



Classical Crypto Quantum Safe Crypto

June 2016

ID Quantique PROPRIETARY



AGENDA

- ▶ Why Encrypt?
- ▶ What Matters in Cryptography
- ▶ The New Threat
- ▶ Quantum Safe Crypto



Swiss company,
founded 2001, based
in Geneva.

World leaders in Quantum-Safe
Crypto.

Spin-off of University
of Geneva, Group of
Applied Physics.

Quantum Key
Generation

Quantum Key
Distribution

Quantum-safe
high-performance
layer 2 encryption

IDQ Partners & Customers (extract)



WHY ENCRYPT?

Submarine internet cables are a gift for spooks

16:54 25 June 2013 by Paul Marks

It's a golden age for spying. The subsea fibre-optic cables that carry telephone and internet traffic are a technological marvel – and a gift to intelligence agencies.

They make landfall at just a handful of locations, meaning vast quantities of data can be sucked out at one site and, according to the prolific US National Security Agency whistleblower Edward Snowden, that is what British intelligence has been doing for the last 18 months.

In a leak to *The Guardian* newspaper on 22 June, Snowden said the UK Government Communications Headquarters (GCHQ) in Cheltenham is siphoning data from at least 200 fibre-optic telecommunications cables – including many of the transatlantic subsea cables that hit British shores at Bude in Cornwall.

The tapping project, known as Tempora, allows phone calls to be monitored, as well as emails on offshore American-hosted webmail services such as Gmail, Yahoo and Outlook. Also included are Google and Yahoo searches, and data from Facebook and Twitter.

J'aime 102 Tweet Share 26



Bude: hotspot for snoops. Jewell/nomadphotography



The growing security risk of fibre tapping

05 Oct 2010

3 Comments



Routine maintenance work or a cleverly disguised team of fibre tappers in action?

Corporate datacentres, with their vast stores of business-sensitive information, present a tempting target for criminal groups. Unfortunately for the would-be cyber crook, today's enterprise security systems are so sophisticated that hacking into an enterprise datacentre is nigh on impossible.

But what if there were another way to get at this valuable data that circumvented most traditional security software?

Welcome to the shady world of fibre tapping, where instead of physically accessing a site or attempting to hack into it, the cyber criminal simply taps the optical fibre leading up to it.

Cases of fibre tapping are relatively rare, but with the cost of fibre tapping devices falling and the number of enterprises storing sensitive data in remote datacentres growing in tandem with the rise of cloud computing, many more are likely in the future.



N



... and everyone's doing it!



Mandiant Report 2013 on systematic Chinese government hacking:

- ▶ The Chinese government (PLA) employs an entire department of professional hackers – APT1
- ▶ APT1 has systematically stolen hundreds of terabytes of data from at least 141 organizations
- ▶ APT1 periodically revisits the victim's network over several months or years (up to 4 years)
- ▶ They steal broad categories of intellectual property for industrial espionage

http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf

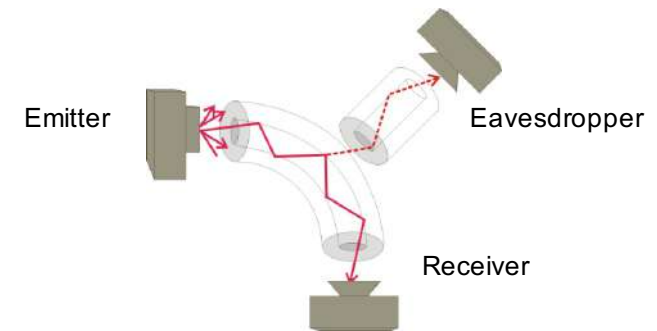
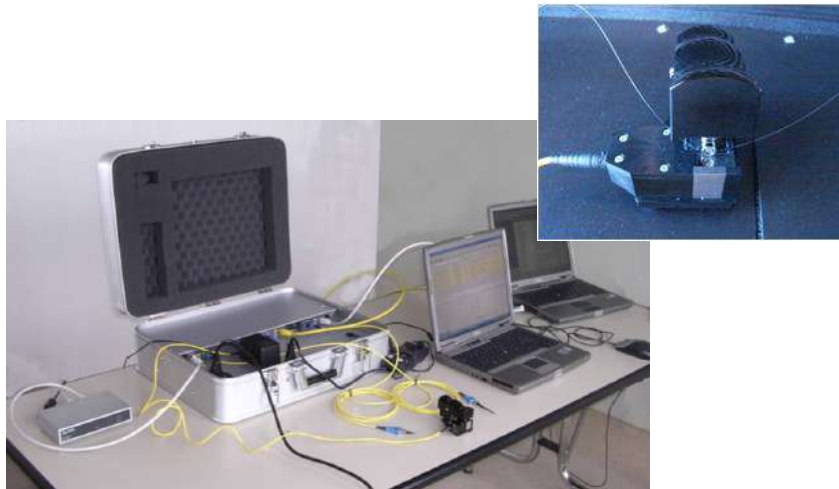
China's Internet 'Hijacking' Creates Worries for Security Experts

- ▶ For 15 minutes in April 2010, network traffic from 15% of world-wide routes was diverted via China before reaching intended destination
- ▶ Using BGP messages, China Telecom supplied erroneous routing information that the fastest path for the diverted routes was through Chinese networks

<http://www.bgpmon.net/chinese-isp-hijacked-10-of-the-internet/>

Optical Tapping for under €500

- ▶ There are multiple ways to intercept an optical fiber
- ▶ The simplest method is fiber bending & coupling
 - No link interruption
 - Moderate insertion loss
 - Trivial manipulation



Data interception over a live optical fiber is feasible with equipment costing less than €500 and available online

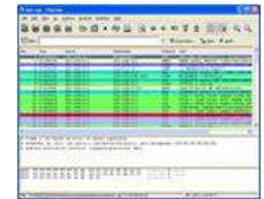
□ For example

- http://www.fods.com/optic_clip_on_coupler.html
- Proposed applications include:
 - Test maintenance
 - Fiber identification
 - Voice communications

False Perceptions of Network Security

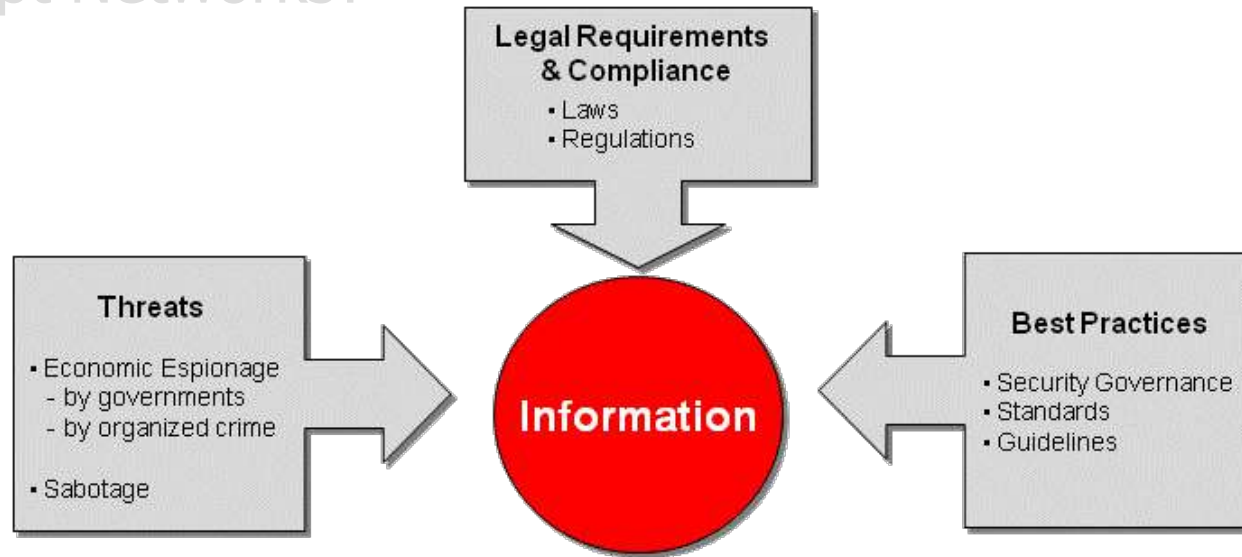


- ▶ **Data is protected by volume... No!**
 - Snowden reports prove that intercepting and analyzing volume traffic is not a major hindrance
 - 10Gbps data flows simply improve the ROI of the hacker
- ▶ **WDM Networks cannot be tapped...No!**
 - Spectral filters and analysers with high separation exist and are cheap
- ▶ **Fibre Channel protocols are safe... No!**
 - Network analyzers specialized in FC can sniff & reconstruct FC traffic
- ▶ **Dark Fibers are Safe...No!**
 - Dark fiber have no inherent protection & can be accessed via multiple points, including telecom stations and manholes
- ▶ **Attenuation Monitoring is adequate protection...No!**
 - Special hacking techniques do not trigger an alarm
- ▶ **VPNs are inherently secure...No!**
 - There is no "privacy" to a VPN – it simply segments data virtually



Legal & Compliance Requirements

Why Encrypt Networks?



