QKD-based Security for 5G and Next Generation Networks

Sergiy Gnatyuk

National Aviation University, Kyiv, Ukraine

Vienna, Austria, 18 November, 2021

About the #speaker

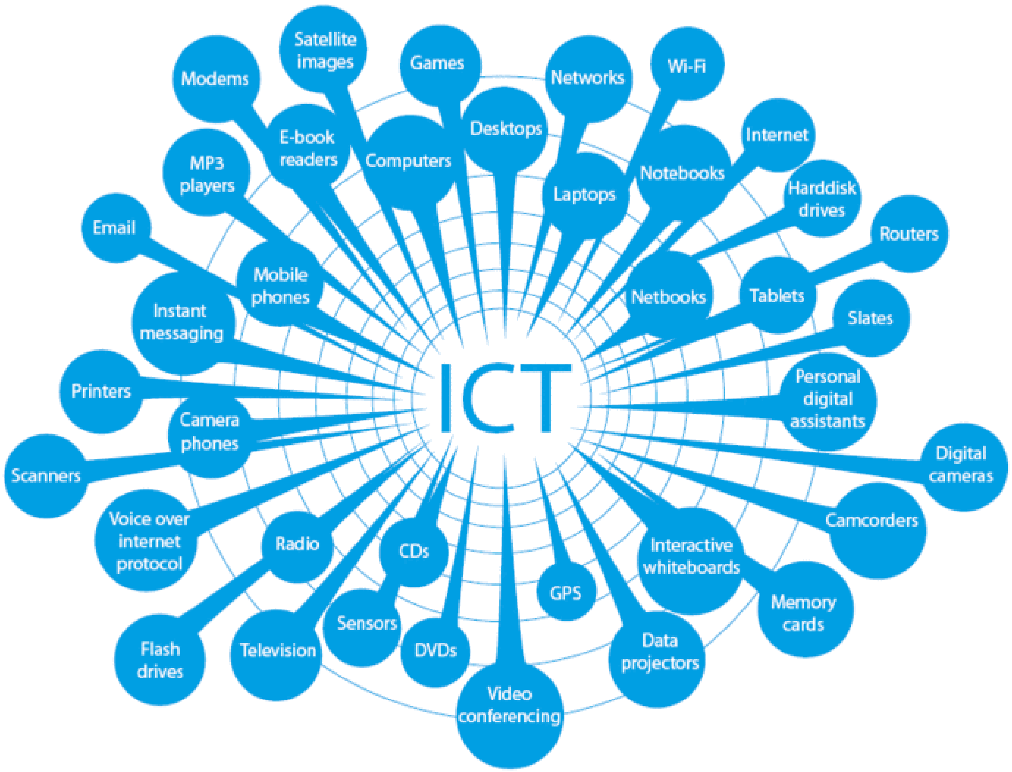
Sergiy Gnatyuk holds PhD and DSc (second academic research degree in Ukraine) in cybersecurity, he is Professor in Computer Science. Sergiy is Professor and Vice-Dean of the Faculty of Cybersecurity, Computer and Software Engineering at National Aviation University as well as Scientific Advisor of the NAU Cybersecurity R&D Lab http://cyberlab.fccpi.nau.edu.ua

Also, Sergiy is a cybersecurity expert and consultant for state and private Ukrainian and international organizations. He is a speaker and organizer of many international cybersecurity events as well as the author of many books, patents and papers.

The topics of the papers and books are cybersecurity, QKD, 5G and NGN security, incidents response, CIIP and others.

+380971934425
s.gnatyuk@nau.edu.ua
sergio.gnatyuk@gmail.com
https://www.facebook.com/sergiy.gnatyuk

Why Quantum Cryptography?



