Practical Cryptography:
Provable Security as a Tool for Protocol Design

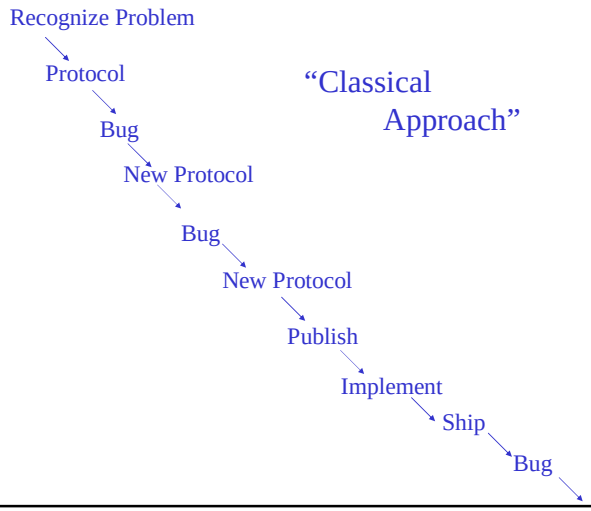
Phillip Rogaway
UC Davis & Chiang Mai Univ
rogaway@cs.ucdavis.edu
http://www.cs.ucdavis.edu/~rogaway

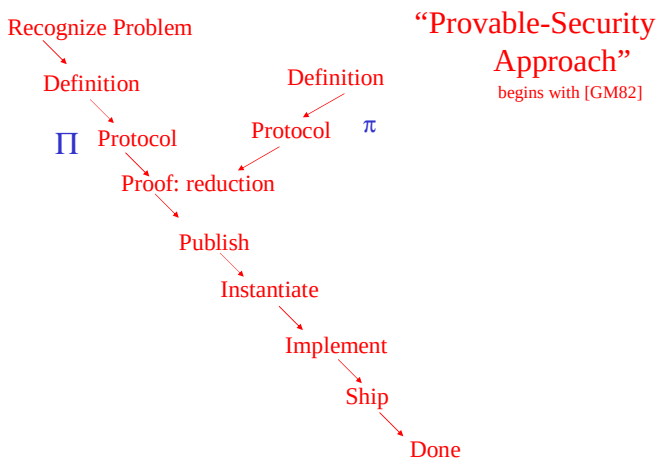
Summer School on Foundations of Internet Security
17-19 June 2002
Duszniki Zdroj, Poland
(three two-hour lectures)

Slides modified and tweaked by Dan Wallach, with permission

Outline from the paper board

0. Opening comments
1. What is "provably security"?
2. Blocks ciphers
   2.1 Syntax
   2.2 Notions of security (prp, prf, kr)
3. Symmetric Encryption
   3.1 Syntax
   3.2 Notions of security (sem, ind, ind$, all under CPA)
4. Relating the notions (ind$, ind, 01)
5. Sample block-cipher-using encryption schemes
6. Security of modes
   6.1 CTR-rand
   6.2 CBC-rand
7. MACs and authenticated encryption
   7.1 Notion of authenticated encryption
   7.2 Notion of MACs
   7.3 Ways to MAC (CBC, XCBC, CW (w/ poly-based universal hash, UMAC)
   7.4 Ways to achieve auth enc (generic composition, IAPM/OCB)
Concluding comments





Primitive π		Protocol Π
Block Cipher	→	Sym enc scheme
Block Cipher	→	MAC
Block Cipher	→	OWF
OWF	→	Block Cipher
Sym enc scheme + MAC	→	AKE
RSA primitive	→	Asym enc scheme

If primitive π is secure **then** protocol Π is secure
If $\nexists$ a good adv for attacking π **then** $\nexists$ no good adv for attacking Π
If $\nexists$ a good adv for attacking Π **then** $\nexists$ a good adv for attacking π

Block-Cipher Syntax

$E: \boldsymbol{K} \times \{0,1\}^n \rightarrow \{0,1\}^n$

where each $E_K(\cdot) = E(K, \cdot)$ is a permutation

Eg: $E_K(X)=X$
$E_K(X)=AES128_K(X)$

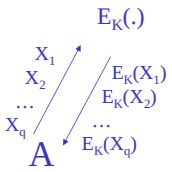
Notions of Block-Cipher Security

Key-recover (kr) under chosen-plaintext attack (CPA)

