Post Quantum Cryptography

Kenny Paterson

Information Security Group

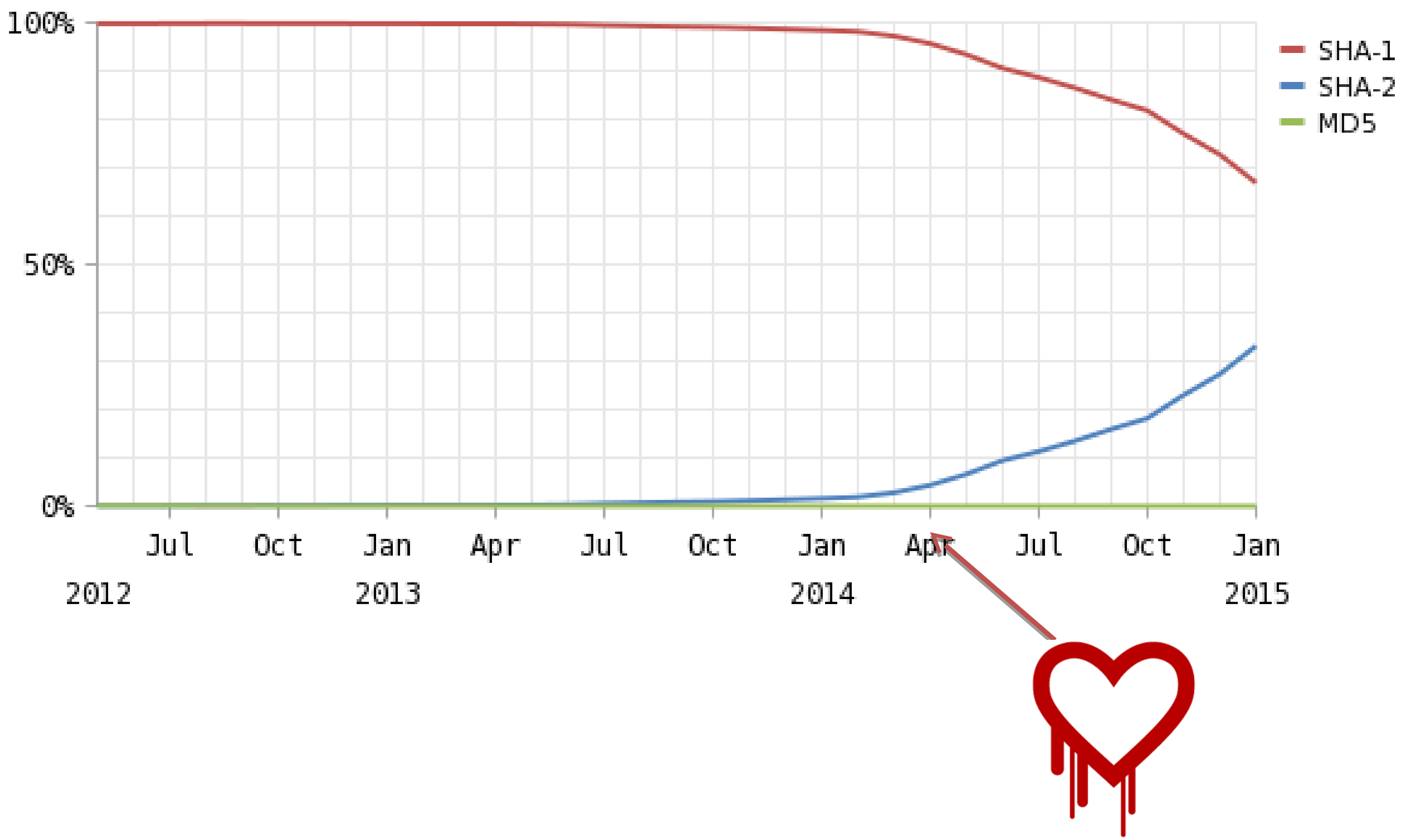
@kennyog

ROYAL HOLLOWAY UNIVERSITY OF LONDON

Lifetime of a Hash Algorithm – SHA-1

- 1995: SHA-1 published (NIST, tweak of 1993 SHA-0 design)
- 1990s: (various attacks on SHA-0, validating switch to SHA-1)
- 2001: SHA-2 published by NIST.
- 2005: Collision attack for SHA-1, estimated at 2^{63} hash operations (Wang et al.).
- 2005 – now: various claims and counter-claims about improvements.
- 2006: NIST deprecates SHA-1 from 2010 by federal agencies for all new applications requiring collision-resistance.
- 2013: Microsoft annonces SHA-1 deprecation from 2016 for new code signing certs.
- 2014: Still no collisions, best estimate is 2^{61} hash operations (Stevens).
- 2015: free-start collisions on SHA-1 using 10 days on a 64-GPU cluster.
- 2017: SHA-1 is still used widely, CAs still resisting removing it entirely.
- 2017 (Feb): first collisions in SHA-1 finally announced, 6.6k core years of computation.
- …

