DISMA Dipartimento di Scienze Matematiche G. L. Lagrange

Gruppo di Crittografia e Teoria dei Numeri

Seminario divulgativo della serie

CRITTOGRAFIA: dalla teoria alle applicazioni

CRITTOGRAFIA QUANTISTICA

Ivo Pietro Degiovanni - INRiM

27 Febbraio 2019 – ore 14:30

Aula Buzano - Dipartimento di Scienze Matematiche
Politecnico di Torino

POLITECNICO DI TORINO

Telsy

INRiM
ISTITUTO NAZIONALE
DI RICERCA METROLOGICA

Quantum Cryptography
QKD

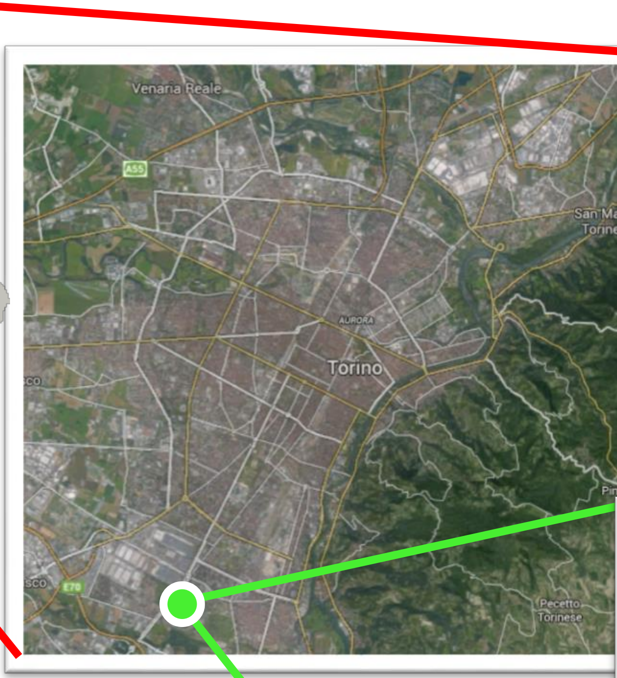
by

Ivo Pietro DEGIOVANNI

POLITECNICO
DI TORINO

Torino, 26th February 2019

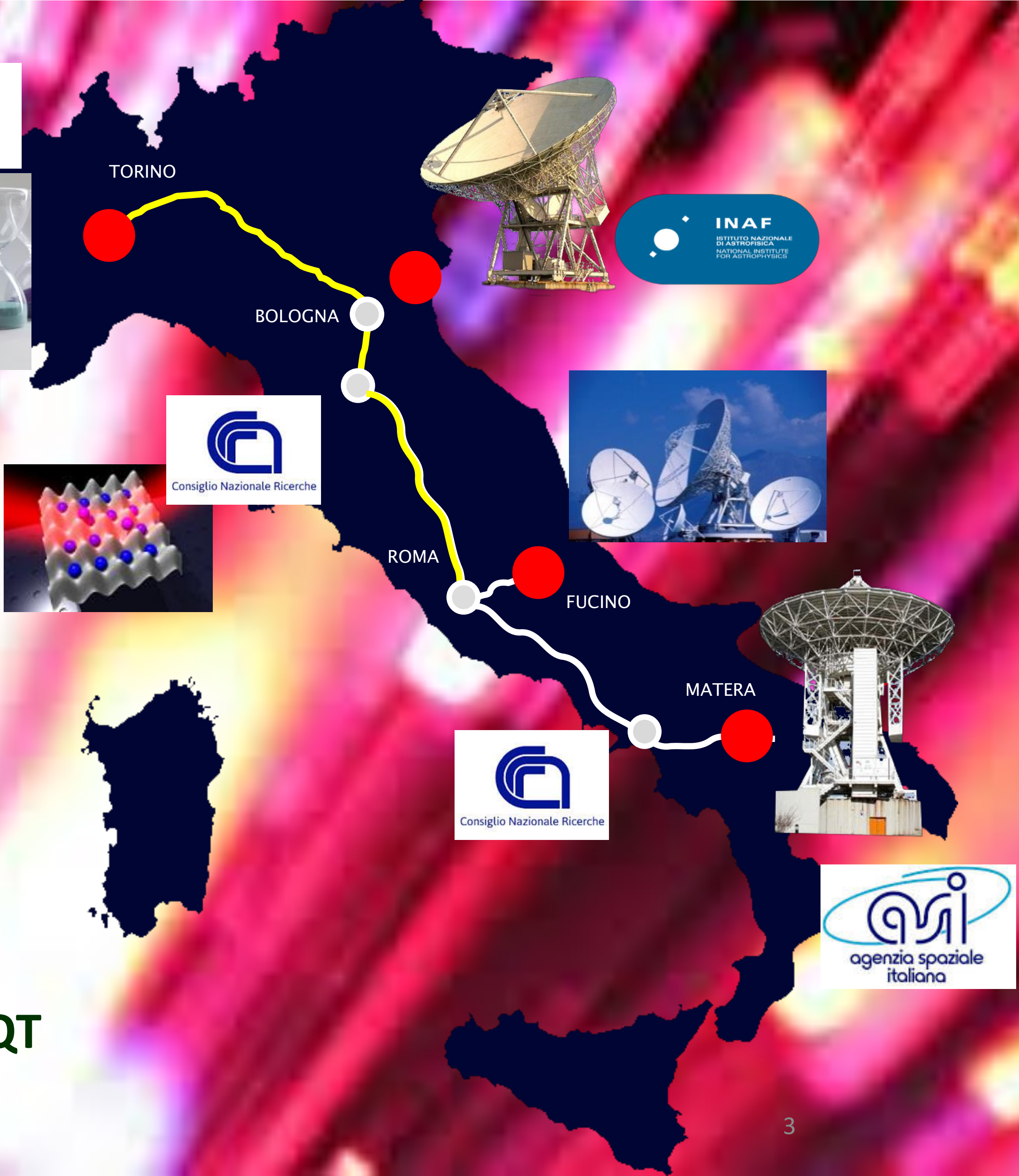
INRIM *in brief …*



INRiM
ISTITUTO NAZIONALE
DI RICERCA METROLOGICA

- Nat. Metrological Institute
- Campus 120.000 m^2
- ***IV*** NMI in Europe
- ***V*** Italian Research Body in Italy
- Strong links with Academia and Industries

INRiM
ISTITUTO NAZIONALE
DI RICERCA METROLOGICA


TORINO
INAF
ISTITUTO NAZIONALE DI ASTROFISICA
NATIONAL INSTITUTE FOR ASTROPHYSICS
BOLOGNA
Consiglio Nazionale Ricerche
ROMA
FUCINO
MATERA
Consiglio Nazionale Ricerche
agenzia spaziale italiana

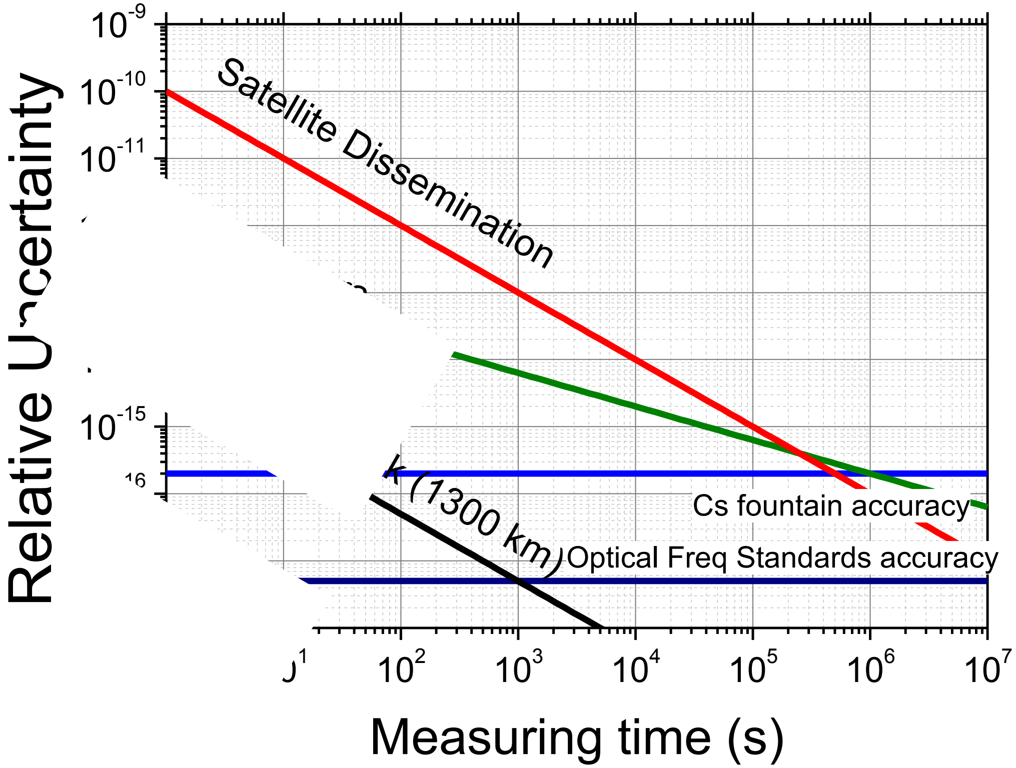
Italian Quantum Backbone

2000 km of fiber fof QT

INRiM
ISTITUTO NAZIONALE
DI RICERCA METROLOGICA

Quantum Clocks Network: the Italian Quantum Backbone

Quantum Clocks comparisons



T/F over fibre ensures the distribution of the best standards otherwise limited by the transfer method

Outline

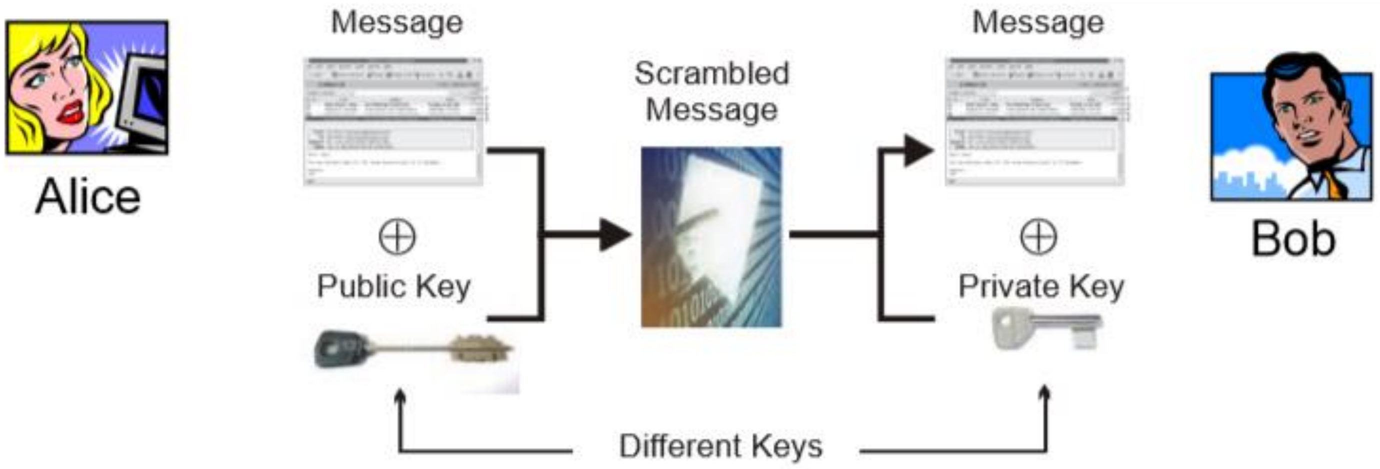
- Why?
- What?
- How?
- Who & Where?

Why … Quantum Cryptography is needed?

The increasing amount of data transmitted and stored raised the need of data security

Why … Quantum Cryptography is needed?

Today, the most sensitive data are hidden exploiting the techniques of "classical" cryptography



E.g. Public-Key Criptography

Why … Quantum Cryptography is needed?

Current Cryptography methods:

Asymmetric (Public-Key) – public Key for encripting, privaye key for decrypting (RSA-Rivest, Shamir, Adleman)

Symmetric – encrypting and decrypting key are identical (AES-Encryption Standard)

Why … Quantum Cryptography is needed?

Asymmetric (Public-Key) Cryptosystems

ALICE

Ciphertext

BOB

Public Key for encrypting

Private Key for decrypting

TRUSTED AUTHORITY *(to ensure the authenticity of the key)*

SECURITY LEVEL: Computational

Public-Key Cryptosystem (e.g. RSA-Rivest, Shamir, Adleman) relies on one-way function (easy to compute in one direction, (may be) "hard" its inversion)

Why … Quantum Cryptography is needed?

Symmetric Cryptosystems

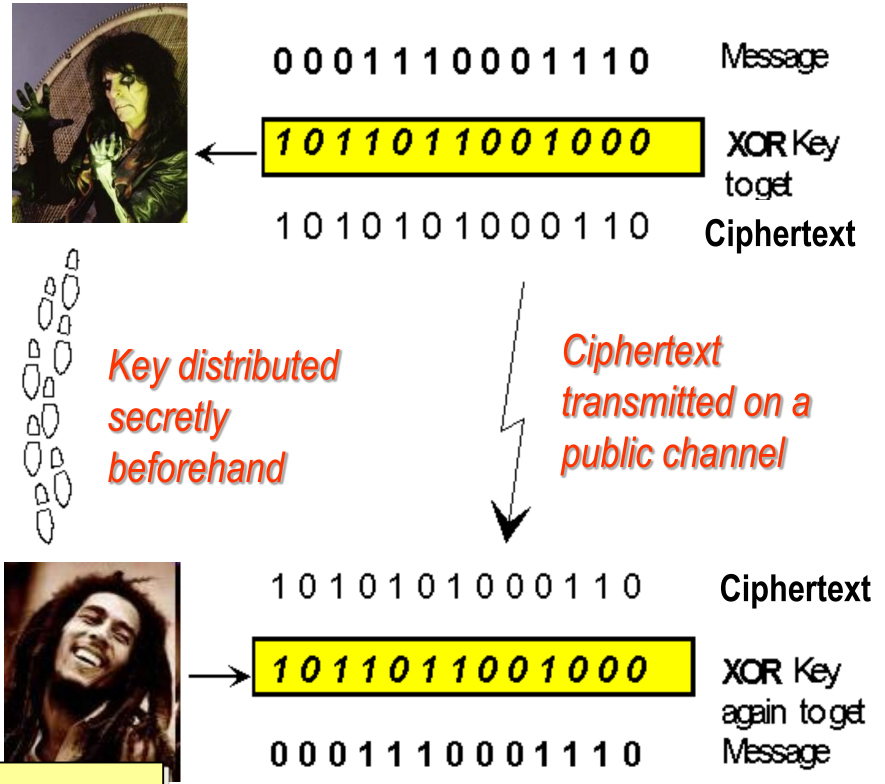
ONE-TIME PAD

Today is the only secure cryptosystem!

OTP allows unconditionally secure transmission over public channels once Alice and Bob share unconditionally secure secret Key (a random string of bits).

