Tunnel VUE

CoreVUE

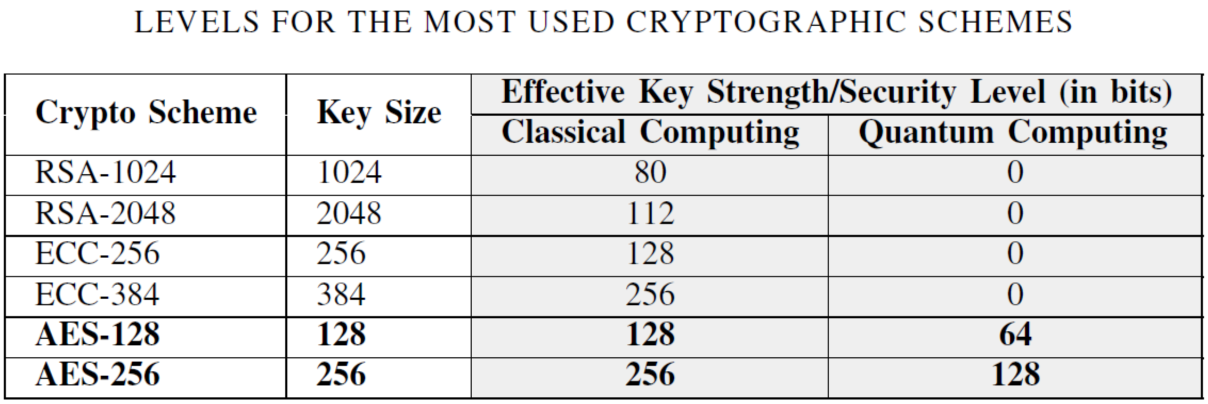
A Multifactor Post-Quantum Security Breakthrough

High Level Description

www.TunnelVUE.com

CoreVUE's technology 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, while allowing universal encryption of all data in transit with no hands-on management including configuration of routers, switches, etc. 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 that uses integer factorization to derive the key. The tactic for today's current industry standard methodology for breaking encryption is that it looks for underlying patterns of characters which compose the encrypted message. The multifactor postquantum method implemented by CoreVUE wraps each packet in an encrypted session (including the very first packet) with a separately-established, unique key for each session and a unique key for every packet within each session, making it impossible to be broken by quantum computers. CoreVUE's key manager does not care about the key size and has no limitation on the size of the code or the size of the key. The only limitations are the ones set by users.

As technology continues to advance to the quantum age, existing methods of encryption and key exchange are continuously being reduced in their effective security as new quantum algorithms are released. Two of the most effective algorithms are Shor's Algorithm[1] and Grover's Algorithm[2]. CoreVUE's method is the answer to these two emerging threats to cryptographic security.



LEVELS FOR THE MOST USED CRYPTOGRAPHIC SCHEMES

Crypto Scheme	Key Size	Effective Key Strength/Security Level (in bits)	
		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**

[3]

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. CoreVUE does not use any form of asymmetric encryption or its derivative Public Key Infrastructure (PKI) for key management and exchange.

[1] https://quantumexperience.ng.bluemix.net/proxy/tutorial/full-user-guide/004-Quantum_Algorithms/110-Shor%27s_algorithm.html

[2] https://quantumexperience.ng.bluemix.net/proxy/tutorial/full-user-guide/004-Quantum_Algorithms/070-Grover%27s_Algorithm.html

[3] Mavroeidis, Vasileios, et al. "The impact of quantum computing on present cryptography." *arXiv preprint arXiv:1804.00200* (2018). https://arxiv.org/pdf/1804.00200.pdf

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 unstructured search of a brute force attack 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. 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.

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

This is possible because every iteration of the session key requires the algorithm to run through the entire space of the second key to determine if it is a valid key or not. But due to the nature of CoreVUE’s dynamic packet key the current implementation of Grover’s Algorithm is not applicable to CoreVUE’s methodology because the implementation of a unique session key over a dynamic packet key creates a one time pad that is multi-factored where the solution to the session key which must be determined first and reversed results on an encrypted message that requires running through all iterations of the dynamic packet key. Since the dynamic packet key changes with each packet, there are no underlying commonalities or visibly shared structure between packets to aid in the decryption of the session key. Since Grover's Algorithm cannot search for what it doesn't know to look for, it does not apply to the CoreVUE methodology.

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[4].

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[5] is solved CoreVUE faces no significant mathematical vulnerabilities including all current publicly available algorithms. CoreVUE’s existence as a key management methodology *is not tied to any specific encryption methodology or key generator.* Even if vulnerabilities are found in the underlying encryption itself it does not weaken CoreVUE in any way as it can be quickly modified to function with any symmetric encryption or key generator as needed. Until a significant breakthrough in mathematics occurs CoreVUE will remain unaffected by advances by computational methodologies.

[4] https://www.sciencedirect.com/science/article/pii/0166218X84900817

[5] http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.515.2584&rep=rep1&type=pdf