HPC

SMART GRID

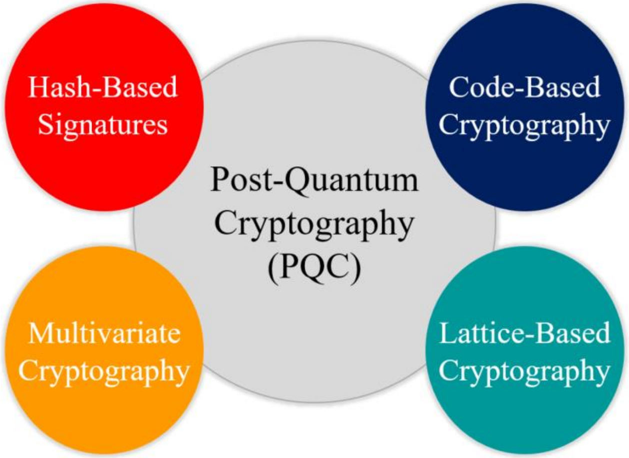
Destructive

Quantum Computing

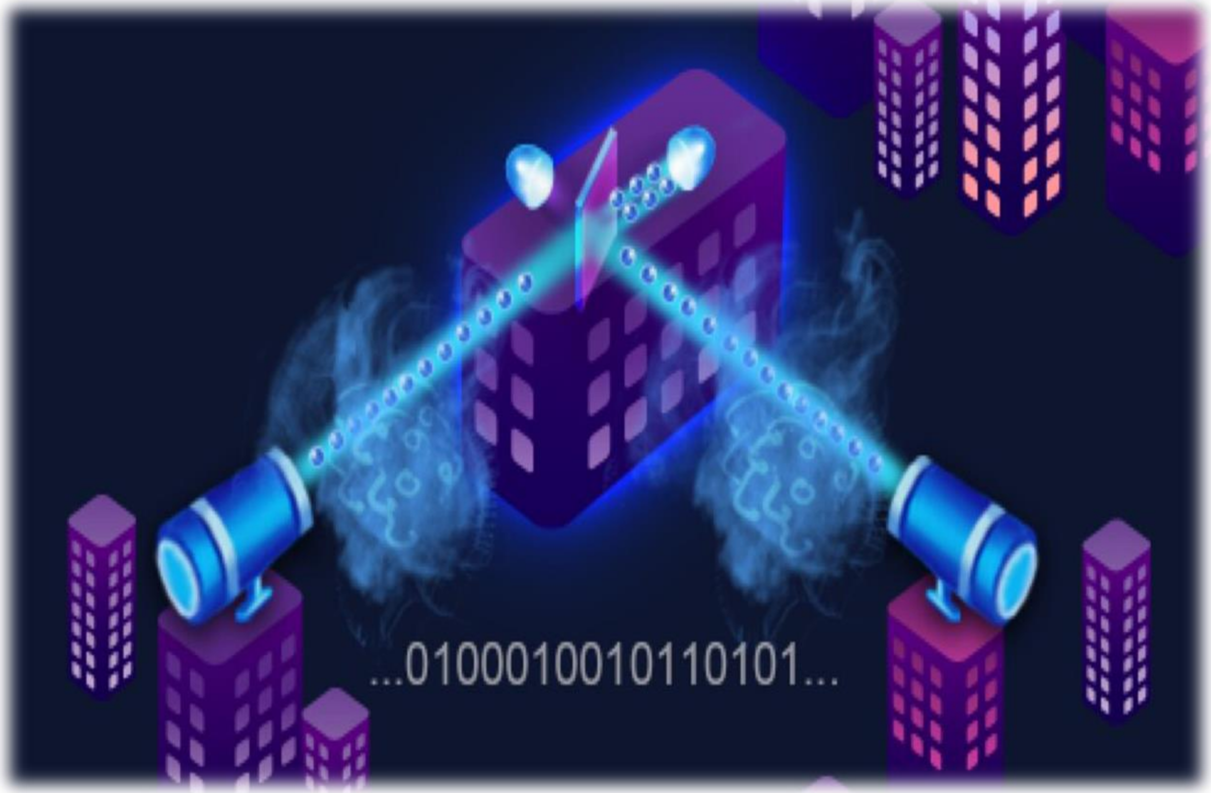
D:WAVE

- unordered database search
- factorization
- logarithm in large discrete fields

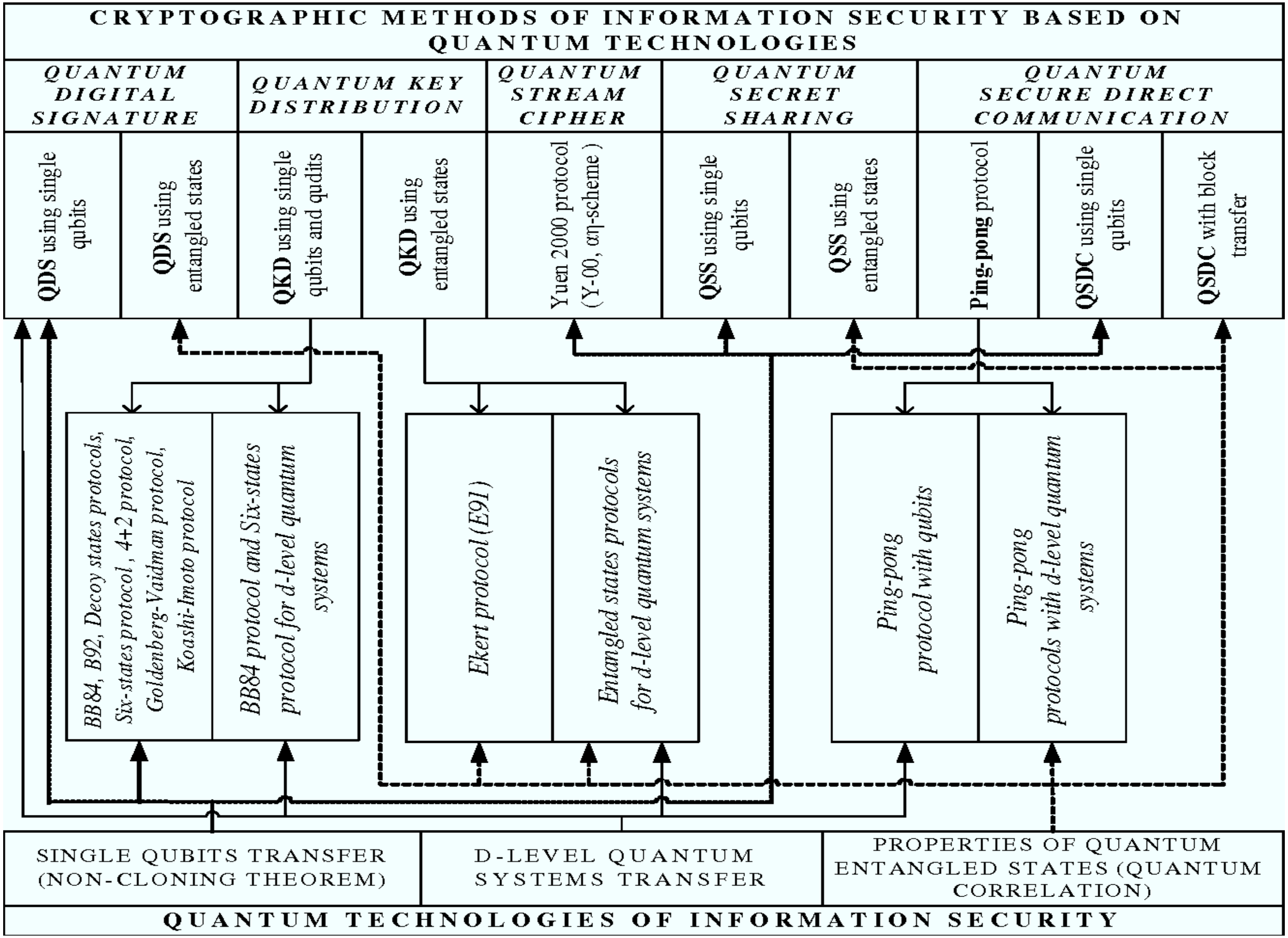
Two ways to protect data



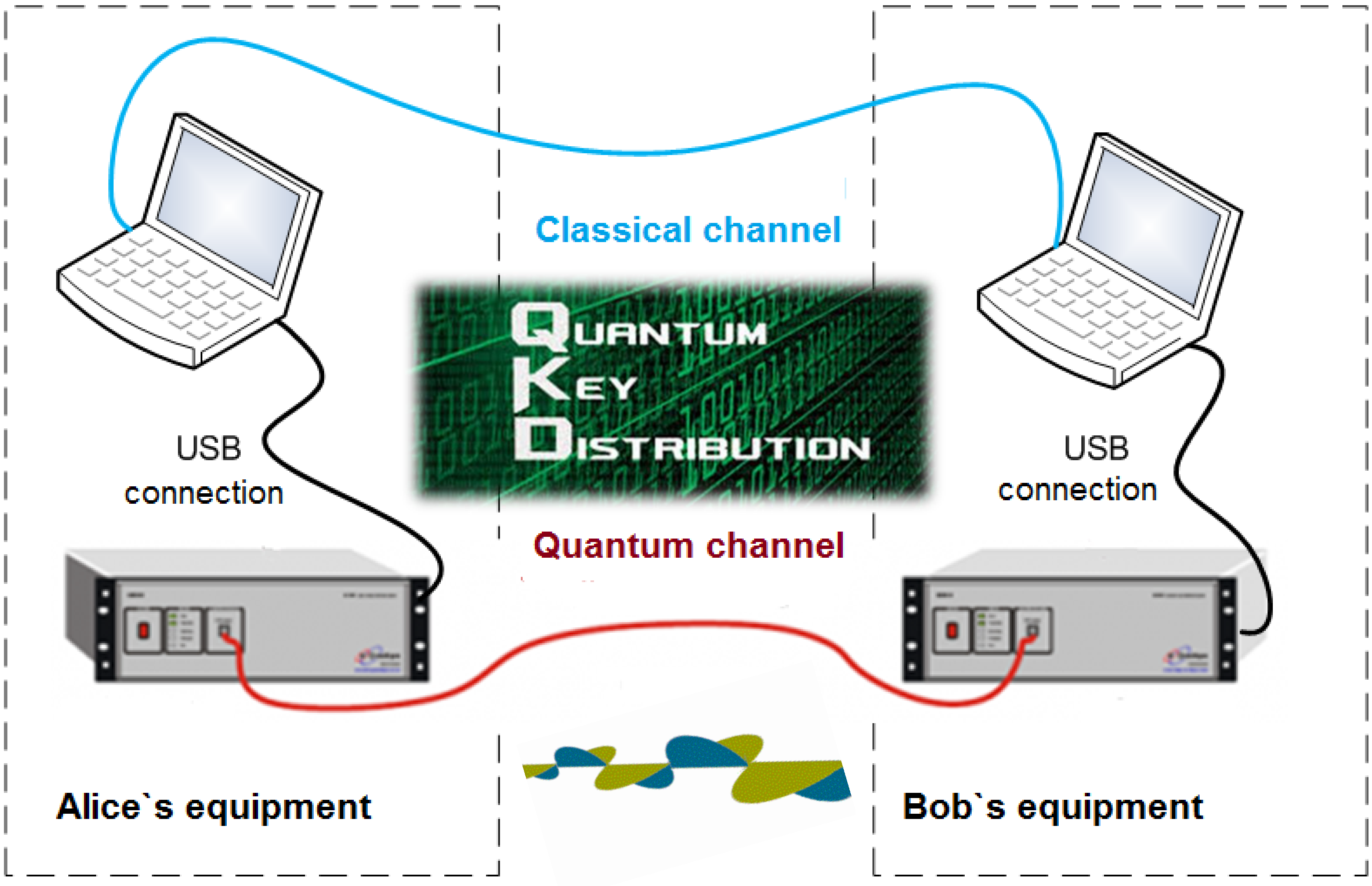
Quantum Cryptography



Modern Quantum Security Direction

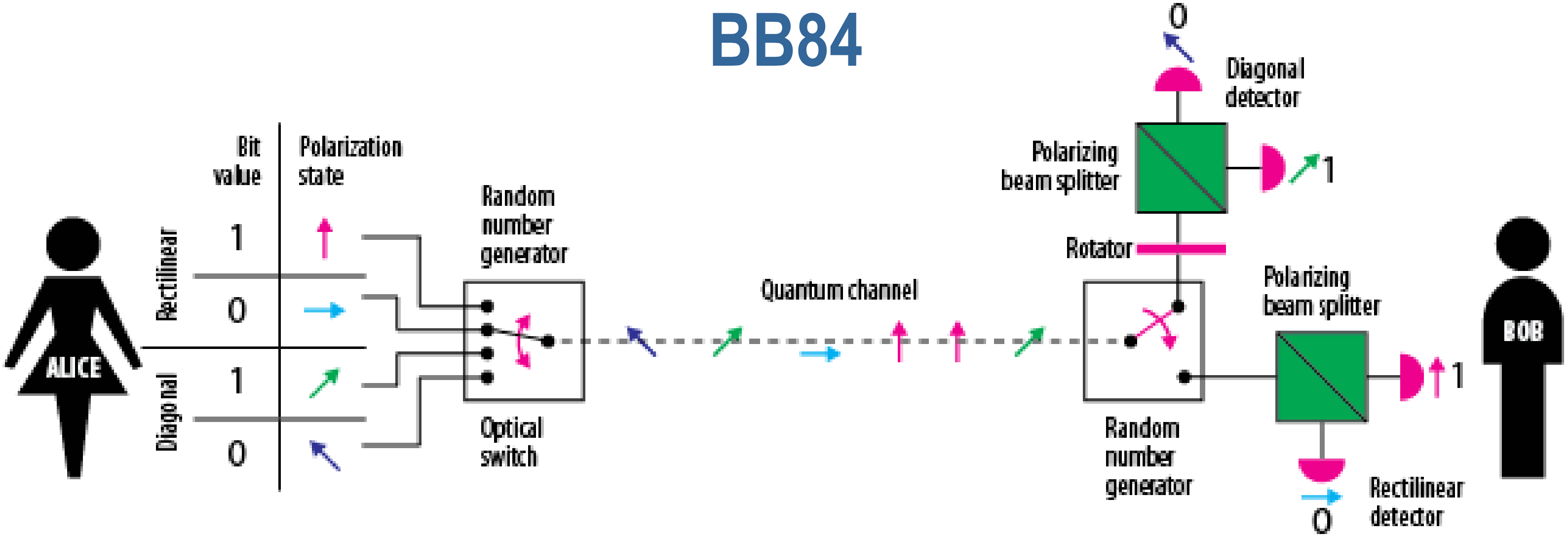


Quantum Key Distribution



Quantum Key Distribution

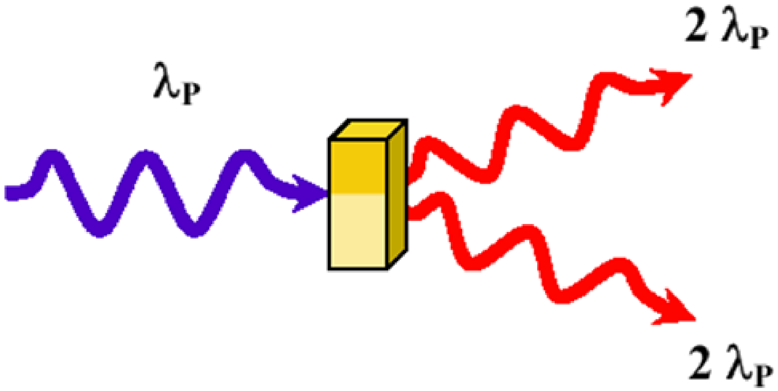
BB84

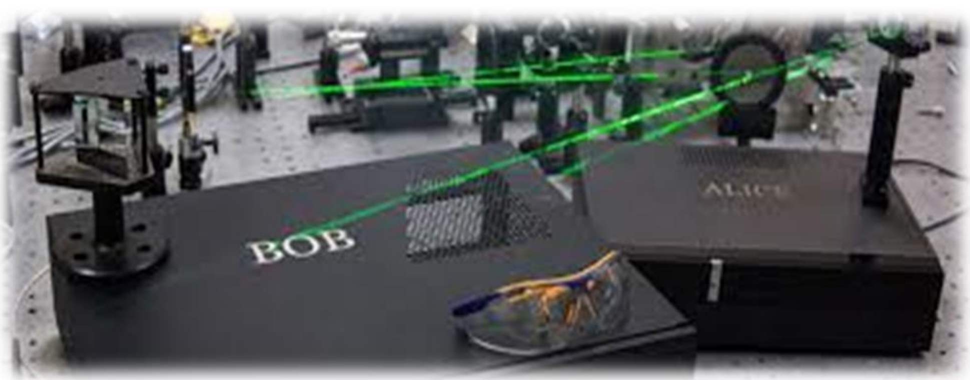


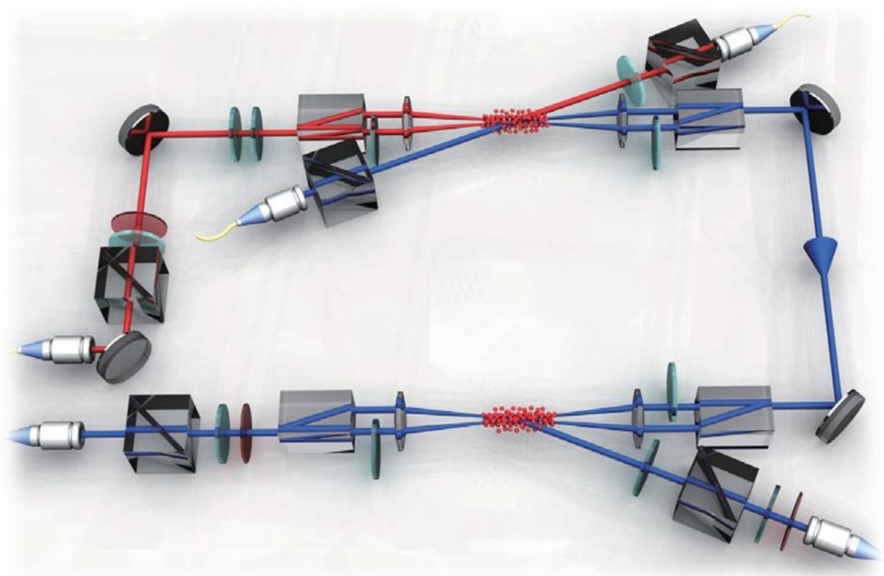
Quantum transmission & detection	ALICE sends photons	↖	↗	→	↑	↑	↗	↖	↑
	ALICE's random bits	0	1	0	1	1	1	0	1
	BOB's detection events	↑	↗	↖	↑	↗	↗	↖	↖
	BOB's detected bit values	1	1	0	1	1	1	0	0
Public discussion (i.e., sifting)	BOB tells ALICE the basis choices he made	Rect	Diag	Diag	Rect	Diag	Diag	Diag	Diag
	ALICE tells BOB which bits to keep		✓		✓		✓	✓	
	ALICE and BOB's shared sifted key	–	1	–	1	–	1	0	–

Image source: UNS Nice (France), Department of Physics

Quantum Secure Direct Communication

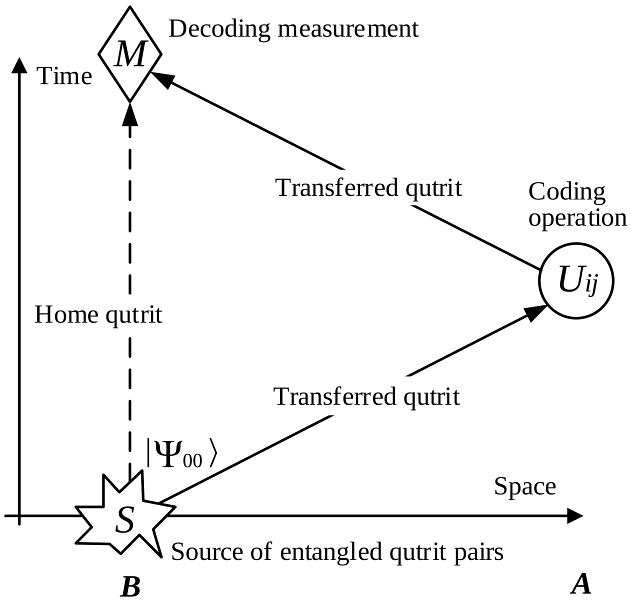




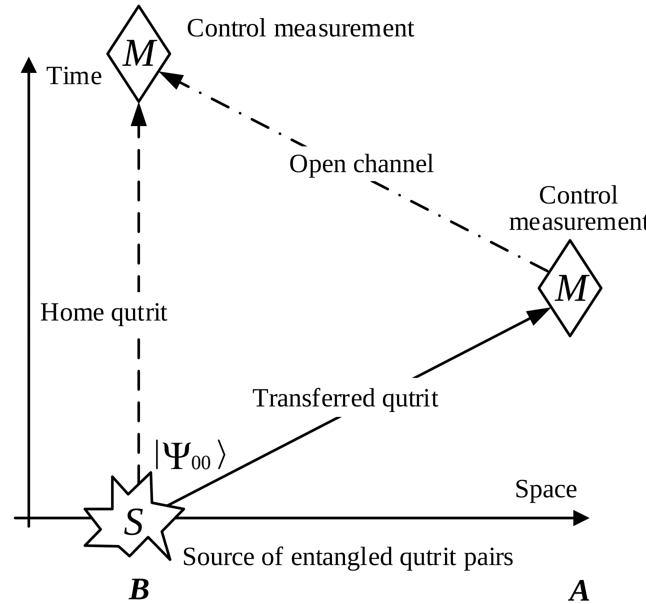


Quantum Secure Direct Communication

Message transferring mode



Eavesdropping control mode



Coding scheme in Bell basis

Поляри-зація СΨ, кут	Квантово-механічне представлення стану кутриту $\lvert\Psi_{ij}\rangle$	Оператор U_{ij} для перетворення $\lvert\Psi_{00}\rangle$ в $\lvert\Psi_{ij}\rangle$, який діє на другий кутрит	Пара тритів
0°	$\lvert\Psi_{00}\rangle = (\lvert 00\rangle + \lvert 11\rangle + \lvert 22\rangle)/\sqrt{3}$	$U_{00} = \lvert 0\rangle\langle 0\rvert + \lvert 1\rangle\langle 1\rvert + \lvert 2\rangle\langle 2\rvert$	00
40°	$\lvert\Psi_{10}\rangle = (\lvert 00\rangle + e^{2\pi i/3}\lvert 11\rangle + e^{4\pi i/3}\lvert 22\rangle)/\sqrt{3}$	$U_{10} = \lvert 0\rangle\langle 0\rvert + e^{2\pi i/3}\lvert 1\rangle\langle 1\rvert + e^{4\pi i/3}\lvert 2\rangle\langle 2\rvert$	10
80°	$\lvert\Psi_{20}\rangle = (\lvert 00\rangle + e^{4\pi i/3}\lvert 11\rangle + e^{2\pi i/3}\lvert 22\rangle)/\sqrt{3}$	$U_{20} = \lvert 0\rangle\langle 0\rvert + e^{4\pi i/3}\lvert 1\rangle\langle 1\rvert + e^{2\pi i/3}\lvert 2\rangle\langle 2\rvert$	20
120°	$\lvert\Psi_{01}\rangle = (\lvert 01\rangle + \lvert 12\rangle + \lvert 20\rangle)/\sqrt{3}$	$U_{01} = \lvert 1\rangle\langle 0\rvert + \lvert 2\rangle\langle 1\rvert + \lvert 0\rangle\langle 2\rvert$	01
160°	$\lvert\Psi_{11}\rangle = (\lvert 01\rangle + e^{2\pi i/3}\lvert 12\rangle + e^{4\pi i/3}\lvert 20\rangle)/\sqrt{3}$	$U_{11} = \lvert 1\rangle\langle 0\rvert + e^{2\pi i/3}\lvert 2\rangle\langle 1\rvert + e^{4\pi i/3}\lvert 0\rangle\langle 2\rvert$	11
200°	$\lvert\Psi_{21}\rangle = (\lvert 01\rangle + e^{4\pi i/3}\lvert 12\rangle + e^{2\pi i/3}\lvert 20\rangle)/\sqrt{3}$	$U_{21} = \lvert 1\rangle\langle 0\rvert + e^{4\pi i/3}\lvert 2\rangle\langle 1\rvert + e^{2\pi i/3}\lvert 0\rangle\langle 2\rvert$	21
240°	$\lvert\Psi_{02}\rangle = (\lvert 02\rangle + \lvert 10\rangle + \lvert 21\rangle)/\sqrt{3}$	$U_{02} = \lvert 2\rangle\langle 0\rvert + \lvert 0\rangle\langle 1\rvert + \lvert 1\rangle\langle 2\rvert$	02
280°	$\lvert\Psi_{12}\rangle = (\lvert 02\rangle + e^{2\pi i/3}\lvert 10\rangle + e^{4\pi i/3}\lvert 21\rangle)/\sqrt{3}$	$U_{12} = \lvert 2\rangle\langle 0\rvert + e^{2\pi i/3}\lvert 0\rangle\langle 1\rvert + e^{4\pi i/3}\lvert 1\rangle\langle 2\rvert$	12
320°	$\lvert\Psi_{22}\rangle = (\lvert 02\rangle + e^{4\pi i/3}\lvert 10\rangle + e^{2\pi i/3}\lvert 21\rangle)/\sqrt{3}$	$U_{22} = \lvert 2\rangle\langle 0\rvert + e^{4\pi i/3}\lvert 0\rangle\langle 1\rvert + e^{2\pi i/3}\lvert 1\rangle\langle 2\rvert$	22

Deterministic QSDC protocol

Standards in Quantum Security

SDO	Document number	Document title	Version	publ. date
ETSI	GS QSC 003	Quantum Safe Cryptography; Case Studies and Deployment Scenarios	V1.1.1	2017-02
ITU-T SG 17	XSTR-SEC-QKD	Security considerations for quantum key distribution networks		2020-03
ITU-T SG 17	X.1710 (ex X.sec-QKDN-ov)	Security framework for quantum key distribution networks		Approved
ITU-T SG 17	X.1714 (ex X.cf-QKDN)	Key combination and confidential key supply for quantum key distribution networks		Approved
ITU-T SG 17	X.sec-QKDN-km	Security requirements for quantum key distribution networks - Key management		*Drafting*
ITU-T SG 17	X.sec-QKDN-tn	Security requirements for quantum key distribution networks -Trusted node		*Drafting*
ITU-T SG 17	X.sec_QKDN_intrq	Security requirements for integration of QKDN and secure network infrastructures		*Drafting*

