



The Quantum Break is Coming Will You Be Ready?



Roger Grimes
Data-Driven Defense Evangelist,
KnowBe4, Inc.
rogerg@knowbe4.com



Roger A. Grimes
Data-Driven Defense Evangelist
KnowBe4, Inc.

About Roger

- 30-years plus in computer security
- Expertise in host and network security, IdM, crypto, PKI, APT, honeypot, cloud security
- Consultant to hundreds of the world's largest and smallest companies and militaries for decades
- Previously worked for Foundstone, McAfee, Microsoft
- Written 10 books and over 1000 magazine articles
- InfoWorld and CSO weekly security columnist since 2005
- Frequently interviewed by magazines (e.g. Newsweek) and radio shows (e.g. NPR's All Things Considered)

Certifications passed include:

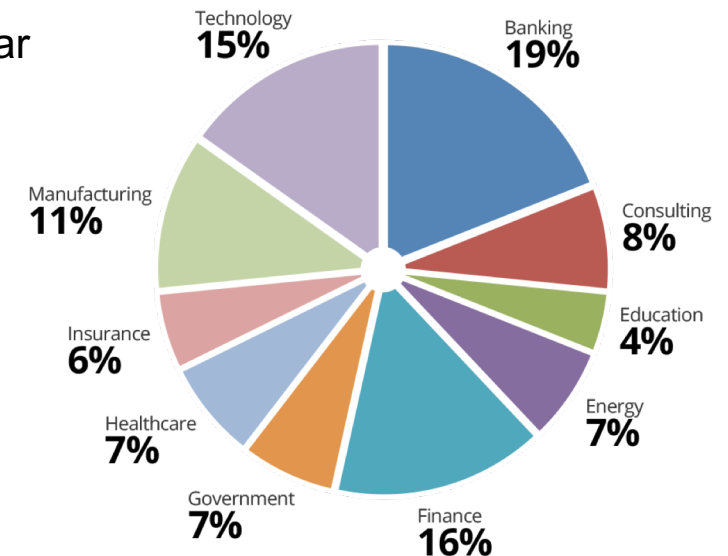
- CPA
- CISSP
- CISM, CISA
- MCSE: Security, MCP, MVP
- CEH, TISCA, Security+, CHFI
- yada, yada

