What can Quantum Cryptographers Learn from History?

Kenny Paterson
kenny.paterson@rhul.ac.uk

Information Security Group
Royal Holloway, University of London

0. Preface

Royal Holloway
University of London

- According to *MIT Technology Review*, in 2003, QC was one of:

  "*10 Emerging Technologies That Will Change the World.*"

- According to Dr. Burt Kaliski, chief scientist at RSA Security (and now a member of MagiQ's Scientific Advisory Board):

  "If there are things that you want to keep protected for another 10 to 30 years, you need quantum cryptography."

Quantum Cryptography

Royal Holloway
University of London

- QC offers unconditional security.
  - Security based only on the correctness of the laws of quantum physics.
- Often contrasted with security offered by public key cryptography.
  - Vulnerable to quantum computers.
  - Vulnerable to algorithmic advances in factoring, discrete logs, etc.

Quantum Cryptography

Royal Holloway
University of London

- QC is often promoted as *the* alternative to public key cryptography for the future.
- For example:

> *"Quantum cryptography offers the only protection against quantum computing, and all future networks will undoubtedly combine both through the air and fibre-optic technologies"*

Dr. Brian Lowans,

Quantum and Micro Photonics Team Leader, QinetiQ.

Quantum Cryptography

Royal Holloway
University of London

- Another example:

"All cryptographic schemes used currently on the Internet would be broken…."

Prof. Giles Brassard,
Quantum Works launch meeting,
University of Waterloo,
27th September 2006.

This Talk

Royal Holloway
University of London

- The road-side of cryptography is littered with the abandoned wrecks of systems that turned out to be insecure in practice (even when secure in theory).

- What lessons can the quantum cryptography community learn from this history?

Learning from History

Royal Holloway
University of London

"Those who cannot learn from history are doomed to repeat it."

George Santayana, *Reason in Common Sense*, The Life of Reason, Vol. 1.

"You must learn from the mistakes of others. You can't possibly live long enough to make them all yourself."

Sam Levenson

Overview

Royal Holloway
University of London

1. Security proofs and their limitations
2. Theory and practice in cryptography
3. Side-channel analysis
4. Key management
5. The need for dialogue
6. Why does this matter to quantum researchers?
7. Closing remarks

1. Security Proofs and Their Limitations

Royal Holloway
University of London

- Security proofs can be very valuable in assessing the security offered by cryptographic schemes.
- Typical approach in the provable security paradigm:
  - Define (generically) the functionality of the scheme.
  - Define the capabilities of an adversary in terms of a game with a challenger.
  - Propose a concrete scheme.
  - Provide a proof that any adversary against the scheme can be transformed into an algorithm to break some computational problem.
  - Transformation via undetectable simulation of the challenger.

Provable Security

Royal Holloway
University of London

- Assume that the computational problem is well-studied and as hard as we believe it to be.
- Then, applying the contra-positive: no adversary can exist.
- A refinement:
  - Relate the adversary's advantage and running time *(Adv,t)* to the success probability and running time *(p,t')* of an algorithm to solve the underlying computational problem.
  - Concrete security analysis.