Netcraft Survey – Uptake of SHA-2 in Browser-Trusted Certificates



Progress in Quantum Computing

http://en.wikipedia.org/wiki/Timeline_of_quantum_computing

Pre 1994: isolated contributions by Wiesner, Holevo, Bennett, etc.

1994: Shor's algorithm – breaks discrete log and factoring problems with poly many gates and depth.

1996: Grover's algorithm – quadratic speed up for search problems, applicable to exhaustive key search.

1998: 2-qubit and 3-qubit NMR

2000: 5-qubit and 7-qubit NMR.

2001: The number 15 is factored!

2005: qbyte announced (8 qubits?)

2006: 12 qubits.

2007: 28 qubits.

(D-Wave: quantum annealing machine)

2008: 128 qubits.

2011: 14 qubits.

2012: The number 21 is factored!

2013 - 2017: ???

Late 2016 onwards: physicists switch focus to **quantum supremacy** as their success metric.

2017: D-Wave 2000Q, with 2000 qubits; IBM unveils 17-qubit machine; Google, MSR doing cool stuff.

(Weak) Analogies

- The threat of large-scale quantum computing is *weakly analogous* to the threat of a break-through in SHA-1 collision finding.
  - Breakthrough might be imminent, but then again it might not.
  - Hard to quantify risk that it will happen, and hard to put time-frame on it.
  - Meaningful results would have substantial impact.
  - Smart people are working on it and have had a lot of research investment.
  - (There are different physical approaches being pursued.)

- On the other hand, maybe QC is a bit like fusion research?
- Some conversations I've been party to:
  - "Large scale QC is only a decade away".
  - "In terms of fundamental physics …. we're pretty close to what we need. There's just tonnes of engineering work…"
  - To break 1024-bit RSA would need ca 250M qubits – Evan Jeffrey , Google/UCSB, RWC 2017.

The Coming Crypt-Apocalypse?

- We don't know if there will be a QC scaling breakthrough or not.
- If one comes, it would be fairly catastrophic – a Crypt-Apocalypse.
    - Shor's algorithm imperils all public key crypto deployed on the Internet today.
    - ECC likely to break sooner than RSA!
    - Capture interesting DH exchanges now, break them later.
- We would expect some warning of impending disaster.
- But replacing crypto at scale takes time.
- And traffic captured now could be broken later, so it's a problem **today** if you have data that needs to be kept secure for decades.

Ways Forward?

Ways Forward – PQC

- Conventional public-key cryptosystems that resist known quantum algorithms.
  - Area is called Post Quantum Cryptography, or PQC.
  - (Some terminological confusion, e.g. quantum-safe, quantum-immune.)
  - Main candidates are lattice-based, code-based, non-linear systems of equations, elliptic curve isogenies.
  - Possibly vulnerable to further advances in quantum algorithms.
  - cf. Soliloquy paper (GCHQ/NCSC); Eldar & Shor quantum algorithm for LWE (now withdrawn).
  - Even conventional security is not yet well understood in all cases.
  - Notable exception: hash-based signatures schemes are particularly mature – XMSS, SPHINCS.

Ways Forward – PQC

- PQC characteristics
  - Current PQC schemes are generally not as performant as pre-quantum schemes.
  - Typically larger public keys, larger key exchange messages/ciphertexts.
  - Particularly challenging to deploy in low-power/wireless/IoT.
  - Often faster cryptographic operations – just matrix multiplication plus noise in some cases.
  - Performance may suffer even more as we refine our understanding of how to choose parameters for security.
    - Better attacks implies larger parameters are needed.
    - Or, eventually, abandonment of a particular approach.
  - Parameter selection is a more complex question than for RSA/ECC.
    - Or: we are where we were for RSA in about 1982.