Key bits cannot be reused without compromising security of the system (the length of the key should equal the length of the message)

Same Key for encrypting and decrypting



0001110001110 Message

1011011001000 XOR Key to get

1010101000110 **Ciphertext**

Key distributed secretly beforehand

Ciphertext transmitted on a public channel

1010101000110 **Ciphertext**

1011011001000 XOR Key again to get Message

0001110001110 Message

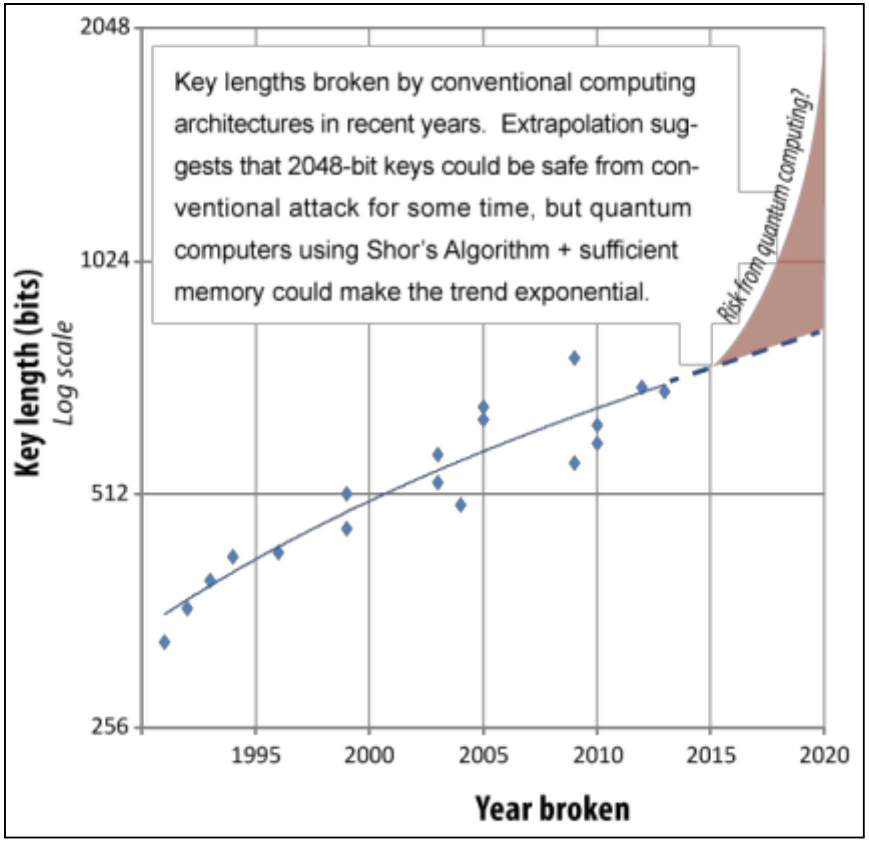
PROBLEM: Key Distribution

SOLUTION 1:
Trusted Couriers
SECURITY LEVEL:??

SOLUTION 2:
Classical Asymmetric Cryptosys.
(e.g. RSA)
SECURITY LEVEL:COMPUTATIONAL

SOLUTION 3: QKD
SECURITY LEVEL: UNCONDITIONAL [?]

Why … Quantum Cryptography is needed?



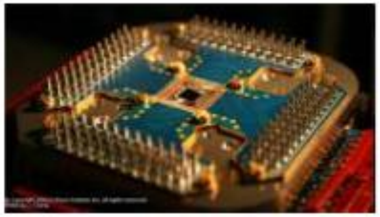
Key lengths broken by conventional computing architectures in recent years. Extrapolation suggests that 2048-bit keys could be safe from conventional attack for some time, but quantum computers using Shor's Algorithm + sufficient memory could make the trend exponential.

These techniques will become COMPLETELY NON-SECURE by more-powerful computer

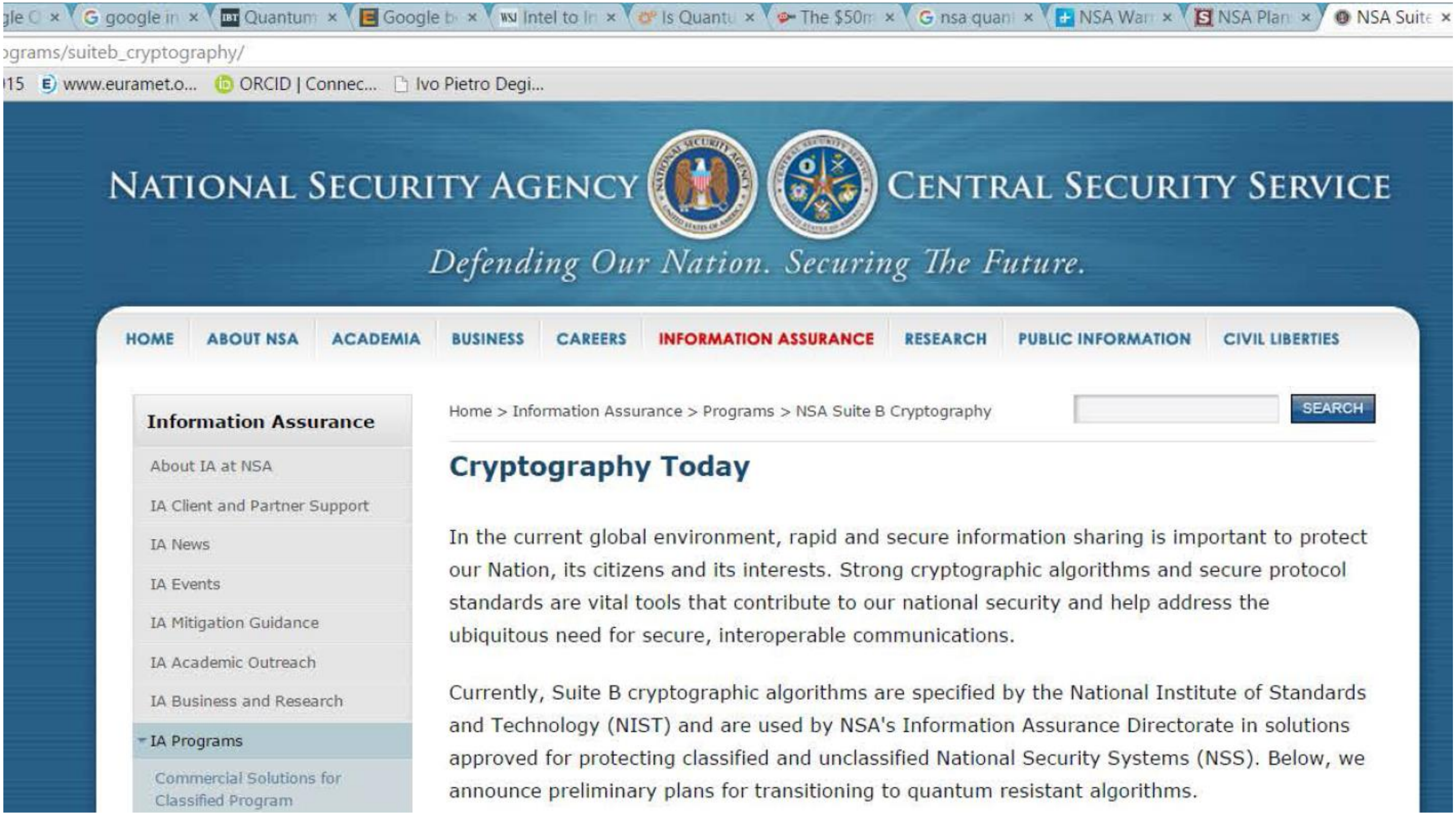
or by the realisation of a QUANTUM COMPUTER, or new mathematical/algorithmical findings.

Why … Quantum Cryptography is needed?

D:Wave
The Quantum Computing Company™



Why … Quantum Cryptography is needed?



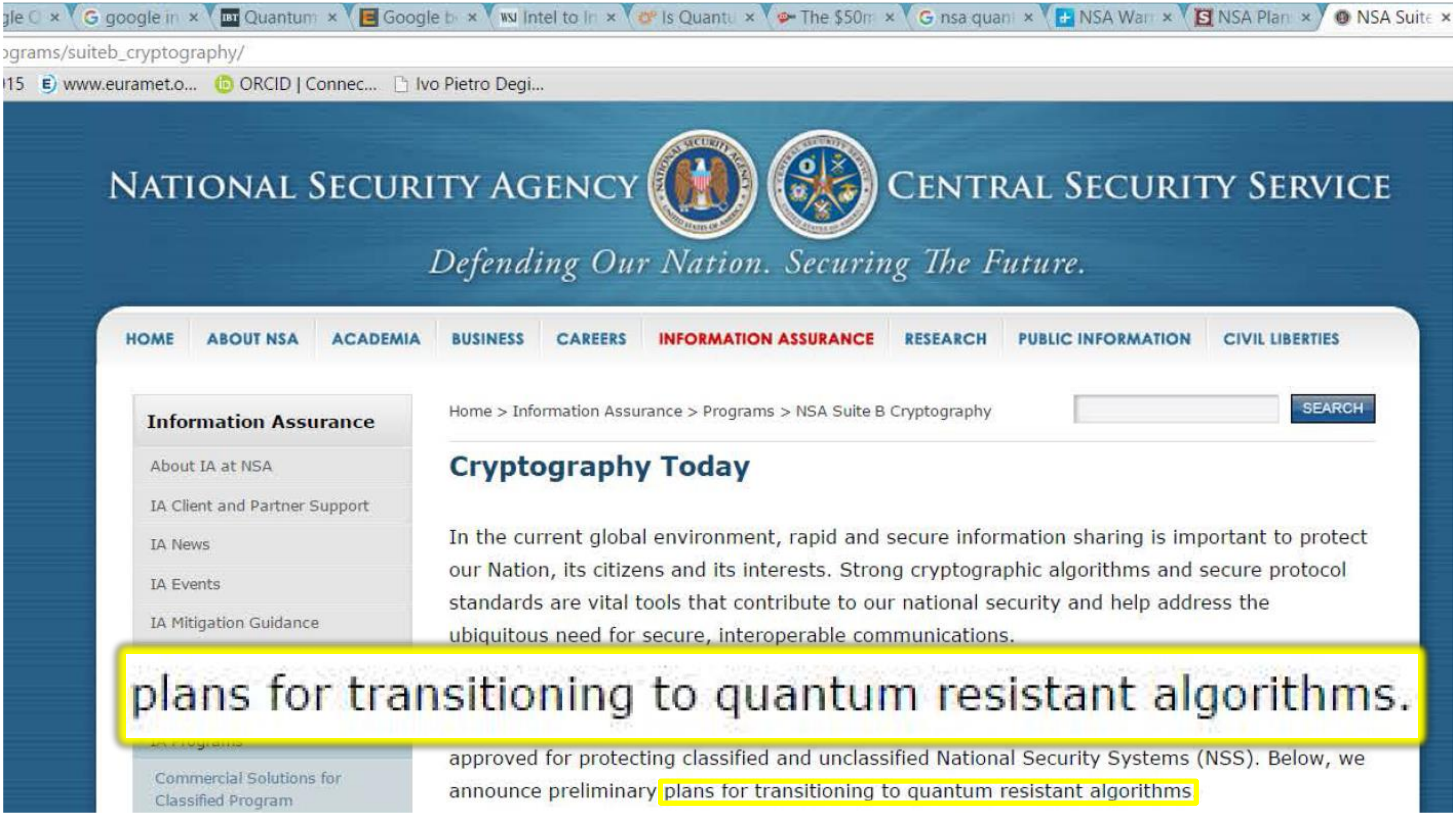
Home > Information Assurance > Programs > NSA Suite B Cryptography

Cryptography Today

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.

Currently, Suite B cryptographic algorithms are specified by the National Institute of Standards and Technology (NIST) and are used by NSA's Information Assurance Directorate in solutions approved for protecting classified and unclassified National Security Systems (NSS). Below, we announce preliminary plans for transitioning to quantum resistant algorithms.

Why … Quantum Cryptography is needed?



Home > Information Assurance > Programs > NSA Suite B Cryptography

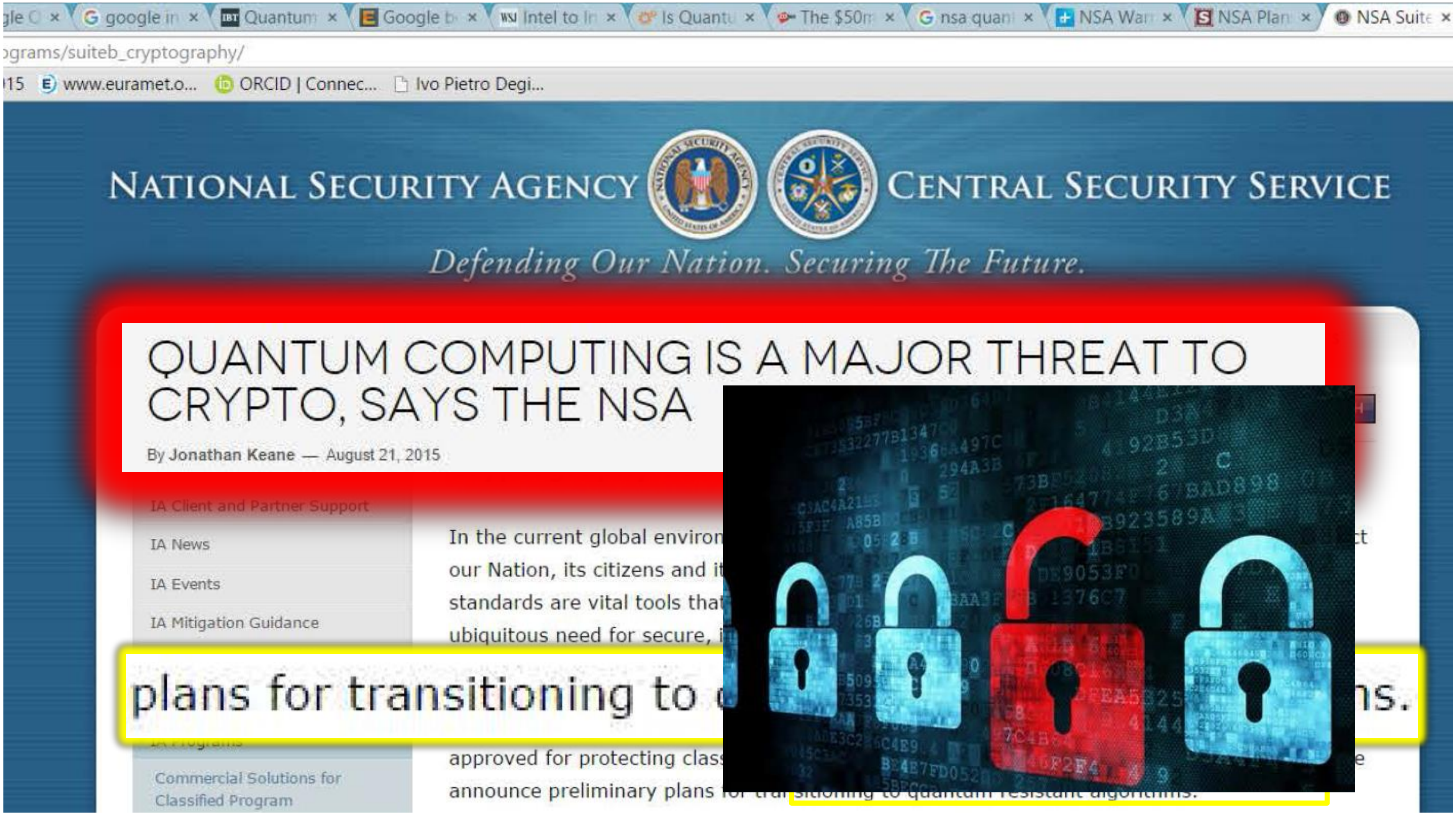
Cryptography Today

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.

plans for transitioning to quantum resistant algorithms.

approved for protecting classified and unclassified National Security Systems (NSS). Below, we announce preliminary plans for transitioning to quantum resistant algorithms.

Why … Quantum Cryptography is needed?



