Public key crypto (quick intro) Provable cryptography

Slides from Bart Preneel and Phil Rogaway

CPA

M_1
M_2
$\ldots$
M_q

$\mathcal{E}_K(.)$

A

$\mathcal{E}_K(X_1)$
$\mathcal{E}_K(X_2)$
$\ldots$
$\mathcal{E}_K(X_q)$

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

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

sem

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

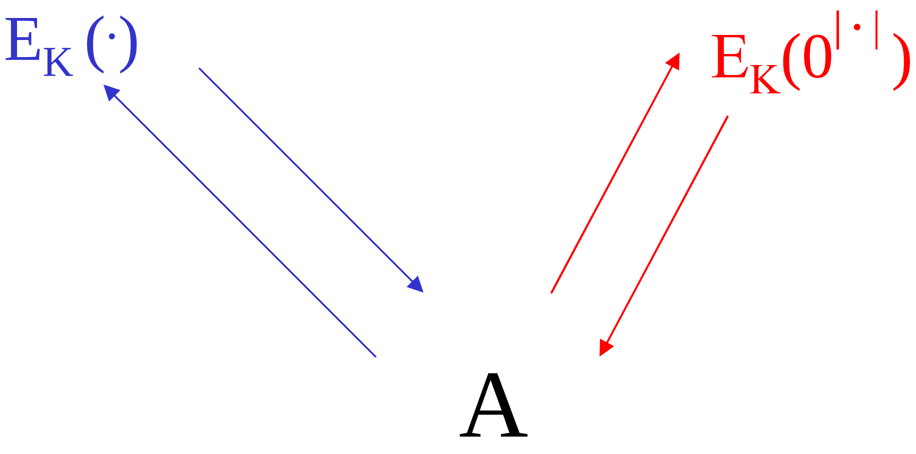
$$\Pr\left[\, K \xleftarrow{\$} \mathcal{K};\ (f, \mathcal{M}) \xleftarrow{\$} A^{\mathcal{E}(K,\cdot)}(\,);\ M, M' \xleftarrow{\$} \mathcal{M};\ C \xleftarrow{\$} \mathcal{E}_K(M') : A^{\mathcal{E}(K,\cdot)}(C, f) = f(M) \,\right]$$

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

ind

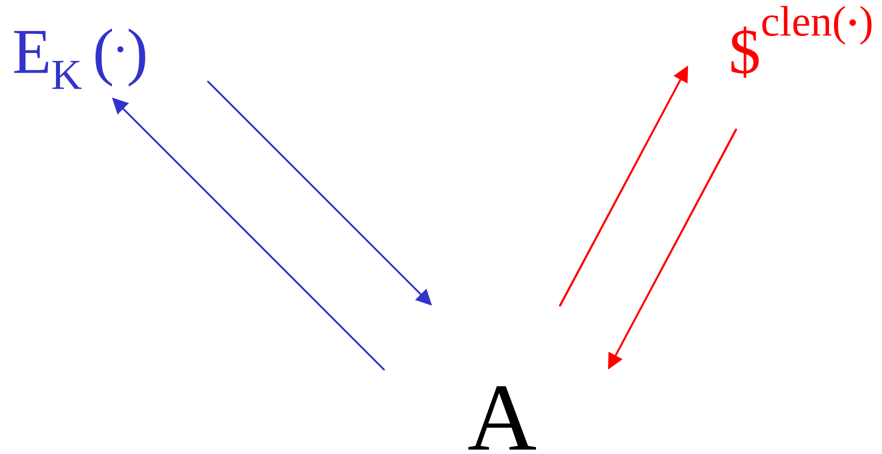
$$\mathrm{Adv}^{\mathrm{ind}}_{\Pi}(A) = \Pr[\ K \xleftarrow{\$} \boldsymbol{K} :\ A^{\boldsymbol{E}(K,\,\cdot)} = 1\ ] -$$

$$\Pr[\ K \xleftarrow{\$} \boldsymbol{K} :\ A^{\boldsymbol{E}(K,\,0^{|\cdot|})} = 1\ ]$$



ind$

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



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

$$b \in \{0,1\} \longrightarrow \boxed{\boldsymbol{E}_K} \xrightarrow{\;C\;} \boxed{A} \longrightarrow b'$$

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

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 $C \leftarrow f(1)$
Run A (C)
When A halts, outputting b
  return b