Over
20,000
Customers

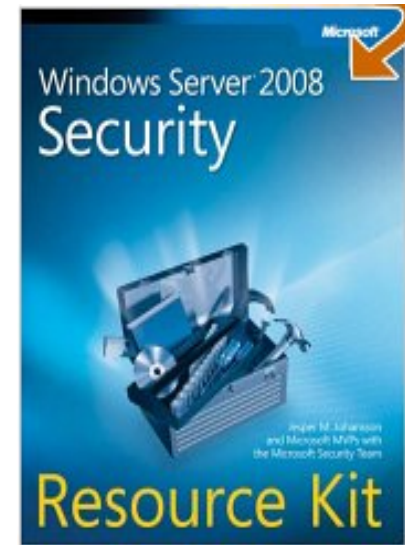
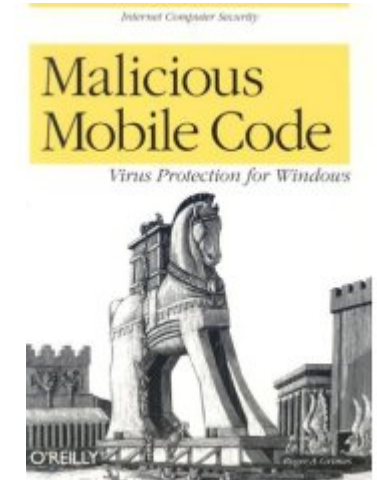
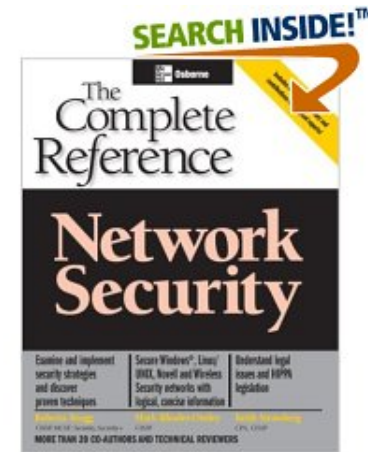
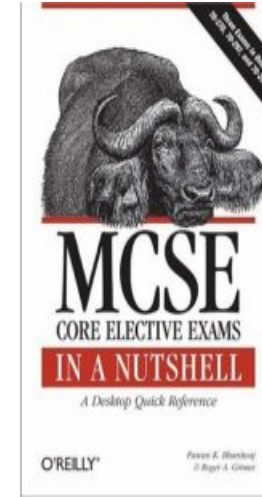
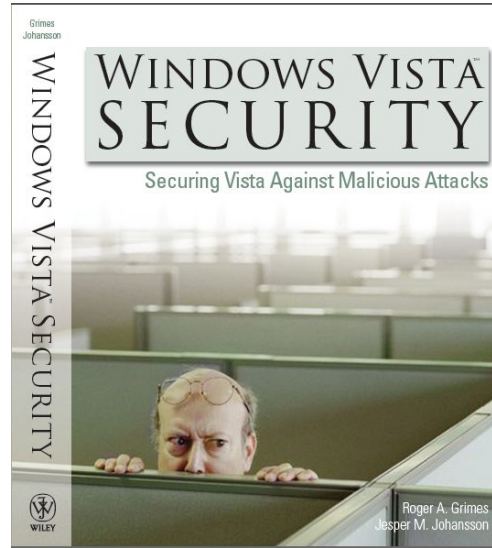
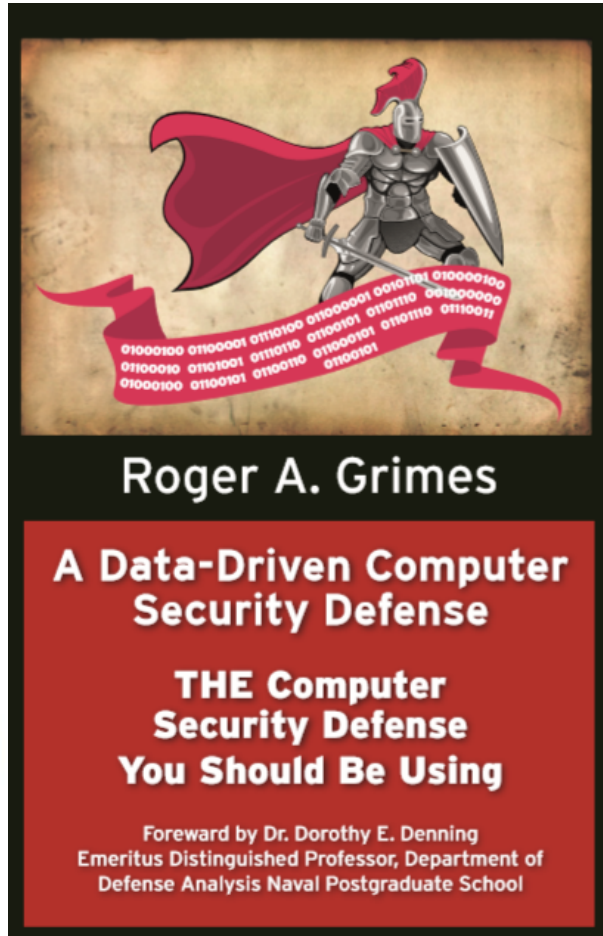
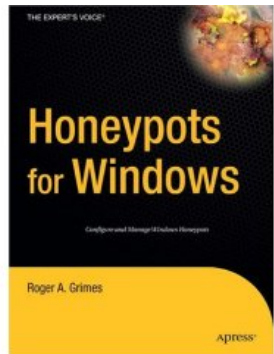
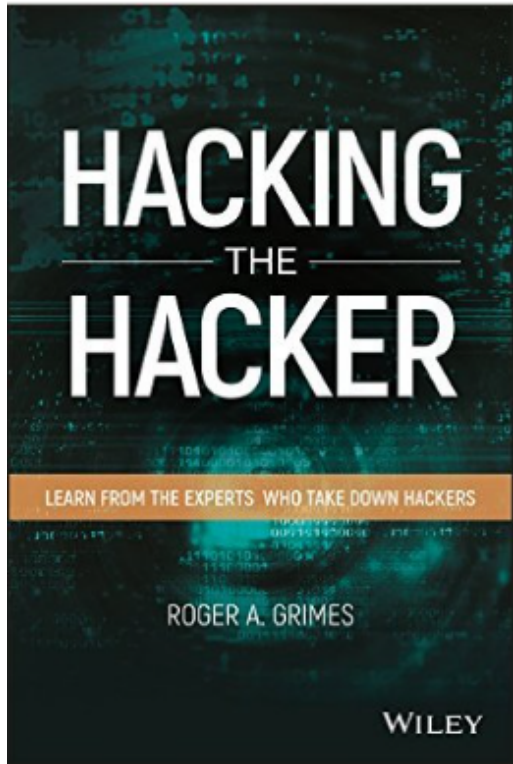
Inc.
500

