The Impact of Quantum Information Technology on Space System Security

Leo Marcus, IATD

Walter Buell, Electronics and Photonics Lab

Richard Ma, IATD

Steven Moss, Electronics and Photonics Lab

Be afraid, very afraid…

- **“There is less danger in fearing too much than too little."**
  - Sir Francis Walsingham, Elizabethan spymaster

(This is a bit too simplistic, of course…I just put it there to get your attention…)

Why

- **Quantum computation can make obsolete much of the cryptography currently in use – thus seriously compromising the security of space systems**
- **The algorithms to break asymmetric crypto (e.g. RSA) are here NOW**
- **Hardware implementation forecasts vary: 20 years is about average.**
- **However: encrypted data from the past (and present) that has been stored by an adversary will be vulnerable to decryption, whenever that happens.**

Simon says …

"… the development of a fully operational quantum computer would imperil our personal privacy, destroy electronic commerce and demolish the concept of national security. A quantum computer would jeopardize the stability of the world. Whichever country gets there first will have the ability to monitor the communications of its citizens, read the minds of its commercial rivals and eavesdrop on the plans of its enemies. Although still in its infancy, quantum computing presents a potential threat to the individual, to international business and to global security."

- *– Simon Singh in "The Code Book"*

What to do about the present and future?

- **Quantum *cryptography* has the potential to allow secret communications that are unbreakable because of the laws of physics, not the purported difficulty of computations.**
  - These methods are invulnerable to quantum computation attacks and can replace asymmetric crypto uses
  - Already in use in limited applications (financial) today.
  - Applications to high-security systems and space (presumably) under intense investigation.
- **There are non-standard "classical" (non-quantum) *asymmetric* cryptographic methods that appear to be invulnerable to quantum computation attacks.**
- **To keep using the same *symmetric* algorithms (e.g. AES) at same security level, double the key length (best quantum algorithm for symmetric crypto gives square-root speed-up)**
- **These considerations should be part of the trade space of security risk-cost-benefit – and part of NSA's Cryptography Modernization Initiative (CMI)**

What to do about the past?

- Evaluate the *required security* lifetime of all legacy encrypted data
- Evaluate progress of quantum computers
- Evaluate the *actual* life expectancy of those data
- Where possible/necessary/feasible, take remedial action to make vulnerable encrypted data obsolete (e.g. change system parameters)
- Where necessary but impossible, duck and cover

Menu

- Security
- Cryptography
- Quantum computation
- Quantum cryptography

Security Pillars

- Confidentiality (information does not leak)
- Integrity (information does not get altered)
- Availability (resources do not get denied)
- (Authentication) (people are who they say they are)
- (Non-repudiation) (people cannot deny doing what they did)

Cryptography

- **Can be used to implement preventive measures against some breaches of the security pillars**
- **Space systems rely heavily on cryptography for system security**
- **Two main categories:**
  - **Public-private key** (asymmetric: different keys for encryption and decryption)
    - Key exchange, authentication
  - **Secret key** (symmetric: same key for encryption and decryption)
    - Session encryption
- **Both categories are integrated into the cryptographic architecture of any system, depending on their advantages (performance and security)**

In a Nutshell

- ***quantum computation* (running quantum algorithms on quantum computers) has the potential for performing in mere seconds computations that are infeasible with conventional computers.**
  - This capability will directly break the most common asymmetric systems, and thereby essentially break much cryptography currently in use.
- ***quantum cryptography* promises unconditionally secure communication**
  - Security of key-distribution based on the laws of quantum physics rather than the assumption of mathematical intractability of certain "one-way" functions

Why?

- **Qcomp:**
  - Because much of the supposed security of encryption (primarily the asymmetric kind) relies on the difficulty (average time) of certain computations. (Symmetric crypto would be less severely affected.)
  - Some of these computations would become “trivial” (= quick, if not cheap…) on quantum computers.
- **Qcrypto:**
  - Because it would make eavesdropping detectable
  - Eavesdropping is ***not*** detectable in conventional cryptography

When?

