Quantum-Safe Security Working Group

What is Quantum-Safe Security?

Introduction: A Short Story

A CIO at a Fortune 500 company receives a call from a Wall Street Journal reporter asking how the company is responding to the announcement of the new commercially available quantum computer that can "break" RSA and Elliptic Curve Cryptography (ECC). This CIO has no plan, so he politely offers a "no comment" to the reporter, and then calls an emergency meeting with his executive team to figure out what can and should be done to protect the company's data residing in the cloud.

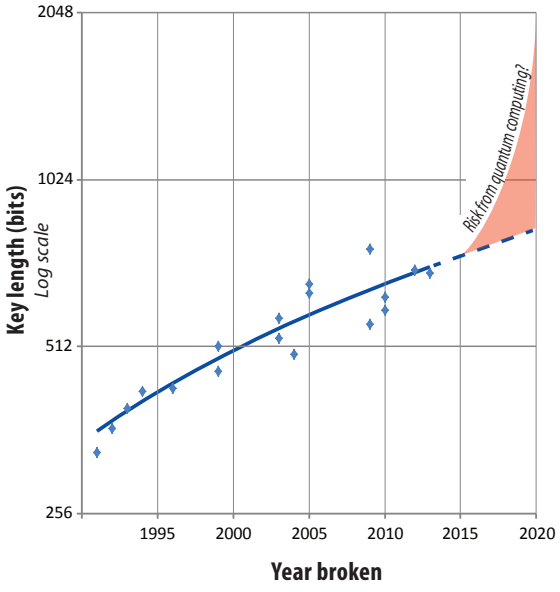
This scenario, while fictional today, is one that could face many executives in the not-too-distant future. There have been many reports of the United States and China investing hundreds of millions of dollars in quantum computing research. Universities and commercial labs around the world are reporting seminal breakthroughs. According to current projections, a multi-purpose quantum computer able to crack the ubiquitous RSA and ECC encryption algorithms will become available by 2030. Taking into account the time needed to build out a quantum-safe infrastructure, efforts need to begin now.

Current Cryptographic Techniques

Transmitting information securely across the web, whether it's only a single credit card number or a full backup of a company's digital assets to the datacenter, is a three-step process. First, the sending and receiving parties exchange an encryption key, using one of several widely accepted algorithms like RSA. Next, the sending party encrypts the data with the exchanged key, using a symmetric algorithm like AES, and sends it to the receiving party. Finally, the receiving party decrypts the data using the exchanged key used to encrypt the data (hence the term "symmetric key"), and uses the data. This has worked well for over thirty years — so what's the problem?

The Threats And Impact

When the RSA algorithm was first introduced, an article in Scientific American in 1977 estimated that it would take 40 quadrillion years to decrypt a message asymmetrically encrypted with RSA-129, a variant of RSA which used a 129 decimal-digit (or 426 bit) key. In fact RSA-129 was factored (cracked) in 1994, less than 20 years later. The figure below shows at what points in time RSA keys of different bit-lengths have or will become vulnerable using standard computers. Although it appears that 1024-bit keys are safe now, it is a proven fact that they will be in jeopardy soon. Larger keys, in particular 2048-bit, will buy us time. Quantum computers, however, will radically change everything. Once perfected, they will be able to rapidly factor RSA keys of any length.



Quantum computers promise to solve, among other things, the thorniest of factorization problems. An early prototype of a quantum computer has recently demonstrated that it can factor a 5-bit asymmetric key. Admittedly, a lot of work remains to go from factoring a 5-bit key to a 2048-bit

one, which is why data encrypted with RSA is safe for the immediate term. However, there is an important angle to consider: RSA-encrypted data that is intercepted and stored today, could be decrypted by quantum computers in the future. And it's not just the RSA and ECC algorithms that are jeopardized by quantum computers—all of the algorithms currently being used to protect encryption keys are subject to the same method of solution.

Proactive Defenses

In anticipation of quantum computers, there are two technologies under development that intend to address the threat: Post-Quantum Algorithms (PQAs) and Quantum Key Distribution (QKD). Both technologies are described in more detail elsewhere, but here is a brief description.

Post-Quantum Algorithms (PQAs) PQAs consist of a number of new algorithms that are designed with the known capabilities of quantum computers in mind. They have already proven resistant to currently known quantum attacks. Because they are implemented purely in software, they can become direct replacements for the software that we use now. In general, PQAs are as fast as or faster than RSA, but they require significantly larger keys. However, they have not yet reached a sufficient level of confidence for their widespread application.

Quantum Key Distribution (QKD) QKD is based on physics. It allows keys to be exchanged between two different locations by using the quantum properties of photons. Should an adversary attempt to intercept the key exchange, changes in the measured quantum properties reveal the attempt and allow for the key to be discarded. Unlike any purely software-based method, QKD systems will remain secure regardless of the computational power available to an adversary. Because it is based on a physical system, QKD requires a supporting fiber or free-space optical infrastructure, and there are limitations on the distance that keys can be exchanged.

The Quantum-Safe Security Working Group (QSSWG) These proactive methods are a start, but until adopted, the threat to encrypted data in the cloud remains. Adoption of new encryption technology cannot, and should not, happen overnight. The Quantum-Safe Security Working Group has been formed within the Cloud Security Alliance to help promote the adoption of technologies that will protect data in the cloud even after quantum computing becomes readily available. For now, the QSSWG recommends the use of both PQA and QKD, in a holistic and integrated solution, to ensure that encrypted data in the cloud is quantum-safe.

References

- Mathematical Games, Martin Gardner, Scientific American, August 1977, *http://www.scientificamerican.com/article/mathematical-games-1977-08/*
- Quantum Safe Cryptography, V1.0.0 (2014-10), ETSI White Paper, ISBN 979-10-92620-03-0.
- The Quantum Algorithm Zoo, A Comprehensive List of Quantum Algorithms, *http://math.nist.gov/quantum/zoo/.*
- Quantum cryptography; Nicolas Gisin, Grégoire Ribordy, Wolfgang Tittel, and Hugo Zbinden; Rev. Mod. Phys. 74, 145, 2002, available on: *http://arxiv.org/abs/quant-ph/0101098v2*