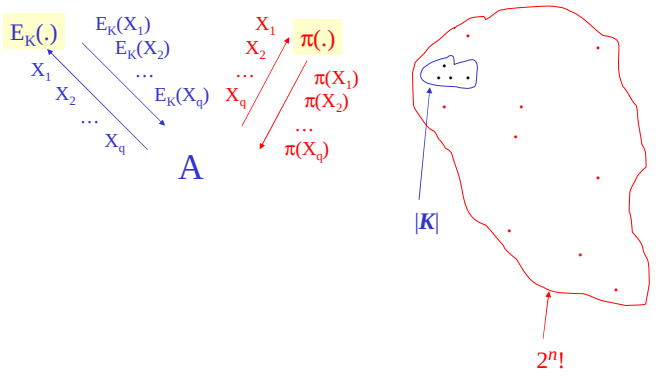
$$\mathrm{Adv}^{\mathrm{kr}}_{E}(A) = \Pr[\, K \xleftarrow{\$} \boldsymbol{K} : A^{E(K,\cdot)} = K]$$

$$\mathrm{Adv}^{\mathrm{kr}}_{E}(t,q) = \max_{A} \{\mathrm{Adv}^{\mathrm{kr}}_{E}(A)\}$$

Runs in time ≤ t
Asks ≤ q queries



PRP-sense of a block cipher being good



$\mathrm{Adv}^{\mathrm{prp}}_{E}(A) = \Pr[\, K \xleftarrow{\$} \boldsymbol{K} : A^{E(K,\cdot)} = 1] -$

$\Pr[\, \pi \xleftarrow{\$} \mathrm{Perm}(n) : A^{\pi(\cdot)} = 1]$

Attacker A responds:
0: it's a permutation
1: it's the cipher

$\mathrm{Adv}^{\mathrm{prp}}_{E}(t,q) = \max_{A} \{\mathrm{Adv}^{\mathrm{prp}}_{E}(A)\}$

Runs in time ≤ t
Asks ≤ q queries

Breaking $E_K(X)=X$

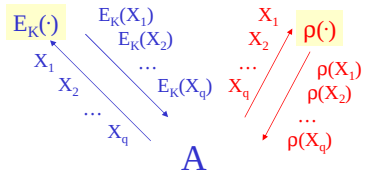
A: Ask 0^n, receiving Y
if $Y=0^n$ return 1 (cipher returns the identity)
else return 0
$\mathrm{Adv}^{\mathrm{prp}}_{E}(A) = 1 - 2^{-n}$ (permutation might also)

$\mathrm{Adv}^{\mathrm{prp}}_{\mathrm{AES}}(t,q) \le t / 2^{128}$ Strong assumption

$\mathrm{Adv}^{\mathrm{prp}}_{\mathrm{AES}}(t,q) \le 2^{-40}$ if $t<2^{80}$, $q<2^{40}$ Weaker assumption

$\mathrm{Adv}^{\mathrm{prf}}_{E}(A) = \Pr[\, K \xleftarrow{\$} \boldsymbol{K} : A^{E(K,\cdot)} = 1] -$

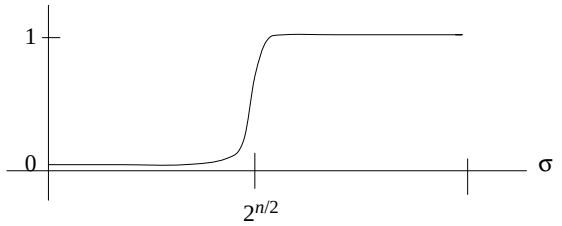
$\Pr[\, \rho \xleftarrow{\$} \mathrm{Rand}(n) : A^{\rho(\cdot)} = 1]$