QUANTUM COMPUTING IS A MAJOR THREAT TO CRYPTO, SAYS THE NSA

By Jonathan Keane — August 21, 2015

IA Client and Partner Support

IA News

IA Events

IA Mitigation Guidance

IA Programs

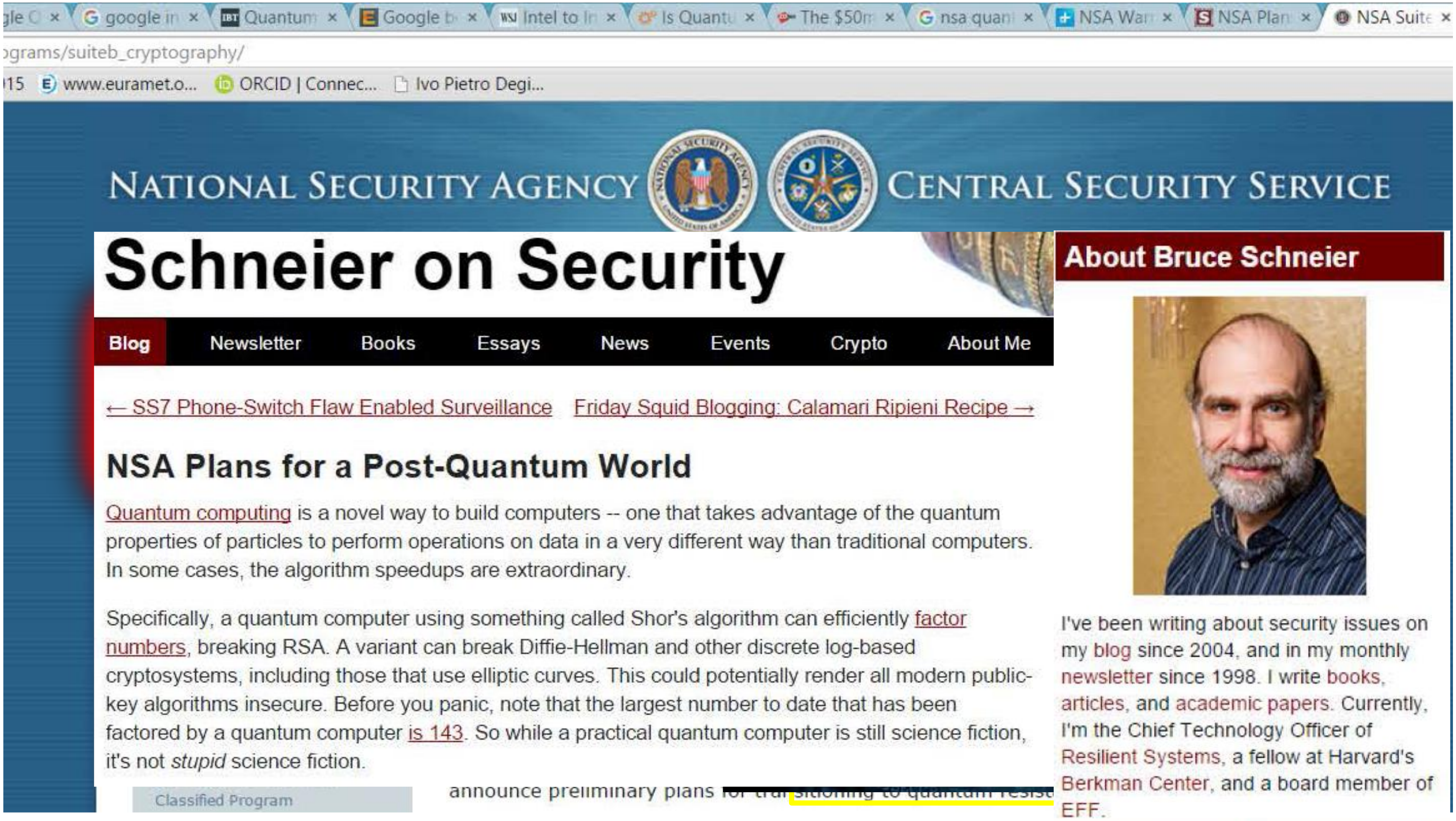
Commercial Solutions for Classified Program

In the current global environ… ct our Nation, its citizens and it… standards are vital tools that… ubiquitous need for secure, i…

plans for transitioning to c… ns.

… e approved for protecting class… announce preliminary plans for transitioning to quantum resistant algorithms.

Why … Quantum Cryptography is needed?



Schneier on Security

← SS7 Phone-Switch Flaw Enabled Surveillance   Friday Squid Blogging: Calamari Ripieni Recipe →

NSA Plans for a Post-Quantum World

Quantum computing is a novel way to build computers -- one that takes advantage of the quantum properties of particles to perform operations on data in a very different way than traditional computers. In some cases, the algorithm speedups are extraordinary.

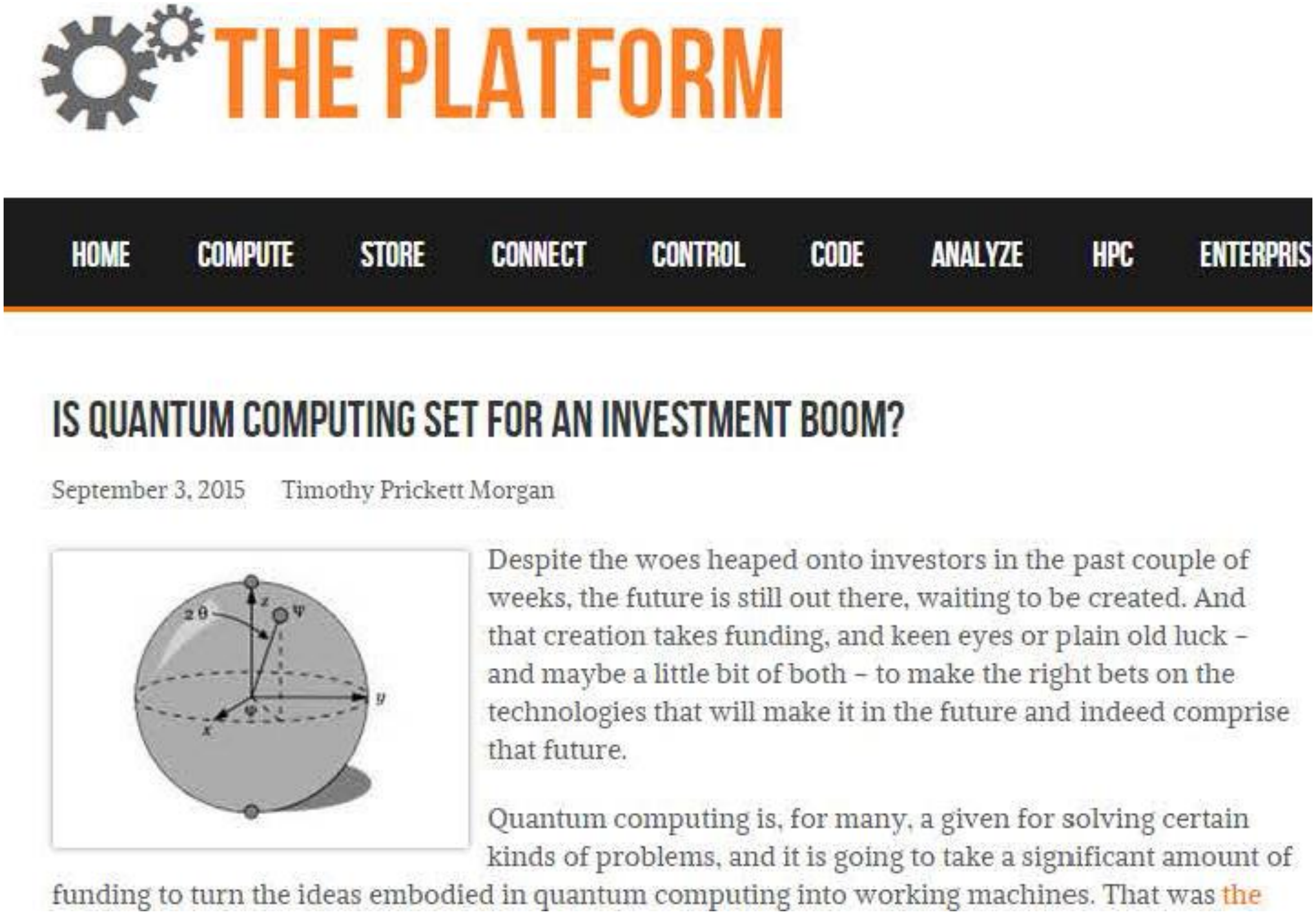
Specifically, a quantum computer using something called Shor's algorithm can efficiently factor numbers, breaking RSA. A variant can break Diffie-Hellman and other discrete log-based cryptosystems, including those that use elliptic curves. This could potentially render all modern public-key algorithms insecure. Before you panic, note that the largest number to date that has been factored by a quantum computer is 143. So while a practical quantum computer is still science fiction, it's not *stupid* science fiction.

announce preliminary plans for transitioning to quantum resist

About Bruce Schneier

I've been writing about security issues on my blog since 2004, and in my monthly newsletter since 1998. I write books, articles, and academic papers. Currently, I'm the Chief Technology Officer of Resilient Systems, a fellow at Harvard's Berkman Center, and a board member of EFF.

Why … Quantum Cryptography is needed?



THE PLATFORM

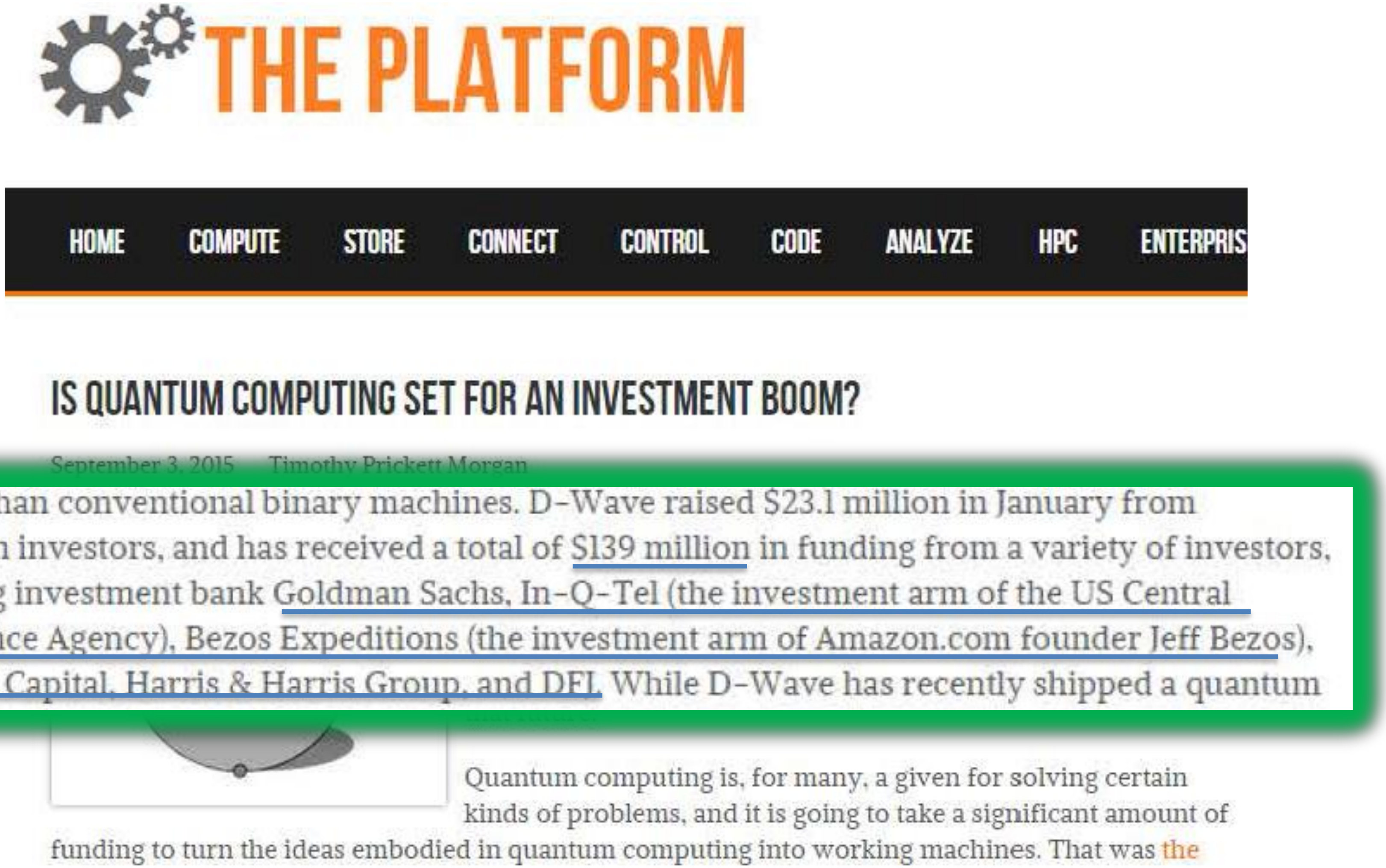
IS QUANTUM COMPUTING SET FOR AN INVESTMENT BOOM?

September 3, 2015 Timothy Prickett Morgan

Despite the woes heaped onto investors in the past couple of weeks, the future is still out there, waiting to be created. And that creation takes funding, and keen eyes or plain old luck – and maybe a little bit of both – to make the right bets on the technologies that will make it in the future and indeed comprise that future.

Quantum computing is, for many, a given for solving certain kinds of problems, and it is going to take a significant amount of funding to turn the ideas embodied in quantum computing into working machines. That was the

Why … Quantum Cryptography is needed?



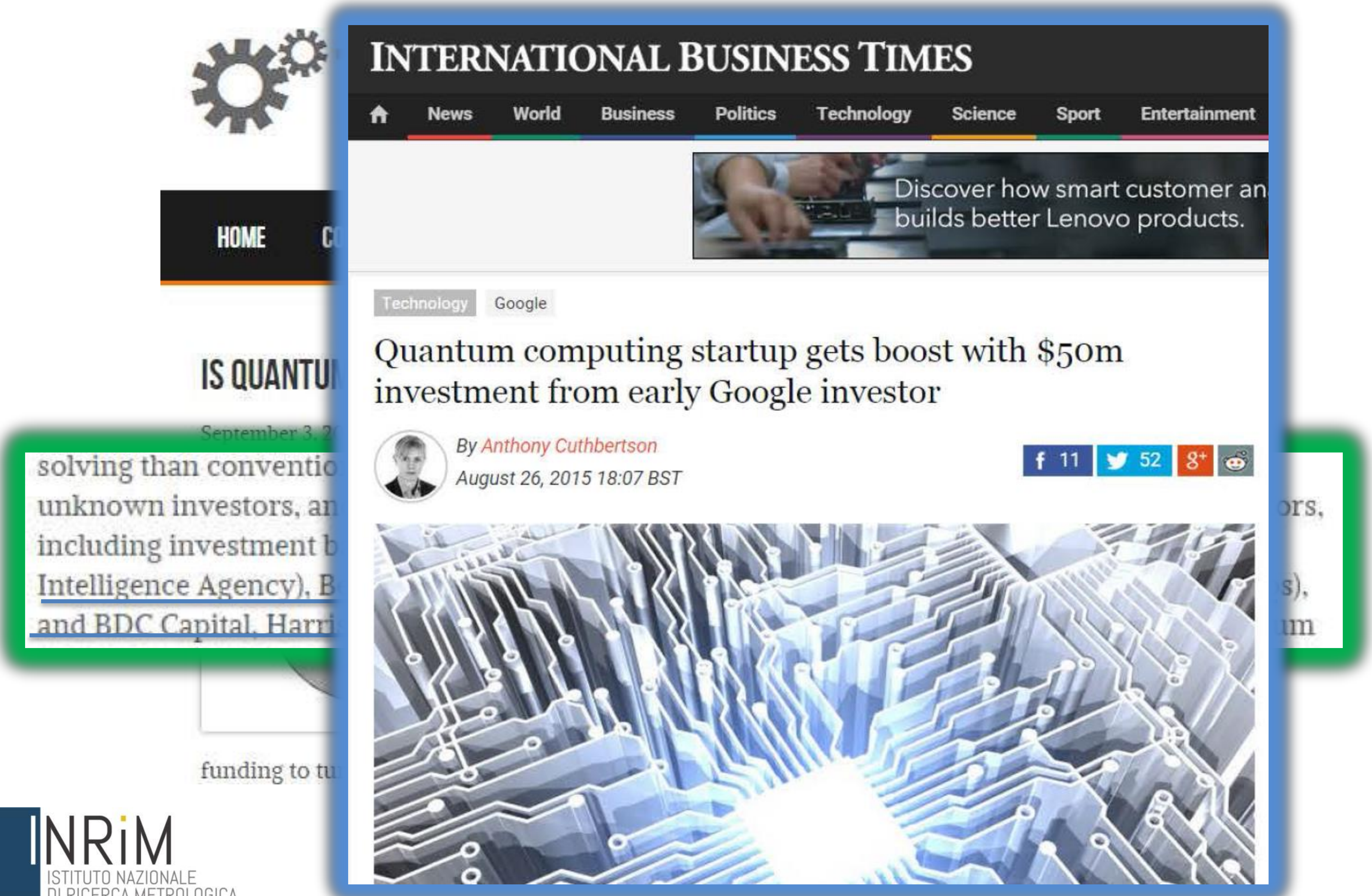
IS QUANTUM COMPUTING SET FOR AN INVESTMENT BOOM?

