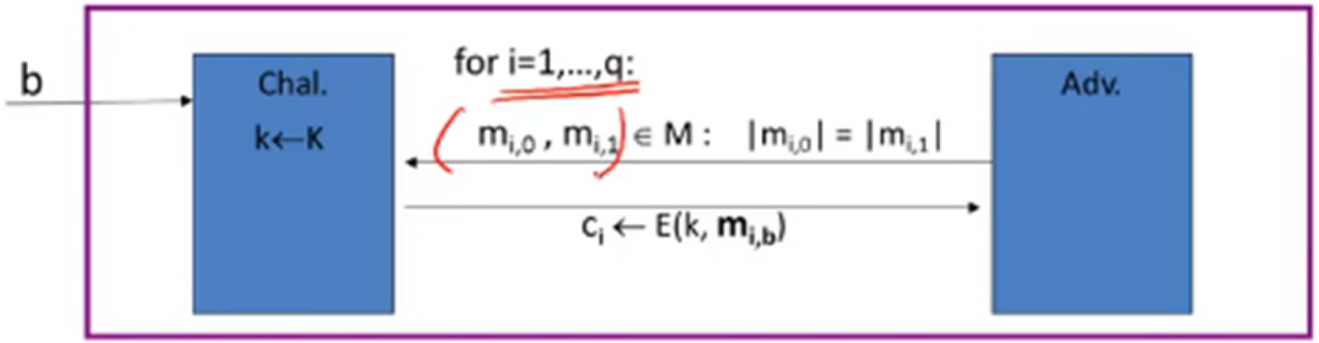
Use Block Ciphers 2:
Many time key

仇渝淇

Semantic Security for many-time key

$E = (E,D)$ a cipher defined over (K,M,C). For $b=0,1$ define EXP(b) as:



Semantic Security for many-time key

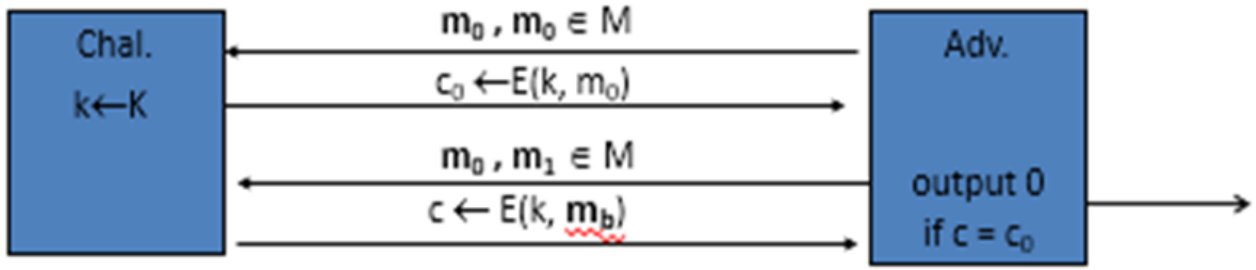
if adv. wants $c = E(k, m)$ it queries with $m_{j,0} = m_{j,1} = m$

Def: E is sem. sec. under CPA if for all "efficient" A:

$Adv_{CPA}[A,E] = |Pr[EXP(0)=1] - Pr[EXP(1)=1]|$

is "negligible."

Ciphers insecure under CPA



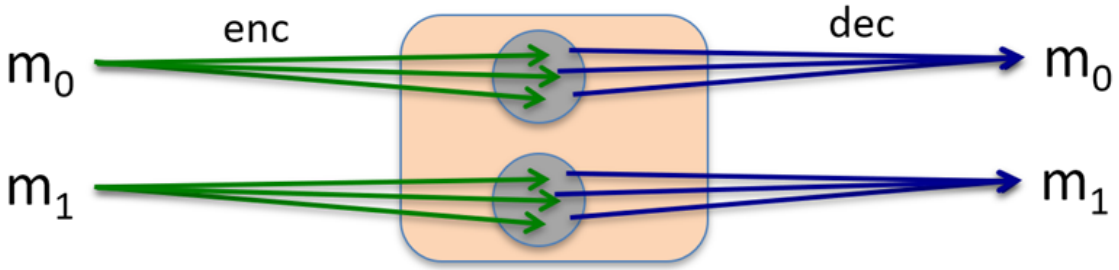
假设E(k,m)总是为msg m输出相同的密文，则:

攻击者可以知道两个加密的文件是相同的，两个加密的包是相同的，等等。

如果密钥是多次使用的→
对于相同的明文消息两次，加密必须
产生不同的输出。

Solution 1: randomized encryption

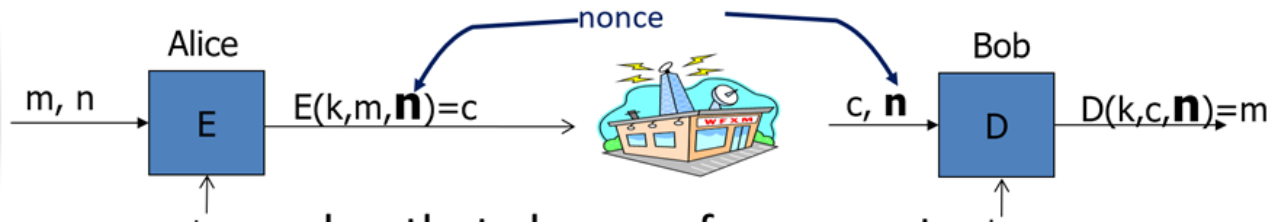
E(k,m)为随机化算法:



对同一消息加密两次得到不同的密文 (w.h.p) ⇒ 密文必须比明文长

Roughly speaking: CT-size = PT-size + "# random bits"

Solution 2: nonce-based Encryption



nonce n: a value that changes from msg to msg.

method 1: nonce is a **counter** (e.g. packet counter)

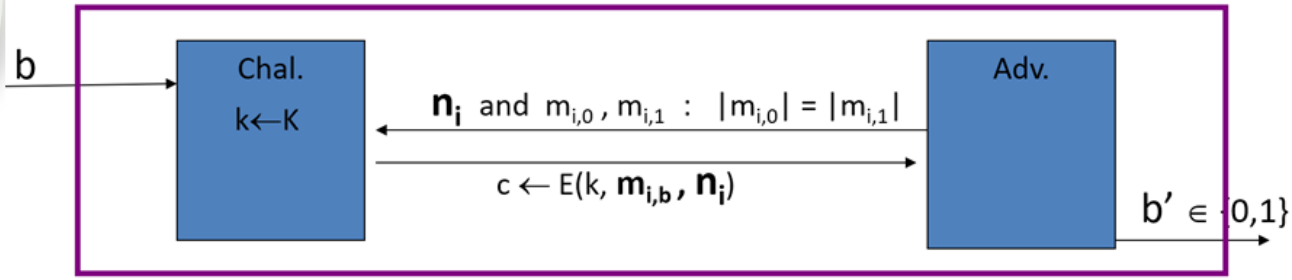
-当加密器保持状态从msg到msg时使用

-如果解密器具有相同的状态，则无需将nonce与CT一起发送

method 2: encryptor chooses a **random nonce** $n \leftarrow \mathcal{N}$

CPA security for nonce-based encryption

System should be secure when nonces are chosen adversarially.



Def: nonce-based $\mathbb{E}$ is sem. sec. under CPA if for all "efficient" A:

$Adv_{nCPA}[A,\mathbb{E}] = |Pr[EXP(0)=1] - Pr[EXP(1)=1]|$ is "negligible."