$\mathrm{Adv}^{\mathrm{prf}}_{E}(A) = 2\Pr[\, b \xleftarrow{\$} \{0,1\};$
if b=1 then $K \xleftarrow{\$} \boldsymbol{K}$, $f = E_K$ else $f \xleftarrow{\$} \mathrm{Rand}(n)$: $A^{f(\cdot)} = b] - 1$

"Switching Lemma" If A asks σ queries

$|\mathrm{Adv}^{\mathrm{prp}}_{E}(A) - \mathrm{Adv}^{\mathrm{prf}}_{E}(A)| \le \sigma^2 / 2^{n+1}$



$\Pr[A^{\pi(\cdot)} = 1] - \Pr[A^{\rho(\cdot)} = 1] \le \sigma^2 / 2^{n+1}$

Def. A (sym, prob) enc scheme is a 3-tuple
$\Pi = (\boldsymbol{K}, \boldsymbol{E}, \boldsymbol{D})$

Finite set

$\boldsymbol{M} \subseteq \{0,1\}^*$

$\boldsymbol{E}: \boldsymbol{K} \times \boldsymbol{M} \to \{0,1\}^*$ is a prob. function

If $M \in \boldsymbol{M}$ and $|M'|=|M|$ then $M' \in \boldsymbol{M}$

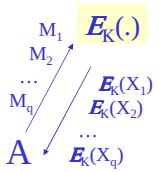
$\boldsymbol{D}: \boldsymbol{K} \times \{0,1\}^* \to \boldsymbol{M} \cup \{*\}$ (det funct)

$M \in \boldsymbol{M}$, $K \in \boldsymbol{K}$, $C \xleftarrow{\$} \boldsymbol{E}_K(M) \Rightarrow \boldsymbol{D}_K(C) = M$

$|C| = clen(|M|)$

13

CPA



support($\boldsymbol{M}$) only has strings of one length

$\Pi = (\boldsymbol{K},\boldsymbol{E},\boldsymbol{D})$

sem

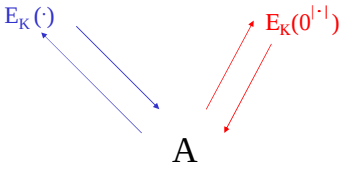
$$\mathrm{Adv}^{\mathrm{sem}}_{\Pi}(A) = \Pr[\, K \xleftarrow{\$} \boldsymbol{K};\ (f, \boldsymbol{M}) \xleftarrow{\$} A^{\boldsymbol{E}(K,\cdot)}();\ M \xleftarrow{\$} \boldsymbol{M};\ C \xleftarrow{\$} \boldsymbol{E}_K(M):$$
$$A^{\boldsymbol{E}(K,\cdot)}(C, f) = f(M)] -$$
$$\Pr[\, K \xleftarrow{\$} \boldsymbol{K};\ (f, \boldsymbol{M}) \xleftarrow{\$} A^{\boldsymbol{E}(K,\cdot)}();\ M, M' \xleftarrow{\$} \boldsymbol{M};\ C \xleftarrow{\$} \boldsymbol{E}_K(M'):$$
$$A^{\boldsymbol{E}(K,\cdot)}(C, f) = f(M)]$$

14

$\Pi = (\boldsymbol{K},\boldsymbol{E},\boldsymbol{D})$

ind

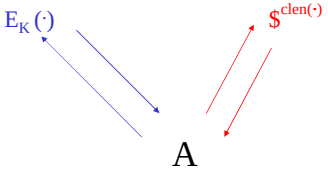
$$\mathrm{Adv}^{\mathrm{ind}}_{\Pi}(A) = \Pr[\, K \xleftarrow{\$} \boldsymbol{K}:\ A^{\boldsymbol{E}(K,\cdot)} = 1\,] -$$
$$\Pr[\, K \xleftarrow{\$} \boldsymbol{K}:\ A^{\boldsymbol{E}(K, 0^{|\cdot|})} = 1\,]$$



