

Presentation of RMAC
A randomized CBC–MAC beyond the Birthday Paradox
Limit,

Éliane JAULMES, Antoine JOUX, Frédéric VALETTTE
Crypto Lab
DCSSI

RMAC: a new construction

Overview

1. CBC–MAC: definitions and properties
2. Security Arguments
3. Application to the **AES**

RMAC: a new construction

Message Authentication Code

- MAC: authentication in secret key settings
- Message $M \longrightarrow \text{MAC}_K(M) = T$
- Sender sends (M, T)
- Receiver verifies $T = \text{MAC}_K(M)$
- Forgery attack on MAC: Find a valid (M, T)

RMAC: a new construction

CBC-MAC

- Built from a block cipher E_K
- Message $M = M_1, M_2, \dots, M_m$: m blocks of n bits
- When the size of M is not multiple of $n \rightarrow$ padding
- Principle: encrypt with E_K in **CBC** mode
- MAC = last output of the **CBC** chain

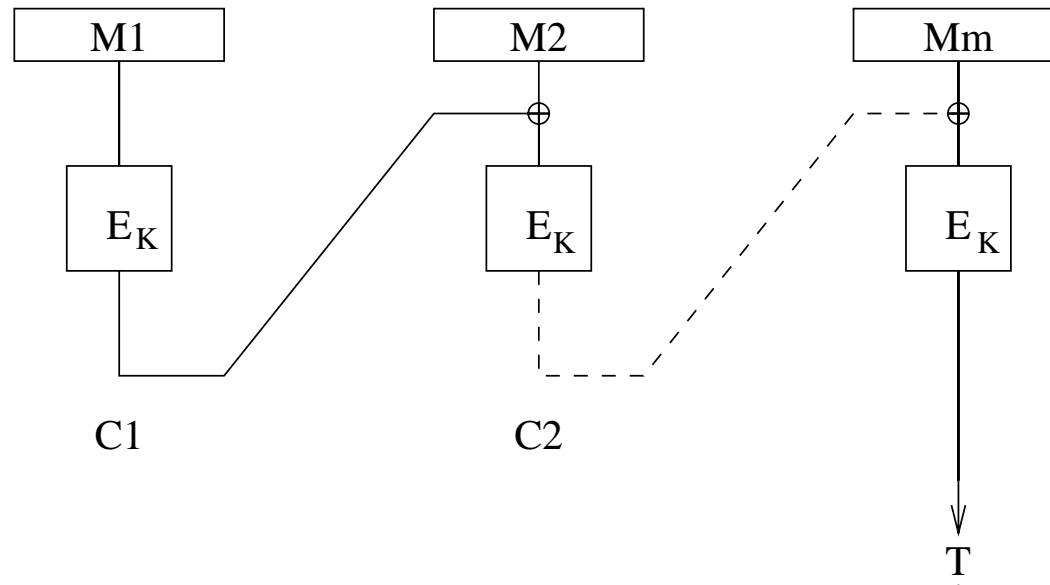
RMAC: a new construction

The Padding

- Classical Padding: $M \rightarrow M||1||0 \quad 0$
- Add '1' and enough '0' to fill the block
- All messages are padded
- From now: message length is a multiple of n

RMAC: a new construction

The elementary CBC-MAC



$$C_0 = 0^n$$

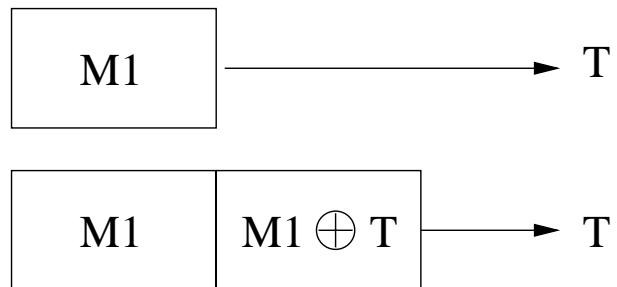
$$C_i = E_K(M_i \oplus C_{i-1}) \text{ for } i \text{ in } 1 \dots m$$

$$T = C_m$$

RMAC: a new construction

Anal sis of the elementary CBC–MAC

- Proven secure for fixed-length messages [BeKiRo-94]
- Insecure when message length varies



