1 April 2019

Security Implications of Quantum Computing – Current Realities

Is quantum computing a cybersecurity threat?

“Quantum computing is the end of cryptography as we know it,” is the current topic du jour. Is this really the case? Fortunately, it is not! To be perfectly clear, quantum computing does not currently present a threat to modern cryptography, nor does it present a threat anytime soon. In fact, it is not clear if quantum computing will ever be a cryptography threat. It is true that Quantum computing might break modern cryptography in the far distant future—likely decades—but that is not inevitable. Given this situation, there are a number of misconceptions and misunderstandings about the impact quantum computing might have on cryptography. This has led to significant uncertainty in the technology marketplace. This paper addresses the possible risks to cryptography posed by quantum computing so that one can make informed decisions about the current implementation of technology solutions which depend on the use of strong cryptography.

> **Comment from Dorothy Denning, Emeritus Distinguished Professor of Defense Analysis, Naval Postgraduate School**
>
> “Cybersecurity researchers and analysts are rightly worried that a new type of computer, based on quantum physics rather than more standard electronics, could break most modern cryptography. The effect would be to render communications as insecure as if they weren’t encoded at all.
>
> Fortunately, the threat so far is hypothetical. The quantum computers that exist today are not capable of breaking any commonly used encryption methods. Significant technical advances are required before they will be able to break the strong codes in widespread use around the internet, according to a new report from the National Academy of Sciences.”[1]

Reality One – Quantum Computers Are Exponentially Faster than Classical Computers

That fact that quantum computers are exponentially faster than classical computers is the reason for all of the interest. While quantum computers are exponentially faster, the potential ability to break modern cryptography is only a remote possibility. It has yet to be proved; there are no quantum computers that are capable of breaking any modern, commonly used encryption methods, and success, if ever, is a long way off. It is only recently, that we have built the first, nascent quantum computers.

[1] https://theconversation.com/is-quantum-computing-a-cybersecurity-threat-107411

Comment from National Academy of Sciences, Engineering and Medicine report

> "Before quantum computers, all known realistic computing devices satisfied the extended Church-Turing thesis, [1 , 2] which said that the power of any computing device built could be only polynomially faster than a regular "universal" computer—that is, any relative speedup would scale only according to a power law. Designers of these "classical" [3] computing devices increased computing performance by many orders of magnitude by making the operations faster (increasing the clock frequency) and increasing the number of operations completed during each clock cycle. While these changes have increased computing performance by many orders of magnitude, the result is just a (large) constant factor faster than the universal computing device. Bernstein et al. showed in 1993 that quantum computers could violate the extended Church-Turing thesis, [4] and in 1994 Peter Shor showed a practical example of this power in factoring a large number: a quantum computer could solve this problem exponentially faster than a classical computer. While this result was exciting, at that time no one knew how to build even the most basic element of a quantum computer, a quantum bit, or "qubit," let alone a full quantum computer. But that situation has recently changed."[2]

Reality Two – Quantum Computing May Have A Major Impact On Cryptography

While it is true that quantum computing may have a major impact on cryptography, may is the operative word. It all depends on developing a large quantum computer capable of running Shor's algorithm on the very large public keys that are commonly used in today's implementations. This is not a forgone conclusion. Much work remains to be done to prove the feasibility, let alone that actual construction of such computers. The concerns have been raised because of the need to protect sensitive information for long periods—thirty to fifty years is typical. If scientists are able to construct such a computer, say forty to fifty years from now, then current sensitive information could be compromised at that time. It is this potential that is the impetus for the development of post-quantum cryptography.

Comment from National Academy of Sciences, Engineering and Medicine report

> "**QUANTUM COMPUTERS AND CRYPTOGRAPHY**
>
> Quantum computing will have a major impact on cryptography, which relies upon hard-to-compute problems to protect data. Shor's algorithm running on a large quantum computer will greatly reduce the required computation (the workfactor) to extract the private key from the asymmetric ciphers used to protect almost all Internet traffic and stored encrypted data. There is strong commercial interest in deploying post-quantum cryptography well before such a quantum computer has been built.