Limitations

Royal Holloway
University of London

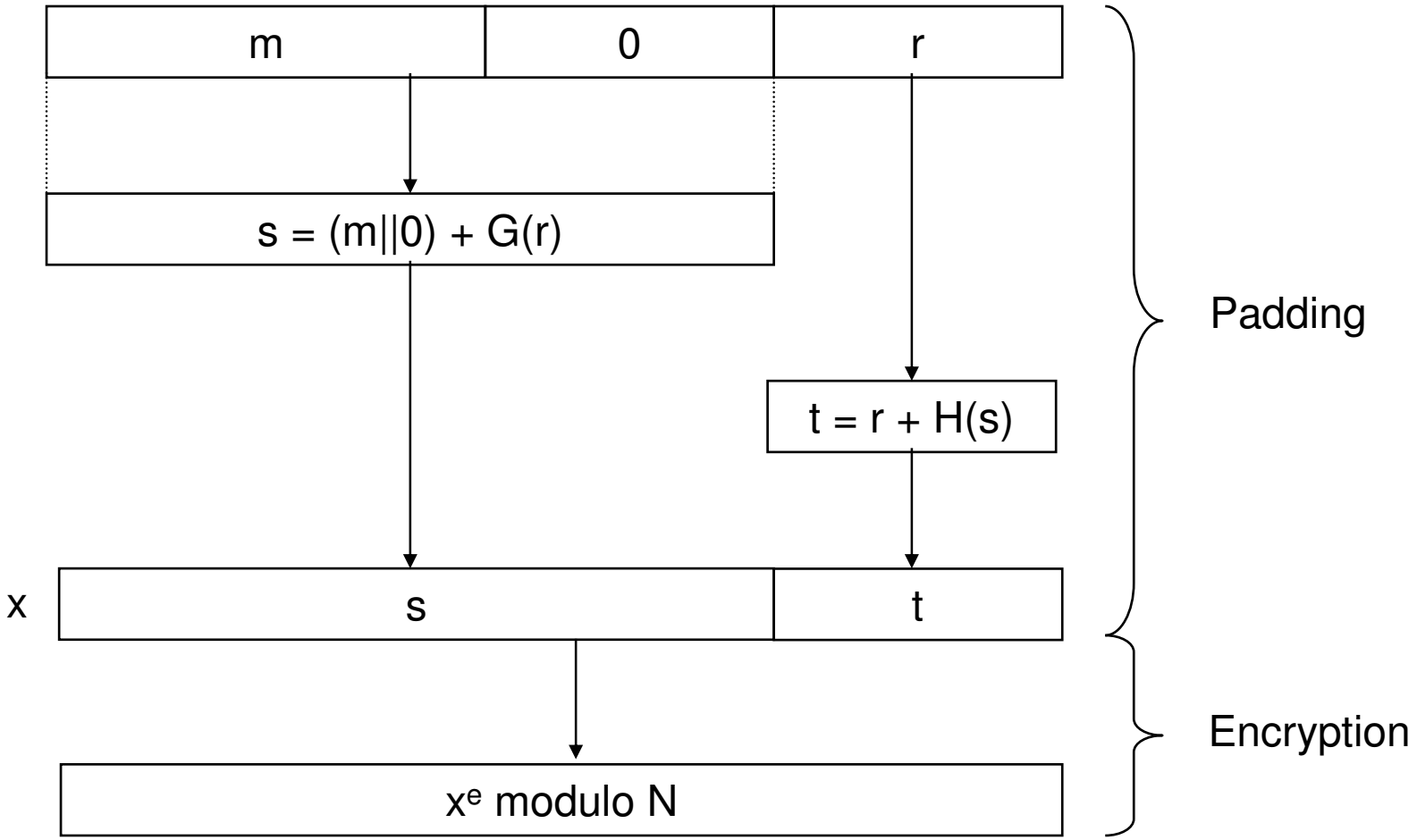
- This approach has its limitations:
  - The proof of security may not be correct.
  - The reduction from the adversary to the computational problem may not be “tight”, so the proof of doubtful meaning in practice.
  - (The model of security may not be comprehensive enough to take into account all practical attacks.)
  - (The security proof may not compose well with further protocols to produce a secure system.)
- The two following examples come from a series of studies by Koblitz and Menezes.

Example 1: RSA-OAEP

Royal Holloway
University of London

- RSA-OAEP:
  - RSA = RSA!
  - OAEP = Optimal Asymmetric Encryption Padding
  - A method for transforming “raw” RSA encryption into a method offering suitably strong security guarantees.
  - Solving a long-standing open problem.
  - Proposed and proved secure by Bellare and Rogaway (1994).
  - Widely standardised (e.g. in SET).