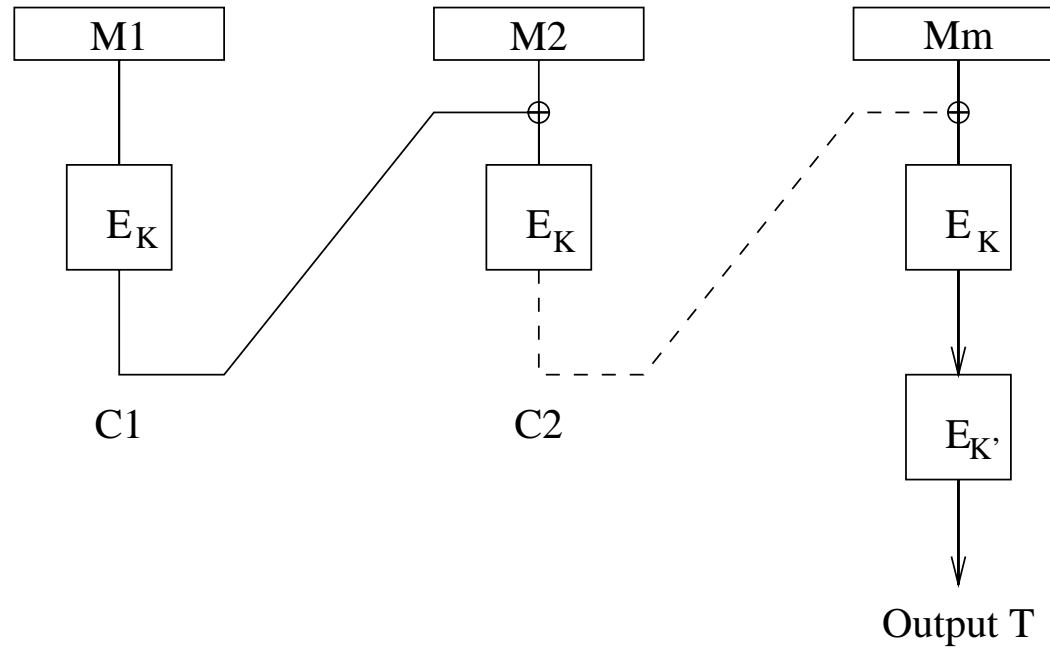
RMAC: a new construction

DMAC

- Elementary CBC–MAC insecure
- Need a secure CBC–MAC for messages of different length
- Solution **DMAC**:
 - At the end of **CBC** chain
 - Encrypt result with $E_{K'}$
 - $K' \neq K$

RMAC: a new construction

Description of DMAC



$$C_i = C_{i-1} \oplus E_K(M_i) \quad \text{for } i = 1, \dots, m$$

$$T = E_{K'}(C_m)$$

RMAC: a new construction

Proving the security

- Model: **DMAC** scheme with random permutations
- Adversary: access to an oracle computing the MAC
- Security proven in this setting
- Replace random permutations by block ciphers
- Secure block cipher \sim random permutation

RMAC: a new construction

Security of DMAC

- Proven secure in [BIR00] and [PeRa97]
- In the preceding model:
 - q questions to the oracle
 - Messages of at most m_{max} blocks

$$\text{Adv}_{\text{DMAC}}(\mathcal{A}) \leq \frac{2q^2 m_{max}^2 + q^2}{2}$$

RMAC: a new construction

Proof idea (1)

- Perfect MAC = random function
- Distinguish our model of **DMAC** from a random function:
 - Distinguish **DMAC** with random functions from a random function
 - Distinguish random functions from random permutations

RMAC: a new construction

Proof idea (2)

E_K and $E_{K'}$ replaced by f_1 and f_2 , random functions

- Entries of f_2 all different \rightarrow random outputs
- Collision: M and M' give same **CBC** output
- Probability to distinguish \equiv Collision probability $V(M, M')$

RMAC: a new construction

Proof idea (3)

- Adversary: q questions of size at most m_{max}
- Collisions: $V(M, M') = \frac{(m + m')^2}{2}$
- Summing for all messages: $\sum_{M, M'} V(M, M') \leq \frac{2q^2 m_{max}}{2}$
- functions \rightarrow permutations: $\mathbf{Adv}^{\text{prf/prp}} \leq \frac{q^2}{2+1}$
- Finally: $\mathbf{Adv}^{\text{Dmac}}(\mathcal{A}) \leq \frac{2q^2 m_{max}^2 + q^2}{2}$

