Tweakable Encryption

Hyoungshick Kim

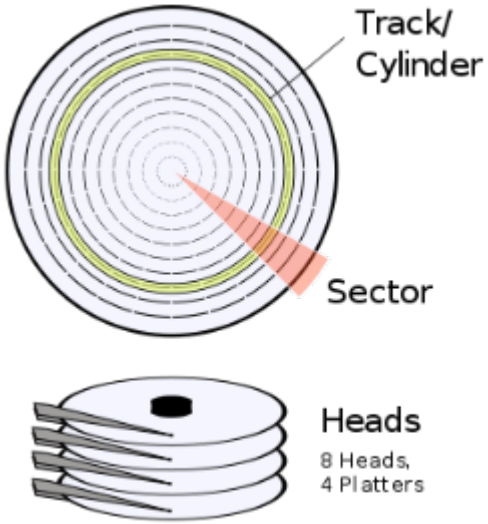
Department of Software

College of Software

Sungkyunkwan University

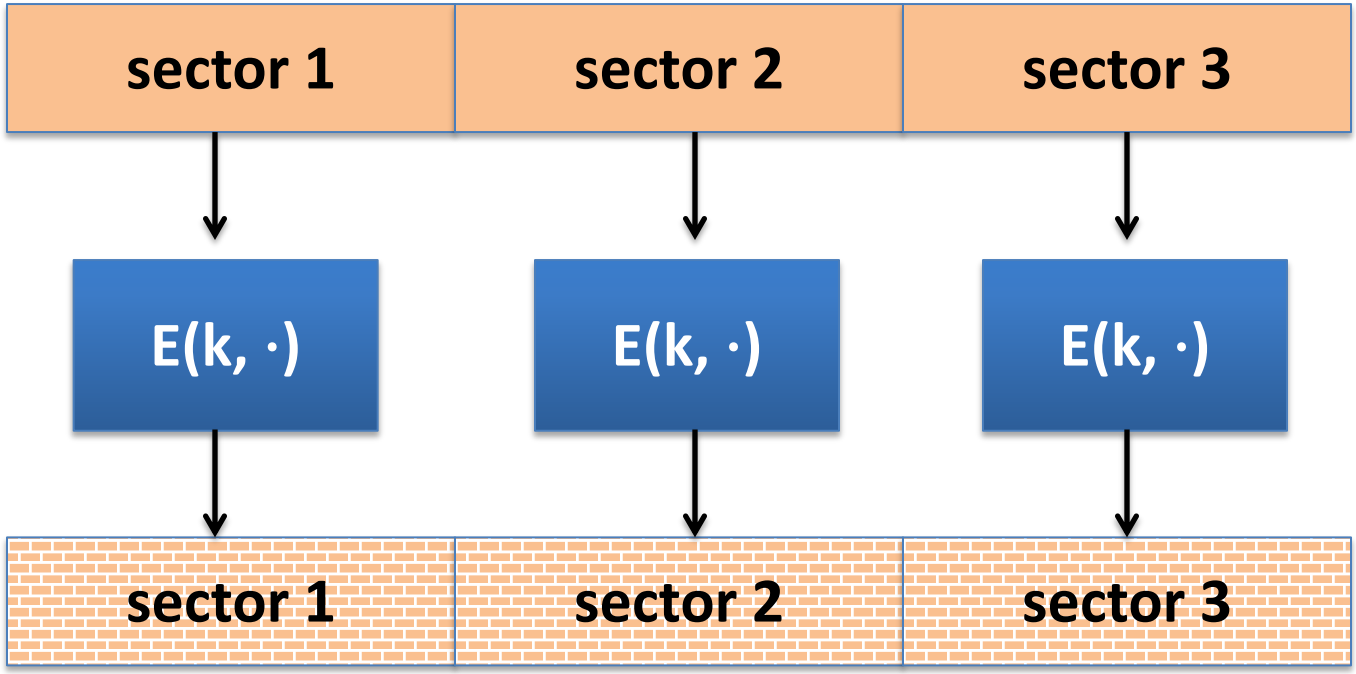
Disk encryption: no expansion

Used for encrypting *fixed*-length data units.



For example, sectors on disk are fixed size (e.g. 4KB).