Example of quantum technology supply chain

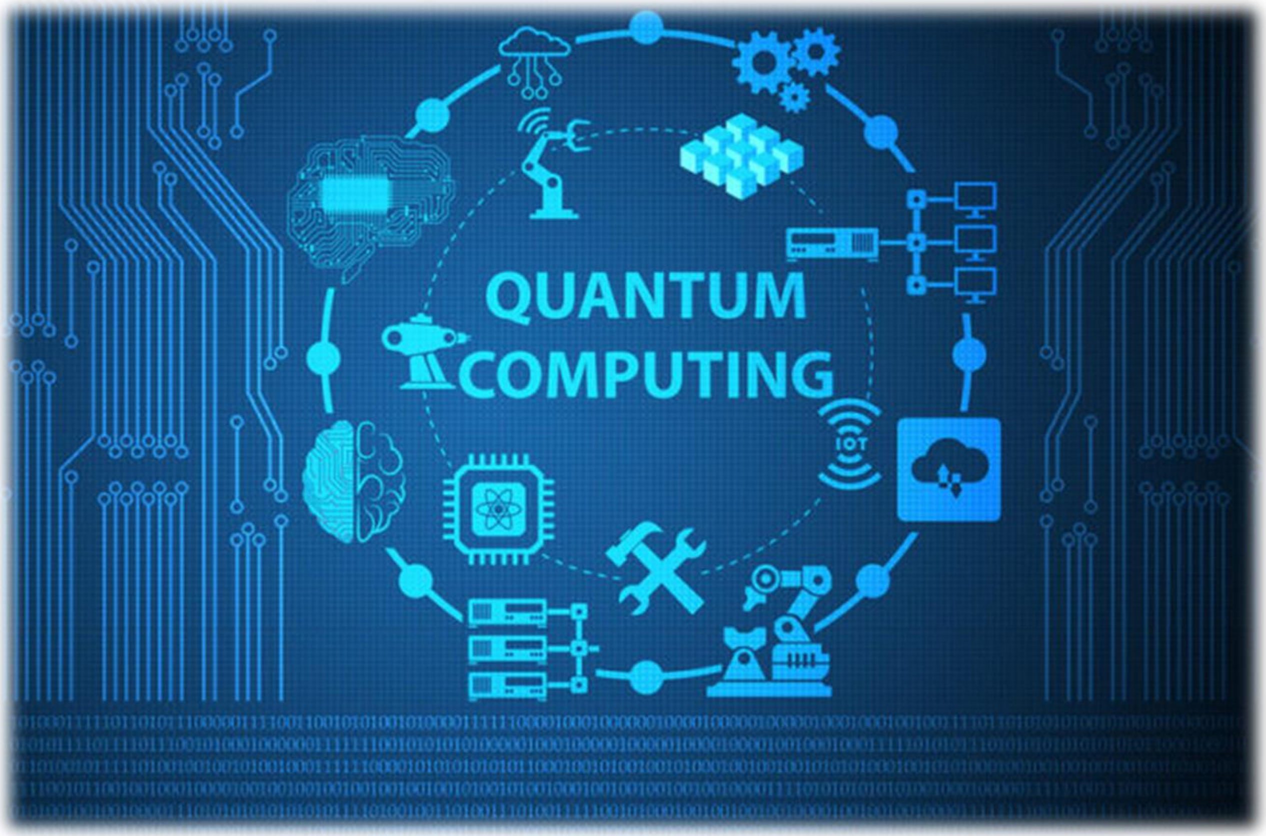
(Source: Quantum Technologies 2020 report, Yole Développement, 2020)

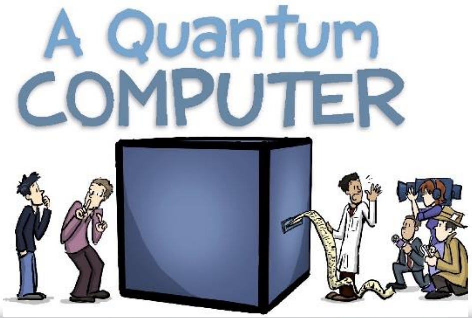
- **Quantum computer**: D-Wave (The Quantum Computing Company), intel, rigetti, IBM, Microsoft, Google
- **Quantum software**: softwareQ, TURING, ZAPATA, Q-CTRL, Atos, 1QBit, ANYON, EeroQ, Q^xBranch
- **QRNG and QKD**: 问天量子, QUANTUMXCHANGE, Crypta Labs, Quintessence Labs, IDQ, Q→NU, 国盾量子 QuantumCTek, Post-Quantum
- **End user**: VW, BAYER, NASA, TOTAL, AIRBUS
- **Photon source**: TOPTICA PHOTONICS, QUANDELA
- **PIC**: XANADU, QuiX
- **Photon detectors**: IDQ
- **Cryo systems**: ColdQuanta, SCONTEL (Superconducting Nanotechnology)
- **Sensors and metrology**: µQUANS, M Squared, THALES, BOSCH

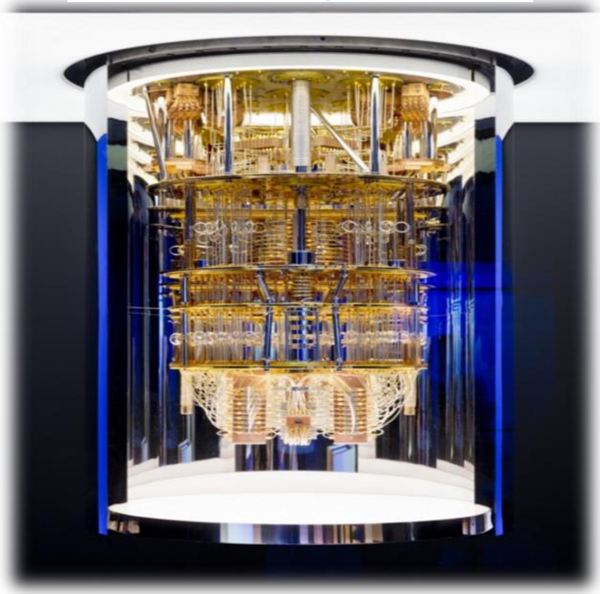
Non exhaustive list

PIC: Photonic Integrated Circuit - QKD: Quantum Key Distribution - QRNG: Quantum Random Number Generator

Quantum Computing







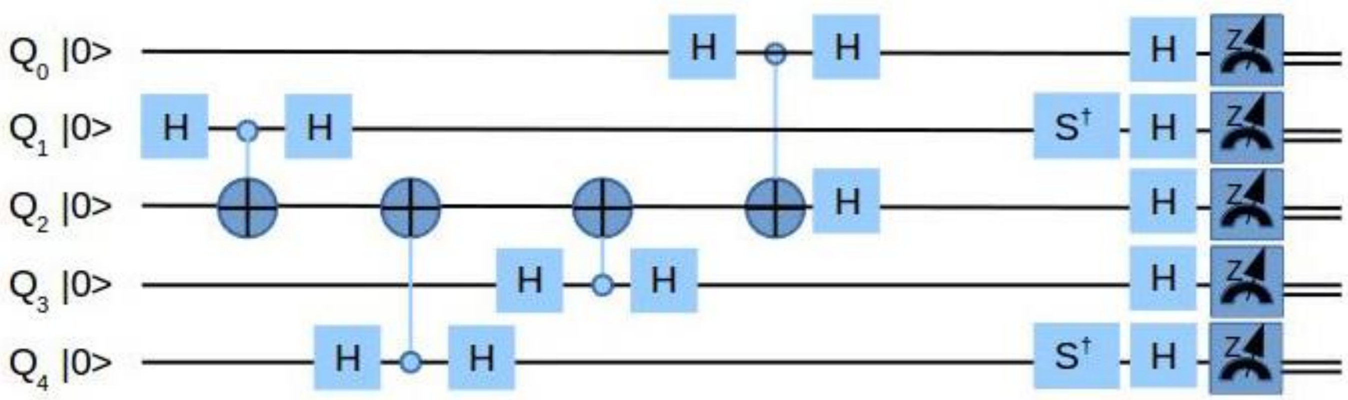
Q-Computer types

Q-Computer can realize

1) Grover algorithm for unordered database search

2) Shor algorithms for:

- factorization;
- logarithm in large discrete fields;
- discrete logarithm for EC etc.



Impact of Q-Computing on Cryptography

1. The impact on symmetric encryption can be mitigated. Running Grover's algorithm on a quantum computer provides a quadratic speedup, which has the effect of cutting the encryption strength in half. In other words, the encryption strength of AES-256 (based on a classical cryptanalytic attack) has an equivalent encryption strength of 128 bit sustaining the quantum cryptanalytic attack. The implication is that AES requires a larger key size to survive an attack from a quantum computer.

2. Asymmetric (public-key) encryption face catastrophic consequences. Running Shor's algorithm on a quantum computer with enough qubits can crack both RSA (based on the hard mathematical problem of large, prime number factorization) and digital signature algorithm (DSA) (based on discrete logarithm-based problems) because Shor's algorithm provides an exponential speedup. The quantum speedup yields many mainstream cryptographic algorithms (RSA, DSA, Elliptic-curve Diffie–Hellman (ECDH), etc.) vulnerable to attack. The potential negative consequences are severe given the ubiquity of asymmetric encryption.

3. Impact on hash functions can be mitigated. Hashing is a one-way mathematical function that maps data, regardless of its size, to a unique, fixed-length output called hash. Many password-based authentication systems, including Microsoft Windows, implement secure hashing. The quantum impact of hashing is similar to that of symmetric encryption. The National Institute of Standards and Technology recommends using SHA-256 (Secure Hash Algorithm 256) or SHA-3 with large output to resist quantum attacks.

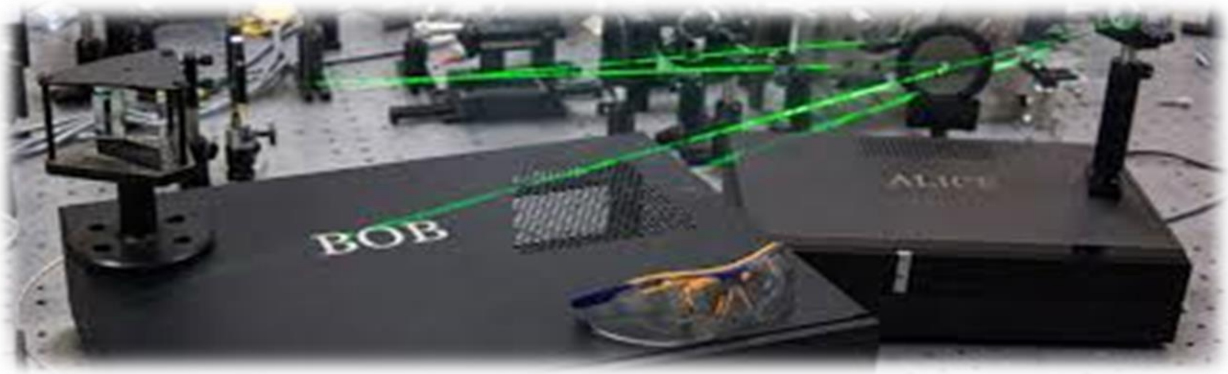
Impact of Q-Computing on Cryptography

Crypto Algorithm	Type	Purpose	Impact from large-scale QC
AES-256	Symmetric key	Encryption	Larger key sizes needed
SHA-256, SHA-3	———	Hash functions	Larger output needed
RSA	Public key	Signatures, key establishment	No longer secure
ECDSA, ECDH (Elliptic Curve Cryptography)	Public key	Signatures, key exchange	No longer secure
DSA (Finite Field Cryptography)	Public key	Signatures, key exchange	No longer secure

Block Ciphers Security against and Q-algorithms

Cryptosystem	Size of block / key, bit	Quantum memory needed for attack, qubit	Security against attack on	
			Message block	Key
AES-128	128/128	128/128	2^{64} ($10^{19,2}$)	2^{64} ($10^{19,2}$)
AES-256	128/256	128/256	2^{64} ($10^{19,2}$)	2^{128} ($10^{38,4}$)
DES	64/56	64/56	2^{32} ($10^{9,6}$)	2^{28} ($10^{8,4}$)
GOST-28147	64/256	64/256	2^{32} ($10^{9,6}$)	2^{128} ($10^{38,4}$)
Kalyna-128	128/128	128/128	2^{64} ($10^{19,2}$)	2^{64} ($10^{19,2}$)
Kalyna-512	512/512	512/512	2^{256} ($10^{76,8}$)	2^{256} ($10^{76,8}$)

Commercial Quantum Security Systems



ID Quantique (SWI)

Quantum Key Distribution

Cerberis QKD Blade

- Provably secure key exchange based on Quantum Key Distribution
- Quantum keys ensure long-term protection and forward secrecy
- Fully automated key exchange with continuous key renewal
- Integrated entropy source based on a Quantum Random Number Generator

Clavis^3 QKD Platform for R&D

- Open QKD platform for R&D applications High-Speed Key Generation and distribution up to 100km
- Coherent One-Way (COW) Protocol (patented by IDQ)
- Hardware Based Key Distillation Protocol (FPGA)

ID Quantique (SWI)

Quantum-Safe Network Encryption

Centauris CN9000 Series

- High-assurance, ultra-low latency encryption
- QRNG-powered 100Gbps encryption
- Robust, scalable and simple
- Upgradeable to Quantum-Safe Security

Centauris CN8000

- Uncompromising performance, flexibility and scalability
- QRNG-powered, multi-link encryption
- Multi-tenant, Ethernet & Fibre Channel encryption
- Upgradeable to Quantum-Safe Security

Centauris CN6000 Series

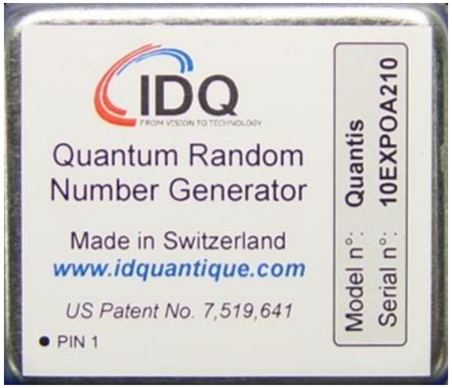
- Robust, business-class encryption
- Addressing the most performance-intensive environments
- Ultra-reliable, defence-grade for enterprise customers
- Upgradeable to Quantum-Safe Security

Centauris CN4000 Series

- High-assurance, transparent, full-line rate encryption
- Versatile, supports all Layer 2 network topologies
- Cost-effective

ID Quantique (SWI)

Quantum Key Generation



Quantis Appliance

- Trusted and certified source of quantum randomness
- Distributed architecture to support multiple applications simultaneously
- Linux kernel pool entropy feeder and HSM entropy injector
- Designed for Data Centre / IT / Telecom environments
- Simple, web-based configuration and management

Quantum Key Factory

- True random number generation platform based on Quantis QRNG
- Live verification of the core QRNG to ensure ongoing trust in the entropy source
- Worldwide government certifications, including Swiss METAS certification and German BSI validation according to AIS 31.
- Best practices in key scheduling, key mixing, key storage, key auditing

ID Quantique (SWI)

Quantum Key Generation

Quantis QRNG Chip

The world smallest QRNG for security, IoT & critical infrastructure applications

- True random numbers for all cryptographic algorithms and protocols
- Seed generation for blockchain
- Computing Device (mobile phones, tablets, servers, etc)
- Artificial Intelligence (Machine and Deep Learning)
- Automotive (V2X, CAN, Infotainment, etc)
- Scientific Modeling & Simulations
- Smart Networks (IoT, SmartGrid, SmartCity, SmartHome, etc)
- Online Gaming and Casinos

ID Quantique (SWI)

Quantum Single-Photon Systems

ID300 Short-Pulse Laser Source

- 1550 nm DFB laser
- 300 ps laser pulses
- 0 to 500 MHz repetition rate

ID230 Infrared Single-Photon Detector

- Free-running & gated
- 25% quantum efficiency
- Low dark count rate <25 Hz

ID281 Superconducting Nanowire

Single-photon detector with 80% quantum efficiency and fastest electronics

- Detection range: 400-2500 nm
- 80% quantum efficiency
- Jitter: 50 ps (FWHM)
- Closed-cycle cryostat

ID Quantique (SWI)

