XTS-AES

Alfredo De Santis

Dipartimento di Informatica
Università di Salerno

ads@unisa.it

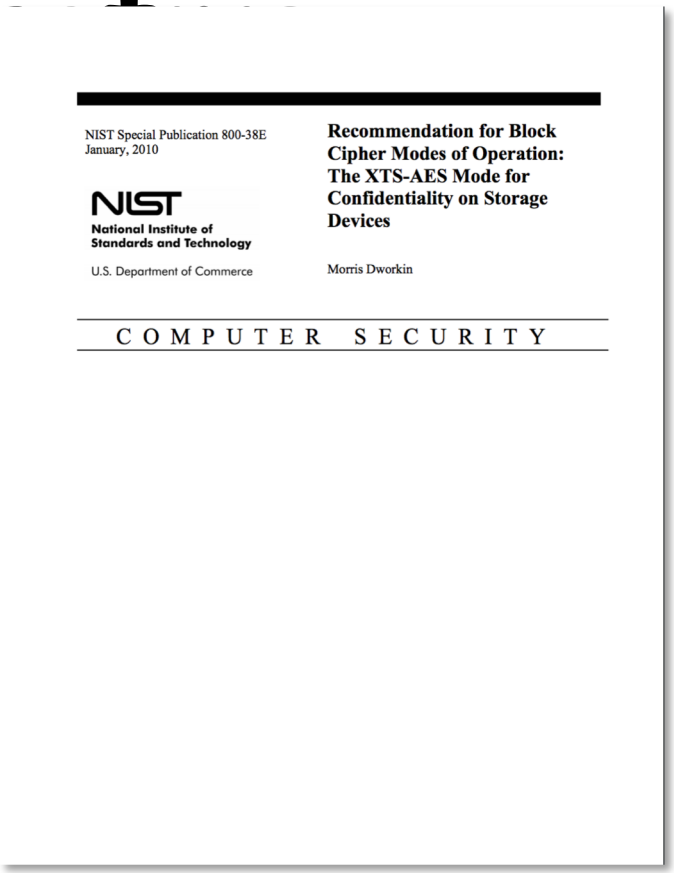
http://www.di-srv.unisa.it/~ads

Ottobre 2019

Modalità operative dei cifrari a blocchi

- NBS FIPS PUB 81, DES modes of operation, National Bureau of Standards, 1981
  - ECB – CBC – CFB - OFB
- NIST SP 800-38A, Recommendation for block cipher modes of operation, National Institute of Standards and Technology, 2001
  - Aggiornamento di ECB – CBC – CFB – OFB ed in più CTR
- NIST SP 800-38E, Recommendation for Block Cipher Modes of Operation: The XTS-AES Mode for Confidentiality on Storage Devices, gennaio 2010
  - XTS-AES già nel IEEE Std 1619-2007
  - XEX-based tweaked-codebook mode with ciphertext stealing

Modalità oper
dei cifrari a b


NIST Special Publication 800-38E
January, 2010

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Recommendation for Block Cipher Modes of Operation: The XTS-AES Mode for Confidentiality on Storage Devices

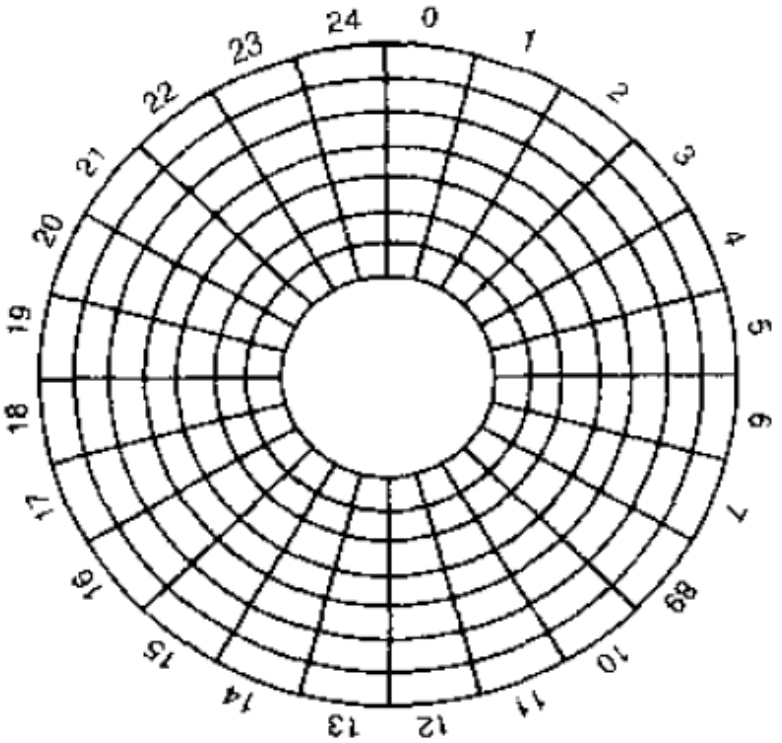
Morris Dworkin

COMPUTER SECURITY

- NBS FIPS PUB 81, DES modes of operat
  Standards, 1981
  - ECB – CBC – CFB - OFB
- NIST SP 800-38A, Recommendation for
  operation, National Institute of Standar
  - Aggiornamento di ECB – CBC – CFB – OFB
- NIST SP 800-38E, Recommendation for Block Cipher Modes of Operation: The XTS-AES Mode for Confidentiality on Storage Devices, gennaio 2010
  - XTS-AES già nel IEEE Std 1619-2007
  - XEX-based tweaked-codebook mode with ciphertext stealing

