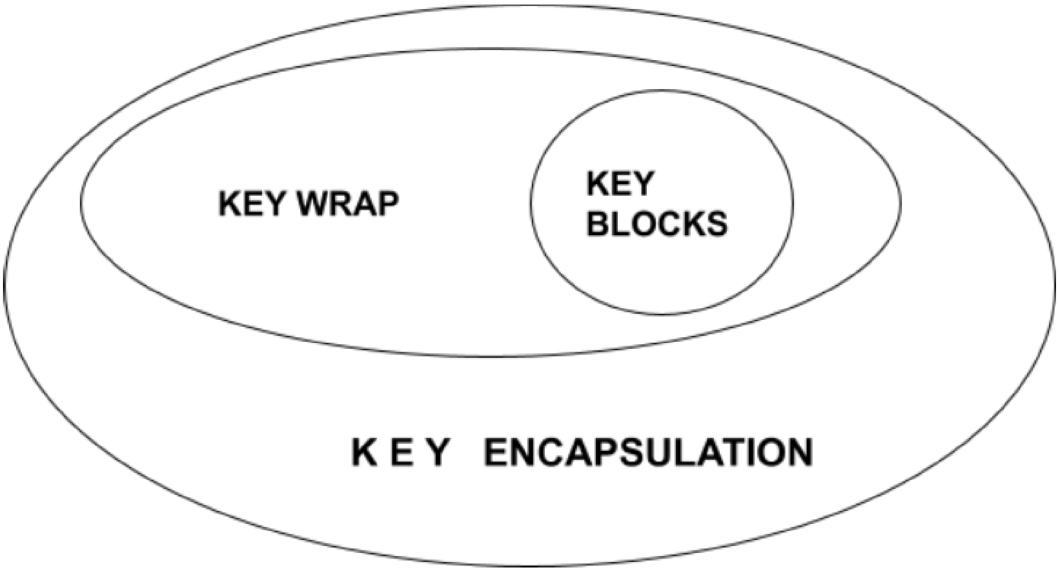
A Brief Reminder about Key Wrapping

Martin Rupp
SCIENTIFIC AND COMPUTER DEVELOPMENT SCD LTD

Contents

1 Key Wrapping vs. Key Encapsulation vs. Key Blocks

Key wrapping shares a similar goal to key encapsulation and key blocks: *protecting cryptographic keys in an insecure environment.* It protects keys by using symmetric key encryption algorithms. However, it focuses more precisely on cryptographically protecting “high-entropy" messages against various attacks.



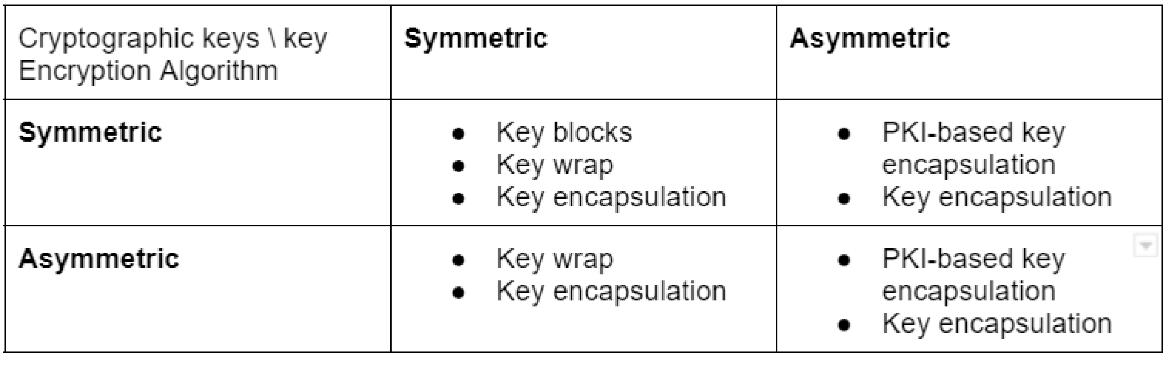
⇒ Key wrapping is a larger set than key blocks because it is not restricted to explicitly protecting a symmetric cryptographic key with a symmetric cipher.

