Quantum Cryptography and the Health Sector

July 7, 2022

Agenda

This presentation will review the basic concepts behind quantum cryptography, and will analyze their impact on cybersecurity in the health sector, along with recommended actions

- Introduction

- Quantum Theory/Mathematics

- Cryptography, Traditional and Quantum

- The Impact on Healthcare

- Recommended Actions

Slides Key:

Non-Technical: Managerial, strategic and high-level (general audience)

Technical: Tactical / IOCs; requiring in-depth knowledge (sysadmins, IRT)

Office of
Information Security
Securing One HHS

**Health Sector Cybersecurity
Coordination Center**

Introduction

Question: What do we do if our encryption is no longer effective?
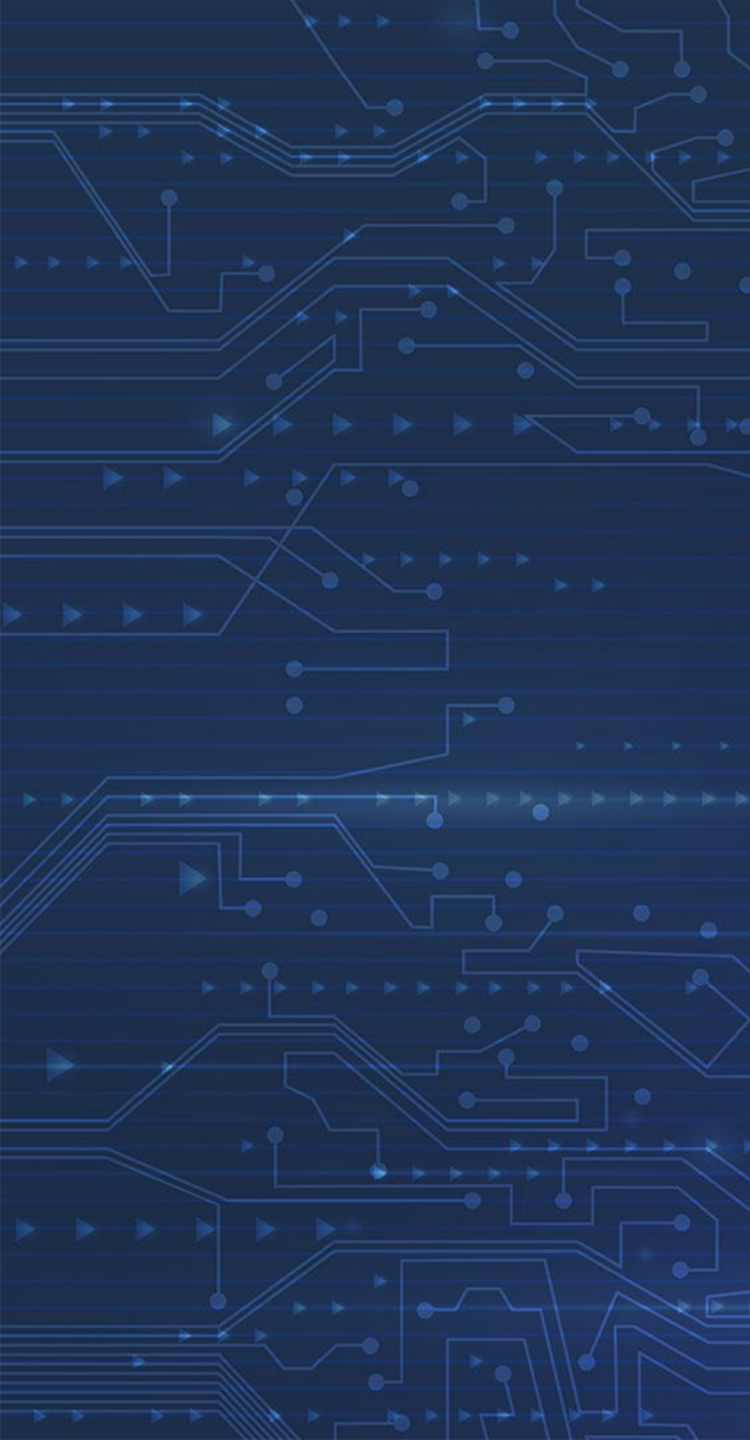
- The modern world is entirely dependent on information technology, and information technology is entirely dependent on cryptography. Examples:
  - System authentication (digital signatures), web surfing, e-mail, instant messaging, protecting data at rest, voice over IP telephony, cellular telephony, etc.
- Modern strong encryption algorithms: SHA-1, SHA-2, TripleDES, AES, MD5, RSA, etc.
- What happens if they fail?
- Cryptography is ubiquitous in many aspects of our lives, and its widespread failure would be impactful
- This presentation will focus on what this means for healthcare organizations

Office of
Information Security
Securing One HHS

**Health Sector Cybersecurity
Coordination Center**

Quantum Theory/Mathematics

What makes quantum computing different from classical computing

A Very Brief History of Quantum Physics

- 1905 - Albert Einstein explains the photoelectric effect, in which light shining on certain metals can release electrons; awarded the Nobel Prize in Physics

