COSIC

imec embracing a better life

KU LEUVEN

Challenges and opportunities. Business Cases for Quantum Key Distribution

Bart Preneel
COSIC KU Leuven and imec, Belgium
Bart.Preneel(at)esat.kuleuven.be
26 September 2018

Outline

Quantum cryptography (QKD)

"Based on the firm laws of physics rather than unproven foundations of mathematical complexity"

- principles
- architectures
- evaluation
- market
- predictions

Defeating counterfeiters with unclonable quantum checks (Wiesner, 1970)

U. Of T. Quantum Check
Serial number: 1011010

Record for U. of T. Quantum Check
Serial number: 1011010 (up, left, right, down, left, up)

Quantum checks are impossible to counterfeit without basis information

Sketch of Bennett-Brassard '84 protocol

Step 1: Alice picks photon polarization from

Step 2: Bob picks measurement basis from

Step 3: Bob records his basis and measurement outcome

basis **outcome**

Step 4: Alice and Bob announce their bases publicly. They keep only the polarization data when they have used the same basis

Step 5: Test for tampering by random sampling and computing quantum bit error rate. If error rate is OK, apply error correction and privacy amplification

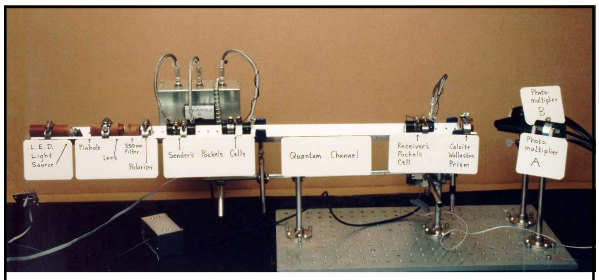
Schedule of BB84 scheme

Alice:
Bob:
Bob:
Same Basis? ✓ ✓ ✓ ✓
Bob:
Raw key: 1 0 0 0

Test for tampering

Alice:
Bob:
Bob:
Same Basis? ✓ ✓ ✓ ✓
Bob:
Raw key: 1 0 0 0

Broadcast and compare a subset of signals



Original Quantum Cryptographic Apparatus built in 1989 transmitted information secretly over a distance of about 30 cm.

Sender's side produces very faint green light pulses of 4 different polarizations.

Quantum channel is an empty space about 30 cm long. There is no Eavesdropper, but if there were she would be detected.

Calcite prism separates polarizations. Photomultiplier tubes detect single photons.

QKD security assumptions

laws of quantum physics are correct

perfect implementation

1. source emits perfect single photons (no multi-photons)
2. noisy but lossless channel (no absorption)
3. perfect detection efficiency (100%)
4. perfect basis alignment (45 degrees)

8

Other QKD protocols

[Ekert'91]: based on entanglement

Demonstration in June 2017 [China, MICIUS satellite]

[Mayers-Yao'98]: Device-independent QKD security proof requires no assumption on the inner working of the devices used for the distribution (could be adversarial)

[Groshanss+'03]: continuous variable QKD

security advantages but harder to implement

9

QKD Architectures

10

QKD Architectures: Terrestrial point to point

Free space: 300m: 1 Mbit/s; up to 23 km

Optical fibre: 10km: 10 Mbit/s & 100km: 10 kbit/s; up to 307 km

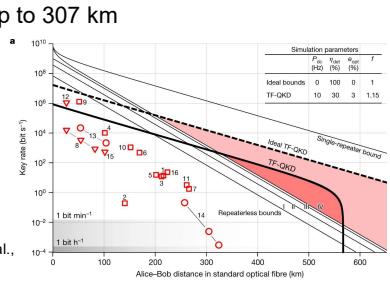


Figure from Lucamarini et al., Nature 2018

11

QKD Architectures: terrestrial network

US: DARPA (2004): 10 nodes

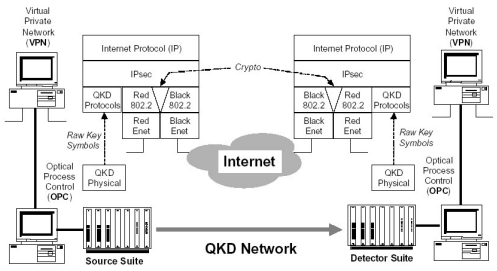


Figure 2. A Virtual Private Network (VPN) based on Quantum Key Distribution.

