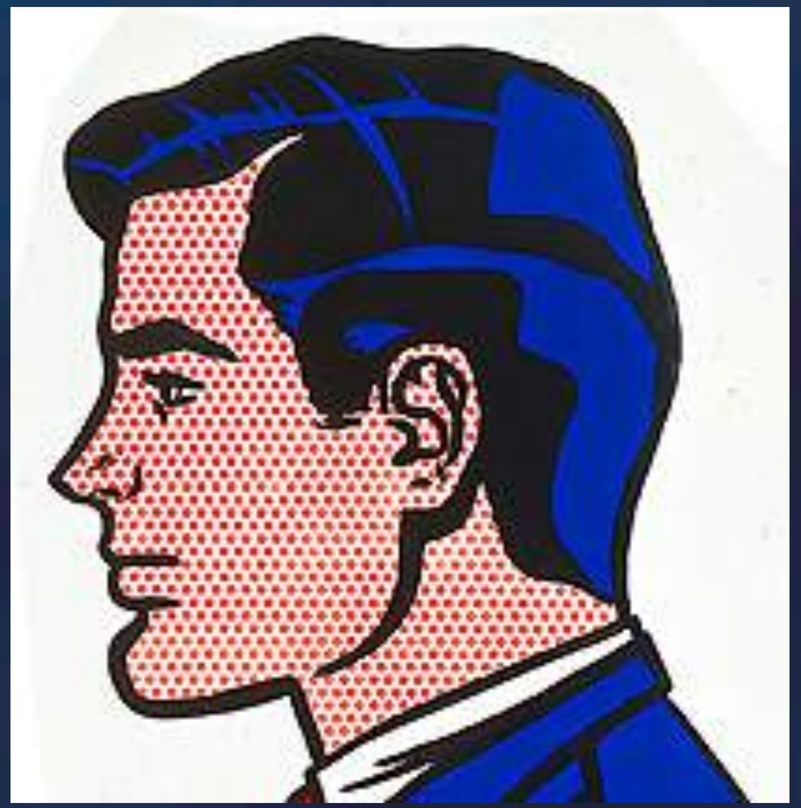
… Firms need to pay attention to these developments and have roadmaps in place to follow through on those recommendations.

<u>A risk is that adversaries could capture and store encrypted data today for decryption in the future, when quantum computers become available</u>.


