IEEE P1619

Security for Storage Data at Rest

Fabio Maino
Cisco Systems
fmaino@cisco.com

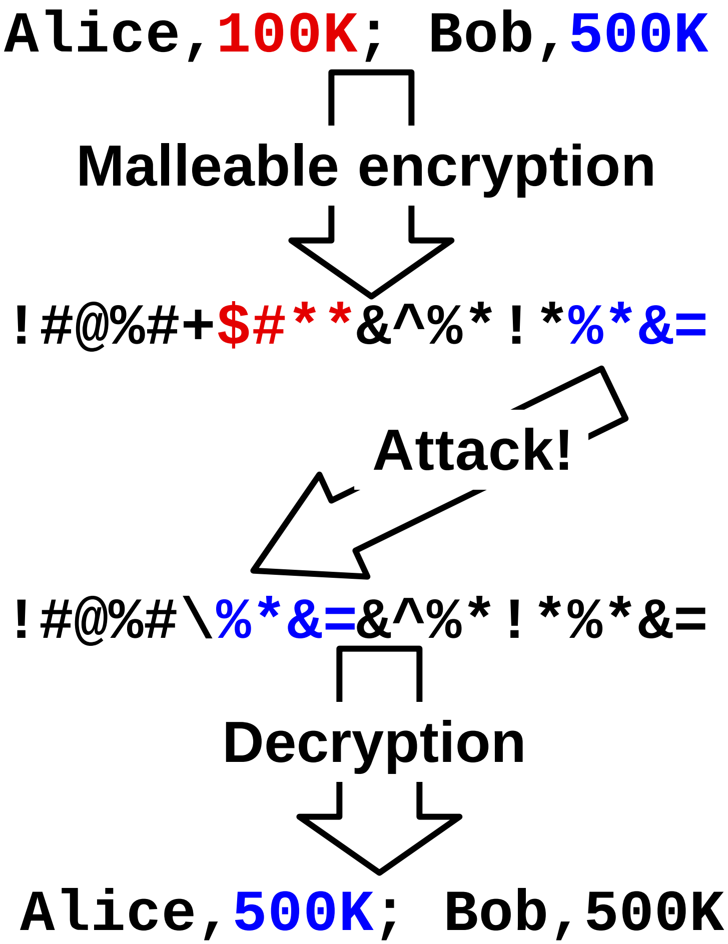
IEEE P1619

- Security for storage data at rest
- Standard security transform that provides confidentiality and pseudo-integrity
    - Applied to 512-byte blocks (up to 2^{128} wide blocks)
    - Without data expansion (no additional integrity tag)
    - Resistant to copy-and-paste attacks
    - Parallelizable for high speed HW
- Standard common format for key backup
    - Allows for decryption of a disk encrypted by any other vendor

Pseudo-Integrity Protection

- **Change in ciphertext produces random plaintext**
  - **The upper-layer applications will likely be "confused" by the result and detect the anomaly**
- **Pseudo-integrity is provided by "tweakable" or "non-malleable" encryption modes**
  - **<u>EME-32-AES</u> (Encrypt-Mix-Encrypt, Halevi)**
    - **Protects the entire 512-byte wide block as a whole**
  - **<u>LRW-AES</u> (Liskov, Rivest, Wagner)**
    - **Protects individually each 16-byte narrow block**
    - **HW Implementations are 50% smaller**
  - **<u>ABL4</u> (Arbitrary Block Length, Mcgrew - Viega)**
    - **Recently proposed as an IP free alternative to EME-32-AES**