Example 1: RSA-OAEP



Example 1: RSA-OAEP

Royal Holloway
University of London

- Bellare and Rogaway (1994) proved that an adversary who can break RSA-OAEP (in a well-defined and strong sense) can solve the RSA-inversion problem.
- Proof actually works for *any* trapdoor one-way function.
- The proof was well-written, the construction simple and the result was rightly celebrated.

Example 1: RSA-OAEP

Royal Holloway
University of London

- But Shoup (2001) discovered a flaw in Bellare and Rogaway's proof.
- The proof was in the literature for seven years before the problem was spotted.
- Fortunately, Shoup and Fujiskai *et al.* were able to repair the proof.
- Simpler constructions and tighter proofs were subsequently discovered.
- **Proofs are not static objects.**

Example 2: Blum-Blum-Shub

Royal Holloway
University of London

- Blum-Blum-Shub pseudo-random bit generator:
  - N =pq is an RSA modulus with p,q = 3 mod 4.
  - Initial seed x_0
  - $x_i = (x_{i-1})^2 \mod N$
  - Output the j least significant bits of x_i
- The larger j is, the faster we can generate bits.
- **Security result**: assuming factoring N is intractable, j=O(loglogN) bits can be securely extracted per iteration.
  - Vazirani and Vazirani; Alexi, Chor, Goldreich and Schnorr; Fischlin and Schnorr; Sidorenko and Schoenmakers.

Example 2: Blum-Blum-Shub

Royal Holloway
University of London

- IETF RFC 1750 (Eastlake *et* al.) states:

  "If you use no more than the $log_2 log_2(x_i)$ low order bits, then predicting any additional bits from a sequence generated in this manner is provable [sic] *as hard as factoring N."*
- Is this statement justified by the security proof?

Example 2: Blum-Blum-Shub

Royal Holloway
University of London

- Analysis by Koblitz and Menezes:
  - Take the best bounds on security and hardness of factoring known in the literature.
  - Apply them for j=9 and N with 768 bits, extracting $M=10^9$ bits from the generator.
  - Allowing a success probability of 0.01 for the adversary, what is the time bound on the adversary?
  - Answer: 2^{-264}
  - Yes, that is a negative sign in the exponent!
- **Concrete security analysis does not always give us results that are useful in practice.**

Lessons for Quantum Cryptography

Royal Holloway
University of London

- We also model adversarial capabilities and provide mathematical proofs for quantum protocols.
- Those models and proofs evolve too.
  - For example, initial proofs of security for QKD only considered limited attack scenarios and perfect devices.
  - Early proposal for quantum bit commitment?
- What value does a claim of unconditional security have in this evolving context?

Lessons for Quantum Cryptography

"If it's provably secure, it's probably not"

Lars Knudsen

2. Theory and Practice

Royal Holloway
University of London

A show of hands please:

Question:

Does using the one-time pad to encrypt provide confidentiality?

Answer:

Of course it does! Shannon told us that!

2. Theory and Practice

Royal Holloway
University of London

A show of hands please:

Question:

Does using the one-time pad to encrypt provide confidentiality?

A better answer:

It depends on the adversary's capabilities and on the system characteristics.

IPsec

Royal Holloway
University of London

- IPsec: a suite of protocols for providing security to IP packets.
- Widely used in Virtual Private Networking systems.
- Also used today in some quantum cryptographic products.
- Standardised by IETF in:
  - RFCs 2401-2411 (second generation)
  - RFCs 4301-4309 (third generation)
    - More than 200 pages of documentation.

Encryption in IPsec

Royal Holloway
University of London

- ESP = Encapsulating Security Protocol.
- IPsec's protocol for providing confidentiality.
- Defined in RFCs 2406 and 4303.
- Encrypts and *optionally* integrity-protects IP packets.
  - Typically using CBC-mode of a block cipher such as AES or DES for encryption.
  - HMAC-SHA-1 or HMAC-MD5 for integrity protection.