2003 Wolf Report revealed

- Optical tap discovered in Verizon telecom station on fiber used by financial institution
- "Secret rooms" installed in AT&T network to eavesdrop on internet traffic carried by optical fiber.
- Eavesdropping on Deutsche Telekom's main connection at Frankfurt International Airport

2013 Snowden Reports revealed

- Systematic large scale interception of undersea and other optical fibers by US & UK governments ("Upstream")
- Systematic large scale clandestine surveillance of internet communications by US government ("Prism")
- Government hacking of telecommunication data or active collusion with telecommunication companies to intercept data by many governments

Legal & Compliance Requirements

Penalties for Data Breaches are also increasing

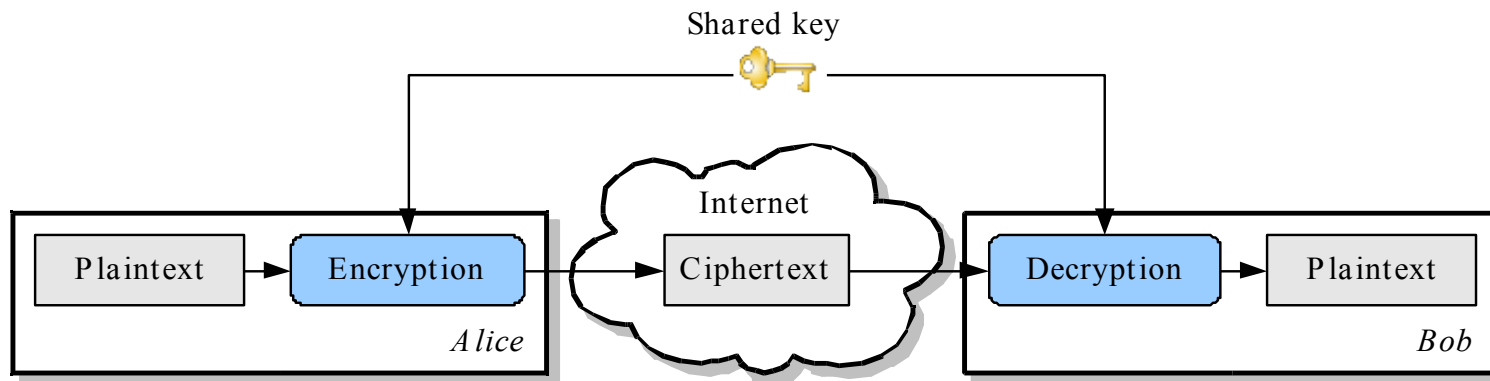


- ▶ There is a general trend towards increasing penalties for data breaches
 - Trend towards increasing penalties in all sectors & most geographies
 - Include the possibility of criminal jail sentence if negligence demonstrated
- ▶ FTC urges data-breach penalties
 - The Federal Trade Commission is hoping US Congress will see fit to legislate monetary consequences for breached companies
- ▶ US Congress wants to introduce 'Personal Data Protection and Breach Accountability Act of 2014'
- ▶ USA - HIPAA healthcare violation penalties rise
- ▶ EU - General Data Protection Regulation (GDPR) – to come in force 2018
 - Requirement to report breach to national authority
 - Proposed fine up to 4% of the annual worldwide turnover
 - Unless data is encrypted!

WHAT MATTERS IN CRYPTOGRAPHY

What is Cryptography?

- ▶ **Cryptography:** The art of taking a message and rendering it unreadable to any unauthorized party
 - ▶ **Cryptanalysis:** The art of code breaking
- } Cryptology
- ▶ **Process:** An encryption key is added to clear text to turn it into ciphertext. The key is then used to decipher the text to turn it back into plaintext



Kerckhoffs' Principle

A cryptosystem should be secure even if everything about the system, except the key, is public knowledge.



Auguste Kerckhoffs
(19 January 1835 – 9 August 1903)

- ▶ The security of the encryption keys are vital to protection of the data

- ▶ They must be unique & truly random
 - How strong are the keys ?
 - How unique are the keys?
 - How easily are they copied?
 - How easily can they be "brute forced" ?
 - How often are they changed?
 - Where are they stored who has access to them?



The Encryption Key is.... key



▶ Is the key really random? Are there “back doors”?

- NIST standards influenced by governments

<http://arstechnica.com/security/2014/01/how-the-nsa-may-have-put-a-backdoor-in-rsas-cryptography-a-technical-primer/>

▶ Is the key really random? Have they been tampered with?

- Intel random number generator (RNG) used for crypto functions in microprocessor could be “dumbed down” from 128 bits of randomness to 32 bits through doping of transistors to produce predictable keys

<http://arstechnica.com/security/2013/09/researchers-can-slip-an-undetected-trojan-into-intels-ivy-bridge-cpus/>

▶ How unique are the keys? How easily are they copied?

- “Minding your Qs and Ps” by renowned Swiss cryptographer Lenstra
- 5% of keys in network devices (like Cisco) are weak keys & can be copied or guessed

<http://www.idquantique.com/news/newsletter-networkencryption-october-2012-en.html?start=2>

<https://factorable.net/weakkeys12.conference.pdf>

The Encryption Key is.... Key (cont.)







- ▶ How often are they changed?
 - Is there real randomness introduced?
 - Is there automated key exchange? How often? The longer a key is used, the more valuable (and dangerous) it becomes

- ▶ Where are they stored and who has access to them?
 - Generated & stored in hardware or software?
 - Where do the crypto operations take place?
 - Is there separation of duties between the network & crypto admin? Or does your telecom operator or network admin own your company?

Layer 2 Encryption Platform: CENTAURIS



CN4010/ 4020	CN6010	CN6100	CN8000
			
Compact desktop enclosure	1U rack mount enclosure	1U rack mount enclosure	4U rack mount enclosure
10/100/1000Mbps	100/1000Mbps	10Gbps	10x10Gbps
RJ45 electrical interfaces (CN4010) Pluggable optical interface (CN4020)	RJ45 electrical interfaces Pluggable optical SFP	Pluggable XFP optical interfaces	Pluggable optical SFP+
External plug pack	Dual redundant AC/DC supplies	Dual redundant AC/DC supplies	Dual redundant AC supplies
	User-serviceable fans/battery	User-serviceable fans/battery	User-serviceable fans/battery
	Quantum TRNG for key generation		Quantum TRNG for key generation
	Support for QKD	Support for QKD	Support for QKD

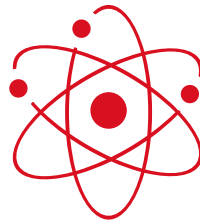


The THREAT: QUANTUM COMPUTERS

Post-Quantum Era? A World with Quantum Computers



Physics



Computer Science

10101010101100
10101011010100
00110110101010
10101010110010

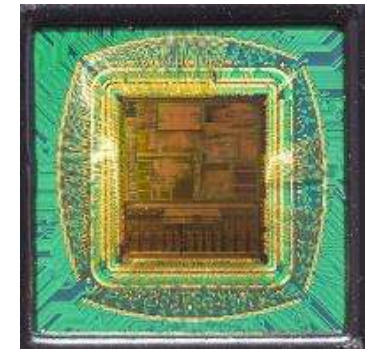


- Computation is a physical process -
 - Bits → Qubits -
- Major consequences in Information Security -