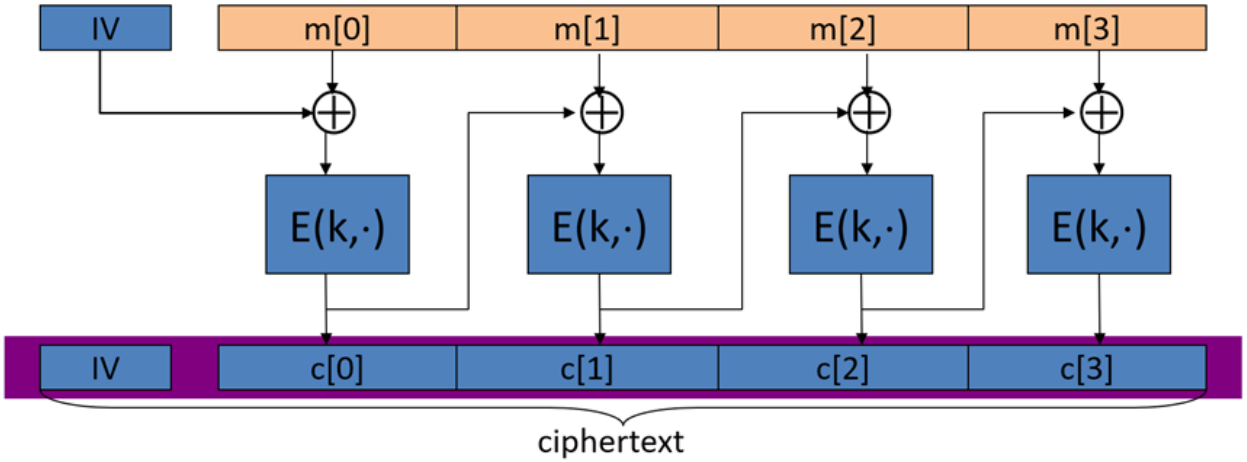
Use Block Ciphers :

Modes of operation:
many time key (CBC)
Cipher Block Chaining
密码分组链接模式

仇渝淇

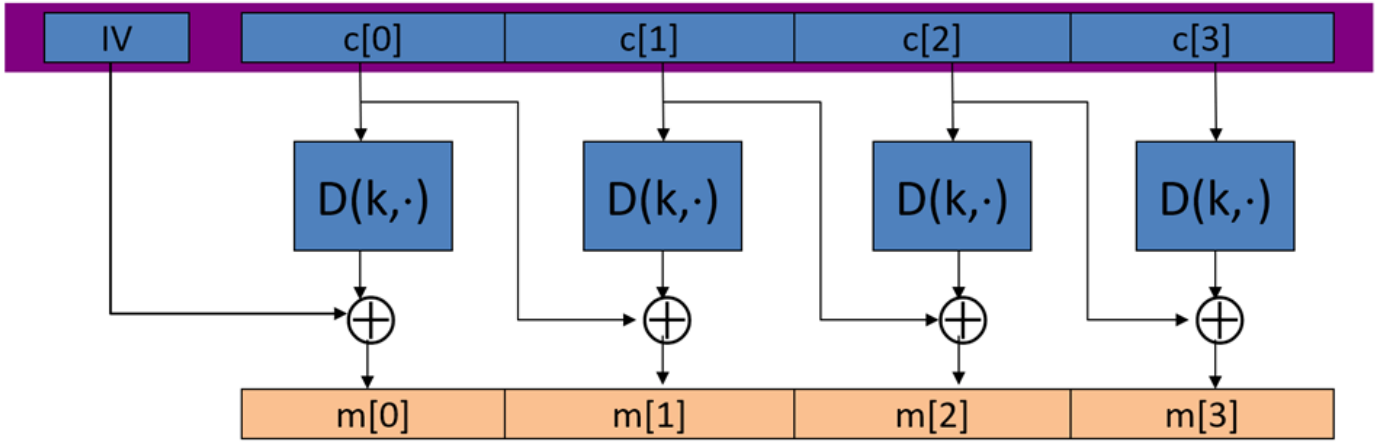
Construction 1: CBC with random IV

Let (E,D) be a PRP. $E_{CBC}(k,m)$: choose **random** IV∈X and do:



Decryption circuit

In symbols: $c[0] = E(k, IV \oplus m[0])$ $\Rightarrow$ $m[0] = D(k, c[0]) \oplus IV$



CBC: CPA Analysis

CBC定理:

对于任意L>0，如果E是(K,X)上的安全PRP，则E_{CBC}为 (K, XL, XL+1)上的加密算法

特别地，假设有一个攻击者A进行了选择明文的Q次询问，存在一个攻击分组密码PRP的攻击者B以下关系成立：

$$Adv_{CPA}[A, E_{CBC}] \leq 2 \cdot Adv_{PRP}[B, E] + 2q^2L^2 / |X|$$

Note: CBC is only secure as long as $q^2L^2 << |X|$

An example

$$Adv_{CPA}[A, E_{CBC}] \leq 2 \cdot Adv_{PRP}[B, E] + 2\,q^2\,L^2 / |X|$$

q = 密文数，L =明文长度

假设我们想要

$Adv_{CPA}[A, E_{CBC}] \leq 1/2^{32}$ $\Leftarrow$ $q^2\,L^2/|X| < 1/2^{32}$

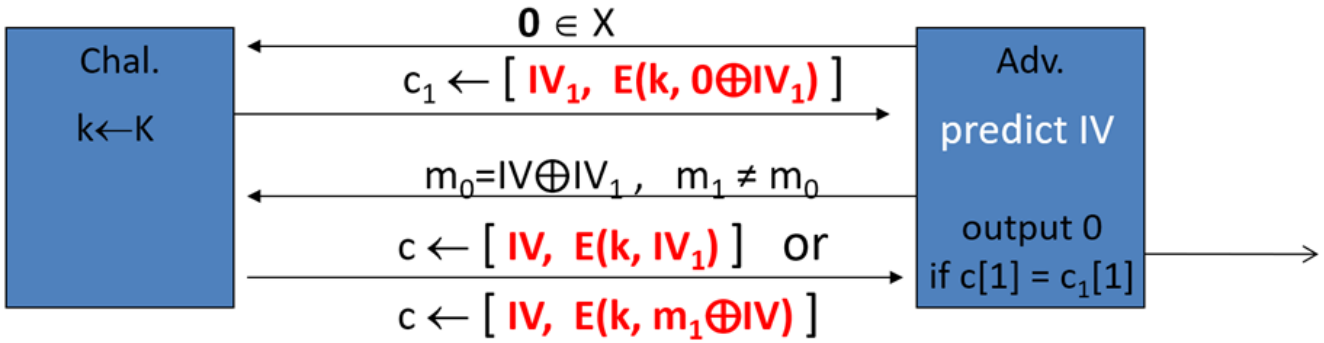
AES: $|X| = 2^{128}$ $\Rightarrow$ $q\,L < 2^{48}$

所以，在2^{48}个AES块之后，必须更改密钥

Warning: an attack on CBC with rand. IV

CBC where attacker can predict the IV is not CPA-secure !!

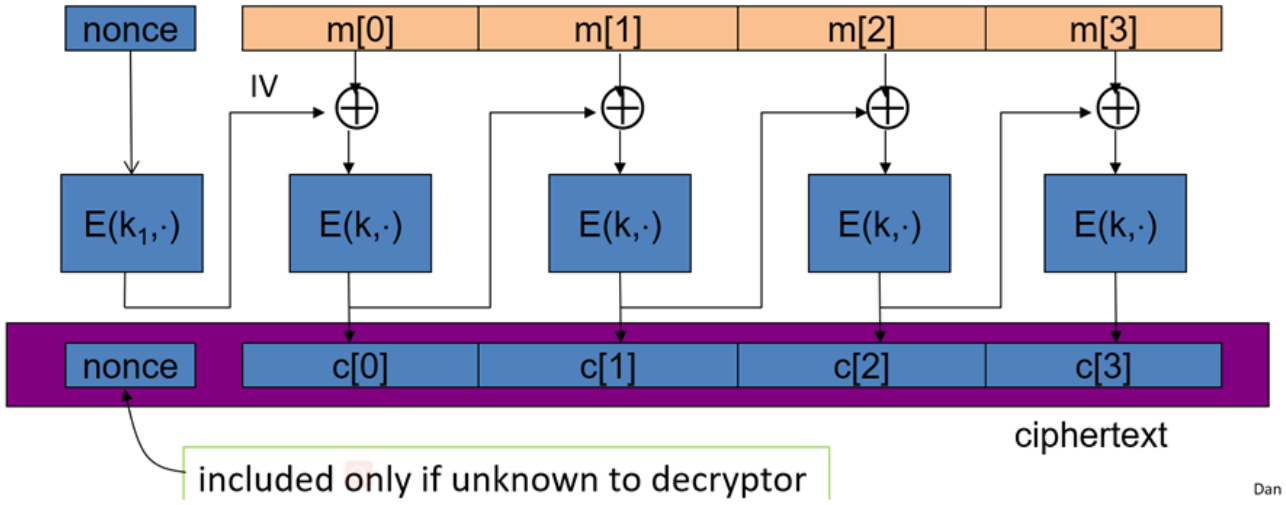
Suppose given $c \leftarrow E_{CBC}(k,m)$ can predict IV for next message