Theory and Practice

Royal Holloway
University of London

- It is very well-known in the theoretical community that encryption on its own is not sufficient to provide a confidentiality service.
- Bellovin (1995, 1996) provided attacks “on paper” showing that ESP is potentially insecure without some form of integrity protection.
- Attacks recognised in versions 2 and 3 of the ESP standard.

Encryption in IPsec

Royal Holloway
University of London

- RFC 2406 includes HMAC to provide integrity protection/data origin authentication.

  "… use of confidentiality without integrity/ authentication … may subject traffic to certain forms of active attacks that could undermine the confidentiality service (see [Bel96])"

- But the RFC still requires that implementations **MUST** still support "encryption only" mode.

Encryption in IPsec

Royal Holloway
University of London

- RFC 4303 no longer requires support for encryption-only ESP.
- And gives strong warnings about Bellovin's attacks.
- But:

  "ESP allows encryption-only … because this may offer considerably better performance and still provide adequate security, e.g., when higher layer authentication/integrity protection is offered independently."

IPsec in Theory and **Practice**

Royal Holloway
University of London

- Developers are *required* by RFC 2406 to support encryption-only ESP.
- Developers rarely pass RFC warnings to end users.
- End users don't read RFCs or technical papers.
- End users might reasonably assume that encryption on its own gives confidentiality.
- Many on-line tutorials do not highlight the dangers of encryption-only IPsec.

IPsec in Theory and **Practice**

Royal Holloway
University of London

- From the IPsec Tunnel Implementation administrator's guide of a well-known vendor:

  "If you require data confidentiality only in your IPSec tunnel implementation, you should use ESP without authentication. By leaving off the authentication service, you gain some performance speed but lose the authentication service."

  http://www.cisco.com/en/US/products/sw/cscowork/ps3994/products_user_guide_chapter09186a00801f596a.html (last accessed 19/5/2006).

Attacking the Linux Implementation

Royal Holloway
University of London

- Paterson and Yau (Eurocrypt 2006) showed that encryption-only ESP is disastrously weak.
- **Headlines**: we broke the Linux kernel implementation of encryption-only ESP:
  - A ciphertext-only attack.
  - AES in CBC-mode.
  - Attack takes 1.4s to recover first plaintext.
  - Near real-time plaintext recovery thereafter.
- Attacks even easier if OTP used in place of CBC-mode.
  - Attacks work by manipulating ciphertext to effect changes to underlying IP packets.
  - Changes produce errors or packet re-routing, revealing plaintext information.

Lessons

Royal Holloway
University of London

- The attacks indicate poor lines of communication between theoreticians, standards developers, implementers and end-users.
- The security message gets “lost in translation”:
  - Backwards compatibility over-rides security.
  - Security-critical checks are left unimplemented.
  - Warnings in RFCs are never seen by users.
  - Ill-informed on-line tutorials.

Lessons for Quantum Cryptography

Royal Holloway
University of London

- Practice often ignores theory.
  - Do QKD vendors remember to switch on some kind of integrity protection?
  - Do they prevent users from switching it off again?
- The lines of communication in the quantum community are currently quite short.
  - Efforts such as QuantumWorks should help keep them so.
  - Research scientists actively engaged with, employed by, or founding QIP companies.
  - Do theorists and experimentalists converse enough?
- The chain may become more stretched as the technology matures and is commoditised/ standardised.

3. Side-channel Analysis

Royal Holloway
University of London

- IPsec example showed that adding integrity protection to encryption is necessary for security.
- Unfortunately, this is not sufficient…
- SSL/TLS:
  - The protocol of choice for e-commerce (and more!)
  - The protocol most people seem to be referring to when discussing the impact of quantum computers on Internet security.

