Tunnel VUE

CoreVUE Synopsis

High Level Technical Description

www.TunnelVUE.com

The Problem/Opportunity

In the foreseeable future, quantum computers will be capable of breaking essentially all public-key cryptosystems currently in use[1]. This will seriously threaten the security and integrity of digital communications because public key cryptography underlays a plethora of applications important to our economy, our security, and our way of life, such as mobile phones, internet commerce, social networks, and cloud computing. This disruption shall make current infrastructure and application protections irrelevant and force the replacement of existing cryptography methods. This catastrophic prediction is immense, high-impact, and imminent. Data encrypted with current cryptosystems systems will not withstand future codebreaking technology and can/will gravely compromise people and organizations.

Impact of Quantum Computing on Common Cryptographic Algorithms

Cryptographic Algorithm	Type	Purpose	Impact from large-scale quantum computer
AES	Symmetric key	Encryption	Larger key sizes needed
SHA-2, SHA-3	---------------	Hash functions	Larger output needed
RSA	Public key	Signatures, key establishment	No longer secure
ECDSA, ECDH **(Elliptic Curve Cryptography)**	Public key	Signatures, key exchange	No longer secure
DSA **(Finite Field Cryptography)**	Public key	Signatures, key exchange	No longer secure

[1] *Source: NIST Report on Post-Quantum Cryptography, NISTIR 8105,* https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.8105.pdf

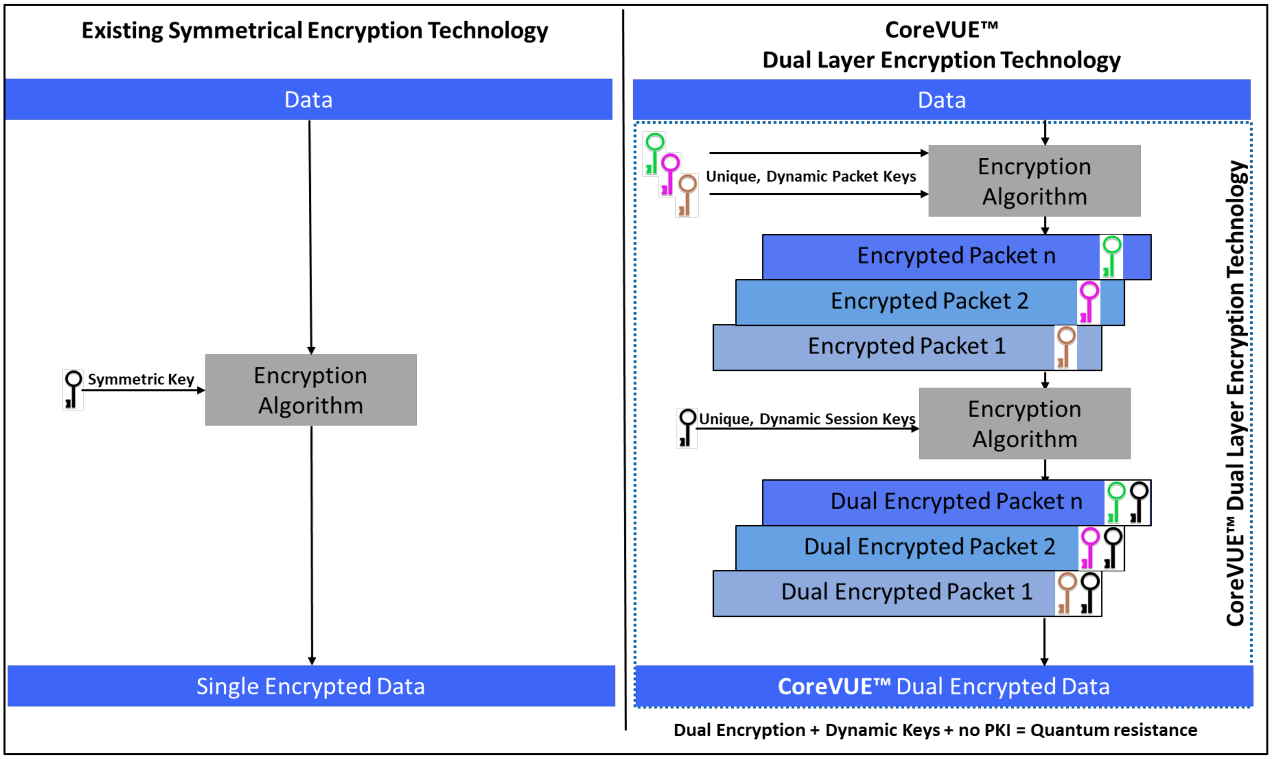
In its 2016 proposal solicitation for post-quantum cryptosystems, NIST wrote "it appears that a transition to post-quantum cryptography will not be simple as there is unlikely to be a simple "drop-in" replacement for our current public-key cryptographic algorithms." NIST did not see CoreVUE™

CoreVUE™ is a extremely powerful breakthrough methodology that implements dual layer encryption together with digital, dynamic, one-time pad emulation, enabling quantum resistant data security everywhere and anywhere in an enterprise, regardless of hardware or operating system.