⇒ Key encapsulation is a global mechanism that encompasses key wrapping and key blocks. Usually, key encapsulation refers to PKI-based key encapsulation, but here we consider the term in its broader acceptance (“encapsulate" a key).

While there isn’t a specific norm for key blocks, they are generally defined following ANSI X9 TR (Technical Report) 31. Hence, a key wrap of a symmetric key using a symmetric key encryption algorithm may not fall automatically into the “key block" category. However, while the opposite might generally be true, etc.

A precise categorization of key wrap algorithms is that they should provide both encryption and authentication but never use nonces (arbitrary numbers). However, this is not always true for all key wrap algorithms.

Below is a table that summarises this:



Cryptographic keys \ key Encryption Algorithm	**Symmetric**	**Asymmetric**
Symmetric	• Key blocks • Key wrap • Key encapsulation	• PKI-based key encapsulation • Key encapsulation
Asymmetric	• Key wrap • Key encapsulation	• PKI-based key encapsulation • Key encapsulation

2 Key Wrap Algorithms

2.1 Security Concerns They Solve

Key wrapping security focuses on providing algorithms that resist several classes of cryptographic vulnerabilities. These vulnerabilities are also common to the key blocks. However, key wraps often solve them differently :

1. **Bad procedures**. This encompasses a broad spectrum of problems: key tests used in production or found in public repository servers such as GitHub.
2. **Bad quality of random number generation**. This happens when the random number generator used is not “random" enough and doesn’t produce consistent data. (*Note that key wrapping algorithms are not supposed to use cryptographic nonces precisely as a radical approach to making key wraps resistant to such attacks.*)
3. **Exhaustive search of 56-bit DES keys**. This may happen when using Triple-DES if an erroneous design allows an attacker to gain information by attacking the two (or three) pieces of the Triple-DES key separately.
4. **Key usage manipulation**. This is a well-known problem that key block design can solve and protect the key, which is typically unciphered and in plaintext.
5. **Vulnerabilities with keys encrypted over more than one block**. When a key is long enough, it can be encrypted over more than one cipher block. This means there must be a way to “bind" all the key blocks together to prevent modification.

2.2 Four Main Key Wrap Algorithms

NIST (see [1]) has extensively studied the key wrapping problem and has published a list of recommended algorithms that are based on AES and Triple-DES:

- **AESKW** (a variant of the AES key wrap specification)
- **TDKW** (similar to AESKW but built from Triple-DES, rather than AES)
- **AKW1** (TDES, two rounds of CBC)
- **AKW2** (TDES, CBC then CBC-MAC)

