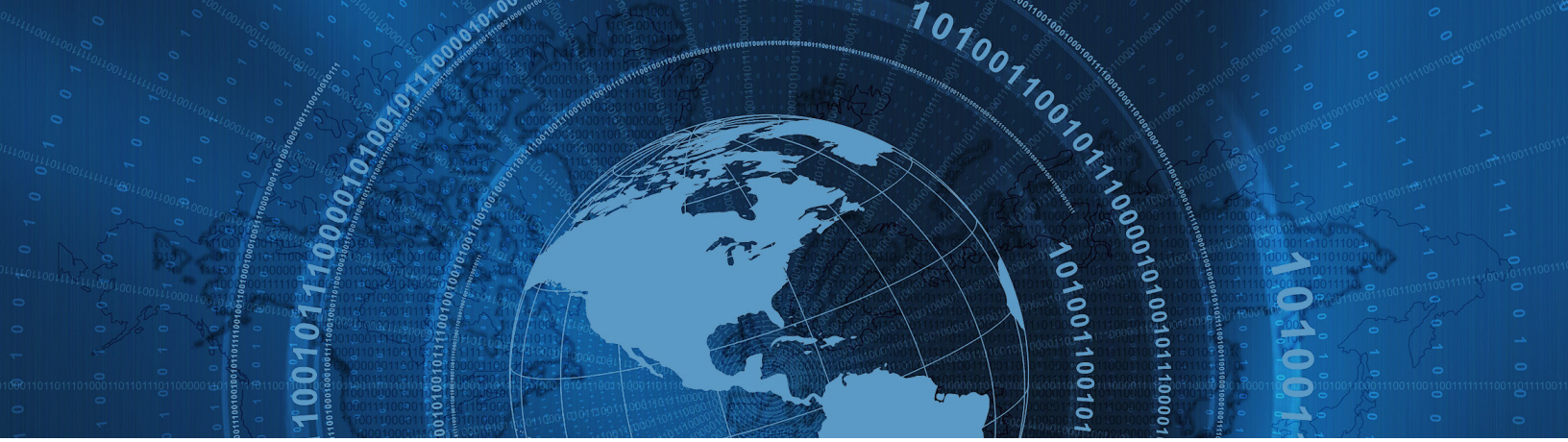

PKMS2 Encryption Protocol White Paper

FEBRUARY 2018

PKMS2 Encryption Protocol

Encryption is a critical element of the global datascape

It offers privacy and security protections, is critical to building and maintaining trust, provides a sense of stability and solidity, empowers commerce, and is the foundation of ubiquitous connectivity. Within the ever-expanding ocean of data being created by this connectivity is a similarly growing sea of sensitive information that includes anything from healthcare records to financial-account information, critical business-planning materials, intellectual property, trade secrets, contracts, and contact lists.

Symmetric Encryption - Most symmetric-key encryption algorithms rely on block ciphers, such as the Advanced Encryption Standard (AES). A block cipher can only encrypt short blocks (e.g., 128 bits for AES) using a secret key (e.g., 128 or 256 bits). In order to securely encrypt multi-block data, block ciphers are then usually employed within more complex methods, referred to as ***modes of operation.***

PKMS2 Encryption Protocol - The Secure Channels Pattern Key, Multi-Segment, Multi-Standard (PKMS2) encryption protocol is a ***patented mode of operation**** used for the encryption & decryption of data for use with trusted, well-known, symmetric block ciphers such as Advanced Encryption Standard (AES) or ARIA.

The current PKMS2 cipher suite includes: FIPS140-2 compliant (AES), and seven other trusted, well-researched, symmetric algorithms including: Serpent, Speck, Simon, ARIA, MARS, Camellia, and Twofish.