Imagine in every data transaction you could automatically & securely change the secret key used to encrypt your next message, and the intended recipient of that encrypted message, could automatically and securely decrypt that message using that key. Every key is used only once and is never reused, there are only two copies of each key, one for the sender and one for the recipient, and the keys are destroyed after each use. In the past this was not possible. The ability to automatically create and digitally distribute a new key to only the one sender and the receiver at each session did not exist, **until now…**

CoreVUE™ Dual Layer Encryption Technology

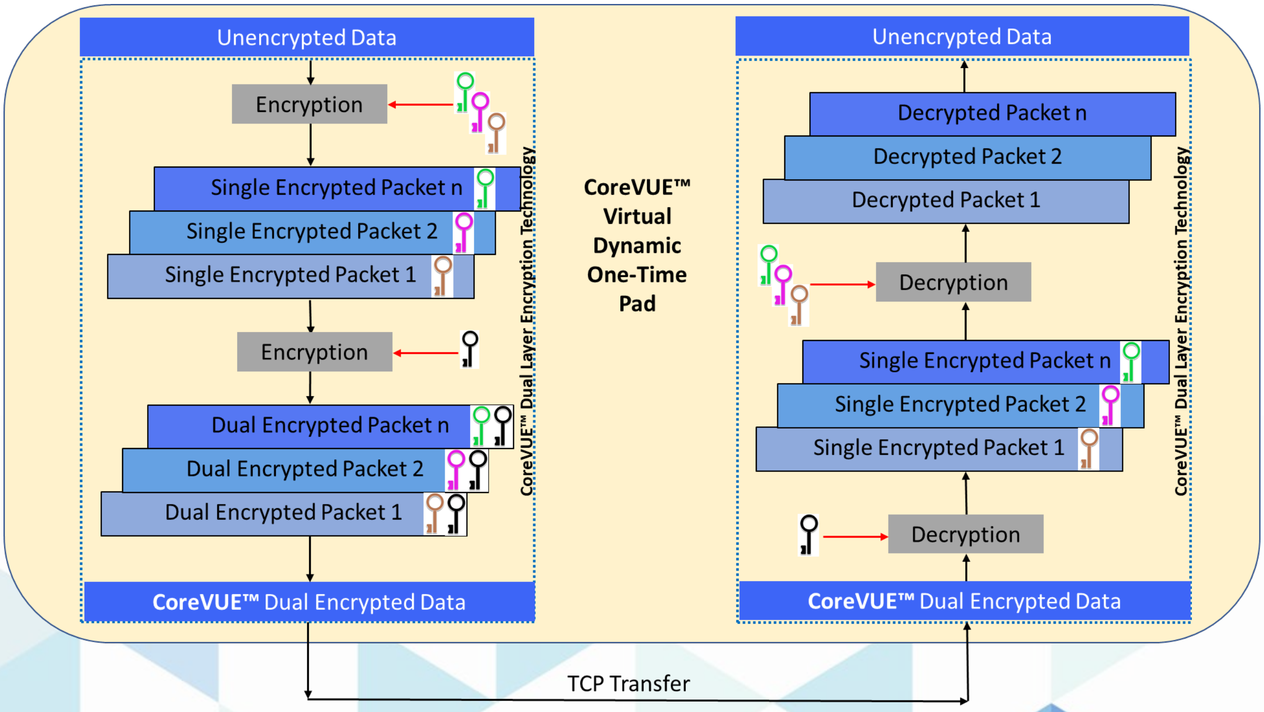
Using any symmetric algorithm, the CoreVUE™ process encrypts every packet with a dynamic packet key that is unique to each packet. Then also for each session, CoreVUE™ generates a new symmetric session key. CoreVUE™ uses that key to double encrypt each packet. Every packet key and every session key is unique and different. This effectively strengthens existing symmetric encryption to quantum resistant encryption -all while maintaining a small operational footprint and low system resource utilization.