- **Quantum computation: 10-30 years**
- **Quantum cryptography: now, for certain applications**

So?

- **Current and past data encrypted by a quantum-vulnerable cryptographic method that has been stored by an adversary will be decrypted in 10-30 years.**
  - This may or may not be irrelevant, bad, or horrendous, depending on the security lifetime of the specific data
- **We may have an alternate, secure cryptography based on quantum principles**

Who?

- **Many known projects at home and abroad in both Qcomp and Qcrypto**
- **Prudent to assume that there are many unknown projects also**

Q: Why introduce quantum mechanics?
A: Computations are carried out in the "real world"

- **"… nature isn't classical, dammit.…" (Richard Feynman)**
- **"I think I can safely say that nobody understands quantum mechanics." (R. F.)**
- **"Anyone who is not shocked by quantum mechanics has not understood it. " (Niels Bohr)**
- **"I do not like it, and I am sorry I ever had anything to do with it." (Edwin Schrödinger)**
- ***"*Quantum computers — devices that collaborate with nearby universes to perform useful computations." (David Deutsch, one of the founders of quantum computation)**
- **"A quantum state is not an objective property of an individual system, but is that information, obtained from knowledge of how the system was prepared, which can be used for making predictions about future measurements…" (J. Hartle, Am. J. Physics (1968))**

Quantum Computation

- A quantum computer deals with “qubits” instead of bits.
- Each qubit (coined 1995 Ben Schuhmacher of Kenyon College) represents a superposition of the states 0 and 1.
- Description of an n-qubit system requires 2^n complex numbers.
- Thus a computation performed on a qubit string of length n is like performing 2^n computations simultaneously.

Using Quantum Computation

- **Using quantum computers against asymmetric crypto (e.g. RSA)**
  - A conventional computer doing 10^10 divisions per second will take much longer than the age of the universe to factor a 100 -digit number.
  - In theory, a quantum computer can do it with the Shor quantum factoring algorithm in a matter of seconds.
- **Current record (Dec. 2001) for factoring on an actual quantum computer: 15 = 3 * 5.**
  - A billion custom-designed molecules in a test tube became a 7-qubit quantum computer
- **Easier to quantum break EC than RSA!**
  - 160 bit elliptic curve cryptographic key could be broken on a quantum computer using around 1000 qubits
  - Factoring the security-equivalent 1024 bit RSA modulus would require about 2000 qubits.

Using Quantum Computation (cont.)

- **Using quantum computers against symmetric crypto**
  - A conventional computer checking a million keys per second would take a thousand years to find a 56-bit symmetric key by brute force (assuming 2^56 = 7X10^16 possible keys)
  - A quantum computer with would take about four minutes (square-root speed-up in number of steps by Grover's algorithm)

Quantum Computer Poll

- In a slightly less than serious poll of a self-selected population of quantum computation experts conducted by Cal Tech in 2005 the question was**:**

"Quantum computers will be commonplace in --- ?"

- **And the answers were:**
  I already have a quantum computer. 27.7% - (78 Votes)
  Less than 10 years. 10.3% - (29 Votes)
  10-20 years. 21.3% - (60 Votes)
  20-30 years. 12.4% - (35 Votes)
  30+ years. 28.1% - (79 Votes)
  Total Votes: 281

Quantum Cryptography

- **Definition: any technique using the principles of quantum mechanics to provide the security to accomplish any of the tasks of traditional cryptography**
- **The principles:**
  - Measurement is not passive
  - Entanglement binds measured values
- **Uses:**
  - Quantum key distribution (QKD): first, and most important
  - Quantum digital signature

Quantum Cryptography

- **Holds the potential for making new unbreakable cryptosystems.**
- **In principle, any classical key distribution can always be passively monitored, without the knowledge of the legitimate users.**
- **Quantum cryptography can provide a method for secure key exchange over an insecure channel based on the nature of photons.** Eavesdropping cannot be prevented, but it can be detected**.**
- **Photons have a polarization, which can be measured in any basis, where a basis is any two directions orthogonal to each other.**
- **If a photon's polarization is read in the same basis twice, the polarization will be read correctly and will remain unchanged.**
- **If it is read in two different bases, a random answer will be obtained in the second basis, and the polarization in the initial basis will be changed randomly.**