Side-channel Analysis of SSL/TLS

Royal Holloway
University of London

- SSL/TLS uses symmetric cryptography as the workhorse for bulk data protection.
- The plaintext data is integrity-protected first, then encrypted.
- Typically using the HMAC algorithm and a block cipher in CBC-mode.
- This combination was proven secure in an appropriate model by Krawczyk (Crypto 2001).

Side-channel Analysis of SSL/TLS

Royal Holloway
University of London

- Vaudenay (Eurocrypt 2002) introduced the notion of a padding oracle attack.
  - CBC mode operates on blocks of data.
  - Plaintext first needs to be padded with redundant data to make it fit into blocks.
  - A padding oracle tells an attacker whether or not a ciphertext was correctly padded.
  - Vaudenay showed that an attacker can leverage such an oracle to decrypt arbitrary ciphertexts.
    - Provided the oracle is available.
    - For certain padding schemes in CBC mode.

Side-channel Analysis of SSL/TLS

Royal Holloway
University of London

- Canvel *et al.* (Crypto 2003) showed that SSL/TLS as implemented in OpenSSL reveals a padding oracle.
  - Time difference in generation of error messages for failure of padding and failure of MAC (checked later than padding).
  - Error messages are in encrypted form and only differ in time by a few milliseconds.
  - Still enough of a cryptanalytic toe-hold to allow recovery of static authentication credentials in SSL/TLS-protected sessions.

Side-channel Analysis of SSL/TLS

- We have a security proof, so what went wrong?
- An example where the model in which the proof holds is not sufficiently broad to capture all practical attacks.
- And an example of open-source security software not necessarily being better than closed-source.
  - Also shown by our IPsec example, and by work of Nguyen analysing GNU Privacy Guard (Eurocrypt 2004).

Lessons for Quantum Cryptography

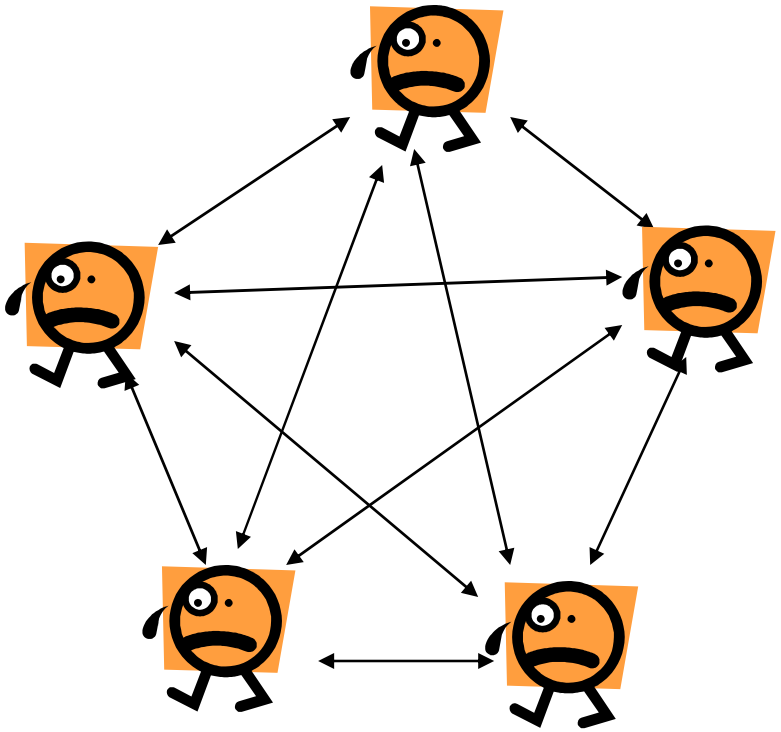
Royal Holloway
University of London

- Security proofs rarely tell the whole story.
  - Systems tend to be far more complex than the set of behaviours captured in a model.
- Watch out for unanticipated side-channels when implementing:
  - Error conditions
  - Timing
  - Power consumption
  - EM radiation
  - ???
- Attacks “outside the model” have already been proposed for QC systems.