Existing Symmetrical Encryption Technology
Data
Symmetric Key
Encryption Algorithm
Single Encrypted Data
CoreVUE™
Dual Layer Encryption Technology
Data
Unique, Dynamic Packet Keys
Encryption Algorithm
Encrypted Packet n
Encrypted Packet 2
Encrypted Packet 1
Unique, Dynamic Session Keys
Encryption Algorithm
Dual Encrypted Packet n
Dual Encrypted Packet 2
Dual Encrypted Packet 1
CoreVUE™ Dual Layer Encryption Technology
CoreVUE™ Dual Encrypted Data
Dual Encryption + Dynamic Keys + no PKI = Quantum resistance

Since each packet is first fully encrypted via a dynamic key that changes with each packet, and then it's encrypted again via a new key each session. An attacker must break both the session key and packet key simultaneously to read only one packet. Without both a packet key and the session key, an attacker is unable to determine if the session key is correct, and yet each packet key must still be individually broken.

With each underlying packet key being different than every other packet key, there are no commonalities between packets to aid in decryption. Data remains confidential even into the quantum age.

CoreVUE™ Virtual Dynamic One-Time Pad


Unencrypted Data
Encryption
Single Encrypted Packet n
Single Encrypted Packet 2
Single Encrypted Packet 1
Encryption
Dual Encrypted Packet n
Dual Encrypted Packet 2
Dual Encrypted Packet 1
CoreVUE™ Dual Layer Encryption Technology
CoreVUE™ Dual Encrypted Data
CoreVUE™ Virtual Dynamic One-Time Pad
Unencrypted Data
Decrypted Packet n
Decrypted Packet 2
Decrypted Packet 1
Decryption
Single Encrypted Packet n
Single Encrypted Packet 2
Single Encrypted Packet 1
Decryption
CoreVUE™ Dual Layer Encryption Technology
CoreVUE™ Dual Encrypted Data
TCP Transfer

The **CoreVUE™** virtual dynamic one time-pad follows all the unbreakable rules of OTP:

- The keys comply with existing block-cypher methodology and can be adjusted to the strength desired;
- The keys are random as generated by a FIPS 140-2 certified random number generator;
- The keys are unique to the specific instance of the **CoreVUE™** enabled process or application;
- There are only two copies any key: one for the sender and one for the receiver;
- The keys are stored in a **CoreVUE™** specific format that is also dual-layer encrypted;
- Each key is used only once, and both sender and receiver destroy their key after use.

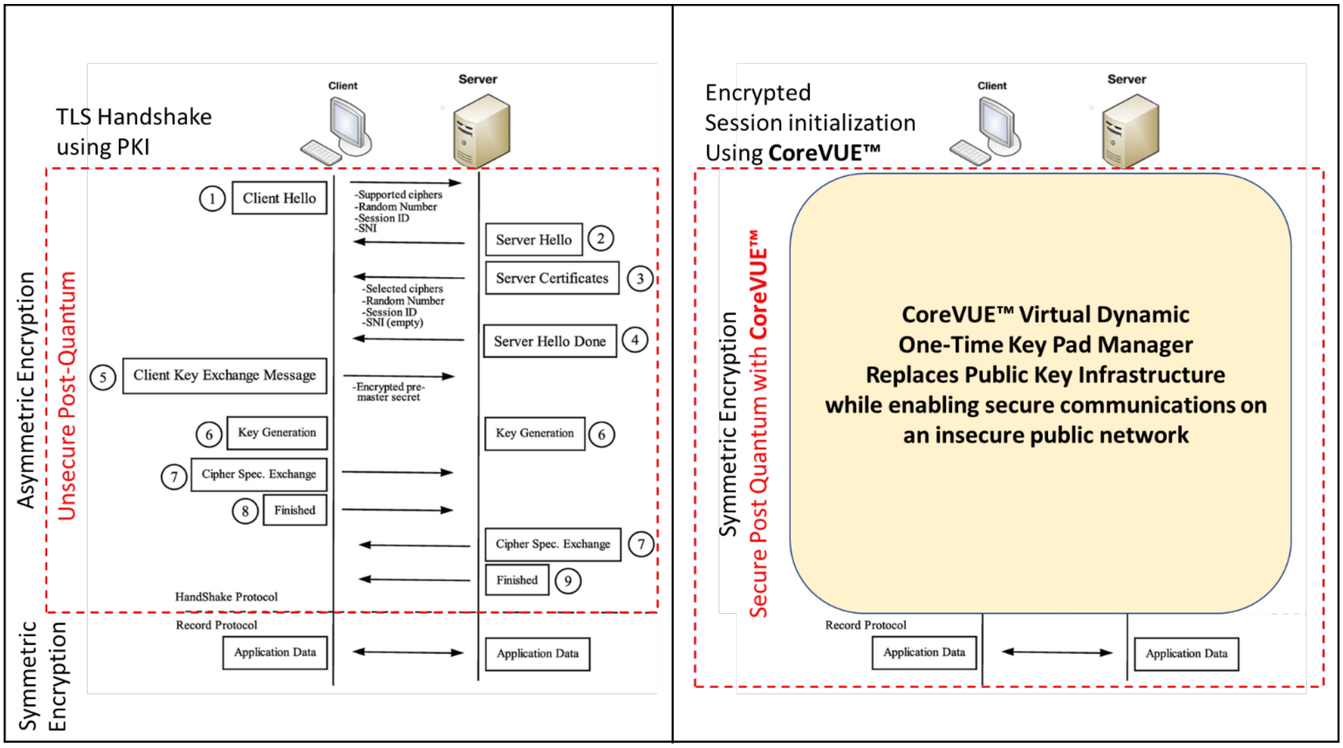
If the entire **CoreVUE™** code was released and the processes and methodologies were public, there would be no way to use that information to recreate the keys or break the encrypted data.