[2] National Academies of Sciences, Engineering, and Medicine. 2019. *Quantum Computing: Progress and Prospects. (Pages xi–xii)* The National Academies Press, Washington, DC. DOI: https://doi.org/10.17226/25196.

> Companies and governments cannot afford to have their now-private communications decrypted in the future, even if that future is 30 years away. For this reason, there is a need to begin the transition to post-quantum cryptography as soon as possible, especially since it takes over a decade to make existing Web standards obsolete (see Section 4.4)."[3]

Reality Three – Public Key Cryptography Compromise At Least A Decade Away (Or Longer)

The potential compromise of current public key cryptography is long way off. "Highly unexpected within the next decade" in the passage referenced below, or "even if the future is 30 years away" in the passage referenced above. It is important to note that that the time frames given in the National Academy of Sciences, Engineering and Medicine report are highly conservative, as they should be.

> **Comment from National Academy of Sciences, Engineering and Medicine report**
>
> "**Key Finding 1:** Given the current state of quantum computing and recent rates of progress, it is highly unexpected that a quantum computer that can compromise RSA 2048 or comparable discrete logarithm-based public key cryptosystems will be built within the next decade. (Chapter 7)
>
> **Key Finding 10:** Even if a quantum computer that can decrypt current cryptographic ciphers is more than a decade off, the hazard of such a machine is high enough—and the time frame for transitioning to a new security protocol is sufficiently long and uncertain—that prioritization of the development, standardization, and deployment of post-quantum cryptography is critical for minimizing the chance of a potential security and privacy disaster. (Chapter 7)
>
> Given the large risk a quantum computer poses to current protocols, there is an active effort to develop post-quantum cryptography, asymmetric ciphers that a quantum computer cannot defeat. These are likely to be standardized in the 2020s. While the potential utility of Shor's algorithm for cracking deployed cryptography was a major driver of early enthusiasm in quantum computing research, the existence of cryptographic algorithms that are believed to be quantum-resistant will reduce the usefulness of a quantum computer for cryptanalysis and thus will reduce the extent to which this application will drive quantum computing R&D in the long term (see Section 4.3)."[4]

[3] National Academies of Sciences, Engineering, and Medicine. 2019. *Quantum Computing: Progress and Prospects. (Page 8)* The National Academies Press, Washington, DC. DOI: https://doi.org/10.17226/25196.

[4] National Academies of Sciences, Engineering, and Medicine. 2019. *Quantum Computing: Progress and Prospects. (Page 9)* The National Academies Press, Washington, DC. DOI: https://doi.org/10.17226/25196.

Reality Four – Symmetric Key Cryptography Cannot be Compromised

It is most important to note that quantum computing cannot compromise symmetric key cryptography. As we know, symmetric key cryptography is one "half" of the cryptography used to secure sensitive information; public key cryptography for key exchange, and symmetric key cryptography for encrypting the sensitive content.