Disclosure of same information



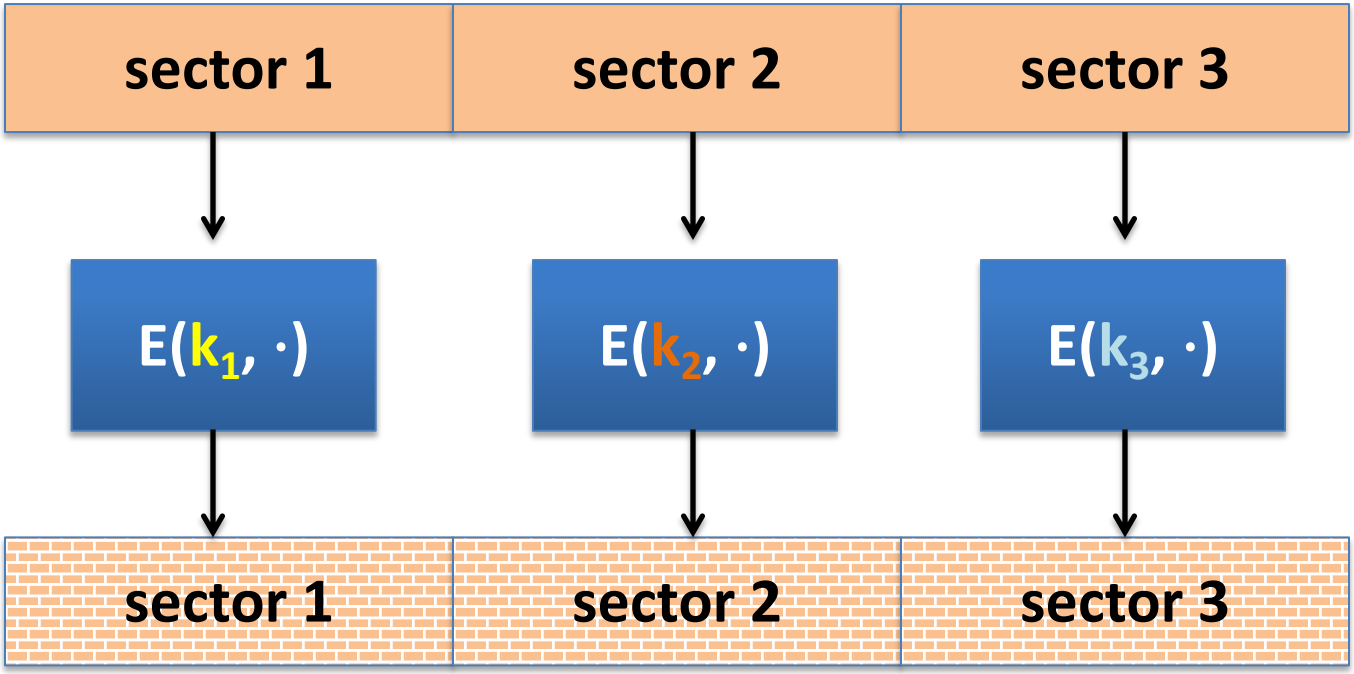
Sector 1 and sector 3 may have same content

- Leaks same information as ECB mode
- E.g., finding empty section on your disk

Limitation of existing modes

- Secure CBC can be implemented with random IVs, but the device offers no place to store them explicitly
- Sector numbers can be used as IVs. But then the IVs are predictable; attackers can generate plaintexts that cancel them out for CBC and CTR

Avoiding the leakage problem



Q. How can we manage (generate and store) individual keys?

$k_t = F(k, t)$, t=1,2,3…

Tweakable block ciphers

Goal: construct **many** different encryptions (based on location of disk where ciphertext file is to be stored) from a key $k \in K$.

Syntax: $\mathbf{E, D: K \times T \times X \longrightarrow X}$

for every $t \in T$ and $k \leftarrow\!\!- K$:

$E(k, t, \cdot)$ is an invertible function on X, indistinguishable from random

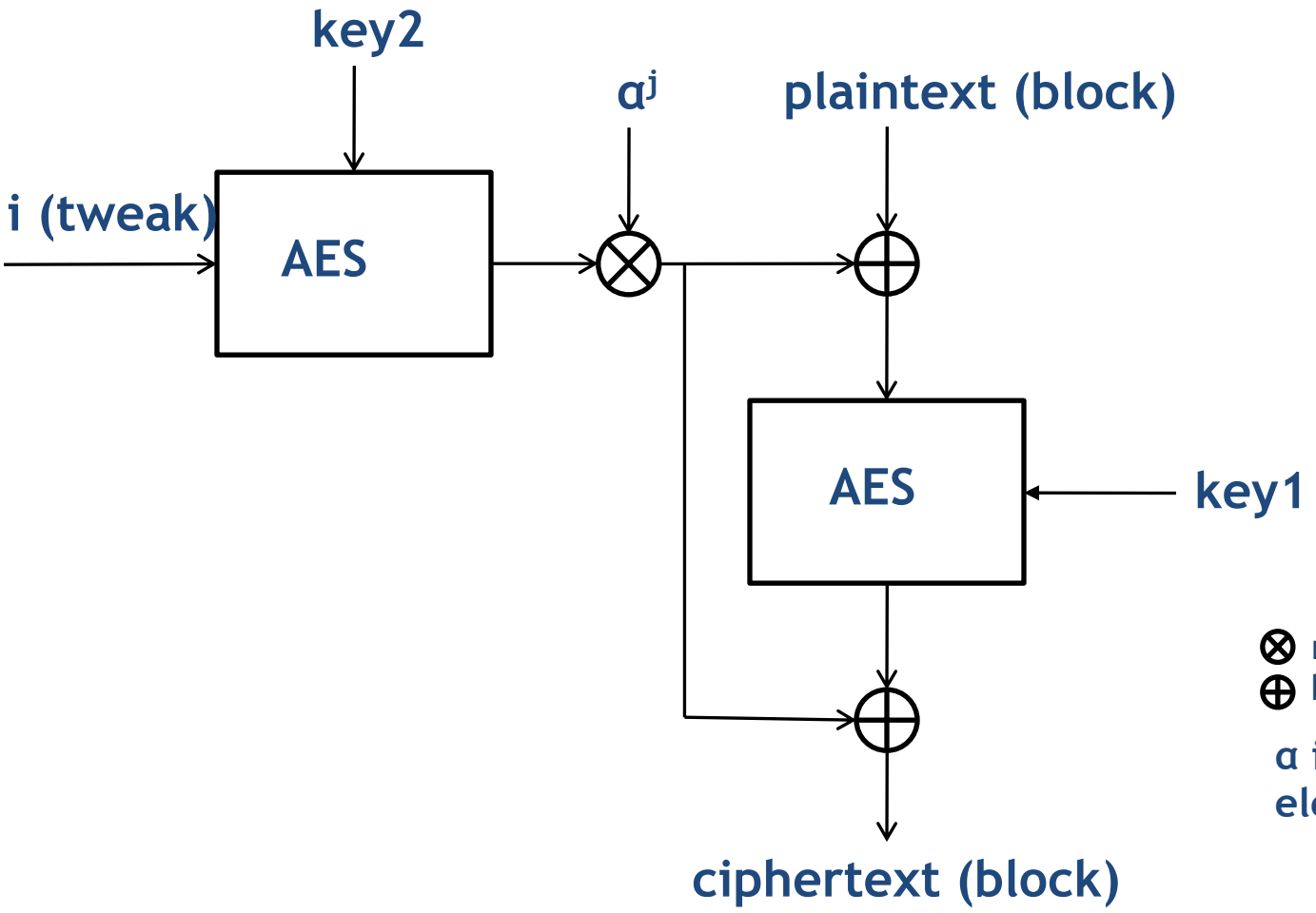
Idea: use a sector number as the tweak

$\Rightarrow$ every sector gets its own independent encryption

AES-XTS mode

- Encryption of block *j* is a function of:
  - 128 bit keys K_1 and K_2
  - "Tweak" value *i* (i.e., sector number)
    - Each sector assigned different tweak value consecutively (like counter in CTR mode)
  - Multiplier α^j
    - α = 000…00010 (that is, α in GF(2^{128}))
    - $\alpha^j = \alpha$ multiplied by itself *j* times mod $x^{128}+x^7+x^2+x+1$
    - Different for each block *j* in sector *i*

AES-XTS mode



⊗ modular multiplication
⊕ bitwise XOR

α is a primitive element of $GF(2^{128})$

i: sector number, j: j_{th} block

Questions?


Sungkyunkwan
Campus
Social
Graduate
Professors
English
Confucian
campus
Zone
Sciences
University
Global
Education
Seoul
Natural
Suwon
Korean
School
university
established
edit
also
Humanities
Science
schools
Administration
ASLE-Korea
Academic
Advanced
constructed
Building
Engineering
located
Joseon
Anniversary
Institute
now
two
Hall
Course
lecturers