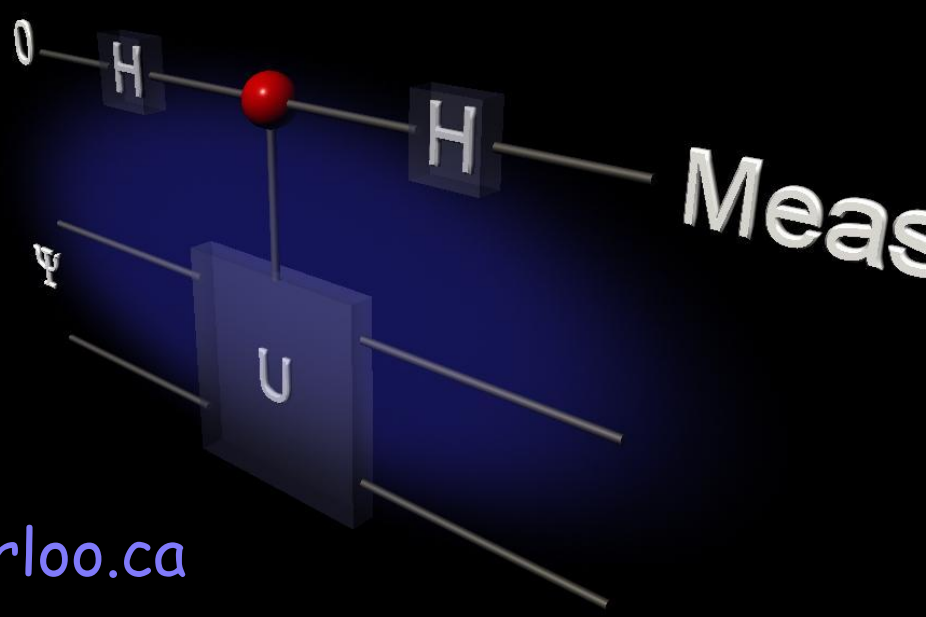
Introduction to Quantum Information Processing



CS467 C&O481 PHYS467

Michele Mosca mmosca@iqc.uwaterloo.ca

Tuesdays and Thursdays 10am-11:15am

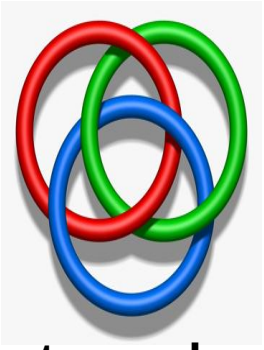
IQC Institute for Quantum Computing

UNIVERSITY OF WATERLOO

PI PERIMETER INSTITUTE FOR THEORETICAL PHYSICS

Cryptography is a foundational pillar of the global information security infrastructure

Cryptography allows us to achieve information security in the “cloud”.

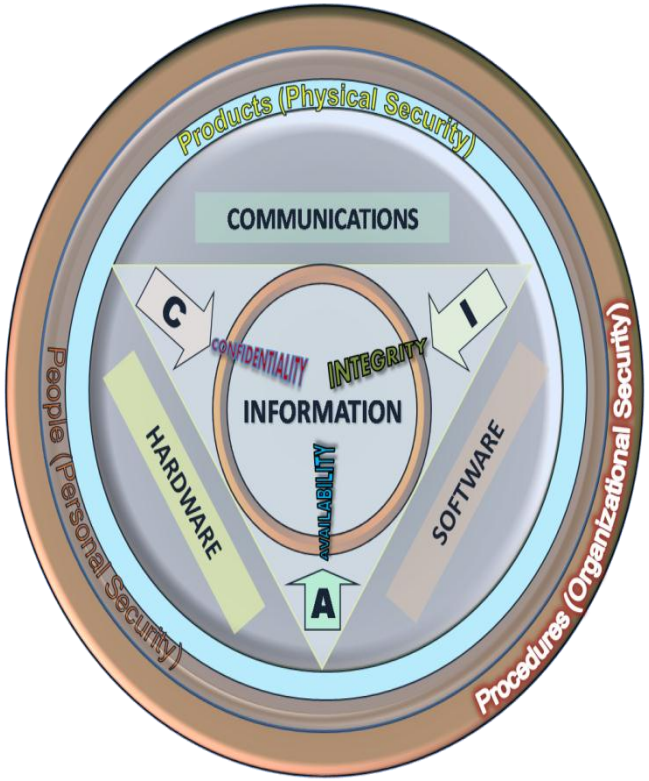


Information is handled by untrusted parties through untrusted media

A foundational pillar for a complex system

Many potential weak links:

- bad trust assumptions
- phishing
- weak passwords
- bad implementations
- side-channel attacks
- cryptography protocol errors
- etc, etc.
- … including things we haven't thought of yet

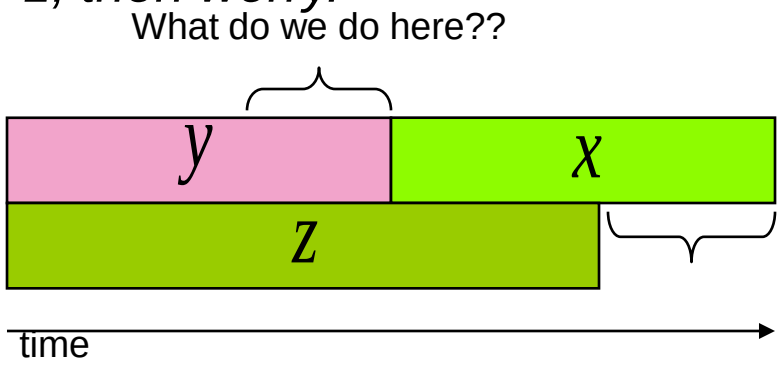


How soon do we need to worry?

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? (*y* years)
- How long will it take for a large-scale quantum computer to be built (or for any other relevant advance)? (*z* years)

THEOREM 1: If x+y > z, then worry.



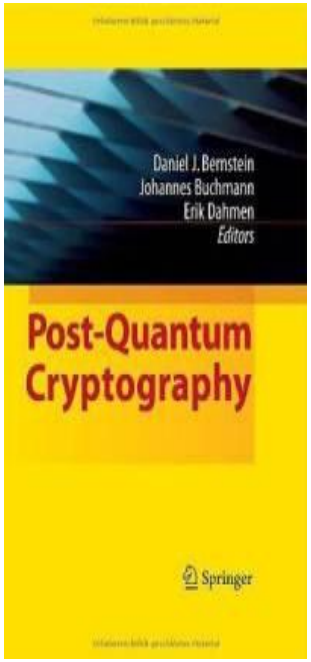
How long to re-tool the cryptographic infrastructure?

