Quantum1Net

Cryptography for a Post-Quantum World

Addressing the Security Challenges Ahead

Introduction

The RSA cryptography platform is now 40 years old. While it has served well in securing the Internet and digital communications, its days are numbered due to the unyielding advance of Moore's law and the emergence of quantum computing. Significant effort and resources are being employed by hackers to crack RSA and other forms of encryption.

The rise of quantum computing makes cracking RSA and various other forms of encryption feasible in the near future. Classical computers use binary bits, which have a value of either zero or one. Strings of these zeroes and ones translate into data, but the nature of the bit means only one calculation can be done at a time. However, with quantum computing, each quantum bit (called a *qubit*) can both be a zero and one at the same time. This difference means quantum computers can store vastly more data, and do many more calculations per second, making them perfect for code breaking applications.

With these quantum computing technologies on the cusp of a breakthrough making the technology ready to crack existing methods of encryption, the time to act is now. Once RSA is cracked, mission critical applications like HTTPS, credit and debit card processing, and government systems face the immediate risk of compromise. The chaos resulting from such a hack would be totally disruptive to the social and economic framework of daily life.

This is why we are developing a quantum generated, key secured data transmission platform called Quantum1Net. Leveraging quantum computing, we are able to provide a level of complexity in cryptographic key generation that is not possible by traditional means. We expect quantum computing to play a key role in the future of encryption.

The End of RSA Encryption

For four decades, electronic communications have been secured by a method known as RSA, named for the three researchers that developed the method: Ron Rivest, Adi Shamir, and Leonard Adleman. The process works due to the difficulty in factoring very large numbers. It takes a large amount of computing power both to produce and then factor these numbers, something that Is all but impossible with traditional computing techniques.[1]

The difficulty in doing so was illustrated in a 2009 study. Researchers found that a 768-bit (232 digit) number took hundreds of machines and nearly two years to crack, while a 1024-bit RSA key takes nearly a thousand times as long[2], and that's the lowest bit RSA key type currently used.

[1] Rivest, R.; A. Shamir; L. Adleman (1978). "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems". Communications of the ACM 21 (2): 120–126.

[2] Kleinjung; et al. (2010-02-18). "Factorization of a 768-bit RSA modulus" (PDF). International Association for Cryptologic Research. Retrieved 2017-11-05.

This means that it's impractical to even attempt to hack RSA encryption keys simply due to the amount of resources necessary to do so, and the so called "factoring problem" is the reason why a 40-year-old encryption strategy remains popular to this day. Hackers look to work fast, but RSA hacking is a slow and laborious process.

RSA security depends on the limits of traditional computing while technology is rapidly advancing and the emergence of quantum computing urgently necessitates a new encryption strategy. Far less resources and time would be necessary to crack even the strongest RSA keys with quantum computing. Quantum computing empowers the first credible threat to RSA encryption since its inception.

Quantum Computing

So, what is quantum computing?

The Traditional computers work by storing data in a string of *bits*, which either hold a value of 0 or 1. Long strings of bits store information, but at any one time that bit can only have one value or another, so only one calculation can be done at one time. Quantum computing works differently. It is based on the unique behavior of subatomic particles to be able to exist in more than one state at a time.

This allows quantum bits, called *qubits*, to store massive amounts of information while at the same time requiring less energy to do so. The result are computers able to run much more complex calculations, and far faster than a traditional computer.[3]

Quantum Computing and Code Breaking

While quantum computers will have a positive effect on the technology industry, their power also presents an immediate security issue. RSA depends on the complexity of factorization of large numbers to keep data encrypted. Due to its architecture, quantum computing becomes an immediate solution to this problem.

