A Review of the Current State of Quantum Computing and its Effects on Secure Voice Encryption Schemes Used Today

Introduction

As new advancements are beginning to allow quantum computers to approach market-readiness, cybersecurity professionals are beginning to address their security frameworks and the potential for post-quantum resistant encryption schemes.

In this paper we look at where quantum computers are in breaking the encryption schemes used for secure voice communications: RSA, ECC, and AES. We show why companies should consider moving towards post-quantum encryption today, and how the United States is competing against China in the fight for quantum computer supremacy.

Types of Quantum Computers

To the uninitiated, a quantum computer is a quantum computer, however when discussing their ability to solve problems, we find several general types. Below are brief descriptions of the two main types of quantum computers that exist today:

Quantum Annealer: This is the least powerful and "easiest" to build quantum computer however it is also the most restrictive regarding the types of problems it can solve [17]. Quantum annealing computers are designed to work on optimization problems, where one tries to find the best solution from a set of possible solutions [17]. For example, the famous traveling salesman problem, where the salesman wants to know what would be the shortest path to take to visit his customers. The most popularized version is D-Wave 2000Q, equipped with 2000-qubits which has outperformed highly specialized algorithms run on state-of-the-art classical servers by factors of 1,000 to 10,000 times [18]. In the commercial world, the auto manufacturer Volkswagen (VW) and D-Wave completed a joint project using a D-Wave quantum computer to optimize traffic flows, using data from 10,000 taxis in Beijing, China [20]. As impressive as these systems are, they are not the quantum computers that will be used to break current VoIP encryption schemes.

Universal Gate Quantum: These are the quantum computers that are forcing the post-quantum encryption discussion. A universal gate quantum computing system relies on building reliable qubits where basic quantum circuit operations, like the classical operations we know, can be put together to create any sequence, running increasingly complex algorithms such as Shor's (to break RSA cryptography) or Grover's (to break AES) [19]. The main difficulty in building these types of quantum computers is being able to research and design chips and test them in an efficient manner to improve coherence (length of time the information is stored and can be manipulated) and qubit reliability [19]. The largest known Universal Gate Quantum computer, Google's Bristlecone, contains 72-qubits in comparison with quantum annealing computers' several thousand qubits, however the former can solve a larger breath of problems.

Current State of Quantum Computing on Key-Exchange Algorithms RSA and ECC

Key-exchange algorithms like RSA and Elliptic Curve Cryptography (ECC) govern the way the server and client determine the symmetric keys to use for securing the RTP stream along with providing a secure stream for the VoIP signaling path. The security of RSA and ECC are based on the difficulty in solving two mathematical problems. RSA bases its difficulty on the factorization of large numbers while ECC bases its difficulty on solving discrete logarithms [1]. Under the hood, both RSA and ECC have similar mathematical structures which allow them to be broken running Shor's algorithm on a quantum system rather quickly [1].

In 1994, Peter Shor showed that a quantum computer could be used to factor a number in polynomial time, thus effectively breaking RSA [2]. Polynomial time for breaking encryption schemes is important because it indicates that it can be run in short enough time to be considered practical. Shor's algorithm makes use of the structure of the factoring problem itself. Instead of looking for factors directly, it uses some mathematical property of factoring. Shor's algorithm reduces the prime factorization problem into a problem of order (or period) finding [2]. Even in 1994, before quantum computers existed, Shor speculated that quantum algorithms could even break RSA on a quantum computer asymptotically faster than encrypting with RSA on a classical computer [3].

When decrypting a message becomes easier then encrypting, the encryption algorithm itself becomes pointless. In quantum computing, the number of qubits needed to break a cryptosystem depends upon the algorithm proposed [1]. For RSA and ECC-based cyphers, it has been shown that a 1,000-qubit quantum computer can break 160-bit elliptical curves, while factorizing a 1024-bit RSA would require 2,000-quibits [1]. For 2048-bit RSA keys, estimates show that a quantum computer consisting of 4,000-qubits would be needed. Today's largest quantum computer is Google's Bristlecone which contains 72-qubits. Bristlecone edged out IBM's 50-qubit quantum computer [6]. Google's Bristlecone could have important potential uses in breaking current cryptography strategies or optimizing searching in the long term. But in the short term, they could potentially be useful for things like modeling complex molecules better than classical computers, finding optimal solutions to complicated problems, and improving artificial intelligence [6].