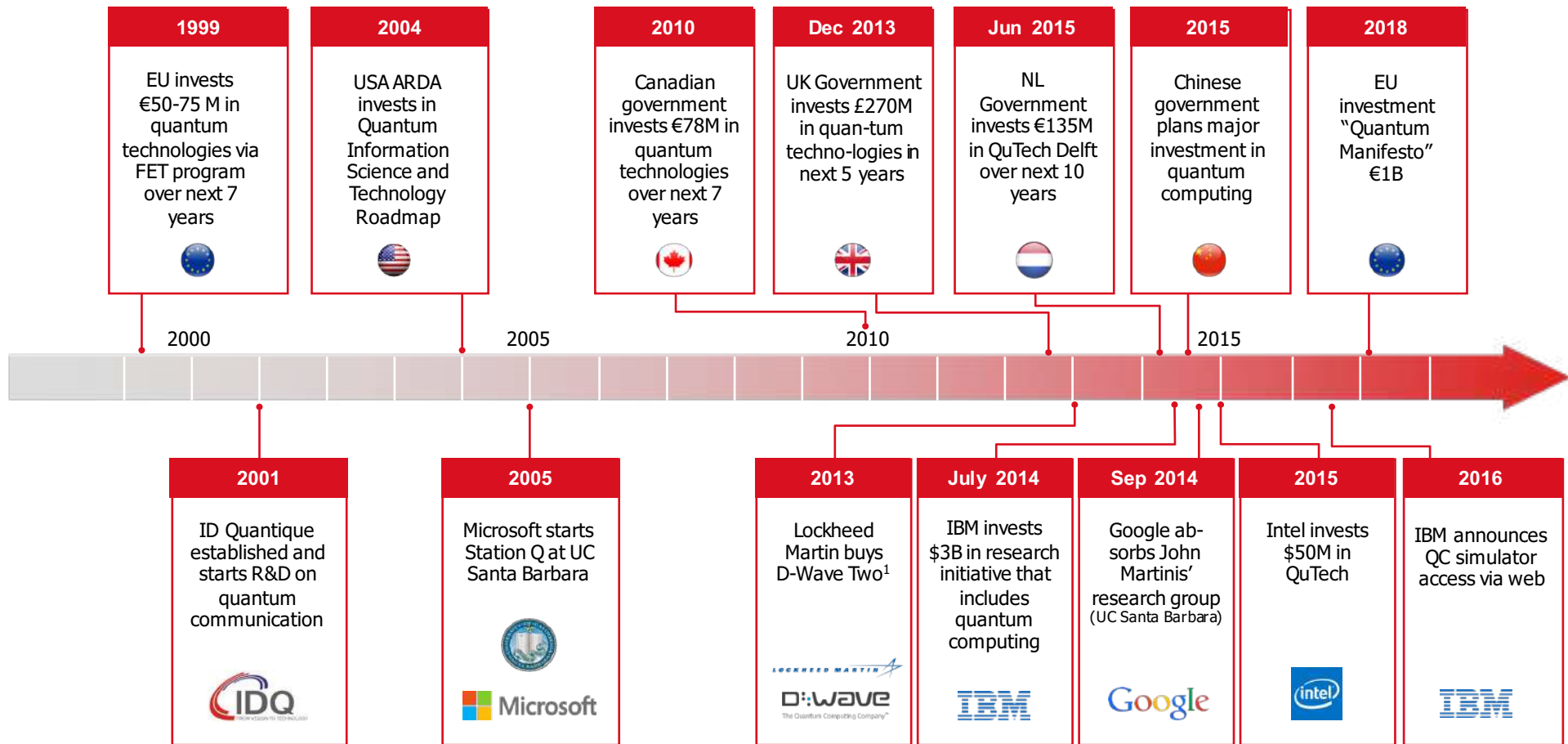
The Quantum Computer



- ▶ Computation with **Qubits**.
- ▶ Main difference: build coherent superposition of states.
- ▶ Behaves like a massively parallel computer.
- ▶ Solves problems in much fewer steps.
- ▶ Opportunity: some “intractable” computations become feasible.
- ▶ Threat: break current public key cryptographic primitives (RSA, ECC...)
 - ↳ This is why Quantum Computing is now discussed in Information Security.



Increasing Interest in Quantum IT

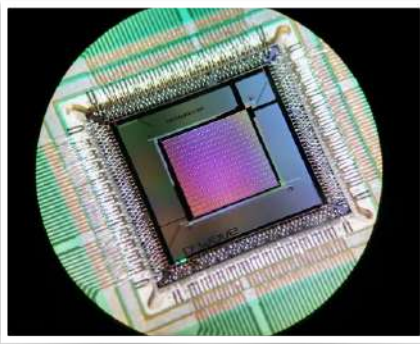


First Practical Quantum "Computer"

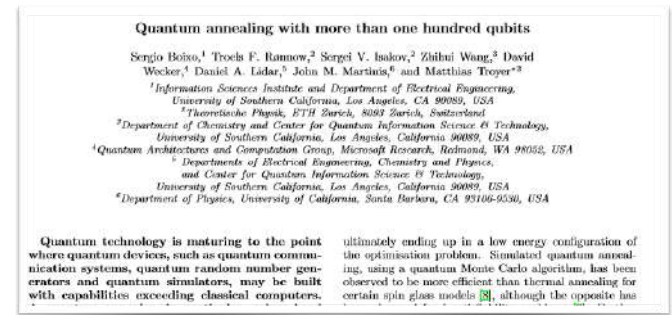


▶ According to the community, **DWave One**

- Solves a lot of the general engineering problems of building quantum computers.
- Quantum "optimizer" rather than universal quantum computer i.e.. cannot run Shor's algorithm.
 - But is this the only danger to current public key crypto?
 - See public DWave patents on "inverse multiplication".