Cryptographers are studying possible quantum-safe codes.

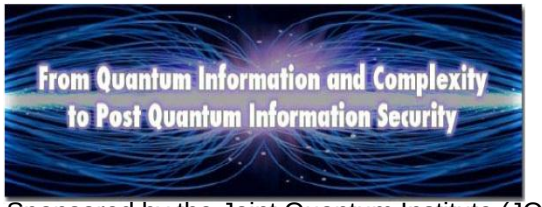
CryptoWorks21

Quantum information experts are researching the power of quantum algorithms, and their impact on computationally secure cryptography.

How easy is it to change from one cryptographic algorithm to a quantum-secure one? Are the standards and practices ready?



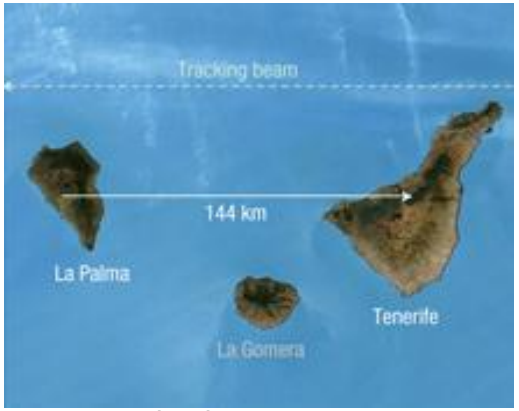
PQCrypto 2011, Taipei. Nov 29-Dec 2



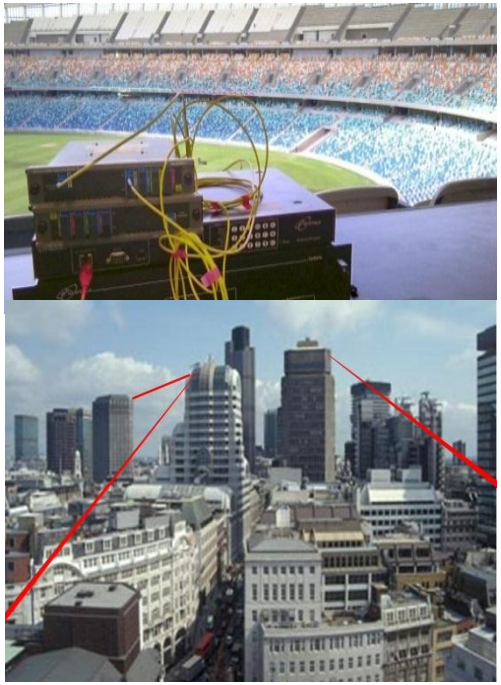
Sponsored by the Joint Quantum Institute (JQI), NIST, and the University of Maryland. October 27-29, 2010

Quantum technologies also offer new security tools

- Quantum communication can provide a new kind of cryptography that is “information theoretically” secure.
- Most famous example is quantum key establishment (QKD) invented by Bennett and Brassard in 1984



Canary Islands:
Longest Free Space distance for QKD



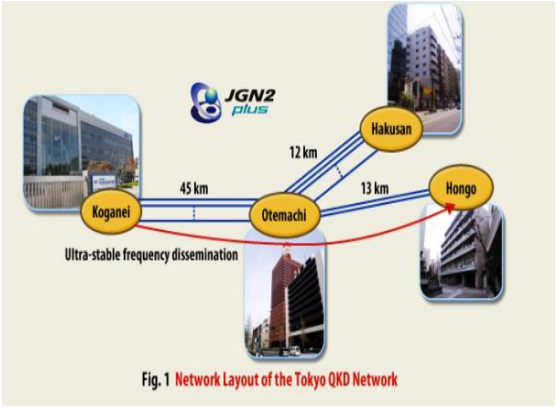


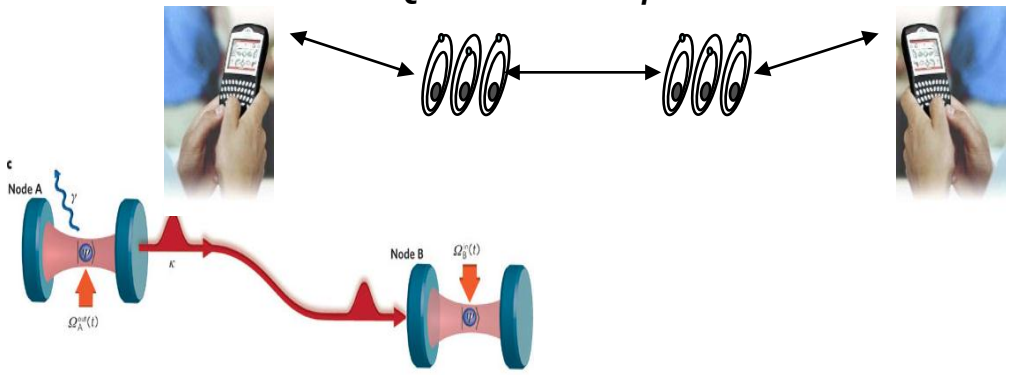
Fig. 1 Network Layout of the Tokyo QKD Network

Towards a quantum internet

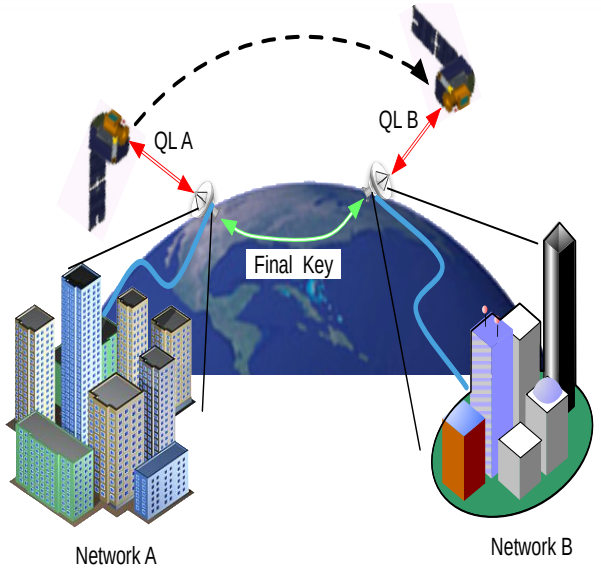
New technologies will achieve reliable quantum communication on global distances, well the beyond current range of about 100 km.

Quantum repeaters, quantum teleportation, and satellites, can someday be used to span the globe.