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

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

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

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

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

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

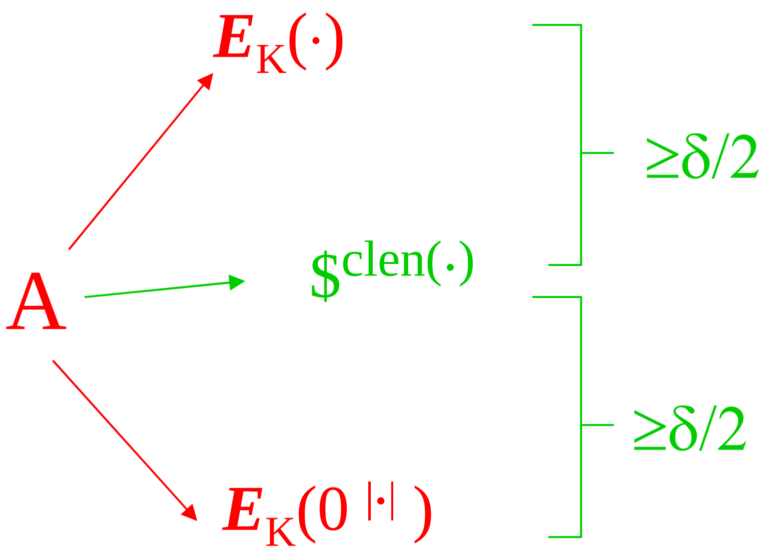
$= 2\Pr[A \text{ returns } b] - 1$

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

ind$ $\Rightarrow$ ind

Let A be an ind-adversary—think of $\delta = \mathrm{Adv}_{\Pi}^{\mathrm{ind}}(A)$ as large.

Construct B that breaks Π in the ind$-sense.



Case 1: Set B=A.

$\mathrm{Adv}_{\Pi}^{\mathrm{ind\$}}(B) \geq \delta/2$

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,

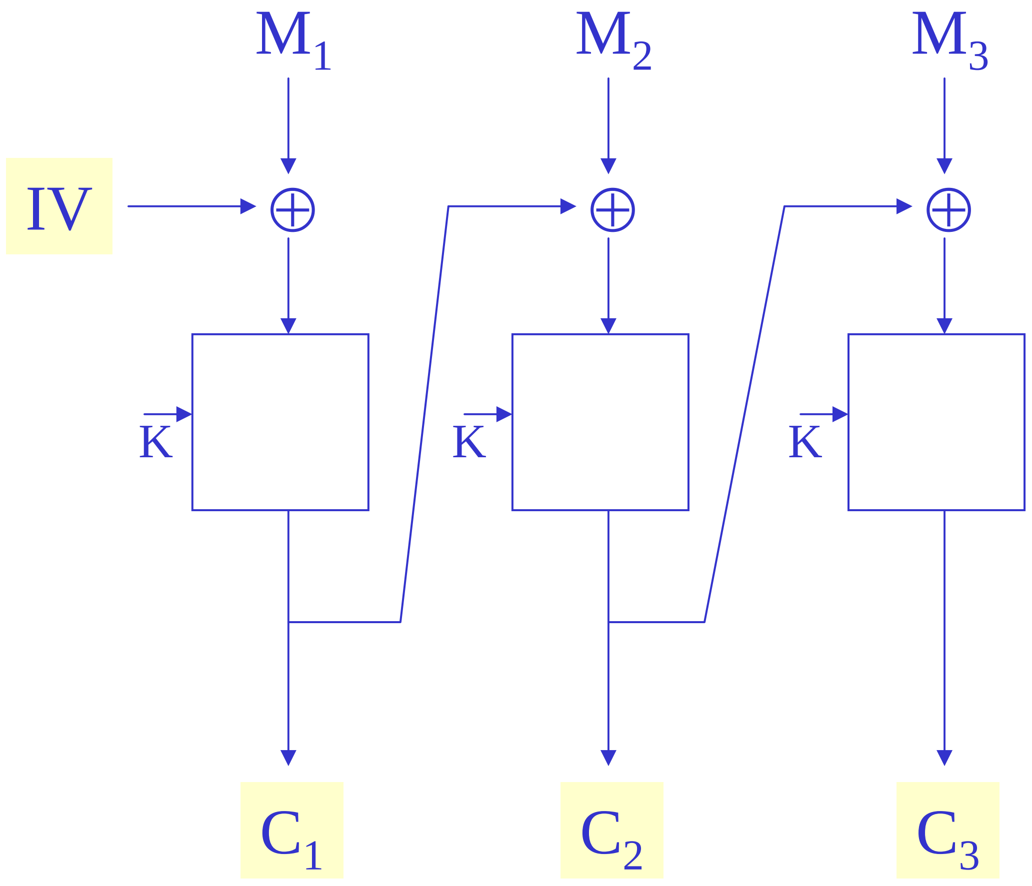
return 1–b

"Hybrid Argument"

