Post-Quantum Security: CoreVUE Breaks Through PKI
A Look at an Emerging Technology in Cybersecurity

Nicholas Edwards
TunnelVUE

Janel Bell Haynes
Trenholm State Community College

Sara Bliss Kiser
Alabama State University

Existing methods of encryption and key exchange are seeing their effectiveness reduced as quantum algorithms are released. This research and resulting proof of concept has created technology simplifying the protection of data in transit using a revolutionary post-quantum encryption key management system that eliminates the need for PKI.

Keywords: PKI, encryption, key exchange, Shor's algorithm, Grover's algorithm, post-quantum

INTRODUCTION

As technology continues to advance to the quantum age, existing methods of encryption and key exchange are continuously seeing their effectiveness reduced as new quantum algorithms are released. Two of the most effective algorithms are Shor's algorithm (IBM Q, 2017b) and Grover's algorithm (IBM Q, 2017a). This research addresses these two emerging threats to cryptographic security.

The research and resulting proof of concept prototype has created technology that simplifies the protection of data in transit using a revolutionary post-quantum encryption key management system that eliminates the need for PKI or other asymmetric key management systems used in today's solutions. The research uses universal encryption of all data in transit with no hands-on management including configuration of routers, switches, etc. (TunnelVue, 2019).

HOW TO ANSWER THE PROBLEM

With the emergence of quantum computers in today's world, the risk to asymmetric encryption rapidly increases, due to its susceptibility to Shor's algorithm which uses integer factorization to derive the key. The current industry standard for breaking encryption is to look for underlying patterns of characters which compose the encrypted message. The multifactor postquantum method created from this research, CoreVUE, wraps each packet in an encrypted session (including the very first packet) with a separatelyestablished, unique key for each session and a unique key for every packet within each session. Thus, making it nearly impossible to be broken by quantum computers. CoreVUE's key manager has no limitation on the size of the code or the size of the key. The only limitations are set by users. In Table 1, a comparison of current standards for security versus those produced by this new technology is presented

TABLE 1
COMPARISON OF CLASSICAL AND QUANTUM SECURITY LEVELS FOR THE MOST USED CRYPTOGRAPHIC SCHEMES

		Effective Key Strength/Security Level (in bits)	
Crypto Scheme	**Key Size**	**Classical Computing**	**Quantum Computing**
RSA-1024	1024	80	0
RSA-2048	2048	112	0
ECC-256	256	128	0
ECC-384	384	256	0
AES-128	**128**	**128**	**64**
AES-256	**256**	**256**	**128**

Mavroeidis, Vishi, Zych, & Josang (2018, p. 4).

Shor's algorithm is effective on asymmetric encryption due to its ability to perform integer factorization to derive primes. This allows Shor's algorithm to solve asymmetric encryptions in polynomial time. Thus, asymmetric keys have an effective key space of nearly zero bits when solved with quantum computing. The prototype produced from this research, CoreVUE, does not use any form of asymmetric encryption or its derivative Public Key Infrastructure (PKI) for key management and exchange.

Grover's algorithm is also effective on symmetric encryption such as AES. It can reduce the key space to the square root of its effective space through the use of an unstructured search through amplitude amplification using differing states to search for a result that is known. This drastically reduces the effective key strength of existing symmetric encryption methodologies. The research has demonstrated that if Grover's algorithm were applicable to the CoreVUE key management methodology, it would suffer only 50% of the standard reduction generally associated with Grover's algorithm due to the double-wrapped dynamic encryption used. This changes the reduction of a 256-bit key from 128 to 192 allowing existing AES encryption to maintain an additional 64 bits of entropy in the key. Table 2 depicts this comparison

TABLE 2
256-BIT VERSUS 128-BIT KEY ENCRYPTION

Methodology	Mathematical Result
Traditional AED deployment with a 256 bit Key	$\sqrt{2^{256}} = 128$
Core VUE AES deployed with 2 (128) bit Keys	$\sqrt{2^{128}} * 2^{128} = 192$

Due to CoreVUE's dynamic multi-factor encryption key management, it mathematically appears as an NP-Complete problem matching the description of a Boolean Satisfiability Problem.

CoreVUE is a multi-factor post-quantum key management mechanism that strengthens existing symmetric encryption systems and industry standard key generators on existing hardware through the post-quantum age. Until P versus NP is solved CoreVUE faces no significant mathematical vulnerabilities including all current publicly available algorithms (Cook, 2003).

REFERENCES

Cook, S. (2003, January). The importance of the P versus NP question. *Journal of the ACM*, *50*(1), 27-29. Retrieved from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.515.2584&rep=rep1&type=pdf

IBM Q. (2017a). *User Guide-Quantum Algorithms-Grover's algorithm*. Retrieved from https://quantumexperience.ng.bluemix.net/qx/tutorial?sectionId=full-user-guide&page=004-Quantum_Algorithms~2F070-Grover%27s_Algorithm

IBM Q. (2017b). *User Guide-Quantum Algorithms-Shor's algorithm*. Retrieved from https://quantumexperience.ng.bluemix.net/qx/tutorial?sectionId=full-user-guide&page=004-Quantum_Algorithms~2F110-Shor%27s_algorithm

Mavroeidis, V., Vishi, K., Zych, D., & Josang, A. (2018, March). The impact of Quantum computing on present cryptography. *International Journal of Advanced Computer Science and Application*, *9*(3), 1-10.

TunnelVUE. (2019). *A Mutlifactor Post-Quantum Security Breakthrough*. Retrieved from https://img1.wsimg.com/blobby/go/f66cc185-9213-4a09-9ae7-6915a8736d69/downloads/quantum4%20doc.pdf?ver=1558552531562