Using Rijndael-256 in AES Modes

Tetsu Iwata
Nagoya University

AES --- 25 years of competing designs and cryptanalysis
April 13, 2026
Gaustablikk Fjellresort, Telemark, Norway

Thanks to Kazuhiko Minematsu for many discussions. Part of the content was presented at DIAC 2013

NIST SP800-38 Series

- NIST AES standardization process (1997-2001)
- NIST modes development (2000-ongoing)
  - Standard modes for AES and TDES
  - SP 800-38A, B, C, D, E, F, G

NIST SP800-38 Series

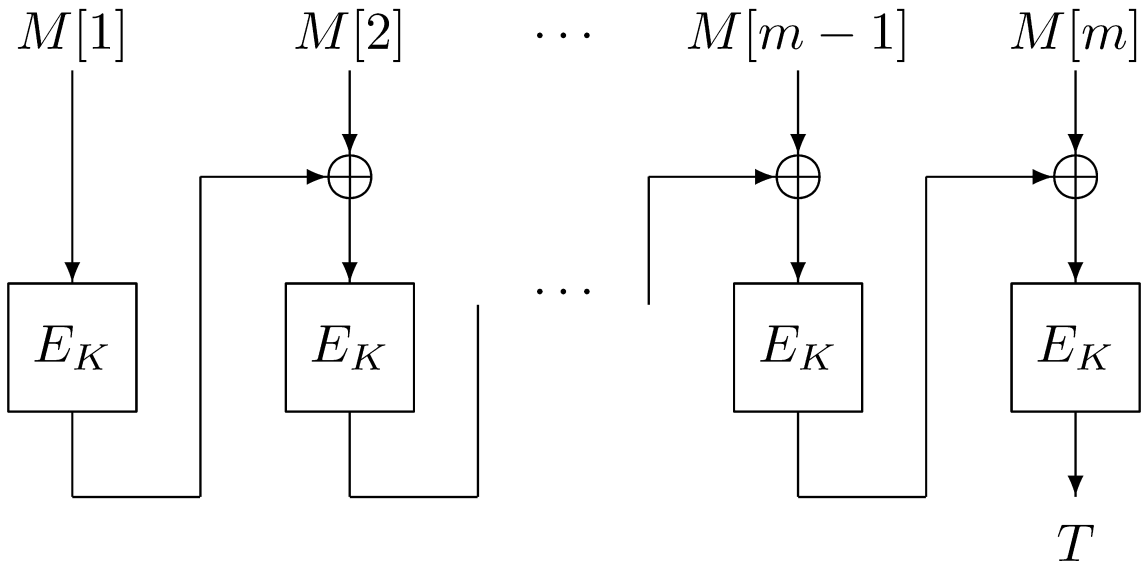
- SP 800-38A, Dec 2001, ECB, CBC, CFB, OFB, CTR
  - Oct 2010, Ciphertext stealing for CBC
- SP 800-38B, May 2005, CMAC
- SP 800-38C, May 2004, CCM
- SP 800-38D, Nov 2007, GCM and GMAC
- SP 800-38E, Jan 2010, XTS-AES
- SP 800-38F, Dec 2012, AES Key Wrap (KW) and AES KW with Padding (KWP)
- SP 800-38G, Mar 2016, FF1 and FF3, for format-preserving encryption

Outline

- AES-CMAC and Rijndael-256-CMAC
- AES-GCM and Rijndael-256-GCM

Development of CMAC

- CBC-MAC: a message authenticate code based on a block cipher



Development of CMAC

- Issues of the basic CBC-MAC and its variants (-2000)
  - does not cover variable-length input
    - Length-extension attack
  - does not cover arbitrarily input length
  - birthday bound security
  - key length
  - number of block cipher calls
  - …

Development of CMAC

- Development of AES (1997-2001) and NIST modes development (2000-ongoing) triggered a few proposals
- 2000-
  - XCBC [BR00]
  - RMAC [JJV02]
  - TMAC [KI03]
  - OMAC [IK03]
  - …

[BR00] Black and Rogaway. CBC MACs for arbitrary-length messages: the three-key construction. CRYPTO 2000.

[JJV02] Jaulmes, Joux, and Valette. On the security of randomized CBC-MAC beyond the birthday paradox limit: A new construction. FSE 2002.