> **Comment from National Academy of Sciences, Engineering and Medicine report**
>
> **"The impact of a quantum computer:** AES is a perfect fit for Grover's algorithm, which was discussed in the previous chapter. The algorithm can identify the secret key over the entire 128-bit key space of AES-GCM in time proportional to the square root of 2^{128}—namely, time 2^{64}. Running the algorithm on a quantum computer is likely to require around 3,000 logical qubits and extremely long decoherence times.
>
> How long would a quantum computer take to run the 2^{64} steps of Grover's algorithm, called Grover steps, to break AES-GCM? That is hard to answer today, since it depends on how long a quantum computer takes to execute each Grover step. Each Grover step must be decomposed into a number of primitive operations to be implemented reversibly. The actual construction of the quantum circuit for each Grover step can substantially increase the number of qubits and coherence times required for physical implementation. Using classical hardware, one can build a special purpose circuit that tries 10^9 keys per second. Assuming a quantum computer can operate at the same speed, it would need about 600 years to run Grover's algorithm for the necessary 2^{64} steps. It would therefore take a large cluster of such quantum computers to crack a 128-bit key in a month. In fact, this is an overly optimistic estimate, because this type of quantum computer requires logical qubits; this not only greatly increases the number of physical qubits required, but, as described in Section 3.2, operations on logical qubits require many physical qubit operations to complete. This overhead is high for "non-Clifford" quantum gates, which are common in this algorithm. As Table 4.1 shows, assuming 200-nanosecond gate times and current algorithms for error correction, a single quantum computer would require more than 10^{12} years to crack AES-GCM.
>
> Even if a computer existed that could run Grover's algorithm to attack AES-GCM, the solution is quite simple: increase the key size of AES-GCM from 128-bit to 256-bit keys. Running Grover's attack on a 256-bit key is effectively impossible, since it requires as many steps as a classical attack on a 128-bit key. Transitioning to a 256-bit key is very practical and can be put to use at any time. Hence, AES-GCM can be easily made secure against an attack based on Grover's algorithm."[5]

[5] National Academies of Sciences, Engineering, and Medicine. 2019. *Quantum Computing: Progress and Prospects. (Pages 100–101)* The National Academies Press, Washington, DC. DOI: https://doi.org/10.17226/25196.

Reality Five – Post-Quantum Cryptography Solutions Will Be Available When Necessary

Post-quantum cryptography solutions are being developed on an expedited basis. "The National Institutes of Science and Technology (NIST) has initiated a process to solicit, evaluate, and standardize one or more quantum-resistant public-key cryptographic algorithms.
The **Round 2 candidates** were announced January 30, 2019. NIST has developed a **Guideline for Submitting Tweaks** for 2nd Round candidates. **NISTIR 8240*, Status Report on the First Round of the NIST Post-Quantum Cryptography Standardization Process is now available.***"[6]
"The NIST process is scheduled to conclude by 2022-2024; its selections are likely to become frontrunners for broader standardization—for example, through the Internet Engineering Task Force (IETF), the International Organization for Standardization (ISO), and the International Telecommunication Union (ITU). Internet systems will likely begin incorporating post-quantum resistant cryptography once the NIST process concludes, if not sooner."[7] This will keep information secure even if large-scale quantum computers become widely available. Furthermore, some standards—IEEE Std 1363.1 and OASIS KMIP—have already been updated to incorporate post-quantum cryptography.

> **Comment from National Academy of Sciences, Engineering and Medicine report**
>
> "4.3 **POST-QUANTUM CRYPTOGRAPHY**
>
> The cryptographic research community has been working to develop replacement algorithms that are expected to be secure against an adversary with access to a large-scale quantum computer. These replacement algorithms, when standardized, will be executable on off-the-shelf classical processors. Their security relies on mathematical problems that are believed to be intractable even for a large-scale quantum computer. These algorithms, currently being evaluated by NIST, are thus expected to remain secure even after large-scale quantum computers are widely available. Like all cryptography, the hardness of these problem cannot be proved, and must continue to be evaluated over time to ensure that new algorithmic approaches do not weaken the cypher."[8]
>
> **Comment from Luther Martin, Distinguished Technologist, Micro Focus**
>
> "**It's not as bad as it sounds**
> But all is not lost. Many well-known public-key encryption algorithms are secure from attacks by quantum computers. Some have already been vetted by reputable standards organizations—IEEE Std 1363.1 and OASIS KMIP (PDF) already specify quantum-safe

[6] https://csrc.nist.gov/Projects/Post-Quantum-Cryptography
[7] National Academies of Sciences, Engineering, and Medicine. 2019. *Quantum Computing: Progress and Prospects. (Page 106)* The National Academies Press, Washington, DC. DOI: https://doi.org/10.17226/25196.
[8] National Academies of Sciences, Engineering, and Medicine. 2019. *Quantum Computing: Progress and Prospects. (Page 105)* The National Academies Press, Washington, DC. DOI: https://doi.org/10.17226/25196.