*PKMS2 Patent No. 13/489,388 PKMS2 Enterprise Patent No. 15/881,648

PKMS2 provides significant improvements in three areas:

Quantum Future Proofing: As a mode of operation, it ***utilizes multiple block ciphers*** (not simply relying on a single cipher) for data protection. Additionally, it provides "fallback security" in the event a cipher used in the PKMS2 process becomes insecure (e.g., has an arbitrary unknown backdoor, or is cryptanalyzed), it will remain provably secure as long as the remaining cipher/key(s) are secure.

Longer Effective Key Length: Provides a provably longer key length than the constituent ciphers being used by PKMS2 (e.g., presuming PKMS2 uses ciphers having 256-bit keys and 128-bit block sizes (e.g., AES-256), this allows PKMS2 to obtain an ***effective key length of at least 387 bits.*** This provides provable and increased security against brute-force attacks.

Superior Patented Design: PKMS2's ***patented layering*** provides provable significant security against message-recovery attacks with respect to the best-known attacks, due to the use of segmentation. It substantially increases the effort required to attack the encryption scheme when attempting to recover the underlying data.

PKMS2's superior patented design provides quantum future-proofing, a longer effective key length, "fallback security", and a host of other encryption benefits that provide superior data encryption.

PKMS2 Encryption Protocol

What Top Cryptology Experts say about PKMS2

PKMS2 Formal Expert Analysis & Validation

(http://www.securechannels.com/peer-reviews)

A mathematical analysis of PKMS2 was conducted by our Vice President of Cryptographic Engineering and verified by three prominent academic cryptographers.

Dr. Jonathan Katz, Vice President Cryptography Engineering, Secure Channels Inc.
Professor, Computer Sciences, University of Maryland and Dir. Maryland Cybersecurity Center (MC2)
Ph.D. Computer Science, Columbia University

Excerpts of his Analysis of PKMS2:

Dr. Katz's report, "Security Analysis of PKMS2," shows that PKMS2 offers significant improvements in three areas:

- "Even if a cipher used in the first layer of the multilayer scheme is insecure (e.g., has an arbitrary, unknown backdoor, or is cryptanalyzed), PKMS2 remains provably secure"
- "The effective key length of PKMS2 is provably up to 50% greater than that of component 256-bit ciphers such as AES"
- "The use of segmentation offers improved security against the best-known message-recovery attacks."

Dr. Yevgeniy Dodis, Professor, Computer Science, Courant Institute of Mathematical Sciences, NYU
Ph.D. Computer Science, M.I.T.

Excerpts of his Analysis of PKMS2:

- "(PKMS2's) segmentation significantly improves security against message recovery attacks"
- "Even if a cipher used in the first layer of the multilayer scheme is insecure (e.g., has an arbitrary, unknown backdoor, or is cryptanalyzed), PKMS2 remains provably secure."

PKMS2 Encryption Protocol

Dr. Matthew Green, Assistant Professor, Computer Science, The Johns Hopkins University
Ph.D. Computer Science, The Johns Hopkins University

Excerpts of his analysis of PKMS2:

- "A number of results in the field of cryptography deal with the problem of double (or multiple) encipherment using block ciphers… The PKMS2 protocol… result produces a much stronger overall construction."
- "These results provide confidence that the PKMS2 protocol is secure under a strong threat model, even against an attacker with significant resources."

Dr. Stefano Tessaro, Assistant Professor, Computer Science, University of California, Santa Barbara
Ph.D. ETH Zurich (Swiss Federal Institute of Technology in Zurich)

Excerpts of his analysis of PKMS2:

- "Secure Channels' PKMS2 is a mode of operation. It however adopts a number of measures to achieve higher security than existing modes of operation, without excessively compromising efficiency."
- "The analysis shows that PKMS2 achieves higher security than existing methods – in particular, the effective length of keys substantially increases. In most practical cases, the increase is between 50% and 100%."
- "We could not identify any problems with the security analysis. All security claims and their proofs are correct, and the proof techniques are non-trivial and sophisticated. The outcome of the analysis also clearly shows that within the efficient constraints imposed on the scheme, PKMS2 achieves essentially the best possible security.'