CoreVUE™ manages data encryption keys to encrypt every packet differently and every session differently.

CoreVUE™ has no limitation on the size of the code or the size of the keys.

CoreVUE™ requires zero human intervention for key management, distribution, storage and usage.

CoreVUE™ & Key Exchange



- **CoreVUE™** eliminates Public Key Infrastructure (PKI) or other asymmetric key management systems.
- **CoreVUE™** enables universal encryption of all data in transit with no hands-on management.
- **CoreVUE™** implements virtual a one-time pad for one-use keys that change for every encryption.
- **CoreVUE™** eliminates the use of asymmetrical encryption.
- **CoreVUE™** resolves the quantum threat from public key cryptosystem by eliminating the use of PKI (or other asymmetric key management systems).
- **CoreVUE™** is a separate, patent pending, licensable product that can be embedded into firmware or software systems as part of any "cybersecurity built-in" initiative in an organization.

CoreVUE™ Quantum Resistance

Quantum computing will disrupt existing cryptography methods making current infrastructure and application protections irrelevant. This disruption is immense, high-impact and imminent.

Current encryption technology relies on public key encryption, digital signatures and key exchanges to protect business commerce, communications, identity and data. These cryptographic schemes are underpinned by a set of vetted algorithms, and the level of protection is based on the strength of the underlying math and difficulty of calculation. Quantum computing processing power can solve the most difficult underlying math problems very efficiently, exposing cryptographic keys, thereby disrupting encryption and enabling exposure of data globally and immediately to threat actors and malicious attackers.

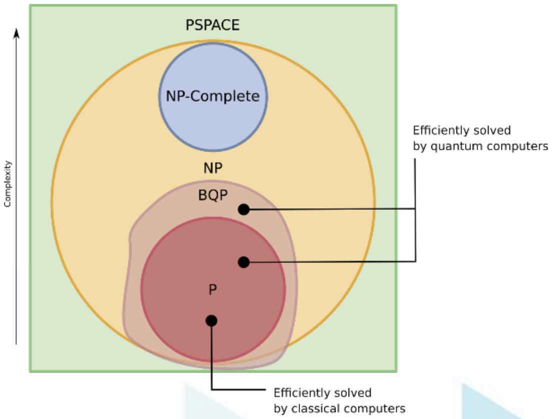
CoreVUE's dynamic dual-layer methodology is not subject to existing quantum algorithms. Shor's Algorithm, a quantum computer algorithm for integer factorization has been proven to decrypt data previously encrypted using asymmetric encryption methods. Because CoreVUE™ does not use any form of asymmetric encryption or its derivative Public Key Infrastructure (PKI), Shor's Algorithm poses no risk to **CoreVUE™**.

Grover's Algorithm is not applicable to our dual-layer implementation because dual layering requires an attacker to break both the session key and the packet key simultaneously, which requires an attacker to run the entire key space for every packet key for each iterative attempt to break the session key. Without both the session key and the packet key, an attacker is unable to determine if the session key is correct. 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 **CoreVUE™**.

Further, if Grover's algorithm is applied to **CoreVUE™** only 50% of the standard reduction generally associated with Grover's Algorithm would be suffered. **CoreVUE™** dual-layer methodology changes the reduction of a 256-bit key from 128 to 192, strengthening 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	$\sqrt{2^{256}} = 128$
Updated AES deployed with 2 (128) bit Keys	$\sqrt{2^{128}} * 2^{128} = 192$

The **CoreVUE™** dynamic, multi-factor, dual-layer encryption technology mathematically appears as an NP-Complete problem matching the description of a Boolean Satisfiability Problem[1]. Until P versus NP[2] is solved **CoreVUE™** faces no significant mathematical vulnerabilities including all current publicly available algorithms. Since **CoreVUE™** 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.


PSPACE
NP-Complete
NP
BQP
P
Complexity
Efficiently solved by quantum computers
Efficiently solved by classical computers

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

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