Ways Forward – PQC

- PQC is rapidly progressing from research towards standardisation and deployment.
  - Facebook Internet Defense Prize (2016) awarded to the NewHope lattice-based key exchange protocol.
  - Experimental deployment of NewHope by Google in SSL/TLS.
  - https://www.imperialviolet.org/2016/11/28/cecpq1.html
  - Increasing amount of **mainstream** crypto research.

Ways Forward – PQC

NIST process, 2016 – 2023(ish) for standardising post-quantum public key algorithms.

- http://csrc.nist.gov/groups/ST/post-quantum-crypto/
- Deadline for submissions is Nov 30, 2017
- **Evaluation criteria**: security, cost, flexibility/simplicity/adoptability.
- **Process (5-7 years)**:
  - First conference (Feb. 2018)
  - 12-18 month evaluation period – public and NIST staff.
  - Second conference.
  - (Optional tweaking.)
  - 12-18 month evaluation period.
  - Third conference.
  - Publication of report and portfolio OR decision for further evaluation.

But What About Quantum Cryptography?

- Quantum Key Distribution promises **unconditional** security.
  - “Security based only on the correctness of the laws of quantum physics”.
  - Unclear how resilient this is to progress in physics, but lets not worry about that too much…
- Often contrasted with security offered by currently deployed public key cryptography.
  - PKC is vulnerable to quantum computers.
  - PKC is vulnerable to algorithmic advances in conventional algorithms for factoring, discrete logs, etc.

QKD

QKD is often promoted as *the* alternative to public key cryptography for the future.

“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.

QKD

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.

QKD

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

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

According to Dr. Burt Kaliski Jr., then chief scientist at RSA Security, current CTO at Verisign:

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

QKD

These examples are all taken from a presentation I gave **10 years ago** (at the Fields Institute, University of Toronto).

So what's the big hold up? Four reasons:

1. QKD does not actually do what it says on tin.
2. QKD has limits on rate and range.
3. Security in theory does not equal security in practice.
4. QKD does not offer significant practical security advantages over what we can currently do at low-cost with conventional techniques.

QKD or PQC? The NCSC/GCHQ View

National Cyber Security Centre

Search

Guidance | Threats | Incident Management | Marketplace | Education & Research | Insight

Home

Quantum key distribution

Created: 04 Oct 2016
Updated: 04 Oct 2016

This white paper describes our current position on quantum key distribution (QKD). QKD is an approach to key distribution that relies on the properties of quantum mechanics to provide security.

Executive summary

Specifically, this paper:

- explores the limitations of QKD systems, including security concerns
- makes the case for research into developing post-quantum public key cryptography as a more practical and cost-effective step towards defending real-world communications systems from the threat of a future quantum computer

QKD or PQC? The NCSC/GCHQ View

Summary

QKD:

- has fundamental practical limitations
- does not address large parts of the security problem
- is poorly understood in terms of potential attacks

By contrast, post-quantum public key cryptography appears to offer much more effective mitigations for real-world communications systems from the threat of future quantum computers.

Full NCSC whitepaper online at:

https://www.ncsc.gov.uk/information/quantum-key-distribution

What Should IETF Do?

- CFRG has done some useful work on developing IDs for hash-based signatures.
  - draft-irtf-cfrg-xmss-hash-based-signatures-09
  - draft-mcgrew-hash-sigs-07
  - Mature, well-understood area, less risky in security terms.
- Other post-quantum schemes are still in their difficult teenage years in research terms.
  - Never mind standardisation and deployment experience.
- NIST's announced process is where the action will be.
  - NIST have the resources needed to run a proper process.
  - The scientific experts will be concentrating their efforts there.

What Should IETF Do?

My personal view:

- IETF should wait for NIST's process to run its course.
- But we should be ready to roll-over to new algorithms once they are finalised.
- Continue to avoid baking-in algorithms, either explicitly or implicitly (e.g. via maximum field sizes).
- Keep an eye on key exchange flow characteristics and understand implications for protocol latency/round trips.
- Understand how to combine pre- and post-quantum elements to make hybrid schemes.
- Identify and resist efforts to pre-empt NIST process by "SDO shopping".

Concluding Remarks

- The Crypt-Apocalypse might be coming… or it might not be.
- PQC could be a massive misdirection, designed to distract cryptographers from things that really matter… or it might not be.
- We can hope that the NIST process will proceed in an orderly fashion and produce a sensible and conservative portfolio of options.
- Meantime, there is some work for IETF to do, to make the transition as smooth as possible.