About Us

- The world's most popular integrated Security Awareness Training and Simulated Phishing platform
- Based in Tampa Bay, Florida, founded in 2010
- CEO & employees are ex-antivirus, IT Security pros
- Former Gartner Research Analyst, Perry Carpenter is our Chief Evangelist and Strategy Officer
- 200% growth year over year
- We help thousands of organizations manage the problem of social engineering



Roger's Books

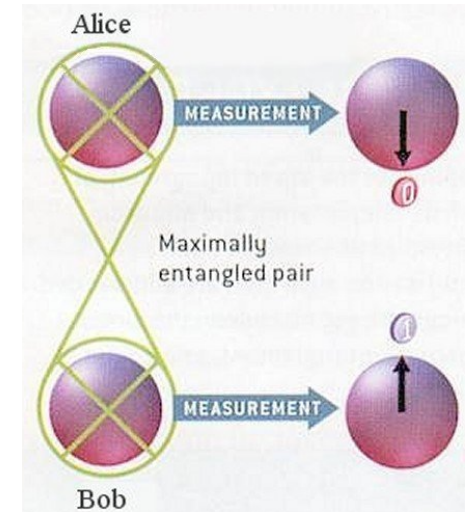


Today's Presentation

- What is Quantum Computing?
- How Long Till Quantum Computing Breaks Public Key Crypto?
- How to Prepare

Quick Strange Quantum Facts

- ❖ A single particle can be two different things in two different places at the same time
- ❖ In a series of ordered actions, a single event can be both “first” or “last”
- ❖ Fuzzy entanglement
 - Two distant objects can be tied to each other so that when one moves it instantly changes the other, and we don't know why
 - A change to a particle today or in the future changes its state in the past
 - Teleportation is absolutely possible
 - Faster than the speed of light is possible
- ❖ Answers can be in another universe



“Those who are not shocked when they first come across quantum theory cannot possibly have understood it.”

Niels Bohr, Quantum Physicist and 1922 Nobel Prize Winner

“Any sufficiently advanced technology is indistinguishable from magic.”

Arthur C. Clarke, sci-fi author

Quantum Break

Summary

- ❖ Soon quantum computers are likely to break most traditional public key crypto and every secret it protects
 - Ex: RSA, DH, ECC, PKI, digital certificates, digital signatures, TLS, HTTPS, VPNs, WiFi protection, smartcards, HSMs, crypto-currencies, two-factor authentication which relies on digital certificates (e.g. FIDO keys, Google security keys, etc.), etc.

What Is Quantum Computing?

The background features a dark, textured world map in the upper right. Below it, several lines of binary code (0s and 1s) are arranged in a slightly curved pattern. In the lower right, there are several circular icons: a bar chart, an envelope, a music note, and a document. A large, faint circular graphic with a grid pattern is visible on the left side. The overall aesthetic is technical and futuristic.

What is Quantum Computing?