Construction 1’: nonce-based CBC

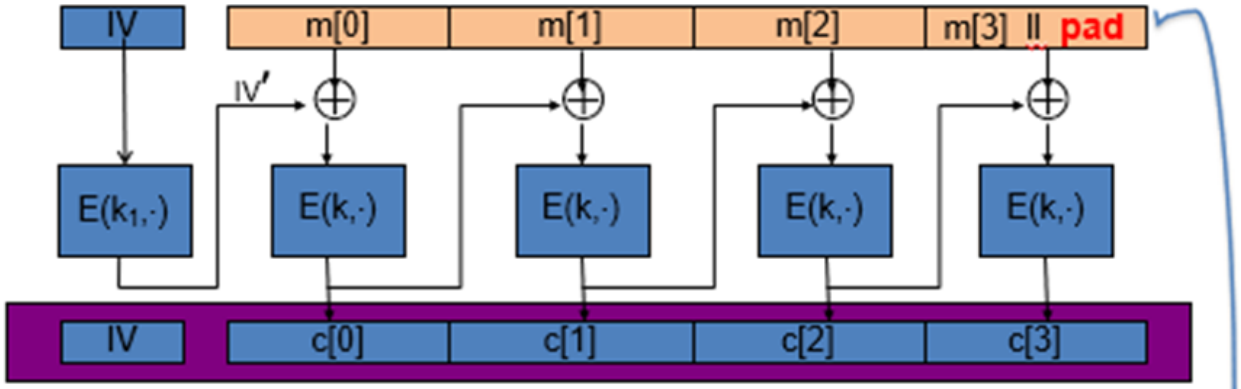
具有唯一nonce的密码块链接:key = (k,k1)

唯一的nonce表示:(key, n)对只用于一条消息



Dan Boneh

A CBC technicality: padding



TLS: for n>0, n byte pad is | n | n | n | ··· | n |

if no pad needed, add a dummy block

Use Block Ciphers :

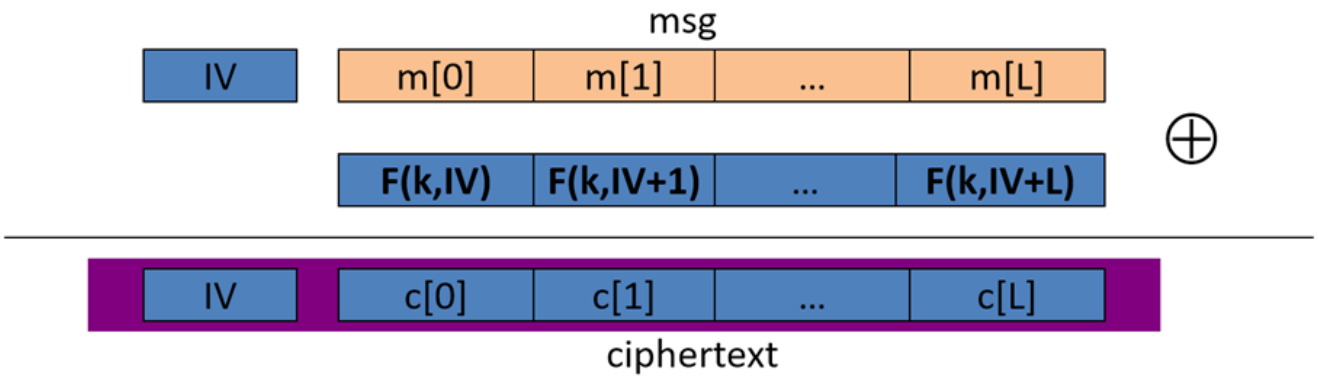
Modes of operation:
many time key (CTR)
Randomized Counter Mode
随机计数器模式