New
Q-safe
algorithms
QKD

Kotelnikov-Shannon Theory on Absolute Security

Transferring secure message using unsecured channel: encryption

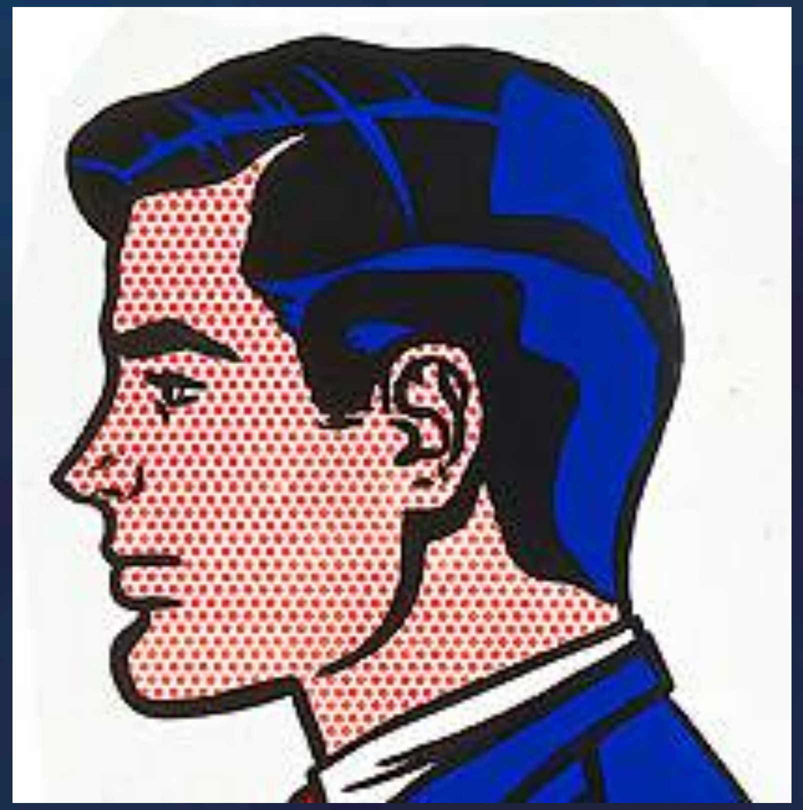


- the key is secret, it is known to only the legitimate users;
- the key length is no shorter than the message length;
- the key is random;
- the key is employed only once.

Idea: make (message)XOR(key) operation with one-time key. Never re-use!

Kotelnikov-Shannon Theory on Absolute Security

Transferring secure message using unsecured channel: encryption



- the key is secret, it is known to only the legitimate users;
- the key length is no shorter than the message length;
- the key is random;