Since qubits can have multiple states at the same time, called superposition of states, allowing for many more computations, quantum computers become a logical code breaking mechanism. Work is already underway, and the NIST expects a quantum computer capable of breaking RSA-2048 in a matter of hours by 2030 to be buildable at a cost of approximately one billion dollars.[4]

While that seems a long way off (and expensive), the actual point where RSA might be broken could be much sooner. If someone wants to pay the money, it's likely a computer could be built that could crack RSA in a matter of weeks or months well within the next decade. It is very difficult

[3] Beall, A. (2017-03-23). "Inside the weird world of quantum computers." Wired UK. Retrieved 2017-11-05.
[4] NIST (2016-04). "Report on Post-Quantum Cryptography" (PDF). National Institute of Standards and Technology. NIST-IR-8105 (draft). Retrieved 2017-11-05.

to say precisely when it will occur – or who might do it yet the ultimate occurrence of large scale quantum computing remains a near certainty

It will be expensive to do, but without our current encryption methods changing the value of the result would be priceless to who ever accomplishes it.

The NSA and Quantum Computing

Quantum computing has gained the attention of the top U.S. spy agency. Documents leaked by the former NSA contractor Ed Snowden in 2014, indicated that the agency was funding an $80 million project aiming to build "a cryptologically useful quantum computer."[5] NSA officials hoped that such a machine would enable them to dramatically improve digital spying efforts.

From the documents, it appears as if the NSA was no closer to a workable quantum computer than others, however it was keeping pace with some of the leading quantum computing labs worldwide. How their work is progressing or if they're any closer to success is unknown.

In 2016, it mentioned the risk in a Q&A document intended for those working with sensitive data. "There is growing research in the area of quantum computing, and enough progress is being made that NSA must act now," it wrote.[6] How it was going to act, the NSA was unsure of itself. It admitted no quantum-computer resistant cryptography method existed, so it was only able to recommend algorithms "believed to be safe from attack by a large quantum computer."

The NSA in other words is no less prepared for encryption in the post-quantum area than the rest of the industry. The race is on to figure out a new encryption method. *MIT Technology Review* points out that cracking today's keys would take a quantum computer with hundreds of millions of qubits. We're currently only capable of a quantum computer of about 2,000 qubits[7], so there's time to figure out the problem.

Luckily, a new method is now being developed that will shield us from the eventual failure of RSA-based encryption. That involves Quantum1Net and the new Quantum Encryption Key.

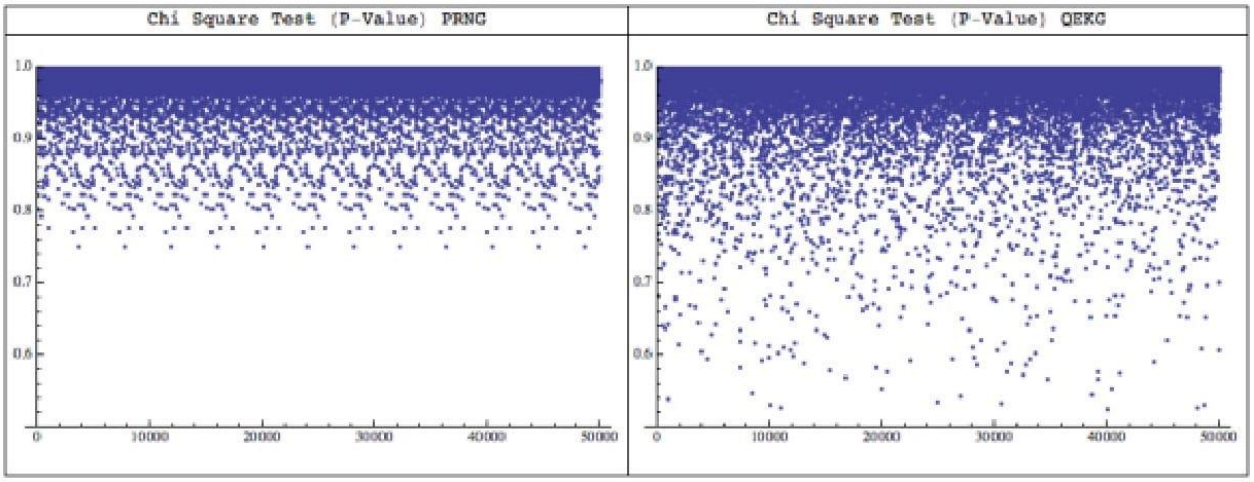
[5] Rich, S. and B. Gellman. (2014-01-02). "NSA seeks to build quantum computer that could crack most types of encryption." Washington Post (web). Retrieved 2017-11-05.
[6] Simonite, T. (2016-02-03). "NSA Says It 'Must Act Now' Against the Quantum Computing Threat." MIT Technology Review. Retrieved 2017-11-05.
[7] Gibney, E. (2017-01-24). "D-Wave upgrade: How scientists are using the world's most controversial quantum computer." Nature (web). Retreived 2017-11-05.