15

ind$

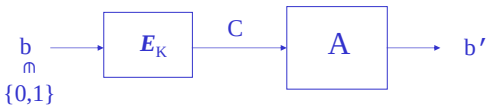
$$\mathrm{Adv}^{\mathrm{ind\$}}_{\Pi}(A) = \Pr[\, K \xleftarrow{\$} \boldsymbol{K}:\ A^{\boldsymbol{E}(K,\cdot)} = 1\,] -$$
$$\Pr[\, K \xleftarrow{\$} \boldsymbol{K}:\ A^{\boldsymbol{E}(K, \$^{clen(|\cdot|)})} = 1\,]$$



16

Lecture 2

Consider a weak form of semantic security: can't recover the key:



$$\mathrm{Adv}^{01}_{\Pi}(A) = 2\,\Pr[b \xleftarrow{\$} \{0,1\};\ K \xleftarrow{\$} \boldsymbol{K};\ C \xleftarrow{\$} E_K(b):\ A(C) = b] - 1$$

Assume A does well at breaking Π in the 01-sense.
Construct B that does well at breaking Π in the ind-sense.

Def of B^f

Compute C ← f(1)
Run A (C)
When A halts, outputting b
return b

$$\mathrm{Adv}^{\mathrm{ind}}_{\Pi}(B) = \Pr[B^{E(K,\bullet)} = 1] - \Pr[B^{E(K,0^{|\bullet|})} = 1]$$

$$= \Pr[K \xleftarrow{\$} \boldsymbol{K};\ C \xleftarrow{\$} \boldsymbol{E}_K(1):\ A(C)=1] - \Pr[K \xleftarrow{\$} \boldsymbol{K};\ C \xleftarrow{\$} \boldsymbol{E}_K(0):\ A(C)=1]$$

$$= \Pr[K \xleftarrow{\$} \boldsymbol{K};\ C \xleftarrow{\$} \boldsymbol{E}_K(1):\ A(C)=1] - (1 - \Pr[K \xleftarrow{\$} \boldsymbol{K};\ C \xleftarrow{\$} \boldsymbol{E}_K(0):\ A(C)=0])$$

$$= \Pr[K \xleftarrow{\$} \boldsymbol{K};\ C \xleftarrow{\$} \boldsymbol{E}_K(1):\ A(C)=1] + \Pr[K \xleftarrow{\$} \boldsymbol{K};\ C \xleftarrow{\$} \boldsymbol{E}_K(0):\ A(C)=0] - 1$$

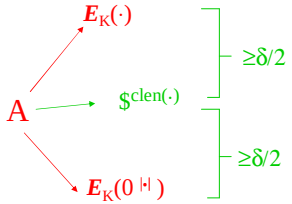
$$= 2\,(\Pr[K \xleftarrow{\$} \boldsymbol{K};\ C \xleftarrow{\$} \boldsymbol{E}_K(1):\ A(C)=1](0.5) + \Pr[K \xleftarrow{\$} \boldsymbol{K};\ C \xleftarrow{\$} \boldsymbol{E}_K(0):\ A(C)=0](0.5)) - 1$$

$$= 2\,(\Pr[A \text{ returns } b \mid b=1]\Pr[b=1] + \Pr[A \text{ returns } b \mid b=0]\Pr[b=0]) - 1$$

$$= 2\Pr[A \text{ returns } b] - 1$$

$$= \mathrm{Adv}^{01}_{\Pi}(A)$$

ind$ ⇒ ind
Let A be an ind-adversary—think of $\delta = \mathrm{Adv}^{\mathrm{ind}}_{\Pi}(A)$ as large.
Construct B that breaks Π in the ind$-sense.



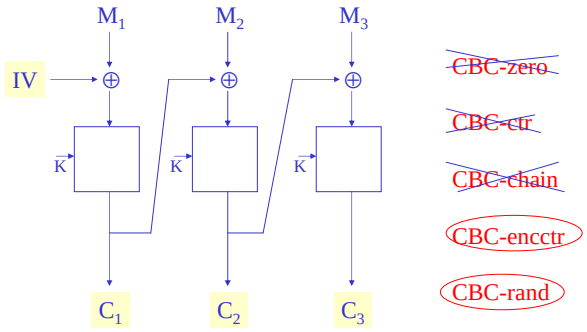
"Hybrid Argument"