RMAC: a new construction

Tight bound: Attack with birthday paradox

- Output T has size n bits
- Query $\sqrt{2^n} = 2^{n/2}$ messages M^i
- \Rightarrow with high probability 2 messages $M^{(1)}$ and $M^{(2)}$ s.t. $T^{(1)} = T^{(2)}$
- $\forall M', \mathbf{DMAC}(M^{(1)} || M') = \mathbf{DMAC}(M^{(2)} || M')$



RMAC: a new construction

Existing solutions

- MACRX [BeGoKr99]: not CBC-MAC based, expands MAC size by a factor 3
- CBC-MAC with counters: maintain counter
- Simple randomized CBC-MAC: L-collisions

Find a randomized CBC-MAC with proven security and easy to use

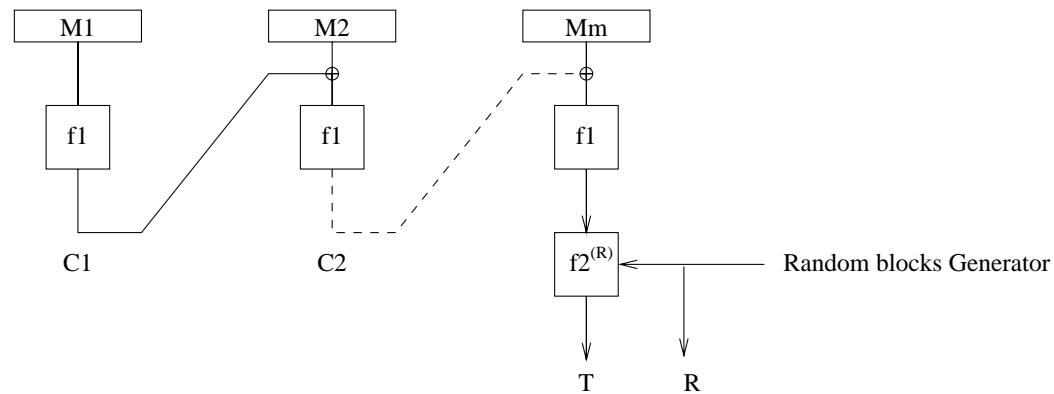
RMAC: a new construction

Principle of RMAC

- **RMAC** = Randomized CBC-MAC
- Apply a random function at the end of **CBC** computation
- MAC = output + information of the chosen function

RMAC: a new construction

Description of our solution: RMAC



$$\begin{aligned}
 &= 0 \\
 C_i &= f_1(M_i \oplus C_{i-1}) \text{ for } i \in \{1, \dots, m\} \\
 T &= f_2^{(R)}(C_m) \\
 &= (T, R)
 \end{aligned}$$

RMAC: a new construction

Description of the model

- f_1 random permutation
- f_2 random permutations
- Adversary has access to two oracles:
 - MAC generation oracle
 - MAC verification oracle

RMAC: a new construction

Security of RMAC

- Optimal construction:
 - Result of MAC on 2 blocks
 - Number of ciphering the same as **DMAC**
- Adversary A asks questions of total size L blocks
- Security in 2 : birthday parado = exhaustive search

$$\text{Adv}^{\text{Rmac}}(A) \leq \frac{nL + L + 1}{2}$$

RMAC: a new construction

Proof idea (1)

- Perfect randomized MAC = family of random functions
- Distinguish our model of **RMAC** from a family of random functions:
 - Distinguish **RMAC** with f_1, f_2) random functions from a family of random functions
 - Distinguish random functions from random permutations

RMAC: a new construction

Proof idea (2)

- Entries of f_2 all different \rightarrow random outputs
- Different \rightarrow random outputs
- Collision: M and M' give same **CBC** output and \equiv
- Probability to distinguish \equiv Collision probability
 - Collisions with the generation oracle
 - Collisions with the verification oracle

RMAC: a new construction

Collisions with generations

- Adversary: total length of queries bounded by L
- Collisions within a group a q messages:

$$\Pr \leq \frac{3q \sum_{i=1}^q m_i}{2}$$

- Size of the groups is less than n with probability $\frac{1}{2^n}$
- Summing for all messages:

$$\Pr \leq \frac{3nL}{2}$$

RMAC: a new construction

Collisions with verifications

- Adversary: total length of queries bounded by L
- A large group may exist but we may only compare with a reference message
- Collisions with a reference message:

$$\Pr \leq \frac{3 \sum_{i=0}^q m_i}{2}$$

- Summing for all messages:

$$\Pr \leq \frac{3L}{2}$$

RMAC: a new construction

Proof idea (3)