Quantum repeaters



Reviews on Quantum Repeaters: Sangouard et al, Rev. Mod. Phys. 83, 33 (2011); Kimble, NATURE, 453 (2008).



A quantum satellite in LEO can interconnect ground networks located anywhere on Earth.

Active research in Canada (QEYSSAT), USA, Europe (Space-QUEST), Japan, China, Singapore.

Quantum-safe cryptography

“post-quantum” cryptography

- classical codes deployable without quantum technologies
- believed/hoped to be secure against quantum computer attacks of the future

+

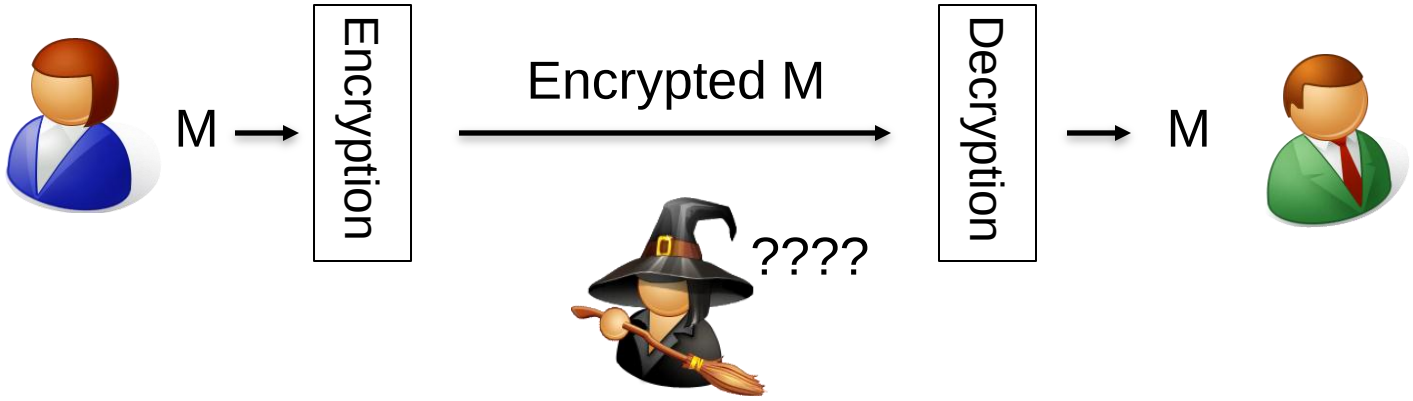
quantum cryptography

- quantum codes requiring some quantum technologies (typically less than a large-scale quantum computer)
- typically no computational assumptions and thus known to be secure against quantum attacks

Both sets of cryptographic tools can work very well together in quantum-safe cryptographic ecosystem

Cryptography

Alice wants to send a message M to Bob in such a way that an eavesdropper Eve cannot obtain information about M



Alice encrypts, and Bob decrypts

Private key cryptography

In a private key cryptosystem, the sender and receiver each have a copy of a private key k, exchanged securely at some earlier point in time.

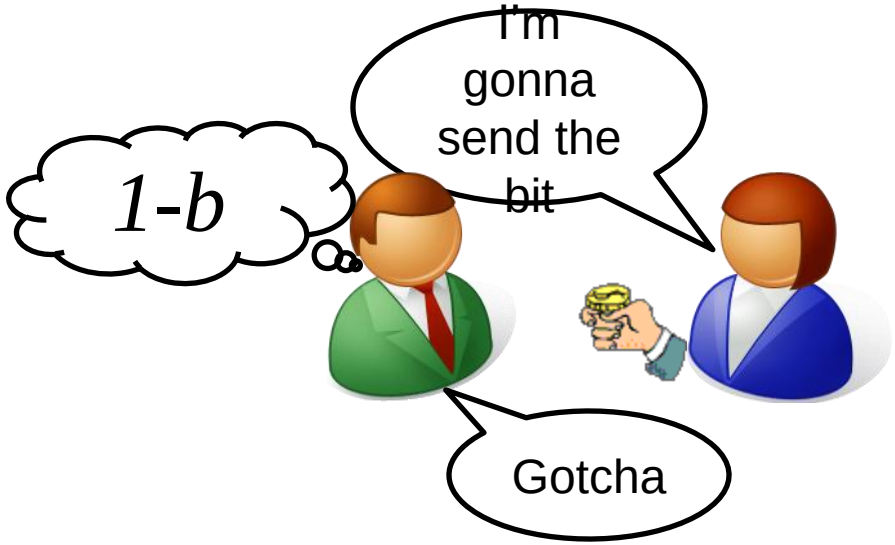
When Alice wants to send to Bob a message, she uses k to encrypt the message before sending it. Bob then uses k to decrypt the encrypted message.

Example: one-time pad

One-time pad

Suppose Alice wants to send Bob a secret bit of information b.

Alice sends Bob b with probability 1/2, and 1-b with probability 1/2. Of course, she needs to make sure Bob knows which one, so he knows whether or not to flip the bit he receives.



One-time pad

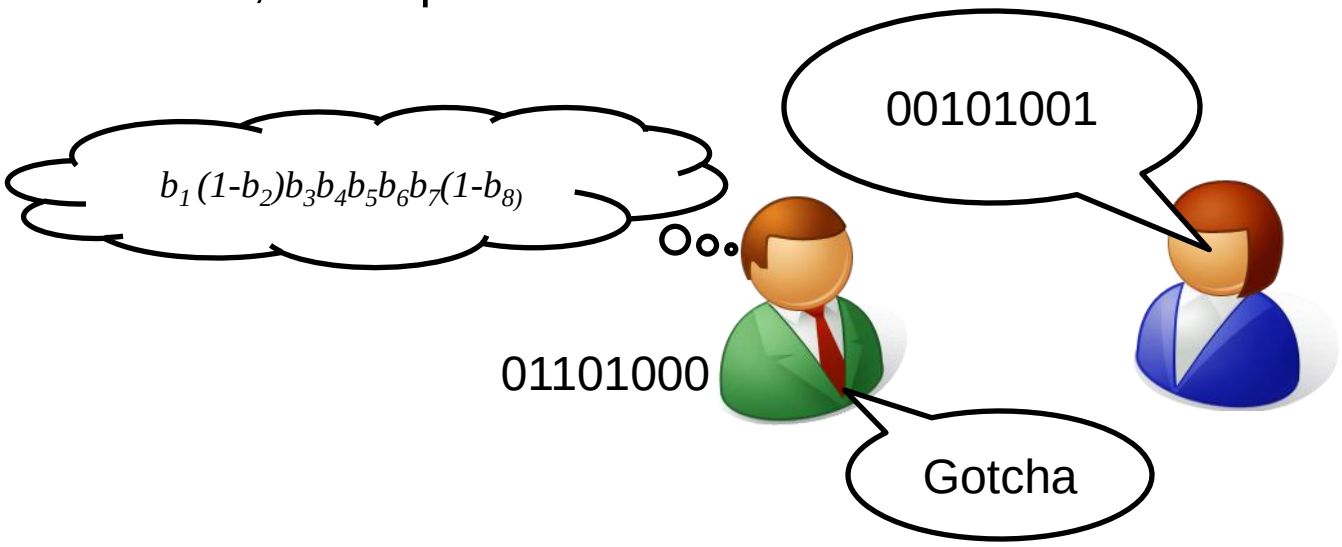
Alice can flip the coins beforehand. Then she can tell Bob in advance in a secret meeting whether b or 1-b is sent.