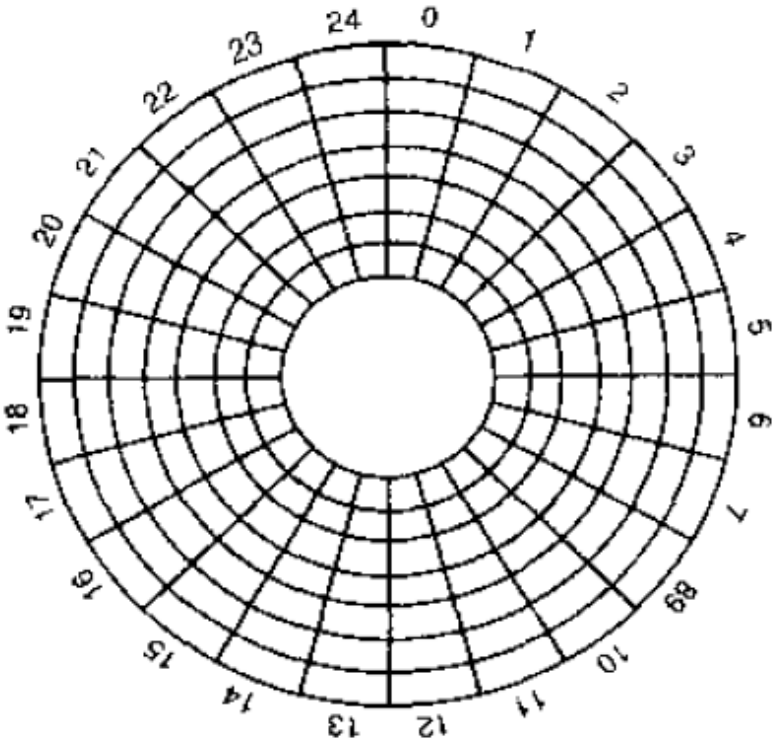
Motivazioni per XTS-AES

- Hard disk partizionati in tracce circolari
- Tracce partizionate in settori di grandezza fissata
  - Minima unità che può essere individualmente letta/scritta
  - Tipicamente 512 byte
  - Può essere suddiviso in blocchi logici
    (con la stessa taglia del cifrario a blocchi)



Motivazioni per XTS-AES

- Hard disk partizionati in tracce circolari
- Tracce partizionate in settori di grandezza fissata
  - Minima unità che può essere individualmente letta/scritta
  - Tipicamente 512 byte
  - Può essere suddiviso in blocchi logici
    (con la stessa taglia del cifrario a blocchi)



Desiderata della cifratura:

- Usare tutto lo spazio
- Dipende solo da:
  - Dati in chiaro
  - Chiave
  - Sector number e block number

Requisiti di progetto per lo standard 1619-2007

- Dati cifrati con grandezza uguale ai dati in chiaro
- Accesso ai dati per blocco in ordine arbitrario
- Nessun uso di metadati oltre alla locazione dei blocchi
- Testo cifrato dipende dalla locazione:
  - Uguali testo in chiaro, uguale chiave, ma locazioni diverse → diversi testi cifrati
  - Uguali testo in chiaro, uguale chiave, uguale locazione → uguale testo cifrato

Requisiti di progetto per lo standard 1619-2007

- Dati cifrati con grandezza uguale ai dati in chiaro
- Accesso ai dati per blocco in ordine arbitrario
- Nessun uso di metadati oltre alla locazione dei blocchi
- Testo cifrato dipende dalla locazione:
  - Uguali testo in chiaro, uguale chiave, ma locazioni diverse → diversi testi cifrati
  - Uguali testo in chiaro, uguale chiave, uguale locazione → uguale testo cifrato

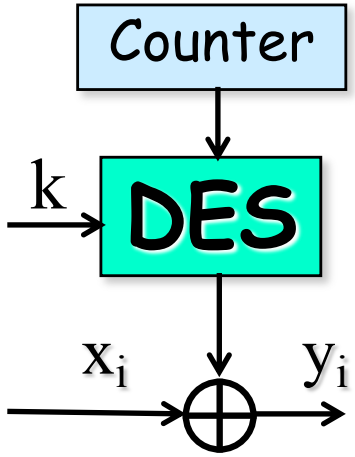
Nessuno dei modi di cifratura ECB/CBC/CFB/OFB/CTR soddisfa i requisiti!

Requisiti di sicurezza per IEEE e NIST

- Non sono espliciti, ci sono solo tracce
- Vediamo quelle nello standard 1619-2007

