Online Cryptography Course Dan Boneh

Odds and ends

Tweakable encryption

Disk encryption: no expansion

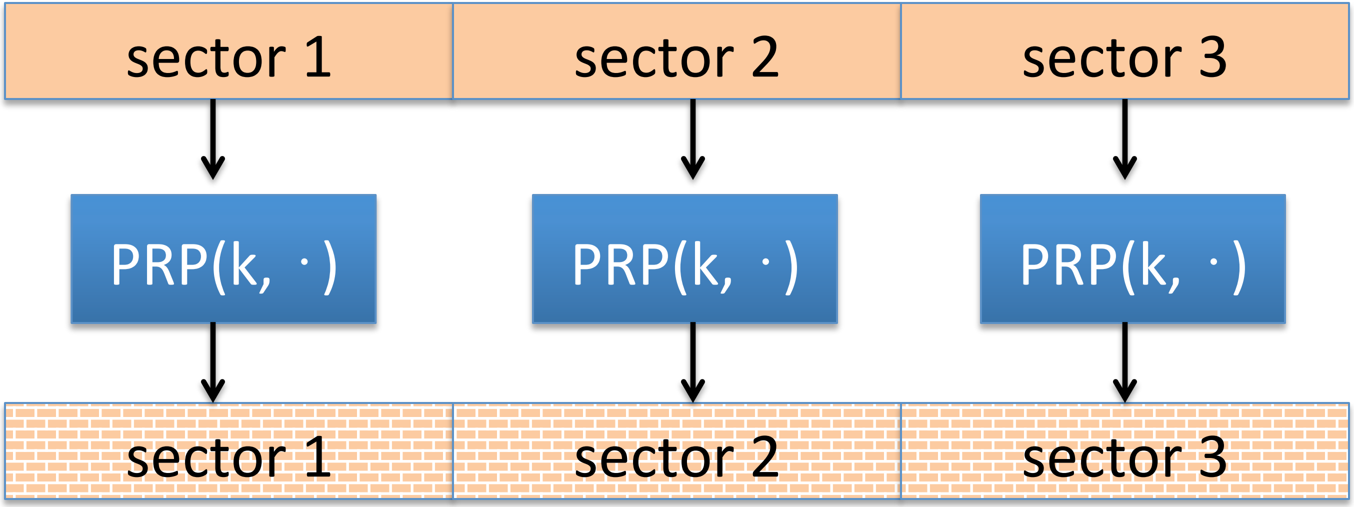
Sectors on disk are fixed size (e.g. 4KB)

⇒ encryption cannot expand plaintext (i.e. M = C)

⇒ must use deterministic encryption, no integrity

Lemma: if (E, D) is a det. CPA secure cipher with M=C then (E, D) is a PRP.

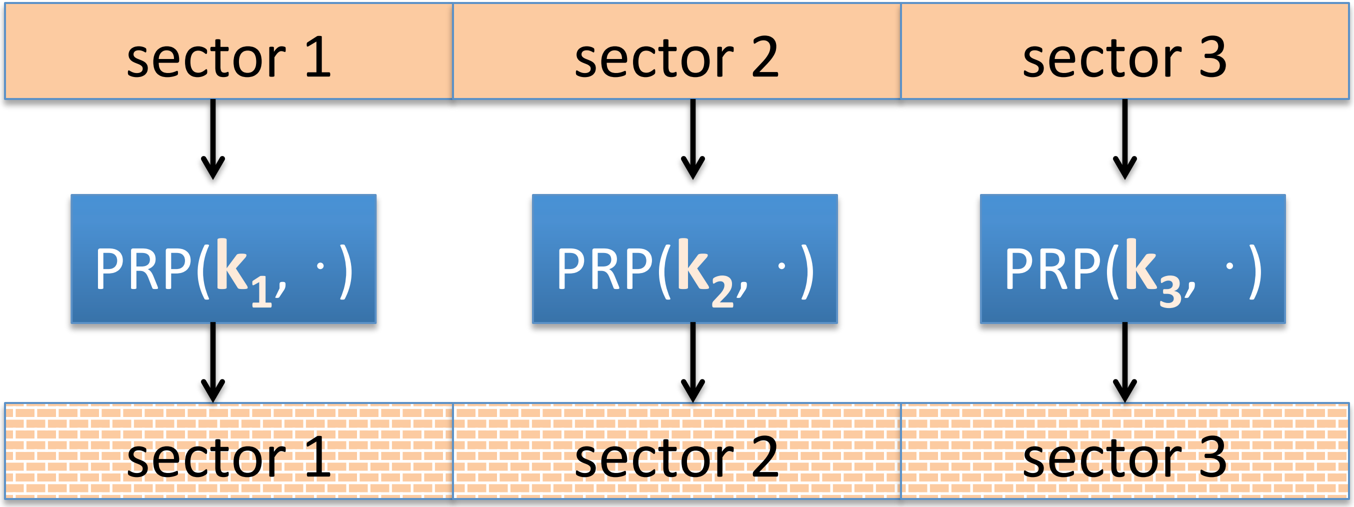
⇒ every sector will need to be encrypted with a PRP