- 1924 – Max Born publishes "Einstein's Theory of Relativity"; first use of "quantum mechanics"

- 1930 – Paul Dirac publishes *The Principles of Quantum Mechanics* textbook, still used today

- 1935 – Erwin Schrödinger uses a thought experiment about a cat in a box when discussing the concept of quantum superposition with Einstein

- 1982 – Richard Feynman delivers his speech, "Simulating Physics with Computers", at the California Institute of Technology; first mention of quantum computing

- 1994 – Peter Shor develops a quantum algorithm that has the potential to decrypt RSA-encrypted communications

- 2013 – D-Wave announces the world's first operational quantum computer

- 2019 – Google and NASA announce they have achieved quantum supremacy

Office of
Information Security
Securing One HHS

Health Sector Cybersecurity Coordination Center

Quantum Theory and Quantum Computing

A significant differentiator between quantum and classical computing is the use of the qubit

- Quantum computers draw data from the manipulation and measurement of quantum particles

- Quantum vs. Classical
  - <u>Classical</u> – Leverage classical information processing
    - Binary values: 0 or 1 (deterministic)
    - Advancements in classical computing (e.g., integrated circuits) still leverage the same classical computing algorithms, just at improved speeds and efficiencies
  - <u>Quantum</u>
    - Quantum bits (Qubits): a <u>superposition</u> of 0 and 1 (probabilistic)

- The <u>qubit vs. the bit</u> is what allows quantum computing to outperform classical computing
  - "X" number of qubits gives you <u>many more possibilities</u> than "X" number of bits