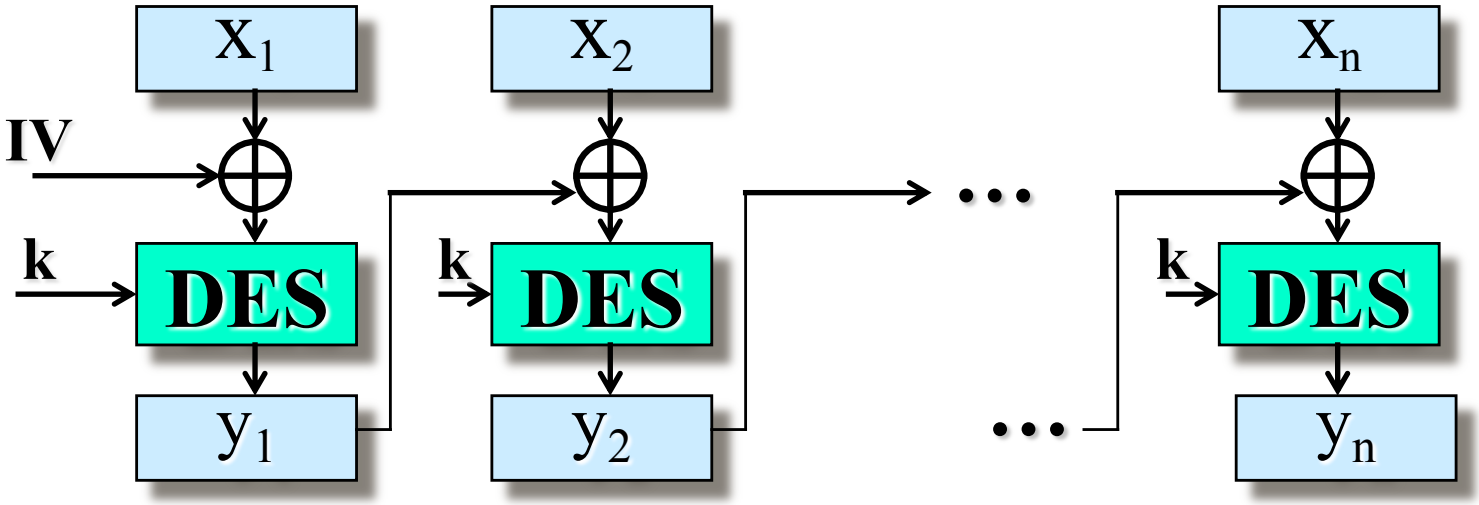
Requisiti di sicurezza per IEEE e NIST

- Non sono espliciti, ci sono solo tracce
- CTR non va bene perché *malleabile*
  - Data una coppia (P,C)
  - C' = C⊕z è il cifrato di P' = P⊕z



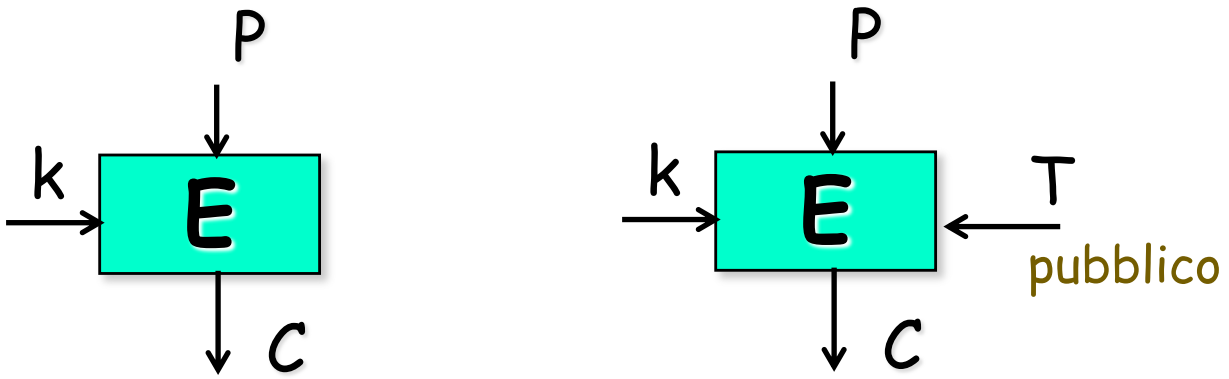
Requisiti di sicurezza per IEEE e NIST

- Non sono espliciti, ci sono solo tracce
- CTR non va bene perché *malleabile*
- CBC (con IV locazione) non va bene perché
  - solo il primo blocco dipende dalla locazione
  - *Malleabile* (*ad es.*, cambio di un bit in y_1 produce cambio del bit corrispondente in x_2)



Concetti usati in XTS-AES
Tweakable Block Cipher

Tweakable Block Cipher

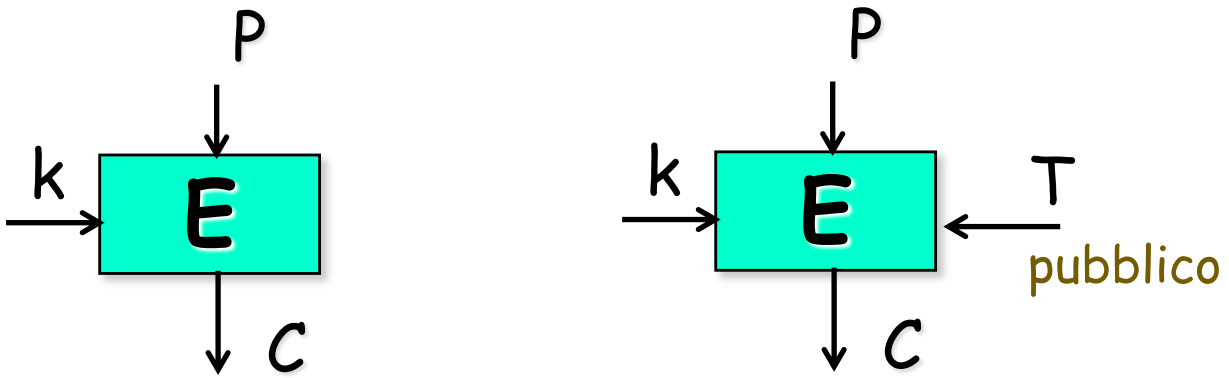


- Famiglia di cifrari indicizzata da T

M. Liskov, R. R. Rivest, and D. Wagner,
Tweakable Block Ciphers,
CRYPTO 2002, vol. 2442 of Lecture Notes in Computer Science, Springer, 2002