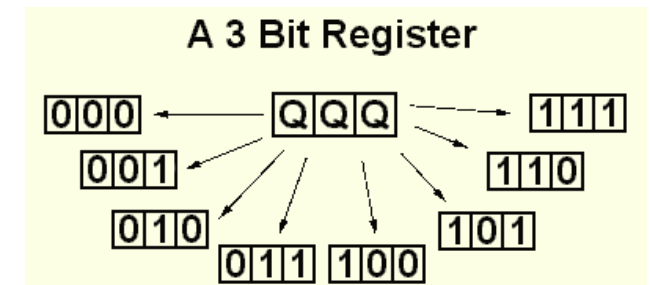
Traditional Computers



- Traditional computers are binary
- Each bit can be 1 or 0, negative or positive charge, on or off
- Each bit can only be one thing at one time

What is Quantum Computing?

- ❖ First theorized in 1959 by Richard Feynman
- ❖ A quantum bit (qubit or qbit or qb) – a qubit can be two states (0 and 1) AT THE SAME TIME
 - 1qb=2bits, 2qb=4bits, 3qb=8bits...
- ❖ Result may be in another universe
 - We have to “infer” the result



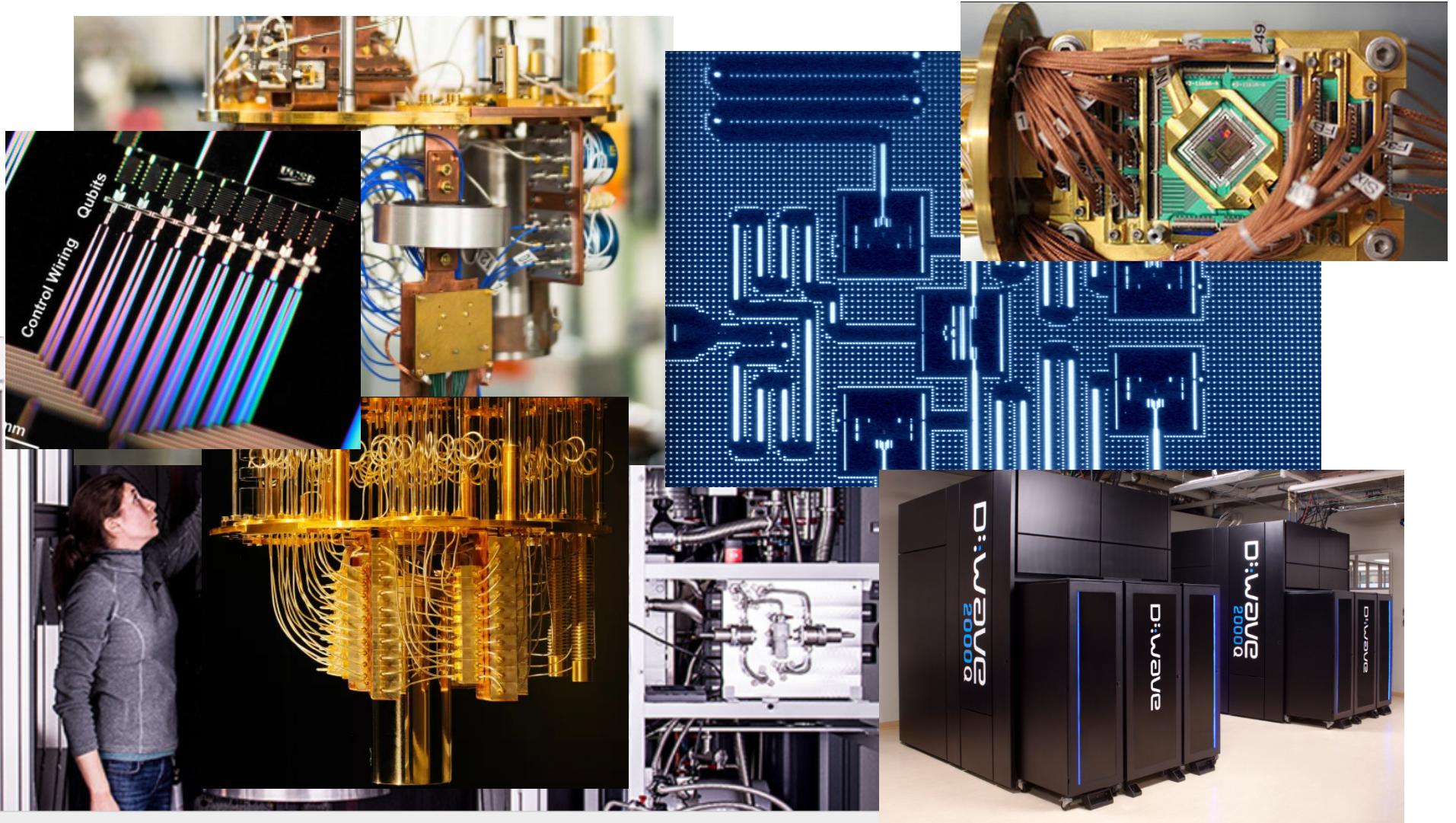
Quantum Computers

What is Quantum Computing?

- 1998 – first working quantum computer, 2-qubits
- 2000 – 5- and 7-qubit computers
- 2006 – 12-qubit computer
- 2007 – 28-qubit computer
- 2012 – 84-qubit computer
- 2015 – 1000-qubit computer
- 2016 – Google develops quantum computer
- 2017 – 2048-qubit computer
- 2017 – IBM, Microsoft, announces quantum computers
- 2018 – Several quantum microprocessors available

What is Quantum Computing?

Real
Quantum
Computers



What is Quantum Computing?

Not All Qubits Are Alike

- ❖ Many different methods: superconducting (-460F temps), trapped ion, Majorana fermion, etc.
 - Each method has advantages and disadvantages
- ❖ Right now, the quantum computers with the highest number of qubits, like 1000+, are called annealing, which aren't great at breaking crypto
- ❖ Universal gate quantum is better at breaking crypto, but so far have a smaller number of stable qubits
 - 72 qubits as of Sept. 2018

Types of Quantum Computers

What is Quantum Computing?

We Need More Stable Qubits

- ❖ Stable qubits are very hard to make (right now)
 - Without the right conditions, they lose their needed quantum properties very quickly (decoherence)
 - Merely “observing” qubits makes them change
- ❖ Need them stable long enough to complete a task
- ❖ Most of today’s qubits need “error correcting” or “stabilization” or be “controllable” to work, which requires many more qubits than just the ones doing the work
- ❖ The number of stable, controllable qubits is increasing over time
 - But right now even those make a mistake once every 200 actions