The Quantum Encryption Key

The Quantum Encryption Key Generator is the heart of Quantum1Net's encryption strategy. To review, generating a random multi-digit number from which mathematical properties are derived in the case of RSA its prime factorization. There is one main issue however, the random generators used are only pseudo-random (commonly referred to as PRNGs), so an RSA key is pseudo-random. Tests have shown that PRNGs exhibit a repetitive pattern of behavior when selecting so called "random numbers." This pattern means that with enough results, a prediction can be made for future number selections. Thus, PRNGs aren't truly random.

Quantum1Net instead relies on a Quantum Encryption Key Generator (QEKG). Because of the properties of quantum computers itself, tests have shown that even in large samples, the numbers selected follow no pattern thus no predictive algorithm can be derived.

The graph below shows our results for a test of both a PRNG and QEKG on a sample 20,000 bit in length 50,000 times. Using a PRNG, after 50,000 tests it is apparent visually that data is predictive even after the first 10,000 or so attempts. With QEKG however that is not the case. Look at the bottom portion of the graph where the dots are more disperse. Unlike the PRNG graph, in the QEKG graph there is no apparent pattern to their locations.



Entropy distribution of 50,000 samples 20,000 bits in length generated by PRNG (left) and QEKG lab prototype (right).

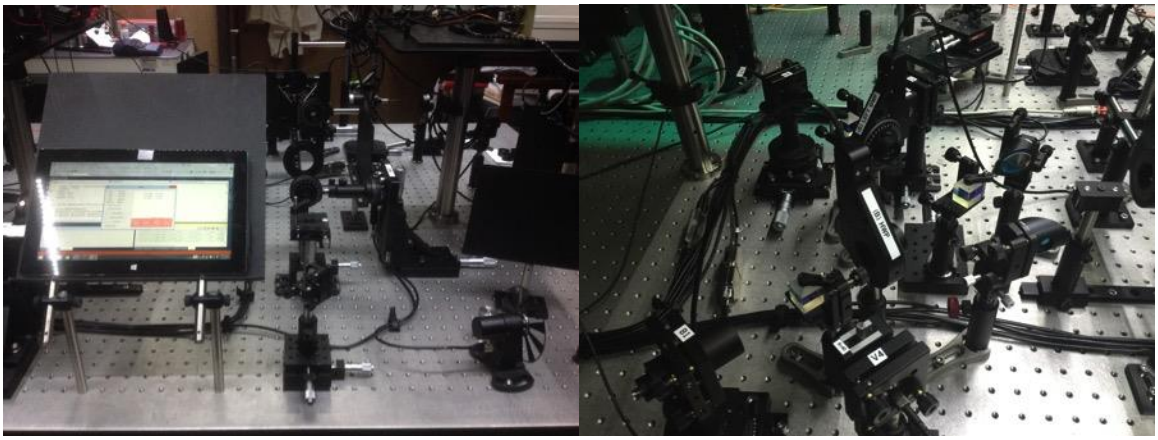
This is possible with a one-qubit quantum optical device; meaning exceptionally large (and expensive) quantum computers are unnecessary to produce quantum encryption keys. We utilize a process known as quantum entanglement in such a way that it produces multiple sets of correlated random numbers so that combining two or more sets can only derive the entire encryption key. While a broader discussion of this process is beyond the scope of this paper, this behavior makes random numbers truly random.

The pattern-like behaviors of PRNGs make *quantum computing* attacks against not only RSA but also other public-key algorithms like Diffie-Hellman and elliptic curve cryptography utilizing Shor's or algorithm or its derivatives effective. Since a QEKG key is produced in a random non-algorithmic manner, systems using these generators will be impervious to such attacks.