- the key is employed only once.

How distribute this key? No RSA/DH because of quantum attackers…

Industry Experience in Quantum Computing

RQC Russian Quantum Center

Quantum-safe (quantum-secured, quantum-resistant) cryptography

Methods that are protected from attacks with quantum computers

Post-quantum Cryptography

New generation of cryptographic algorithms, that are based on mathematical tasks with equivalent (or comparable) complexity both for classical and quantum computers

Quantum Cryptography (Quantum communications, quantum key distribution and etc)

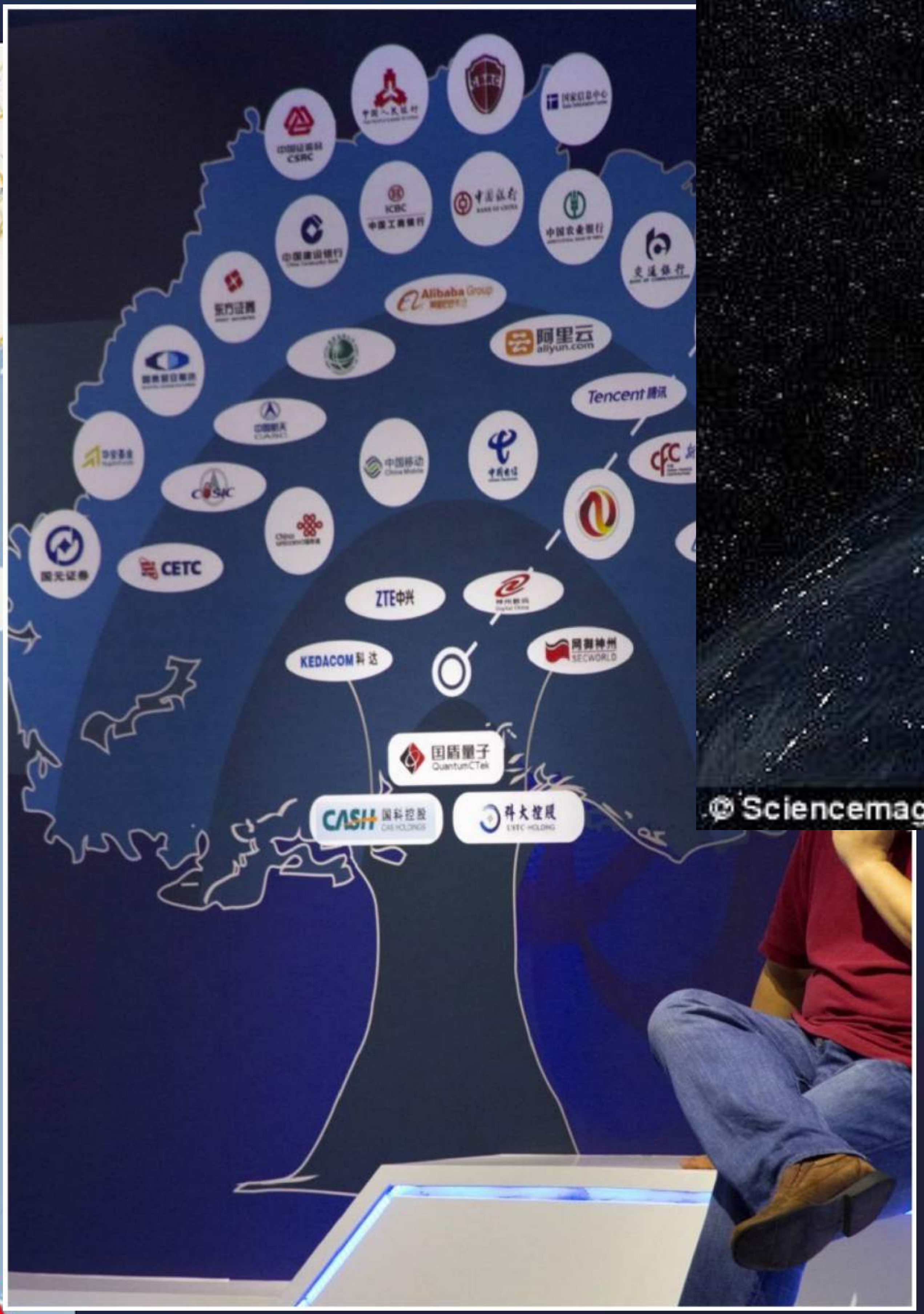
Using of quantum states for distribution of keys for encryption.