Centauris CV1000 Virtual Encryptor

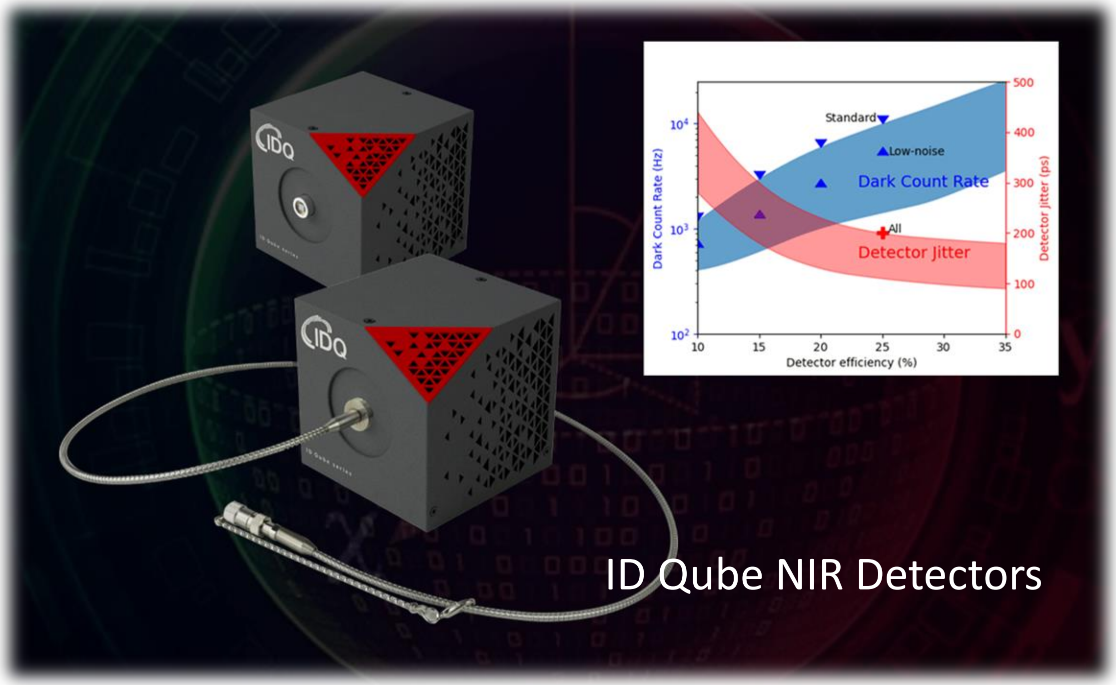
- WAN & SD-WAN encryption (provider-play)
- Concurrent multi-Layer encryption
- Virtualised network encryption
- East-West data centre traffic encryption

<u>Virtualised Encryption, Real-World Security and Performance</u>

- Agile, scalable solution
- Multi-Layer (L2, L3 & L4) network architectures
- 100% interoperability with Centauris encryptors
- Cost-effective

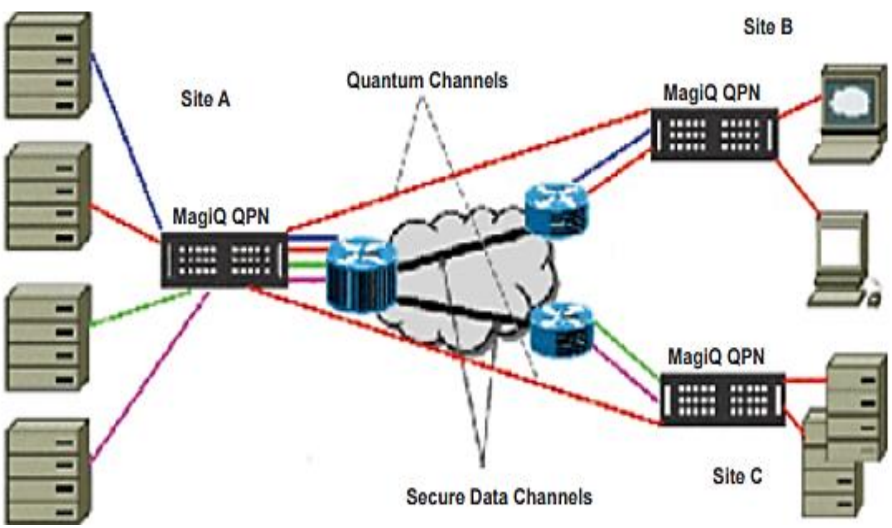
New!

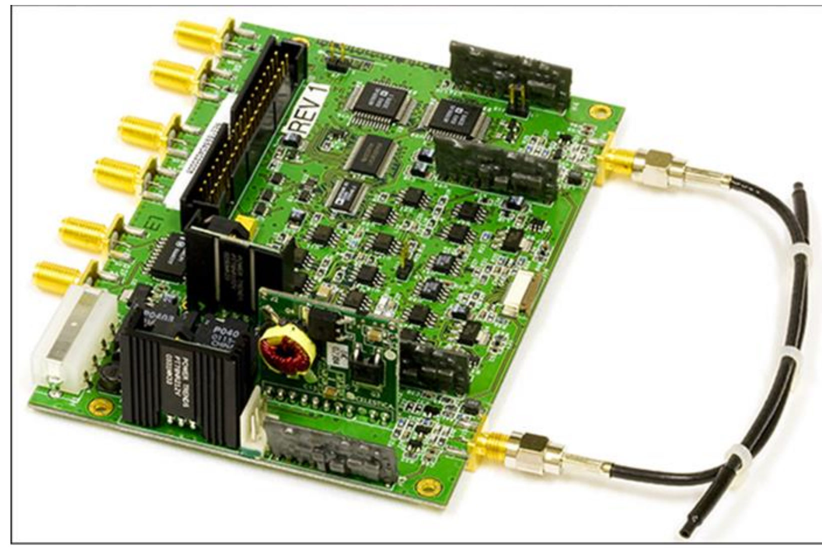
ID Quantique (SWI)



MagiQ Technologies (USA)

QPN-5505

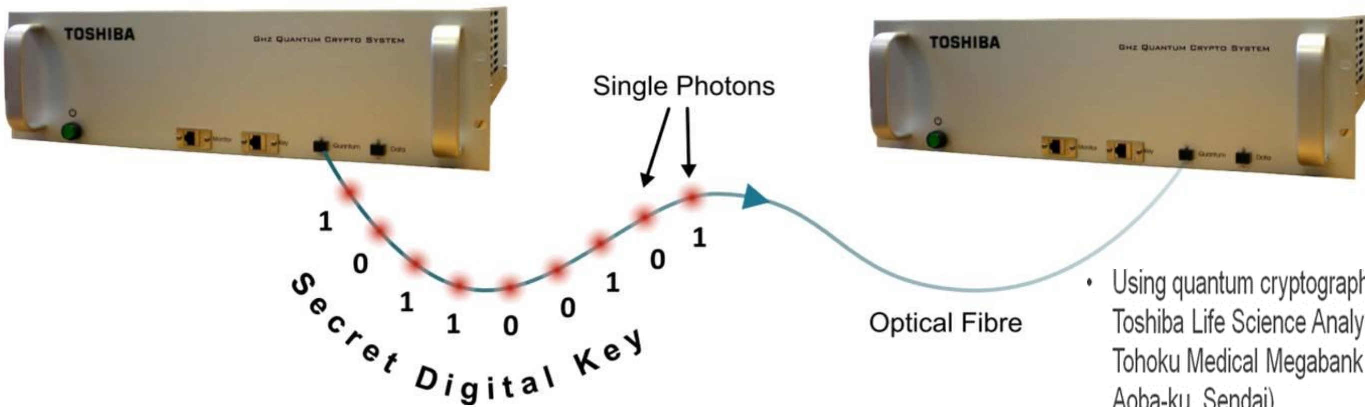




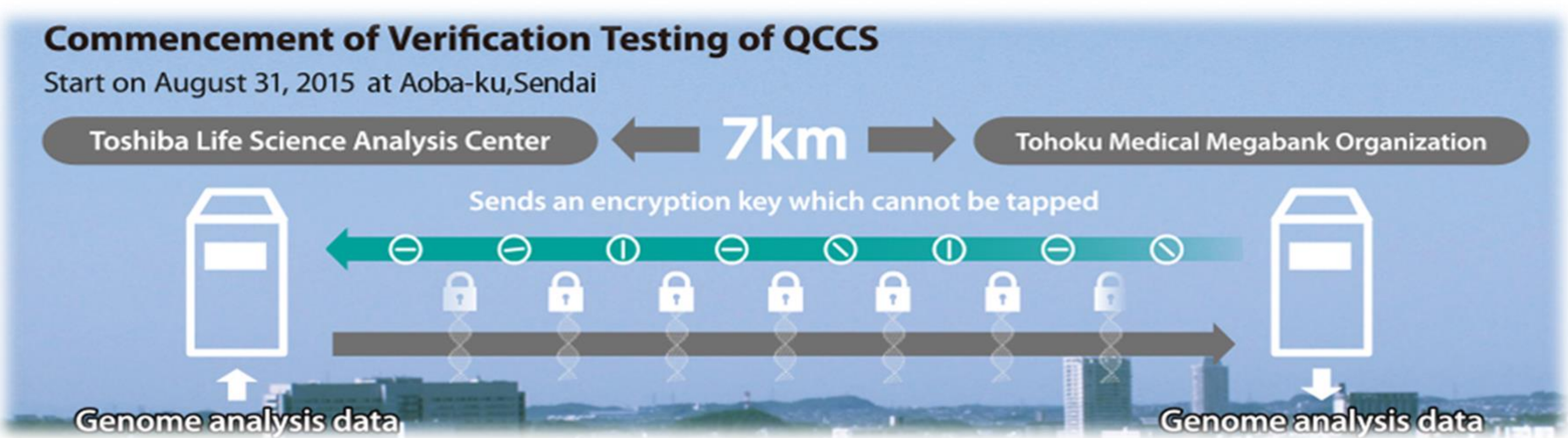
Toshiba (JPN)

Secret Digital Key Exchange Using Quantum Key Distribution

TOSHIBA



- Using quantum cryptographic communication to send genome analysis data from Toshiba Life Science Analysis Center (Minamiyoshinari, Aoba-ku, Sendai) to Tohoku Medical Megabank Organization, Tohoku University (in Seiryo-machi, Aoba-ku, Sendai)
- The test period is two years (from August 2015 to August 2017).



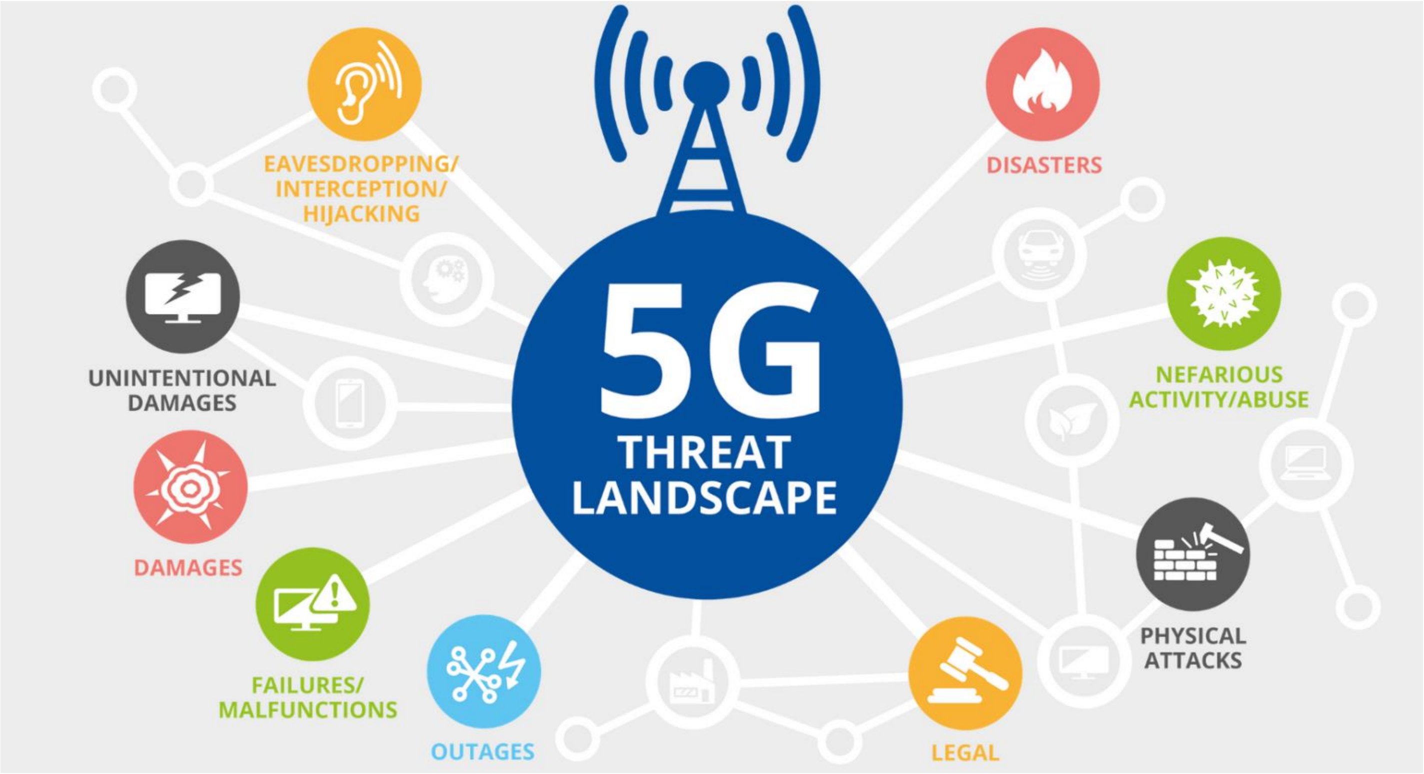
Labs Quintessence (AUS)

qCrypt is a unique vendor-neutral, encryption key management and policy management solution, addressing the toughest challenges in key management.

Cryptography and Security

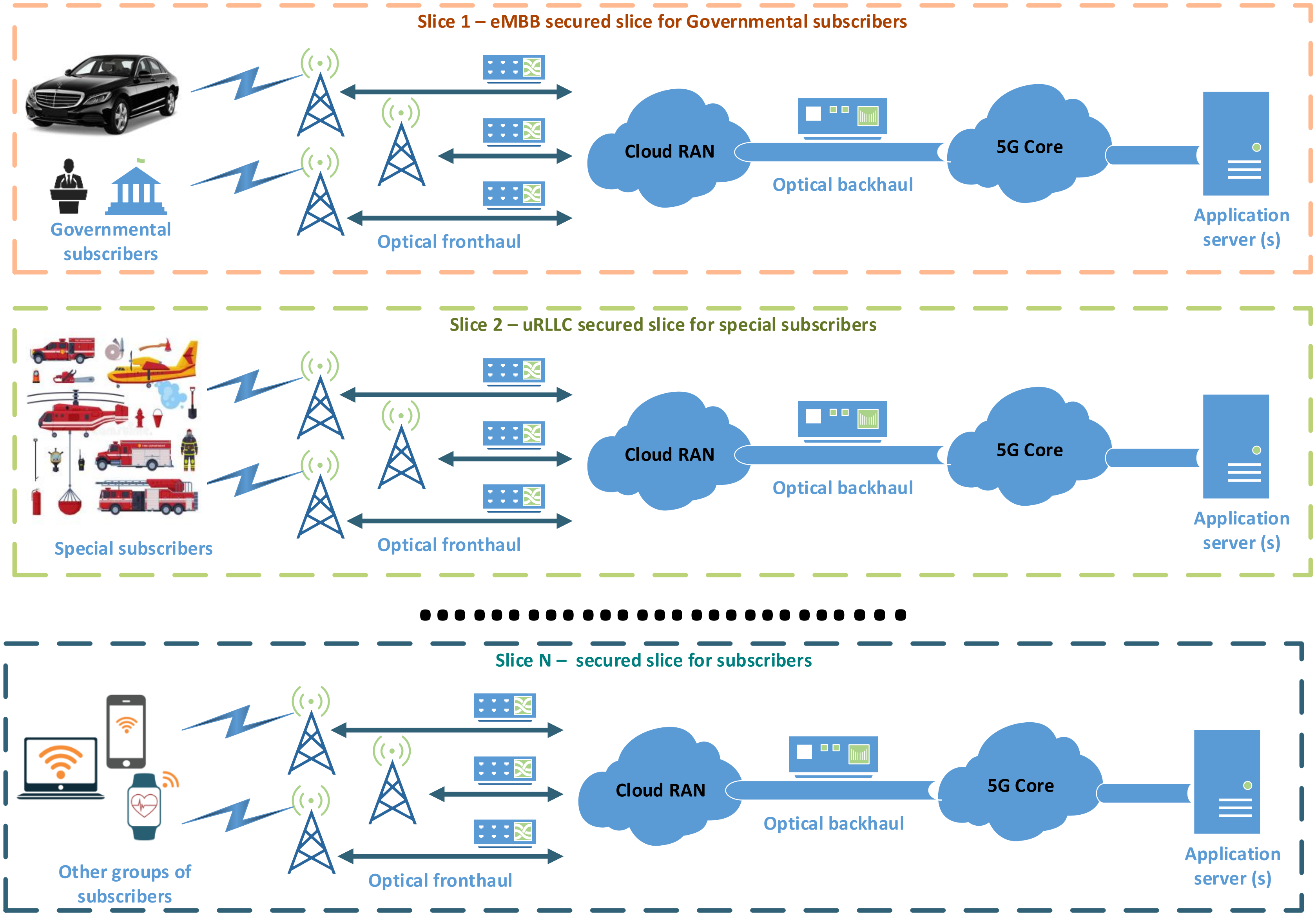
- FIPS 140-2 Level 1 and FIPS 140-2 Level 3 cryptographic modules.
- One-time pad, symmetric key and asymmetric key ciphers, key derivation, random objects, and certificates supported
- Encrypted keystore with Hardware Security Module (HSM) protected root of trust with the embedded HSM option. Otherwise, Trusted Platform Module (TPM) protected root of trust.
- Granular, hierarchical and auditable access control
- Supports both attended and unattended secure start-up
- Event log, audit log, date and time of transaction, management and user reports
- Up to 100,000 end-client systems per node, 200 key requests per second per node