What is Quantum Computing?

Today we have:

The richest nations, dozens of companies, spending tens of billions of dollars on quantum computing:

- Quantum microprocessors
- Cloud-connected quantum computers you can play with
- Quantum random number generators
- Quantum programming languages, development kits, compilers
- Quantum networking
- Quantum encryption

Quantum
Computers

What is Quantum Computing?

Quantum Supremacy

Point in time when quantum computers can solve problems that traditional binary computers cannot

- Need at least 49 “perfect” qubits, and probably a lot more
- We are either there already, or very near
- Google first thought they were there in 2017
- Intel says they have a quantum supremacy chip now
- China says they are the closest of anyone

What is Quantum Computing?


What Will Quantum Computers Give Us?

- New understanding of physics and our universe
- Solve complicated math quickly
- Give us incredible precision (military, weather, traffic mgmt.)
- New medicines, better solar cells, new chemicals
- True artificial intelligence
- Things we cannot imagine right now

What is Quantum Computing?

What Will Quantum Computers Give Us?

- ❖ Break most traditional public key crypto and every secret it protects
 - Any algorithm whose security relies on one of three hard mathematical problems: the integer factorization problem, the discrete logarithm problem or the elliptic-curve discrete logarithm problem
 - Ex: RSA, DH, ECC, PKI, digital certificates, digital signatures, TLS, HTTPS, VPNs, HSMs, smartcards, WiFi protection, crypto-currencies, two-factor authentication which relies on digital certificates (e.g. FIDO keys, Google security keys, etc.), etc.
- ❖ New unbreakable encryption

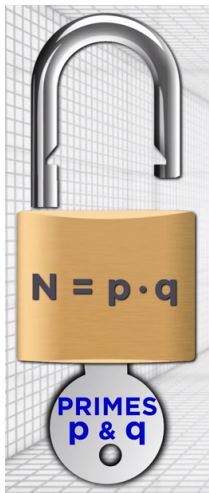
The background features a dark brown color with a world map in the upper right. In the center, there are several lines of binary code (0s and 1s). Below the map, there are several circular icons: a photo, an envelope, a music note, and a document. A line graph is also visible, showing an upward trend. The text "DISK ALERT" is faintly visible in the background.