Case 1: Set B=A.
$\mathrm{Adv}^{\mathrm{ind\$}}_{\Pi}(B) \geq \delta/2$

Case 2: Adv B^f behaves as follows:
Run A
When A asks its oracle x,
Ask $f(0^{|x|})$ and return it to A.
When A outputs a bit b,
return 1–b

$$\mathrm{Adv}^{\mathrm{ind\$}}_{\Pi}(t,q) \leq 2\,\mathrm{Adv}^{\mathrm{ind}}_{\Pi}(t+\mathrm{tiny}, \mu)$$
$$\mathrm{tiny} = O(\mu)$$

Suppose ∃ an adv A that runs in time t and asks queries totaling μ bits and breaks Π in the ind-sense with advantage δ.
Then ∃ an adv B that runs in time t + O(μ) and asks queries totaling μ bits and breaks Π in the ind$-sense with advantage ≥ δ/2



~~CBC-zero~~

~~CBC-ctr~~

~~CBC-chain~~

CBC-encctr

CBC-rand

violating ind

CBC-zero

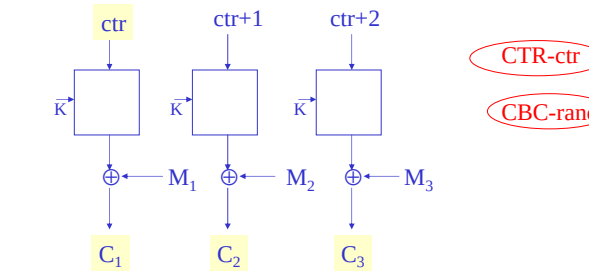
Ask $0^n \rightarrow C_1$
Ask $1^n \rightarrow C_2$
if $C_1 = C_2$ then return 0 else return 1

CBC-ctr

Ask $0^n \rightarrow C_1$
Ask $0^{n-1}\,1 \rightarrow C_2$
if $C_1 = C_2$ then return 1 else return 0

CBC-chain

Ask $0^n \rightarrow IV_1\ C_1$
Ask $C_1 \rightarrow IV_2\ C_2$
Ask $C_2 \rightarrow IV_3\ C_3$
if $C_2 = C_3$ then return 1 else return 0



CTR-ctr

CBC-rand

Claim: CTR-rand is secure if its block cipher is a good PRP:
Let A be an adv attacking CTR[E]. Construct B that attacks E.

Adversary B^f behaves as follows:

Run A.
When A asks its oracle to encrypt $M=M_1 \cdots M_m$
ctr $\leftarrow$ {0,1}
compute pad = f(ctr) f(ctr+1)…f(ctr+m-1)
return to A (ctr, pad$\oplus$M)
When A halts, outputting a bit b,
return b

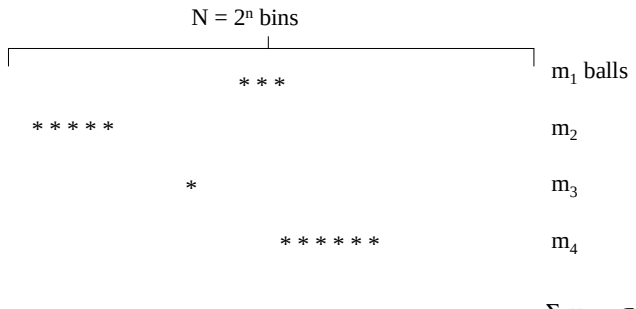
$\mathrm{Adv}^{\mathrm{prp}}_{E}(B) = \Pr[B^{E_K}=1] - \Pr[B^{\pi}=1]$
$\geq \Pr[B^{E_K}=1] - \Pr[B^{\rho}=1] - \sigma^2 / 2^{n+1}$ (switching lemma)
$= \Pr[A^{\mathrm{CTR}[E_K]}=1] - \Pr[A^{\mathrm{CTR}[\rho]}=1] - \sigma^2 / 2^{n+1}$