[KI03] Kurosawa and Iwata. TMAC: Two-key CBC MAC. CT-RSA 2003.

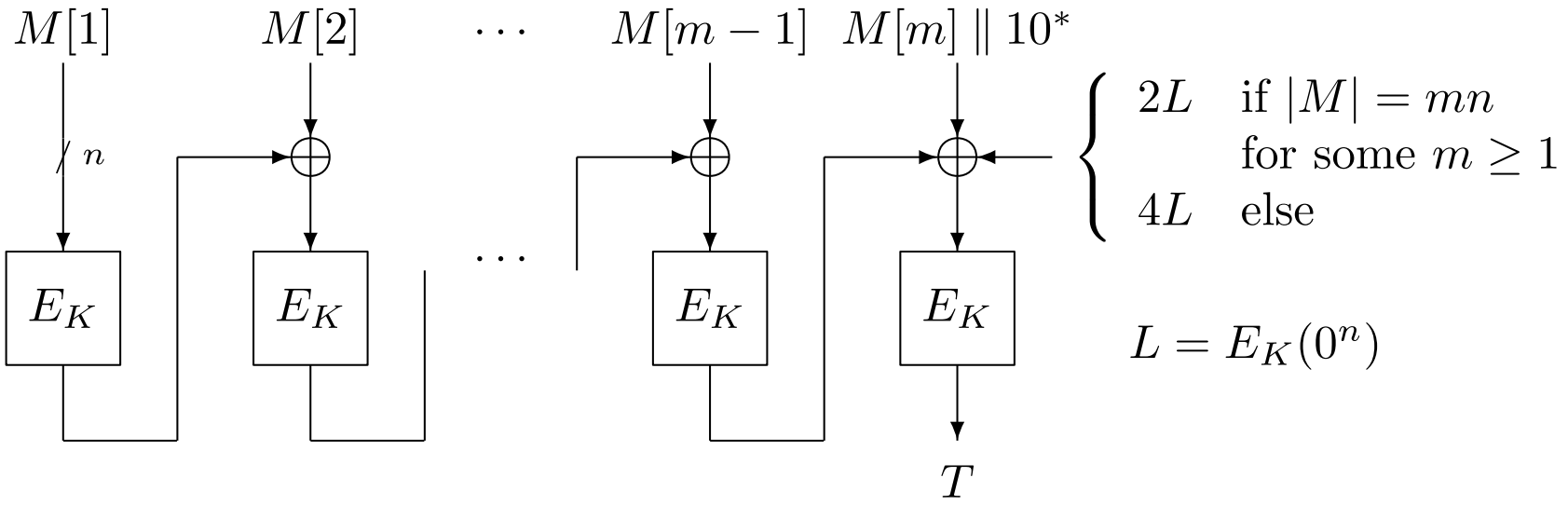
[IK03] Iwata and Kurosawa. OMAC: One-key CBC MAC. FSE 2003.

Development of CMAC

- NIST modes development (2000-ongoing)
- 6 MAC proposals (-2002)
  - OMAC, PMAC, RMAC, TMAC, XCBC, XECB
- NIST eventually selected OMAC in 2005 in NIST SP 800-38B, and named it CMAC for Cipher-based MAC
  - “The core of the CMAC algorithm is a variation of CBC-MAC that Black and Rogaway proposed and analyzed under the name XCBC in Ref. [2] …
    Iwata and Kurosawa proposed an improvement of XCBC and named the resulting algorithm One-Key CBC-MAC (OMAC) in Ref. [6] …
    The OMAC1 variation efficiently reduces the key size of XCBC. CMAC is equivalent to OMAC1.” [NIST SP 800-38B]