Office of
Information Security
Securing One HHS

**Health Sector Cybersecurity
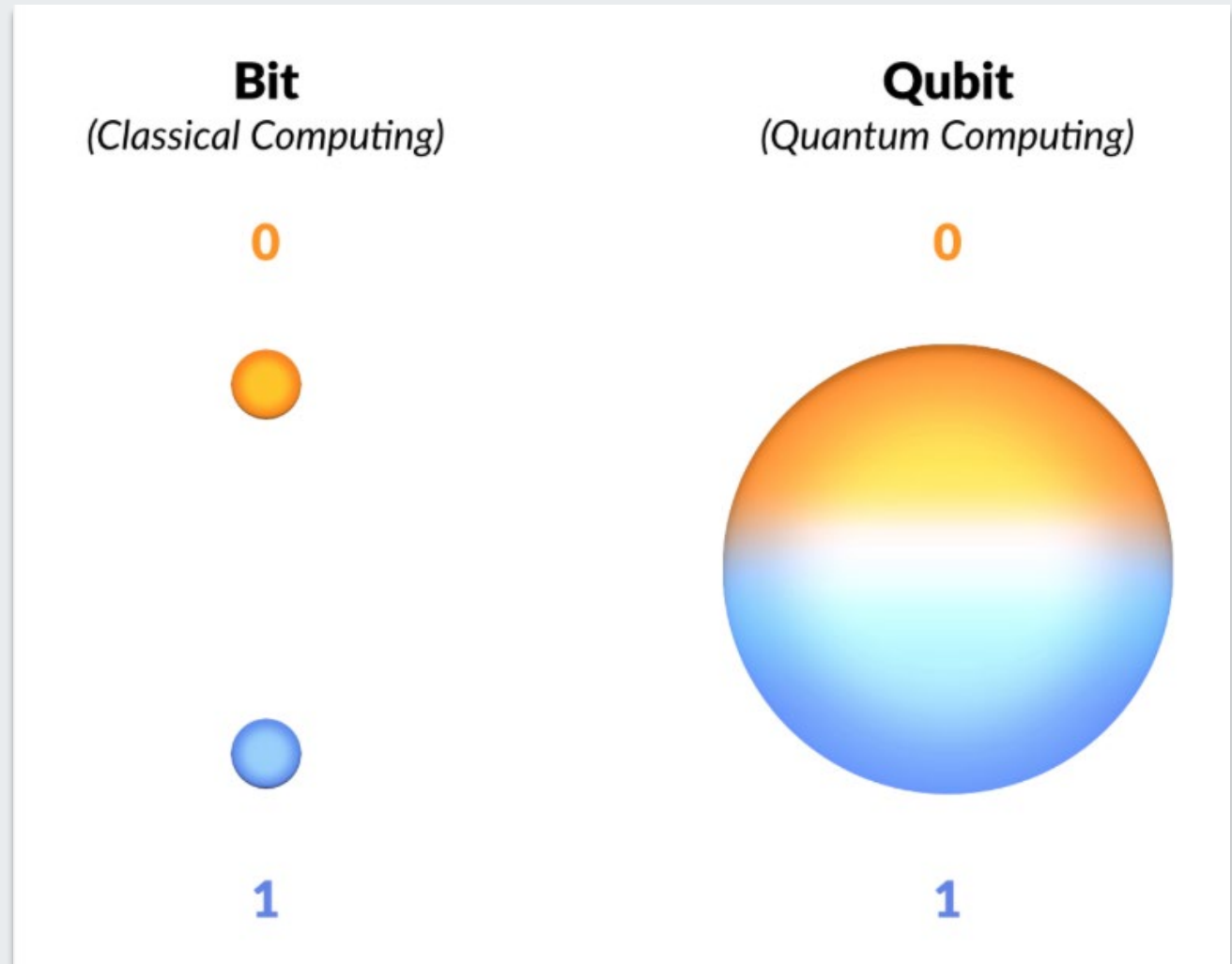Coordination Center**

Superposition

A binary digit (bit) can only have two possible values

A quantum bit (qubit) can have many more possible values

Rather than having a clear position, unmeasured quantum states occur in a mixed "superposition"

Bit
(Classical Computing)
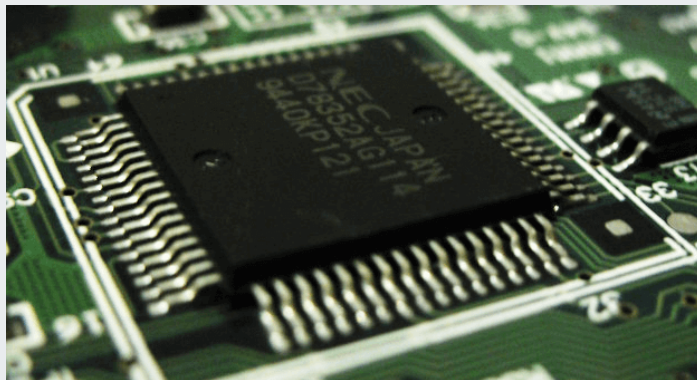
Qubit
(Quantum Computing)

0

0

1

1

Quantum Computing = Much More Speed

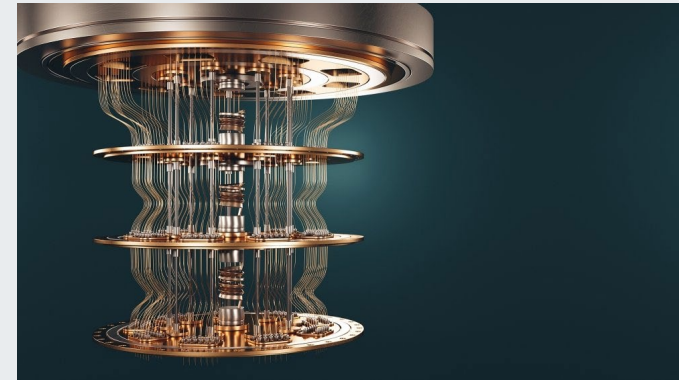What value does the qubit bring to computing?

Classical Computers

- The potential classical computing power of a system doubles when you add hardware (transistors, microprocessors, etc.).

Quantum Computers

- The potential quantum computing power of a system doubles when you add an additional qubit.

Office of **Information Security**
Securing One HHS

Health Sector Cybersecurity Coordination Center

Cryptography: Traditional and Quantum

The next major step forward for cryptography

Cryptography

Cryptography allows for instantaneous secure communications

- Cryptography: The use of codes or advanced mathematics to facilitate secure communications, especially across a long distance

- Quantum Cryptography: Exploiting quantum mechanical properties to perform cryptographic tasks

- Two basic models for cryptography: Private (secret) key and public key (asymmetric)
  - Private Key – The same key is used by the sender and received, and therefore, it must be protected from disclosure; often used for file encryption or VPN tunnelling
  - Public Key – Two separate keys are used (public and private); a public key can be distributed, but only the private key can be used to decrypt; often used for digital signatures or e-mail encryption