5G Quantum Security Projects



5G communications

5G slices



Slice 1 – eMBB secured slice for Governmental subscribers
Governmental subscribers
Optical fronthaul
Cloud RAN
Optical backhaul
5G Core
Application server (s)
Slice 2 – uRLLC secured slice for special subscribers
Special subscribers
Optical fronthaul
Cloud RAN
Optical backhaul
5G Core
Application server (s)
Slice N – secured slice for subscribers
Other groups of subscribers
Optical fronthaul
Cloud RAN
Optical backhaul
5G Core
Application server (s)

IDQ + SK Telecom

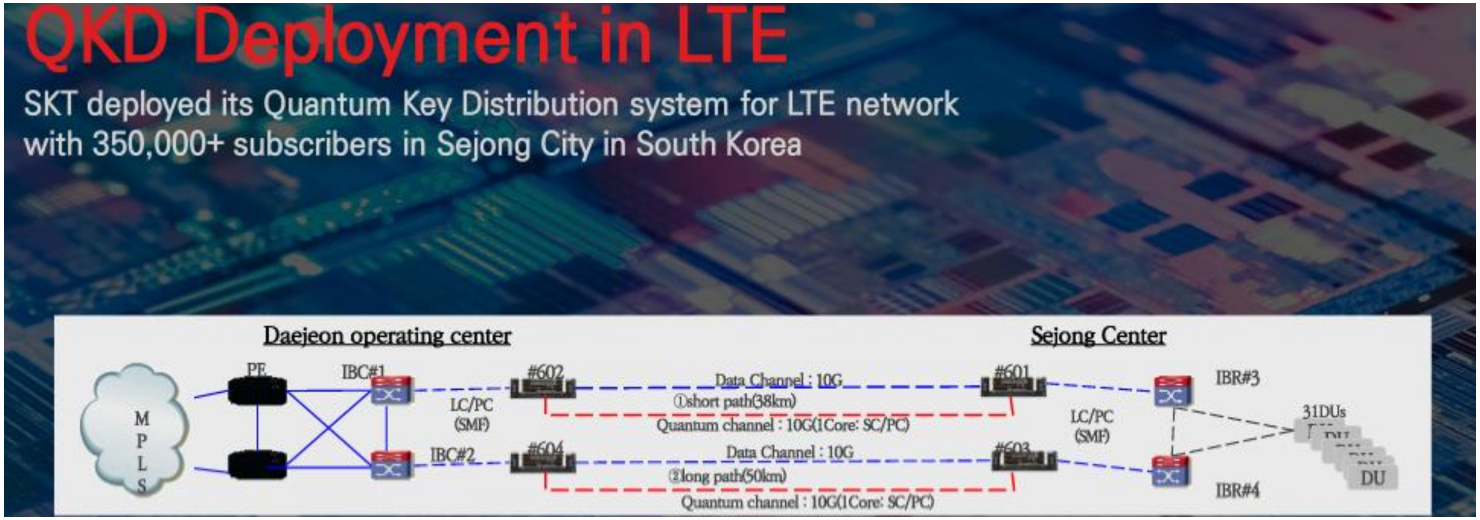
+

Geneva, Switzerland, 26 February 2018

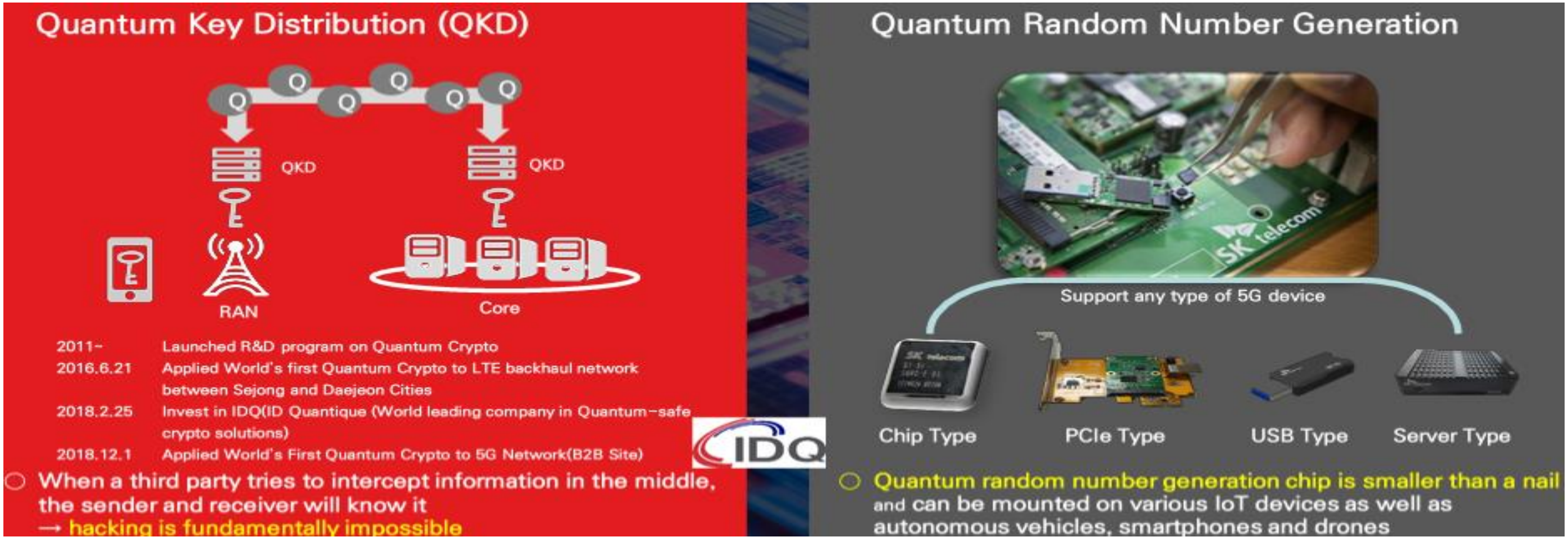
ID Quantique and SK Telecom join forces to form the global leader in quantum communications and quantum sensing technologies

ID Quantique announced today a strategic investment plan of US$ 65 million from SK Telecom, intended to develop IDQ's quantum technologies for the telecom and IoT markets. In the hyper-connected 5G era where some 43 billion devices worldwide based on data by market research firm Gartner about expected number of connected devices in 2026 get connected through wireless networks, the importance of cybersecurity in mobile communications will rise exponentially.

IDQ + SK Telecom



+



Two Generations of Q-Smartphone

Geneva, May 14th 2020

ID Quantique and SK Telecom announce the world's first 5G smartphone equipped with a Quantum Random Number Generator (QRNG) chipset

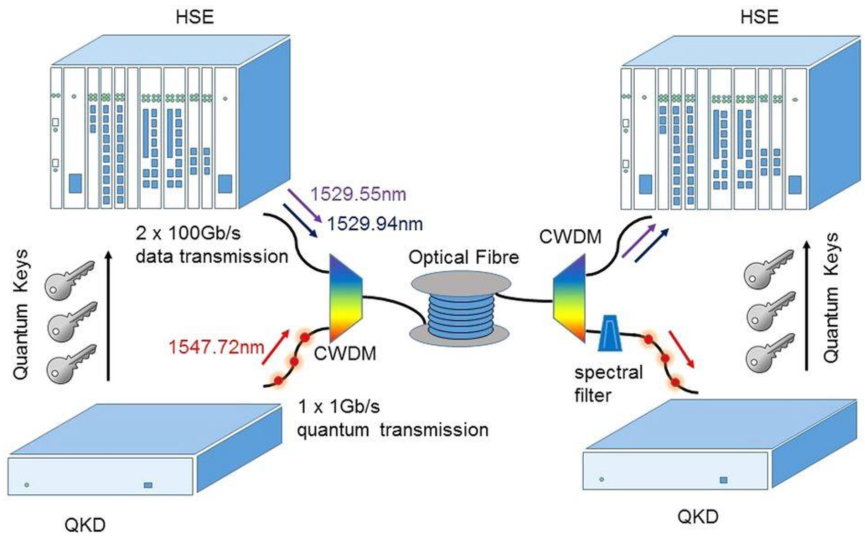
ID Quantique (IDQ), the world leader in quantum-safe security solutions, today announced that its newest Quantum Random Number Generator (QRNG) chip has been integrated in the 'Galaxy A Quantum', a custom edition of the Samsung Galaxy A71 5G smartphone commercialized by SK Telecom (NYSE:SKM), Korea's Telecom giant, to protect its customers' most valuable information.

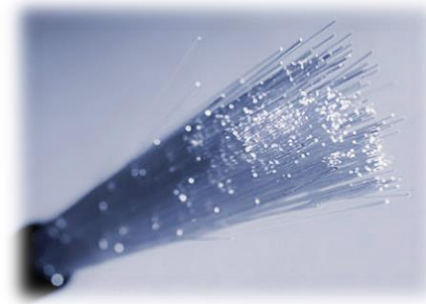
ID Quantique and SK Telecom unveil the Samsung Galaxy Quantum2, the newest QRNG-Powered 5G smartphone with even more embedded secured applications

13th April 2021

The Samsung Galaxy Quantum2 is the second smartphone equipped with quantum technology, designed to protect customers' information. It will be a new choice for customers who value both performance and security.

UK practical quantum-secured high-speed fibre network





BT announced today that it has built the UK's first practical quantum-secured high-speed fibre network between Cambridge and the BT Labs in Adastral Park, Ipswich, in a collaborative project led by the Quantum Communications Hub, part of the UK National Quantum Technologies Programme. The quantum-secured link runs across a standard fibre connection through multiple BT exchanges over a distance of 120km, making it the first high-speed 'real-world' deployment of quantum-based network security in the UK. The network link, which is capable of transferring 500Gbps of data, will explore and validate use cases for QKD. This will include how the technology can be deployed to secure critical national infrastructure, as well as to protect the transfer of critical data, such as sensitive medical and financial information.

DT strategic investment in ID Quantique

Deutsche Telekom

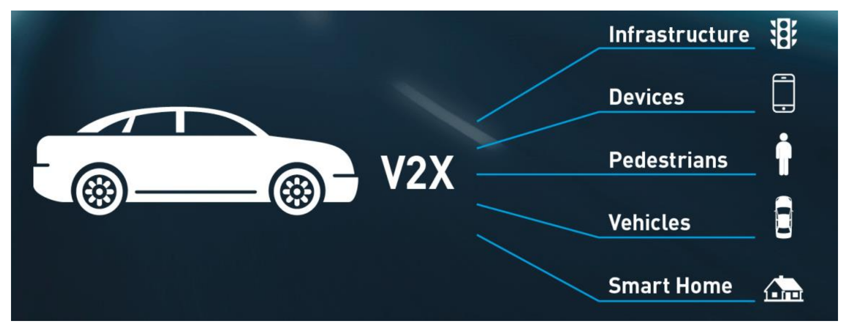
ID Quantique announced today a strategic investment plan from Deutsche Telekom, intended to develop IDQ’s quantum technologies for the telecom and IoT markets in the new 5G era. The investment is part of a joint agreement between Deutsche Telekom and SK Telecom, a majority investor in IDQ since February 2018, in order to strengthen their competitiveness in 5G and offer specialised highly secure 5G services.

V2X Security by Quantum

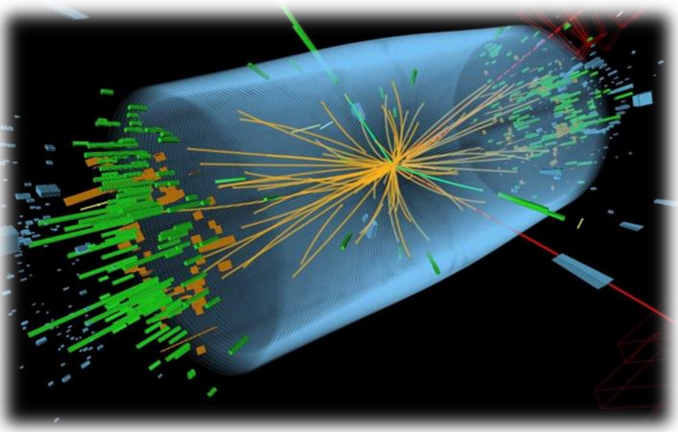
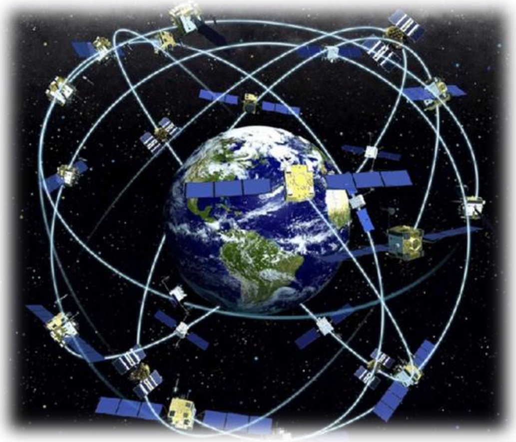
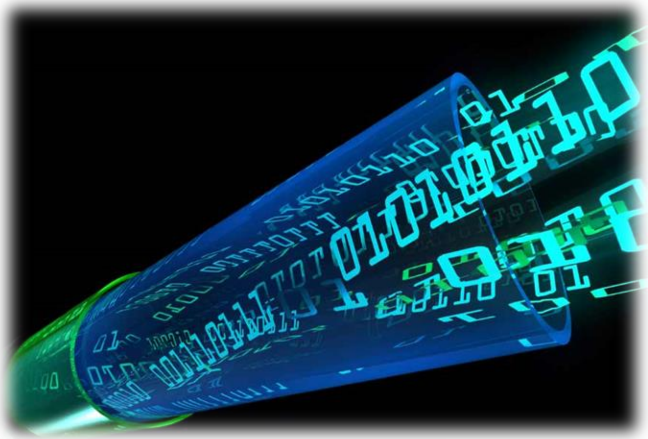
WEBINAR REPLAY:

Quantum Technology's impact on automotive V2X security

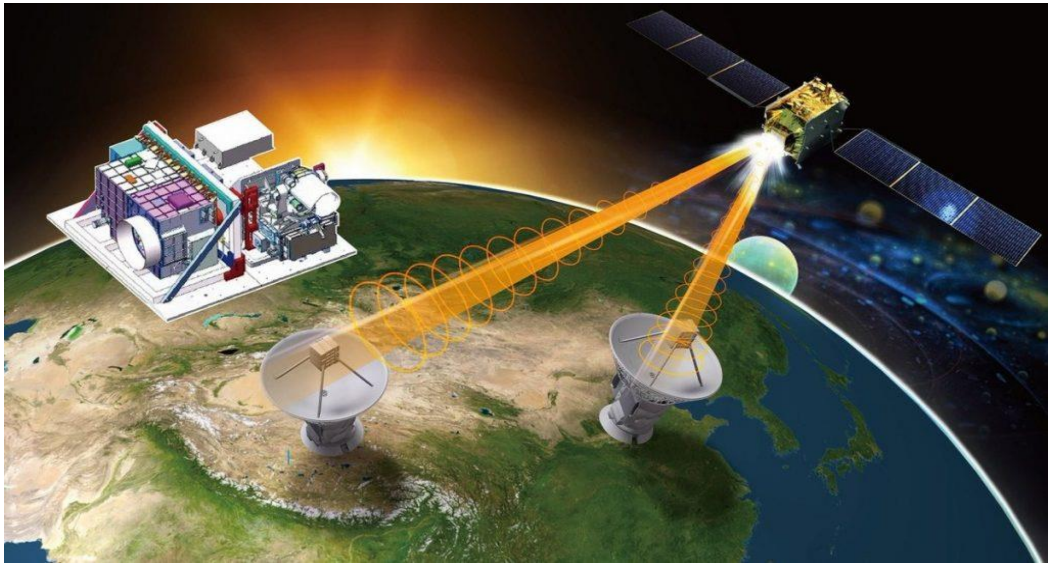
Watch our webinar to understand how Quantum-enhanced security provides V2X products with the highest level of trust for customers.