Concetti usati in XTS-AES
Tweakable Block Cipher

Tweakable Block Cipher

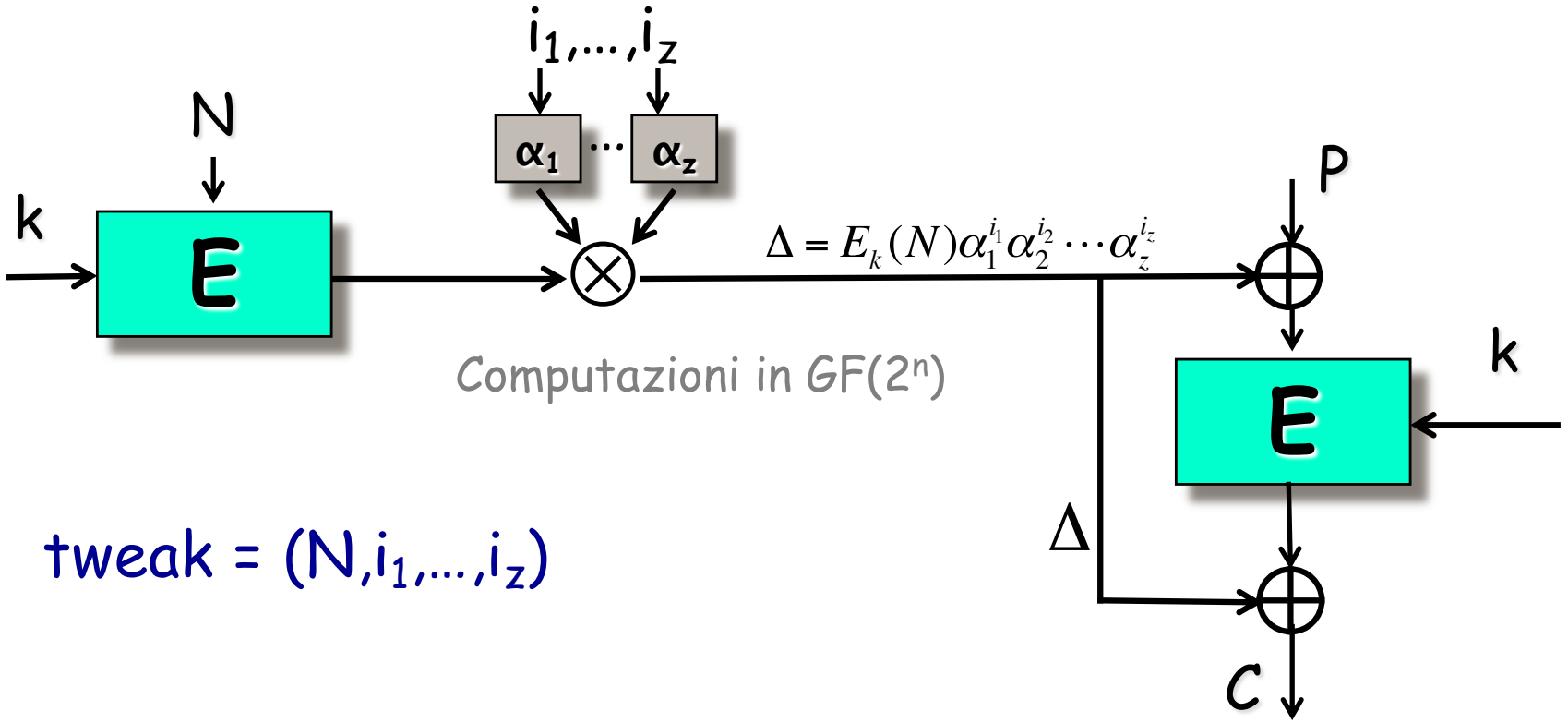


- Famiglia di cifrari indicizzata da T
- Idea: Possiamo usare T come indirizzo del blocco

M. Liskov, R. R. Rivest, and D. Wagner,
Tweakable Block Ciphers,
CRYPTO 2002, vol. 2442 of Lecture Notes in Computer Science, Springer, 2002

Concetti usati in XTS-AES
XOR-Encrypt-XOR

Costruzione di un tweakable block cipher



tweak = (N,i_1,…,i_z)

P. Rogaway,
Efficient instantiations of tweakable blockciphers and refinements to modes OCB and PMAC,
ASIACRYPT 2004, vol. 3329 of Lecture Notes in Computer Science, Springer, 2004

XTS

XEX with tweak and ciphertext stealing

XTS-AES

$key = key_1 || key_2$ (si può usare AES-128, AES-256)

Settore = $P_1, P_2, \ldots, P_m$ (blocchi di 128 bit)

Cifratura = $C_1, C_2, \ldots, C_m$ (blocchi di 128 bit)

$$C_j = AES_{key_1}(P_j \oplus X) \oplus X$$

X dipende da locazione e da chiave key_2

Xor-Encrypt-Xor (XEX)

XTS-AES

$key = key_1 || key_2$ (si può usare AES-128, AES-256)

Settore = $P_1, P_2, \ldots, P_m$ (blocchi di 128 bit)

Cifratura = $C_1, C_2, \ldots, C_m$ (blocchi di 128 bit)

$$C_j = AES_{key_1}(P_j \oplus X) \oplus X$$

X dipende da locazione e da chiave key_2

$$X = AES_{key_2}(i) \otimes \alpha^j$$

Xor-Encrypt-Xor (XEX)

XTS-AES

$key = key_1 || key_2$ (si può usare AES-128, AES-256)

Settore = $P_1, P_2, \ldots, P_m$ (blocchi di 128 bit)

Cifratura = $C_1, C_2, \ldots, C_m$ (blocchi di 128 bit)