12

QKD Architectures: terrestrial network

EU SECOQC (2008):

- 5 nodes
- 5-11 Kbit/s over 20-25 km

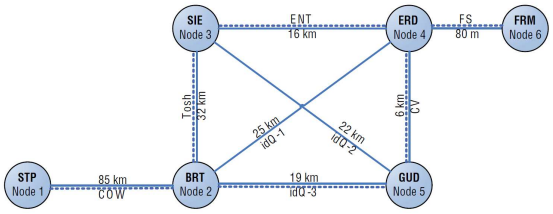


Figure: Peev et al. New Journal of Physics

QKD Architectures: terrestrial network

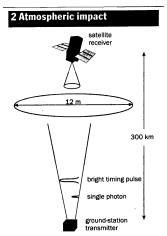
Beijing-Shanghai Network (2017):

- 32 nodes total distance 2000km
- 20 kbit/s

QKD Architectures: space-based

Chinese satellite (2006) at 500 km altitude

Transferring key over 2500 km (need to store it for 2 hours)

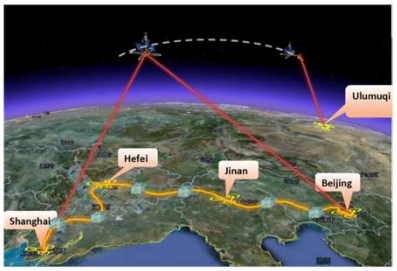


Lift-off: QUESS will study quantum teleportation in space

http://physicsworld.com/cws/article/news/2016/aug/16/china-launches-world-s-first-quantum-science-satellite

QKD Architectures: hybrid

Space based + terrestrial



Technology assessment

Quantum cryptography: positive

Has the potential to be more secure because its security does not degrade with progress in computation or cryptanalysis

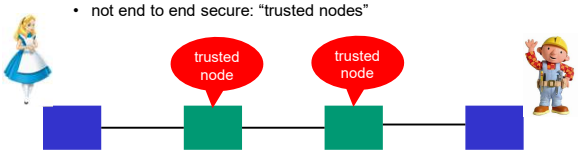
Laws of physics rather than mathematics/complexity theory

- but see Bernstein'18: Is the security of quantum cryptography guaranteed by the laws of physics?

Single photon based hence very suited for optical communications

Quantum cryptography: negative

- Very expensive
- Requires authenticated channel (prior shared secret) between Alice and Bob
- Too slow, so still need to use AES for bulk encryption (hence not unconditionally secure)
- Encryption in data link layer only:
  - limited distance
  - not end to end secure: "trusted nodes"



19

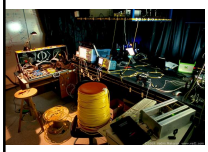
Quantum cryptography: negative

- Security problems
  - side channel attacks
  - device imperfections
  - calibration errors
- Conformance testing complex
- Performance depends on physical characteristics of channel
- More vulnerable to DOS

20

Quantum hacking

http://www.iet.ntnu.no/groups/optics/qcr/



21

Quantum cryptography: improvements

Three-layer architecture = complex

- short-lived public key cryptography for authentic channel between Alice and Bob (it does not matter if it gets broken after 1 day)
- quantum crypto to generate secret key (10-100 Kbit/s)
- symmetric cryptography (AES) for bulk data but change the key every few milliseconds

Device independent QKD

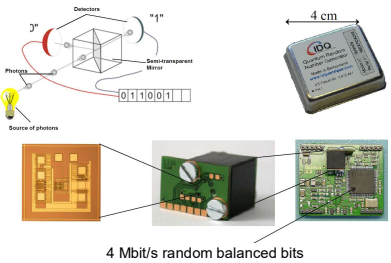
Quantum repeaters

- for long distances still believed to be 10-15 years away

22

Quantum Random Number Generators

Easier to achieve
True randomness



4 Mbit/s random balanced bits

Slide credit: Gisin

23

Hurley-Smith and Hernandez-Castro RWC 2018

https://rwc.iacr.org/2018/Slides/Castro.pdf

Heavily biased due to thermal noise
Need strong post-processing

24

What does GCHQ say? [Oct. 2016]

For all the practical, business and security reasons given above, at this point in time we

- do not endorse QKD for any government or military application
- advise against replacing any existing public-key solutions with QKD for commercial applications

25

What does BSI say? [2016]

Both practically and in terms of security, quantum cryptography is therefore not currently regarded as a strong alternative to post-quantum methods

26

What does the US Air Force Scientifc Advisory Board (SAB) say? [2015]

The service should spend its money elsewhere

https://www.defensenews.com/2015/08/09/air-force-study-shows-potential-limits-of-quantum-tech/

27

What does Adi Shamir say? [2007]