Copy-and-Paste Attack



Alice,100K; Bob,500K

Malleable encryption

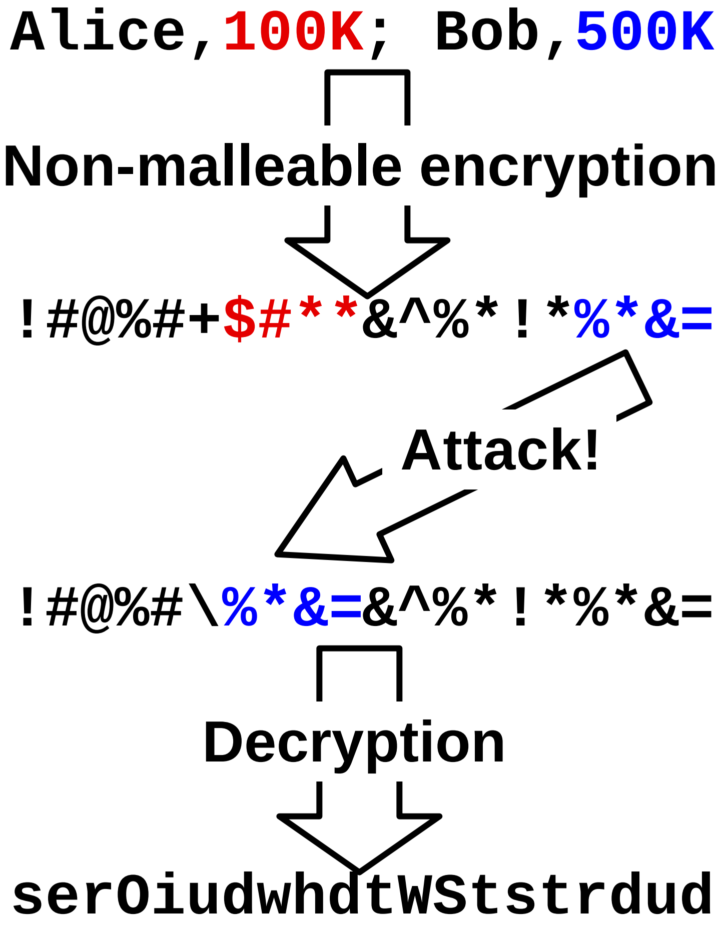
!#@%#+$#**&^%*!*%*&=

Attack!

!#@%#\%*&=&^%*!*%*&=

Decryption

Alice,500K; Bob,500K



Alice,100K; Bob,500K

Non-malleable encryption

!#@%#+$#**&^%*!*%*&=

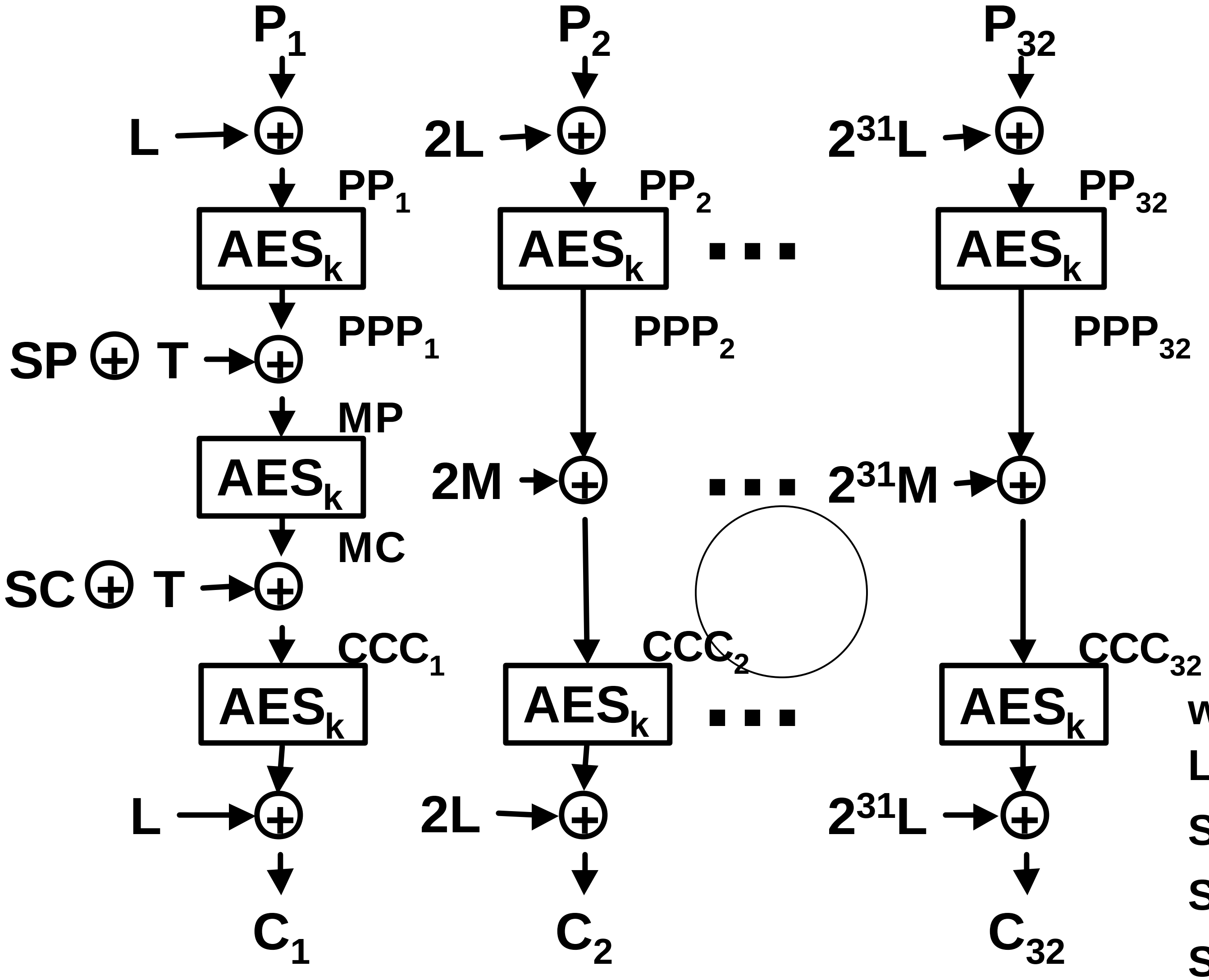
Attack!