- Keys are mathematically generated

Office of
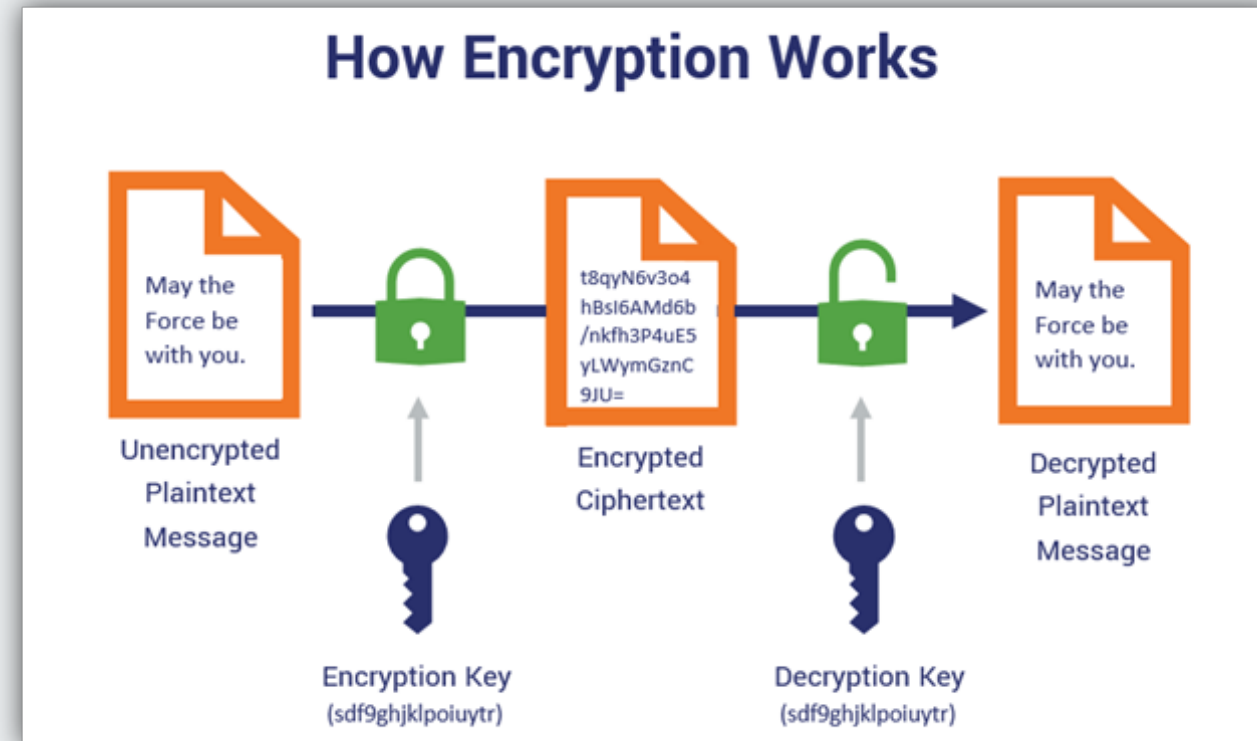**Information Security**
Securing One HHS

**Health Sector Cybersecurity
Coordination Center**

Private Key Cryptography

Private key cryptography requires that a single key, which is used for both encryption and decryption, always be protected

- Also known as secret key cryptography

- One key is used to encrypt and decrypt

- Key management is simple

- Key must always be protected

- If the key is compromised, the entire system is compromised

Office of
Information Security
Securing One HHS

**Health Sector Cybersecurity
Coordination Center**

Public Key Cryptography

Public key cryptography requires that the public key be distributed to anyone who wishes to send a protected message to a private key holder

- Also known as asymmetric cryptography

- One key is used to encrypt (public), the other is used to decrypt (private)

- Key management can be more complex

- The private key must always be protected, but the public key can be freely distributed