With the understanding that building a large enough quantum computer can break current key-exchange algorithms, how far are we from breaking ECC or RSA? In a February 2018 Forbes' article titled "Mind the Gap -- How Quantum Computers May Leave Today's Online Services Vulnerable", Dustin Moody, from the National Institute of Standards and Technology (NIST), estimated that it will take 15 years for quantum computers to break RSA-2048 [4]. The quantum computers we have today are still slow to handle any real-time quantum decryption of key-exchange algorithms [4]. NIST Internal Report 8105 entitled "Report on Post-Quantum Cryptography" estimated that it is likely that a quantum computer capable of breaking 2000-bit RSA in a matter of hours could be built by 2030 for a budget of about a billion dollars [5].

Current State of Quantum Computing on AES Encryption

AES is a type of block cipher algorithm currently used in securing the RTP stream containing the voice packets in a VoIP call. AES has been chosen because of its very high security levels and performance combined with its rapidity of calculation, ability to resist various types of attacks, and ability to be run on a large variety of platforms [6]. AES also has the advantage of occupying very little memory, consequently making it very suitable for low memory capacity devices like Smart cards [6]. The block cipher length is fixed at 128-bit: encryption keys of this algorithm can be 128, 192 or 256 bits [6].

Unlike RSA, which is based on the difficulty of factoring large numbers, the difficult math problem for AES is solving systems of multivariate quadratic equations, often called the MQ problem [8]. Solving a system of linear equations is relatively easy. If there are n equations in n unknowns, then via processes such as Gaussian elimination it can be solved in a bound time frame of n^3[6]. However, in AES, the problem is much harder because a computer would need to solve a system of m equations with n unknowns each of which increases the difficulty tremendously [6].

For AES, quantum computing is considered a minor threat with the only known quantum-based decryption algorithm being Grover's algorithm [1]. Grover's algorithm offers a square root speed-up over classical brute force algorithms. For example, Grover's algorithm could find the secret key of an AES-128-bit scheme in roughly 2^64 iterations [1]. In a 2015 arXiv paper titled "Applying Grover's Algorithm to AES: Quantum Resource Estimation", it was found that the number of logical qubits needed to implement a Grover attack on AES was about 3,000-qubits for AES-128 and 7,000-qubits for AES-256 [9]. However, due to the large circuit depth of unrolling the entire Grover iteration, it seems challenging to implement this algorithm on an actual physical quantum computer [8].

Under the hood, AES uses a substitution-permutation network to scramble and unscramble data, and as such, its security is weakened slightly by quantum attacks. To compensate for this weakening, it is necessary to simply double the key length, with no change to the algorithm. This creates a secure cipher, resistant to quantum attack. So, selection of a quantum-resistant algorithm like AES-256, judiciously configured and carefully integrated, will result in a cryptosystem that will be secure today and in decades to come [7].

Why the Push Towards Post-Quantum Encryption?

Since the "quantum-decryption apocalypse" is several years away, what is the big rush in switching our cryptographic schemes now? Are there any major benefits?

There are several benefits for moving forward today with upgrading.

Data-at-Rest: Even though voice communication is safe today, if it stored for posterity via recordings or converted to a secure text-based document, it could be broken once quantum computers are powerful enough. This is often referred to as securing data-at-rest.

Replacing crypto schemes takes time: If the quantum-decryption apocalypse were to occur six months or even a year from now, would you have enough time to update all servers and smart devices? Simply doubling the target security level is adequate, but generally imposes much more noticeable costs upon public-key systems than upon AES; these costs motivate research aimed at understanding the exact impact of Grover's algorithm, to be able to use smaller key sizes [12].

Planning for alternatives to CAC and PIV: Smart cards, including Personal Identity Verification (PIV) cards and Common Access Card (CAC), are used by the U.S. federal government to ensure that the right people have access to the right information (and physical facilities) at the right time. Millions of smart cards have been issued to government employees and approved contractors, all of which are securely connected via complex yet interoperable PKIs. However, smart cards use public key cryptography which will be broken by a large-scale quantum computer [13].

Standardization: Several standardization bodies have recognized the urgency of switching to cryptosystems that remain secure against attacks by quantum computers. This is an important development because many applications of cryptography require all parties to use the same cryptographic system; standardization is a prerequisite for widespread deployment [12].

Bring Your Own Devices (BYOD): Organizations that allow employees to use their smart phones for company business will need to determine how to upgrade devices that can't handle or don't support the latest encryption schemes. Typically, smart phones use encryption schemes that are built into the operating system. Given that not everyone updates their devices and that people use devices with outdated operating systems and hardware it can prove to be difficult and time consuming to ensure that everyone is safe.

NSA and CSS Recommendations

In 2016, the National Security Agency (NSA) and Central Security Service (CSS) published an Information Assurance Directorate (IAD) titled "Commercial National Security Algorithm Suite and Quantum Computing FAQ". The document defines a set of public standards that may be used to protect national security systems (NSS) until public standards for quantum resistant cryptography exist [14]. Even though these standards are intended for government programs, they are also very relevant for the commercial space.