Quantum cryptography will be failed overkill

- 2002 ACM Turing Award
- 2017 Japan Prize
- 2018 Royal Society foreign member

28

Roadmapping and TRLs

Origin: NASA 1974; adopted by ESA in 2000 and by EU in 2013

TRL	9	Commercialized
	8	Pre-production
	7	Field Test
	6	Prototype
	5	Bench / Lab Testing
	4	Detailed Design
	3	Preliminary Design
	2	Conceptual Design
	1	Basic Concept

29

EU Quantum Technologies Flagship Roadmap

within 3 years (by 2020)

High TRL:

- certification and standards for devices and systems

Medium TRL:

- QKD systems will be enhanced to obtain higher key rates (> 10 Mbit/s), lower costs and with multiplexer features
- longer distances will be bridged with trusted nodes or repeaters
- advanced protocols will be provided that offer e.g., digital signatures and position-based verification

30

EU Quantum Technologies Flagship Roadmap
within 6 years (2023)

High TRL:
- longer distance networks with trusted nodes and lower cost end nodes

Medium TRL:
- higher secret key rates (> 100 Mbit/s) over metropolitan distances
- device-independent systems and entanglement-based protocols over > 10 km

31

EU Quantum Technologies Flagship Roadmap
within 10 years (2027)

High TRL: autonomous QKD systems and networks

Medium TRL:
- device-independent QKD over metropolitan distances
- QKD over 1000 km

Low TRL: protocol demonstrations such as cloud computing and photonic networks

32

Quantum Technologies in Space project:
(2017)

rolling out small, medium and large satellites
fully-functional systems with global coverage
will take at least 10 years

33

EU view on Quantum Communications (= EU language for QKD) (2018)

Most advanced among quantum technologies
Used in niche applications for point-to-point
Additional layer of security in the networks
Essential to protect digital technologies

R&D investment of 200 M€ in next 10 years plus
- QKD testbed (2018 call) 15 M€
- ESA Artec-Scylight

34

Commercial QKD products available on the market today!

MAGIQ TECH

Pioneers left the market:
- MagiQ Technologies (New York)
- SmartQuantum (France)
- SeQureNet (Paris)

35

IQ Quantique

- Distance over 100 km of commercial telecom fibers
- Long-term stability through "auto-compensation" ("Plug and Play" set-up)

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

36

Selling or announcing QKD products

- Alibaba Group (China)
- Applied Communication Sciences (USA)
- Cryptographic (UK)
- ID Quantique SA (Switzerland)
- IDQ-Jiuzhou Quantum Technologies (China)
- KETS Quantum Security Ltd. (UK),
- Oki Electric Industry Company Ltd. (Japan)
- Anhui Qasky Quantum Science and Technology (China)
- QuantumCTek (China)
- Qubitekk (US) (formerly GridCOM)
- QuintenssenceLabs (Australia)
- ROI Optoelectronics Technology (China)
- Senetas (Australia)
- ZTE Corporation (China)

37

Research on QKD technology

- Airbus (France)
- Austrian Institute of Technology (AIT) (Austria)
- Boeing (USA)
- BT (UK)
- Fujitsu Laboratories Ltd. (Japan)
- Huawei (China)
- HP Enterprises (US)
- IBM (US)
- Infineon Technologies (Germany)
- Korea Institute of Science and Technology (KIST) (Republic of Korea)
- Leonardo Finmeccanica (Italy)
- Lockheed Martin (US)
- Los Alamos National Laboratory (USA)
- Mitsubishi Electric Corp.(Japan)
- NEC Corp. (Japan)
- Nippon Telegraphy and Telephone Corp. (Japan)
- NICT (Japan)
- Oak Ridge National Laboratory (USA)
- National Institute for Standards and Technology (NIST) (USA)
- QinetiQ (UK)
- Raytheon BBN Technologies (USA)
- Safran (France)
- Samsung (Republic of Korea)
- Sandia National Laboratories (USA)
- Thales (France)
- Toshiba Corp. (Japan).