Nice quote from Mermin on QKD

- Pause to savour the strange character of this situation. Nobody has figured out how to exploit quantum mechanics to provide a secure means for directly exchanging meaningful messages. The secure exchange is possible only because the bit sequences are random. On the face of it one would think nothing could be more useless than such a transmission of noise. What is bizarre is that human ingenuity combined with human perversity has succeeded in inventing a context in which the need to hide information from a third party actually provides a purpose for such an otherwise useless exchange of random strings of bits.
  - **David Mermin, Lecture Notes on Quantum Computation, Cornell 2005**

Desirable QKD Attributes

- Confidentiality – good
- Authentication – weak
- Rapid key delivery – depends
- Robustness (strength against accidental or deliberate denial of service) – could be improved
- Distance and location independence – weak
- Resistance to traffic analysis -- weak

Quantum Crypto Summary

- **Quantum key exchange for use by one-time pad or symmetric cipher is very secure**
  - BB84 uses polarization; other protocols use entanglement
- **Of course, there are potential attacks, for example, if standard asymmetric crypto is used to authenticate Alice and Bob…**
- **Security depends on technological level of adversary only at the time of the key exchange, in contrast to complexity-based systems which can be broken by future developments.**
- **There is much ongoing experimental work in developing such systems.**
- **Main question is whether quantum cryptography will arrive in time to save us from quantum computers.**

Recent Developments:

The state of the art (research and technology) is changing rapidly!

- Quantum keys have been transmitted over distances on the order of 7 km in the air (China, April 05), showing feasibility of satellite quantum crypto
- or 70 km via optic fiber
- 256-bit key can be changed 4 times per second via QKD
- There are recent "polarization-insensitive" methods to perform quantum key distribution that allow photon detection to be performed very accurately over long distances.
- So-called quantum internet could connect distributed elements in a quantum computer.
- http://www.quantenkryptographie.at/

  Bank Transfer via Quantum Cryptography Based on Entangled Photons, 21 April 2004, Vienna

More recent developments

- A group at Harvard has measured the decoherence time for a singlet state to be about 10 nsec. They also used a spin echo technique from NMR to stave off decoherence for 1 microsecond. They claim "…if a further factor of 10 could be obtained, and if the qubit could be controlled with the gigahertz clock speeds of today's fastest microprocessors, then coherence would last long enough to meet a key benchmark: the ability to perform 10,000 operations."
- Quantum cryptographic protocols are so secure because they may detect eavesdropping. Nonetheless, with the new tool QI telecloning, the identity and location of the eavesdropper could be guaranteed uncompromised

And more

- **"In-Band Quantum Key Distribution (QKD) on Fiber Populated by High-Speed Classical Data Channels." OFC/NFOEC conference in Anaheim, CA March 7, 2006**
- **MagiQ/Verizon collaboration**
  - bridged two separate spans of 80km by cascading a number of MagiQ's QPN 7505 devices. The commercial fiber network is made up of spans, typically 80km, linked together to complete metro area networks and long haul networks. Cascading of quantum cryptography devices enables the deployment of quantum cryptography throughout the telecommunications network
  - demonstrated that quantum keys can be mixed with other optical signals on one strand of fiber. Previously, quantum cryptography devices required a dedicated dark fiber strand, which is costly and not always available, for the transmission of quantum keys. The multiplexing of quantum keys with data on one strand significantly reduces the cost of deploying quantum cryptography.
  - “Practical deployments of quantum cryptography are now feasible for highly secure communications for service providers, banks, and the military.” – Press Release

Audio/Video Resources

- David Deutsch, Lectures on Quantum Computation: http://www.quiprocone.org/Protected/DD_lectures.htm
- Many luminaries, Lectures on Quantum Computation: http://www.fields.utoronto.ca/audio/00-01/