4. Key Management

Royal Holloway
University of London

Brassard's "quadratic curse":



Key Management

Brassard's "quadratic curse":

n parties who wish to engage in pairwise secure communication need $n^2/2$ symmetric keys to be pre-distributed.

This is troublesome even for 2 parties and 1 key!

The perceived beauty of QKD:

QKD solves the problem of key distribution. Thus it overcomes the quadratic curse.

Key Management

Royal Holloway
University of London

- Current QKD protocols require an authentic channel for public discussion.
  - Without this channel, MITM attacks are trivial.
- Everybody knows this (even if they sometimes forget to say it), but what are the consequences?

- To build an unconditionally secure authentic channel, we (in practice) require a symmetric key to be pre-distributed to every pair of communicating parties.
  - Use it in, say, the Wegman-Carter MAC.
- Once we have this key, we can stretch it to arbitrary length, with unconditional security.

An Inconvenient Truth

Royal Holloway
University of London

- QKD does not solve the key distribution problem at all.
  - It also suffers from the quadratic curse in thin disguise.
- Just like today's systems, QKD needs good key management to:
  - Get the symmetric keys in place.
  - Protect them during their lifetime.
  - Handle synchronisation and updates to keys.
  - Cater for their eventual expiry and safe destruction.
  - And now we can't use public key techniques to help us (if we want to claim unconditional security).
- Key management is generally difficult and costly, and sometimes poorly understood.

Example 1: WEP in IEEE 802.11b

Royal Holloway
University of London

- WEP = Wired Equivalent Privacy
- Part of IEEE 802.11b wireless LAN standard.
- WEP deployed in millions of wireless laptops and access points.
- One approach to lifting the quadratic curse…

The WEP Fiasco

Royal Holloway
University of London

- All parties in a network use the same key.
- The same key and the same algorithm are used for both entity authentication and encryption.
- Use a CRC as the integrity mechanism in combination with stream cipher encryption.
- Use a 24-bit initialization vector (IV) for the stream cipher.
- Combine the IV with the shared key in an insecure manner.
  - Fluhrer, Mantin and Shamir attack, as implemented in WEPcrack.
- Provide only manual mechanisms for setting and updating keys.

Example 2: GSM

Royal Holloway
University of London

- GSM = Groupe Systeme Mobile/Global System for Mobile Telecomms.
- Developed by ETSI in early 1980's.
- Now deployed in 200+ countries, 1 billion+ subscribers.

- 128-bit unit key embedded in tamper-resistant SIM card and in Authentication Centre (AuC).
  - Requires secure manufacturing plant, physically secure AuCs, secure delivery of media containing key batches.
- AuC assists local mobile network to:
  - Authenticate SIM.
  - Establish symmetric key for encrypting voice traffic on wireless link from handset to base-station.

GSM Security Architecture

Royal Holloway
University of London

- GSM uses a symmetric key hierarchy.
  - Unit key used for SIM authentication.
  - Encryption key securely derived from unit key and random number during authentication protocol.
  - No public key cryptography.
- GSM security architecture has no known major weaknesses.
  - Though algorithms showing signs of age.
- Deployed at very large scale.
- Smooth evolution to (UMTS) 3g security architecture.

GSM vs WEP

Royal Holloway
University of London

- Security as part of design at outset vs security as an afterthought.
- Security by experts vs security by enthusiasts.
- Security by economic necessity vs security as someone else's problem.
  - Need to protect operators' investment in bandwidth vs unregulated spectrum.
- Security through careful key management vs insecurity through no key management.

Lessons for Quantum Cryptography

Royal Holloway
University of London

- Good key management is at least as hard as good cryptography.
- QKD does not significantly simplify key management.
- QKD can benefit from everything we've learned over the years about building large-scale authentication architectures:
  - GSM/UMTS, banking networks, Kerberos systems if we want QKD with unconditional security.
  - EMV, X.509 & SSL/TLS if we want to use PKI.