!#@%#\%*&=&^%*!*%*&=

Decryption

serOiudwhdtWStstrdud

EME-32-AES (Wide-block)



where:

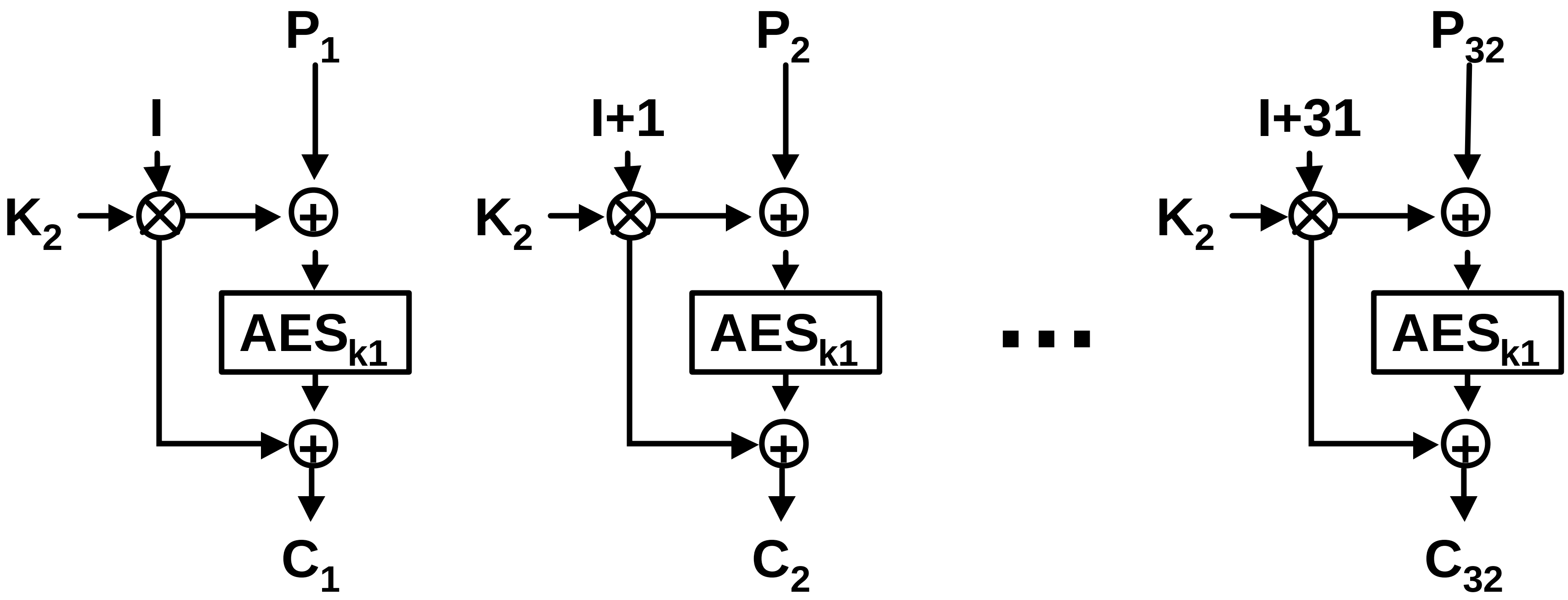
$L = AES_k(0)$

$SP = MP \oplus MC$

$SP = PPP_2 \oplus \ldots \oplus PPP_{32}$

$SC = CCC_2 \oplus \ldots \oplus CCC_{32}$

LRW-AES (Narrow-block)



Key Backup Format

- Standard format to store keys and parameters of the security transform applied to the blocks
- XML format
- Keys are optionally encrypted with a key-encryption key
- ID, Standard Version, Key Scope, Transform, Keys
- Key scope expressed as:

    KEY_SCOPE_START (LBA of first wide-block)

    KEY_SCOPE_LENGTH (number of wide-blocks)

CAP and P1619

- Is there any need for a wide-block size different from 512 bytes?
- Is there any need for a security transform for the extra 8 bytes that CAP is defining?
  - Integrity tag?
  - Encryption of all 520 bytes?
  - encrypt the first 518 bytes and add a CRC of ciphertext to allow downstream diagnosing?
- Other questions?

More Info

- **SISWG web site http://siswg.ieee.org/**
- **Check mailing list archive for updated docs: http://grouper.ieee.org/groups/1619/email/**
- **Send comments at stds-p1619@ieee.org**