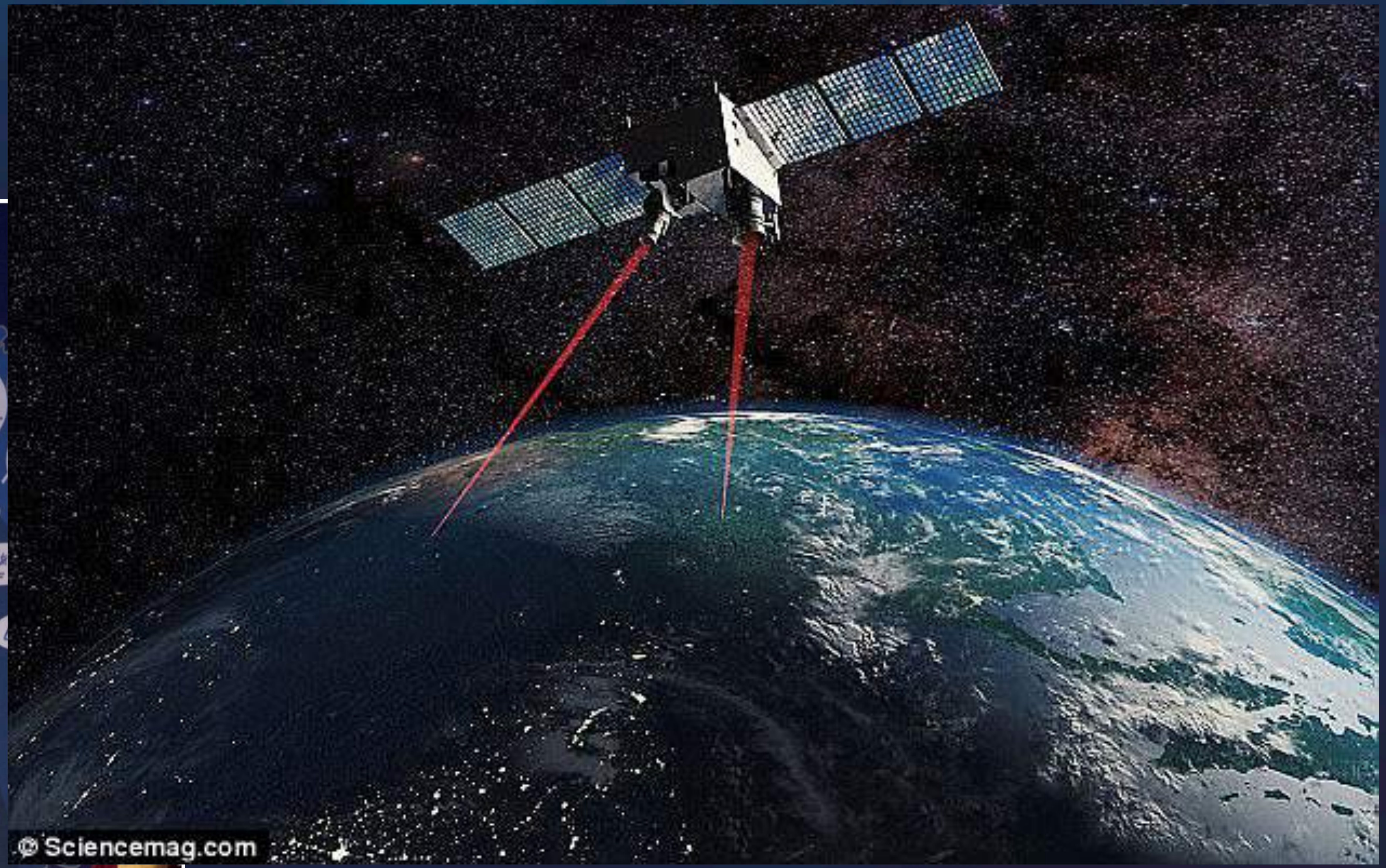
Quantum Key Distribution

- Split photons
- Copy quantum states
- Measure without disturbing

Quantum Key Distribution

2000 km "Quantum backbone"





Quantum satellite: cryptography more than 1200 km, teleportation more than 500 km