To an observer who does not know the information exchanged by Alice and Bob when they met in secret, the bit transmitted by Alice appears completely random.

One-time pad

This can easily be extended to an n bit message

While together, Alice and Bob generate a string of n bits called the key. After they separate, Alice wants to send Bob an n bit message. If the ith key bit is 0, Alice leaves the ith bit of her message unchanged. Otherwise, she flips it.



One-time pad

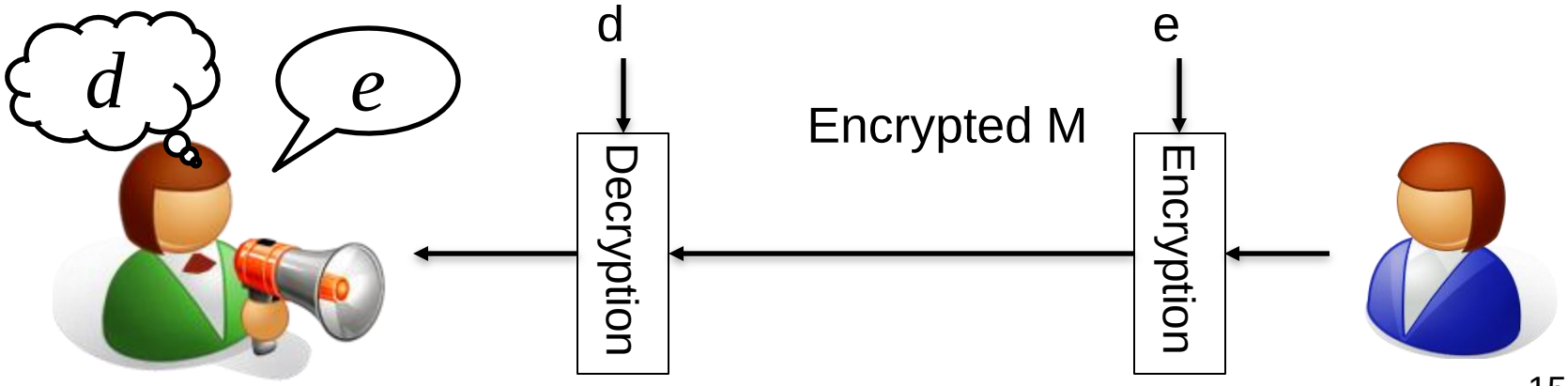
To an observer who does not know the key, the string of bits sent by Alice does not give any information about the original message. The security is perfect!

However, it can be proved that to make this work, for every bit you want to exchange, you need one bit of key, which must be exchanged securely.

Public Key Cryptography

Public key cryptography makes it possible to get around the main problem of establishing large secret keys in advance.

The solution is to have two distinct keys, an encryption key or public key, e, and a decryption or private key, d. Your public key is used to encrypt messages intended for you, and your private key is used (by you) to decrypt any messages encrypted with your public key.



Public Key Cryptography

Of course, there must be some relationship between d and e in order for this to work. However, this relationship must not allow others to determine easily d from e.

There are systems that implement this approach in practice. The most popular ones are RSA and ECC.

These schemes can usually be proved to be hard to break (computationally secure) under the assumption that some underlying problem is hard. Proving the security of RSA requires assuming that factoring is hard. Proving the security of ECC requires assuming that the discrete logarithm problem on the additive group of points on an elliptic curve is hard.

Public Key Cryptography

In practice, public key cryptography is usually used to exchange symmetric keys, which are then used in a conventional symmetric cipher.

e.g. AES. One could even use the one-time pad encryption, however the unconditional security guarantees don't apply, since an eavesdropper with unbounded computational power can determine the key.

In practice, one can separate public-key authentication (digital signatures), from key establishment (via public-key encryption).

For long-term security, it suffices that the authentication was valid during the execution of the key establishment protocol, and that the key establishment protocol is secure in the long-term. i.e. the authentication protocol only requires "short-term" security.

Quantum Cryptographic Tools

The problem with computational security is that it requires a computational assumption.

Factoring is believed to be hard on a classical computer, but perhaps there is some unknown polynomial-time algorithm. And there is a polynomial-time quantum one.

A one-time pad, however, is "unconditionally" secure, which means it has no computational assumptions (of course, the usual conditions regarding trust and physical security apply).

Quantum key distribution allows us to get over the main drawback of the one-time pad. It gives a way of sharing a random key in an unconditionally secure way, without prior secure physical exchange. One only requires an authenticated communication channel (not a private channel).

Quantum Information Security

- Quantum mechanics provides intrinsic eavesdropper detection.

- e.g. no-cloning theorem: there is no transformation that will copy an unknown quantum state, i.e.

$$|\psi\rangle|0\rangle|workspace\rangle \mapsto |\psi\rangle|\psi\rangle|\ junk(\psi)\rangle$$