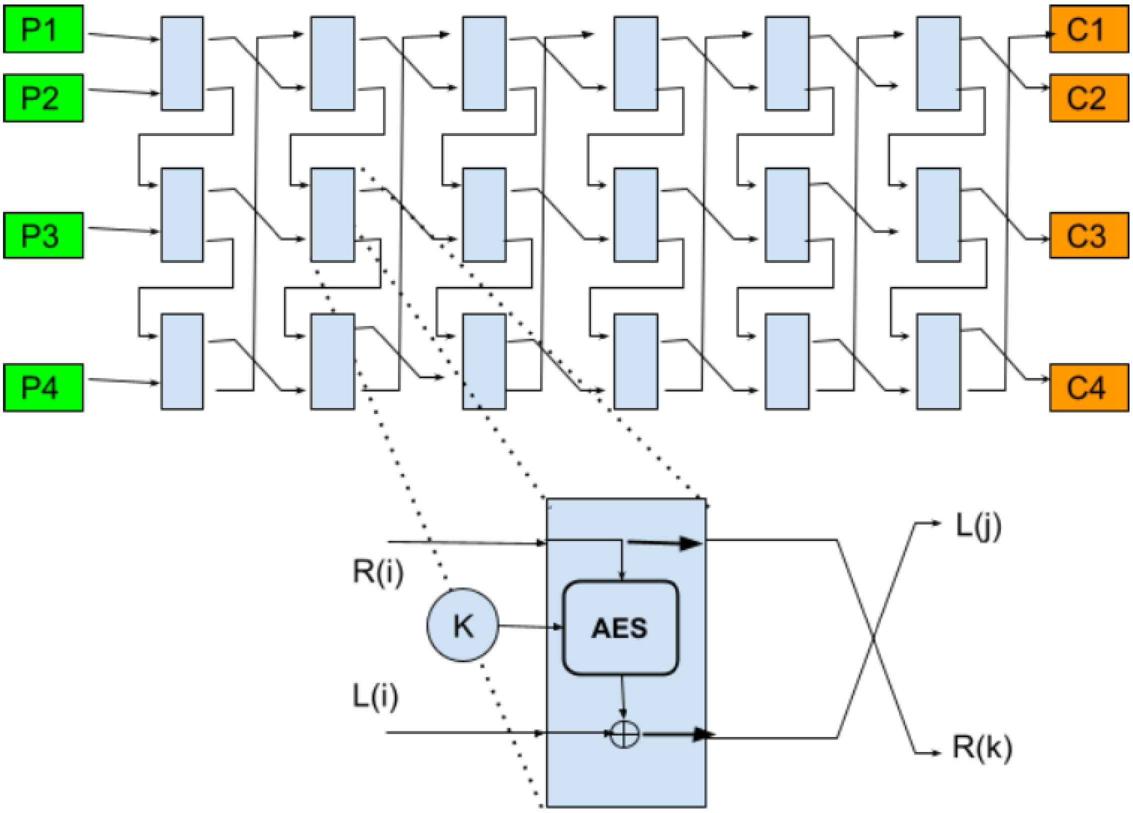
These algorithms have been proposed with the goal of resisting adaptive chosen ciphertext attacks (see [4]). However, NIST has primarily selected AESKW and TDKW as they offer a deterministic authenticated encryption (DAE) mode of operation for the advanced encryption standard (AES) block cipher and, for legacy reasons, of the Triple-DES (please refer to the next chapter in this article for further details about DAE).

X9-102 [3] also proposes these four algorithms, but with slight variations compared to NIST.
In what follows, we describe them according to the X9-102 standard.

2.2.1 AESKW

Since a key wrap does not use nonces, it is not possible to bind blocks by using CBC, CTR with a MAC, or AEX. Instead, a more sophisticated system must be used. AESKW is based on a (nonstandard) Feistel network. The network is of a dimension 6 x (n-1), where n is the portion of the 64-bit block to be encrypted, and *each* box of the network is based on the AES codebook. For example, to encrypt (wrap) a key data of length 4 x 64 bits, it needs to use 6x3=*18* AES encryption boxes. The fundamental difference between a key wrap and key blocks is immediately seen here: no nonce, no MAC-ing, but instead, an 'all-in-one' algorithm.