This IAD provided two key items:

- An announcement stating that the following should no longer be used when connecting to a NSS:
  - ECDH and ECDSA with NIST P-256
  - SHA-256
  - AES-128
  - RSA with 2048-bit keys
  - Diffie-Hellman with 2048-bit keys

- An announcement stating that the following, at a minimum, should be used:
  - RSA 3072-bit or larger
  - Diffie-Hellman 3072-bit or larger
  - ECDH with NIST P-384
  - ECDSA with NIST P-384
  - SHA-384
  - AES-256

One item to point out is that the above recommendation is a transitory step until a better set of algorithms is available. As of this paper, no new recommendations have been made. NIST is currently reviewing 69 quantum-resistant cryptographic algorithms that would protect sensitive government information well into the foreseeable future [15]. NIST held a workshop in April 2018 for all accepted candidate algorithms with the next steps being for the cryptographic community to start the difficult work of ensuring that these submissions meet NIST's requirements [15]. Note that the review is planned to take 2 years with a draft available between 2022 and 2024 [16].

United States vs. China in the Race to Quantum Supremacy

Companies around the world are moving forward with building quantum computers that can deliver on the promises made of working in the quantum realm. For the first time, companies in the United States could be surprised by the technological leaps of other nations, particularly China. With universities in China and US technology companies racing to develop quantum computers, it is necessary to understand what each country is doing to becoming leaders in this field.

In January 2018, Intel showed off Tangle Lake, a 49-qubit quantum processor. Then in March, Bristlecone, a 72-qubit quantum processor by Google, was unveiled with the goal of achieving quantum supremacy [10]. Add to the mix the companies such as Rigetti Computing, which focus on making programmable "quantum logic gates" available to customers [10].

To continue this boost in industry and academia in leading the quantum race, the U.S. House of Representatives introduced the National Quantum Initiative Act (H.R. 6227) which calls for acceleration in basic research, establishes collaboration, promotes standards development, and establishes research and education centers. The act also calls for allocation of US$625 million to the Department of Energy for FY 2019 to 2023, US$250 million to the National Science Foundation, and US$400 million to the Department of Commerce which houses the National Institute for Standards and Technology (NIST) [10]. In total the U.S. will be devoting US$1.275 billion over five years to support research and development efforts in quantum technology.

Even with this funding increase, the. U.S government's effort is still dwarfed by China's efforts, whose government announced last September that it would build the world's largest quantum research facility in Hefei province. The $10 billion, 4-million-square-foot national laboratory is slated to be completed around March 2020 and is dedicated to making major advances in quantum technology, including computers, sensors, and cryptography [11]. As South China Morning Post recently stated, this intensive focus on quantum computing and technology highlights China's efforts to "transform itself from the factory of the world into an advanced economy built on high-tech industries" [10]. China also sees that quantum technologies will impact others such as fiber-optic, thus China's push for a "Broadband China" strategy which aims at increasing the percentage of households with broadband access from 40% in 2015 to 70% in 2020. Compare this to the U.S. where fewer than 20% of households currently have access to fiber optics and with much of the country relying on copper-based services or none at all [10].

China's first major milestone in this area was the 2016 launch of its Micius quantum satellite, which can anchor a secure ground-to-space quantum communications network. China has also made key advances in developing a similarly "unhackable" 2,000-kilometer quantum communications network from Shanghai to Beijing [11]. Another major milestone came earlier this year when their scientists managed to pack 18-qubits into just six connected photons [11]. The key reason this is important is that it increases the "degrees of freedom". A typical quantum experiment involves just one degree of freedom across all the particles involved. But particles, like photons, have many degrees of freedom. The result is even faster computations [11].

It may be too early to say which country will be the leader in the quantum realm, however it seems like the U.S. will lead in hardware while China will lead in software and applications. This should be a concern for the U.S. government since China is becoming an even greater economic force and soon will be an equally large cyber security juggernaut.

About REDCOM Laboratories, Inc.

At REDCOM we consider ourselves to be the leaders in secure voice communications. We look at problems holistically, with the intent on understanding the big picture along with the underlying reasoning for it. Our secure voice platforms are used throughout government and military agencies ranging from tactical edge to administrative offices. If you would like to learn more about REDCOM, please visit www.redcom.com.