- If the private key is compromised, the entire system is compromised

Office of
Information Security
Securing One HHS

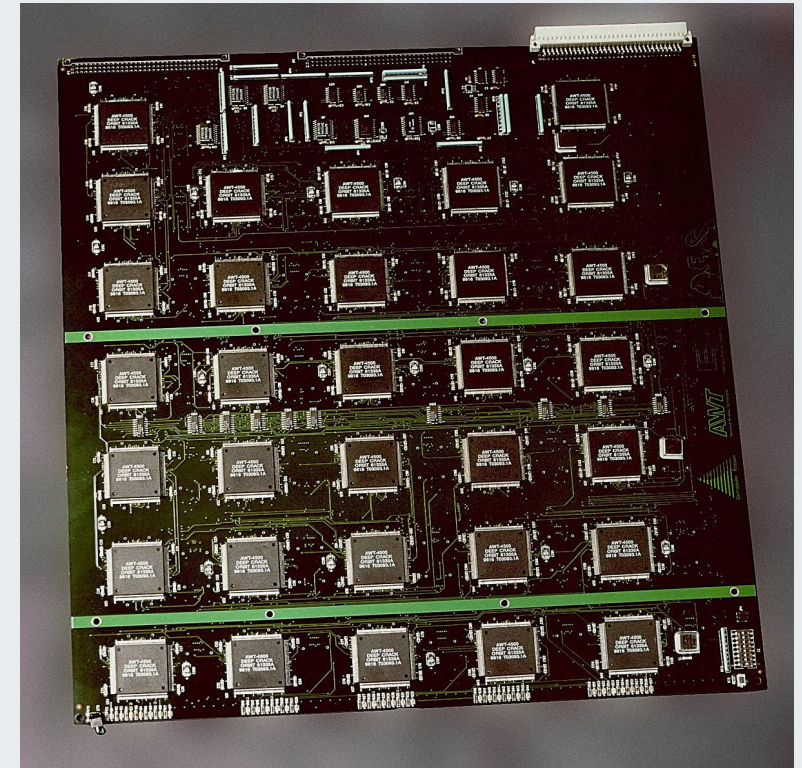**Health Sector Cybersecurity
Coordination Center**
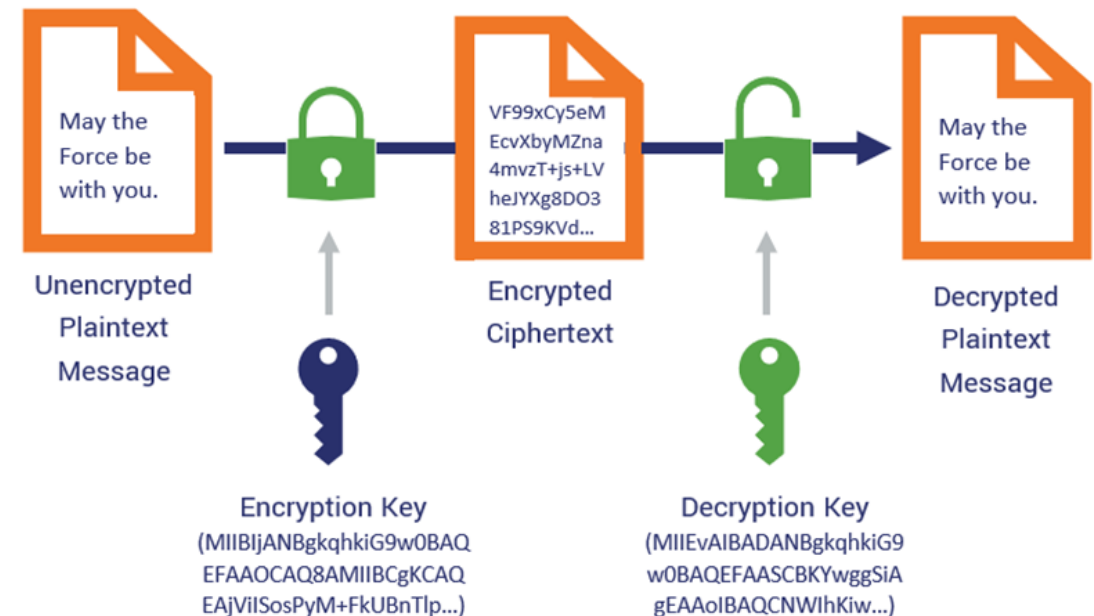
Brute Force Attack Overview

A brute force cryptographic attack consists of an attacker repeatedly attempting to calculate and submit keys to guess the correct one, and decrypt protected data

- Attacker generates a key, tests it, and upon failure, begins again
  - May be randomly or orderly (dictionary attack)
- Known as an exhaustive key search
  - Will eventually search entire key space (longer key size means longer search)
- Potentially time consuming
- Processor intensive
  - Processing power is critical due to the need to complete a task that is highly iterative; speed is helpful

Deep Crack, the DES encryption cracker, developed by the Electronic Frontier Foundation. (Image source: Darknet Diaries)
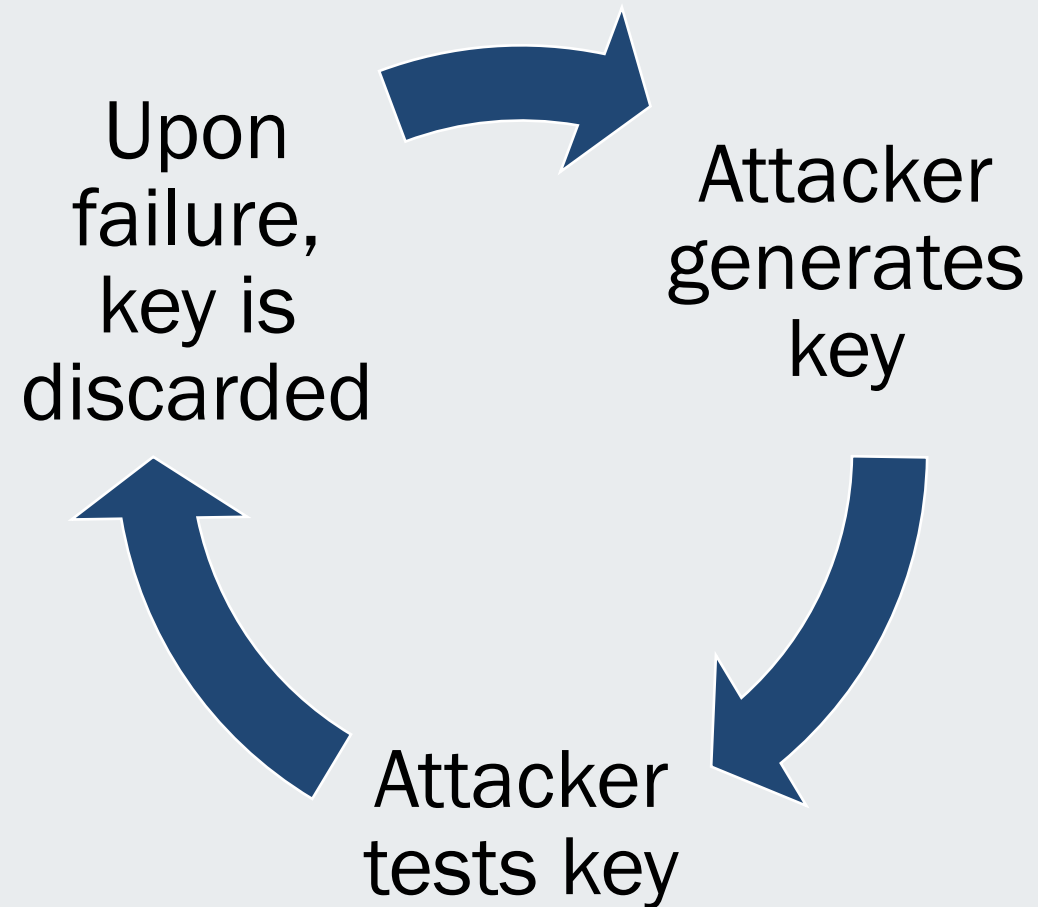
Brute Force Attack