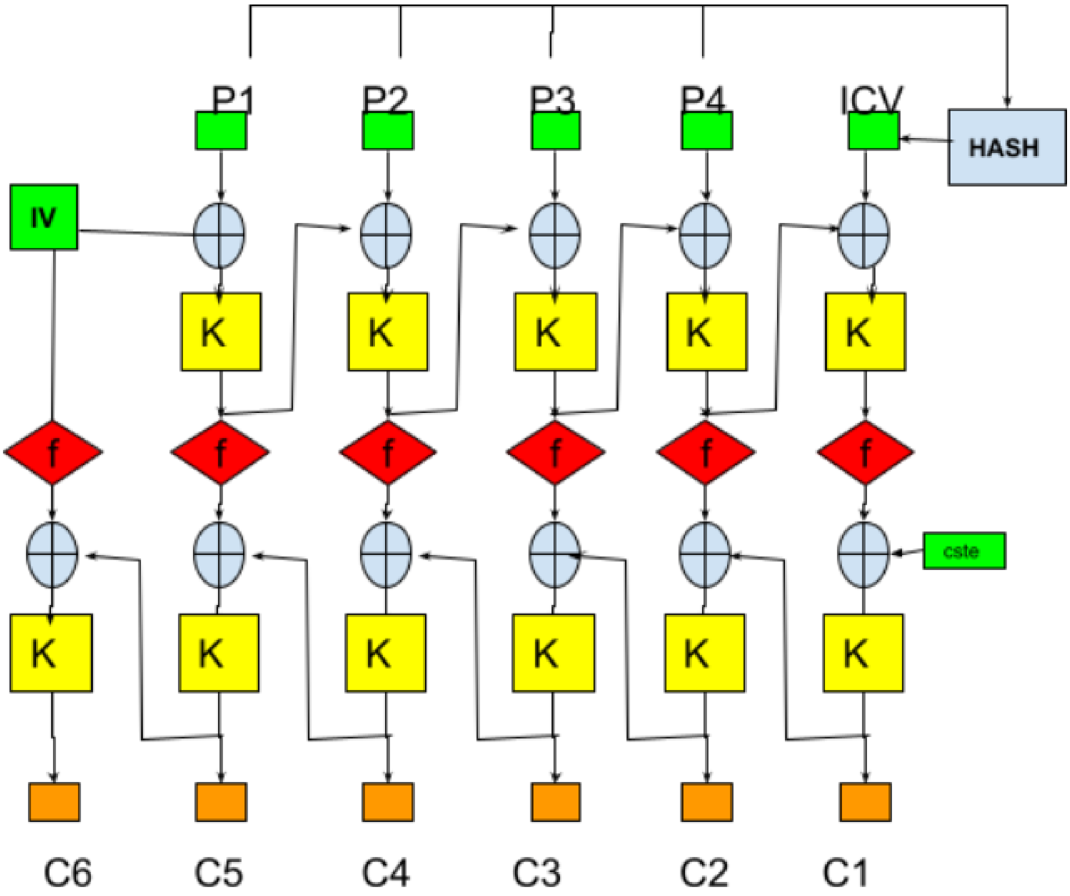
As a result, the AESKW involves much more cryptographic processing than a "standard" TR-31 key block. It may not be suitable for devices with small processors or older devices used for legacy reasons.



All the AES cells (boxes) use the same key-encryption key, K. Generally, n must be such that $n \geq 2$. However, some norms may impose it to be even greater.

2.2.2 TDKW

The TDKW is essentially the same as the AESKW, but Triple-DES boxes replace the AES boxes. That algorithm is generally used for legacy reasons.
AKW1
The AKW1 (and the AKW2) do not use a Feistel network but instead, two rounds of Triple-DES ciphers. They also embed hashing algorithms in the ciphering. Here is an example of the ciphering operations with 4 blocks P(1)...P(4):