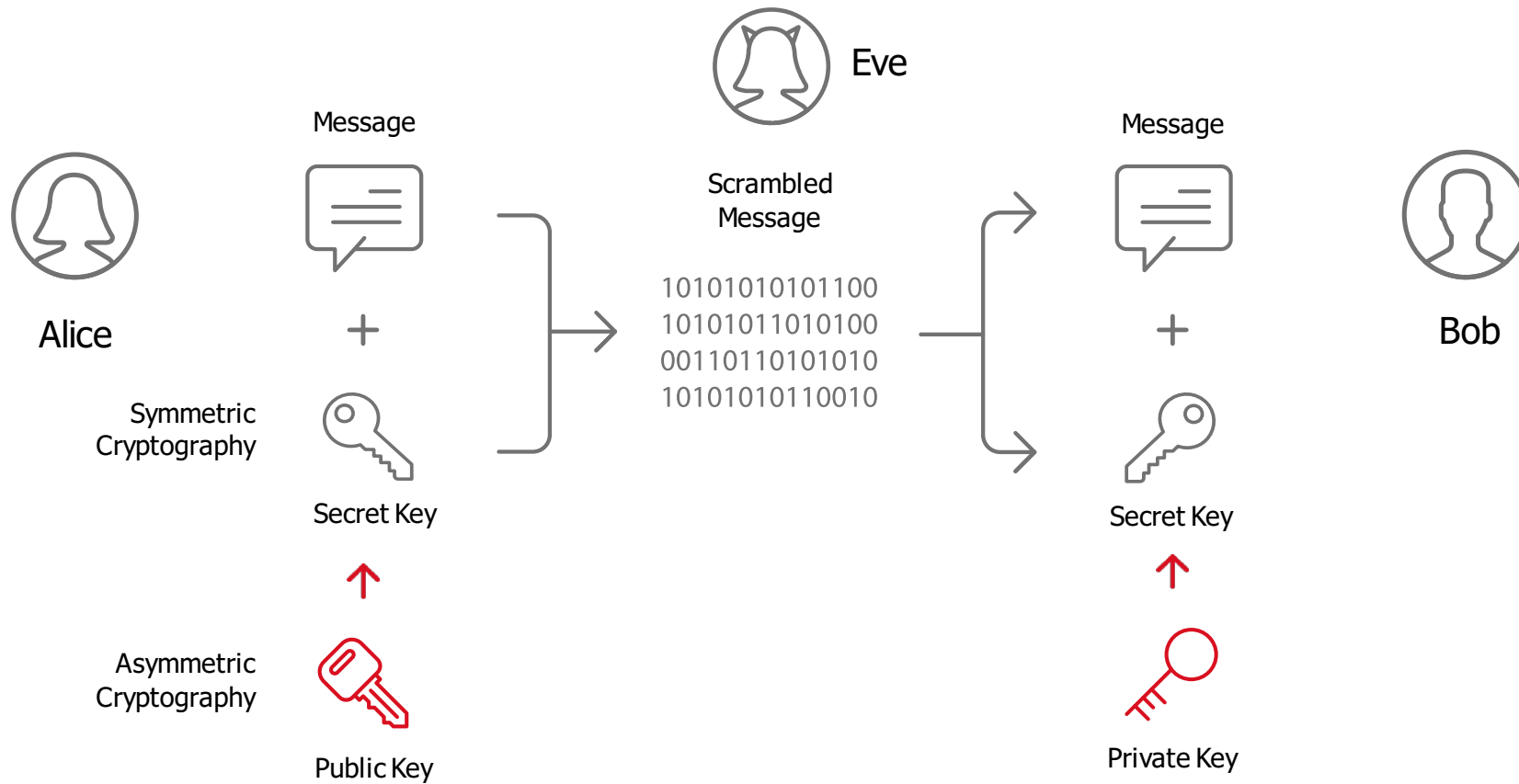
▶ **DWave Two** is already available



arXiv:1304.4595v2 [quant-ph] 21 Jul 2013



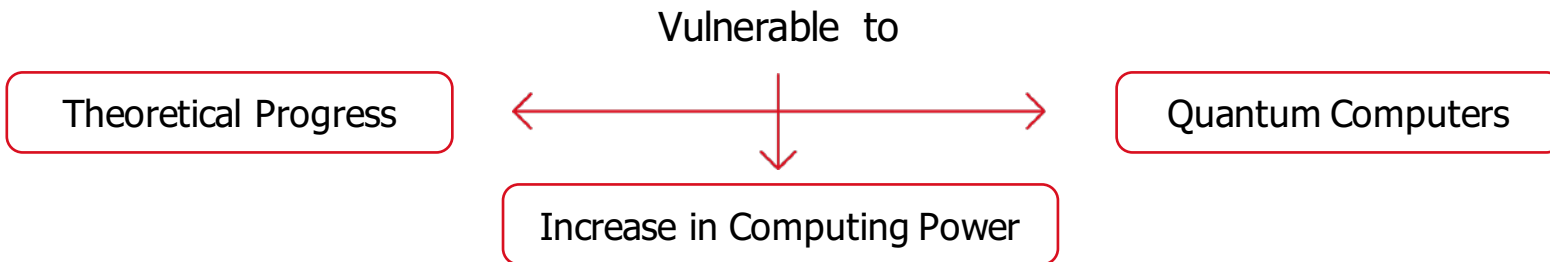
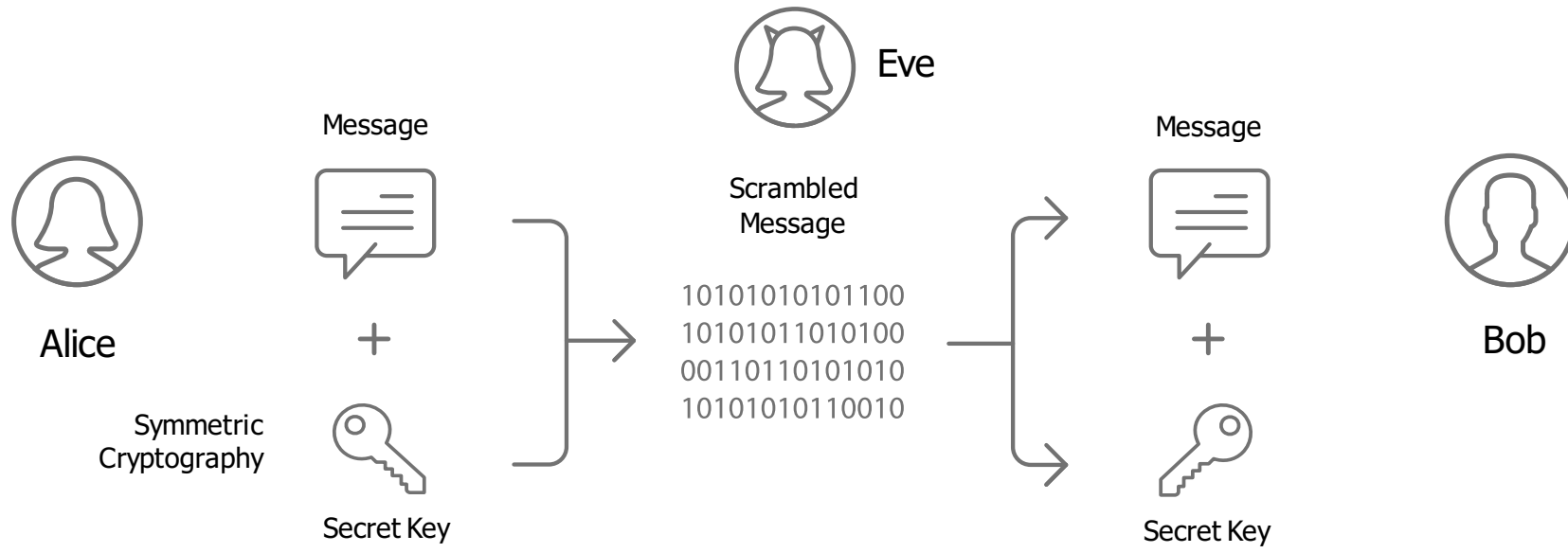
Public Key Cryptography: Threats



$$2'357 \times 4'201 = ?$$

$$A \times B = 9'901'757$$

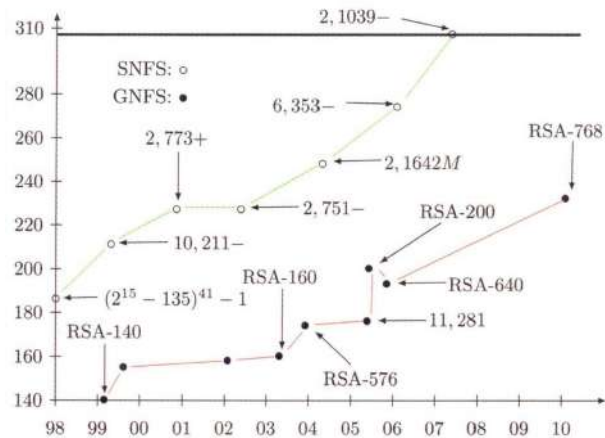
Public Key Cryptography: Threats



Shor's Algorithm

- ▶ Peter Shor, 1994
- ▶ Quantum algorithm for integer factorization

$O((\log N)^3)$ vs. $O(e^{1.9 (\log N)^{1/3} (\log \log N)^{2/3}})$



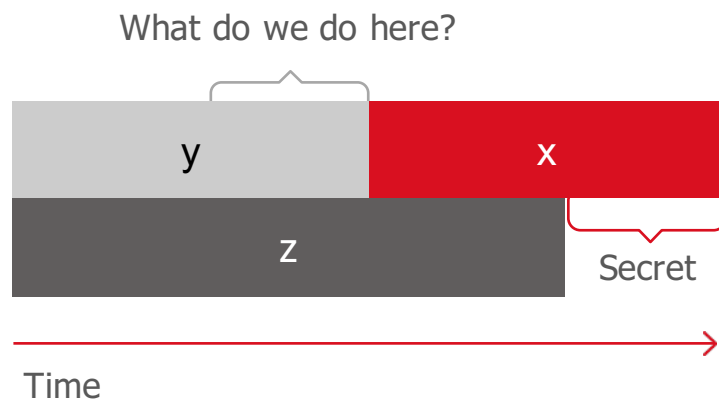
Can break RSA, Elliptic Curve & Diffie Hellman

Grover's Algorithm

- ▶ Lov Grover, 1996
- ▶ Quantum algorithm to perform search in an unsorted database
- ▶ $O(n^{1/2})$ vs $O(n)$
- ▶ Key halved for symmetric cryptography
AES-128 → 64 bits security
AES-256 → 128 bits security

When Do We Need to Start Worrying?

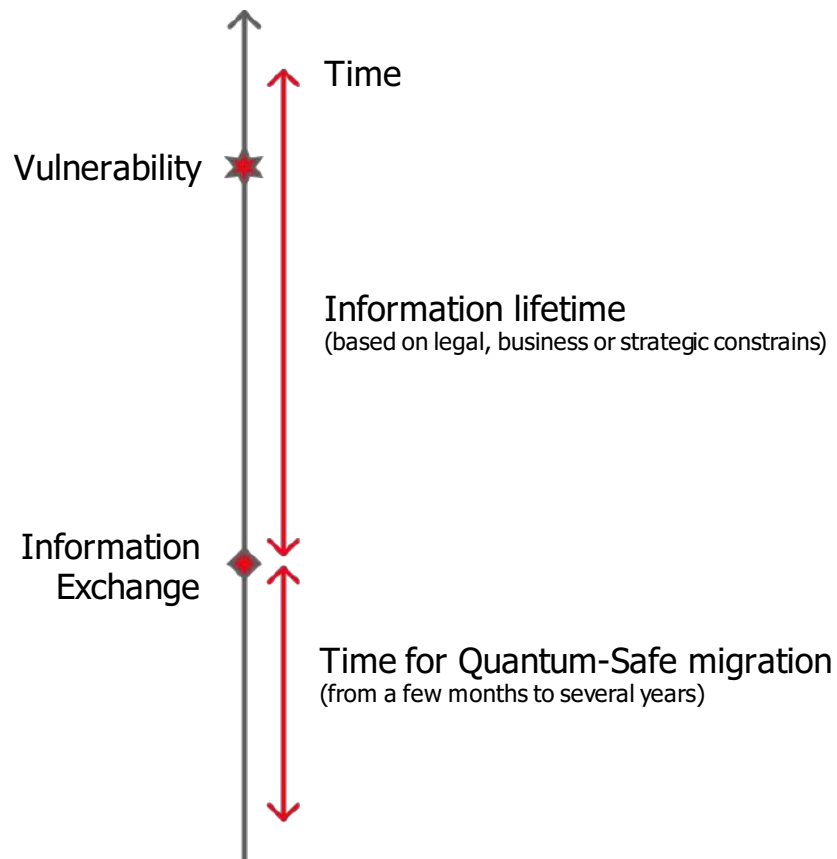
Theorem 1: If $x + y > z$, then worry



► Depends on:

- How long do you need encryption to be secure? (x years)
- How much time will it take to re-tool the existing infrastructure with large-scale quantum-safe solution? (y years)
- How long will it take for a large scale quantum computer to built (or for any other relevant advance? (z years))

When Do We Need to Start Worrying?