Others Quantum Projects

Quantum Science Satellite «Micius»



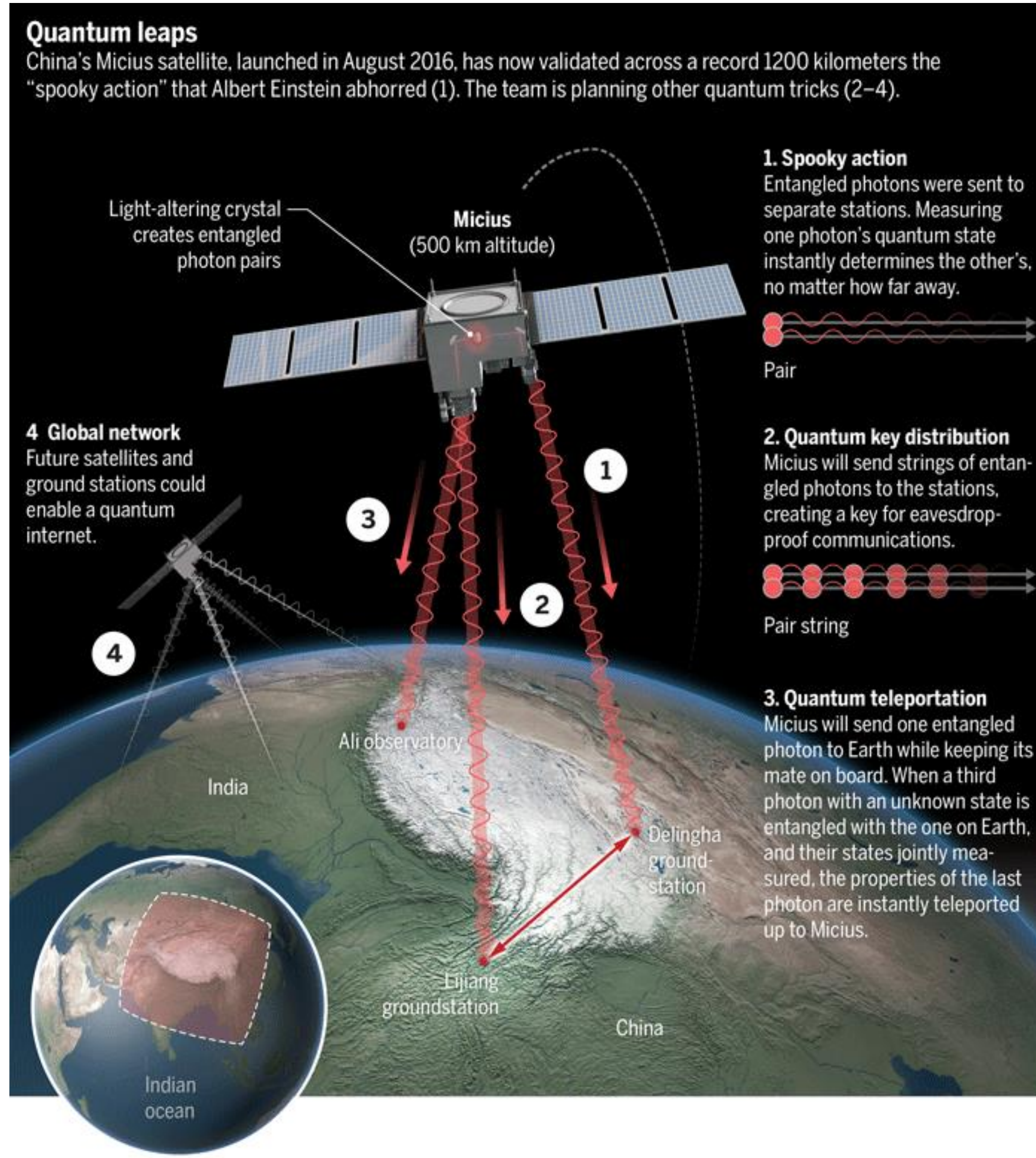
China Xinhua News
@XHNews

China launched world's 1st quantum satellite on top of a Long March-2D rocket from Jiuquan Satellite Launch Center

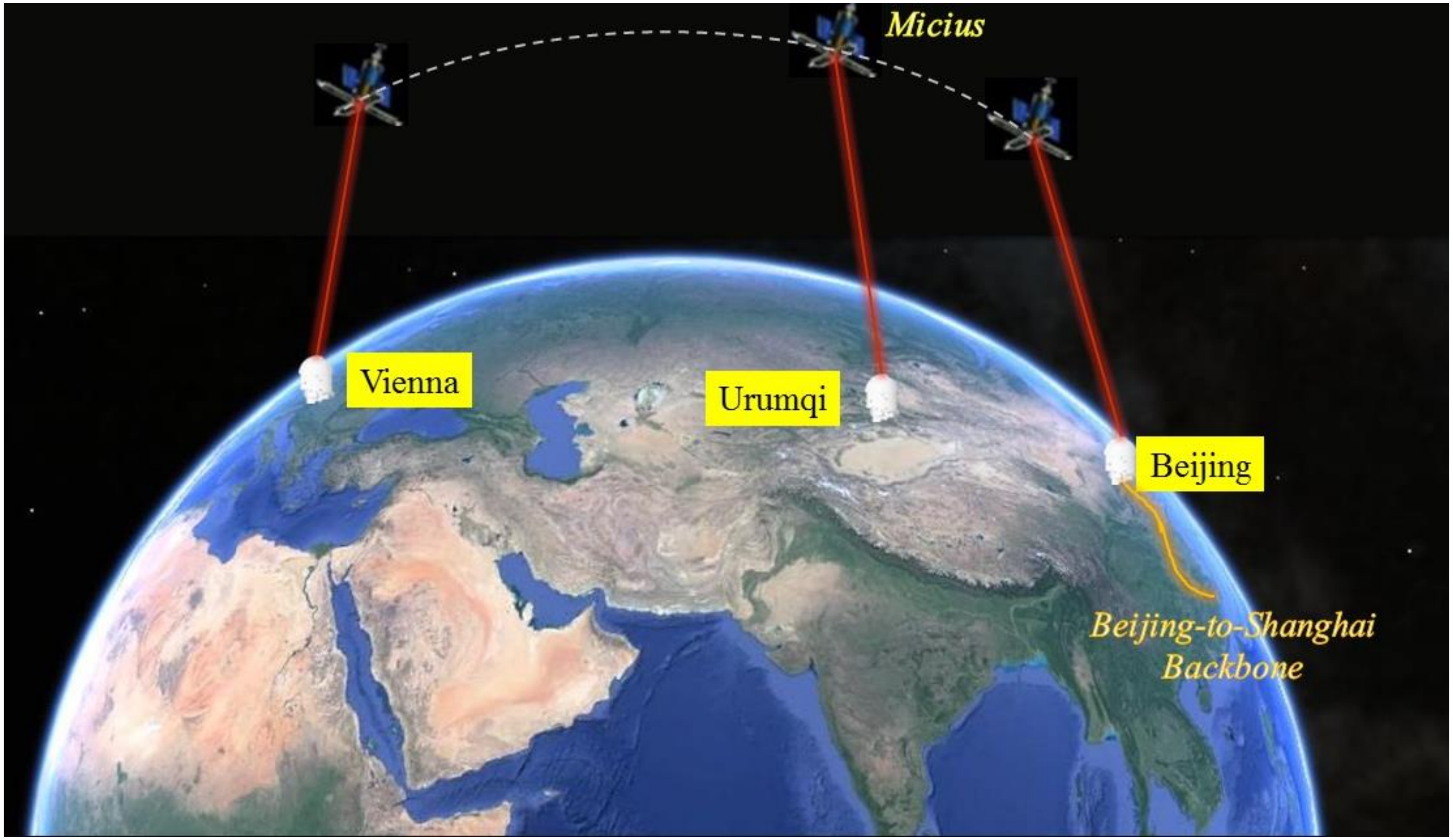
20:15 - 15 серп. 2016

- Bank of Communications,
- Industrial and Commercial Bank of China
- Alibaba.

Quantum Science Satellite «Micius»

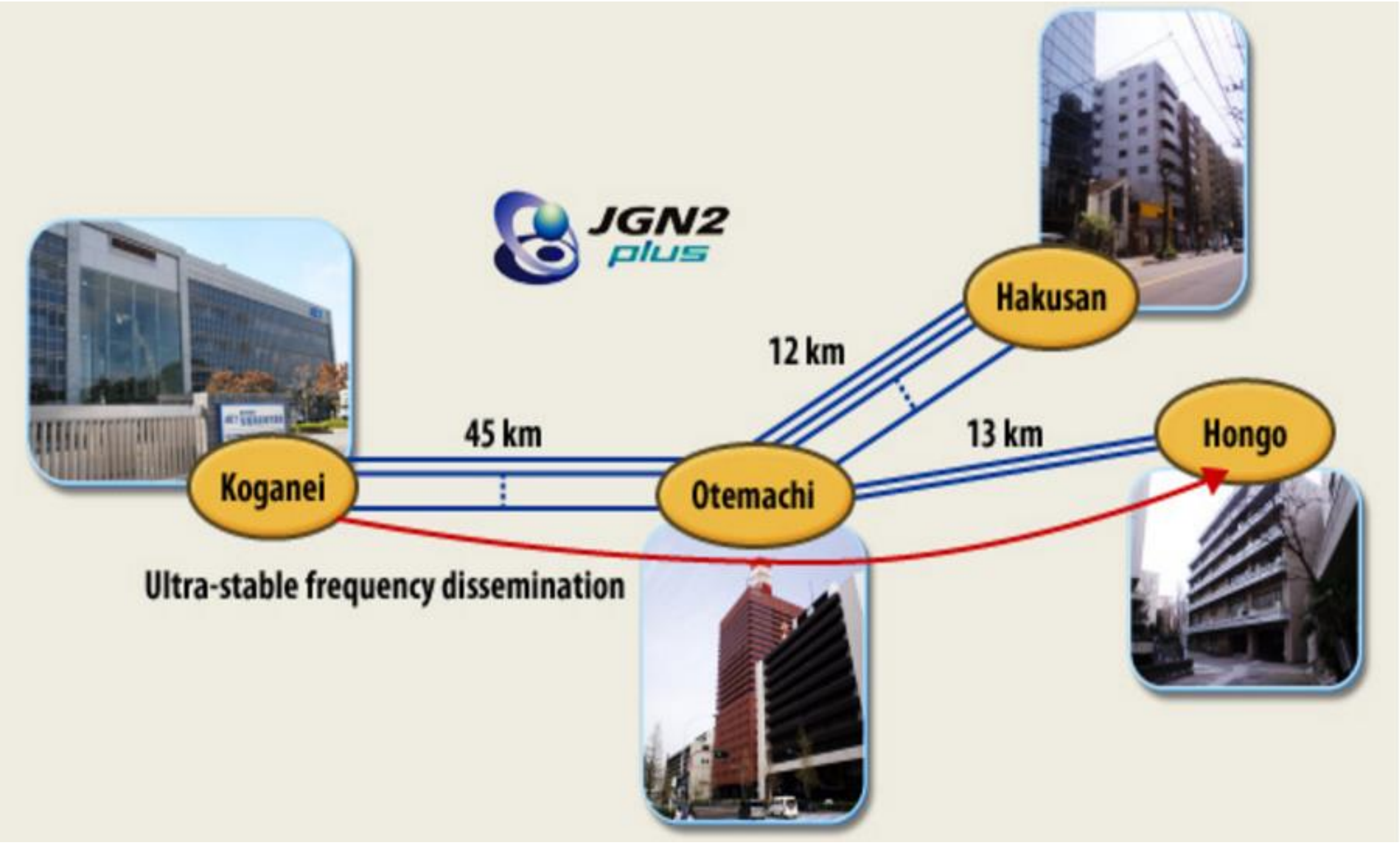


Intercontinental Satellite Quantum Communication

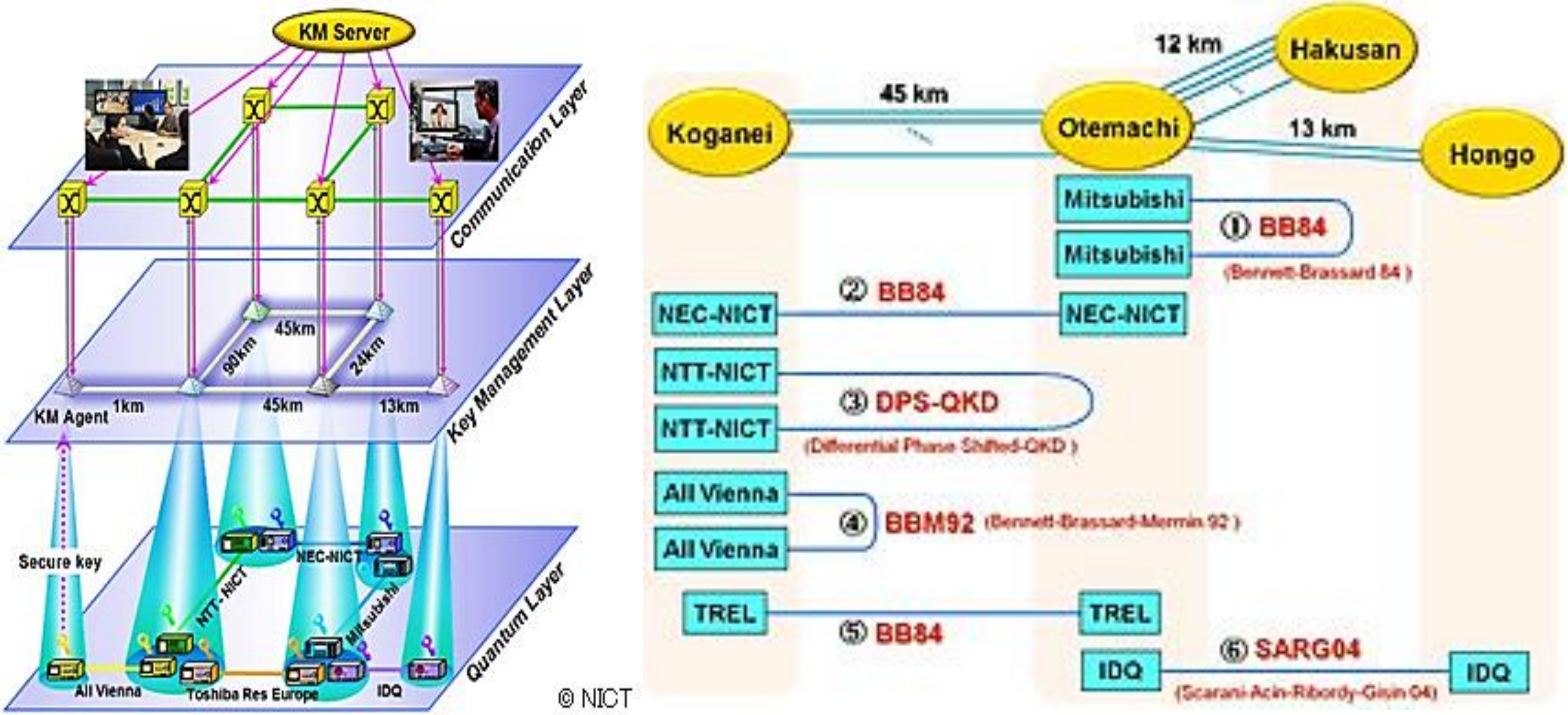


Austria - China
> 7400 km

Tokyo QKD Network (scheme)



Tokyo QKD Network (layers)



Quantum-Safe IPVPN

New!