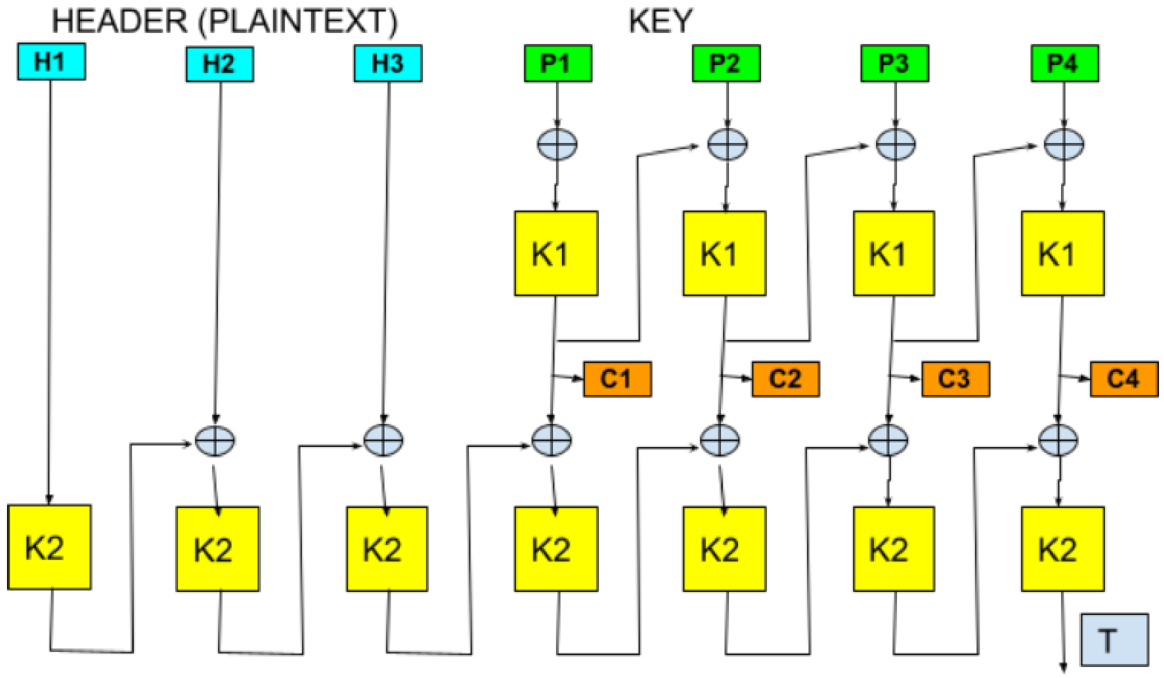


Each of the yellow boxes is Triple-DES in CBC mode, and the red diamonds are inverting (flipping) the bits. Note that the hashing mechanism is based initially on SHA-1, while as of 2020, chosen prefix attacks against SHA-1 are practical. A single encrypting key is used in all the Triple-DES boxes.

AKW1 is different from AESKW since it uses a nonce (the IV) and therefore may achieve semantic security while AESKW cannot. AKW1 is not achieving DAE. Besides, it doesn't provide a way to authenticate an unencrypted plaintext "header" while the other three key wrap algorithms allow this.

AKW2

The AKW2 method was developed initially for the ATM/POS environment. It is also used in environments where processing power is limited. Below is an example of an AKW2 variant that can also process a header:



The yellow boxes are Triple-DES ciphers. Like AKW1, AKW2 is based on a two-round CBC cipher, but with two different keys, K1 and K2, derived from the key-encryption key K. T is a CBC-MAC and acts as a control vector.

3 Deterministic Authenticated Encryption (DAE) Algorithms and Key Wrapping

Deterministic encryption means that with a given key K, the same plaintext will always produce the same ciphertext. An authenticated encryption (AE) is a cryptographic algorithm that provides both confidentiality and integrity. Here integrity means that an attacker can't flip a bit of the encrypted message with the goal that the decrypted plaintext message will be modified. If such a bit is flipped, the decryption algorithm will simply not work. A deterministic algorithm implies no nonce, no random IV, etc.

Key wrapping is often seeking DAE instead of 'conventional' AE. Since the data to encrypt is a cryptographic key, which is by definition carrying some of the highest possible entropy, there is no purpose in protecting a cryptographic key by injecting randomness. In other terms, the general philosophy behind key wrapping is that one does not protect data generated by a random or pseudo-random process (e.g., cryptographic keys) by injecting other random data.

4 Future of Key Wrapping

Key wrapping algorithms are a topic for research. They may replace key blocks entirely in the near future since key wrapping ciphers are generally more sophisticated and more elaborated than their key block counterparts. For example, the SIV (the Synthetic Initialization Vector) is a possible replacement for key blocks since it achieves provable DAE.

5 References

[1] NIST Special Publication 800-38F December 2012: Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping

[2] ISO 20038-2017: Banking and related financial services — Key wrap using AES

[3] ANSI X9.102-2008 (R2017): Symmetric Key Cryptography For The Financial Services Industry - Wrapping Of Keys And Associated Data

[4] Request for Review of Key Wrap Algorithms November 2004 (Accredited Standards Committee X9, Incorporated)

[5] Deterministic Authenticated-Encryption, A Provable-Security Treatment of the Key-Wrap Problem P. ROGAWAY T. SHRIMPTON