- Adversary: total length of queries bounded by L
- Collisions:

$$\Pr \leq \frac{3nL + 3L + 1}{2}$$

- PRF/PRP switching:

$$\text{Adv} \leq \frac{nL + L}{2}$$

- Finally:

$$\text{Adv}_{\text{Rmac}}(\mathcal{A}) \leq \frac{nL + L + 1}{2}$$

RMAC: a new construction

Application a block cipher

- $f_1 = E_K$
- $f_2 = E_{\oplus K'}$
- f_2 not chosen at random but among a **known** family
- need to modify the model

RMAC: a new construction

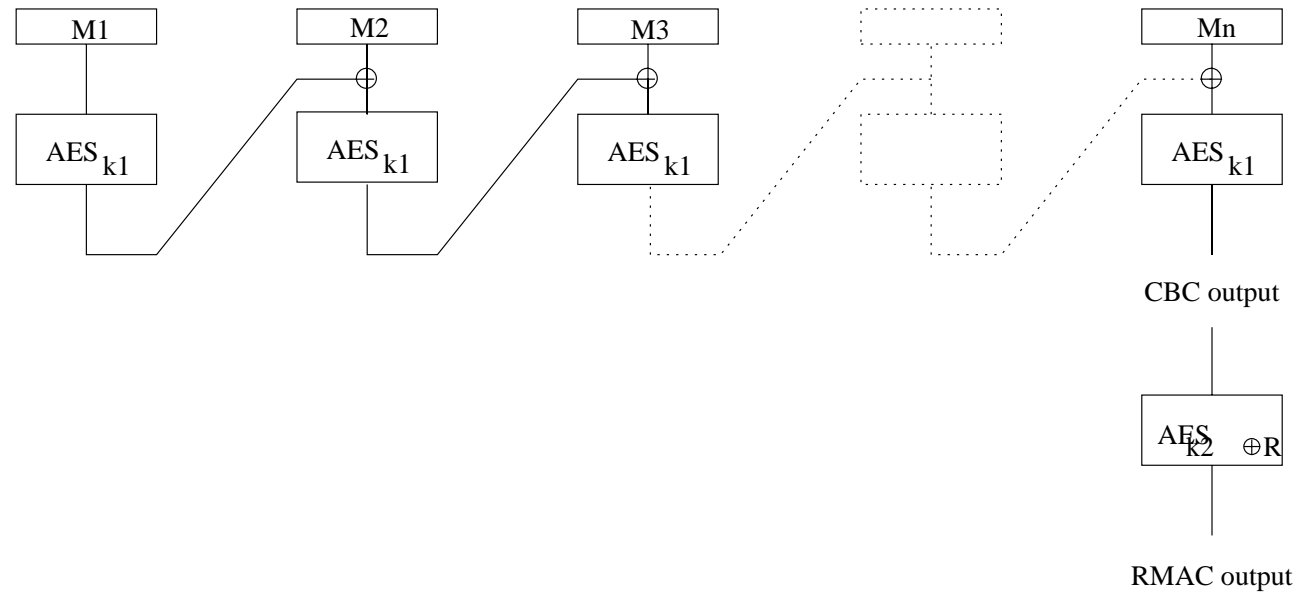
New model

- f_2 chosen in a known family F
- Adversary has access to F through an oracle
- The security becomes:

$$\text{Adv}^{\text{RMAC}}(\mathcal{A}) \leq \frac{5nL + L + 2}{2}$$

RMAC: a new construction

Application to the AES



$$= 0^{128}$$

$$C_i = \mathbf{AES}_{K_1}(M_i \oplus C_{i-1}) \text{ for } i \text{ in } 1 \dots m$$

$$T = \mathbf{AES}_{K_2 \oplus R}(C_m)$$

$$\mathbf{RMAC}(M) = (T, C_m)$$

RMAC: a new construction

Advantages of this construction

- Computation time identical to **DMAC**:
 - $m + 1$ computations
 - 2 keys
- The security is

- Secure for $L \leq 2^{118}$
$$\text{Adv}_{\text{RMAC}}^{\text{AE}} \leq \frac{5 \cdot 128L + L + 2}{2^{128}} + \frac{t}{2^{128}} \leq \frac{645L + t}{2^{128}}$$

RMAC: a new construction