RSiS S. RAJARATNAM SCHOOL OF INTERNATIONAL STUDIES
Nanyang Technological University, Singapore

RSIS COMMENTARY

www.rsis.edu.sg

No. 006 – 13 January 2023

The Cryptography Race: Securing Systems Before Quantum Computers Arrive

By Dr David Joseph

SYNOPSIS

The quantum threat to cybersecurity is a topic gaining awareness, but just how tangible is it? What are the solutions? And what are the challenges facing both "red" and "blue" teams in this game of cat-and-mouse?

COMMENTARY

IN 1994, Peter Shor published a quantum algorithm which could perform specific mathematical tasks incredibly efficiently, so long as one had access to highly controlled hardware being developed in the then nascent and esoteric field of quantum computing. The problems that quantum computers could solve – doing long division and other closely related problems were its forte – did not seem to be of much interest to the general population. For most of the population, the realities of performing computation on a quantum scale were practically science fiction; to cryptographers, however, it represented a far off, albeit existential threat.

Public key cryptography, less than two decades old at the time, relied upon the hardness of solving the exact same set of mathematical problems that Shor's algorithm solves efficiently using a quantum computer. Yet this threat was not completely unseen – one of the co-inventors of RSA (a widely used public key cryptography system), Adi Shamir, had even stated as early as 1989 that "the basis of modern public key cryptography… has become dangerously dependent on the difficulty of a single problem." Three decades on from Shor's initial paper, the modern computational information infrastructure that governs the world we live in is highly dependent on those exact same problems.

The Threat from Advances in Quantum Computing

However, over the past five years there has been renewed fervour among quantum scientists. Their optimism is driven by a small number of engineering breakthroughs which have brought quantum computation to the brink of reality. Enormous hurdles remain, but now we have a clearer picture of the roadmap ahead. Organisations – both public and, increasingly, private – are beginning to toil towards building large fault-tolerant quantum computers capable of cracking our current encryption. No-one knows for sure, but some experts believe we could see such a machine breaking our encryption within 10 years.

The threat of such a quantum machine would be two-fold. The first is to confidentiality: a quantum adversary would be able to decrypt traffic that has been exchanged between parties who believe that the only ones who can read the data are those with whom they have securely exchanged a key. The problem here is that such data can be downloaded and stored as of today, known as the “store now, decrypt later” threat. The second threat is to authenticity, as with a quantum computer, one could forge digital signatures, proclaiming to be Google, Amazon, a government website, or any party using insecure signature algorithms. This false identity can then be used to gain trust and access for malevolent means.

Emergence of Post-Quantum Cryptography

Meanwhile, in the intervening 30 years, mathematicians and cryptographers have not been resting on their laurels. They have developed a wide suite of algorithms to ensure confidentiality and authenticity using other mathematical problems, which they believe will remain resistant to quantum attacks. These algorithms are known together as post-quantum cryptography (PQC). PQC algorithms are categorised by their underlying “hard problem,” with flavours such as lattices, codes, hashes, and more. For the past five years, the US government has been running the most prominent PQC standardisation process in the world to select the public key cryptosystems of the next era.

Such standardisation cannot be rushed. Even after many years of prodding and poking at cryptosystems, late-stage algorithms such as Rainbow (Multivariate) and SIKE (Isogenies) have been broken, potentially undermining confidence in the remaining candidates. For this reason, many promote a hybrid approach to migration (combining PQC and traditional cryptography), so that systems maintain their current levels of security even if the PQC algorithm is subsequently broken. Nevertheless, the cryptographic community does have strong confidence in the algorithms recently announced to be standardised.

From Standardisation to Integration

Once complete, these standardised mathematical formulae will begin to permeate into web browsers, email, government communications, 5G, and practically every secure communication protocol across the internet and telecommunications. But the integration will not happen by itself. Untangling the internet’s spaghetti history of cybersecurity protocols, patches, poor security implementations, and more, will take teams of engineers many years to perform. Their task is simple: find public key cryptography wherever it exists, rip it out (if vulnerable), and replace it with quantum-resistant standardised successors.

No-one knows exactly how long we have until large fault-tolerant quantum computers arrive. That depends on the best efforts and scientific breakthroughs of the world's leading quantum engineers, corporations, and government programmes. But the transition to quantum-resistant communications must happen for organisations to retain the trust of their users in an era where quantum computers exist, and cybersecurity and privacy top the global data agenda.

Dr David Joseph is a Research Scientist at SandboxAQ. This commentary is based on remarks delivered at a RSIS event.

S. Rajaratnam School of International Studies, NTU Singapore
Block S4, Level B3, 50 Nanyang Avenue, Singapore 639798
T: +65 6790 6982 | E: rsispublications@ntu.edu.sg | W: www.rsis.edu.sg