Let C be the event of a collision in the inputs to the blockcipher

$= \Pr[A^{\mathrm{CTR}[E_K]}=1] - \Pr[A^{\mathrm{CTR}[\rho]}=1 \mid \overline{C}]\ \Pr[\overline{C}]$
$\quad - \Pr[A^{\mathrm{CTR}[E_K]}=1 \mid C]\ \Pr[C] - \sigma^2 / 2^{n+1}$
$= \Pr[A^{\mathrm{CTR}[E_K]}=1] - \Pr[A^{\$}=1]\,(1 - \Pr[C])$
$\quad - \Pr[A^{\mathrm{CTR}[E_K]}=1 \mid C]\ \Pr[C] - \sigma^2 / 2^{n+1}$
$= \Pr[A^{\mathrm{CTR}[E_K]}=1] - \Pr[A^{\$}=1] + \Pr[C]\Pr[A^{\$}=1]$
$\quad - \Pr[A^{\mathrm{CTR}[E_K]}=1 \mid C]\ \Pr[C] - \sigma^2 / 2^{n+1}$
$\geq \Pr[A^{\mathrm{CTR}[E_K]}=1] - \Pr[A^{\$}=1] - \Pr[C] - \sigma^2 / 2^{n+1}$
$= \mathrm{Adv}^{\mathrm{ind\$}}_{\mathrm{CTR}[E]} - \Pr[C] - \sigma^2 / 2^{n+1}$

The problem is now an information theoretic one. Claim $\Pr[C] \leq \sigma^2 / 2^{n+1}$ (see next slide). We then have

$\geq \mathrm{Adv}^{\mathrm{ind\$}}_{\mathrm{CTR}[E]} - \sigma^2 / 2^{n}$



Adversary wants to create a collision.
Best way to do this is to toss one ball at a time.
$\Pr[C] \leq 1/N + 2/N + \ldots + (\sigma\text{-}1)/N$
$\leq \sigma^2/2N$

Lecture 3

Th. Let $E: K \times \{0,1\}^n \rightarrow \{0,1\}^n$.
Let A attack CBC[E]. Assume A runs in time t_A and asks σ total blocks and achieves advantage $\delta_A = \mathrm{Adv}^{\mathrm{ind\$}}_{\mathrm{CBC}[E]}(A)$.

Then an adv B that attacks E and runs in time at most t_B and asks at most q_B queries and achieves advantage at least $\delta_B = \mathrm{Adv}^{\mathrm{prp}}_{E}(B)$ where
$t_B = t_A + O(\sigma)$
$q_B = \sigma$
$\delta_B = \delta_A - \sigma^2 / 2^n$

Def of B^f

Run A
When A asks its oracle $M = M_1 \cdots M_m$
Choose $IV \leftarrow C_0 \xleftarrow{\$} \{0,1\}^n$
for $i \leftarrow 1$ to m do $C_i \leftarrow f(C_{i-1} \oplus M_i)$
return to A $(IV, C_1 \cdots C_m)$
When A outputs a bit, b,
return b

$$\Pr[A^{CBC[\pi]} = 1]$$

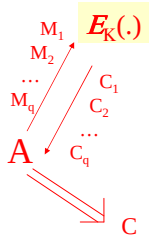
$$\mathrm{Adv}^{prp}_{E}(B) = \Pr[B^{E_K} = 1] - \Pr[B^{\pi} = 1]$$

$$\mathrm{Adv}^{ind\$}_{CBC[E]}(A) = \Pr[A^{CBC_E} = 1] - \Pr[A^{\$} = 1]$$

$$\begin{aligned}\mathrm{Adv}^{ind\$}_{CBC[E]}(A) - \mathrm{Adv}^{prp}_{E}(B) &= \Pr[B^{\pi} = 1] - \Pr[A^{\$} = 1] \\ &= \Pr[A^{CBC[\pi]} = 1] - \Pr[A^{\$} = 1] \\ &= \Pr[A^{CBC[\rho]} = 1] - \Pr[A^{\$} = 1] + \sigma^2/2^{n+1}\end{aligned}$$