How Long Till Quantum Computing Breaks Public Key Cryptography?

When Will Quantum Break Public Key Crypto?

Quantum Break

- ❖ A **prime number** is any whole number after 1 that can only be divided by itself or one and get a whole number
 - 2,3,5,7,11,13,17,23,29,31, and so on
- ❖ Most traditional public key crypto (e.g. RSA, Diffie-Hellman, etc.) is based on the work effort needed to factor large prime number equations
 - $p * q = n$, p and q are prime numbers, n is a public key, can be very hard to figure out p and q
 - Simple Ex: $3 \times 5 = 15$

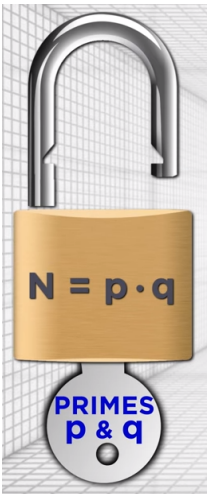


When Will Quantum Break Public Key Crypto?

Quantum Break

Another Simple Example

- $p \cdot q = 187$, what's p and q ?
- Answer: p and $q = 17$ and 11
- $p \cdot q = 84773093$, what's p and q ?
- Answer: p and $q = 9539$ and 8887

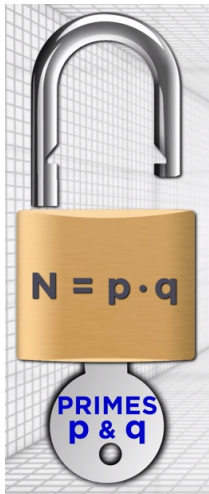


When Will Quantum Break Public Key Crypto?

Quantum Break

Another Simple Example

- Now assume N is a prime number 2048-bits long
- Traditional computers are not good at figuring out N
- Takes more guesses than all atoms in the known universe



When Will Quantum Break Public Key Crypto?

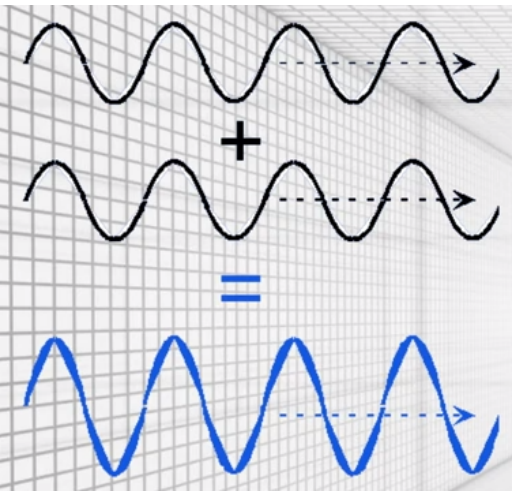
Quantum Break

Prime Factoring Speed

- ❖ As of Sept. 2018, the largest known successful factored primes is RSA-768 (by traditional computers)
 - Took 4 years and the equivalent of almost 2000 years of computing on a single core 2.2 GHz AMD Opteron
 - RSA-2048 would take billions of years using every traditional computer and resource in existence
- ❖ Quantum computers can break encryption algorithms that rely upon the work effort needed to factor equations involving large prime numbers
- ❖ Quantum computers with 49 – 10,000 stable qubits, can do it in 100 seconds
 - We have 72-stable or more qubits today

When Will Quantum Break Public Key Crypto?

Quantum Break



How Quantum Computers Do It

Shor's Algorithm (1994)

- ❖ Start by creating all the possible answers for $N=p*q$ all at once (superposition of states)
 - Quantum Quick:
 - Classical speed- 2^{2048} calculations, one per CPU
 - Quantum - 2048 calculations done all at once
- ❖ Transform answers so that most likely correct answers (p & q) easy to see above all others

When Will Quantum Break Public Key Crypto?