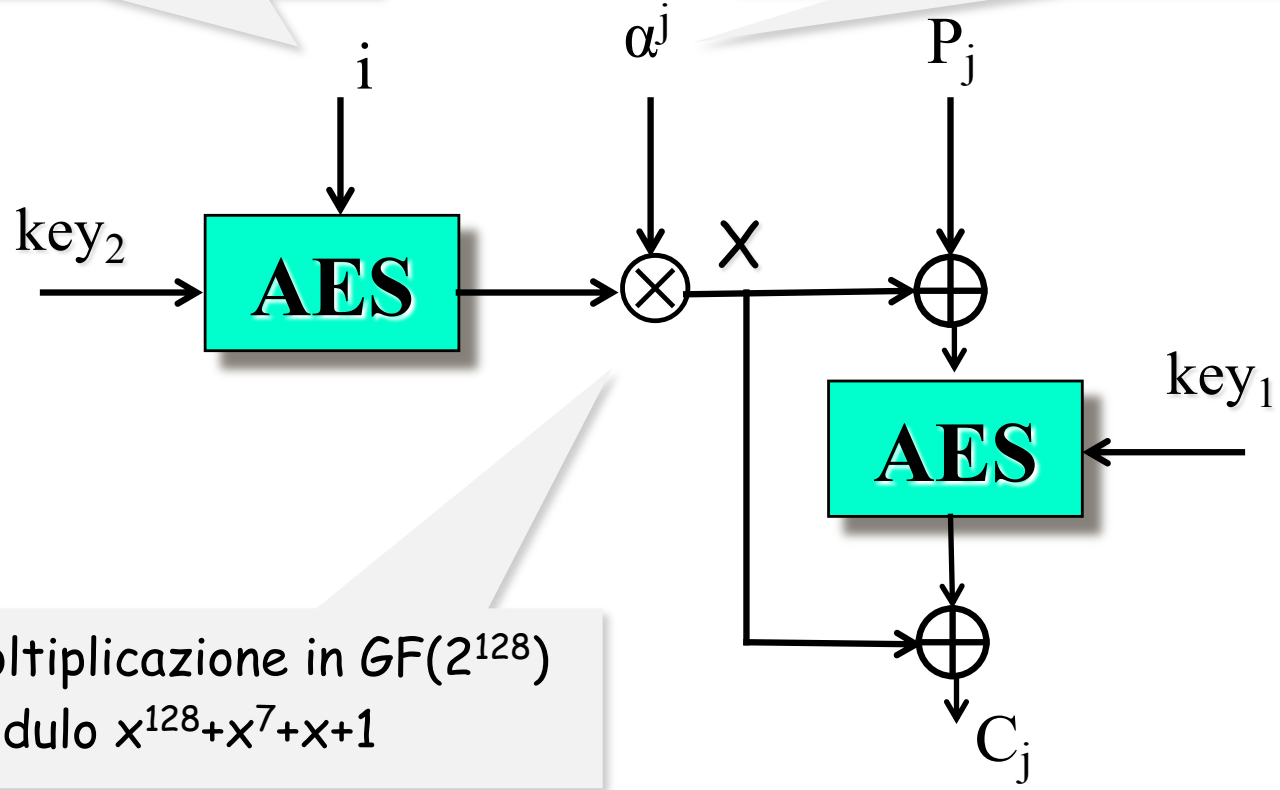
$$C_j = AES_{key_1}(P_j \oplus X) \oplus X$$

$$P_j = AES^{-1}_{key_1}(C_j \oplus X) \oplus X$$

XTS-AES
cifratura blocco

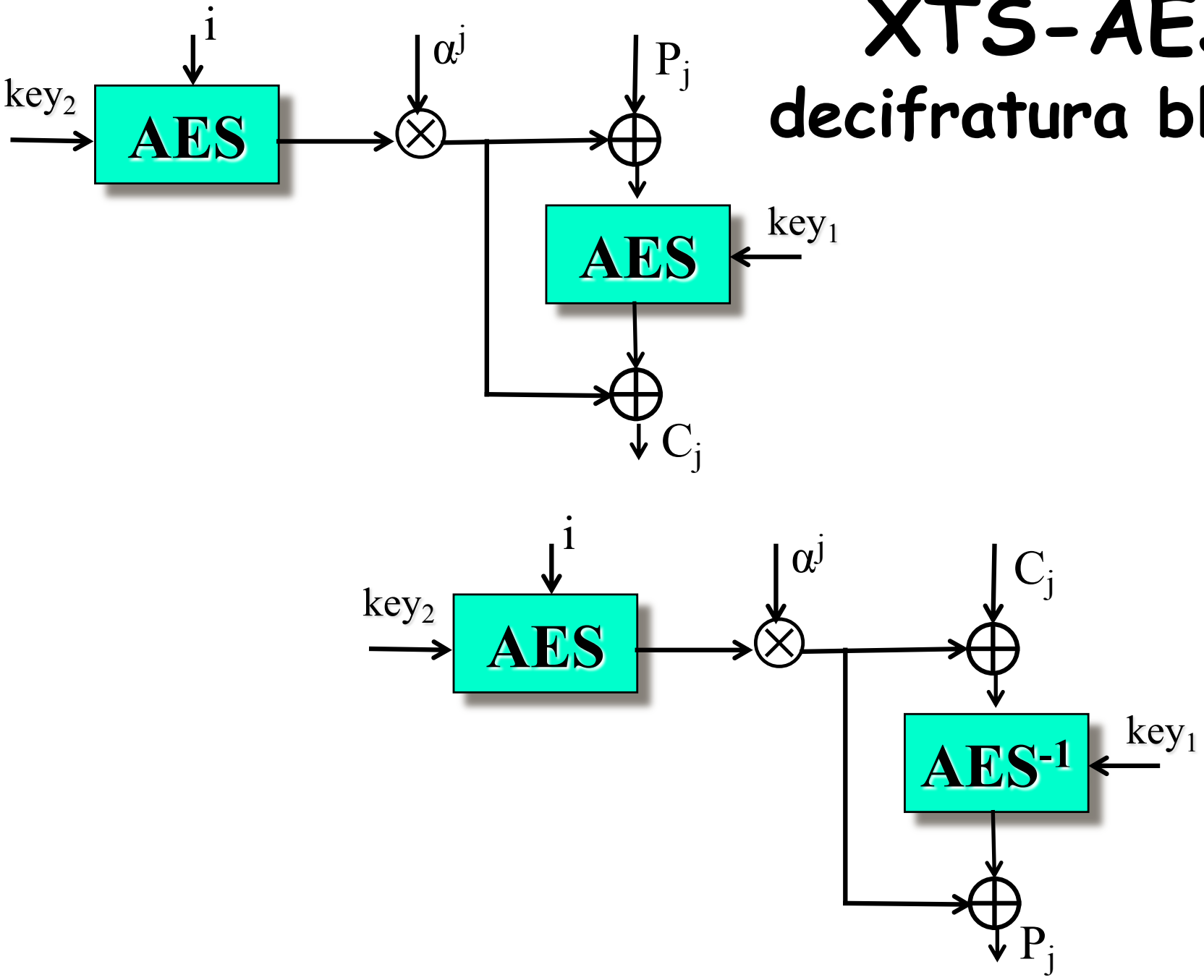
Valore tweak di 128 bit
Sono assegnati ai settori