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

$$\mathrm{tiny} = O(\mu)$$

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 (IV = 0)

Ask $0^n \to C_1$

Ask $1^n \to C_2$

if $C_1 = C_2$ then return 0 else return 1

CBC-ctr ($IV_i = i$)

Ask $0^n \to C_1$

Ask $0^{n-1} 1 \to C_2$

if $C_1 = C_2$ then return 1 else return 0

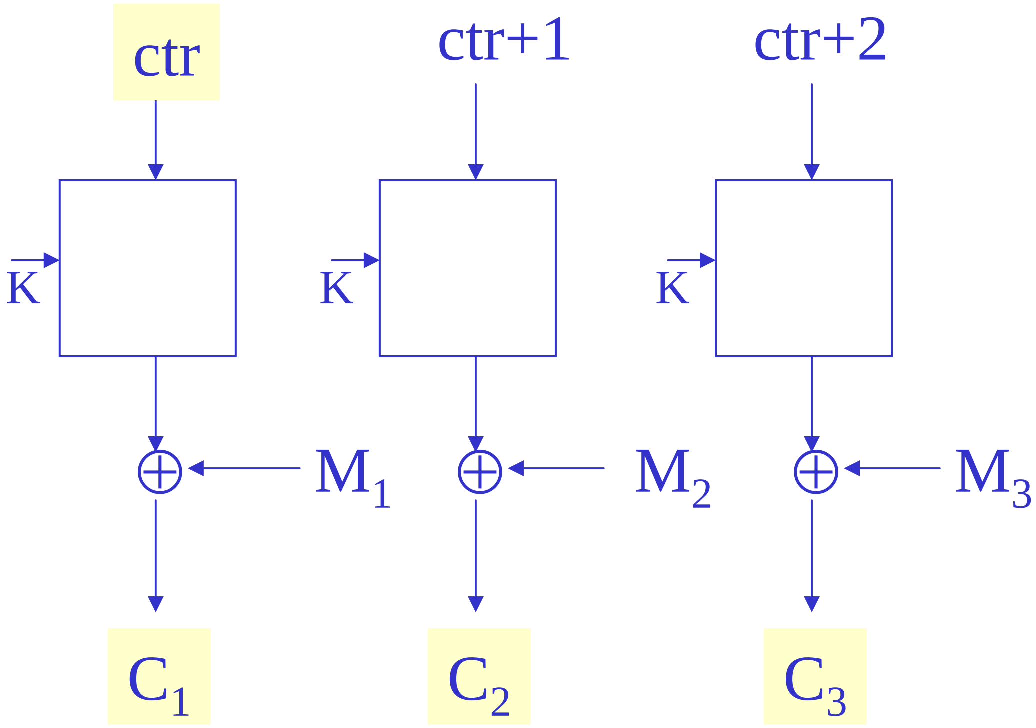
CBC-chain (IV_i = last block of ciphertext)

Ask $0^n \to IV_1 \ C_1$

Ask $C_1 \to IV_2 \ C_2$

Ask $C_2 \to IV_3 \ C_3$

if $C_2 = C_3$ then return 1 else return 0



CTR-ctr

CBC-rand

Proof outline (from *Goldwasser and Bellare*, chapter 6)

- We know that one-time-pad is secure
- Replace block-cipher with *random* function (R)
- R(i++) = one-time-pad

- Shannon proved that “idealized” counter mode give any attacker zero advantage

- Construct difference between ideal and actual protocol (ind$)

- Assume adversary A can distinguish ideal and actual protocol
- Prove that adversary B could use A to distinguish the block cipher from PRF

- Therefore, assuming any B should have low advantage (strong cipher), then
- *Any* A therefore has a low advantage

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

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

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

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

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

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

$N = 2^n$ bins

* * * m_1 balls

* * * * * m_2

* m_3

* * * * * * m_4

$\Sigma\, m_{in} = \sigma$

Adversary wants to create a collision.