Attacker:

- Generates a key

- Tests the key

- Discards the key if it fails, and starts over

If/when the attacker generates and tests a matching key, they will be able to decrypt data, and the system is then considered compromised.

Upon failure, key is discarded → Attacker generates key → Attacker tests key →

Quantum Computing vs. Classical Cryptography

Quantum computing adds significant speed to brute force attacks against classical cryptography systems, which is what makes the attacks feasible

- Why do modern (classical) cryptographic algorithms provide security? Because modern (classical) computing does not have enough power to break them.
  - A brute force attack continuously generates random keys until one works.

- The additional speed gained by quantum computing allows for a successful attack on a classical cryptographic system.

- Quantum supremacy is the moment that a quantum computer gains the ability to perform a task that a classical computer never could.
  - Coined by John Preskill, professor of theoretical physics at the California Institute of Technology.

- A quantum resistant algorithm is any algorithm that is anticipated to remain secure once quantum computing becomes fully developed.

Office of
Information Security
Securing One HHS

**Health Sector Cybersecurity
Coordination Center**

Quantum Cryptography: Impact on Healthcare

Maintaining operations and protecting data over the long run

Healthcare and Cryptography: Protecting PHI

Protecting personal health information (PHI) is one of the primary reasons for using encryption in healthcare

- Protecting personal health information:
  - One report from Stanford University estimates a 48% growth in medical data each year
  - According to Politico, 50 million Americans had their sensitive health data breached in 2021
  - Stolen health records can be sold for as much as $1,000 each on the black market

- Health Insurance Portability and Accountability Act (HIPAA) cryptography requirements:
  - The HIPAA Security Rule requires healthcare entities to implement safeguards, such as encryption, that renders electronic Protected Health Information (ePHI) "unreadable, undecipherable or unusable" so that any "acquired healthcare or payment information is of no use to an unauthorized third party."

- National Institute of Standards and Technology (NIST)
  - FIPS 140-2: Security Requirements for Cryptographic Modules

- AES 128, 192 and 256-bit encryption are commonly recommended standards

Office of
Information Security
Securing One HHS

**Health Sector Cybersecurity
Coordination Center**

Sensitive Data Storage

Where is sensitive data (PHI and other data) stored in a healthcare organization?

- EHR/EMR systems

- Mobile/Medical devices

- Cloud

- Email

- Servers

- Wireless (networked) medical devices

- Databases

- Vendor/Business associate systems

- Laptop computers

- Desktop computers

- Calendar software

- Operating systems

- Backup (online and offline)

- Applications

Office of
Information Security
Securing One HHS

**Health Sector Cybersecurity
Coordination Center**

Sensitive Data in Motion

Healthcare data – both PHI and other sensitive information – must also be protected during transmission

- Telehealth and remote patient monitoring

  - Collecting real-time patient data for analysis

  - Includes medical devices, mHealth apps

- Telemedicine

- Hybrid medical workforce

- Remote patient access to records

- Cloud access

- Deployment of temporary, modular hospitals/clinics

  - Crisis response, pandemic, etc.

  - Access to rural and other underserved areas

- Video surveillance for physical security

- Vendor/Business associate systems

- Medical professional collaboration

Office of
Information Security
Securing One HHS

Health Sector Cybersecurity Coordination Center

Recommended Actions

Mitigating against quantum threats to cryptography

Initiate a Discussion

Planning for quantum threats begins with a discussion among the proper stakeholders

- Quantum risk assessment – Understanding where you are potentially vulnerable

- Stand up a working group dedicated to evaluating your organization's quantum posture

- Ideally, representation should include:
  - Executive leadership
  - Middle management (information technology)
  - Senior technical professionals

- Initial meeting should solidify:
  - Membership list
  - Membership roles and responsibilities
  - Frequency of future meetings (quarterly, monthly)
  - Milestones and goals

Office of
Information Security
Securing One HHS

**Health Sector Cybersecurity
Coordination Center**

Important Questions to Ask

What does your organization need to determine in order to remain secure?