Quantum Key Distribution

RQC | Russian Quantum Center

СБЕРБАНК

Б. Андроновский переулок

АМИКОН

Ул. Вавилова

VPN-tunnel

Quantum Key Distribution

RQC | Russian Quantum Center

СБЕРБАНК

Б. Андроновский переулок

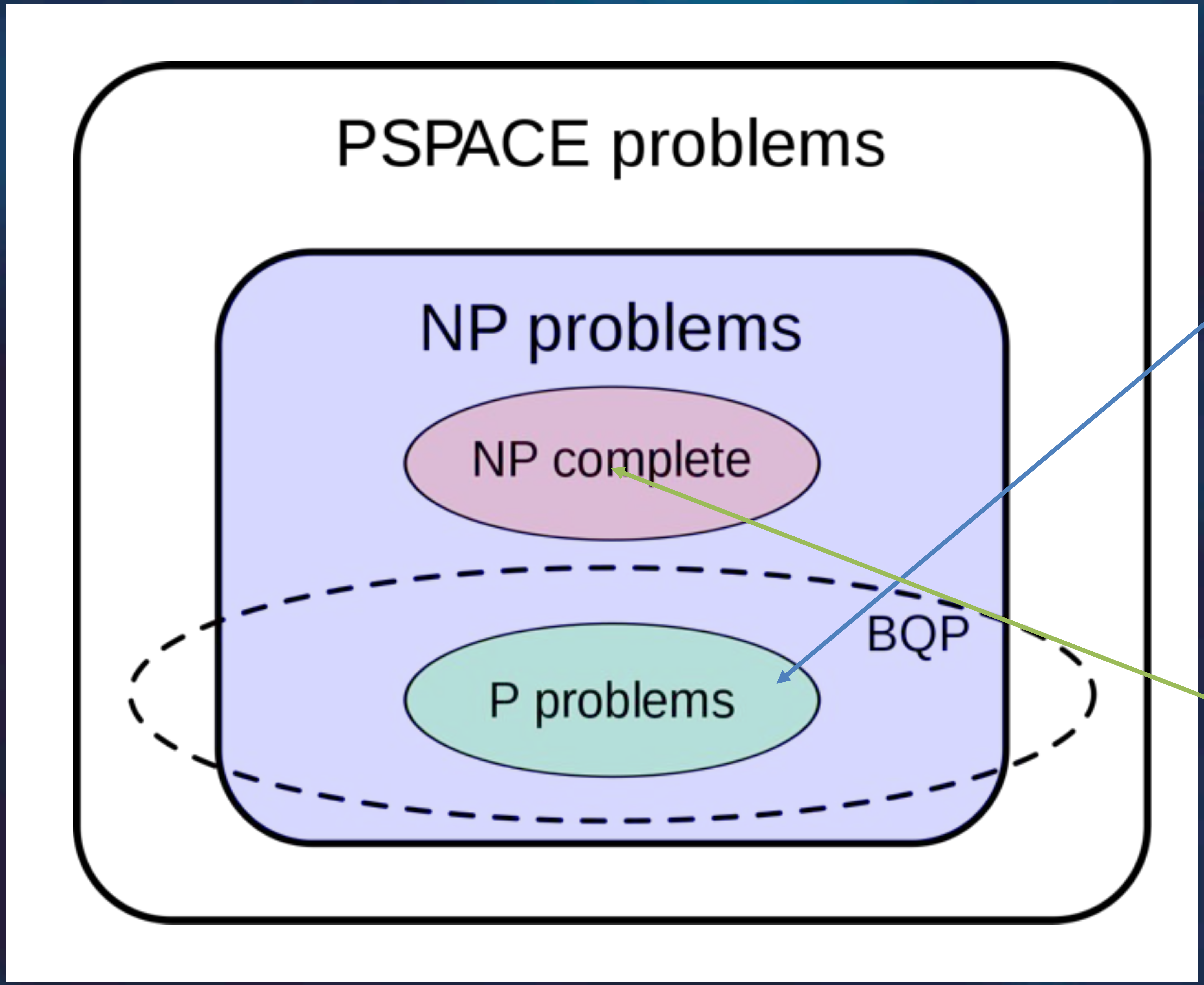
АМИКОН

VPN-tunnel

Ул. Вавилова


New
Q-safe
algorithms
QKD

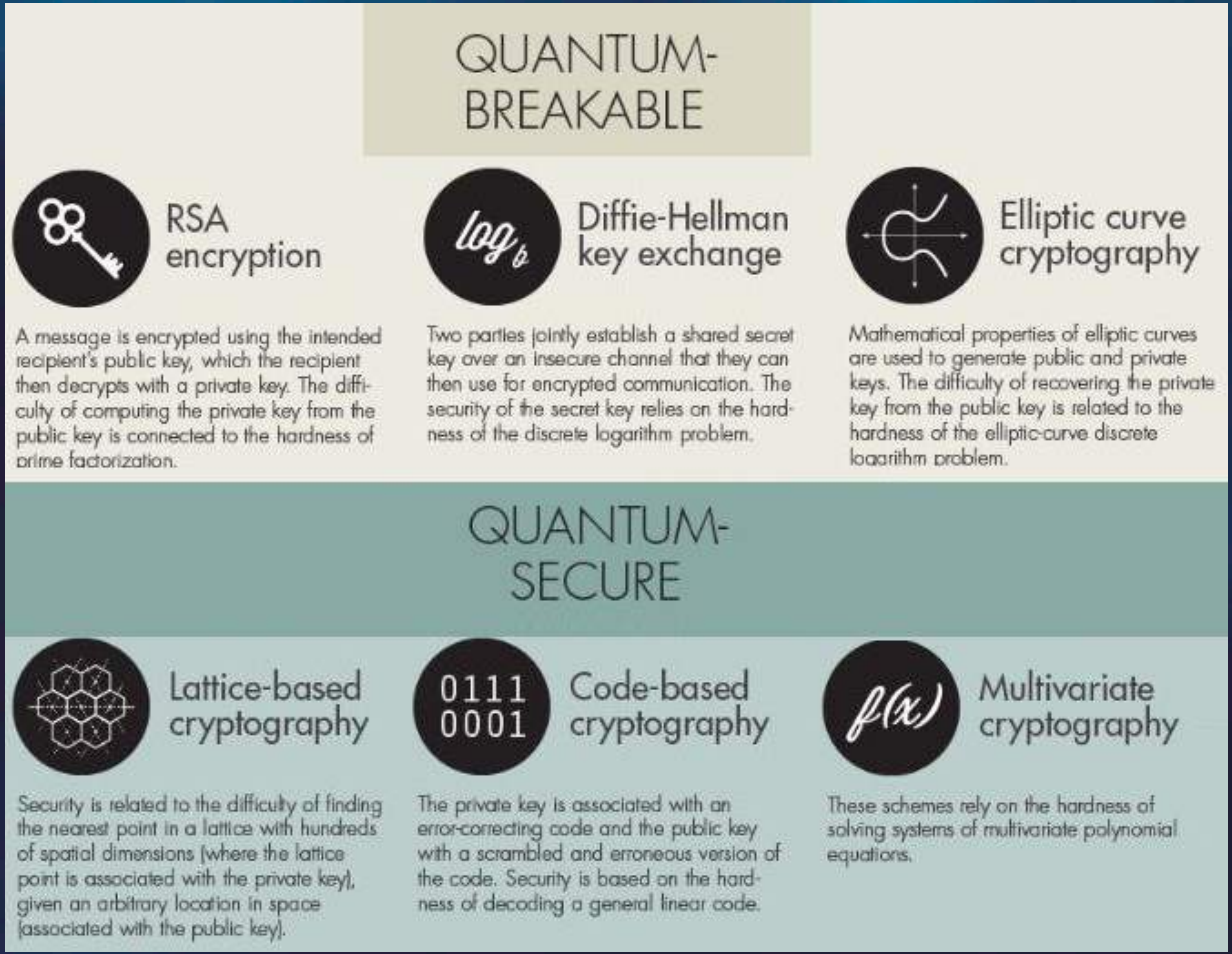
Post-Quantum Algorithms



Cryptography of today. To break it a classical computer need exponential time (very slow), quantum needs polynomial time (very fast).

Post-quantum cryptography. Tasks with equivalent (or comparable) complexity both for classical and quantum computers.

Post-Quantum Algorithms



Make quantum-security update with us: our core solution

PQRL Library: This is a set of tools that allows upgrading your products and infrastructure to quantum security quickly, simply, and conveniently.