Best way to do this is to toss one ball at a time.

$$\Pr[C] \le 1/N + 2/N + \ldots + (\sigma-1)/N$$
$$\le \sigma^2/2N$$

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

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

$$\|$$

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

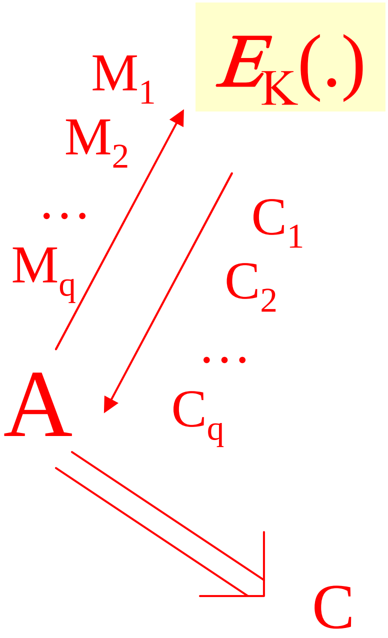
$$\|$$

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

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

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

Authenticity



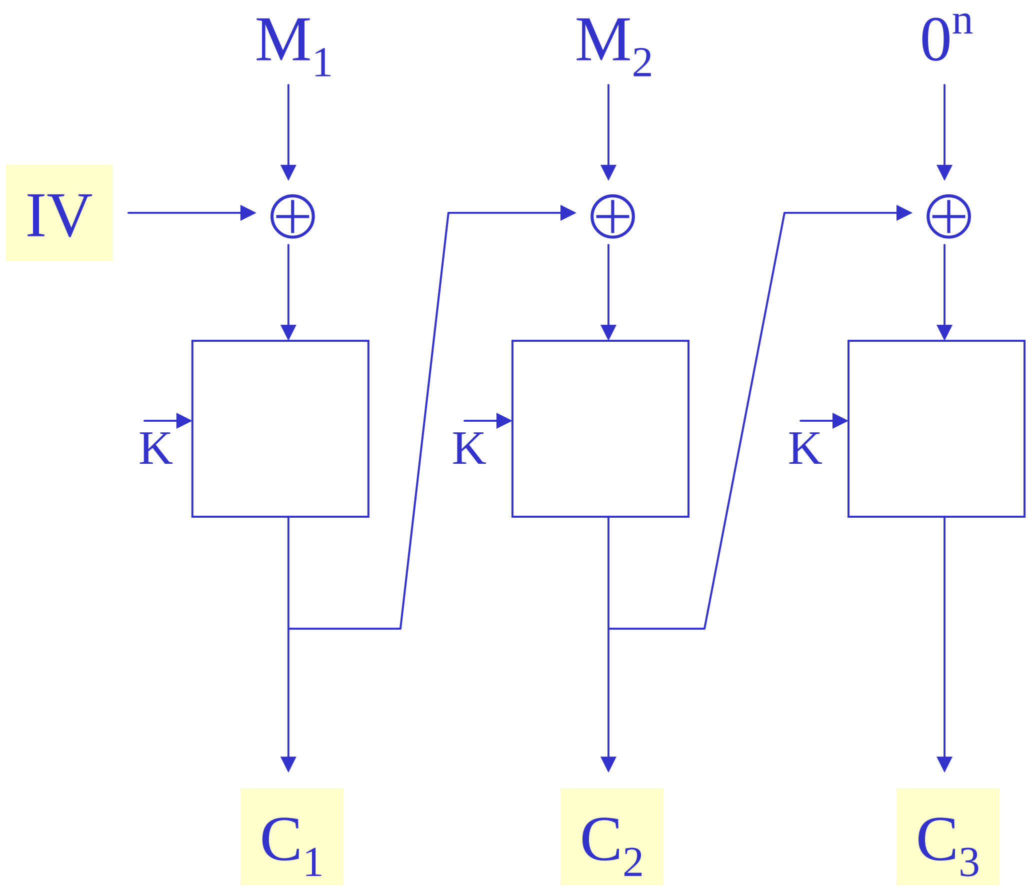
A "wins"

if $C \notin \{C_1, \ldots, C_q\}$

and

$\boldsymbol{D}_K(C) \neq *$

"Encrypt-with-redundancy"



Attack:

Ask **0 0** $\rightarrow$ IV C_1 C_2 C_3

Forge

IV C_1 C_2

MAC "Message Auth. Code" $MAC_K(M)$

$$\sigma$$

$$S^K \xrightarrow{\;M \,.\, MAC_K(M)\;} R^K$$

Compute $\sigma' = MAC_K(M)$

Check if $\sigma = \sigma'$

$MAC_K(\cdot)$

M_1, M_2, …, M_q

σ_1, σ_2, …, σ_q

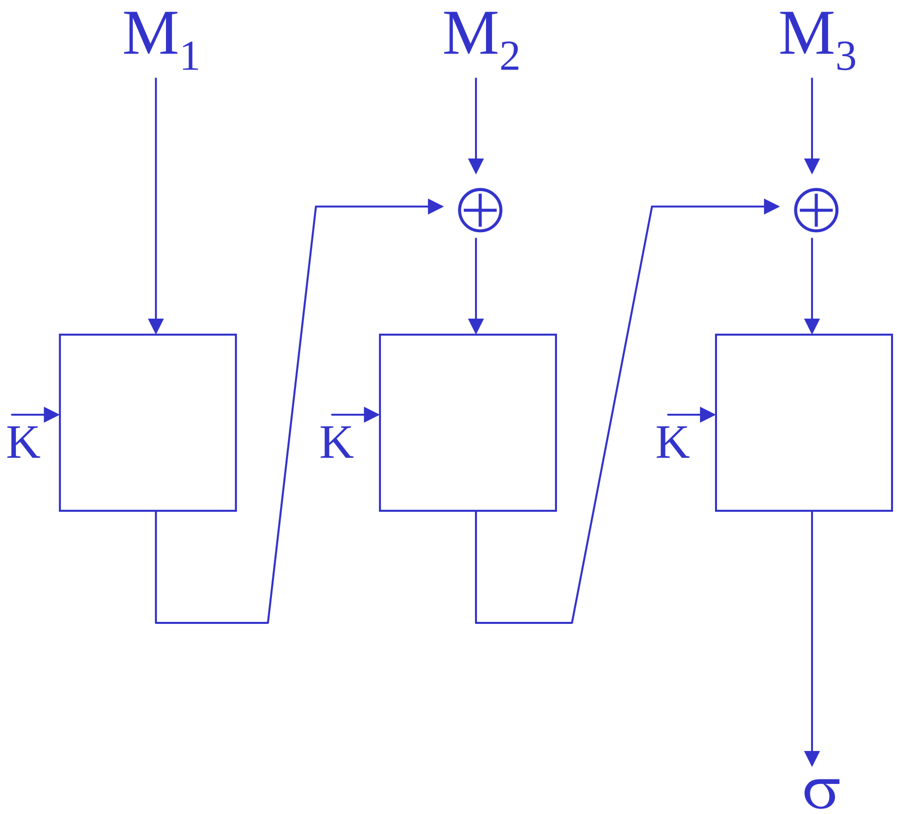
A

(M, σ)

A **wins** if $\sigma = MAC_K(M)$ and $M \notin \{M_1, \ldots, M_q\}$

"A forgery"

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



CBC MAC

To forge:

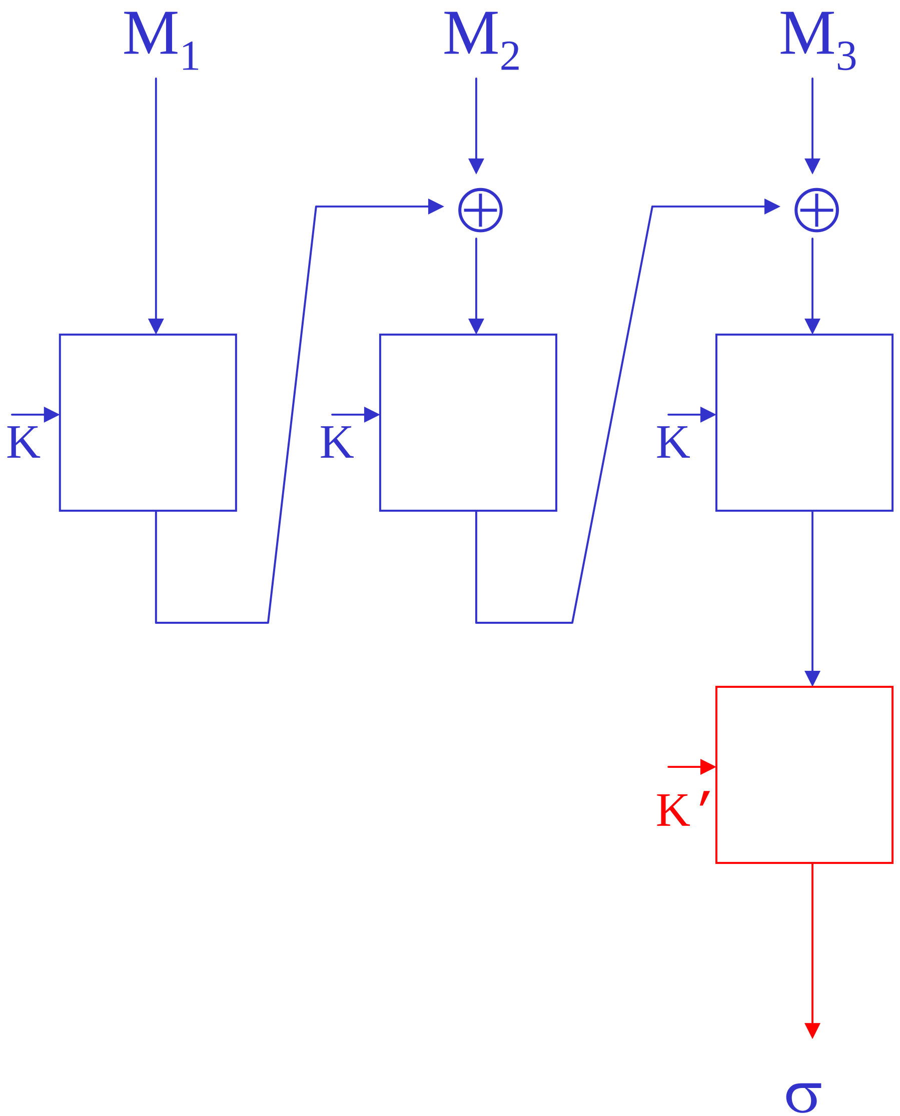
Ask $\mathbf{0} \rightarrow \sigma_1$

Forge

$(\mathbf{0}\ \sigma, \sigma)$

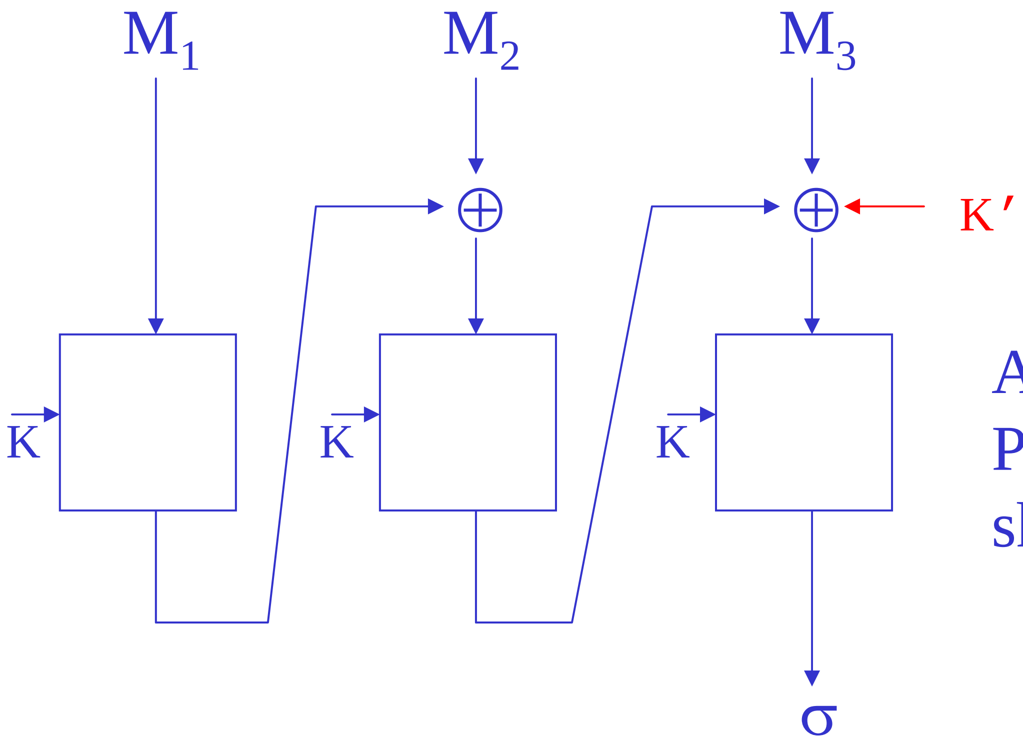
The CBC MAC is Incorrect across msgs of Varying lengths.