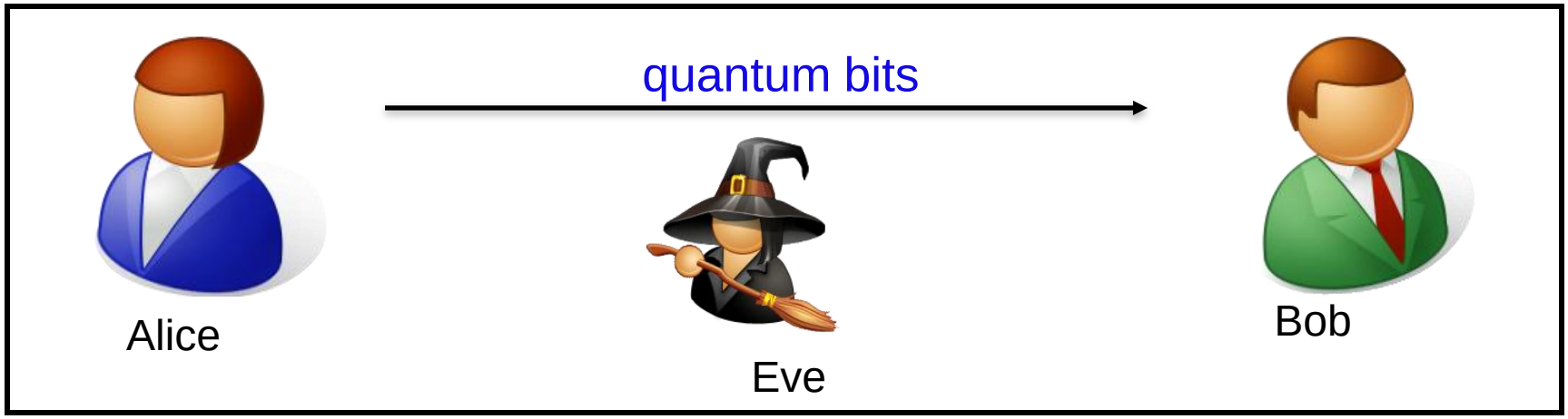
  is not possible.

Quantum Information Security

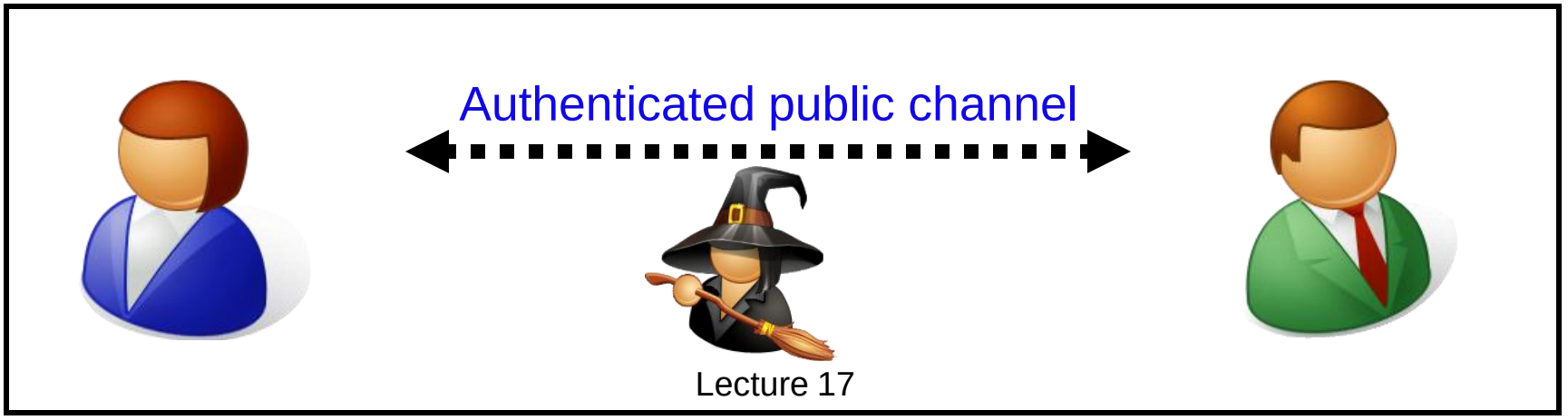
• More generally, any procedure that extracts information about an unknown quantum state, MUST disturb the state (on average).

• There is a fundamental quantifiable tradeoff between information extraction and disturbance.

Quantum Key Distribution (QKD) (general idea)



Alice and Bob measure their qubits



Quantum Key Distribution (QKD) (general idea)

Alice and Bob publicly discuss the information they measured to assess how much information Eve could have obtained.

If Eve's information is very likely to be below a certain constant threshold, they can communicate further and distill out a very private shared key ("privacy amplification").

Otherwise they abandon the key.

QKD

This sort of eavesdropper detection can be used to develop “unconditionally” secure key exchange protocols.

Roughly speaking, Alice and Bob exchange some quantum signals, perform some tests and statistically bound how much information Eve could have obtained.

They then perform classical privacy amplification to reduce Eve’s information to an arbitrarily small amount with arbitrarily high probability.

BB84 protocol

Alice encodes one bit in either the {$|0\rangle$, $|1\rangle$} basis or {$|0\rangle + |1\rangle$, $|0\rangle - |1\rangle$} basis and sends Bob one of the following states

$$|0\rangle, |1\rangle, |0\rangle + |1\rangle, |0\rangle - |1\rangle.$$

Once Bob receives the state, Alice tells him whether she sent one of $|0\rangle$ or $|1\rangle$, or one of $|0\rangle + |1\rangle$, $|0\rangle - |1\rangle$.

In the first case, Bob can measure the state and determine which state Alice sent.

BB84 protocol

In the second case, Bob first applies a Hadamard gate (which maps |0⟩ + |1⟩ to |0⟩, and |0⟩ - |1⟩ to |1⟩), and then measures to determine which state Alice sent.

$$|0\rangle + |1\rangle \xrightarrow{Hadamard} |0\rangle \xrightarrow{measure} |0\rangle$$

$$|0\rangle - |1\rangle \xrightarrow{Hadamard} |1\rangle \xrightarrow{measure} |1\rangle$$

Bob tells Alice which state she sent.

Alice confirms that he is correct.

Eavesdropper

This is an example of how a particular attack by an eavesdropper can be detected:

Suppose Alice sends Bob one of the states $|0\rangle$, $|1\rangle$, $|0\rangle + |1\rangle$, $|0\rangle - |1\rangle$.

Remember, Eve cannot clone the quantum state.

Suppose Eve intercepts the signal, measures it in either $\{|0\rangle, |1\rangle\}$ basis or $\{|0\rangle + |1\rangle, |0\rangle - |1\rangle\}$ basis, records the answer, and sends the resulting state on to Bob.

Once Bob receives the state, Alice tells him whether she sent one of $|0\rangle$ or $|1\rangle$, or one of $|0\rangle + |1\rangle$, $|0\rangle - |1\rangle$.

Eavesdropper

Suppose that Eve measures in {|0⟩, |1⟩} basis.

Bob measures the state and correctly determines which state Alice sent.

The eavesdropper is not detected!

In the second case, Bob applies a Hadamard gate, and then measures. With 50% probability, Bob will get the wrong answer.