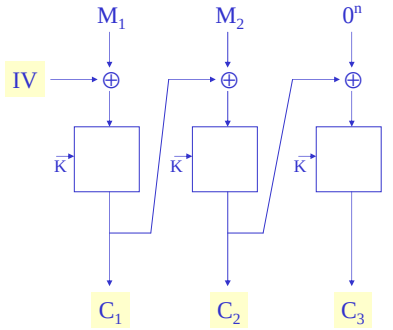
Now a purely inf theoretic question. "Game-playing" to Show first difference at most $\sigma^2 / 2^{n+1}$

Authenticity



A "wins"
if $C \notin \{C_1,\ldots,C_q\}$
and
$D_K(C) \neq *$

"Encrypt-with-redundancy"



Attack:
Ask **0 0** → IV C_1 C_2 C_3

Forge
IV C_1 C_2

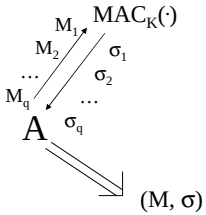
MAC "Message Auth. Code" $\mathrm{MAC}_K(M)$

σ

$M \;.\; \mathrm{MAC}_K(M)$

$S^K \longrightarrow R^K$

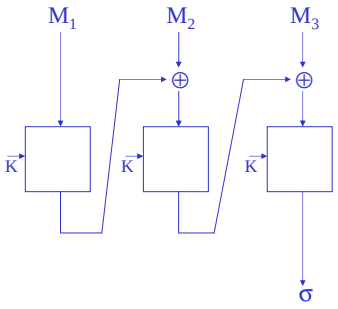
Compute $\sigma' = \mathrm{MAC}_K(M)$
Check if $\sigma = \sigma'$



(M, σ)

A **wins** if $\sigma = \mathrm{MAC}_K(M)$ and $M \notin \{M_1,\ldots,M_q\}$
"A forgery"

$\mathrm{Adv}^{mac}_{\Pi}(A) = \Pr[K \xleftarrow{\$} \boldsymbol{K}: A^{\mathrm{MAC}_K(\cdot)} \text{ forges}]$

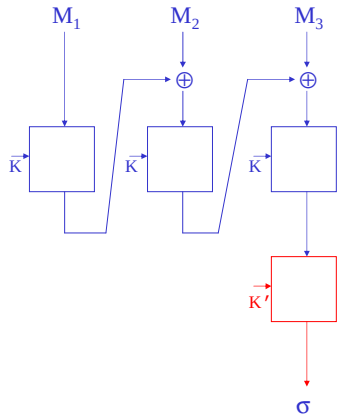


CBC MAC

To forge:
Ask **0** $\rightarrow \sigma_1$
Forge
(**0** σ, σ)

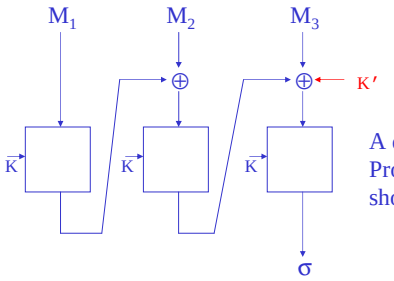
The CBC MAC is Incorrect across msgs of Varying lengths.

[BKR] Correct, with bound $3\sigma^2/2^n$ for msgs of some one fixed length.

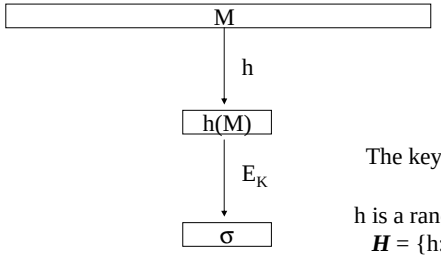


Fixing the CBC MAC

Encrypted CBC (from RACE project). Shown provably secure (when E a PRP) by [Petrank, Rackoff]



A different fix. Provably security shown in [Black, R]

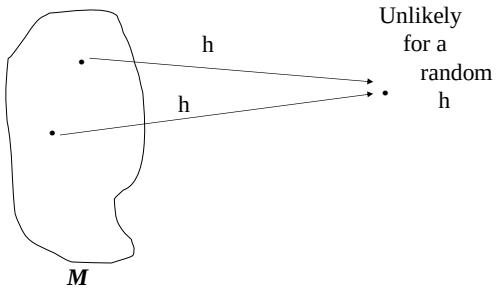


Carter-Wegman paradigm

The key for the MAC is (h,K)

h is a random element of
$\boldsymbol{H} = \{h: \boldsymbol{M} \rightarrow \{0,1\}^n\}$