References

[1] Mavroeidis, Vasileios, et al. "The Impact of Quantum Computing on Present Cryptography." International Journal of Advanced Computer Science and Applications, vol. 9, no. 3, 2018, doi:10.14569/ijacsa.2018.090354

[2] Blanda, Stephanie. "Shor's Algorithm – Breaking RSA Encryption." AMS Grad Blog, 30 Apr. 2014, blogs.ams.org/mathgradblog/2014/04/30/shors-algorithm-breaking-rsa-encryption/

[3] Shor, P. W. (1997). Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM Journal on Computing, 26(5), 1484-26. doi:http://dx.doi.org/10.1137/S0097539795293172

[4] Vamosi, Robert. "Mind the Gap -- How Quantum Computers May Leave Today's Online Services Vulnerable." Forbes, Forbes Magazine, 28 Feb. 2018, www.forbes.com/sites/robertvamosi/2018/02/27/mind-the-gap-how-quantum-computers-may-leave-todays-online-services-vulnerable/#342523d52ced

[5] Chen, Lily, et al. "Report on Post-Quantum Cryptography." NISTIR 8105, Apr. 2016, doi:10.6028/nist.ir.8105.

[6] Mandelbaum, F. "Google Unveils Largest Quantum Computer Yet, but So What?" Gizmodo, gizmodo.com/google-unveils-largest-quantum-computer-yet-but-so-wha-1823546420.

[7] Chang, Linus. "How Secure Is Today's Encryption against Quantum Computers?" BetaNews, betanews.com/2017/10/13/current-encryption-vs-quantum-computers/.

[8] Nover, Harris. "Algebraic Cryptanalysis of AES: An Overview" www.math.wisc.edu/~boston/nover.pdf.

[9] Grassl, Markus, et al. "Applying Grover's Algorithm to AES: Quantum Resource Estimates." Post-Quantum Cryptography Lecture Notes in Computer Science, 2016, pp. 29–43., doi:10.1007/978-3-319-29360-8_3.

[10] Herman, Arthur, and Idalia Friedson. "Quantum Computing: How to Address the National Security Risk." www.quintessencelabs.com/wp-content/uploads/2018/09/Quantum-National-Security-Risk.pdf.

[11] Herman, Arthur. "At Last America Is Moving On Quantum." Forbes, Forbes Magazine, 20 Aug. 2018, www.forbes.com/sites/arthurherman/2018/08/20/at-last-america-is-moving-on-quantum/#5551753c5327

[12] Bernstein, Daniel J, and Tanja Lange. "Post-Quantum Cryptography - Dealing with the Fallout of Physics Success." 4 Sept. 2017, pp. 1–20., eprint.iacr.org/2017/314.pdf

[13] Morris, Jeffery. "Implications of Quantum Information Processing On Military Operations." The Cyber Defense Review, 29 May 2015, cyberdefensereview.army.mil/CDR-Content/Articles/Article-View/Article/1136004/implications-of-quantum-information-processing-on-military-operations/.

[14] "Commercial National Security Algorithm Suite and Quantum Computing FAQ." Cryptome.Org, NSA, CSS, and IAD, Jan. 2016, cryptome.org/2016/01/CNSA-Suite-and-Quantum-Computing-FAQ.pdf.

[15] Allen, Thelma A. "Candidate Quantum-Resistant Cryptographic Algorithms Publicly Available." NIST, 28 Dec. 2017, www.nist.gov/news-events/news/2017/12/candidate-quantum-resistant-cryptographic-algorithms-publicly-available.

[16] Computer Security Division, et al. "Workshops and Timeline - Post-Quantum Cryptography | CSRC." NISTIR 8179 Criticality Analysis Process Model | CSRC, csrc.nist.gov/projects/post-quantum-cryptography/workshops-and-timeline.

[17] Desjardins, Jeff. "The 3 Types of Quantum Computers and Their Applications." Visual Capitalist, 14 Mar. 2016, www.visualcapitalist.com/three-types-quantum-computers/.

[18] "D-Wave Intros 2000-Qubit Quantum Computer, Reveals First Buyer." D-Wave Intros 2000-Qubit Quantum Computer, Reveals First Buyer | TOP500 Supercomputer Sites, 24 Jan. 2017, www.top500.org/news/d-wave-intros-2000-qubit-quantum-computer-reveals-first-buyer/.

[19] Marchenkova, Anastasia. "What's the Difference between Quantum Annealing and Universal Gate Quantum Computers?" Medium, Quantum Bits, 28 Feb. 2016, medium.com/quantum-bits/what-s-the-difference-between-quantum-annealing-and-universal-gate-quantum-computers-c5e5099175a1.

[20] "D-Wave Systems." D-Wave Closes $50M Facility to Fund Next Generation of Quantum Computers | D-Wave Systems, 15 May 2017, www.dwavesys.com/press-releases/d-wave-closes-50m-facility-fund-next-generation-quantum-computers.