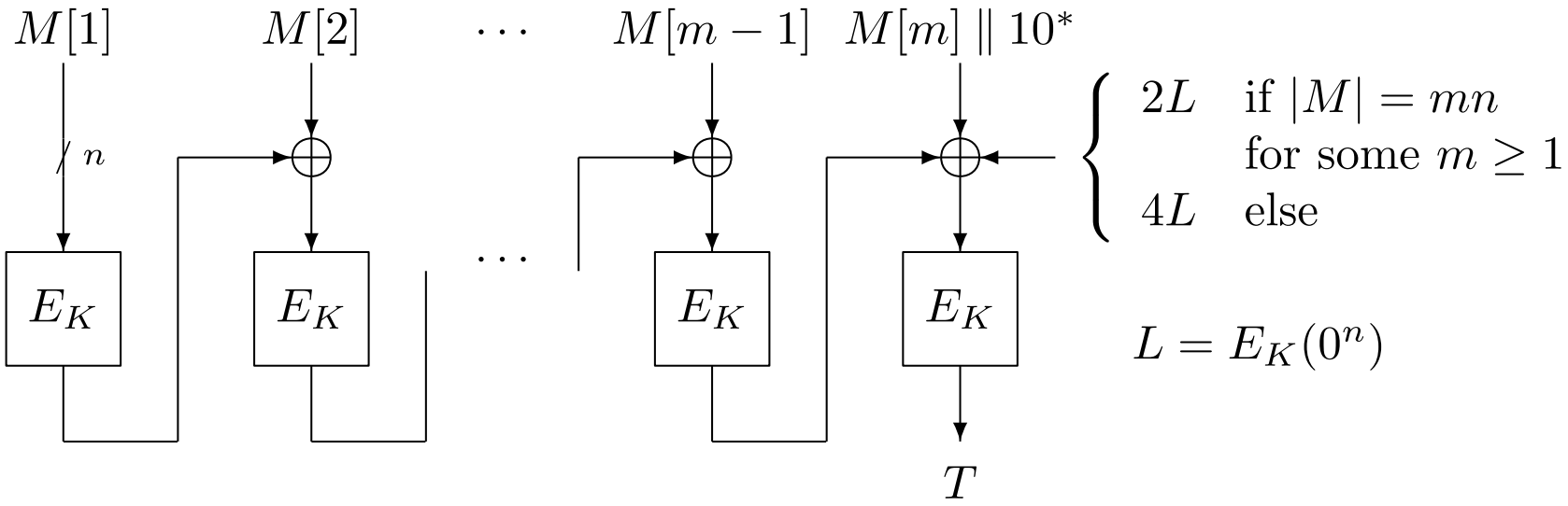
OMAC [IK03]

- Key $= K, k$ bits
- $1 + \lceil |M|/n \rceil$ block cipher calls



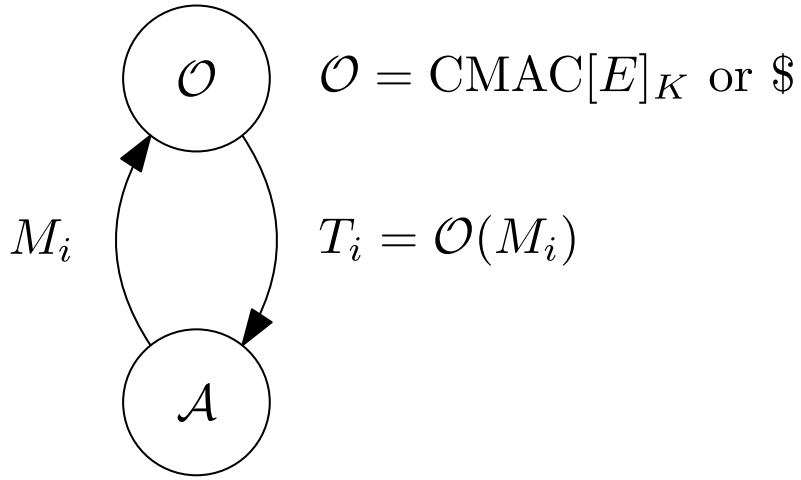
Proving the Security of CMAC

- Goal: CMAC ≈ random function
- $M[1] = 0^n$ implies L appears in the MAC computation
  - has to deal with the dependency