- ▶ “Wait and see” approach is too risky.
- ▶ Encrypted data can be (and is being) downloaded & analyzed offline.
- ▶ Next generation of cryptographic infrastructure:
 - Must have quantum-safe alternatives
 - Should have algorithmic agility built in
- ▶ If quantum computer available in 2030, and information lifetime is 10 years, then a cryptographic infrastructure needs to be in place by 2020.

Be quantum-ready by 2020!

The SOLUTION:
QUANTUM SAFE CRYPTO

ETSI Proposes Move to Quantum-Safe Cryptography




- ▶ Ongoing international efforts to develop standards around quantum-safe cryptography, eg. ETSI.
- ▶ Quantum-safe cryptography includes algorithms and techniques which are not vulnerable to quantum computing.
 - Post Quantum Crypto (aka quantum-resistant algorithms)
 - Quantum Key Distribution
- ▶ ETSI White Paper on Quantum Safe Cryptography published mid 2014 recommends moving to quantum-safe crypto.
- ▶ The ETSI whitepaper states:

Without quantum-safe encryption, everything that has been transmitted, or will ever be transmitted, over a network is vulnerable to eavesdropping and public disclosure.



When NSA goes Public...

A screenshot of the NSA website's 'Information Assurance' page. The header includes the NSA and Central Security Service logos and the tagline 'Defending Our Nation. Securing The Future.' The navigation menu includes links for HOME, ABOUT NSA, ACADEMIA, BUSINESS, CAREERS, INFORMATION ASSURANCE (highlighted), RESEARCH, PUBLIC INFORMATION, and CIVIL LIBERTIES. The main content area contains three paragraphs of text.

NATIONAL SECURITY AGENCY   CENTRAL SECURITY SERVICE

Defending Our Nation. Securing The Future.

HOME ABOUT NSA ACADEMIA BUSINESS CAREERS **INFORMATION ASSURANCE** RESEARCH PUBLIC INFORMATION CIVIL LIBERTIES

“In the current global environment, rapid and secure information sharing is important to protect our Nation, its citizens and its interests. Strong cryptographic algorithms and secure protocol standards are vital tools that contribute to our national security and help address the ubiquitous need for secure, interoperable communications”.

“IAD will initiate a transition to **quantum resistant algorithms** in the not too distant future.”

“Our ultimate goal is to provide cost effective **security against a potential quantum computer.**”

The Solution: Quantum-Safe Cryptographic Infrastructure



- ▶ **“Post-quantum” algorithms (aka quantum-resistant algorithms)**

$$e = r * h + m \pmod{q}$$

- ▶ Classical codes deployable without quantum technologies.
 - Eg. Lattice, matrix -based algorithms
- ▶ Believed to be secure against Shor’s algorithm but no guarantee that there will not be other quantum attacks.
- ▶ Recommended for quantum-safe digital signatures & end point encryption.

Quantum Key Distribution



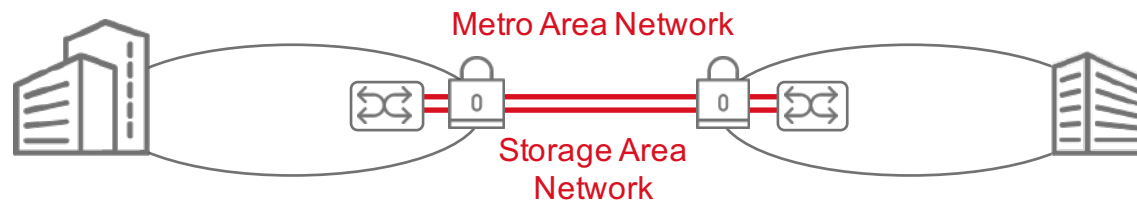
- ▶ Hardware solution.
- ▶ Typically no computational assumptions and thus known to be secure against future quantum attacks.
- ▶ Recommended for encryption of high-value information with requirement for long-term confidentiality.
 - E.g. Data center interconnect, government data

Both sets of cryptographic tools can work together to form a quantum-safe cryptographic infrastructure

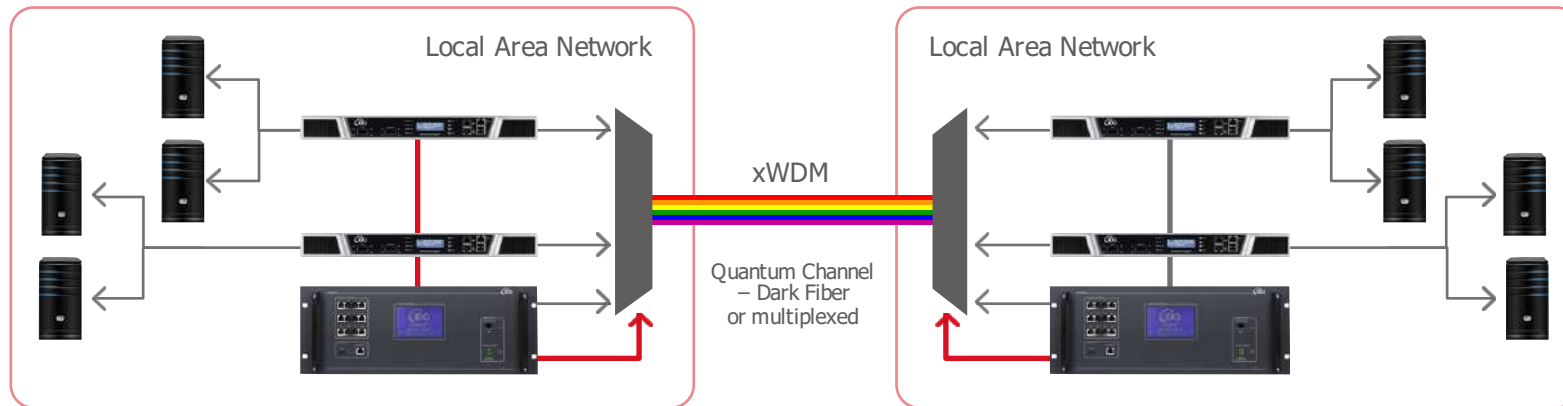
IDQ QKD Scenarios: Today



- ▶ Supporting an existing encrypted link, IDQ QKD currently
 - Addresses distances up to 100km.
 - Can be multiplexed up to distances of 30km, but requires a dark fiber for the actual quantum exchanges for distances between 30km-100km.
 - Works in point-to-point mode.
- ▶ Suitable for layer 1 or layer 2 topologies
 - LAN / MAN / SAN
 - Meshed WAN
- ▶ Use cases
 - Protection of mission critical data on data centre and MAN interconnections.



Quantum-Enabled Network Encryption: Today



China Quantum Network (IDQ not – yet - involved)



Quantum Backbone

- Total Length 2000 km
- 2013.6-2016.12
- 32 trustable relay nodes
- 31 fiber links
- Metropolitan networks
 - Existing: Hefei, Jinan
 - New: Beijing, Shanghai
- Customer: China Industrial & Commercial Bank; Xinhua News Agency; CBRC



Italian Quantum Network (IDQ involved)



► Approach planned in several phases

- 2015 Turin – Novara (test)
- 2016 Turin – Florence
- 2017 Florence – Rome – Matera
- 2017+ completion via Sicily, Malta, Sardinia (OTA)

Swiss Quantum Network (IDQ involved)



- ▶ Project with Swiss Government/Military
- ▶ Secure Management Network of the army



QUANTUM KEY GENERATION

Random Numbers in Cryptography



- ▶ Main uses of cryptography are to ensure:
 - Confidentiality (secrecy of the data)
 - Integrity (the data has not been tampered with)
 - Authentication (data sent to the right person in the right order)
 - Non-repudiation (can prove who sent the data)
 - Secure access control (via secure tokens or passwords)
- ▶ The key is the cornerstone of secure cryptosystems
- ▶ Kerckhoffs' Principle:
 - "A cryptosystem should be secure even if everything about the system, except the key, is public knowledge."
- ▶ To provide adequate security the key must be:
 - Unique
 - Truly random (unpredictable)
 - Stored, distributed & managed security



Auguste Kerckhoffs
(19 January 1835 – 9 August 1903)