This means the data was tampered with!

$$|0\rangle + |1\rangle \xrightarrow{\textit{Eve measures}} \begin{matrix} 50\%|0\rangle \\ 50\%|1\rangle \end{matrix} \xrightarrow{\textit{Hadamard}} \begin{matrix} 50\%|0\rangle + |1\rangle \\ 50\%|0\rangle - |1\rangle \end{matrix} \xrightarrow{\textit{measure}} \begin{matrix} 50\%|0\rangle \\ 50\%|1\rangle \end{matrix}$$

$$|0\rangle - |1\rangle \xrightarrow{\textit{Eve measures}} \begin{matrix} 50\%|0\rangle \\ 50\%|1\rangle \end{matrix} \xrightarrow{\textit{Hadamard}} \begin{matrix} 50\%|0\rangle + |1\rangle \\ 50\%|0\rangle - |1\rangle \end{matrix} \xrightarrow{\textit{measure}} \begin{matrix} 50\%|0\rangle \\ 50\%|1\rangle \end{matrix}$$

Practicalities

One typically uses photons to communicate quantum information, and storage is not presently practical.

So Bob cannot store the photons, and wait for Alice to tell him which bases she used.

So, the protocol is modified so that Bob picks a random basis and measures the photon as soon as it is received. Later, Bob and Alice use classical communication to announce their bases, and discard instances where they didn't pick the same random basis (which is about half of the time).

Dealing with errors

State preparation, transmission, and detection are not perfect, and so there must be some tolerance for errors.

Since the “intercept and resend” attack yields a 25% error rate, then 25% is an upper bound on the tolerable error rate. Otherwise we could not distinguish a correct transmission with errors, from one under the “intercept and resend” attack.

Error correction allows Alice and Bob to correct their strings to produce a common string (with high probability).

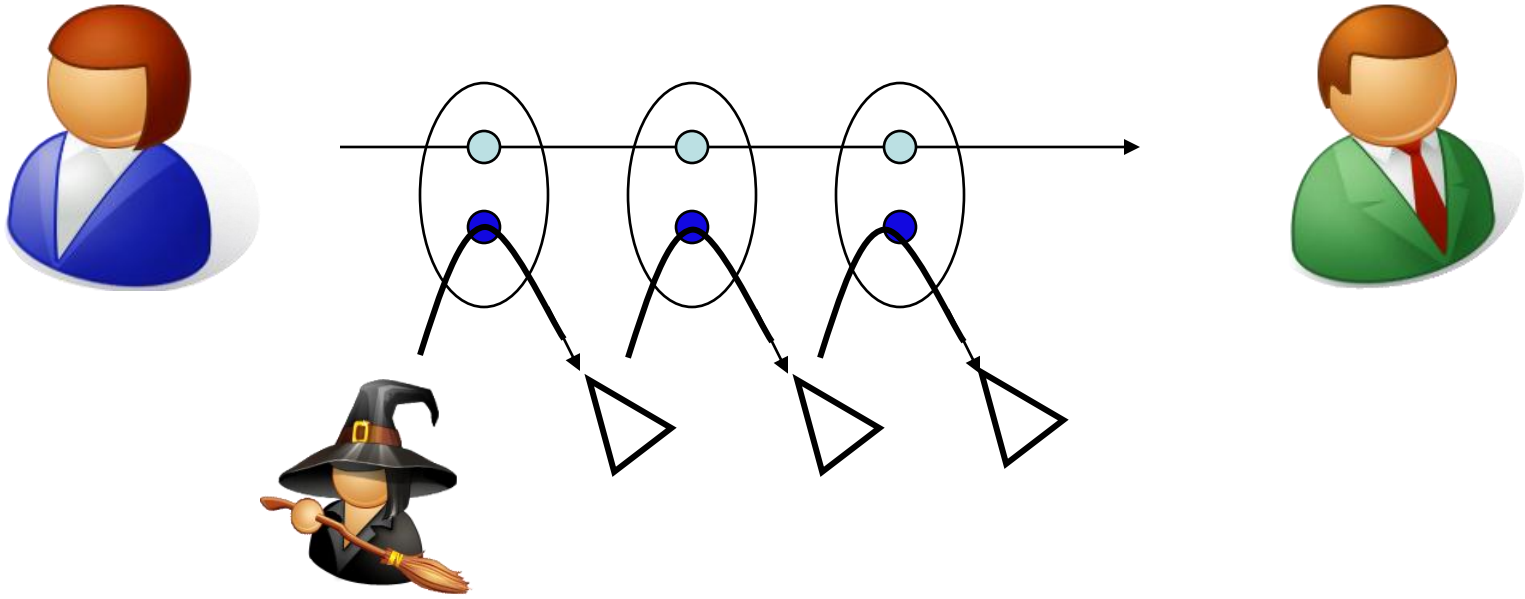
For error rates substantially less than 25% (e.g. 10%), it is possible for Alice and Bob to perform “privacy amplification” in order to “squeeze out” any correlation Eve has with their shared string.

More general attack models

The “intercept and resend” attack is a simple attack, and we don’t just want security against a specific attack.