38

Building blocks

- Crypta Labs (UK)
- Nucrypt LLC (US)
- Quantum Opus (US)
- Qutools (Germany)
- Single Quantum (The Netherlands)
- Universal Quantum Devices (Canada)

Telcos

- AT&T (USA)
- Batelle (USA)
- BT (UK)
- China Quantum Technologies (QTEC) (China)
- GEANT (EU)
- Korea Telecom (Republic of Korea)
- KPN (The Netherlands),
- Nokia (Finland)
- Telefonica (Spain)
- South Korea Telecom (Republic of Korea)

39

Market assessment

40

Changing role of cryptography

Communications

Storage

During computation

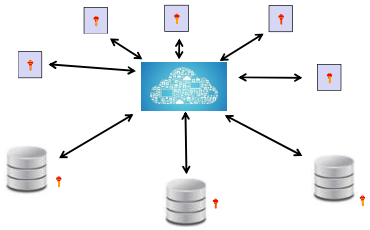
41

From Big Data to Small Local Data

Data stays with users

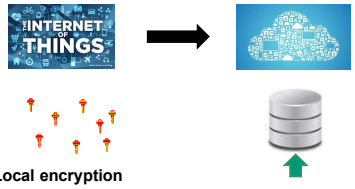
42

From Big Data to encrypted data MPC (Multi-Party Computation)



43

From Big Data to Encrypted Data



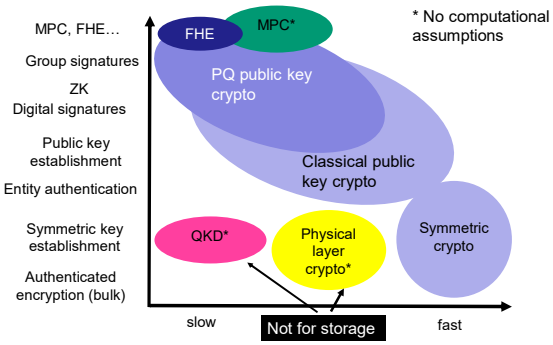
Local encryption with low multiplication depth

Encrypted data

Can still compute on the data with somewhat Fully Homomorphic Encryption

44

From Big Data to Encrypted Data



Inspired by M. Sasaki

45

Market segments (1/2)

Government communications: military and diplomatic (security of 20+ years)

- trusted nodes less of an issue
- non-EU suppliers of critical components
- certification difficult

Point-to-point backbones between datacenters and main branches (financial/insurance)

- image building

46

Market segments (2/2)

Critical infrastructure:

- data authentication more important than confidentiality

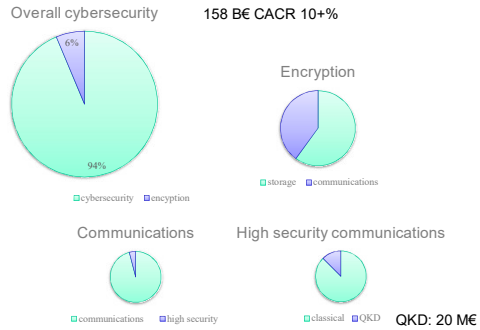
Space:

- cost effective?

Optimization of optical communications

47

Market assessment: EU Cybersecurity 2016



48

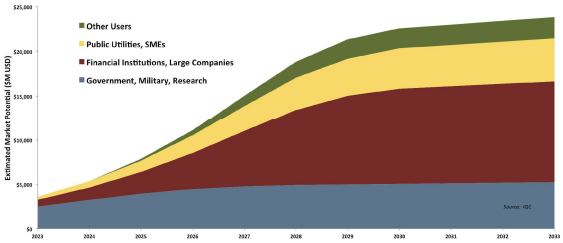
Market prediction

Prediction is very difficult
especially of the future

49

IQC Market forecast (2014)

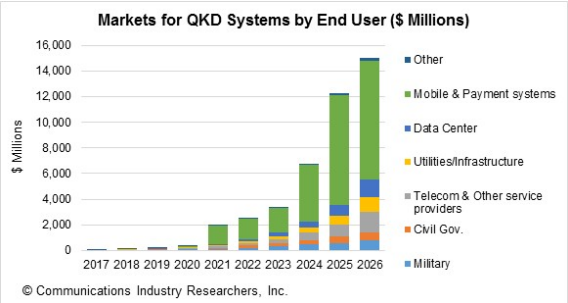
2014: 30 M$



50

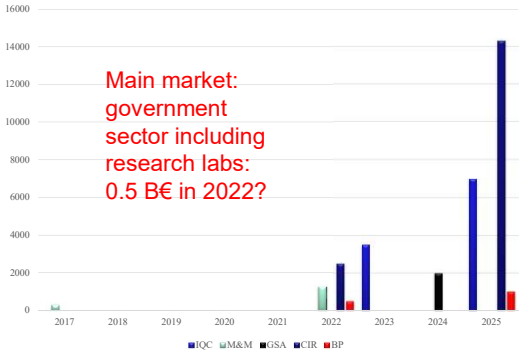
Communications Industry Research (2017)

Quantum repeaters: 107 M$ by 2022



51

QKD Forecasts



Main market:
government
sector including
research labs:
0.5 B€ in 2022?

