Navigating the Quantum Leap: A Comprehensive Review of Transitioning to Post-Quantum Cryptography Standards

Joseph Winkie

CyberSecurity Service Provider Internship Program, ICS 296 & 396, Fall 2023

Advisors: Dr. Curtis Arnold, Chief Scientist – Cyber, & Dr. Robert Adamove, Sr. Associate, (Core4ce)

The problem is…

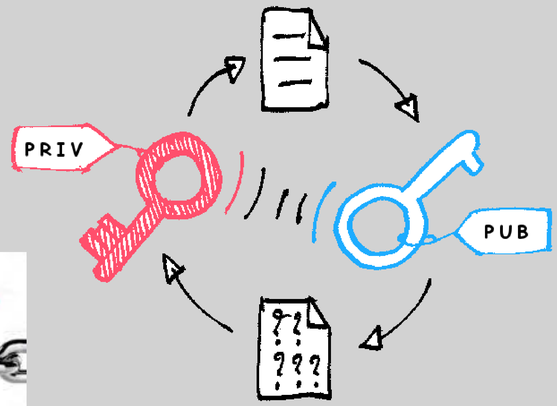
- There is an undeniable probability that quantum computing will erode the security of public-key cryptography such as RSA should it reach a theoretically ideal state.

The purpose is to…

- Examine existing security systems/security threats related to cryptography that exist both prior and because of quantum computation capabilities
- Evaluate ways to ensure that existing security systems evolve to match this novel threat on the horizon with minimal turmoil.
- Develop a holistic perspective of cryptography where existing research has primarily focused on encryption algorithms themselves.

The approach is to…

- Focus on the greater system these cryptographies play a role in.
  - This meta-study is not intended to develop a novel insight into the cryptographic systems themselves.
- Analyze potential implications such as
  - Additional overhead (Ott et al., 2019)
  - Long migration time (Bene & Kiss, 2023).
  - Impacts to transmission technologies



Discussion & Conclusion:

- There is ambiguous evidence of existing quantum computing technology cracking RSA encryption from Joshi et al. (2022).
- Bene & Kiss (2023) recommend the use of hybrid cryptography to continue protecting encrypted content with current standards while the new cryptography is maturing
- Primary side effects of adding quantum resistant cryptography to existing security systems is the migration time and additional overhead (Bene & Kiss, 2023 and Ott et al., 2019)
- Utilizing hardware acceleration can help soften the impact of the additional overhead
- QRC requires larger key sizes and more computation than surrounding protocols may tolerate until they are updated (Ott et al., 2019)
- Early migration to these protocols will encourage natural development of hardware and software optimizations

The path forward is to…

- Research the efficacy of various quantum resistant cryptography standards.
- Explore experimental hybrid cryptography implementations.
- Learn specifics of hardware and software optimizations required.
- Begin general transition efforts as soon as possible.

References:

Bene, F., & Kiss, A. (2023). Public key infrastructure in the post-quantum era. 2023 IEEE 17th International Symposium on Applied Computational Intelligence and Informatics (SACI). https://doi.org/10.1109/saci58269.2023.10158562

Joshi, A., Mehta, A., Shetty, H., Kurnbhar, R., & Kosamkar, V. (2022, May). Breaking RSA Encryption Using Quantum Computer. International Journal of Research and Analytical Reviews (IJRAR), 9(2), 885-887. https://www.researchgate.net/profile/Aayush-Joshi-2/publication/362696967_Breaking_RSA_Encryption_Using_Quantum_Computer/links/62fa45eeeb7b135a0e39b612/Breaking-RSA-Encryption-Using-Quantum-Computer.pdf

Ott, D., & Peikert, C. (2019). Identifying research challenges in post quantum cryptography migration and cryptographic agility. arXiv preprint arXiv:1909.07353.