Random Numbers in Cryptography

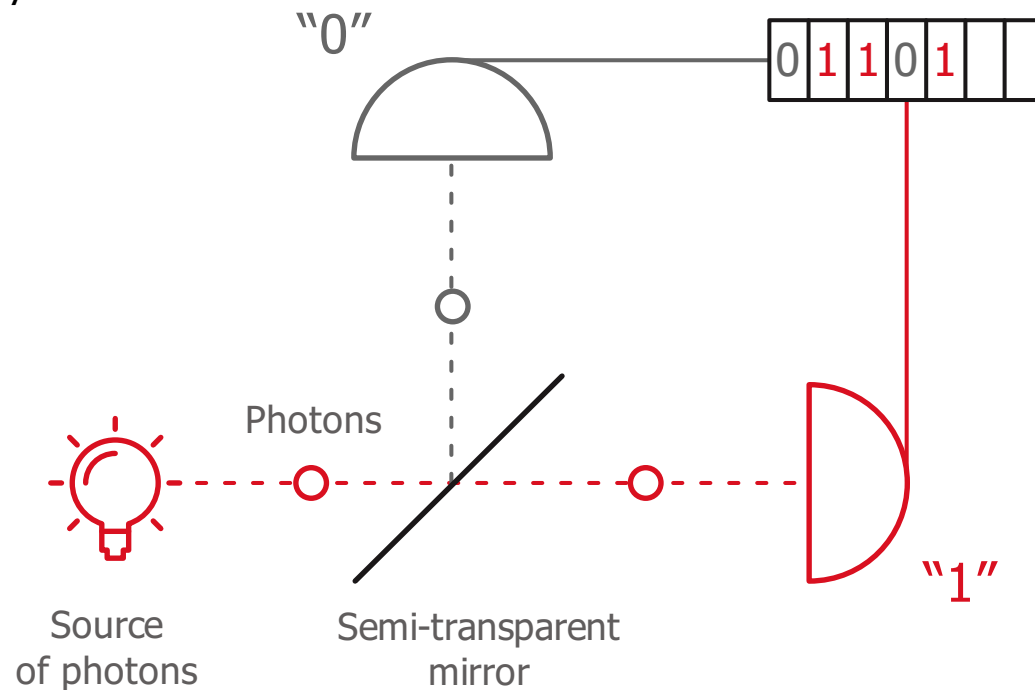
1 1 0 1 0 1
0 0 0 1 1
1 1 0 1 0
1 0 0 1 1
0 1 1 0
1 0 1 0 1 1
0 1 1 0
1 0 1 1 0
0 1 1 1
1 0 1 0 1 1

- ▶ Random numbers are difficult to produce.
 - Computer programs are deterministic.
 - Computers cannot produce random numbers without special hardware.
- ▶ Impossible to prove randomness of a finite sequence a posteriori.
 - Possible only to test the statistical properties of the random numbers.
 - When generating random numbers, understanding the method used is critical.

True Random Number Generator based on Quantum Physics



- ▶ Physical Random Number Generator exploiting a phenomenon described by quantum physics:
- ▶ Provably random



Quantis QRNG Solution



- ▶ Random bit rate:
 - 4 Mbps or 16 Mbps
- ▶ The most stringently tested and certified QRNG in the world.
- ▶ Used in IDQ's QKD solution.

Advantages

- ▶ Speed.
- ▶ Simple process that can be modelled → influence of environment can be ruled out.
- ▶ Live monitoring of elementary components possible to detect total failure.
- ▶ Instant full entropy.



Classical vs. Quantum RNGs

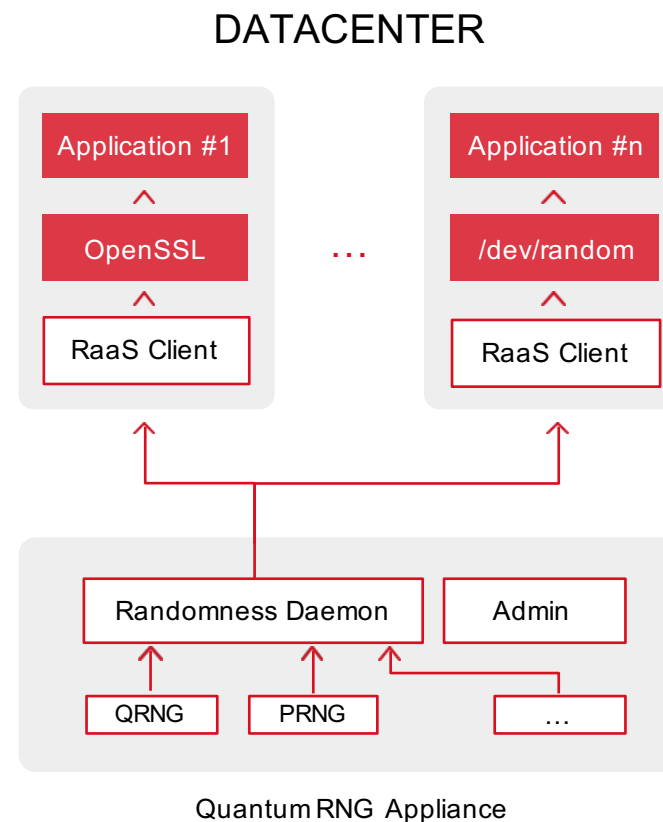


Category	Classical RNG	Quantum RNG
Source of randomness	Chaotic process (classical physics) -(Complex) environmental influence -Indefiniteness of initial conditions (chaos)	Quantum process -Fundamental laws of physics
Is the process randomness provable	No	Yes
What are the underlying assumptions?	Empirically-tested assumptions	Fundamental laws of physics
Is the quality of the randomness influenced by external factors?	Yes, possibly	No
Does the underlying technology allow live monitoring?	No	Yes
Does the underlying technology fail gracefully?	No	Yes
Is the result truly random?	Probably	Provably

Quantis Network Appliance: Randomness-as-a-Service

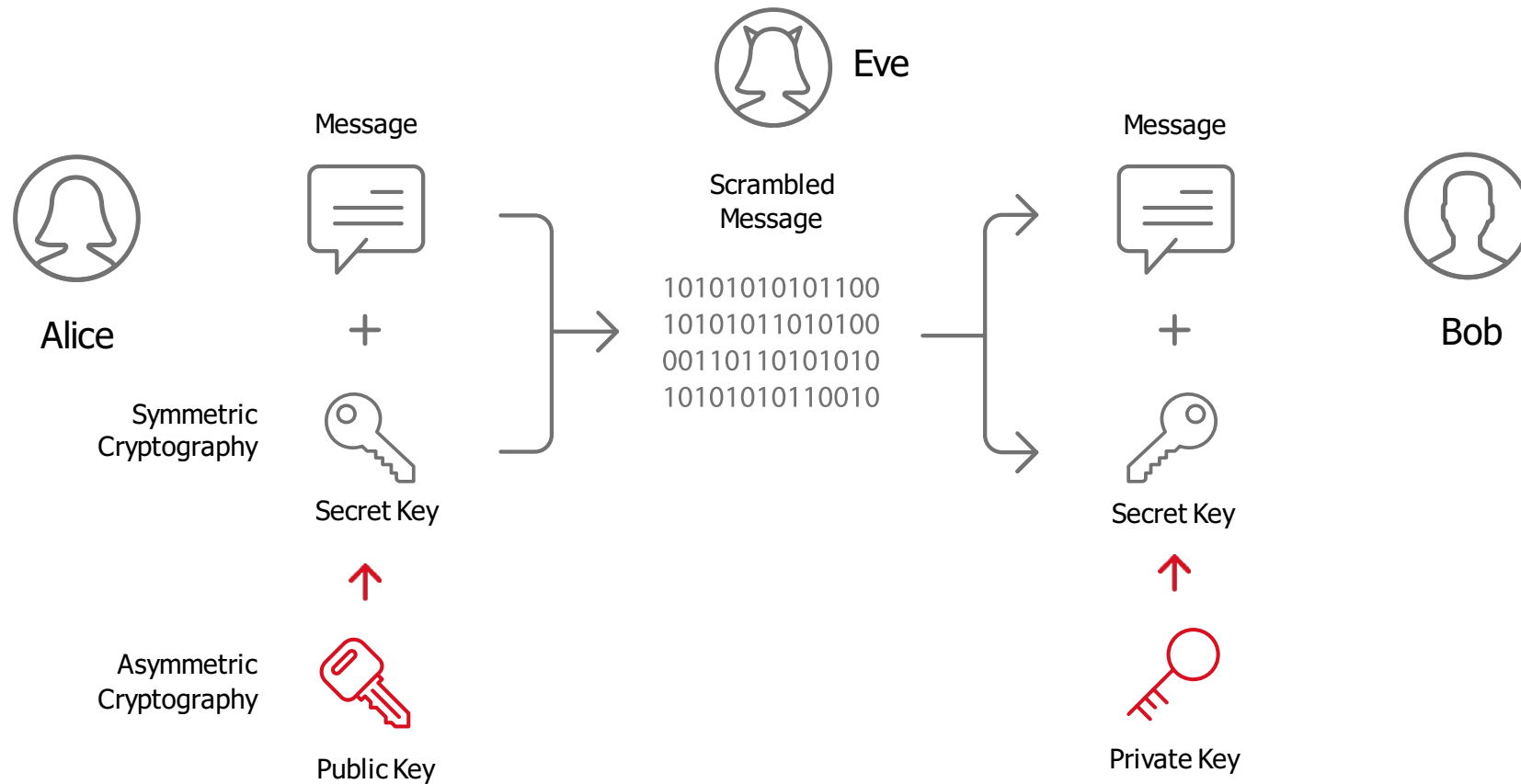


- ▶ Based on IDQ's quantum RNG.
- ▶ Hardware source of trust for cloud or distributed environments to provide secure keys for:
 - Crypto key generation for cloud & network environments (virtual machines, VPNs, etc).
 - Seeding of deterministic RNGs and commercial HSMs.
 - Randomness as a service.
 - Online gaming.

