FSOKX PODCAST

Focused Intelligence in Financial Services

A Division of TurtleBay Advisory Services

Quantum Computing's Impact on General Cryptography Implementations

By Louis Stoll

January 2022

Abstract: The Race for Quantum Supremacy in the 2nd decade of the 21st Century will shape future markets and societal trends much as the 'Arms Race' and the 'Race to the Moon' created watershed events that shaped subsequent history. While today's current quantum computing abilities continue to become adapted for optimization purposes, organizations should be prepared for bad actors looking to defeat cryptography and exploit industries. As the world continues to make breakthroughs towards quantum supremacy, these discoveries undermine security constructs foundational to e-commerce and social life as currently known in the world. This paper will analyze the high-level impact of Quantum Computing on general commerce and social life. By setting forth a list of risks and consequences resulting from quantum computing breakthroughs, this paper is intended as a call-to-action from modern information technology providers, commercial enterprise implementers and public consumers in the public communication marketplace to prepare against these bad actors.

Keywords: Cryptography, quantum supremacy, e-commerce, quantum computing

Introduction:

Internet commerce, more commonly referred to as 'e-commerce' is conducted across publicly shared communications services which use well-established and well-thought-out security mechanisms. These security mechanisms are based on the general concept of encryption in which plain-text information is manipulated to be indecipherable to un-authorized individuals. Built on centuries of experience with cryptographic techniques and methods, today's systems have demonstrated remarkable integrity in protecting secured information. While the methods necessary to break the cypher takes 100s or thousands of years by conventional computing methods, quantum supremacy results in near real time deciphering for many 'hardened' encryption techniques. For more complex encryption techniques, this could mean hours or days to decipher. Therefore, discontinuity in current practices has been created by quantum computing techniques and technology's ability to eliminate the time barrier, which provided protection from deciphering.

As a result, what was previously secure information transmission is now rendered to be the same as open text transmission. Albeit this is not an issue of concern for the present, organizations need to start preparing for this breakthrough to protect the future of secured information transmission. To expand further, appendix one identifies a list of major services and sources known to be at risk as a result of this future breakthrough.

In the author's view, three subjects limit the risk of e-commerce and public communications as it is currently implemented from compromise and unintentional disclosure.

1. Limited Availability of actual quantum computing resources.
2. Algorithm implementation of operational decryption with an integrated quantum computing platform.
3. Identification of Targets of Opportunities for Exploitation.

Each of these are dealt with in order in the following paragraphs.

Limitations of Access to Quantum Capabilities

In the first half of 2021, there were only two or three quantum computing solutions demonstrating useful functionality. This technology was still substantially unproven with major theoretical physics challenges to the viability of quantum computing solutions. In the final six months of 2021 these questions were resolved to the point that it is no longer a theoretical possibility. Instead, it's a question of scalability and time till they become commercially available.

Created in a development environment, that were previously limited as architecture matured are now available in open source allowing for both friend and foe to develop algorithms that can be used for malicious purposes.

For example, China has publicly touted its work in quantum computing claiming to have achieved quantum supremacy months ago.[i] The scope of their work claims to be entirely benign and focused purely on academic goals, but little is known of their programs and scope of their efforts. Additionally, past Chinese efforts in other areas have been positioned as benign until strategic advantage could be achieved at which point, they exercised their full strength and capability. With, China's history of accomplished electronic espionage and sabotage (as do most all countries) the threat imposed by a cryptographic supremacy based in China would have a chilling effect on general information privacy and a similar effect on global economies. [ii]

Therefore, Chinese quantum computational capabilities and directions, need to be actively monitored and asses to allow appropriate private and governmental countermeasures to occur. The Department of Homeland Security, is actively working on Cryptographic Solutions and strategies, but private industries have not

yet embarked on creating a Post Quantum Encryption plan that is tied to threat sources, such as China. Additionally, changes to China's, and other potential threats quantum computing focus needs to be monitored for countermeasures to be implemented across the entirety of existing communications infrastructure.

Future research should focus on the public identification and classification of quantum algorithm centers of expertise. This includes monitoring surveillance activity for proper scoping of technical response activities, supporting requests for funding and establishing project milestones for counter measures.

Changes in the focus and scope of western public communications infrastructure need to be studied and coordinated to allow for accurate updates to risk profiles while maintaining operational capability.

Algorithm Implementation

Following the availability of quantum computing resources, another factor of consideration in decreasing risk is algorithm implementation. With changing risk levels, these milestones need to be defined and standardized for response planning to be performed. Historically, similar activities were tried after the 9/11 attacks with the implementation of threat condition level. These activities have proved to be confusing and problematic to understand by private industries and the general public. Thus, the coordination and escalating/de-escalating of risk levels needs to be well defined and planned for all parties to be able to continue operating based on the risk level.

One theory includes the highest risk level as a complete compromise and lack of trust in existing security algorithms and associated commercial uses. A current state risk level would be the presumption of all information still being protected, while intermediate levels is the intention that each level assumes less trustworthiness of conventional pre-quantum implementations.