Problem: sector 1 and sector 3 may have same content

- Leaks same information as ECB mode

Can we do better?



Avoids previous leakage problem

- … but attacker can tell if a sector is changed and then reverted

Managing keys: the trivial construction **k_t = PRF(k, t)** , t=1,…,L

Can we do better?

Tweakable block ciphers

Goal: construct **many** PRPs from a key $k \in K$.

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

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

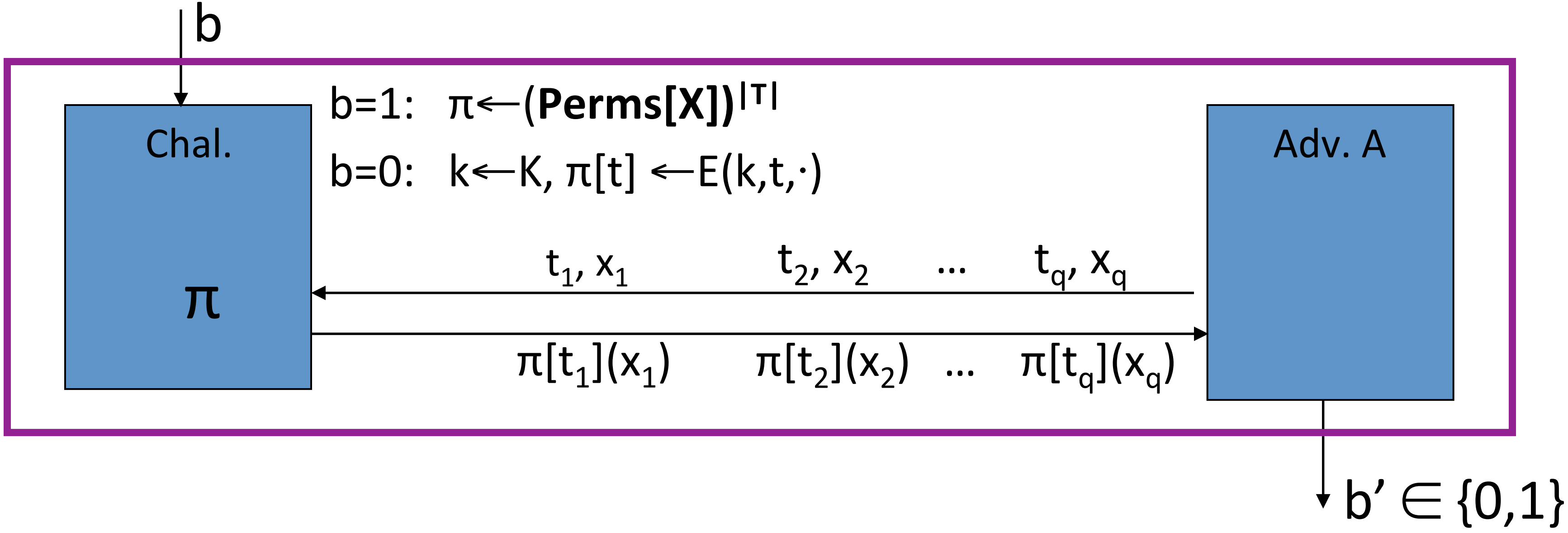
$\mathbf{E(k, t, \cdot)}$ is an invertible func. on X, indist. from random