September 3, 2015 Timothy Prickett Morgan

solving than conventional binary machines. D-Wave raised $23.1 million in January from unknown investors, and has received a total of $139 million in funding from a variety of investors, including investment bank Goldman Sachs, In-Q-Tel (the investment arm of the US Central Intelligence Agency), Bezos Expeditions (the investment arm of Amazon.com founder Jeff Bezos), and BDC Capital, Harris & Harris Group, and DFJ. While D-Wave has recently shipped a quantum

Quantum computing is, for many, a given for solving certain kinds of problems, and it is going to take a significant amount of funding to turn the ideas embodied in quantum computing into working machines. That was the

Why … Quantum Cryptography is needed?



IS QUANTU

September 3, 2

solving than conventio

unknown investors, an … ors,

including investment b

Intelligence Agency), B … s),

and BDC Capital, Harri … um

funding to tu

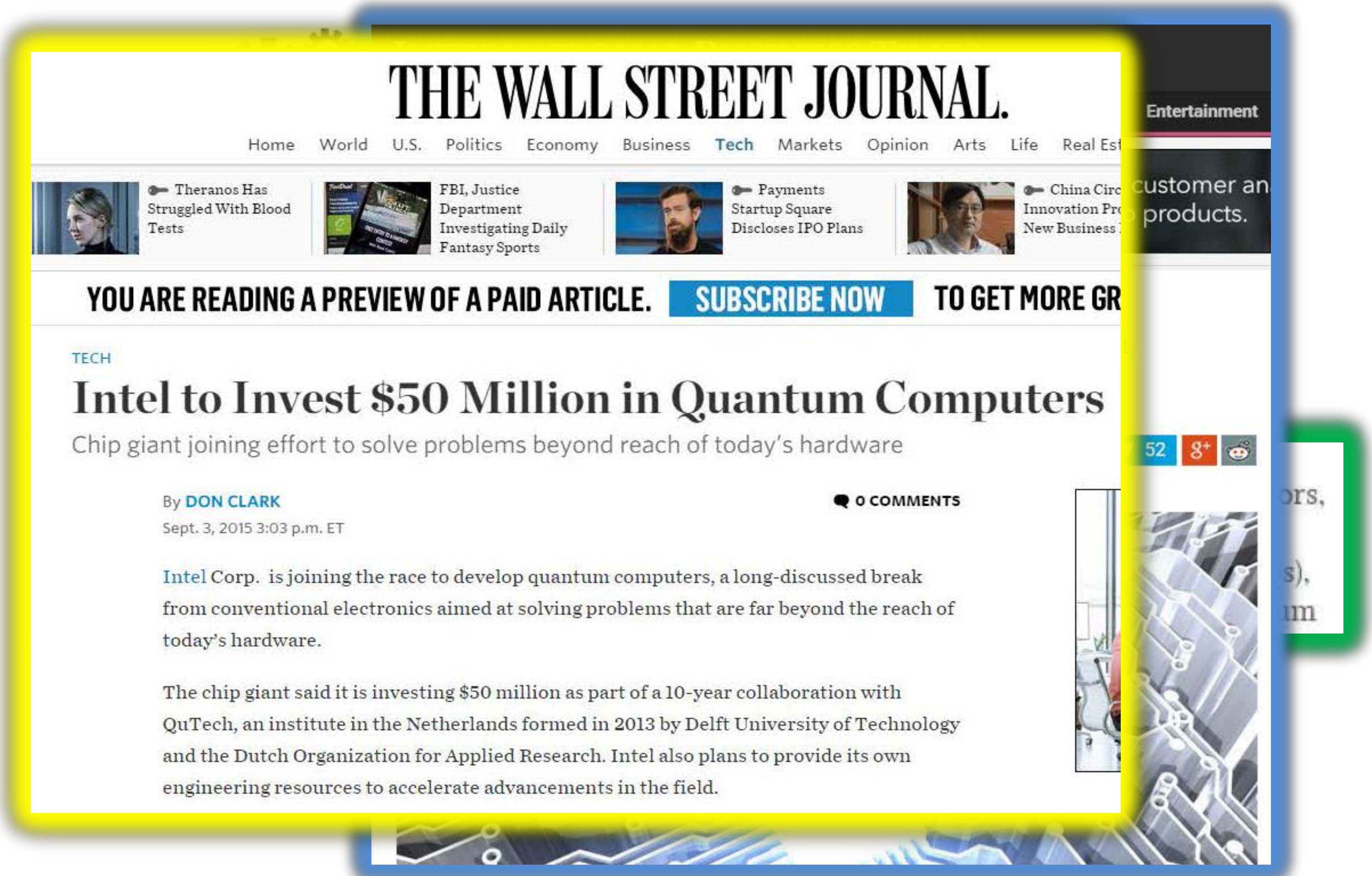
INTERNATIONAL BUSINESS TIMES

Quantum computing startup gets boost with $50m investment from early Google investor

By Anthony Cuthbertson

August 26, 2015 18:07 BST

Why … Quantum Cryptography is needed?



THE WALL STREET JOURNAL.

Theranos Has Struggled With Blood Tests

FBI, Justice Department Investigating Daily Fantasy Sports

Payments Startup Square Discloses IPO Plans

China Circ Innovation Pr New Business

YOU ARE READING A PREVIEW OF A PAID ARTICLE. SUBSCRIBE NOW TO GET MORE GR

TECH

Intel to Invest $50 Million in Quantum Computers

Chip giant joining effort to solve problems beyond reach of today's hardware

By DON CLARK

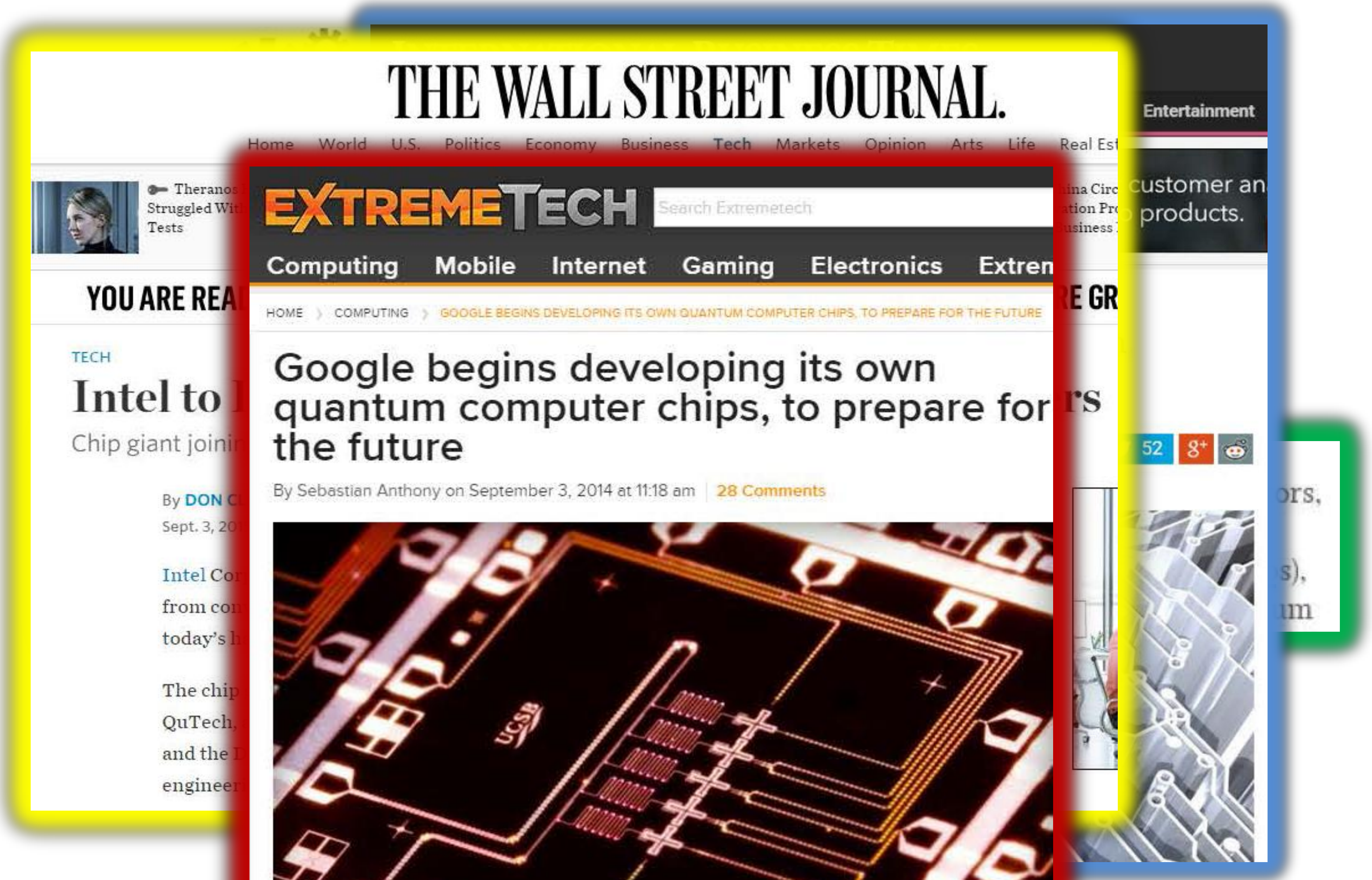
0 COMMENTS

Sept. 3, 2015 3:03 p.m. ET

Intel Corp. is joining the race to develop quantum computers, a long-discussed break from conventional electronics aimed at solving problems that are far beyond the reach of today's hardware.

The chip giant said it is investing $50 million as part of a 10-year collaboration with QuTech, an institute in the Netherlands formed in 2013 by Delft University of Technology and the Dutch Organization for Applied Research. Intel also plans to provide its own engineering resources to accelerate advancements in the field.

Why … Quantum Cryptography is needed?



THE WALL STREET JOURNAL.

Home World U.S. Politics Economy Business Tech Markets Opinion Arts Life Real Est

Theranos Struggled Wit Tests

ina Circ ation Pro usiness

YOU ARE REA

E GR

TECH

Intel to

rs

Chip giant joinin

By DON C

Sept. 3, 20

Intel Cor from con today's h

The chip QuTech, and the I engineer

Entertainment

customer an products.

52

ors,

s),

m

EXTREMETECH

Search Extremetech

Computing Mobile Internet Gaming Electronics Extrem

HOME › COMPUTING › GOOGLE BEGINS DEVELOPING ITS OWN QUANTUM COMPUTER CHIPS, TO PREPARE FOR THE FUTURE

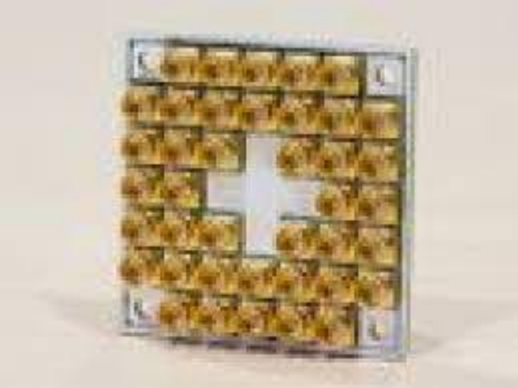
Google begins developing its own quantum computer chips, to prepare for the future

By Sebastian Anthony on September 3, 2014 at 11:18 am | 28 Comments

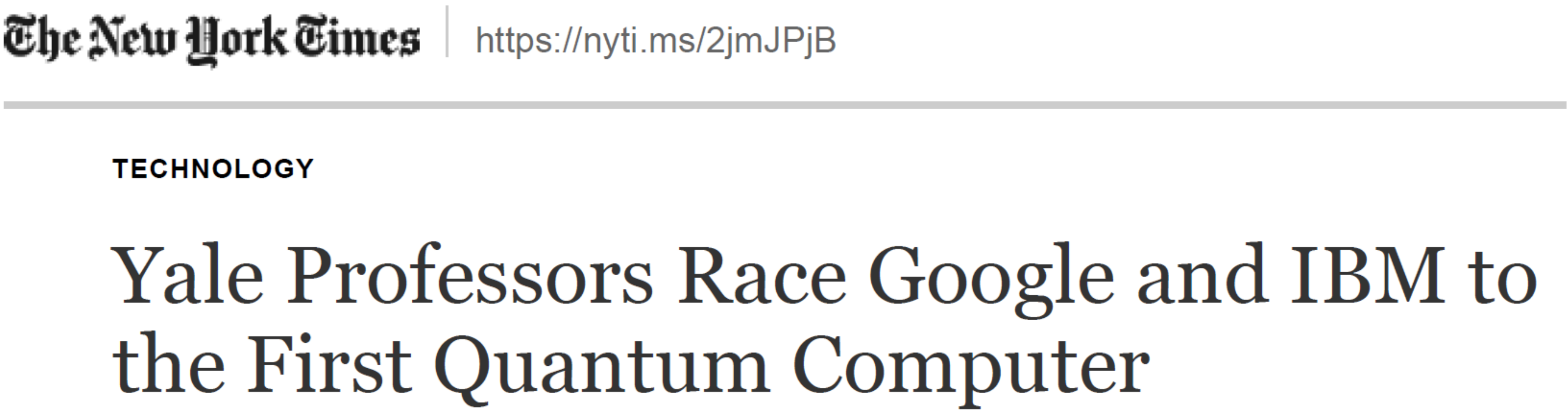
Why … Quantum Cryptography is needed?

The Guardian

The Guardian view on quantum computing: the new space race



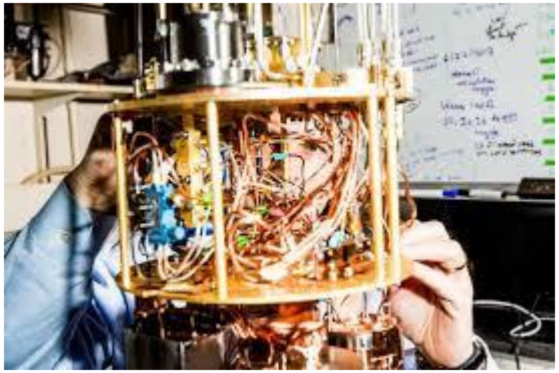
Why … Quantum Cryptography is needed?