Lessons for Quantum Cryptography

Royal Holloway
University of London

- Quantum cryptography is *not* the only solution to the threat of quantum computers.
  - Because quantum computers do not significantly dent symmetric systems.
  - Simply use 256-bit AES to frustrate Grover: still 2^{128} effort for key search.
  - Use a key hierarchy to limit the exposure of individual keys.
  - Not unconditionally secure, but pragmatic.
    - Main risk is a severe cryptanalytic attack on AES.
    - So use the 5 AES competition finalists in sequence if you are really conservative.

Lessons for Quantum Cryptography

Royal Holloway
University of London

- Security in the real world is driven by economics:
  - What is the value of the information we need to protect?
  - What is the risk of its being compromised?
  - What is the minimum amount we need to spend to reduce that risk to an acceptable level?
- With this kind of analysis, there seem to be few applications where the benefits of QKD justify its currently high costs.
  - Because we can achieve “good enough” security using existing approaches.
  - Because QKD currently faces several severe obstacles to widespread deployment.
  - Because QKD may not offer unconditional security in practice.
- But don’t stop trying!

5. The Need For Dialogue

Royal Holloway
University of London

- What is *classical* cryptography?
- Two possible answers:
  - Everything in cryptography that is non-quantum.
  - Everything in cryptography prior to Shannon.
- The “two cultures” do not even agree on the meaning of this simple term.

- Note that I have not used the term in this talk!

Statements Overheard Recently

Royal Holloway
University of London

"If you don't change keys often enough, brute force attacks become much easier for an attacker."

"The cost of factoring grows exponentially with the number of digits on a classical computer."

"All cryptographic schemes used currently on the Internet would be broken…"

The Need for Dialogue…

… should by now be obvious!

The Need for Dialogue

Royal Holloway
University of London

But the dialogue needs to extend far beyond the immediate cryptographic community, to include:

- Security engineers.
- The security industry and potential users of the technology.
- Government and standardisation bodies.
- The media.