Geneva, October 7th 2021

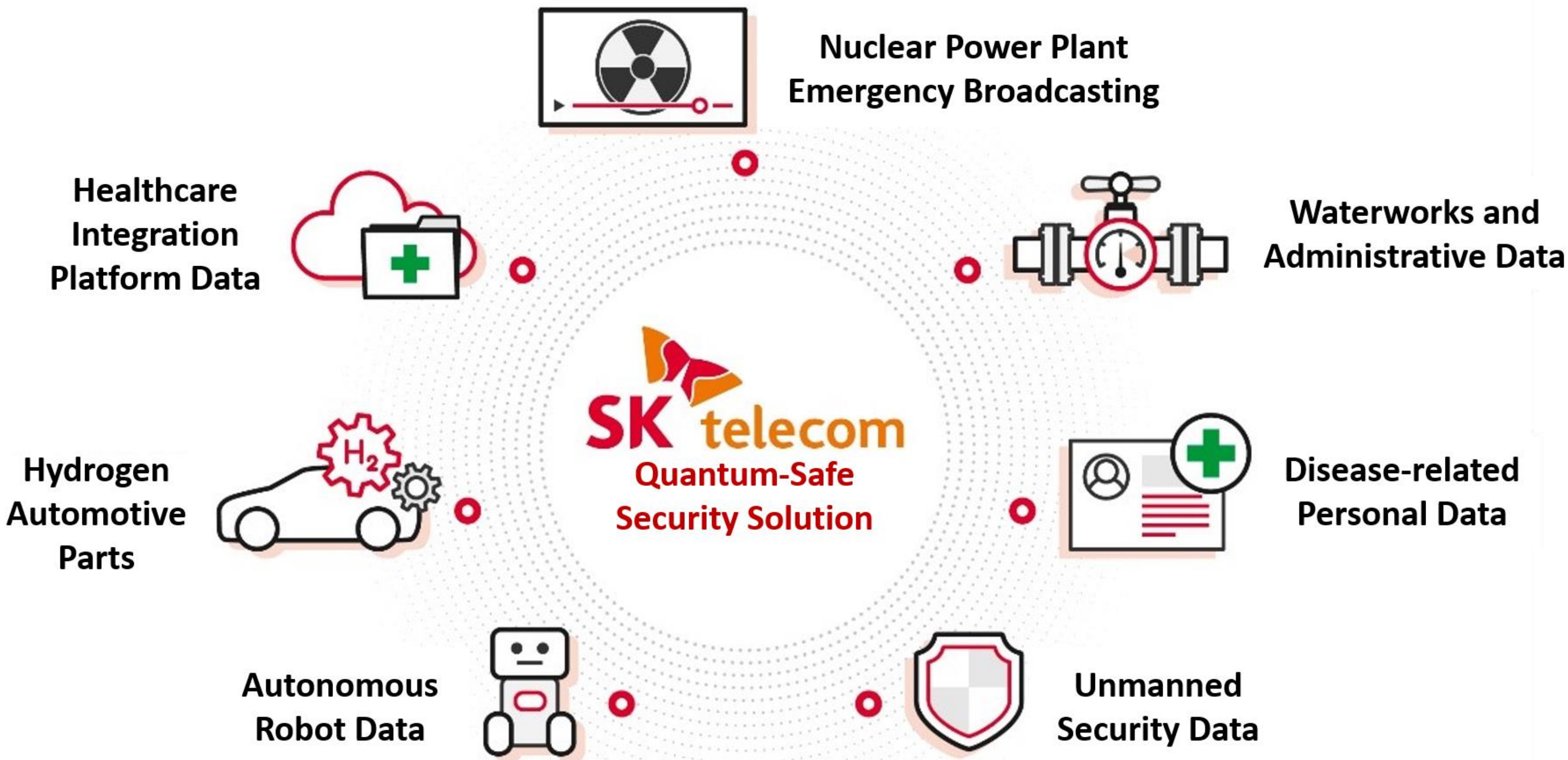
Telefonica, Fortinet and ID Quantique (IDQ) have jointly demonstrated the first Quantum-Safe IPVPN connection suitable for offering a fully managed datacenter interconnection service

Telefonica is actively preparing a new generation of connectivity solutions that can resist highly sophisticated cyber-attacks made possible with the development of quantum computers. These quantum computers, once sufficiently powerful, may be able to break current public-key cryptography schemes based on prime number factorisation, such as the widely used RSA algorithm.

New!

Quantum Secure CI in SK

IDQ + SK telecom



New!

Unique Quantum Lab

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BUT opens a unique laboratory of quantum security

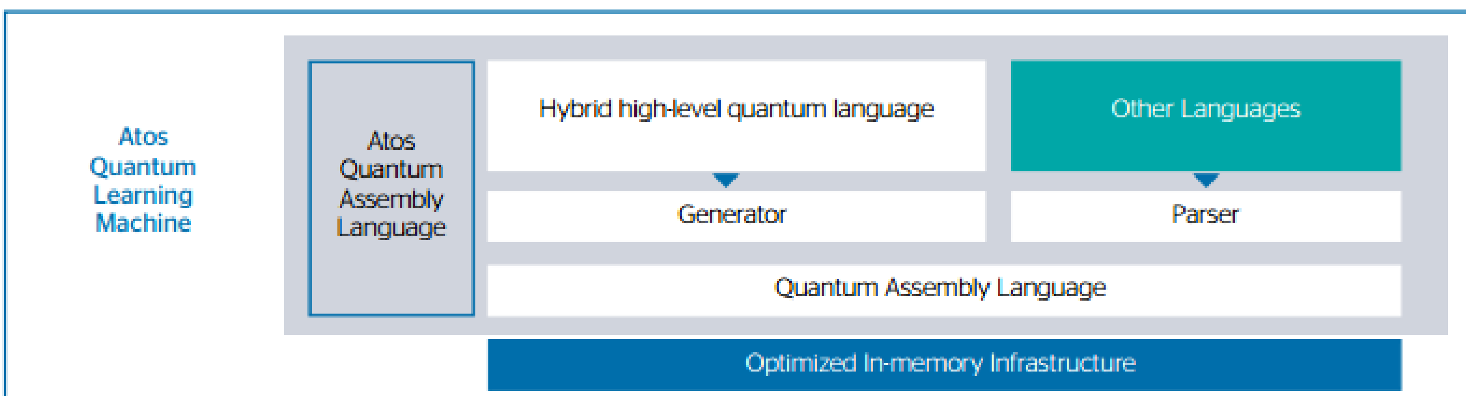
As of today, the new laboratory with the so-called quantum communication infrastructure is available to experts from the Faculty of Electrical Engineering and Communication of the Brno University of Technology. The laboratory will enable scientists to work on next-generation computer networks that will also be protected from quantum computer attacks, to which the vast majority of current networks, including the Internet, are vulnerable.

Thanks to special equipment, experts will be able to **work on the protection of sensitive data, even before the construction of a quantum computer,** for which the current level of security would be an easily overcome obstacle. **For example, data related to state security** or generally critical **infrastructure could fall into strange hands**. At the same time, it is necessary to protect the information passed between the Czech Republic and international institutions, such as the European Union or NATO.

Atos Quantum Learning Machine

<u>Atos Quantum targets</u> :

- Developing a **quantum simulation platform**
- Designing innovative **computing architectures**
- Developing new **quantum safe cryptography algorithms**
- Creating an **algorithm development and programming cluster** for Big Data, AI, HPC, CS



Quantum coding languages

- Open Quantum Assembly Language (OpenQASM)
- Q#
- LIQUi (Language-Integrated Quantum Operations)
- Quantum Computation Language (QCL)
- Quipper
- Quantum pseudocode
- QML

Our selected results in QKD

Our team

Sergiy Gnatyuk
DSc, PhD, Associate Professor
Scientific Adviser of the Lab

Tetyana Okhrimenko
PhD, Associate Professor
Chief of the Lab

Roman Odarchenko
DSc, PhD, Associate Professor
Project Manager / Lecturer

Viktoriia Sydorenko
PhD, Associate Professor
Researcher / Lecturer

Vasyl Kinzeryavyy
PhD, Associate Professor
Researcher and Consultant

Andriy Gizun
PhD, Associate Professor
Researcher / Lecturer

Yuliia Polishchuk
PhD Student,
Junior Researcher

Oleh Polihenko
PhD Student, Technical
Specialist / Lecturer

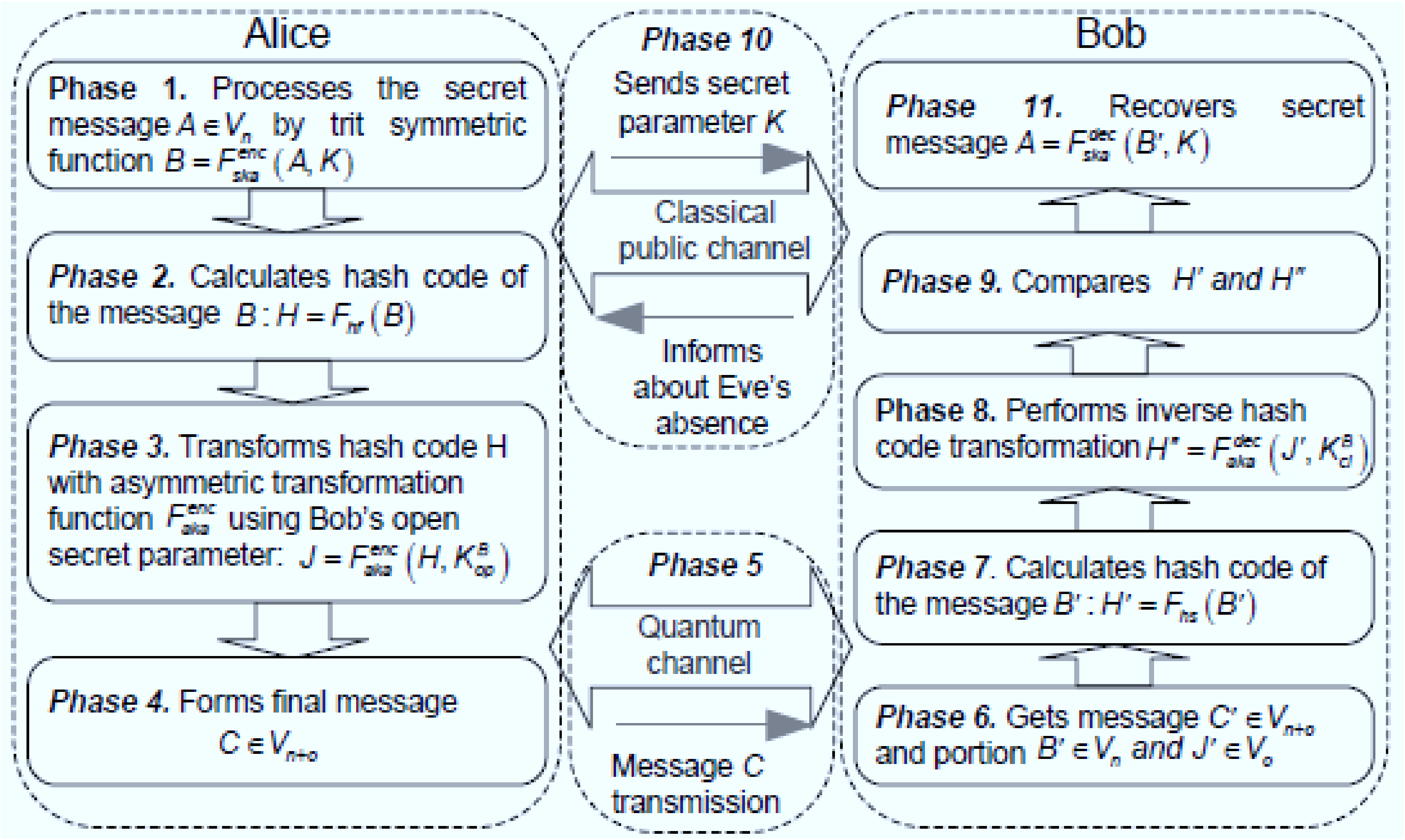
Sergiy Dorozhynskyy
PhD Student, Developer and
Junior Researcher

Bohdan Horbakha
Student, Developer and
Technical Specialist

Vladyslav Griga
PhD Student, Junior Researcher
and Technical Specialist

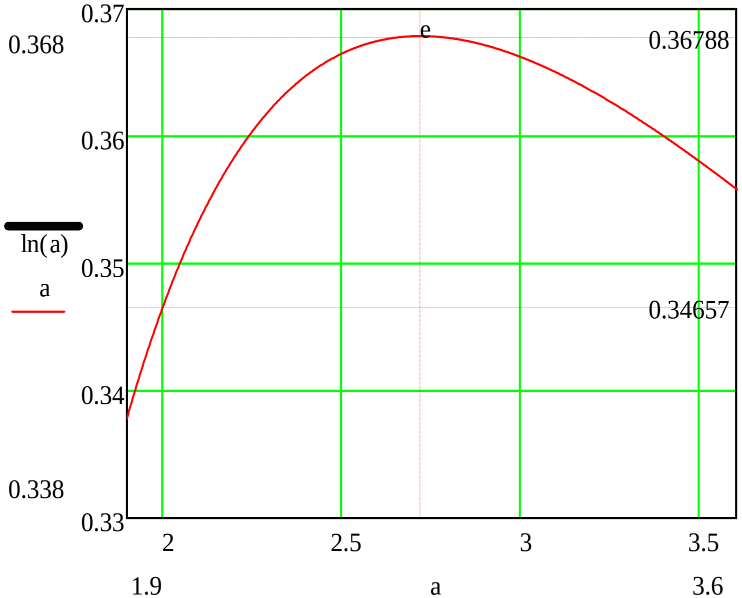
Ivan Azarov
Developer and Technical
Specialist

Improved deterministic protocols [1/3]



51

Improved deterministic protocols [2/3]