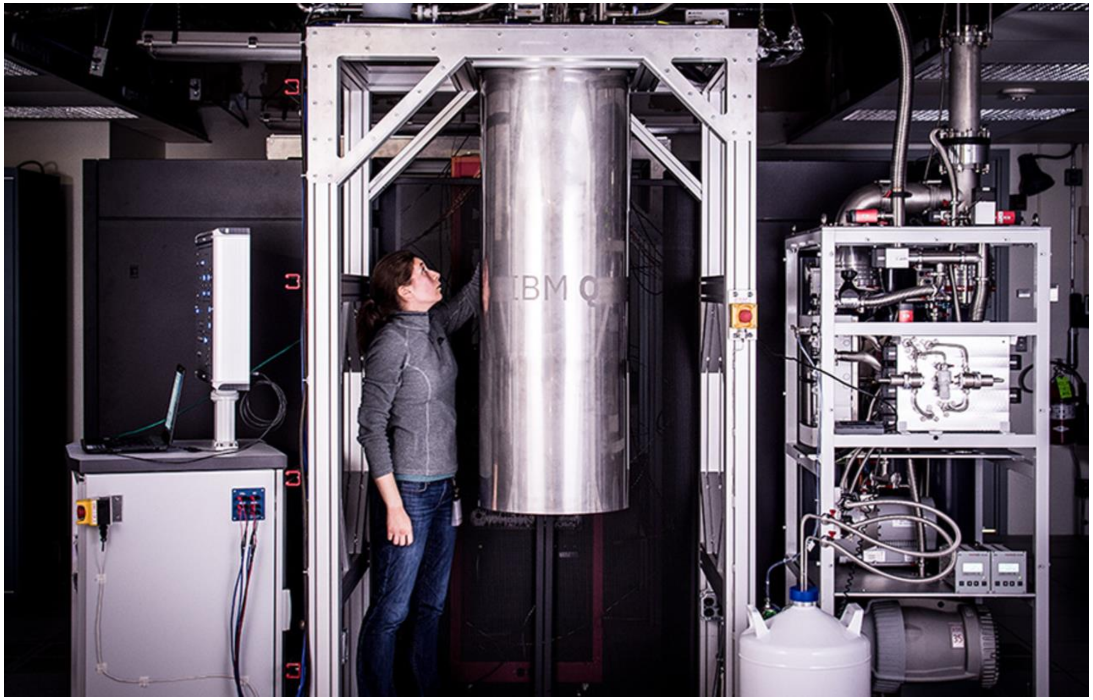


The New York Times | https://nyti.ms/2jmJPjB

TECHNOLOGY

Yale Professors Race Google and IBM to the First Quantum Computer





Why … Quantum Cryptography is needed?

49-qubit quantum computer presented by Intel

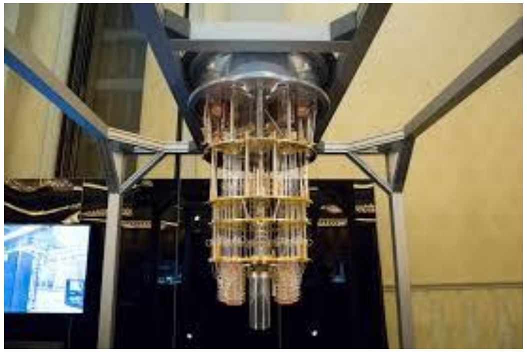
Japan unveils first quantum computer as race for faster machines heats up

Russians Lead the Quantum Computer Race With 51-Qubit Machine

Baidu has entered the race to build quantum computers

The Chinese tech giant lags its peers in quantum computing but hopes to incorporate the technology into its business in the next five years.

Why … Quantum Cryptography is needed?



FT FINANCIAL TIMES

Microsoft and Google prepare for big leaps in quantum computing

Companies set to give big boost to potentially revolutionary technology

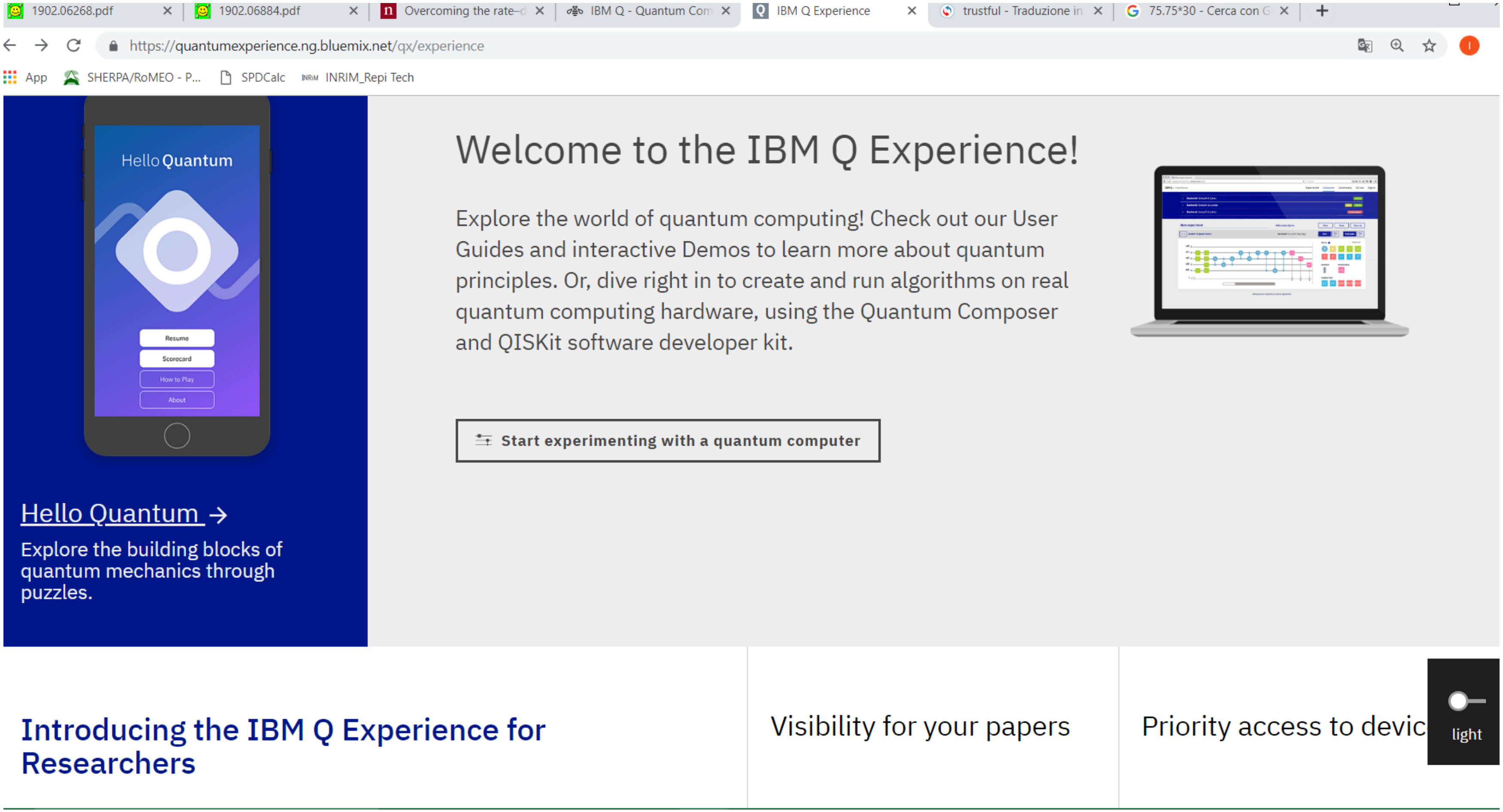
Google's New 72-Qubit Processor Could Help Quantum Computing Go Mainstream

HOW'S YOUR QUANTUM COMPUTER PROTOTYPE COMING ALONG?
GREAT!
THE PROJECT EXISTS IN A SIMULTANEOUS STATE OF BEING BOTH TOTALLY SUCCESSFUL AND NOT EVEN STARTED.
Dilbert.com DilbertCartoonist@gmail.com

Computing with Quantum Physics

A faster, cheaper path to exascale

Why … Quantum Cryptography is needed?



1902.06268.pdf | 1902.06884.pdf | Overcoming the rate-d | IBM Q - Quantum Com | IBM Q Experience | trustful - Traduzione in | 75.75*30 - Cerca con G

https://quantumexperience.ng.bluemix.net/qx/experience

App | SHERPA/RoMEO - P... | SPDCalc | INRIM_Repi Tech

Hello Quantum

Resume

Scorecard

How to Play

About

Hello Quantum →

Explore the building blocks of quantum mechanics through puzzles.

Welcome to the IBM Q Experience!

Explore the world of quantum computing! Check out our User Guides and interactive Demos to learn more about quantum principles. Or, dive right in to create and run algorithms on real quantum computing hardware, using the Quantum Composer and QISKit software developer kit.

Start experimenting with a quantum computer

Introducing the IBM Q Experience for Researchers

Visibility for your papers

Priority access to devic

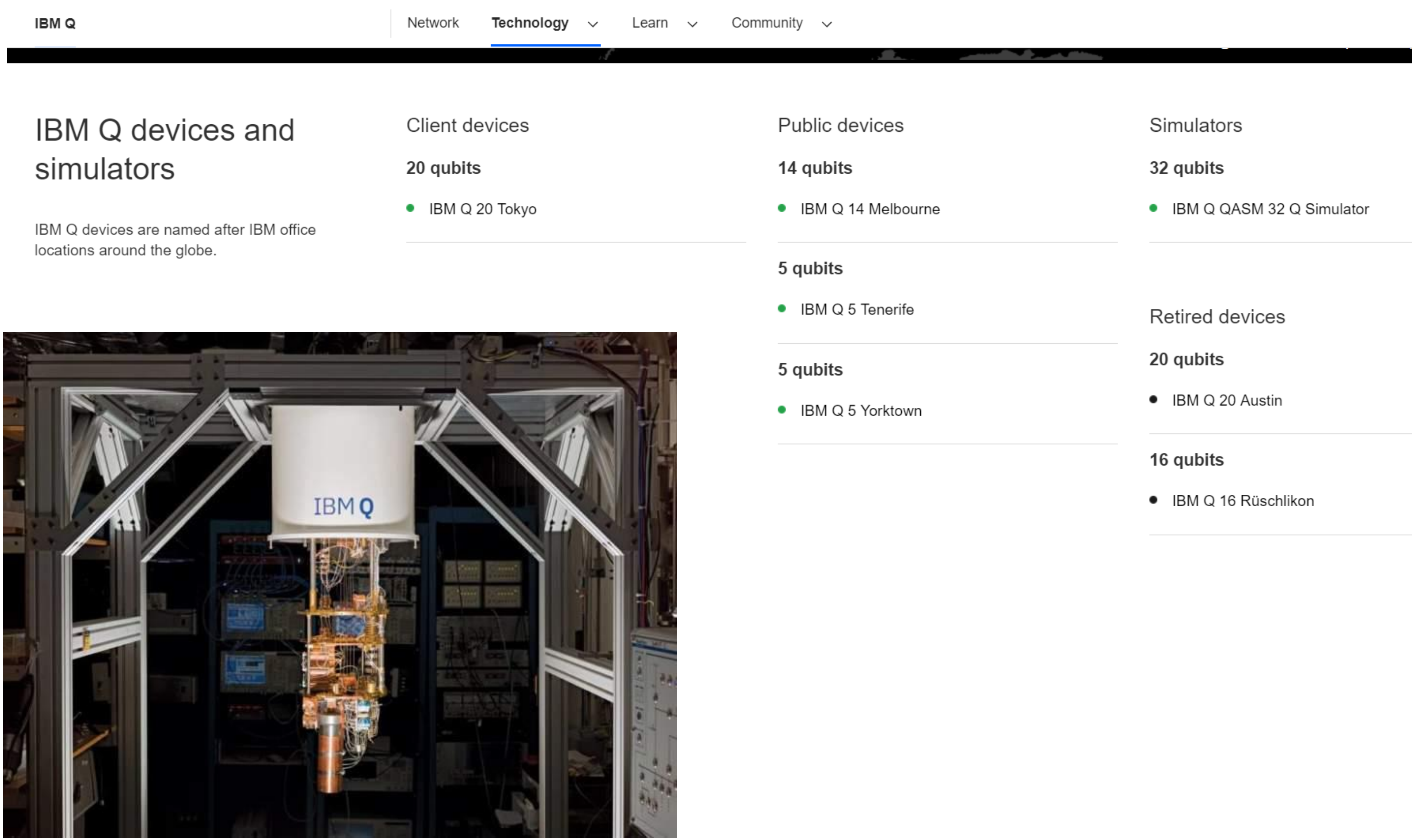
light

https://quantumexperience.ng.bluemix.net/qx/experience

https://www.research.ibm.com/ibm-q/

INRiM ISTITUTO NAZIONALE DI RICERCA METROLOGICA

Why … Quantum Cryptography is needed?



IBM Q

Network Technology Learn Community

IBM Q devices and simulators

IBM Q devices are named after IBM office locations around the globe.

Client devices

20 qubits

- IBM Q 20 Tokyo

Public devices

14 qubits

- IBM Q 14 Melbourne

5 qubits

- IBM Q 5 Tenerife

5 qubits

- IBM Q 5 Yorktown

Simulators

32 qubits

- IBM Q QASM 32 Q Simulator

Retired devices

20 qubits

- IBM Q 20 Austin

16 qubits

- IBM Q 16 Rüschlikon

https://www.research.ibm.com/ibm-q/

Why … Quantum Cryptography is needed?

The UK National Quantum Technologies Programme

£270M

UK Government investment in quantum technologies research

- To exploit the potential of quantum science and develop a range of emerging technologies with the potential to benefit the UK.
- A multi-stakeholder, technology-focused initiative to last for an initial period of five years.

EPSRC Pioneering research and skills

Technology Strategy Board Driving Innovation

[dstl]

NPL National Physical Laboratory

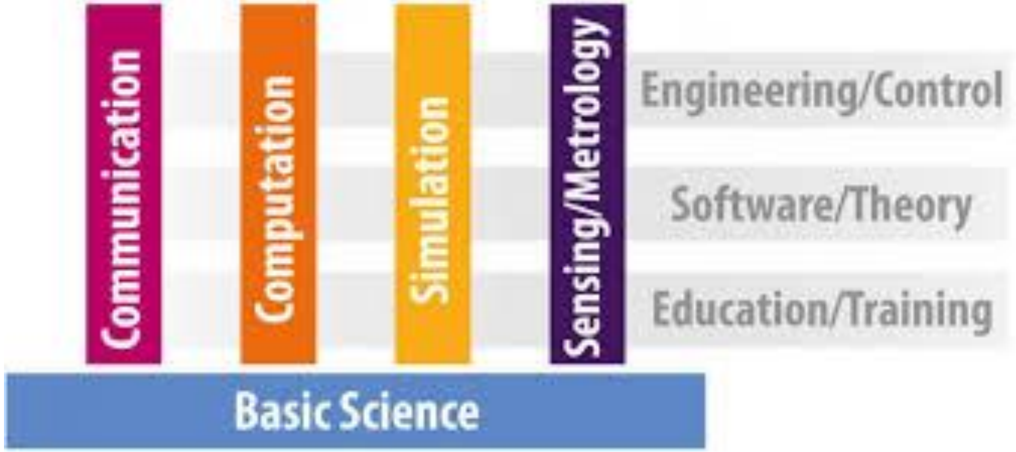
CESG

Department for Business Innovation & Skills

Why … Quantum Cryptography is needed?

European Commission launched €1 billion quantum technologies flagship

European Commission



INRIM
ISTITUTO NAZIONALE
DI RICERCA METROLOGICA

What … is Quantum Cryptography?