Quantum Break

Bottom Line

- ❖ Many quantum physicists think we'll have enough stable qubits within 5 years (if it's not already done) to break public crypto which uses the large prime factoring work effort for protection
 - Dr. Mark Jackson of Cambridge Quantum Computing thinks 5 years or less, maybe 2-3 years
- ❖ But who really knows??

When Will Quantum Break Public Key Crypto?

Quantum Break

Bottom Line

In 2016, NIST/NSA, “NOW” is the time to prepare



Commercial National Security Algorithm Suite and Quantum Computing FAQ



Q: Why is now the right time to make an announcement?

A: Choosing the right time to champion the development of quantum resistant standards is based on 3 points: forecasts on the future development of a large quantum computer, maturity of quantum resistant algorithms, and an analysis of costs and benefits to NSS owners and stakeholders. NSA believes **the time is now** right—consistent advances in quantum computing are being made, there are many more proposals for potentially useful quantum resistant

<https://cryptome.org/2016/01/CNSA-Suite-and-Quantum-Computing-FAQ.pdf>

How You Can Prepare for the Quantum Break



Preparing for Quantum Break

Scenarios

What do the different possible break scenarios look like?

Preparing for Quantum Break

Break Scenarios

- It's already happened but we don't know about
- It's going to happen in the next few years
- It's going to happen after the next few years
- It's never going to happen

I would not put my money on the last one.

Timing

Preparing for Quantum Break

Break Scenarios

- Stays in the realm of nation-states for a long-time
- Gets picked up by monied groups and competitors
- Available in cloud form for cheap
- Past crypto breaks went from the realm of millions of dollars to accomplish to tens of thousands of dollars in just a few years
- Interested parties are likely storing encrypted communications for future breaks already

Speed/Cost

Will We Be Prepared?

Preparing for Quantum Break

Break Scenarios

- ❖ If we are lucky, the quantum break prep proceeds like the global SHA1 to SHA2 migration (slower than we liked, but orderly, and ahead of the worst problems)
- ❖ Might happen faster than companies and vendors are prepared
 - NSA said to move to post-quantum in Jan. 2016, what have you or any of your vendors or partners done?
- ❖ Likely to be a mix of prepared and not prepared when time comes

Preparing for Quantum Break

Preparing

- ❖ Education (this slide deck and keeping up on advances)
 - Your company, your vendors, your third parties
- ❖ Take a data protection inventory – what secrets really need to be protected, and for how long? Which are at risk from quantum break?
- ❖ Use/Be moving toward quantum-resistant crypto, where and when possible
- ❖ Pressure your vendors over quantum break preparation
- ❖ At least demand crypto-agility
- ❖ Prevent eavesdropping on very high-value data

Prepare

Preparing for Quantum Break

Post-Quantum Protections

Symmetric encryption is not as vulnerable

- ❖ **AES** is still good
 - Double your key size and you should be fine
- ❖ **SNOW 3G**
 - Word-based synchronous stream cipher

Unfortunately, traditional public key crypto is used to protect the transmission of plaintext symmetric keys most of the time

Prepare

Preparing for Quantum Break

Post-Quantum Protections

Quantum-Resistant Hashes

- ❖ **Lamport signatures**
- ❖ **Merkle Signature Scheme**
 - Merkle trees
 - XMSS (Extended Merkle Signature Scheme)
- ❖ **SPHINCS+**
 - Used with SHAKE256, SHA-256, and Haraka
- ❖ **Picnic Signature Algorithm**
 - Demonstrated by Microsoft in PKI to protect HSMs

Prepare

Preparing for Quantum Break

Post-Quantum Protections

Use quantum-resistant key management ciphers, which use symmetric key protection instead of public key

- **Kerberos** is a great example
- **Network Switching Subsystem** used by GSM cell phones is quantum-resistant
- **Supersingular Isogeny Diffie–Hellman** key exchange (SIDH)
- **Ring Learning With Errors Key Exchange** (RLWE-KEX)
- **New Hope** (Google Project)