Therefore, the race is on to ensure that a practical real-world system is in place using the QEKG, which is precisely what Quantum1Net is currently working to accomplish.

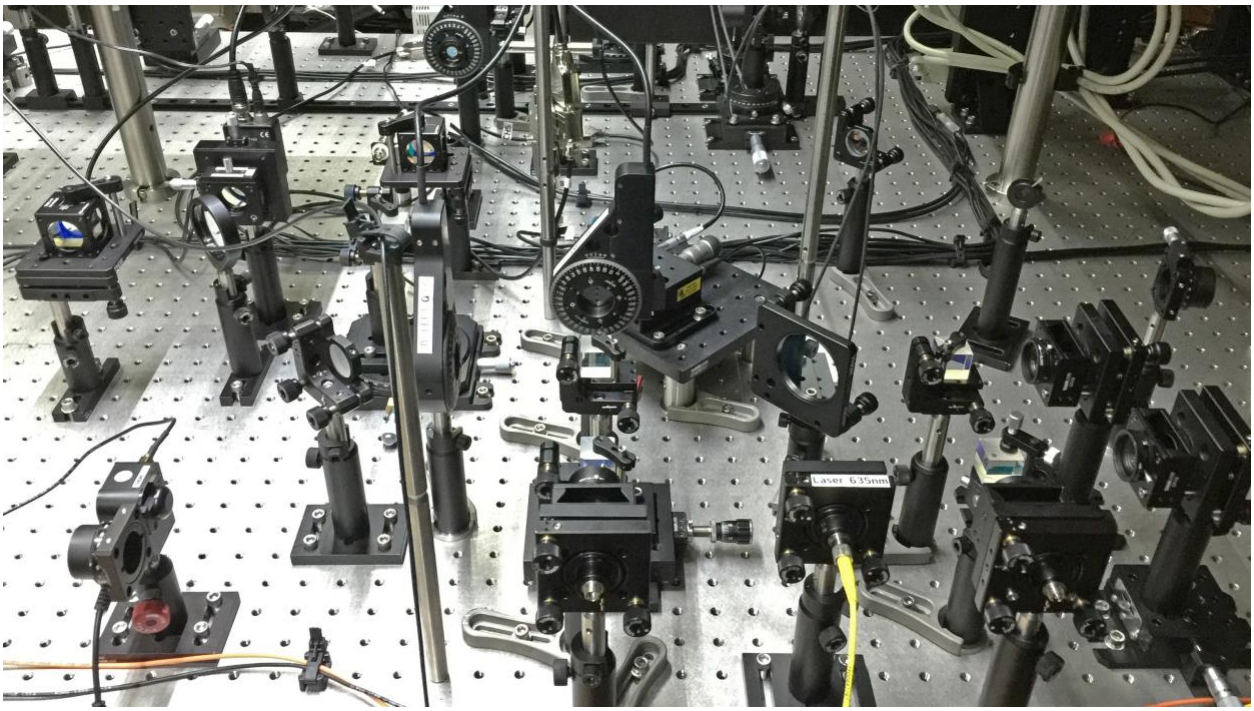
Quantum1Net Prototype

The laboratory prototype of Quantum1Net's Quantum Random Number Generator, which has been in development since 2014, is based on a one-qbit optical device, that uses four photon detectors and time-to-digital (TDC) converter to generate sets of perfect random numbers with timestamps. The quantum device consists of an entangled photons source, and linear optical elements, which sets the quantum system to the desired state. Two configurations have been developed to generate sets of 4 and 6 elements respectively. The output of the TDC is the temporary queue, from which sets of unique random numbers or encryption keys can be requested, creating a real time, on demand encryption and decryption system.



The transaction data (text or binary) is encrypted using combination of encryption keys and multidimensional Cellular Automata, making quantum-computing algorithms, such as Shor's factorization algorithm for which RSA is vulnerable, ineffective.

Quantum nature of the Quantum1Net's key generator ensures that the keys are produced can be processed with very little computing overhead.


Laser 635nm