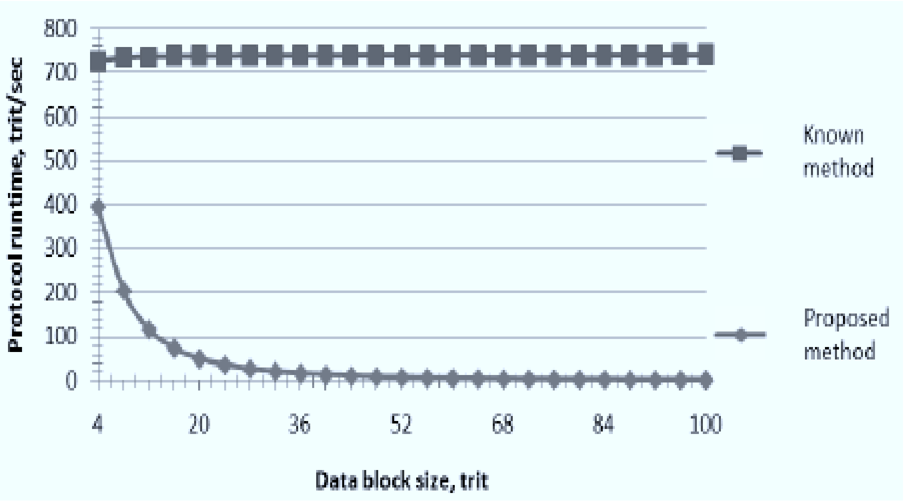
Natural-logarithmic information density (quantity of the information)

Comparison with known approach

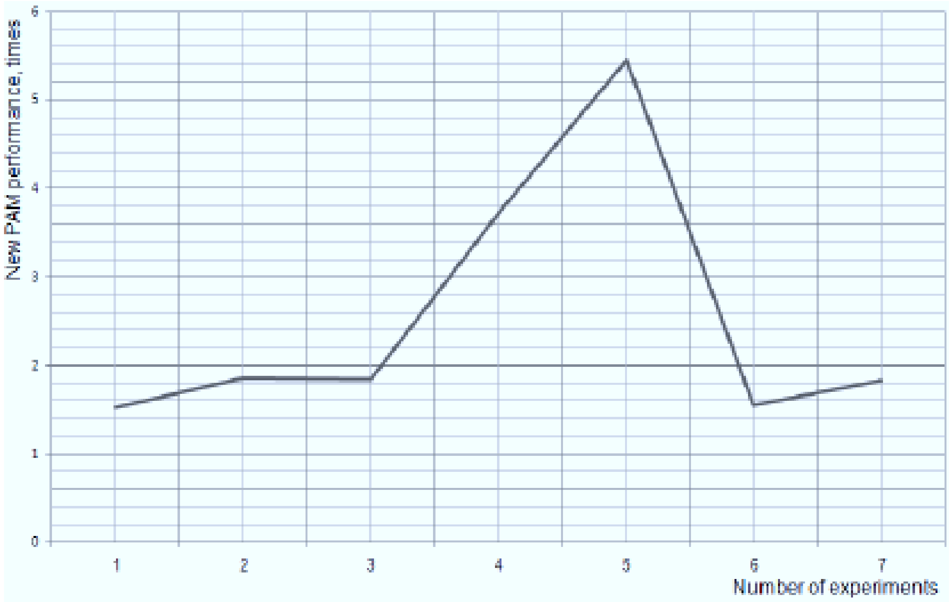
№	Known method		Proposed method	
	Operation	Runtime	Operation	Runtime
1.	$M_i = F_{gen}(K, i, r^2)$	$\frac{l \cdot r^2}{V_{gen}}$	$k_i = F_{gen}(K, i, r)$	$\frac{l \cdot r}{V_{gen}}$
2.	$B_i = A_i \cdot M_i$	$\frac{l \cdot (2r^2 - r)}{V_x}$	$B_i = A_i + k_i$	$\frac{l \cdot r}{V_x}$
3.	$B_i' = F_{kv}(B_i, q)$	$\left(\frac{l \cdot r}{V_{kv}}\right) \cdot (1+q)$	$H = F_{hf}(B)$ $J = F_{aka}^{enc}(H, K_{op}^{B})$	$\frac{4 \cdot l \cdot r}{V_x}$
4.	$M_i' = F_{kl}(M_i)$	$\frac{l \cdot r^2}{V_{kl}}$	$B_i' = F_{kv}(B_i, q)$ $J' = F_{kv}(J, q)$	$\left(\frac{l \cdot r + 96}{V_{kv}}\right) \cdot (1+q)$
5.	$(M_i')^{-1} = F_{obr}(M_i')$	$\frac{l \cdot (4r^3 - 4r^2)}{V_x}$	$H' = F_{hf}(B')$ $H'' = F_{aka}^{dec}(J', K_{cl}^{B})$	$\frac{4 \cdot l \cdot r}{V_x}$
6.	$A_i' = B_i' \cdot (M_i')^{-1}$	$\frac{l \cdot (2r^2 - r)}{V_x}$	$K' = F_{kl}(K)$	$\frac{96}{V_{kl}}$
7.	-	0	$k_i' = F_{gen}(K', i, r)$	$\frac{l \cdot r}{V_{gen}}$
8.	-	0	$A_i' = B_i' - k_i'$	$\frac{l \cdot r}{V_x}$

52

Improved deterministic protocols [3/3]



Speed investigation



Comparative analysis of efficiency (r > 4)

Improved protocol allows to minimize the amount of switching between message transmission and eavesdropping control modes as well as uses ternary pseudo-random sequences instead of reverse hashing with reversible ternary matrices.

It provides protocol speed increasing at least in 1.52 time, while maintaining the resistance to non-coherent attacks.

53

PRNG and TRIT STS [1/3]

Randomness assessment tests

- NIST Statistical Test Suit
- Diehard tests by G. Marsaglia
- Dieharder
- TestU01
- Knuth tests

TriGen v.2.0 PRNG was developed and studied in practice.

Therefore, analyzing the results of the study it can be conclude that NIST STS technique cannot be used to evaluate the quality of the trit sequences (this technique is oriented on bit sequences evaluation), and the developed method as well as PRNG based on it for evaluating trit sequences quality suitable for use in practice *(next slide).*

TriGen v.2.0

Input: initialization vector VI , secret key K , $VI \in V_{240}$, $K \in V_{96}$, parameter b .

Output: output sequence $M = (M_1, \dots, M_b)$, $M \in V_{96b}$, $M_q \in V_{96}$, $q \in \overline{1, b}$.

1. $x_i = VI_i$, $y_j = VI_{6+j}$, $k_j = K_j$, $i \in \overline{1,6}$, $j \in \overline{1,4}$.

2. *For* $q = 1;\ q \le b;\ q{+}{+}$ *do*

2.1. *For* $j = 0;\ j < 4;\ j{+}{+}$ *do*

2.1.1. $x_1 = (Sbox(x_1 + k_1) \oplus x_4) <<< k_4$; $x_2 = (Sbox(x_2 + k_2) + x_5) >>> k_3$;

$x_3 = Mix((x_3 + x_6) \oplus y_3) <<< x_1$;

2.1.2. $k_1 = Sbox((Sbox(x_1 \oplus k_1) + x_5) \oplus y_1)$; $k_2 = Sbox(Mix(x_2 + k_2 + x_6) \oplus y_2)$;

2.1.3. $y_1 = Sbox(((k_1 + y_1) <<< x_2) \oplus k_3)$; $y_2 = Mix(Sbox(((k_2 + y_2) >>> x_3) \oplus k_4))$;

2.1.4. $x_4 = (Sbox(x_4 + k_3) \oplus x_1) <<< k_2$; $x_5 = (Sbox(x_5 + k_4) + x_2) >>> k_1$;

$x_6 = Mix((x_6 + x_3) \oplus y_1) <<< x_4$;

2.1.5. $k_3 = Sbox((Sbox(x_4 \oplus k_3) + x_2) \oplus y_3)$; $k_4 = Sbox(Mix(x_5 + k_4 + x_3) \oplus y_4)$;

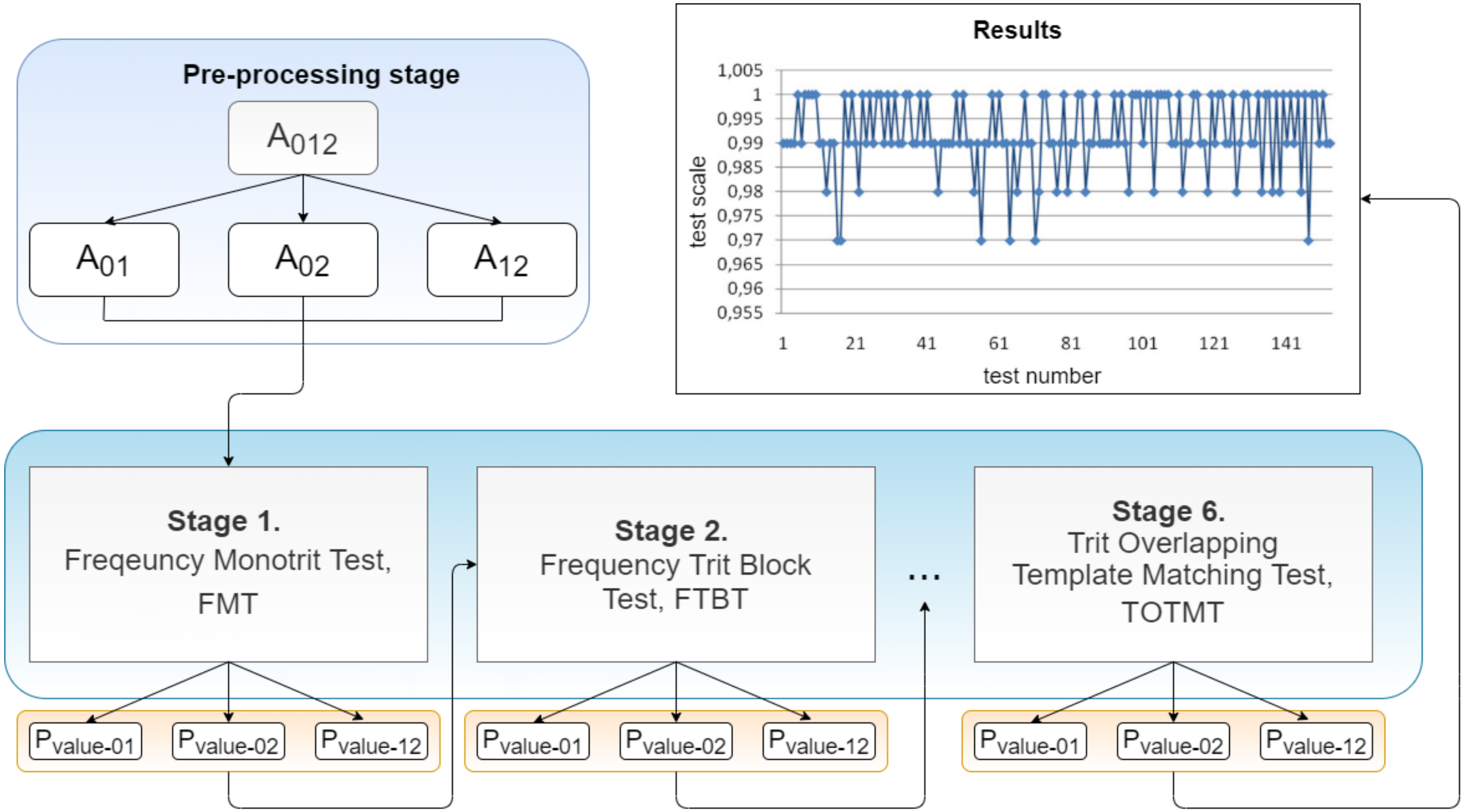
2.1.6 $y_3 = Sbox(((k_3 + y_3) <<< x_5) \oplus k_1)$; $y_4 = Mix(Sbox(((k_4 + y_4) >>> x_6) \oplus k_2))$.

2.2. $M_q = (y_1 \mid y_2 \mid y_3 \mid y_4)$

Pseudocode of TriGen v.2.0 PRNG

54

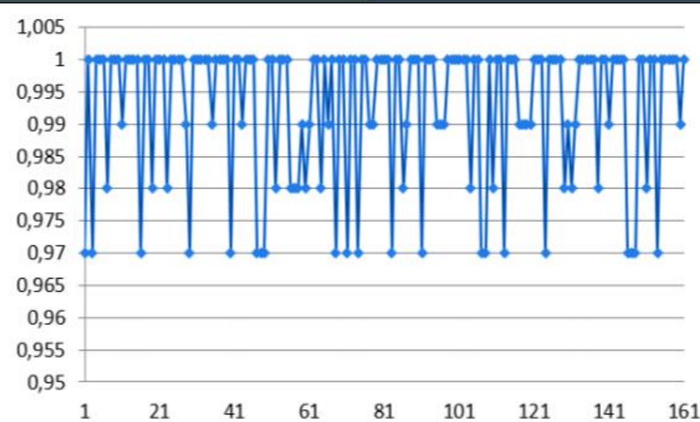
PRNG and TRIT STS [2/3]



Stage 1. Frequency Monotrit Test, FMT
Stage 2. Frequency Trit Block Test, FTBT.
Stage 3. Trit Runs Test, TRT.
Stage 4. Trit Test for the Longest Run in a Block, TTLROB.
Stage 5. Non-overlapping Template Matching Trit Test, NTMTT.
Stage 6. Trit Overlapping Template Matching Test, TOTMT.

55

Software tool TRIT STS



56

Our Plans for the Future

National Quantum Cybersecurity System of Ukraine (during 2022-2027)

- State Scientific and Research Institute of Cybersecurity Technologies and Information Protection
- National Aviation University
- Institute of Physics of the NAS of Ukraine
- Cybersecurity and Cryptography companies and R&D centers

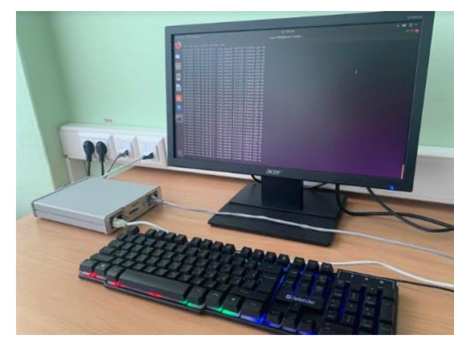
QuantUA

QKD + PQ Symmetrical Algorithm + Additional Procedures (Authentication, Privacy Amplification, PRNG etc.)

57

About NAU Cybersecurity R&D Lab

- development and optimization of web-sites / web-appl.;
- penetration testing and security analysis of web-sites / ICS / software-hardware complexes;
- information security / cybersecurity audit;
- encryption algorithms / PRNGs / hash-functions development, software / hardware realization and security level assessment;
- software realization of algorithms of any complexity in C / C++, Python, Java;
- designing and implementation of printed circuit boards and antennas, digital electronics of any complexity;
- deep investigation of software / hardware solutions in IT, cybersecurity, telecommunications;
- designing and conducting training courses, workshops and laboratory testing in information security (cybersecurity) / CIIP / cryptography / computer networks / AI / ML / Big Data etc.



http://cyberlab.fccpi.nau.edu.ua/

DEEPSEC

IN-DEPTH SECURITY CONFERENCE EUROPE
16 TO 19 NOVEMBER 2021

FROM
UKRAINE
WITH
LOVE

Thank you for your attention!

NATIONAL AVIATION UNIVERSITY

ФАКУЛЬТЕТ КІБЕРБЕЗПЕКИ, КОМП'ЮТЕРНОЇ ТА ПРОГРАМНОЇ ІНЖЕНЕРІЇ

Sergiy Gnatyuk

+380971934425
s.gnatyuk@nau.edu.ua
sergio.gnatyuk@gmail.com
https://www.facebook.com/sergiy.gnatyuk