Changes to risk level would call for more drastic risk avoidance activities to maintain operational capability. This results from a greater need to retire compromised systems and solutions as necessary to manage risk. Since private industry tends to respond slowly to unanticipated threats and conditions, aggressive planning and coordination needs to occur to provide the necessary insight and justification to perform technology change.

<u>Identification of Vulnerable Targets for Exploitation</u>

The final factor of consideration is identifying "Targets of Opportunities" for exploitation. Assuming a reasonable risk profile can be established this renders existing communication techniques ineffective. This requires a prioritized matrix of risk response activities to be developed that evaluates asset value against probability of compromise. The matrix should include an actionable list of assets with specific time certain milestones either professionals or computers must take to protect them from being comprised. Additionally, the analysis needs to consider that real time compromise is not necessary for financial and reputation damage to occur.

For instance, streams of transmitted data can be captured and analyzed through post processing solutions to decrypt and harvest high value data days, weeks or months after the incident. Given intense social data mining over the last decade, this is a cause of concern as citizen social security identities have been revealed, and detailed knowledge of military and industrial databases of employee qualifications and associations have been discovered.[iii], [iv]

Decrypting data streams after the fact allows for compromises of trade secret information, personal, and confidential information including identity disclosure and all sources and methods transmitted through pre-quantum cryptographic techniques.

To be clear, most countermeasures probably will not require quantum computing capability, but exposure of encrypted information probably will occur regardless of countermeasures. This comes after communicated information has been captured for subsequent analysis. Therefore, this risk is immediate and current action needs to be taken to assess and safeguard communications and data, where possible. Due to the shift of 5G technology, this is particularly troublesome as this technology has already been cryptographically compromised to capture streams of encrypted data. 5G technology was thought to not be of major concern until the reality of quantum computing caused the collapse of current cryptographic infrastructure as described. [v]

The financial threat associated with compromising captured information is immediate and scope reduction methods are needed to quickly minimize the impact of information being compromised. These steps include:

1. Critical review of Analysis of schemas for information that is cloud based versus information contained in private networks.
2. Identification and implementation of alternative methods and techniques for disclosure (physical and telephonic dissemination versus electronic disclosure).
3. Surveillance of public and dark web sources for content, sources and similar types of data.
4. Collaboration with law enforcement on disaster response and business continuity plans.
5. Entities require surveillance of all authorized user access profiles to identify inappropriate and suspicious data usage/disclosure and rapidly identify areas of compromise when internal disclosure has occurred.

Summary

All are at risk- Every individual and company that performs confidential or secure communications using the "Internet" including all B2B, B2C and governmental G2B and G2C communications as well as C2C communications are at risk.

Existing Risk Drivers Not Useful as Driving Force – Traditional driving forces of managing liability and prioritizing business challenges won't respond fast enough. Typically, companies wait till events start to appear and trend before taking large scale action. Therefore, liability claims will be numerous for unauthorized disclosure of information and service will be denied out of necessity as the first landmark decisions for the general public good. As a result, loss of confidence and inability to operate will create existential moments of crisis and opportunity with the strong entities surviving and weaker organizations being acquired or absorbed. This becomes troublesome if international players can plan for these events and take advantage of compromised competitors during a flurry of cyber-attacks resulting from compromised encryption technologies.

The legal system could be flooded as well with damage claims ranging from loss of life to the failure of public infrastructure to large scale financial suits for denial-of-service attacks. This could extend to common significant fraud and corruption occurring from group arguments over the damage as they try to respond and survive.

Business will need to adapt as the laggards are penalized by governments and the marketplace for their lack of effort and counter measures as the look for punishment and holding someone responsible grows.

Appendix One

Summary of Sources and Systems at Risk

- Loss of availability, integrity, authentication, confidentiality, and non-repudiation due to malicious actors for all public communications.
- Impact to all public communications.
- Impact to stored and archived data that are not secured through a physical prevention of access.
    - All systems serving data would be vulnerable regardless of operating system to discretionary security system compromise (equivalent to all users having root access).
    - All repositories whether online or offline where encryption is assumed to keep data secure from disclosure and compromise.
- Impact to all hardware and software methods and products that rely on DES derived encryption methods including any number of bits of encryption (DES was 128bit but any length of encryption using this technology would be vulnerable).

Commonly Used Transactions and Services at Risk

- All Online and E-Commerce (Amazon, Alibaba, PayPal, etc.).
- All Banks, Stock Brokerage, Health and Non-Health Insurance Services.
- eHealth Services including all patient portal, online pharmacy, online lab reporting to providers and patients.
- All social media C2C services where confidentiality is assumed.

- All private VOIP and mobile communication services.

Appendix Two

Quantum Computing Key Terms

This is a complied list of key terms one needs to know when understanding quantum computing. All definitions are from the Merriam-Webster Dictionary and the National Institute of Standards Technology.

Cipher- "A message in a code" (Merriam-Webster).

Cryptography- "The enciphering and deciphering of messages in secret code or cipher. Computerized encoding and decoding of information" (Merriam-Webster).