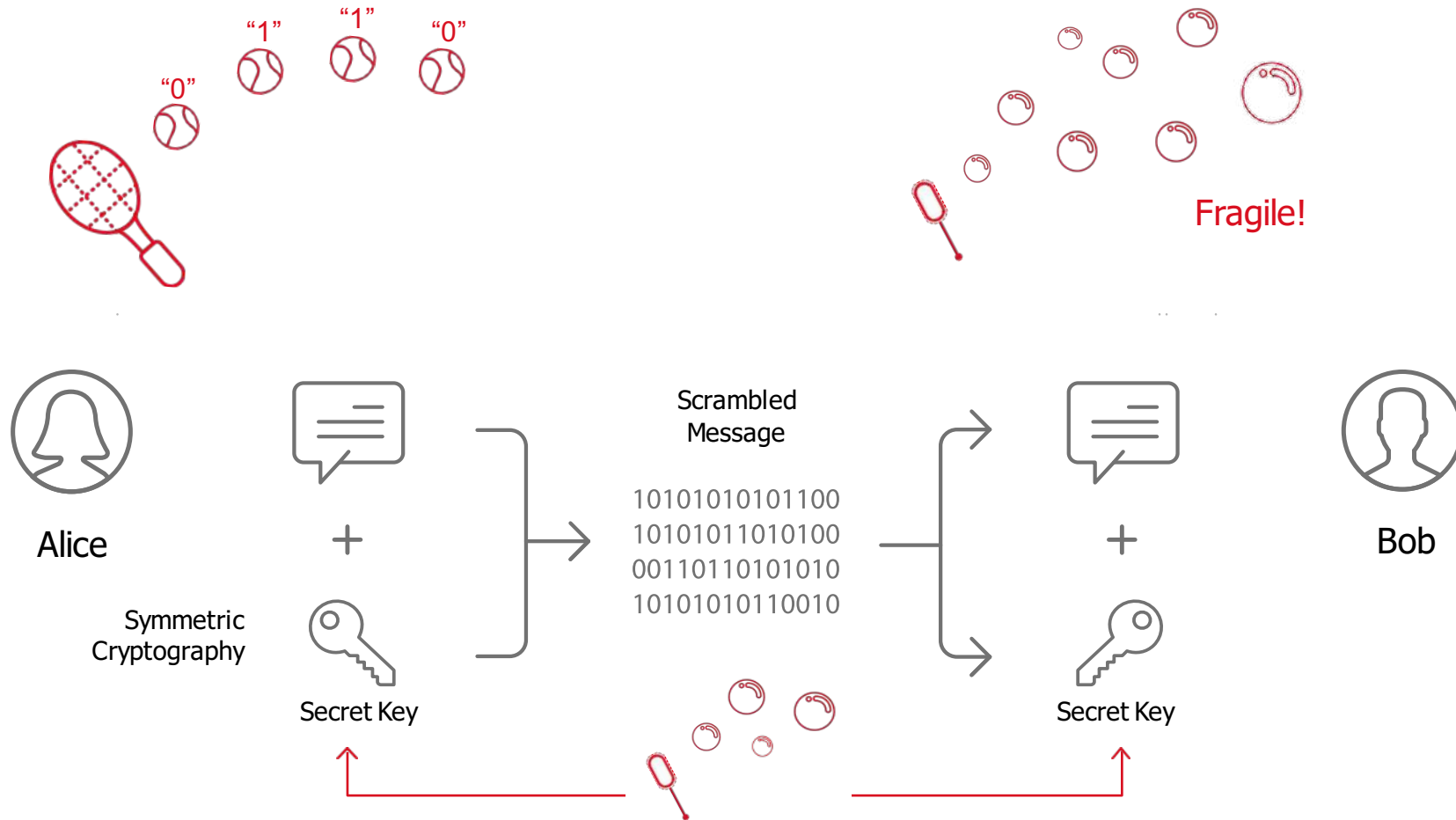


QUANTUM KEY DISTRIBUTION

Public Key Cryptography: Threats



Quantum Cryptography = Quantum Key Distribution (QKD)



Quantum-Enabled Network Encryption: Today



▶ Transparent Layer 2 Encryption

- AES-256 up to 100Gbps
- Multiprotocol (Ethernet, Fibre Channel)

