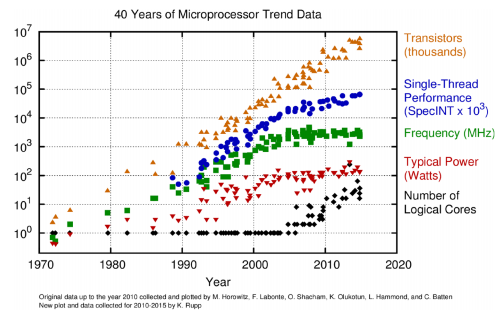
Quantum Computing’s Biggest Threat: An Overview of how Quantum Computing is Changing Cybersecurity

**Intro**

Quantum computing is a newer form of computing that has sparked significant interest. As opposed to transistors, which represent ones and zeros, quantum computers have qubits, which represent probabilities [5]. This allows for quantum computing to be optimized for iterative and repeatable tasks with slight variation [14]. They have been to simulate, model, and develop new technologies in most every scientific field as well as the social sciences [11]. Many researchers also ascribe quantum computing to an extension of Moore’s law, which models how computers roughly double in speed every 18 months [16].



Representation of Moore’s Law, where transistor density has caused an increase in computer speed. Researchers say that quantum computers may be the next step with this [5].

Because quantum computers solve problems faster, they can also break encryption methods significantly faster [1]. In traditional cryptography, methods are usually encrypted and decrypted using a secret key that only the client or server know [12]. This is what most modern encryption standards rely on, such as RSA and AES [12]. In these current encryption standards, however, the speed at which quantum computers can decrypt information without knowing the secret key is astronomical [10]. Because most web traffic dealing with private information relies on these standards, these quantum computers, people’s private data is in jeopardy [8]. Quantum cryptographers are therefore working on a new standard of encryption.

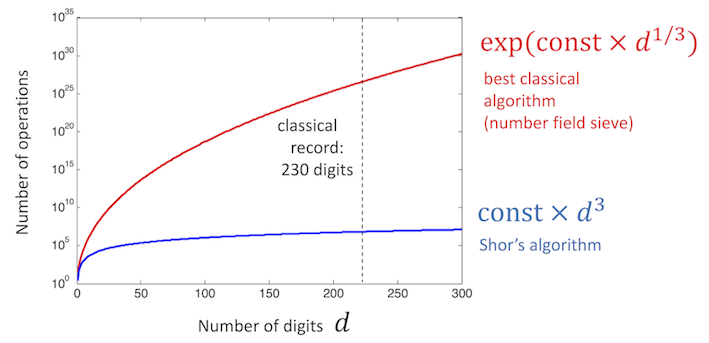
What are quantum computers? What is cybersecurity?

How are quantum computers starting to change cybersecurity?

**Quantum Decryption**

The security of current encryption standards relies on certain mathematical properties: most notably, the hardness of factoring integers [3]. These properties make encrypted data practically infeasible to solve in a timely manner. However, when these properties are undermined, the problems can be solved easily, and they are no longer secure.

In 1995, AT&T researcher Peter Shor introduced a new algorithm (now known as Shor’s algorithm) that can factor integers quickly [17]. Shor predicted his algorithm would be most effective on a quantum computer [17]. Today, researchers prove this repeatedly in quantum implementation of Shor’s algorithm [2]. Because of Shor’s algorithm, today, current encryption algorithms like RSA and AES are vulnerable to quantum computers. Quantum computers achieve sub polynomial time complexity when solving to decrypt RSA [3]. The change in speed is exponential because it requires significantly fewer operations because of quantum technology and its new way of solving problems..



On quantum computers, clearly, Shor’s algorithm is faster because it requires much fewer operations.

Despite there being multiple versions and iterations of Shor’s algorithm, the core principles behind it remain [14]. Even though AES and RSA are insecure when attacked by quantum computers, they still remain secure in most other cases [3]. AES and RSA remain the industry standard of encryption for this reason.

**Quantum Encryption**

Quantum computers have also introduced new ways of encryption. In part inspired by Shor’s algorithm threatening the longevity of the RSA and AES encryption standard, new research is occurring in using quantum computers to encrypt data [3].

The most common type of quantum encryption is based on a lattice approach. Lattice problems use linear combinations of many vectors for encryptions, which means they are hard to reverse engineer. Unlike RSA, they do not rely on the hardness of factoring, and instead rely on what has been mathematically proven to be a significantly harder problem that cannot be solved by a quantum computer in reasonable time (given infinite time, any computer could solve any problem) [18]. Lattice approaches and other similar quantum key exchange algorithms have been mathematically proven against most all major types of cybercrime [1]. A notable implementation of this lattice approach combined a lattice based keyword encryption system that followed a traditional key exchange like the one used in the RSA algorithm [7].

Another competing approach within quantum cryptography is what is being called “Lizard” [13]. The Lizard approach uses iteration and randomized linear combinations with different offsets. In using these randomly added numbers, it is somewhat similar to RSA. It still remains secure, as it follows the same assumptions that make the lattice approach secure. On a single core implementation, it was able to symmetrically encrypt and decrypt in less than a millisecond [13].

Both the lattice approach and the lizard approach seem to be secure. It seems that though the lattice approach is stronger, the lizard approach is faster [13]. The two methods may both have a place in the future for different purposes. They can also be combined with other security methods to make them even more secure, such as two-factor authentication [8].