- How much data do you have?
- What are the varying sensitivity levels of your data?
- Where is it stored? How is that storage protected?
- How long do you need to store/protect it? Legally? Operationally?
- Who should have access to it?
  - Internal (employees, contractors, vendors, etc.)
  - External (patients, customers, etc.)
- Which aspects of your operations are dependent on cryptography?
  - Authentication systems
- NIST Quantum-Resistant Cryptographic Algorithm Announcement: https://www.nist.gov/news-events/news/2022/07/nist-announces-first-four-quantum-resistant-cryptographic-algorithms
- NIST Cryptographic Agility Guidance: https://www.nccoe.nist.gov/crypto-agility-considerations-migrating-post-quantum-cryptographic-algorithms

Office of
Information Security
Securing One HHS

**Health Sector Cybersecurity
Coordination Center**

Conclusion

Any healthcare organization risk management plan should incorporate quantum technologies into it

- Quantum computing is inevitable; it is the future
- Public and private sector health organizations rely heavily on cryptography
  - This reliance will translate into vulnerabilities as quantum cryptography continues to develop
- The most important step any healthcare organization can do now is begin the planning process:
  - Enterprise data gathering
  - Situational awareness related to quantum technologies
  - Laws, regulations and standards
- There is no immediate threat (that we are aware of) that existing cryptographic technologies will be in jeopardy in the immediate future, but the process of getting ahead of this will be long-term and require significant time and resources

Office of
Information Security
Securing One HHS

Health Sector Cybersecurity Coordination Center

Reference Materials

References

Cryptographic Standards and Guidelines
https://csrc.nist.gov/Projects/cryptographic-standards-and-guidelines

NIST: Post-Quantum Cryptography Standardization
https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization

NIST: Post-Quantum Cryptography Overview
https://csrc.nist.gov/projects/post-quantum-cryptography

NIST SP 800-77 Rev. 1 Guide to IPsec VPNs
https://csrc.nist.gov/publications/detail/sp/800-77/rev-1/final

NIST SP 800-52 Rev. 2 Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations
https://csrc.nist.gov/publications/detail/sp/800-52/rev-2/final

Department of Homeland Security: Post-Quantum Cryptography
https://www.dhs.gov/quantum

National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems
https://www.whitehouse.gov/briefing-room/statements-releases/2022/05/04/national-security-memorandum-on-promoting-united-states-leadership-in-quantum-computing-while-mitigating-risks-to-vulnerable-cryptographic-systems/

Office of
Information Security
Securing One HHS

**Health Sector Cybersecurity
Coordination Center**

References

How close are we to breaking encryption with quantum computing?
https://www.idginsiderpro.com/article/3532897/how-close-are-we-to-breaking-encryption-with-quantum-computing.html

Why Encryption is Essential in Healthcare Cybersecurity Strategies
https://www.healthitanswers.net/why-encryption-is-essential-in-healthcare-cybersecurity-strategies/

Cryptography safe for now, but urgent need to build quantum skills
https://www.zdnet.com/article/cryptography-safe-for-now-but-urgent-need-to-build-quantum-skills/

How will quantum computing impact your industry?
https://www.zdnet.com/article/how-will-quantum-computing-impact-your-industry/

White House: Prepare for cryptography-cracking quantum computers
https://www.bleepingcomputer.com/news/security/white-house-prepare-for-cryptography-cracking-quantum-computers/

OpenSSH goes Post-Quantum, switches to qubit-busting crypto by default
https://nakedsecurity.sophos.com/2022/04/11/openssh-goes-post-quantum-switches-to-qubit-busting-crypto-by-default/

Encryption, zero trust and the quantum threat -- security predictions for 2021
https://betanews.com/2020/12/24/security-predictions-2021/

Quantum computers: How to prepare for this great threat to information security
https://www.helpnetsecurity.com/2020/11/06/quantum-computers-threat/

Office of
Information Security
Securing One HHS

**Health Sector Cybersecurity
Coordination Center**

References

More on NIST's Post-Quantum Cryptography
https://www.schneier.com/blog/archives/2020/09/more_on_nists_p.html

US Plans Quantum Internet
https://www.infosecurity-magazine.com/news/us-plans-quantum-internet/

Quantum Loop: US Unveils Blueprint for 'Virtually Unhackable' Internet
https://www.securityweek.com/quantum-loop-us-unveils-blueprint-virtually-unhackable-internet

NIST's Post-Quantum Cryptography Program Enters 'Selection Round'
https://www.nist.gov/news-events/news/2020/07/nists-post-quantum-cryptography-program-enters-selection-round

Singapore researchers tapping quantum cryptography to enhance network encryption
https://www.zdnet.com/article/singapore-researchers-tapping-quantum-cryptography-to-enhance-network-encryption/