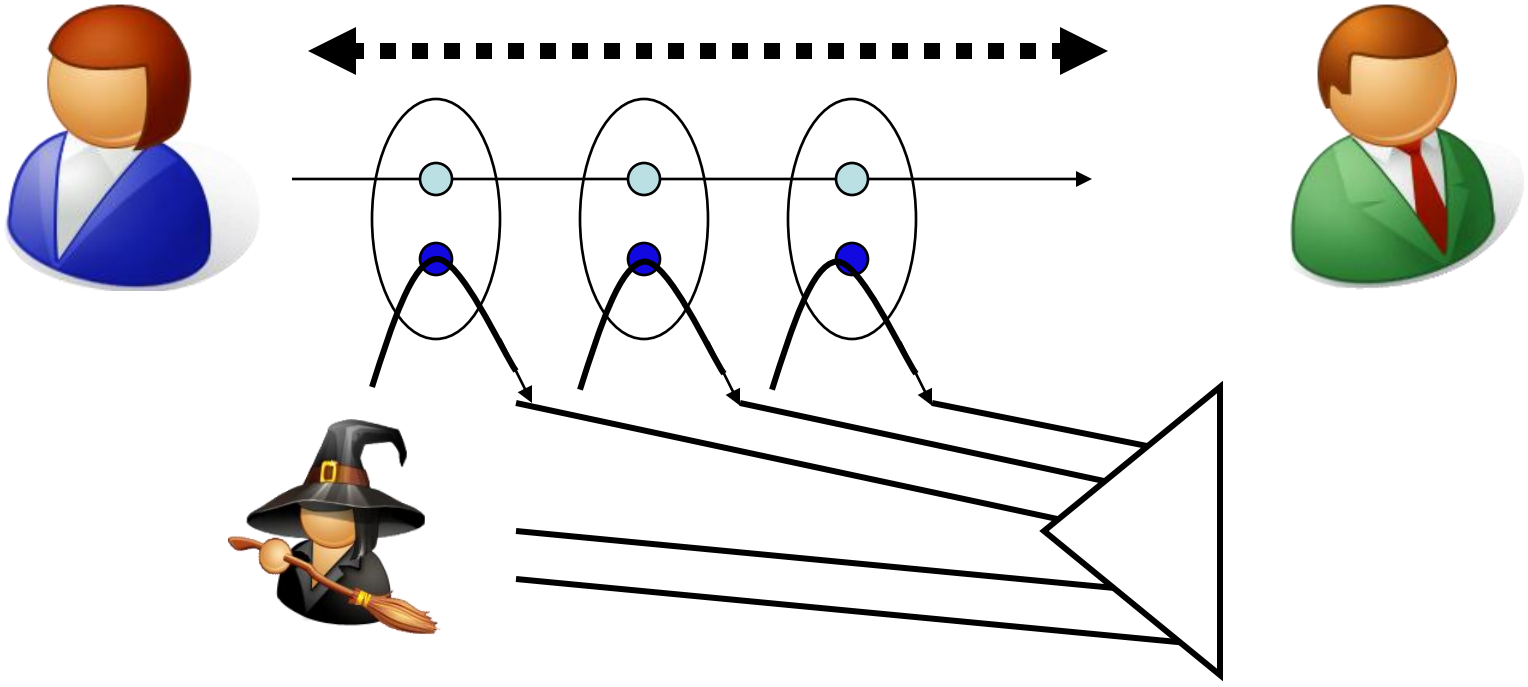
“Individual” attacks

Eve couples each qubit individually to a separate quantum ancilla, which she measures independently.



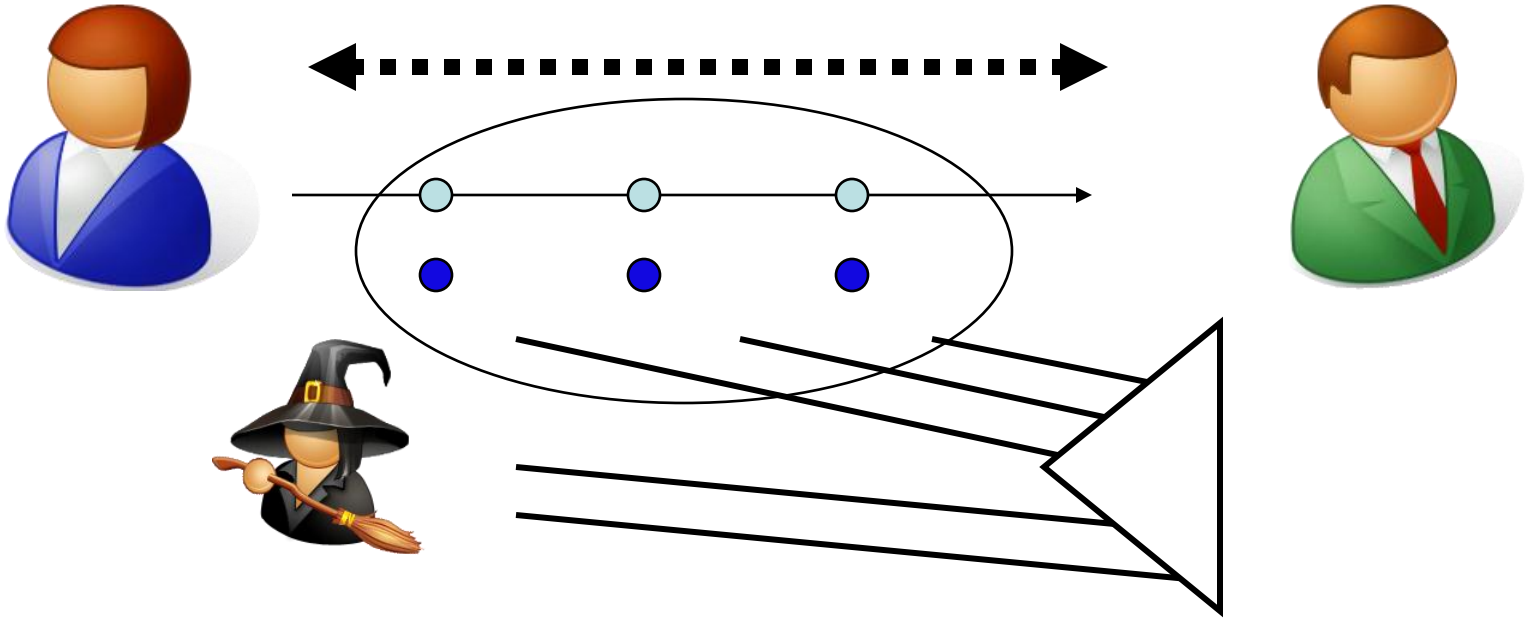
“Collective” attacks

Eve couples each qubit individually to a separate quantum ancilla, and she later does a joint measurement on her system.



“Coherent” attacks

Alice prepares all her qubits, gives them to Eve, who does whatever she likes with them, and passes on some message to Bob.



Security of QKD

The BB84 QKD scheme, with appropriate physical assumptions, is secure against coherent attacks

(Mayers'96, Lo-Chau'98, and much follow-up work, including Lütkenhaus et al, Gottesman et al.).

Security of QKD

There are however attacks on commercial quantum systems, using properties of the physical devices used in the implementation.

Recent device independent proposals for QKD try to avoid these situations.