Cryptography is the art of rendering a message unintelligible to **any unauthorized** party

An algorithm -a Cipher- combines the message with some additional information –the Key- producing a cyphertext. The system is secure if the cyphertext can be unlocked only by the Key

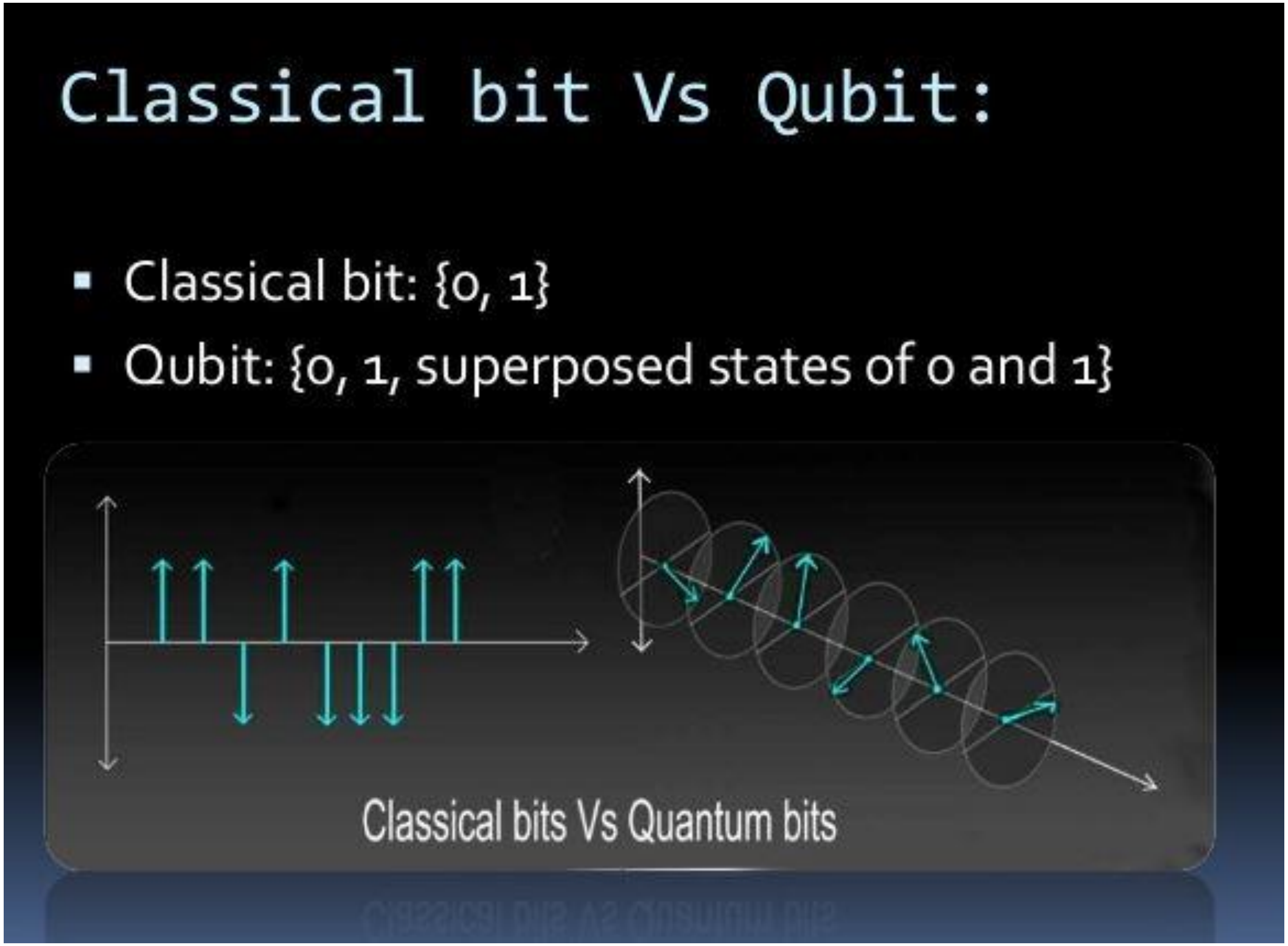
Quantum Mechanics is counterintuitive and bizarre

The Non-Cloning Theorem (Heisenberg Uncertainty principle) does ***not*** *allows us to clone (discriminate) non-orthogonal states with certainty (and without disturbing the measured system).*

Quantum Cryptography (QKD) is able to distributed unconditionally secure Keys by means of single quantum systems

QM does not prevent eavesdropping, it only allows the detection of the presence of an eavesdropper, as this presence induces differences in the generated Keys. Unconditional secure Keys are established once Alice and Bob constantly monitor the security of the quantum communication channel

What … is Quantum Cryptography?



Classical bit Vs Qubit:

- Classical bit: {0, 1}
- Qubit: {0, 1, superposed states of 0 and 1}

Classical bits Vs Quantum bits

What … is Quantum Cryptography?

No-Cloning theorem

Schrodinger Eq. → **Unitary Evolution** $\widehat{U}$ $\qquad \widehat{U}\widehat{U}^\dagger = I$

Q-Cloner: $\widehat{U}|\psi\rangle|b\rangle|M\rangle = |\psi\rangle|\psi\rangle|M_\psi\rangle$

Case $|0\rangle$ $\qquad \widehat{U}|0\rangle|b\rangle|M\rangle = |0\rangle|0\rangle|M_0\rangle$

Case $|1\rangle$ $\qquad \widehat{U}|1\rangle|b\rangle|M\rangle = |1\rangle|1\rangle|M_1\rangle$

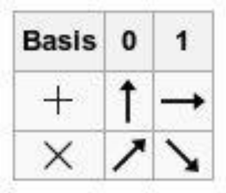
Case $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$

$$\widehat{U}|\psi\rangle|b\rangle|M\rangle = \alpha\widehat{U}|0\rangle|b\rangle|M\rangle + \beta\widehat{U}|1\rangle|b\rangle|M\rangle = \alpha|0\rangle|0\rangle|M_0\rangle + \beta|1\rangle|\rangle|M_1\rangle$$

$$\neq |\psi\rangle|\psi\rangle|M_\psi\rangle$$

How … does Quantum Cryptography work?

BB84 protocol [Charles H. Bennett and Gilles Brassard (1984)]

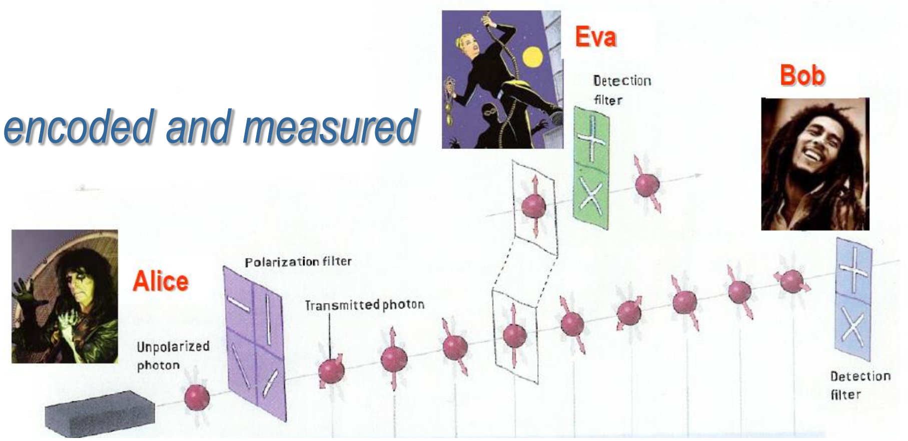


Basis	0	1
+	↑	→
×	↗	↘

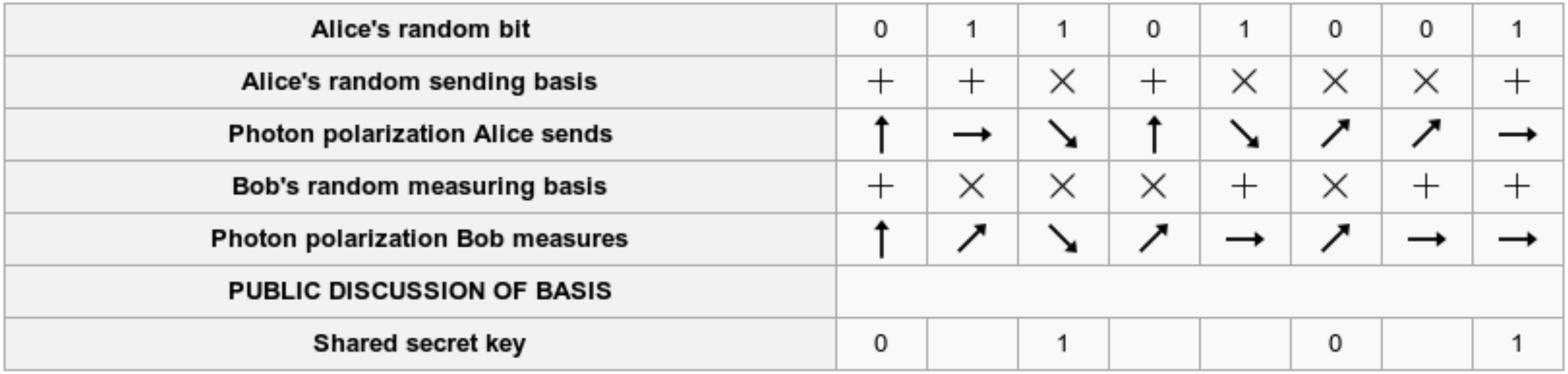
Step 1: *Alice sends Bob a string of polarization encoded photon*

Step 2 : *Bob measures the string of encoded photons using random bases (rectilinear or diagonal).*

Step 3 : *Alice and Bob publicly compare the bases they encoded and measured in, and discard all results where they do not match.*



The result is the Shared Secret Key

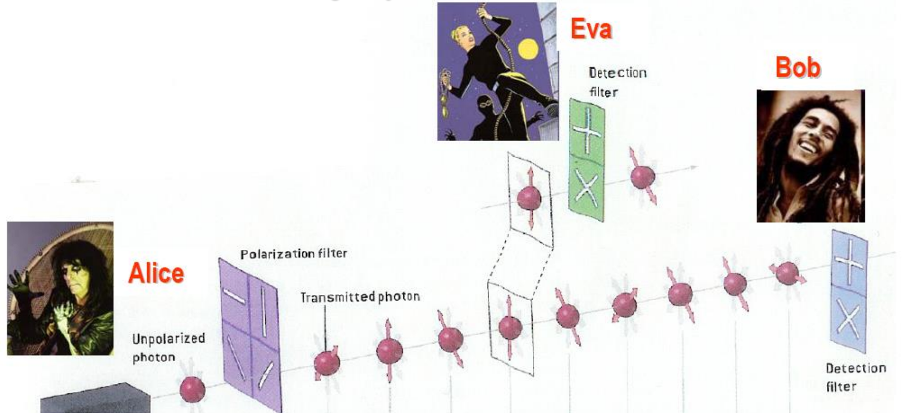


Alice's random bit	0	1	1	0	1	0	0	1
Alice's random sending basis	+	+	×	+	×	×	×	+
Photon polarization Alice sends	↑	→	↘	↑	↘	↗	↗	→
Bob's random measuring basis	+	×	×	×	+	×	+	+
Photon polarization Bob measures	↑	↗	↘	↗	→	↗	→	→
PUBLIC DISCUSSION OF BASIS								
Shared secret key	0		1			0		1

How … does Quantum Cryptography work?

Eavesdropping Detection

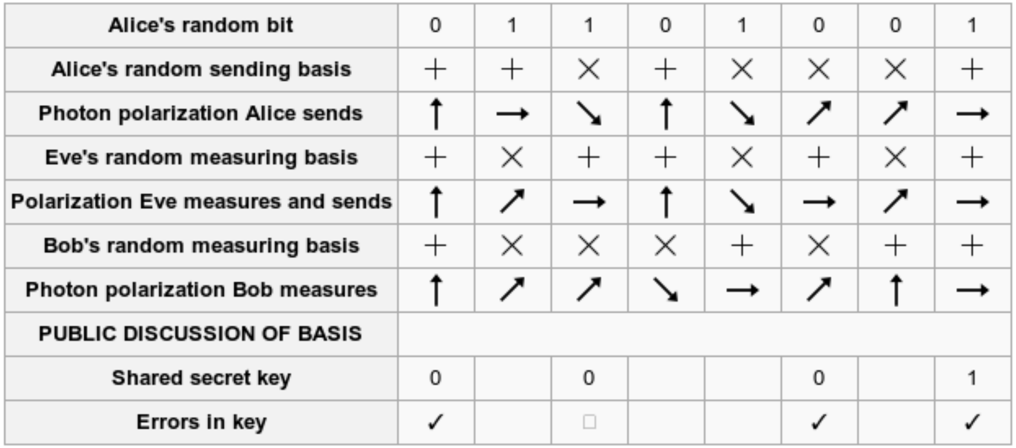
If Eva tries to gain information about the photons polarization, the laws of quantum physics dictates that the quantum state of the photons are altered, thus causing errors in Bob's measurements.
Alice and Bob compare a subset of the shared Key. If the *QBER* (*$QBER=N_{wrong}/N_{key}$*) violates a certain threshold, the Key distribution process is aborted and repeated.



Example: *Intercept – Resend Attack*

Eva duplicates the Bob measurement system

- *Eva receives Alice's encoded photon. If she guesses the base correctly, then she just has to encode a new photon and send it on to Bob.*
- *If Eve guesses incorrectly, she will just generate a new randomly encoded photon to send to Bob.*
- *Therefore, the probability an intercepted photon generates an error in the key string is 0.5 X 0.5 = 0.25*



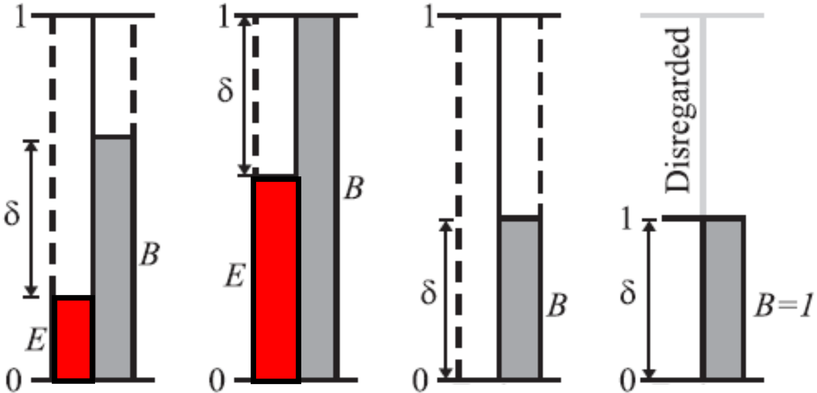
Alice's random bit	0	1	1	0	1	0	0	1
Alice's random sending basis	+	+	×	+	×	×	×	+
Photon polarization Alice sends	↑	→	↘	↑	↘	↗	↗	→
Eve's random measuring basis	+	×	+	+	×	+	×	+
Polarization Eve measures and sends	↑	↗	→	↑	↘	→	↗	→
Bob's random measuring basis	+	×	×	×	+	×	+	+
Photon polarization Bob measures	↑	↗	↗	↘	→	↗	↑	→
PUBLIC DISCUSSION OF BASIS								
Shared secret key	0		0			0		1
Errors in key	✓		□			✓		✓

How … does Quantum Cryptography work?

Eavesdropping Detection

PROBLEM: *shared Key contains Errors due to:*

- *Eva*
- *Real-world devices imperfections*



Shared Key

Error Correction

E=0
Privacy Ampl.