Application: use sector number as the tweak

⇒ every sector gets its own independent PRP

Secure **tweakable** block ciphers

$E, D: K \times T \times X \longrightarrow X$. For b=0,1 define experiment EXP(b) as:



b

Chal.

π

b=1: $\pi \leftarrow (\mathbf{Perms[X]})^{|T|}$

b=0: $k \leftarrow K$, $\pi[t] \leftarrow E(k,t,\cdot)$

t_1, x_1 t_2, x_2 … t_q, x_q

$\pi[t_1](x_1)$ $\pi[t_2](x_2)$ … $\pi[t_q](x_q)$

Adv. A

$b' \in \{0,1\}$

- Def: E is a secure tweakable PRP if for all efficient A:

$$\mathrm{Adv}_{\mathrm{tPRP}}[A,E] = \Big|\Pr[\mathrm{EXP}(0)=1] - \Pr[\mathrm{EXP}(1)=1]\Big|$$ is negligible.

Example 1: the trivial construction

Let (E,D) be a secure PRP, E: $K \times X \longrightarrow X$.

- The trivial tweakable construction: (suppose K = X)

$$E_{tweak}(k, t, x) = E\big(E(k, t), \; x\big)$$

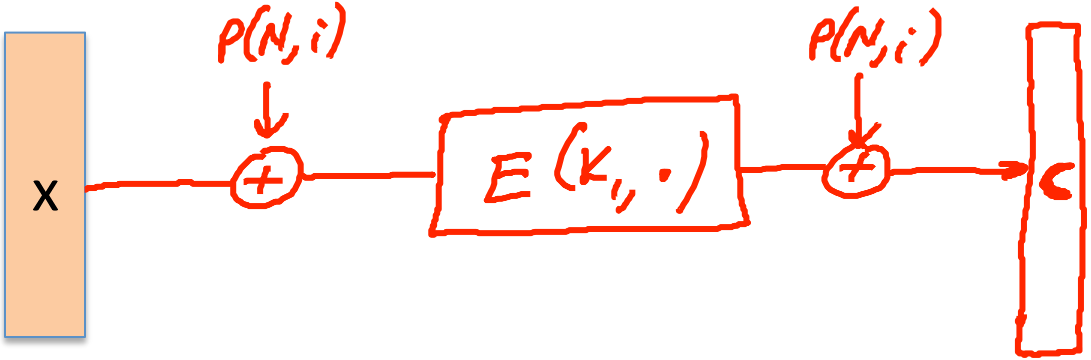
$\Rightarrow$ to encrypt n blocks need 2n evals of E(.,.)

2. the XTS tweakable block cipher [R'04]

Let (E,D) be a secure PRP, E: $K \times \{0,1\}^n \longrightarrow \{0,1\}^n$.

- XTS: $E_{tweak}\Big(\ (k_1,k_2),\ (t,i),\ x\Big) =$

$N \longleftarrow E(k_2,\ t)$

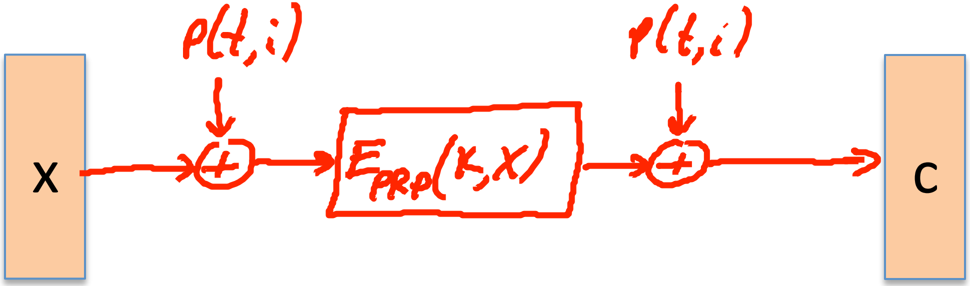


⇒ to encrypt n blocks need n+1 evals of E(.,.)