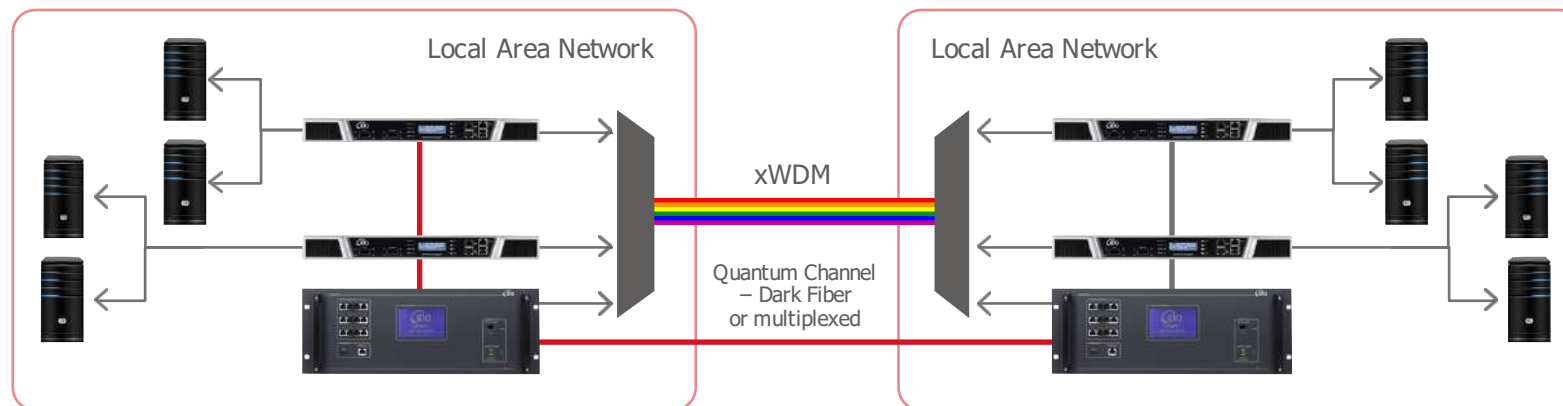


▶ Provably secure key distribution

- Distilled key distribution rate: 1000 bps over 25km/6dB
- Range: 100km



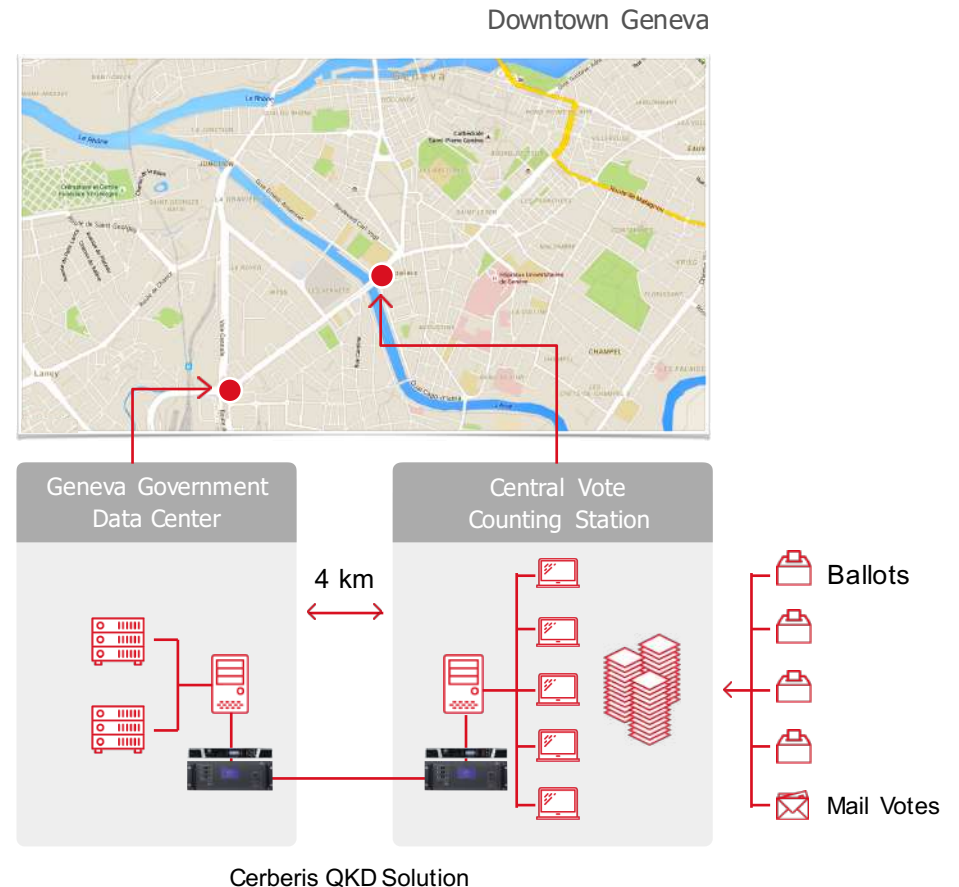
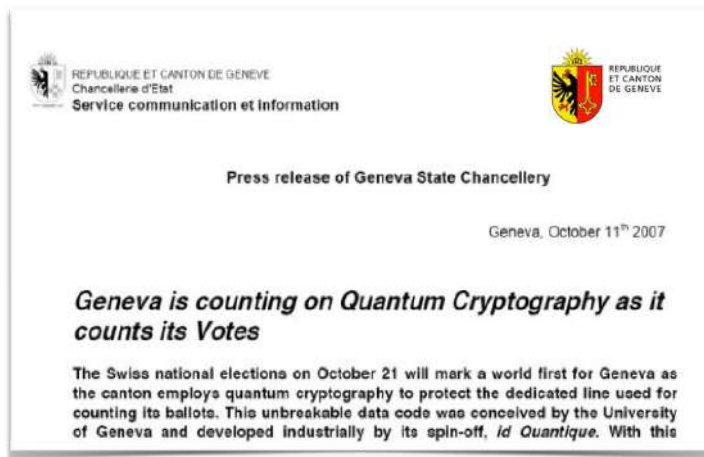
Quantum key server



QKD in Government & Public Administration



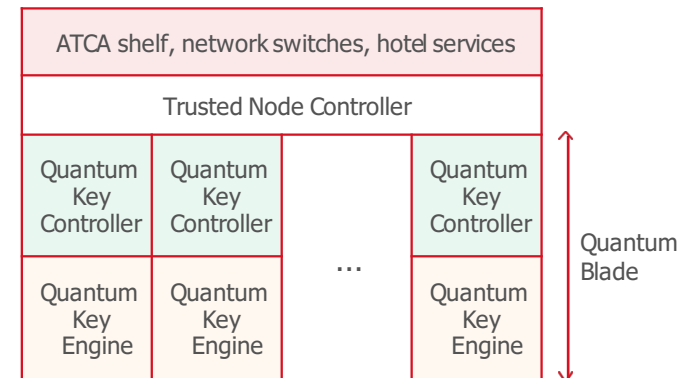
- ▶ Geneva (Switzerland) uses QKD to guarantee confidentiality & integrity of data during federal & cantonal elections.
- ▶ Working since October 2007.



Next: QKD Blade in Trusted Node Architecture



- ▶ The QKD Blade can be used in a Trusted-Node environment for long distances or multipoint environments.
- ▶ Two blades linked by a Trusted Node Controller.
 - Secure quantum key exchange between the blades.
 - Manages node discovery and provides route tables for quantum network.
 - Manages and routes key transactions.
 - Fault tolerant dynamic path finding algorithm.
 - Routing balances security and quality of service.
 - Finds least cost path across the QKD network.
 - Uses alternate routes when available.

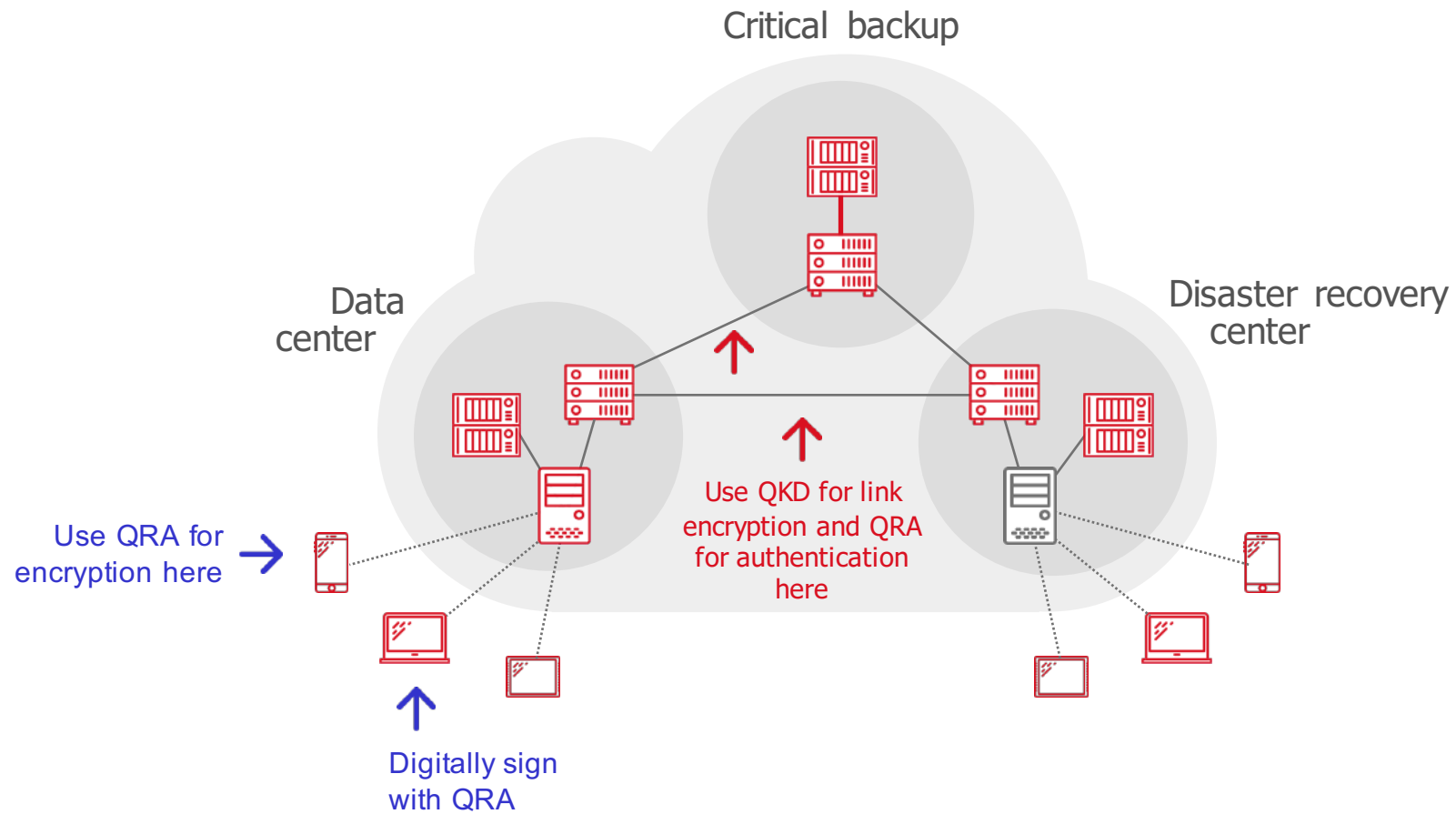


A Global Network Based on Free Space QKD



- ▶ Free Space QKD
 - QKD links with LEO satellites & UAVs.
 - UAV acts as a trusted node to transport the key to the necessary location.
- ▶ Free space QKD is moving out of the lab & into industry
 - Chinese have announced plans for QKD satellite in 2016.
 - IDQ feasibility studies available upon request.

Protect the Assets in Line with the Risk



Representante e Integrador para Latinoamérica

- **GLOBAL INTERACTIVE GROUP SRL**



- **ENFORCE ONE S.A. |**



- Alicia Moreau de Justo N° 740, Piso 3 of. 1
Puerto Madero, Buenos Aires. Argentina. CP1107)

info@gigsrl.com • www.gigsrl.com