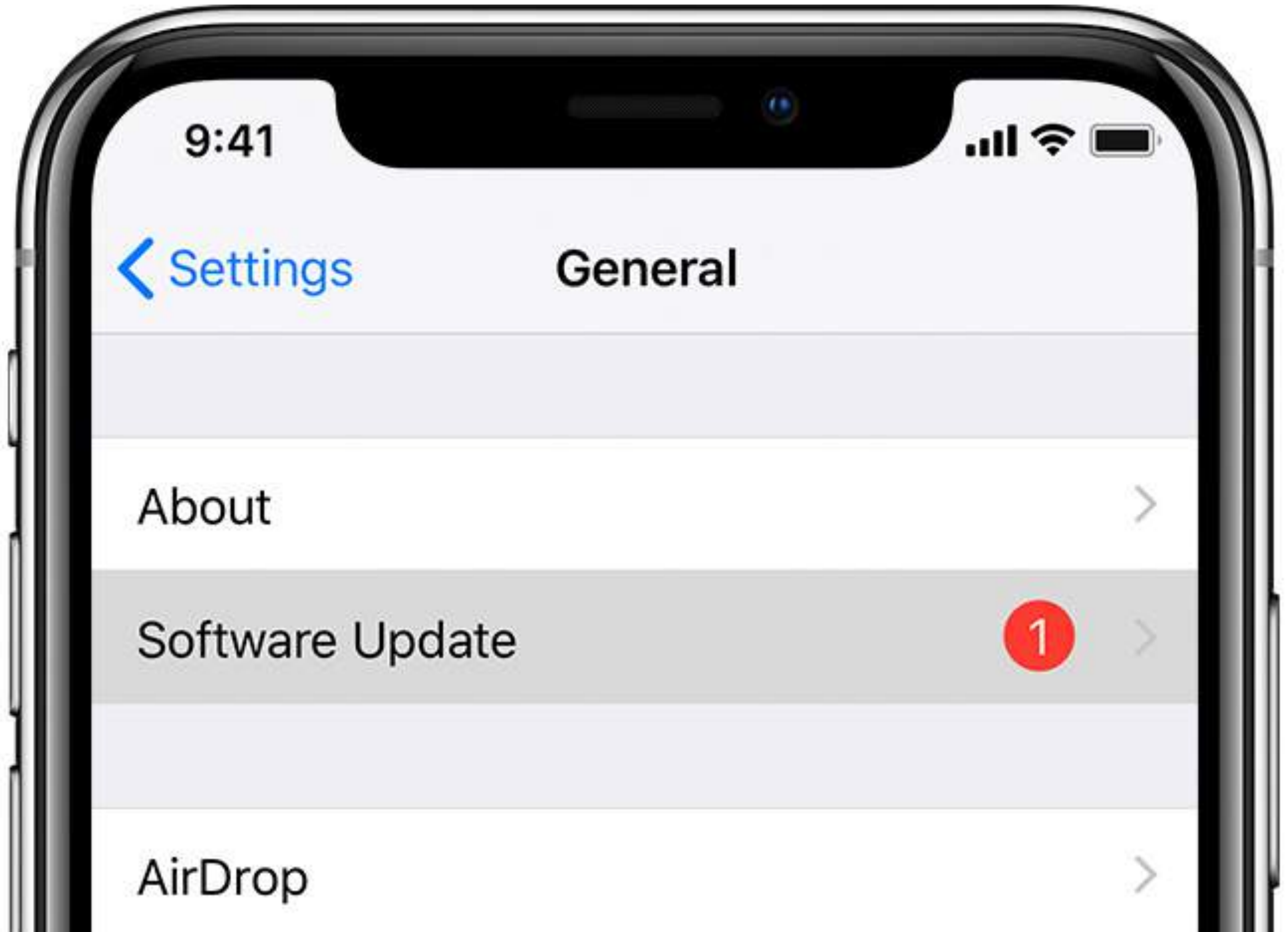
Easy-to-use

Documentation and support

Examples

Benchmarks and optimization

Version control



Think Big — Scale Fast

RQC | Russian Quantum Center

Thank you for your attention!

Aleksey Fedorov

Make quantum-security update with us: our core solution

Cross-platform	OpenSSL Integration	Cryptography schemes	Easy to use
Linux on x86-64, ARM v7 **Windows** 2012+ on x86-64 **Android**, ARM v7	TLS 1.3 **NewHope** For Key Distribution: **SPHINCS+** For Digital signature: Implemented the most promising post-quantum algorithms of the NIST contest.	Lattice-based Code-based Hash-based Multivariate-based Supersingular Isogeny-based	Regular Updates Adding new post-quantum algorithms, following OpenSSL update cycle, backward compatibility, bug fixing. Well-documented code with examples. Implementation on C without dependencies.

Make quantum-security update with us: our core solution

	PQLR SDK		End Products		
Industry	Private Data	Industrial IOT	Financial Data	Medical / DNA	Connected Vehicles
Target Client	Acronis	BOSCH	SBERBANK	Genotek	KAMAZ
Use-Case	Post-quantum data integrity control in backup and data recovery solutions.	Integration of lightweight post-quantum cryptography into the Industrial IoT hardware gateways.	Quantum-protected virtual communication channels. Quantum-secure corporate communications.	Quantum Secure Identity Systems through browsers' extention. Work In Progress 2020, Q1	V2X Quantum-Secured Data Transfer. Firmware Integrity Control (Securing Post Quantum Signatures and Authentication).