[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]

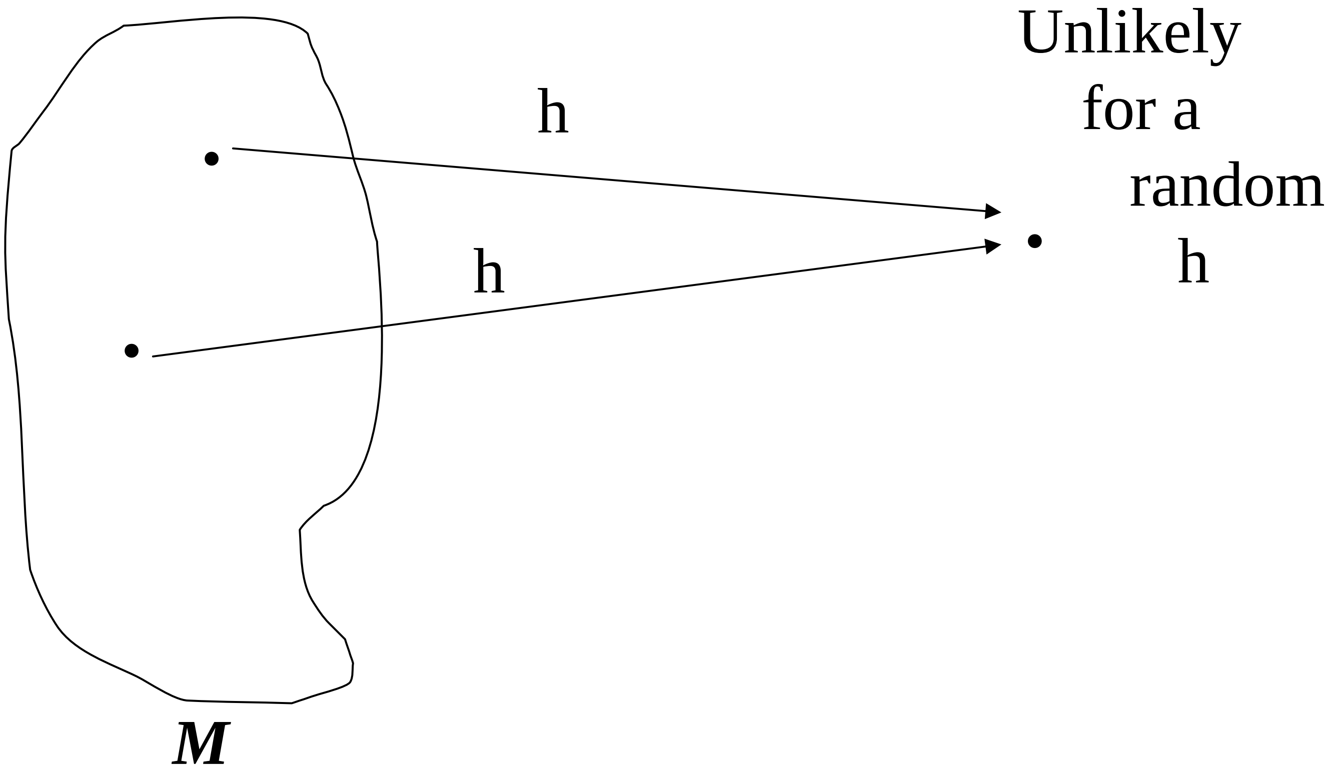
Carter-Wegman paradigm

$$\begin{tikzcd} M \arrow[d, "h"] \\ h(M) \arrow[d, "E_K"] \\ \sigma \end{tikzcd}$$

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′,
$\Pr_h [h(M)=h(M')] \leq \varepsilon$