52

Conclusions

- QKD is an exciting technology
- Very large R&D investments in China and EU
- Interesting spill-overs
- But QKD struggling in market
  - solving the wrong problems
  - answer looking for a problem
  - trusted nodes are problematic
- Market driven by a few governments and government research labs

53

Bart Preneel, COSIC KU Leuven and imec

ADDRESS: Kasteelpark Arenberg 10, 3000 Leuven
WEBSITE: homes.esat.kuleuven.be/~preneel/
EMAIL: Bart.Preneel@esat.kuleuven.be
TWITTER: @CosicBe
TEL +32 16 321148

54

Further reading (1/3)

A. Acin, N. Brunner, N. Gisin, S. Massar, S. Pironio, V. Scarani, "Device-Independent Security of Quantum Cryptography against Collective Attacks," Physical Review Letters, 2007, 98(23), 230501.

C.H. Bennett, G. Brassard. "Quantum Cryptography: Public Key Distribution and Coin Tossing," Proc. of IEEE International Conference on Computers, Systems and Signal Processing, volume 175, page 8. New York, 1984. http://researcher.watson.ibm.com/researcher/files/us-bennetc/BB84highest.pdf

D.J. Bernstein, "Is the Security of Quantum Cryptography Guaranteed by the Laws of Physics?" March 2018, https://arxiv.org/abs/1803.04520

BSI, "The State of IT Security in Germany 2016," https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Securitysituation/IT-Security-Situation-in-Germany-2016.pdf

E. Diamanti, H.-K. Lo, B. Qi, Z. Yuan, Practical Challenges in Quantum Key Distribution," npj Quantum Information 2016, 2, 16025, https://www.nature.com/articles/npjqi201625.

A.K. Ekert, "Quantum Cryptography Based on Bell's Theorem," Physical Review Letters, 1991, 67(6), pp. 661-663.

ETSI, "Quantum Key Distribution: Use Cases," ETSI GS QKD 002, V1.1.1, June 2010.

ETSI, "Quantum Safe Cryptography and Security. An Introduction, Benefits, Enablers, and Challenges," ETSI White Paper No. 8, June 2015.

55

Further reading (2/3)

S.. Ghernaouti-Helie, I. Tashi, T. Laenger, C. Monyk, "SECOQC Business White Paper," April 2009, https://arxiv.org/abs/0904.4073

F.. Grosshans, G. Van Assche, J. Wenger, R. Brouri, N.J. Cerf, P. Grangier, "Quantum Key Distribution using Gaussian-Modulated Coherent States," Nature 2003, 421, pp. 238--241.

Institute for Quantum Computing, "Quantum Cryptography. 2014, Market Study & Business Opportunities Assessment," University of Waterloo, 2014.

N. Jain, B. Stiller, I. Khan, D. Elser, C. Marquardt, G. Leuchs, "Attacks on Practical Quantum Key Distribution Systems (and How to Prevent Them)," arXiv:1512.07990v2, https://arxiv.org/abs/1512.07990}, 17 September 2016.

A.M. Lewis, M. Travagnin, "The Impact of Quantum Technologies on the EU's Future Policies. PART 2 Quantum Communications: from Science to Policies," JRC Science for Policy Report, 2018.

M. Mosca, "Cybersecurity in an Era with Quantum Computers: Will We Be Ready?" IACR eprint, https://eprint.iacr.org/2015/1075.pdf

D. Moskovich, "An Overview of the State of the Art for Practical Quantum Key Distribution," May 2015, https://arxiv.org/abs/1504.05471

56

Further reading (3/3)

K.G. Paterson, F.C. Piper, R. Schack, "Quantum Cryptography: A Practical Information Security Perspective," in Quantum Communication and Security, NATO Advanced Research Workshop M. Zukowski, S. Kilin, J. Kowalik (Eds.), pp. 175-180, IOS Press, 2007. Updated version https://arxiv.org/abs/quant-ph/0406147

Quantum Flagship High-Level Expert Group, "Final Report," 28 June 2017, http://ec.europa.eu/newsroom/document.cfm?doc_id=46979

Quantum Technologies in Space (QT Space), "Intermediate Strategic Report for ESA and National Space Agencies," November 2017.

V. Scarani, C. Kurtsiefer, "The Black Paper of Quantum Cryptography: Real Implementation Problems," Theoretical Computer Science, 2014, 560, pp. 27-32, https://arxiv.org/abs/0906.4547

D. Stebila, M. Mosca, N. Lütkenhaus "The Case for Quantum Key Distribution," December 2009, https://arxiv.org/abs/0902.2839

57