E=0
Secret Key

It is necessary to:

- *Correct errors in the key* → *Error Correction Protocols*
- *Nullify Eva's information on the Key* → *Privacy Amplification, Advantage Distillation …*

QBER < 0.12 → Alice and Bob can distill a unconditionally secure Key

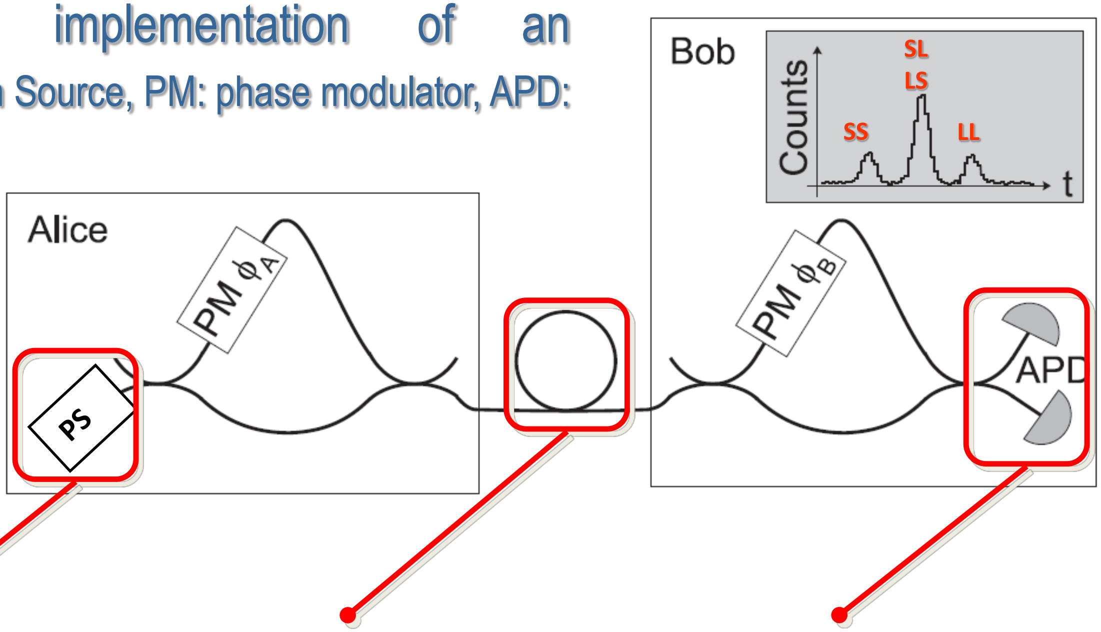
How … does Quantum Cryptography work?

Real World Implementations

- *Open-Air QKD* (aiming to: Ground-Satellite, Satellite-Satellite QKD)
- *Optical Fiber-based QKD*

Double asymmetric Mach-Zehnder implementation of an interferometric system for QKD (PS: photon Source, PM: phase modulator, APD: avalanche photodiode).

Temporal count distribution recorded as a function of the time passed since the emission of the pulse by Alice. Interference is observed in the central peak (LS-SL) when the phase modulations are properly selected.



Technological Challenges: ***PHOTON SOURCES*** ***QUANTUM CHANNES*** ***SINGLE-PHOTON DETECTORS***

How … does Quantum Cryptography work?

QUANTUM CHANNELS: Single-Mode fibers @ Telecom Wavelength

Adv.s: Lower attenuation

Disv.s: Decoherence (***Geometric phase, Birefringence, PMD, Chromatic Dispersion***)

PHOTON SOURCES: Faint Laser Pulses

Adv.s: Coupling Efficiency, Bandwidth, Costs

Disv.s: Poissonian Statistics (***Nonzero probability of having more than one photon per pulse***)

(**Alternatives:** *Heralded Single-PS based on PDC, Quantum Dots, Impurities in Diamond, …*)

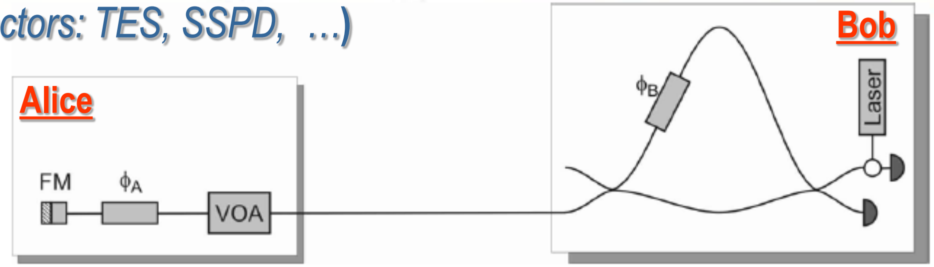
PHOTON DETECTORS: APD operating in Geiger mode

Adv.s: , Room Temperature Operation

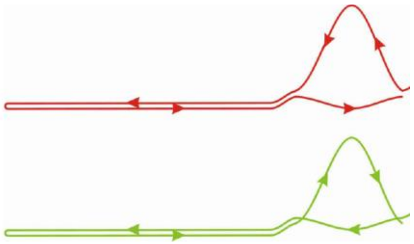
Disv.s: Dark counts (***Gated mode***), On/Off Detection

(**Alternatives:** *Superconducting Detectors: TES, SSPD, …*)

Real World QKD



The two interfering paths



QKD in the Real World

Who … is selling QKD devices?

IDQ
FROM VISION TO TECHNOLOGY

MagiQ

quintessencelabs

SK telecom

国盾量子
QuantumCTek

Who … has research program on QKD?

TOSHIBA
Leading Innovation >>>

HUAWEI

SELEX
Sistemi Integrati
A Finmeccanica Company

swisscom

THALES

Telcordia.

MITSUBISHI
ELECTRIC
Changes for the Better

hp
invent

NTT

NEC Empowered by Innovation

Telefonica

…

Who … is using QKD devices?

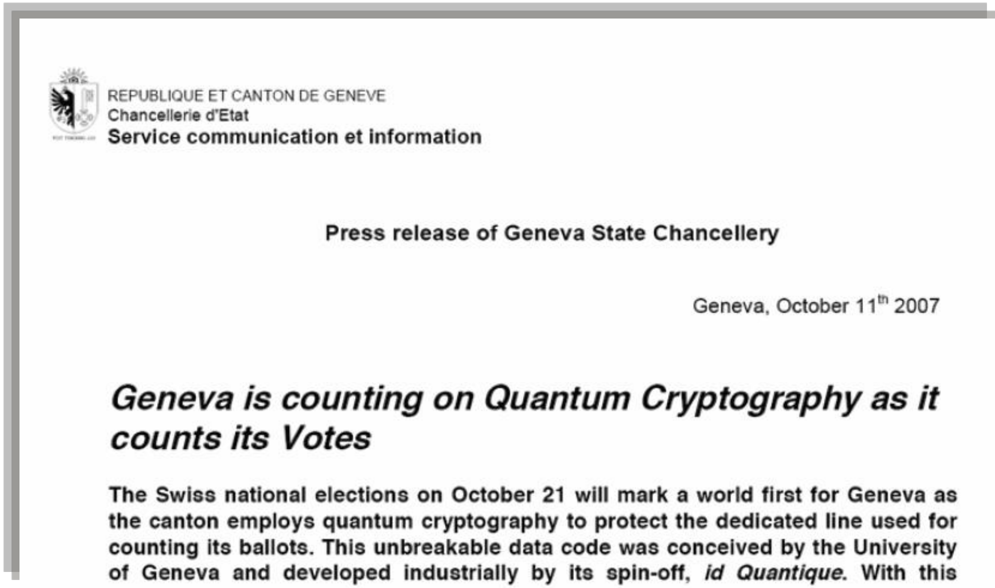
***2004** - World's first bank transfer using QKD*

***2004** - DARPA QKD Network in Massachusetts*

***2006** - QKD used in Geneva for Swiss elections*

***2008** - World's first computer network protected by QKD in Vienna*

"Some Computer System Officer are convinced by QKD. … QKD already protects well established banks and indistries!!!" **(N. Gisin, ETSI Workshop, 22/6/2010)**



REPUBLIQUE ET CANTON DE GENEVE
Chancellerie d'Etat
Service communication et information

Press release of Geneva State Chancellery

Geneva, October 11th 2007

Geneva is counting on Quantum Cryptography as it counts its Votes

The Swiss national elections on October 21 will mark a world first for Geneva as the canton employs quantum cryptography to protect the dedicated line used for counting its ballots. This unbreakable data code was conceived by the University of Geneva and developed industrially by its spin-off, *id Quantique*. With this

Who … is using QKD devices?

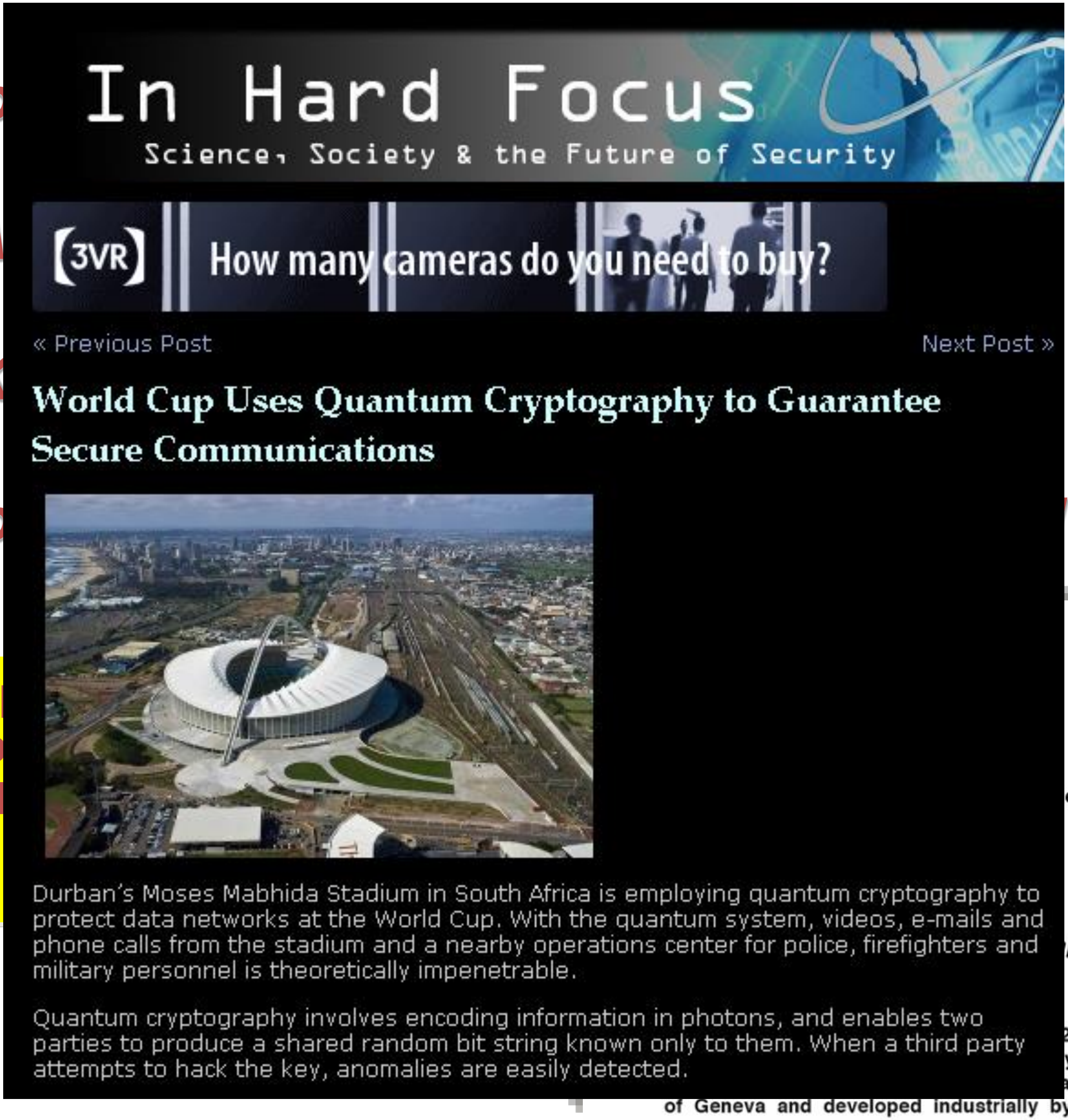
2004 - Wo

2004 - DA

2006 - QK

2008 - Wo … **by QKD in Vienna**

“Some Com
convinced b
protects wel
indistries!!!”
22/6/2010)



In Hard Focus

Science, Society & the Future of Security

« Previous Post   Next Post »

World Cup Uses Quantum Cryptography to Guarantee Secure Communications

Durban’s Moses Mabhida Stadium in South Africa is employing quantum cryptography to protect data networks at the World Cup. With the quantum system, videos, e-mails and phone calls from the stadium and a nearby operations center for police, firefighters and military personnel is theoretically impenetrable.

Quantum cryptography involves encoding information in photons, and enables two parties to produce a shared random bit string known only to them. When a third party attempts to hack the key, anomalies are easily detected.

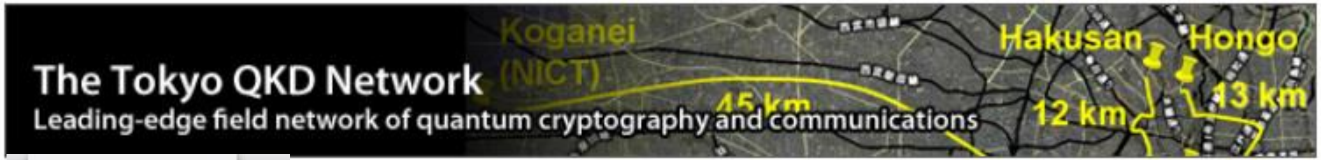
eva State Chancellery

Geneva, October 11th 2007

ntum Cryptography as it

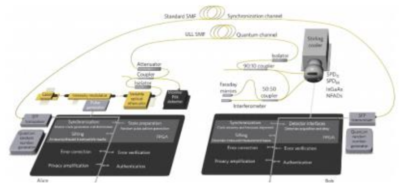
21 will mark a world first for Geneva as
y to protect the dedicated line used for
a code was conceived by the University
of Geneva and developed industrially by its spin-off, *id Quantique*. With this

Who … is building QKD infrastructures?



The Tokyo QKD Network

Leading-edge field network of quantum cryptography and communications



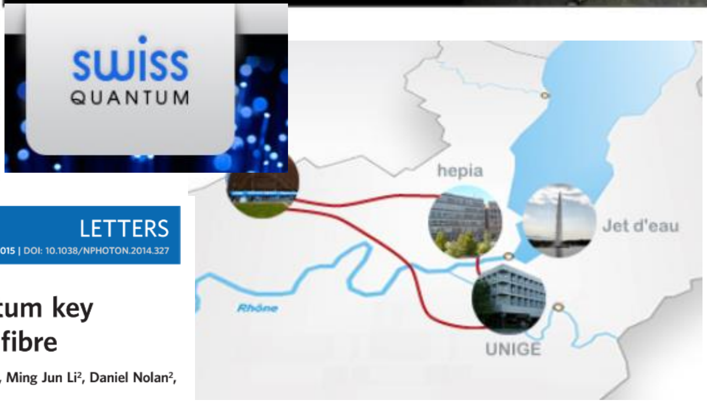
nature photonics

LETTERS

PUBLISHED ONLINE: 9 FEBRUARY 2015 | DOI: 10.1038/NPHOTON.2014.327

Provably secure and practical quantum key distribution over 307 km of optical fibre

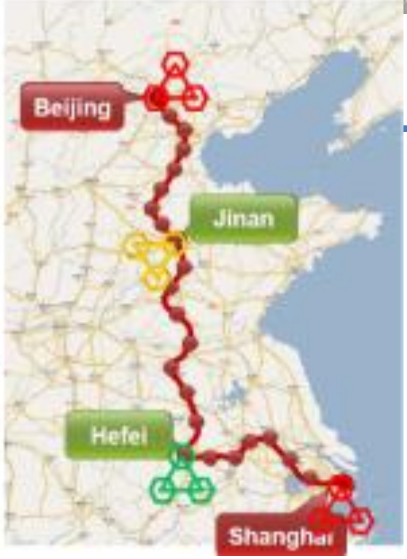
Boris Korzh[1]*, Charles Ci Wen Lim[1]*, Raphael Houlmann[1], Nicolas Gisin[1], Ming Jun Li[2], Daniel Nolan[2], Bruno Sanguinetti[1], Rob Thew[1] and Hugo Zbinden[1]