Elemento primitivo $\alpha=0^{126}10$
Esponenziazione in $GF(2^{128})$



Moltiplicazione in $GF(2^{128})$
modulo $x^{128}+x^7+x+1$

XTS-AES
decifratura blocco

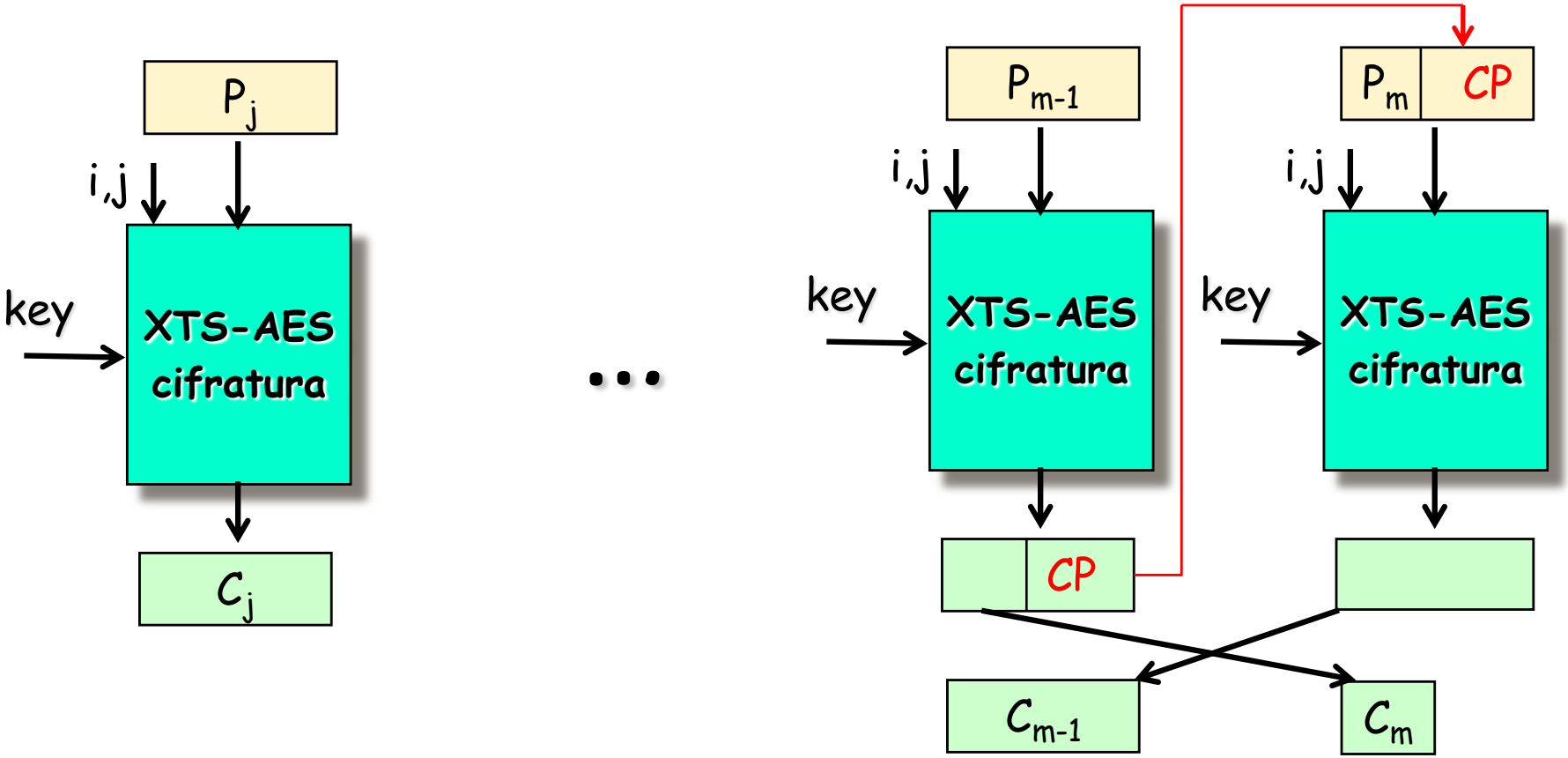


Ciphertext Stealing