Prepare

Preparing for Quantum Break

Post-Quantum Protections

There are many quantum-resistant asymmetric ciphers, including

- **Lattice-based** (e.g. NTRU, etc.)
- **Multi-variate-based** (e.g. Rainbow, Unbalanced Oil & Vinegar)
- **Code-based** (e.g. RLCE, McEliece, etc.)
 - https://en.wikipedia.org/wiki/Post-quantum_cryptography

Unfortunately, almost none are generally available

Prepare

Preparing for Quantum Break

Post-Quantum Protections

Use quantum-based ciphers and components, including

- ❖ Quantum Random Number Generator
 - Verifiably and guaranteed random
 - Many existing ones
 - Online one at <https://qrng.anu.edu.au/>
- ❖ Quantum Key Distribution (QKD)
- ❖ Quantum Encryption
 - Perfectly secure in theory
 - If anyone observes the data, you'll know

Prepare

Preparing for Quantum Break

Post-Quantum Protections

Quantum-resistant asymmetric ciphers require larger key sizes

Prepare

Algorithm	Type	Public Key	Private Key	Signature
NTRU Encrypt ^[34]	Lattice	6130 B	6743 B	
Streamlined NTRU Prime	Lattice	1232 B		
Rainbow ^[35]	Multivariate	124 KB	95 KB	
SPHINCS ^[18]	Hash Signature	1 KB	1 KB	41 KB
BLISS-II	Lattice	7 KB	2 KB	5 KB
GLP-Variant GLYPH Signature ^{[10][36]}	Ring-LWE	2 KB	0.4 KB	1.8 KB
New Hope ^[37]	Ring-LWE	2 KB	2 KB	
Goppa-based McEliece ^[14]	Code-based	1 MB	11.5 KB	
Random Linear Code based encryption ^[38]	RLCE	115 KB	3 KB	
Quasi-cyclic MDPC-based McEliece ^[39]	Code-based	1232 B	2464 B	
SIDH ^[40]	Isogeny	751 B	48 B	
SIDH (compressed keys) ^[41]	Isogeny	564 B	48 B	
3072-bit Discrete Log	not PQC	384 B	32 B	96 B
256-bit Elliptic Curve	not PQC	32 B	32 B	65 B

Preparing for Quantum Break

Post-Quantum Protections

Open Safe Project (<https://openquantumsafe.org/>)

- Group dedicated to helping to implement post-quantum crypto
- Open source C-library (**liboqs**) to implement some post-quantum ciphers
- API
- Testing and benchmarking
- Forked quantum-resistant versions of OpenSSL and OpenSSH

Prepare

Preparing for Quantum Break

Post-Quantum Protections

Enable **Perfect Forward Secrecy** Where Possible

- Generates random (public) encryption keys per session for the purposes of key agreement
- Means that the compromise of one key and/or message cannot immediately/easily lead to the compromise of others
- Can be enabled in Kerberos, HTTPS, OpenSSL, some public key crypto algorithms

Prepare

Preparing for Quantum Break

Preparing – More Of Your Secrets May Become Known

More of your secrets are likely to be compromised and used against you in the future

- One of the fastest growing categories of phishing/social engineering is that of spearphishing email coming from a trusted source's real email account using previously discussed information
- Quantum break is certainly going to make this more common
- Even if your company is not compromised, people and third parties with the secret information may be

Key Take Aways

- Quantum computers are likely to break traditional public key crypto “soon”
- You can start preparing now
- Don’t just wait for quantum supremacy to be announced without a solid, thoughtful, plan in place

KnowBe4
Human error. Conquered.

» Learn More at «

www.KnowBe4.com/Resources

Resources



Free Phishing Security Test

Find out what percentage of your users are Phish-prone



Free Domain Spoof Test

Find out now if hackers can spoof an email address of your own domain.

Questions?

Thank You!

Roger A. Grimes– Data-Driven Defense Evangelist, KnowBe4

rogerg@knowbe4.com

Twitter: [@rogeragrimes](https://twitter.com/rogeragrimes)