*Cryptographic Algorithm- "*Well-defined procedure or sequence of rules or steps, or a series of mathematical equations used to describe cryptographic processes such as encryption/decryption, key generation, authentication, signatures, etc." (NIST).

Encryption- "The act or process of encrypting something: a conversion of something (such as data) into a code or cypher" (Merriam-Webster).

Quantum Computer- "A computer that takes advantage of the quantum properties of qubits to perform certain types of calculation extremely quickly compared to conventional computers" (Merriam-Webster).

*DES (Data Encryption Standards)- "*The symmetric encryption algorithm defined by the Data Encryption Standard" (NIST).

References

Barker, W., Polk, W., & Souppaya, M. (2021). Getting ready for post-quantum cryptography: Exploring challenges associated with adopting and using post-quantum cryptographic algorithms. https://doi.org/10.6028/nist.cswp.04282021

Chen, L. (2017). Cryptography standards in Quantum Time: New wine in an old wineskin? *IEEE Security & Privacy*, *15*(4), 51–57. https://doi.org/10.1109/msp.2017.3151339

Chen, L., Jordan, S., Liu, Y.-K., Moody, D., Peralta, R., Perlner, R., & Smith-Tone, D. (2016). Report on post-quantum cryptography. *National Institute of Standards and Technology* , (8105). https://doi.org/10.6028/nist.ir.8105

Chief Information Officer, & Hysen, E., Preparing for Post-Quantum Cryptography Memo (2021). Retrieved from https://www.dhs.gov/sites/default/files/publications/usm_quantum_memo_0.pdf.

Kaur, D. (2020, December 21). *Is China leading the quantum computing race?* Tech Wire Asia. Retrieved from https://techwireasia.com/2020/12/is-china-leading-the-quantum-computing-race/#:~:text=China%20has%20invested%20heavily%20in%20quantum%20computing%2C%20with,a%20calculation%20faster%20than%20a%20conventional%20computer%20could.

Lecher, C., & Brandom, R. (2019, March 17). *Is Huawei a security threat? Seven experts weigh in.* . The Verge. Retrieved January 24, 2022, from https://www.theverge.com/2019/3/17/18264283/huawei-security-threat-experts-china-spying-5g

Lord , N. (2020, October 6). *Top 10 biggest government data breaches of all time in the U.S.* Digital Guardian. Retrieved January 24, 2022, from https://digitalguardian.com/blog/top-10-biggest-us-government-data-breaches-all-time

Maryville University . (2021, January 26). *Top cyber breaches of the last decade*. Maryville Online. Retrieved from https://online.maryville.edu/blog/the-top-cyber-security-breaches-of-the-last-decade/

Moody, D., Alagic, G., Apon, D. C., Cooper, D. A., Dang, Q. H., Kelsey, J. M., Liu, Y.-K., Miller, C. A., Peralta, R. C., Perlner, R. A., Robinson, A. Y., Smith-Tone, D. C., & Alperin-Sheriff, J. (2020). Status report on the second round of the NIST post-quantum cryptography standardization process. *National Institute of Standards and Technology*, (8309). https://doi.org/10.6028/nist.ir.8309

Skjong, A. (2021, December 3). *Honeywell superpositions itself in the quantum computing industry with new company quantinuum*. tech.mn. Retrieved from https://tech.mn/news/2021/12/03/honeywell-superpositions-itself-in-the-quantum-computing-industry-with-new-company-quantinuum

U.S Department of Homeland Security, Cybersecurity & Infrastructure Security Agency, National Institute of Standards & Technology . (2021, October). *Post-Quantum Cryptography FAQ - dhs.gov*. DHS. gov. Retrieved from https://www.dhs.gov/sites/default/files/publications/post_quantum_cryptography_faq_3_seals_october_2021_508.pdf

---

[i] **Is China Leading the Quantum Computing Race,** December 21,2021, Dashveenjit Kaur, https://techwireasia.com/2020/12/is-china-leading-the-quantum-computing-race/#:~:text=China%20has%20invested%20heavily%20in%20quantum%20computing%2C%20with,a%20calculation%20faster%20than%20a%20conventional%20computer%20could.

[ii] **IS HUAWEI A SECURITY THREAT? SEVEN EXPERTS WEIGH IN**, Mar 17, 2019, Colin Lecher and Russell Brandom https://www.theverge.com/2019/3/17/18264283/huawei-security-threat-experts-china-spying-5g

[iii] **The Top Cybersecurity Breaches of the Last Decade, 2022 Maryville University,** https://online.maryville.edu/blog/the-top-cyber-security-breaches-of-the-last-decade/

[iv] **Top-10-biggest-us-government-data-breaches-all-time, 2020 Digital Guardian,** https://digitalguardian.com/blog/top-10-biggest-us-government-data-breaches-all-time

[v] **IS HUAWEI A SECURITY THREAT? SEVEN EXPERTS WEIGH IN**, Mar 17, 2019, Colin Lecher and Russell Brandom https://www.theverge.com/2019/3/17/18264283/huawei-security-threat-experts-china-spying-5g