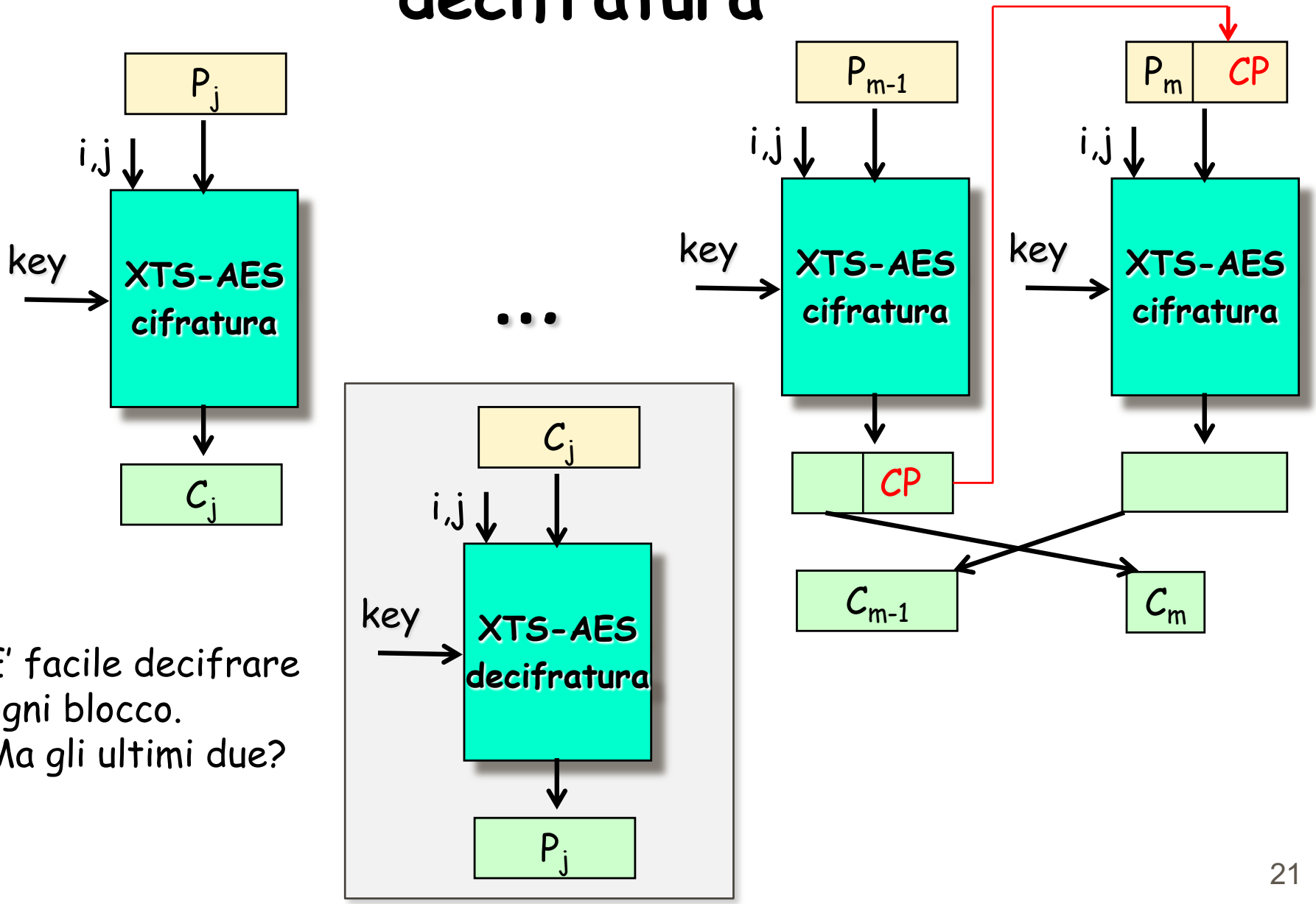
Se ultimo blocco è lungo 1,2,… oppure 127 bit

- Possiamo usare padding
  - Testo cifrato più lungo del testo in chiaro
- Ciphertext Stealing
  - Testo cifrato grande come testo in chiaro