仇渝淇

Construction 2: rand ctr-mode

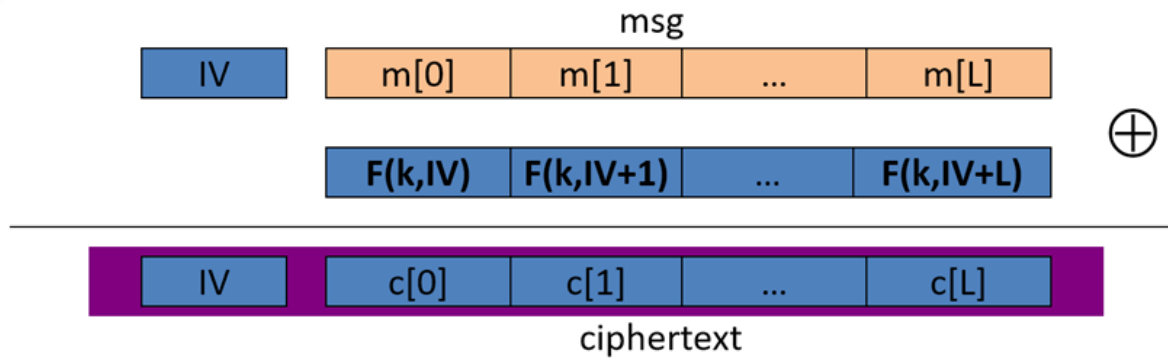
Let $F: K \times \{0,1\}^n \longrightarrow \{0,1\}^n$ be a secure PRF.

E(k,m): choose a random $IV \in \{0,1\}^n$ and do:

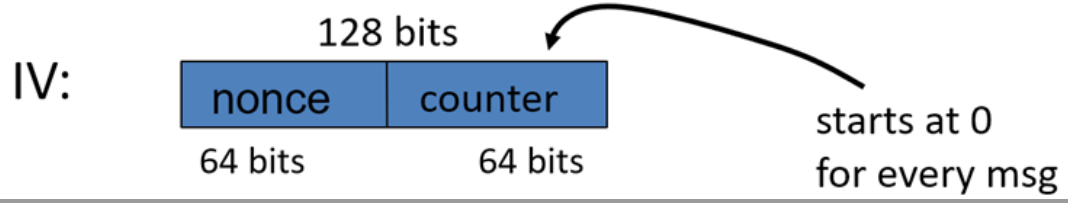


note: parallelizable (unlike CBC)

Construction 2’: nonce ctr-mode



为确保F(k,x)不使用超过一次，选择IV为:



rand ctr-mode (rand. IV): CPA analysis

$$Adv_{CPA}[A, E_{CTR}] \le 2 \cdot Adv_{PRF}[B, E] + \mathbf{2\, q^2\, L\, /\, |X|}$$

q = # messages encrypted with k , L = length of max message

Suppose we want $Adv_{CPA}[A, E_{CTR}] \le 1/2^{32}$ $\Leftarrow$ $q^2 L / |X| < 1/ 2^{32}$

- AES: $|X| = 2^{128} \Rightarrow q L^{1/2} < 2^{48}$

  So, after 2^{32} CTs each of len 2^{32}, must change key

  (total of 2^{64} AES blocks)

Comparison: ctr vs. CBC

	CBC	ctr mode
uses	PRP	PRF
parallel processing	No	Yes
Security of rand. enc.	q^2 L^2 << |X|	q^2 L << |X|
dummy padding block	Yes	No
1 byte msgs (nonce-based)	16x expansion	no expansion

(对于CBC，可以通过窃取密文来解决虚拟填充块)

Summary

- PRPs和PRFs:块密码的有用抽象。
- 研究了两个安全概念:(防止窃听的安全，不提供对篡改密文的安全)

  1.semantic security against one-time CPA

  2. semantic security against many-time CPA

  这两种模式都不能确保数据完整性。
- 安全结果总结如下表:

Goal \ Power	one-time key	Many-time key (CPA)	CPA and integrity
Sem. Sec.	steam-ciphers det. ctr-mode	rand CBC rand ctr-mode	later