Def: Family of hash functions $\boldsymbol{H} = \{h: \boldsymbol{M} \rightarrow \{0,1\}^n\}$
is **ε-AU** (almost universal) if for all M, M′ ∈ M, M≠M′,
$Pr_h[h(M)=h(M')] \leq \varepsilon$



37

Eg construction

$M = M_m \ldots M_0 \qquad |M_i|=128$

$M(X) = X^m + M_{m-1} X^{m-1} + \cdots + M_1 X + M_0$

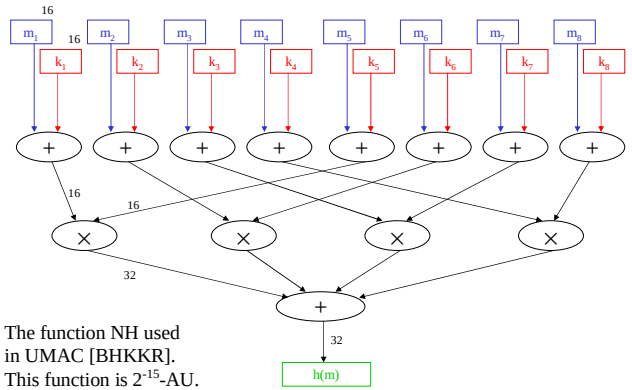
All operations in $GF(2^{128})$

There are 2^{128} elements of ***H***, each described by a 128-bit R:
$h_R(M) = M(R)$. Can be efficiently evaluated.

Claim: ***H*** is $m/2^{128}$-AU where m upperbounds the number of blocks on any message M in the message space ***M***

Proof: Pr [M(R) =M′(R)] = Pr[poly(R) =0] ≤ $m/2^{128}$ because poly(·) is a nonzero polynomial of degree at most m and therefore has at most m zeros, and so that chance that a random point in the field is one of these zeros is at most m / the size of the field.

38

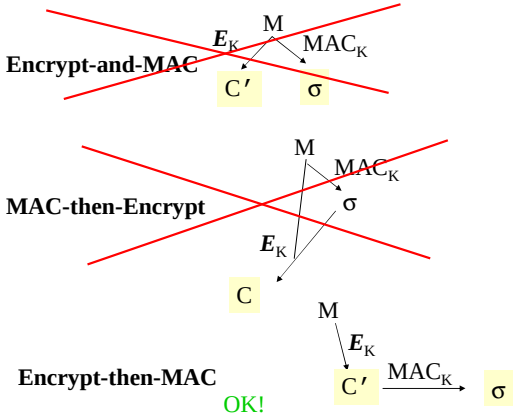


The function NH used in UMAC [BHKKR]. This function is 2^{-15}-AU. The above can be computed In just four instructions on a Pentium processor, allowing one to MAC at about 1cpb.

39

Authenticated Encryption via Generic Composition

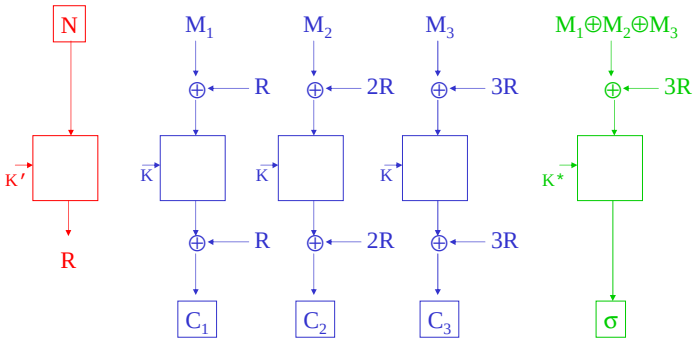
(see [Bellare, Namprempre])



40

Authenticated Encryption via Fancy Modes

(see IAPM [J] and OCB [RBBK])



41