Is it necessary to encrypt the tweak before using it?

That is, is the following a secure tweakable PRP?

$E(k, (t,i), x)$:



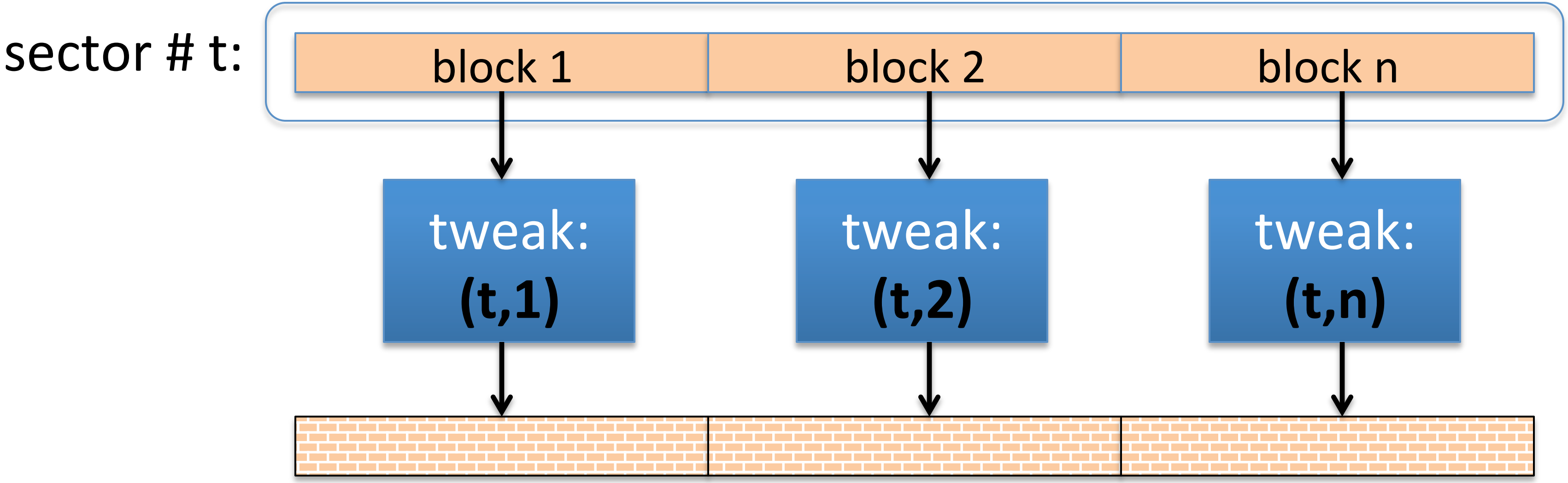
○ Yes, it is secure

○ No: $E\big(k, (t,1), P(t,2)\big) \oplus E\big(k, (t,2), P(t,1)\big) = P(t,1) \oplus P(t,2)$

○ No: $E\big(k, (t,1), P(t,1)\big) \oplus E\big(k, (t,2), P(t,2)\big) = P(t,1) \oplus P(t,2)$

○ No: $E\big(k, (t,1), P(t,1)\big) \oplus E\big(k, (t,2), P(t,2)\big) = 0$

Disk encryption using XTS



- note: block-level PRP, not sector-level PRP.
- Popular in disk encryption products:

Mac OS X-Lion, TrueCrypt, BestCrypt, …

Summary

- Use tweakable encryption when you need many independent PRPs from one key

- XTS is more efficient than the trivial construction
  - Both are narrow block: 16 bytes for AES

- EME (previous segment) is a tweakable mode for wide block
  - 2x slower than XTS

End of Segment