Ciphertext Stealing

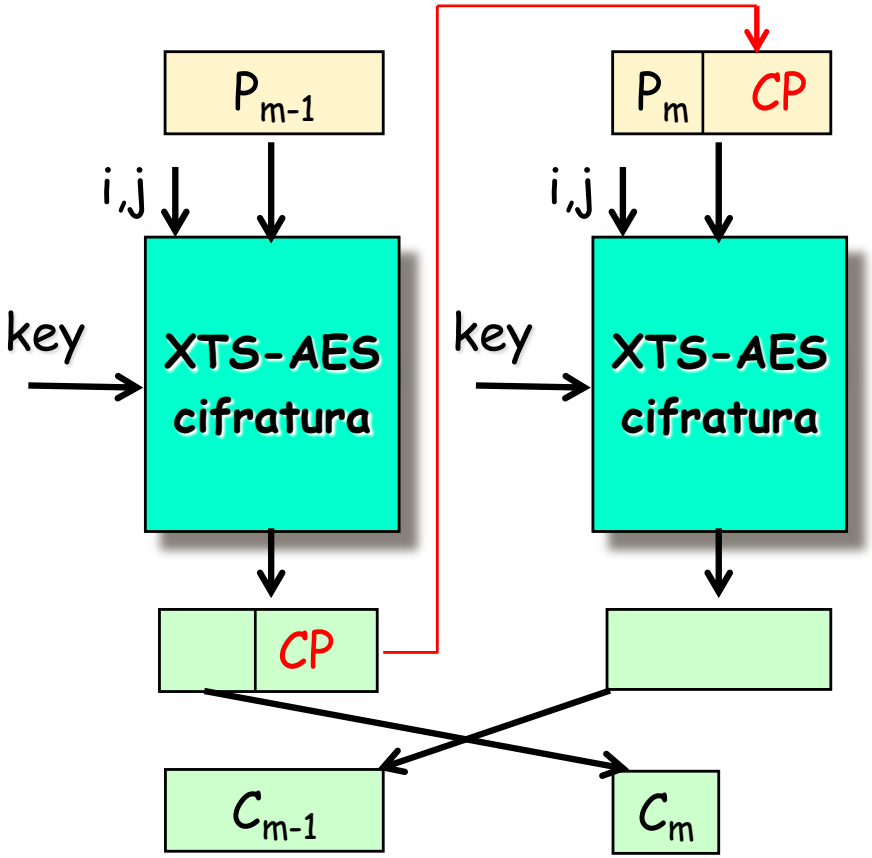


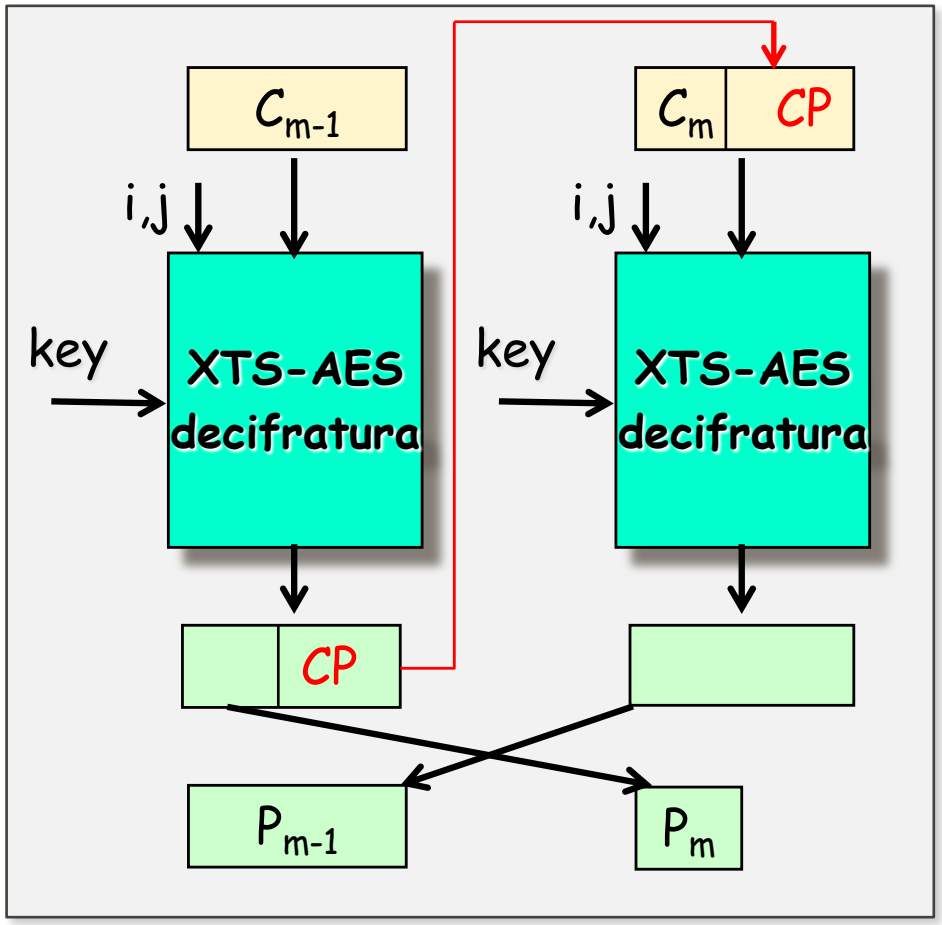
Ciphertext Stealing
decifratura



- E' facile decifrare ogni blocco.
- Ma gli ultimi due?

Ciphertext Stealing
decifratura





XTS-AES

Si può usare anche una sola chiave

- e non key_1 e key_2

XTS-AES

Implementato in

- **Software**
  - BestCrypt, dm-crypt, FreeOTFE, TrueCrypt, DiskCryptor, FreeBSD e OpenBSD
  - Nativo in Mac OS X Lion (nel FileVault)
  - BitLocker di Windows 10
- **Hardware**
  - SPYRUS Hydra PC Digital Attaché
  - Kingston DataTraveler 5000

'Debolezza' XTS

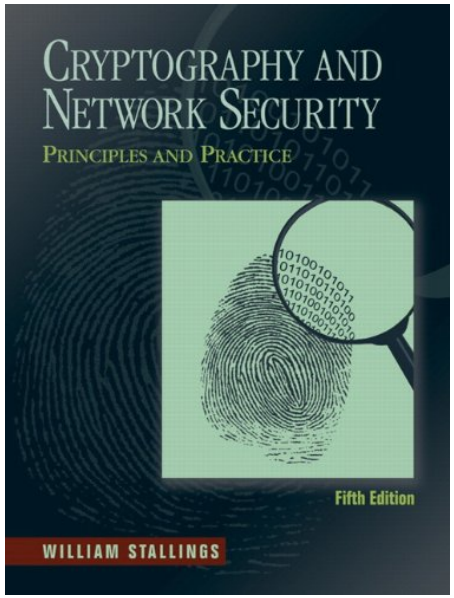
Non fornisce autenticazione,
ma solo confidenzialità

Bibliografia

- Cryptography and Network Security

  by W. Stallings, 2010

  - cap. 6 par. 6.7 "XTS-Aes Mode for Block-Oriented Storage Devices"



Domande?