How close are we to breaking encryption with quantum computing?
https://www.idginsiderpro.com/article/3532897/how-close-are-we-to-breaking-encryption-with-quantum-computing.html

How rapid advances in quantum computing are reshaping cybersecurity
https://www.computing.co.uk/opinion/4013424/rapid-advances-quantum-computing-reshaping-cybersecurity

Podcast: The Google-IBM "quantum supremacy" feud
https://www.technologyreview.com/s/615268/podcast-google-ibm-quantum-supremacy-computing-feud/

Office of
Information Security
Securing One HHS

**Health Sector Cybersecurity
Coordination Center**

References

Quantum internet: the next global network is already being laid
https://theconversation.com/quantum-internet-the-next-global-network-is-already-being-laid-131355

Chaos & Order: The Keys to Quantum-Proof Encryption
https://www.darkreading.com/edge/theedge/chaos-and-order-the-keys-to-quantum-proof-encryption-/b/d-id/1337026

Podcast: The Overhype and Underestimation of Quantum Computing
https://insidehpc.com/2020/01/podcast-the-overhype-and-underestimation-of-quantum-computing/

Will quantum computing overwhelm existing security tech in the near future?
https://www.helpnetsecurity.com/2019/12/13/quantum-computing-security-tech/

The race for quantum-proof cryptography
https://www.csoonline.com/article/3488857/the-race-for-quantum-proof-cryptography.html

Race is on to build quantum-proof encryption
https://www.ft.com/content/5c31399c-ca6e-11e9-af46-b09e8bfe60c0

Harvesting Attacks' & the Quantum Revolution
https://www.darkreading.com/vulnerabilities---threats/harvesting-attacks-and-the-quantum-revolution/a/d-id/1335870

How long before quantum computers break encryption?
https://www.helpnetsecurity.com/2019/09/30/quantum-computers-break-encryption/

Office of
Information Security
Securing One HHS

**Health Sector Cybersecurity
Coordination Center**

References

Cryptography & the Hype Over Quantum Computing
https://www.darkreading.com/risk/cryptography-and-the-hype-over-quantum-computing/a/d-id/1335551

IBM Announces Quantum Safe Encryption
https://www.darkreading.com/application-security/ibm-announces-quantum-safe-encryption/d/d-id/1335632

Quantum computing: The new moonshot in the cyber space race
https://www.helpnetsecurity.com/2019/08/23/cyber-space-race/

Explainer: What is post-quantum cryptography?
https://www.technologyreview.com/s/613946/explainer-what-is-post-quantum-cryptography/

What does quantum computing mean for cybersecurity, healthcare and the internet?
https://www.htxt.co.za/2019/04/02/what-does-quantum-computing-mean-for-cybersecurity-healthcare-and-the-internet/

Webinar: The Pending Impact of Quantum Computing on Cybersecurity
https://securityintelligence.com/events/webinar-the-pending-impact-of-quantum-computing-on-cybersecurity/

Quantum Ransomware
https://thedfirreport.com/2022/04/25/quantum-ransomware/

Office of
Information Security
Securing One HHS

**Health Sector Cybersecurity
Coordination Center**

? Questions

FAQ

Upcoming Briefing

- July 21 – Web Application Attacks in Healthcare

Product Evaluations

Recipients of this and other Healthcare Sector Cybersecurity Coordination Center (HC3) Threat Intelligence products are **highly encouraged** to provide feedback. To provide feedback, please complete the HC3 Customer Feedback Survey.

Requests for Information

Need information on a specific cybersecurity topic? Send your request for information (RFI) to HC3@HHS.GOV.

Disclaimer

These recommendations are advisory and are not to be considered as federal directives or standards. Representatives should review and apply the guidance based on their own requirements and discretion. The HHS does not endorse any specific person, entity, product, service, or enterprise.

Office of
Information Security
Securing One HHS

Health Sector Cybersecurity Coordination Center

About HC3

The Health Sector Cybersecurity Coordination Center (HC3) works with private and public sector partners to improve cybersecurity throughout the Healthcare and Public Health (HPH) Sector. HC3 was established in response to the Cybersecurity Information Sharing Act of 2015, a federal law mandated to improve cybersecurity in the U.S. through enhanced sharing of information about cybersecurity threats.

Office of
Information Security
Securing One HHS

Health Sector Cybersecurity Coordination Center

What We Offer

Sector and Victim Notifications
Direct communications to victims or potential victims of compromises, vulnerable equipment, or PII/PHI theft, as well as general notifications to the HPH about current impacting threats via the HHS OIG.

Alerts and Analyst Notes
Documents that provide in-depth information on a cybersecurity topic to increase comprehensive situational awareness and provide risk recommendations to a wide audience.

Threat Briefings
Presentations that provide actionable information on health sector cybersecurity threats and mitigations. Analysts present current cybersecurity topics, engage in discussions with participants on current threats, and highlight best practices and mitigation tactics.

Contacts

HHS.GOV/HC3

HC3@HHS.GOV