Fin

Thanks.

Discussion!

Extra Slides

1. QKD Does Not Solve the Key Distribution Problem

- QKD systems enable Alice and Bob to share keying material about which Eve has no information.
- Roughly: exchange of quantum states, followed by a **reconciliation phase**.
- The reconciliation phase requires Alice and Bob to exchange information about measurements over an **authentic channel**.
- Otherwise: person-in-the-middle attacks.
- How do we build authentic channels in practice?
- Using (asymmetric) signatures or (symmetric) Message Authentication Codes.

1. QKD Does Not Solve the Key Distribution Problem

- (Asymmetric) signatures are not unconditionally secure!
- (Though the signatures need only remain secure during execution of reconciliation phase.)

- (Symmetric) Message Authentication Codes **can** be unconditionally secure, but need a symmetric key in place in order to work.
- But that's the very problem QKD is meant to be solving!
- How to break the circularity?
- Perform a initial key distribution (we'll come back to this), then split resulting QKD key for future MACs and encryption.
- **Unconditionally secure QKD is actually unconditionally secure key expansion.**

2. QKD Has Limits on Rate and Range

- Impressive gains in secure bit rate of QKD have been made.
- 1 Mbit/s of secure key now achievable over, say, 50km.
- (But watch out for whether theoretical bounds on security are achieved.)
- But for unconditional security, we need to consume 1 bit of key for every bit of data we wish to securely communicate.
  - Use keying material in one-time pad: C = P XOR K.
  - Users would be disappointed with 1 Mbit/s!
  - So we are forced to **sacrifice unconditional security** and resort to hybrid systems: use QKD to effect rapid key changes for conventional encryption algorithms.
  - Use, say, 256-bit keys in a suitable AES-based AEAD scheme to give good security against Grover's algorithm.
  - Is this valuable compared to purely conventional means of providing the same functionality?

2. QKD Has Limits on Rate and Range

- Less impressive gains have been made concerning range.
- Going above 200km in commercial fibre optic cable seems hard because of dispersion losses.
- Cannot amplify QKD signals (quantum no-cloning theorem).
- Free-space even harder: ground-to-space proposals now being replaced by ground-UAV-space proposals in QKD slideware!
- (Notwithstanding: proposed Chinese satellite network employing QKD.)

- Why does the range limit matter?

2. QKD Has Limits on Rate and Range

- When I buy something from amazon.com, my browser uses TLS.
- This is an end-to-end secure communications protocol that does not care how far away Amazon's server is.
- I use it because I want to protect my private data from a range of different eavesdroppers.
  - A nosy ISP.
  - An ISP compelled by a government agency, cf. TEMPORA.
  - Rogue employees working for an on-path network provider.
  - Entities unknown between me and Amazon's server.
- **Daisy-chaining together QKD systems cannot provide this.**

2. QKD Has Limits on Rate and Range

- Is it worth using QKD to protect individual network links if other links in the end-to-end communication are unprotected?

- Or is QKD's application limited to single-hop applications, e.g. data-centre-to-data-centre within a few 10's of kilometers?

3. Security in Theory vs Security in Practice

- Applying the holographic principle to QKD, aka side-channel attacks (Bernstein).
- (cf. Bennett-Brassard'84: audio side channel).
- Makarov and quantum hacking: http://www.vad1.com/
- Bright lights and flooding photon detectors.
- Can all be portrayed as part of QKD's evolution towards practical deployment.
- But, still, we were promised unconditional security?

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

Lars Knudsen

4. QKD Does Not Offer Significant Advantages Over Carefully Designed Conventional Approaches

Basic argument goes as follows:

- Unconditionally secure QKD needs pre-agreed symmetric keys.
- But if you allow us a pre-agreed symmetric key, we can achieve all the conventional security I need.
- Use heavy-duty key derivation on master key to create next master key and next session key.
- This won't be unconditionally secure, but neither is QKD in practice (because of limits on key rates).
- We can do all this without using any special hardware and with no range limitations; it's all tried and tested technology.
- **Technical differences**: what happens in the event of master key compromise is different in hybrid QKD system and full conventional system; what happens if key derivation function is broken?
- **Whimsical variation**: fill pairs of hard disks with random bits from a quantum RNG, do cost evaluation.