> algorithms. So if progress in quantum computing ever threatens to make today's public-key algorithms crackable, it will be easy to move to quantum-safe alternatives. That is the caveat to becoming quantum-safe."[9]

Reality Six – Major Impediments Remain to Commercially Viable Quantum Computing

It appears that the high speed of quantum computing has been the primary driver of the quantum cryptography discussion. However, fast quantum processor speed is not enough. Here are two of the many major impediments that have yet to be overcome.

1. The noise and decoherence nature of quantum mechanics limit quantum computing's practical application to cryptography. This is particularly the case with digital NISQ (Noisy Intermediate-Scale Quantum) computers, the ones which show the most promise for breaking current public key cryptography. Unless there is a major breakthrough in error correction and achieving repeatable, reliable results, however, these issues will significantly impede any meaningful decryption efforts for the foreseeable future.
2. Persistent quantum memory and quantum-speed circuitry do not exist and are not anticipated. This means that all quantum computation must swap data and code commands through standard CMOS memory and circuitry, constraining quantum processes to snippets of quantum-chip-resident code and data, and performance dependent on classical network I/O and CMOS execution speeds.

> **Comments from National Academy of Sciences, Engineering and Medicine report**
>
> "**Finding:** There is no publicly known application of commercial interest based upon quantum algorithms that could be run on a near-term analog or digital NISQ computer that would provide an advantage over classical approaches."[10]
>
> "**Finding:** Quantum computers are unlikely to be useful as a direct replacement for conventional computers, or for all applications; rather, they are currently expected to be special-purpose devices operating in a complementary fashion with conventional processors, analogous to a co-processor or accelerator."[11]

Reality Seven – Current Quantum Computing Approaches Will NOT Break Current Cryptography

As we have seen, "Quantum computing is NOT the end of cryptography as we know it." In spite of all of the excitement, and the tremendous resources and energy being devoted to quantum cryptography worldwide, it is important to recognize that the current solutions are not able to

[9] https://techbeacon.com/security/quantum-computing-end-security-we-know-it

[10] National Academies of Sciences, Engineering, and Medicine. 2019. *Quantum Computing: Progress and Prospects. (Page 83)* The National Academies Press, Washington, DC. DOI: https://doi.org/10.17226/25196.

[11] National Academies of Sciences, Engineering, and Medicine. 2019 *Quantum Computing: Progress and Prospects. (Page 87)* The National Academies Press, Washington, DC. DOI: https://doi.org/10.17226/25196.

break current cryptography, nor can they be scaled reasonably to achieve this result. We, of course, need to keep our eye on the progress within quantum computing, but for the time being it remains, at best, a very distant threat.

> **Comment from National Academy of Sciences, Engineering and Medicine report**
>
> "**Finding:** While much progress has been made in the development of small-scale quantum computers, a design for a quantum computer that can scale to the size needed to break current cryptography has not been demonstrated, nor can it be achieved by straightforward scaling of any of the current implementations."[12]

Selected Resources

https://theconversation.com/is-quantum-computing-a-cybersecurity-threat-107411

https://techbeacon.com/security/quantum-computing-end-security-we-know-it

https://www.nap.edu/catalog/25196/quantum-computing-progress-and-prospects

Author

Dan Corcoran
TrustWrx Strategic Security Advisor

Director, Information Security, ID Analytics; Cybersecurity responsibility for Intuit's TurboTax, Mint and Quicken offerings; Director of Information Security at Electronic Arts, Director of Security at VeriSign, Chief Scientist for Security Services at Equifax Secure (1998-2000), and Manager of Network Design at Electronic Data Systems. Author of: *A User's Guide to X.509 v.3 Digital Certificates*.

[12] National Academies of Sciences, Engineering, and Medicine. 2019. *Quantum Computing: Progress and Prospects. (Page 113)* The National Academies Press, Washington, DC. DOI: https://doi.org/10.17226/25196.