Unlikely
for a
random
h
h
h
M

Eg construction

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

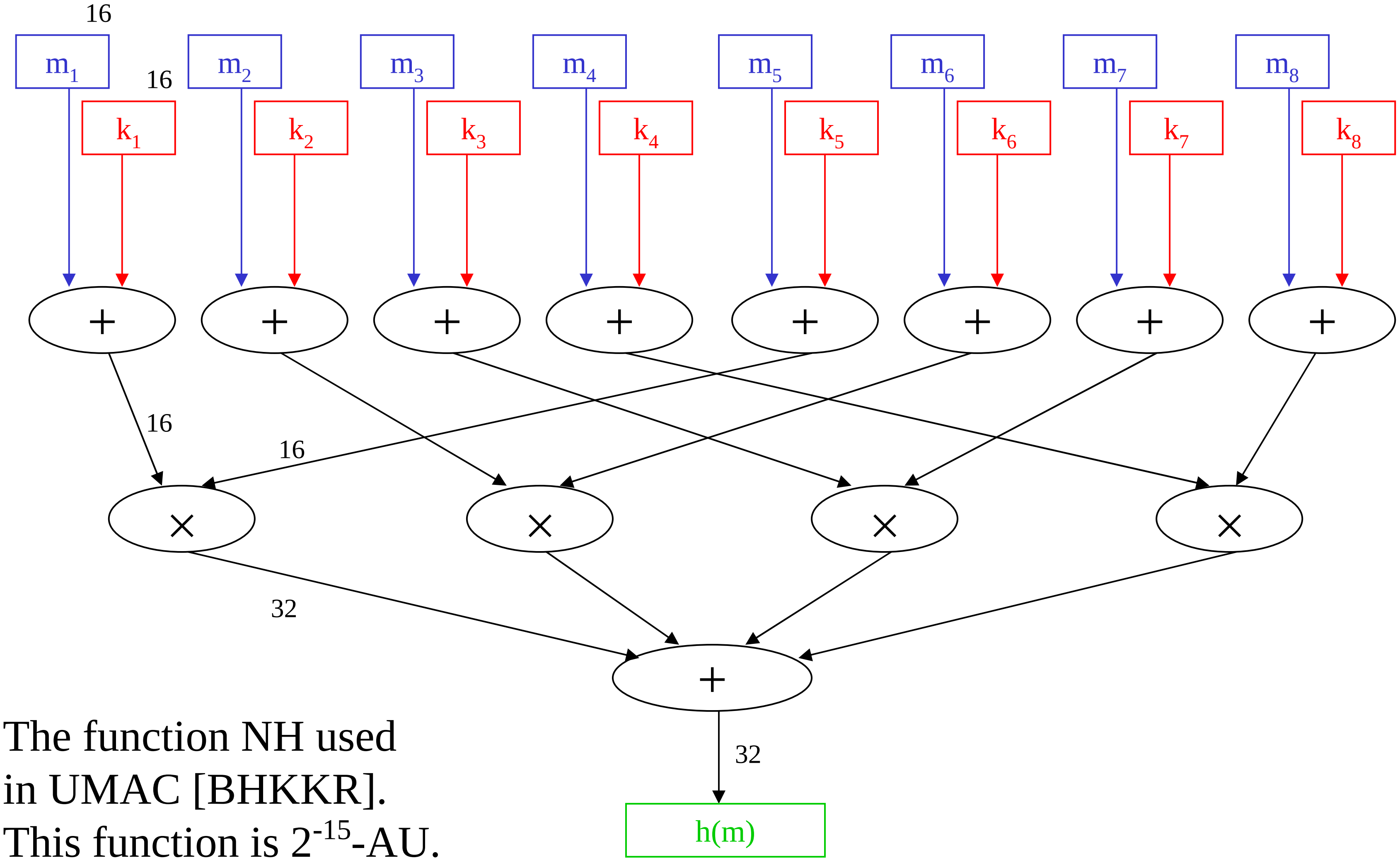
$M(X) = X^m + M_{m-1} X^{m-1} + \cdots + M_1 X + M_0$

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: $\Pr[\, M(R) = M'(R)] = \Pr[poly(R) = 0] \le m/2^{128}$ because $poly(\cdot)$ 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.



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.

Authenticated Encryption via Generic Composition

(see [Bellare, Namprempre])

Encrypt-and-MAC

$$C' \xleftarrow{\boldsymbol{E}_K} M \xrightarrow{MAC_K} \sigma$$

MAC-then-Encrypt

$$\begin{tikzcd} M \arrow[r, "MAC_K"] \arrow[dr, "\boldsymbol{E}_K"'] & \sigma \arrow[d] \\ & C \end{tikzcd}$$

Encrypt-then-MAC

$$M \xrightarrow{\boldsymbol{E}_K} C' \xrightarrow{MAC_K} \sigma$$

OK!

Authenticated Encryption via Fancy Modes

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