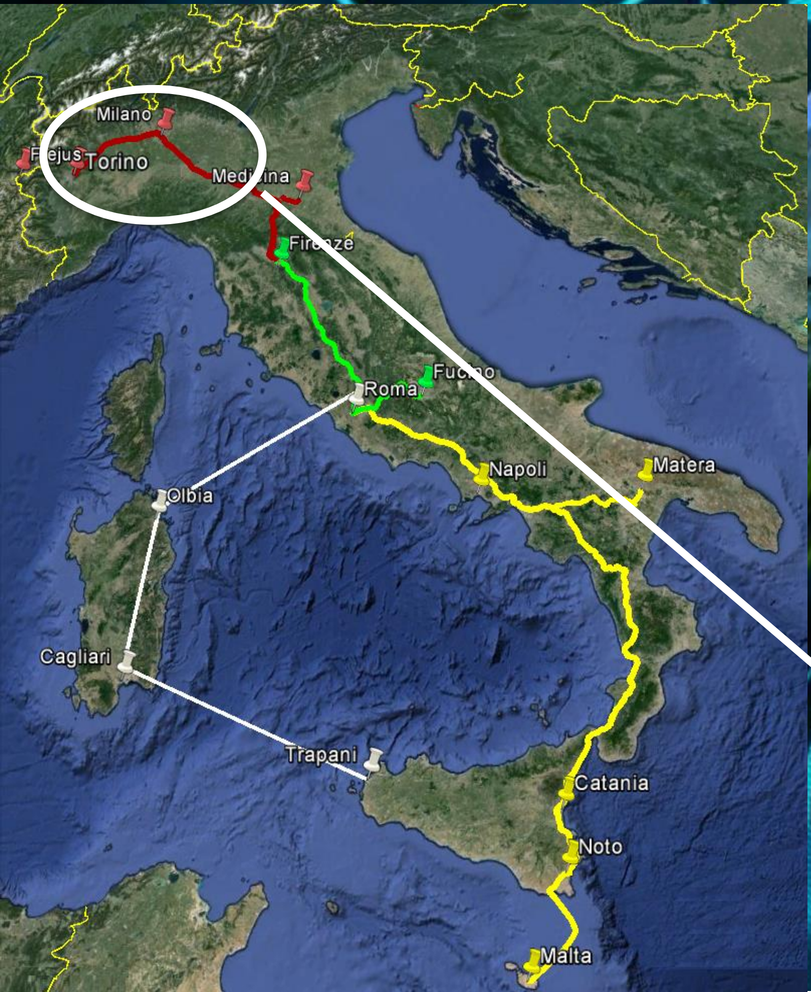
VIENNA
SIE
QBE
SECOQC
ERD
GUD
BREIT
St Pölten
Google

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



The Italian Quantum Backbone: QKD

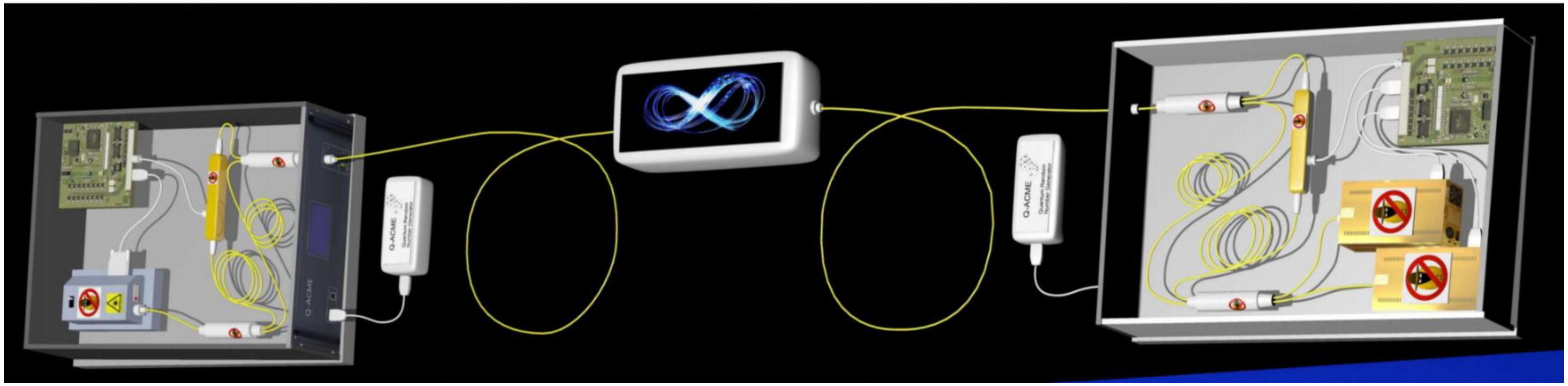


First tests of coexistence in the same I-QB fibre infrastructure of QTD and QKD.

Quantum Metrology for Q-Techies

An Industry Specification Group (ISG) of the European Telecommunications Standards Institute (ETSI) has been installed from October 2008 to address standardization issues in QKD, to support the commercialization of QKD devices on various levels and stages.

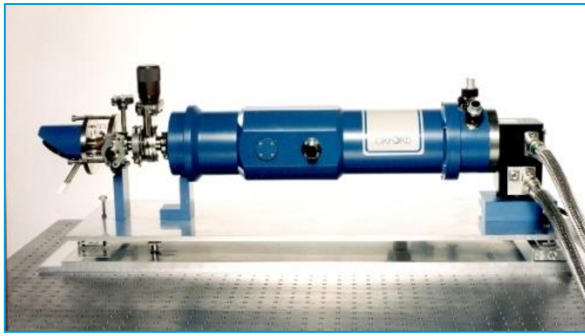
Quantum Radiometry is **necessary** to the standardization framework for providing traceable characterization techniques at single-photon level.

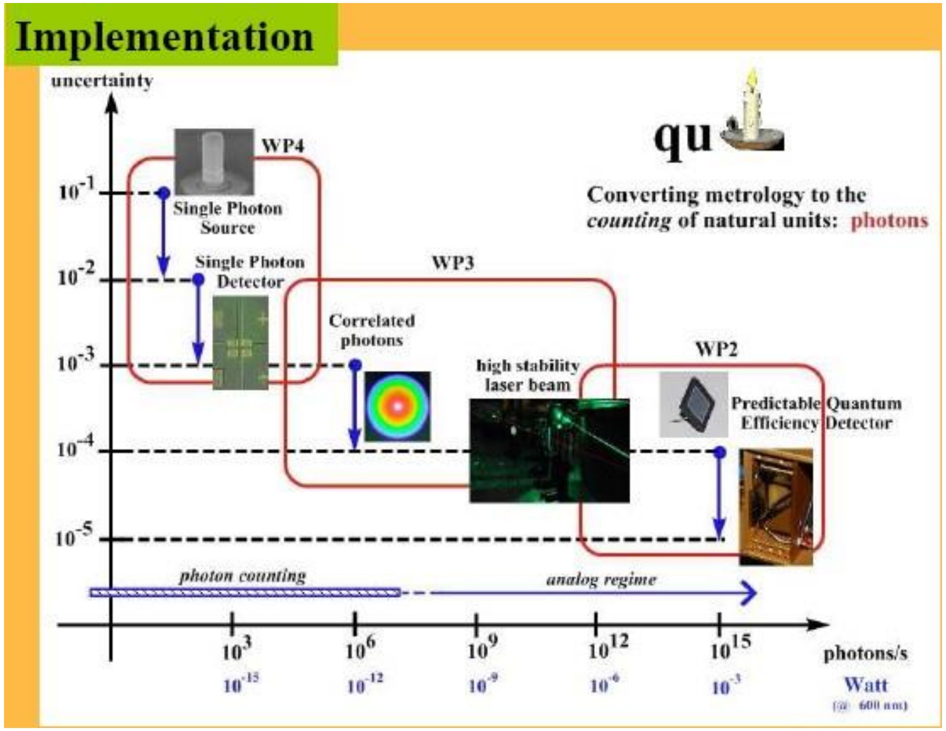


Quantum Metrology for Q-Techies

Quantum Radiometry: Effort to create a linkage between the typical optical power measurement regime of conventional radiometry and the single-photon counting regime

Le Système international d'unités
The International System of Units
SI





NPL National Physical Laboratory

PTB

CMI

INRiM ISTITUTO NAZIONALE DI RICERCA METROLOGICA

MIKES

Justervesenet

METROSERT

EURAMET European Association of National Metrology Institutes

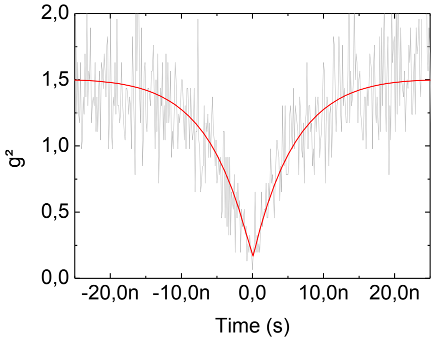
iMERA PLUS

EMRP European Metrology Research Programme
Programme of EURAMET

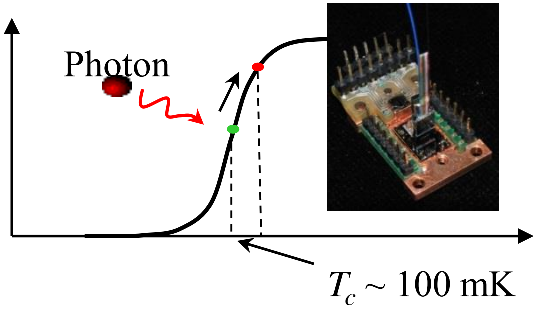
INRiM ISTITUTO NAZIONALE DI RICERCA METROLOGICA

Quantum Metrology for Q-Techies

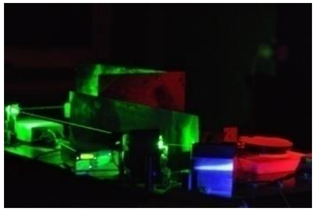
QUANTUM RADIOMETRY TARGETS



- Develop suitable metrics for
  - single photon sources
  - photon counting detectors

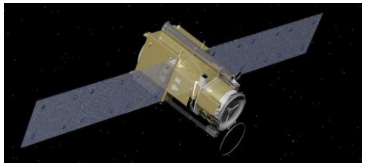


- Develop methods and measurement facilities for characterising non-classical properties of light:
  - antibunching
  - indistinguishability
  - entanglement
  - quantumness



Quantum Metrology for Q-Techies

Projects on single-photon metrology



iMERA PLUS

qu

Project Coordinator: **INRIM**

Quantum Candela: radiometric measurements in the natural units, the number of photons

EMRP
European Metrology Research Programme
Programme of EURAMET
The EMRP is jointly funded by the EMRP participating countries within EURAMET and the European Union

SIQUTE

Project Coordinator: **PTB**

Deterministic and efficient single-photon sources for quantum metrology

EMRP
European Metrology Research Programme
Programme of EURAMET
The EMRP is jointly funded by the EMRP participating countries within EURAMET and the European Union

MIQC

Project Coordinator: **INRIM**

Metrology for Quantum Key Distribution (QKD) in fiber

EMPIR EURAMET
The EMPIR initiative is co-funded by the European Union's Horizon 2020 research and innovation programme and the EMPIR Participating States

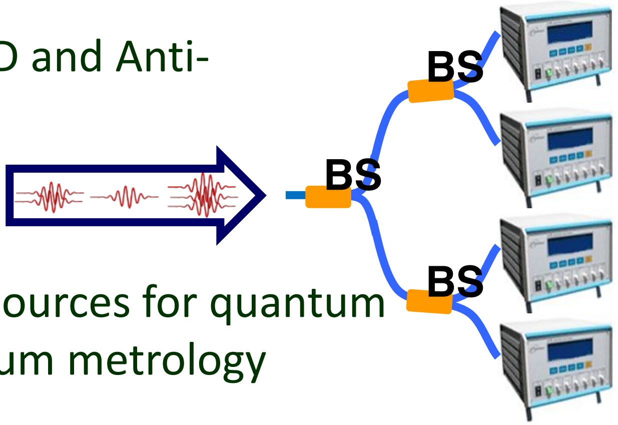
MIQC2

Project Coordinator: **INRIM**

Metrology for free-space QKD and Anti-"Quantum-Hacking"

EMPIR EURAMET
The EMPIR initiative is co-funded by the European Union's Horizon 2020 research and innovation programme and the EMPIR Participating States

SIQUST

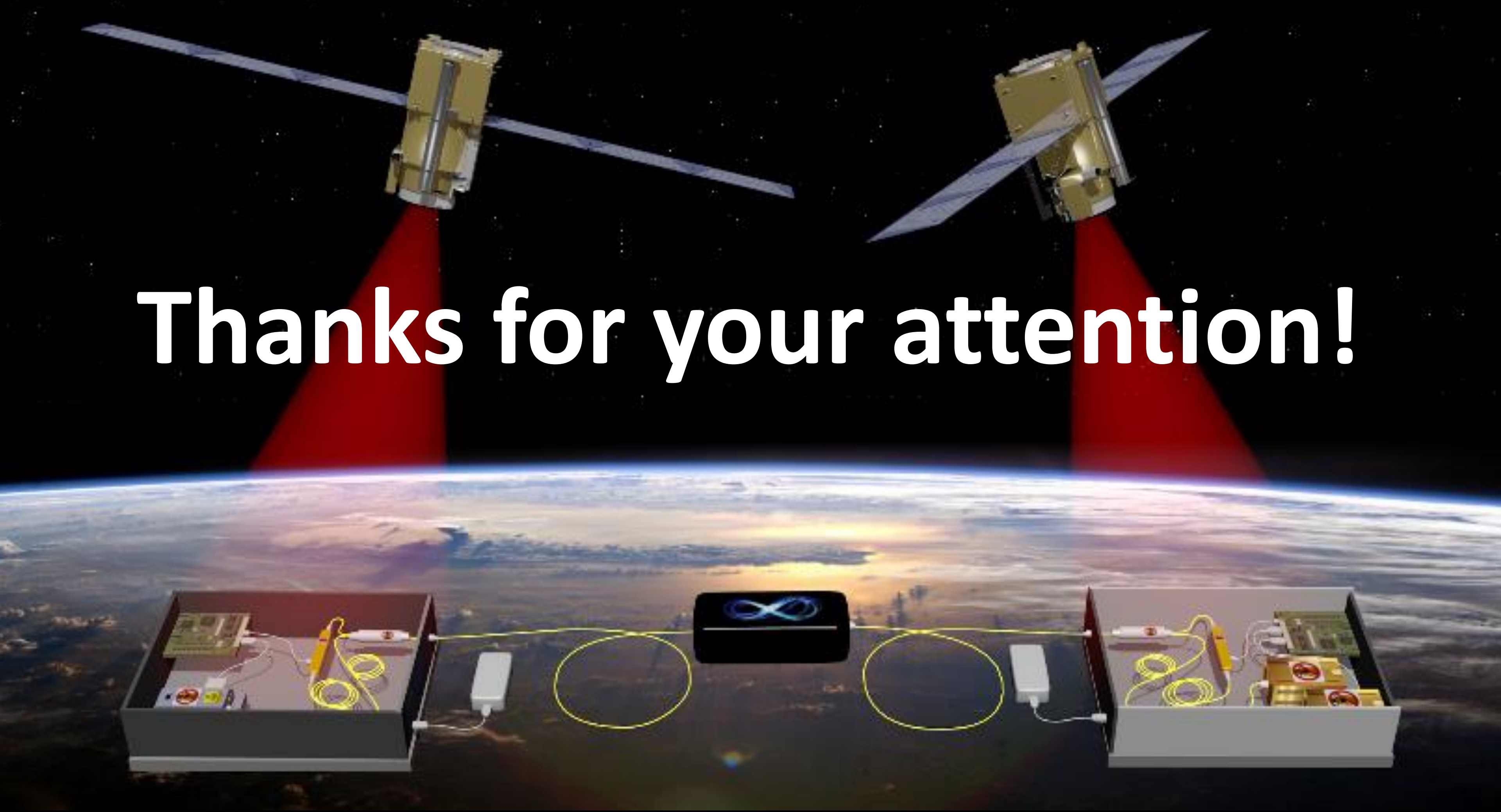


Efficient single-photon sources for quantum technologies and quantum metrology

Project Coordinator: **PTB**

INRiM
ISTITUTO NAZIONALE
DI RICERCA METROLOGICA

Thanks for your attention!



INRiM
ISTITUTO NAZIONALE
DI RICERCA METROLOGICA