**Threats to Consumer**

This new encryption scheme for quantum computers has been mathematically proven [1]. Quantum computers on the other hand remain incredibly expensive [9], despite some attempts to build quantum computers with cheaper more industry standard materials [19]. Regardless of the short term, it is predicted that the increased presence in shifts such as this will result in more widespread quantum computers over the long term [19]. Consequently, the effects of the current situation in security are likely to amplify in the future [5].

In the short term, realists are evaluating what security they can have at what cost [9]. Interconnected networks of servers on quantum computers have shown to be a comparatively economical route to establishing quantum-proof security in modern times [9]. This approach involves having a centrally located quantum computer to perform encryption and decryption on incoming and outgoing data [9].

Still, despite the vulnerabilities that exist within RSA and AES, they remain the current encryption standard [12]. Researchers have called it practically infeasible for everyday people to buy quantum computers [9]. This may be the reason for why these standards remain.

**Conclusion**

Quantum computing is certainly changing the game of cybersecurity in the modern era. Still, AES and RSA remain the dominant encryption standard. This is likely due to the fact that quantum computers remain difficult to get from the public [9].

However, new encryption standards are being developed that use quantum computers to encrypt data. These new encryption methods no longer rely on the hardness of factoring, as AES and RSA do. This means that they are impervious to Shor’s algorithm. Quantum proof cryptography all in all seems to demand quantum cryptography itself.

**References**

[1] E. Biham, M. Boyer, P.O. Boykin, T. Mor, V. Roychowdhury, “A Proof of the Security of Quantum Key Distribution,” Journal of Cryptology, vol 19, no. 4, pp. 381-439, Oct. 2006.

[2] A. Politi, J. C. F. Matthews, J. L. O’Brien. “Shor’s Quantum Factoring Algorithm on a Photonic Chip,” Science, vol 325, no. 5945, pp. 1221, Sept. 2009.

[3] E. Blakely, “Factorizing RSA Keys, An Improved Analogue Solution,” New Generation Computing, vol. 27, no. 2, pp. 159-176, Apr. 2008.

[4] Y. Yang, S. Yang, F. Wang, “Post-Quantum Secure Public Key Broadcast Encryption with Keyword Search,” Journal of Information Science & Engineering, vol. 33, no. 2, pp. 485-97, Mar. 2017.

[5] M. Moller, C. Vuilk, “On the Impact of Quantum Computing Technology on Future Developments in High-Performance Scientific Computing,” Ethics & Information Technology, vol. 19, no. 4, pp. 253–69. Aug. 2017.

[6] D. Huang, W. Zhong, J. Zhong, D. Jiang, H. Wu, “Optimization and Implementation of Efficient and Universal Quantum Key Distribution,” Journal of Electrical & Computer Engineering, vol. 2020, pp. 1-9, Jan. 2020.

[7] Y. Yang, M. Ma, “Semantic Searchable Encryption Scheme Based on Lattice in Quantum-Era”, Journal of Information Science & Engineering, vol. 32, no. 2, pp. 425-438, Mar. 2016.

[8] D. Zhu, X. Li, J Wu, L. Song, “A Quantum Key-Based Mobile Security Payment Scheme.” International Journal of Performability Engineering, vol. 15, no. 8, pp. 2165–72, 2019.

[9] R. Wiegele, P. Schartner. “Building a Quantum Network: How to Optimize Security and Expenses.” Journal of Network & Systems Management, vol 18, no. 3, pp. 283–99, 2010

[10] J. Burke, A. Lewis, M. Overton, “The Speed of Shor's R-algorithm, IMA Journal of Numerical Analysis, vol. 28, no. 4, pp. 711-720, Oct. 2008.

[11] M. Matthias, C. Vuik, “On the Impact of Quantum Computing Technology on Future Developments in High-Performance Scientific Computing,” Ethics & Information Technology, vol 19, no. 4, pp. 253–69, Aug. 2017

[12] S. Herbert, E. Junaeti, T. Hayatno, “Analysis of Attacks on Mail Disposition Systems Secured by Digital Signatures Equipped with AES and RSA Algorithms,” Pertanika Journal of Science & Technology, vol. 26, no. 3, Jul. 2018.

[13] J. Cheon, D. Kim, J. Lee, Y. Song, “Cut Off the Tail! A Practical Post-quantum Public-Key Encryption from LWE and LWR,” 11th International Conference, SCN, 2018.

[14] L. Wang, J. Li, L. Gu, J. Yan Z. Qu, “An Efficient Construction of Quantum Attack Resistant Proxy Re-Encryption Based on (Semi) group Factorization Problems,” Fundamenta Informaticae, vol. 157, no. 1–2, pp. 47–62, 2018.

[15] S. Mohamed, R. Wille, R. Karri,“Locking the Design of Building Blocks for Quantum Circuits.” ACM Transactions on Embedded Computing Systems, vol. 18 no. 5 pp. 1–15, 2019.

[16] P, Ferdinand, “The End of Moore’s Law: Opportunities for Natural Computing?” New Generation Computing vol. 35, no. 3, pp. 253–69, 2017.

[17] P. Shor,. “Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer.” SIAM Review, vol. 41, no.. 2, pp. 303–32, Jun. 1999.

[18] O. Regev, “On lattices, learning with errors, random linear codes, and cryptography,” Proceedings of Symposium on Theory of Computing, pp. 84-93, 2005.

[19] A. Ousalem, Y. Bourezig, Z. Nabi, B, Bouabdallah, “Ab Initio Study of the Structural, Electronic, and Magnetic Properties of Co2FeGa and Co2FeSi and Their Future Contribution to the Building of Quantum Devices,” Turkish Journal of Electrical Engineering & Computer Sciences, vol. 26, no. 3, pp. 1249 - 1260, June 2019.