NATURE PHOTONICS | LETTER

Hacking commercial quantum cryptography systems by tailored bright illumination

Lars Lydersen, Carlos Wiechers, Christoffer Wittmann, Dominique Elser, Johannes Skaar & Vadim Makarov

Affiliations | Contributions | Corresponding author

Nature Photonics **4**, 686–689 (2010) | doi:10.1038/nphoton.2010.214
Received 02 April 2010 | Accepted 11 July 2010 | Published online 29 August 2010

PRL **105,** 070501 (2010) PHYSICAL REVIEW LETTERS week ending 13 AUGUST 2010

Proposal for Implementing Device-Independent Quantum Key Distribution Based on a Heralded Qubit Amplifier

Nicolas Gisin,[1] Stefano Pironio,[1,2] and Nicolas Sangouard[1]
[1]*Group of Applied Physics, University of Geneva, 1211 Geneva 4, Switzerland*
[2]*Laboratoire d'Information Quantique, Université Libre de Bruxelles, Belgium*
(Received 22 March 2010; revised manuscript received 13 July 2010; published 12 August 2010)

Practical Issues

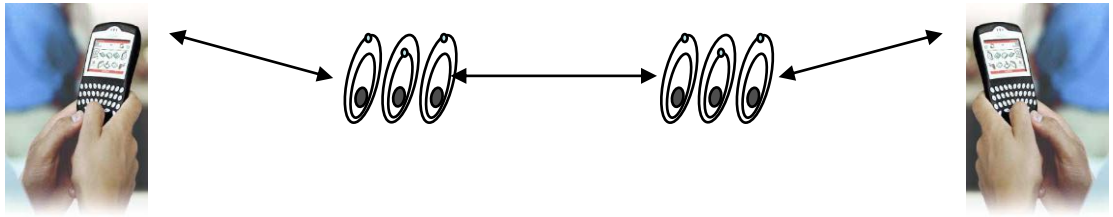
- Distance
- Key rate
- Do we really need it?

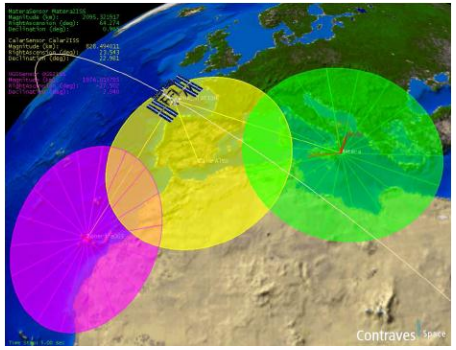
Distance
Quantum communication networks

At present, reliable quantum communication can be achieved along modest distances (approx. 100km)

Quantum repeaters, quantum teleportation, and possibly satellites, can someday be used to span the globe.

Quantum repeaters

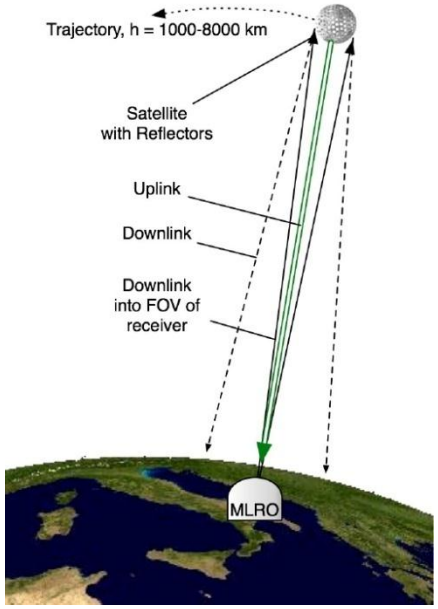




Satellite-based quantum communications terminal employing state-of-the-art technology, Pfennigbauer et al., JON **4,** 549 (2005)

Space-QUEST
Quantum Entanglement in Space Experiments
www.quantum.at/quest

Experimental verification of the feasibility of a quantum channel between Space and Earth
Villoresi et al. New Journal of Physics 10, 033038 (2008)



Key rate
Quantum communication networks

Recent developments have brought the key rate up to a few kilobits per second on long distances and megabits per second for shorter distances (1-10km)

These developments include better sources and detectors, and also important theoretical developments, such as the “decoy state” method that allow us to achieve secure QKD with more practical (i.e. farther from perfect) sources and detectors.

Why use QKD in practice?

- K. G. Paterson, F. Piper, and R. Schack (2004)
  - "Quantum cryptography: a practical information security perspective" (formerly, "Why quantum cryptography?")
  - Published in Quantum Communication and Security, Proceedings, NATO Advanced Research Workshop, edited by M. Zukowski S. Kilin and J. Kowalik, p. 175-180 (IOS Press, Amsterdam, 2007) http://arxiv.org/abs/quant-ph/0406147
- R. Alleaume, *et al.* (2007)
  - "SECOQC white paper on quantum key distribution and cryptography" http://arxiv.org/abs/quant-ph/0701168
- D. Stebila, M. Mosca, and N. Lütkenhaus (2009)
  - "The case for quantum key distribution"
  - Proceedings of QuantumComm 2009 Workshop on Quantum and Classical Information Security, Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, volume 36, page 283--296. Springer, 2010.
- D. Bernstein (2009)
  - "Cost-benefit analysis of quantum cryptography" http://www.dagstuhl.de/Materials/index.en.phtml?09311
- S. Kunz-Jacques and P. Jouquet (2011)
  - "Using hash-based signatures to bootstrap quantum key distribution" http://arxiv.org/abs/1109.2844
- L. Ioannou and M. Mosca (2011)
  - "A new spin on quantum cryptography: Avoiding trapdoors and embracing public keys" http://arxiv.org/abs/1109.3235
- M. Mosca, D. Stebila, and B. Ustaoglu (2012)
  - "Quantum key distribution in the classical authenticated key exchange framework http://arxiv.org/abs/1206.6150

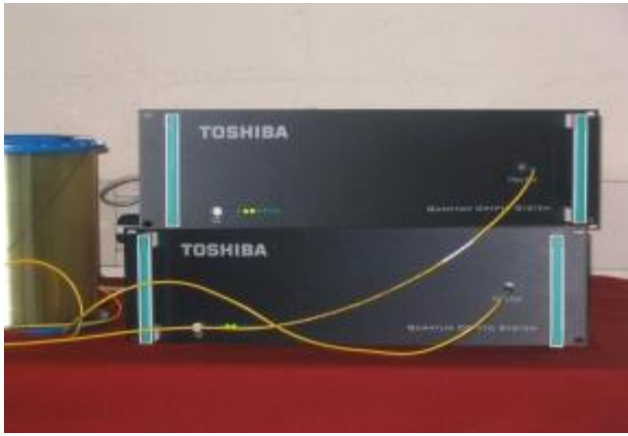
Commercial QKD products and research

MagiQ QPN™ Security Gateway

Uncompromising VPN Security™

"Quantum Cryptography: when your link has to be very, very secure."

By Bill Schweber, EDN, 12/6/05



id Quantique

A Quantum Leap For Cryptography

NEC

Empowered by Innovation

IBM

National Institute of Standards and Technology

NIST

...working with industry to foster innovation, trade, security and jobs

Telcordia