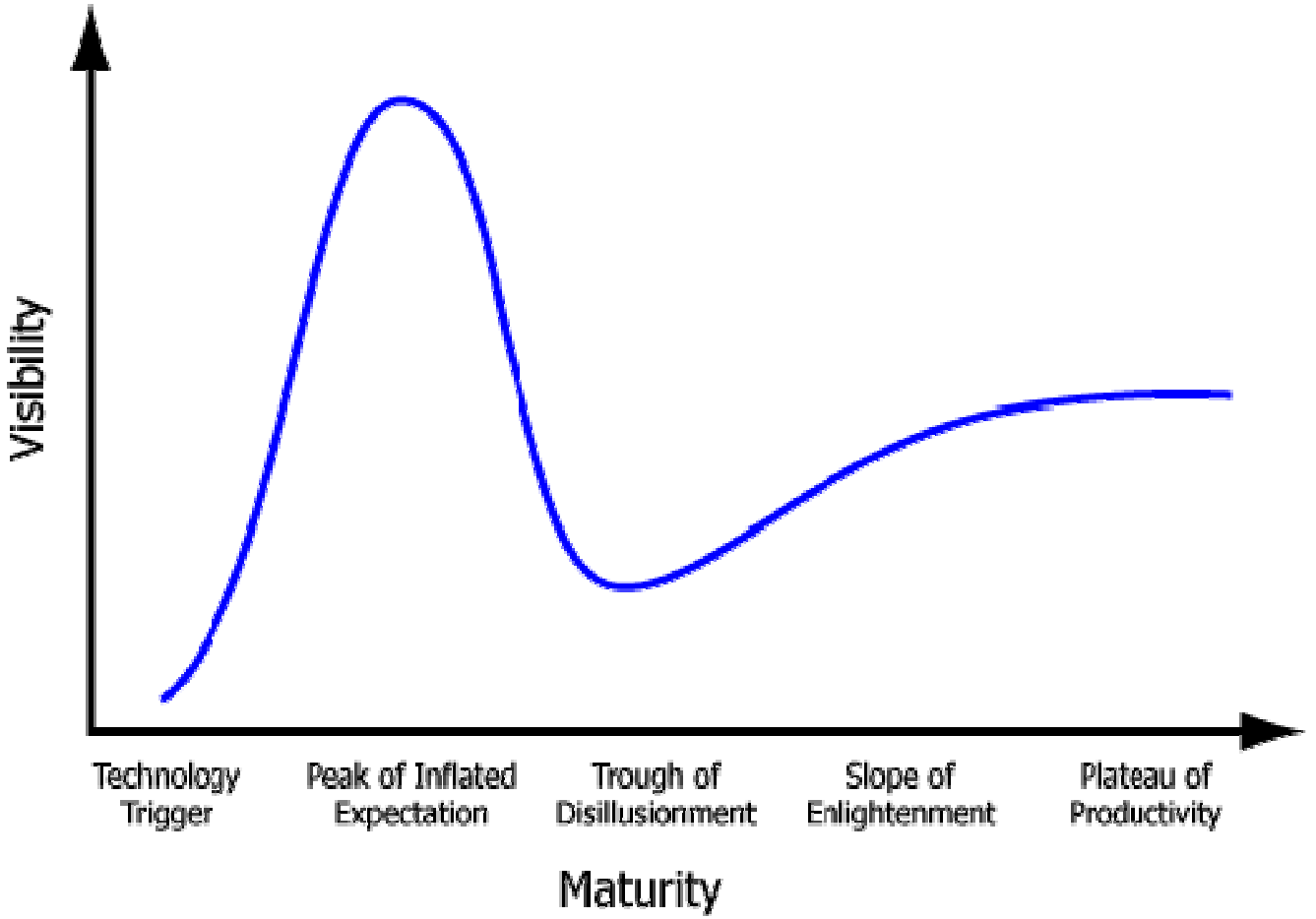
This dialogue is getting underway…

6. Why Does This Matter to Researchers?

Royal Holloway
University of London

- Impressive experimental and theoretical progress.
- Quantum cryptography promises much, but is only just taking its first hesitant commercial steps.
- Many issues that are not “fundamental science” in nature now need to be resolved.
- Quantum cryptography may be in danger of being over-hyped.
- And hype is often followed by backlash.

Gartner's Technology Hype Cycle



Hype

- Hype helps to create interest, investment and eventual market acceptance for a technology.
- Hype in the Information Security arena also creates an attractive target for hackers.
  - Oracle's "unbreakable" claims.
- The bigger the hype, the harder the fall.
  - Whether or not the attack is against an unconditionally secure quantum component of a system.

Hype

Royal Holloway
University of London

"To knock a thing down, especially if it is cocked at an arrogant angle, is a deep delight of the blood."

George Santayana

A deliberately provocative personal opinion, to get the panel discussion going:

Because of the high expectations that have now been created, the future well-being of the greater field of QIP is largely dependent on QKD being a success in the short-term.

So is the community putting its money on the wrong horse?

7. Closing Remarks

Royal Holloway
University of London

- Quantum cryptography does not work in a vacuum!
  - Cryptography plays a small, yet important, role in building secure systems.
- Do not under-estimate the complexity gap between designing *protocols* that are unbreakable in *theory* and building *systems* that are secure in *practice.*
- Cool-headed evaluation is needed to assess the commercial prospects for quantum cryptography.
  - Is unconditional security really needed?
  - Is it even achievable?

Acknowledgements

- Analysis in Section 1 from a recent paper by Neal Koblitz and Alfred Menezes (http://eprint.iacr.org/2006/229)
- Analysis in Section 4 extracted from joint paper with Fred Piper and Ruediger Schack (http://eprint.iacr.org/2004/156)