Proving the Security of CMAC

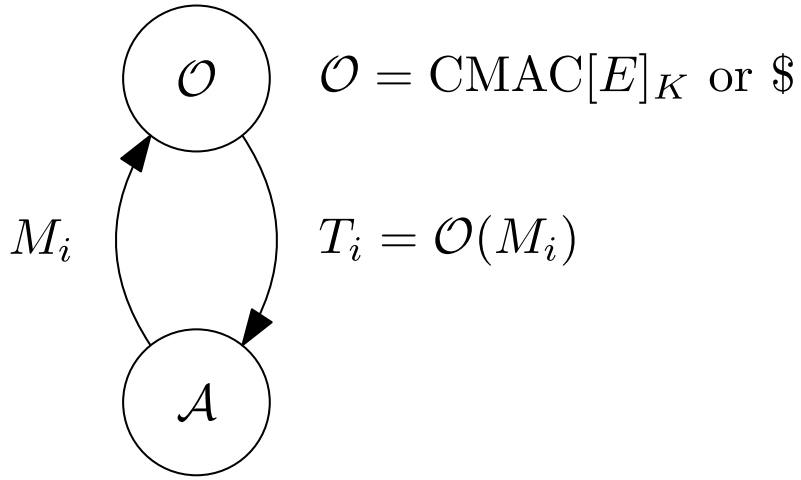
- Goal: CMAC ≈ random function
- Approach: $\mathrm{CMAC}[E]_K \approx \mathrm{CMAC}[P] \approx$ random function \$



Proving the Security of CMAC

- q: number of queries, σ: total number of blocks in all the queries, ℓ: the max block-length among the queries
  - $M_1 = M_1[1] \,||\, M_1[2] \,||\, M_1[3]$
  - $M_2 = M_2[1] \,||\, M_2[2]$
  - $M_3 = M_3[1] \,||\, M_3[2] \,||\, M_3[3] \,||\, M_3[4]$

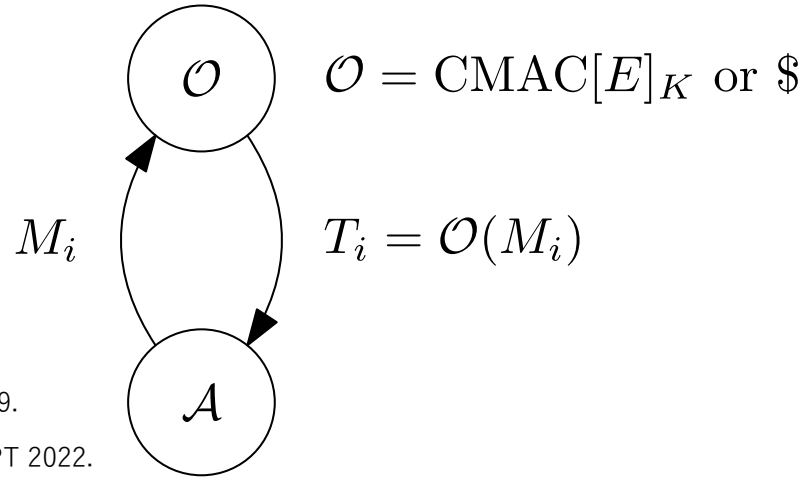
    $\Rightarrow \quad q = 3, \sigma = 9, \ell = 4$
- Original security bound [IK03]: $O(\ell^2 q^2 \,/\, 2^n)$



Proving the Security of CMAC

- q: number of queries, σ: total number of blocks in all the queries, ℓ: the max block-length among the queries
  - $M_1 = M_1[1] \,||\, M_1[2] \,||\, M_1[3]$
  - $M_2 = M_2[1] \,||\, M_2[2]$
  - $M_3 = M_3[1] \,||\, M_3[2] \,||\, M_3[3] \,||\, M_3[4]$

    $\Rightarrow \quad q = 3, \sigma = 9, \ell = 4$
- Original security bound [IK03]: $O(\ell^2 q^2 \,/\, 2^n)$
- Bound in [IK04]: $O(\sigma^2 \,/\, 2^n)$
- Bound in [Nan09]: $O(q\sigma \,/\, 2^n)$ if $\ell < 2^{n/3}$
- Bound in [CJN22]: $O(q^2 / 2^n \;+\; q\ell^2 \,/\, 2^n)$



[Nan09] Nandi. Improved security analysis for OMAC as a pseudorandom function. J. Mathematical Cryptol., 2009.

[CJN22] Chattopadhyay, Jha, and Nandi. Towards Tight Security Bounds for OMAC, XCBC and TMAC. ASIACRYPT 2022.

Proving the Security of CMAC

- Bound in [IK04]: $O(\sigma^2 / 2^n)$

$$\mathbf{Adv}^{\mathrm{prf}}_{\mathrm{CMAC}[E]}(\mathcal{A}) \leq \mathbf{Adv}^{\mathrm{prp}}_{E}(\mathcal{A}') + \frac{4\sigma^2}{2^n}$$

- If E = AES

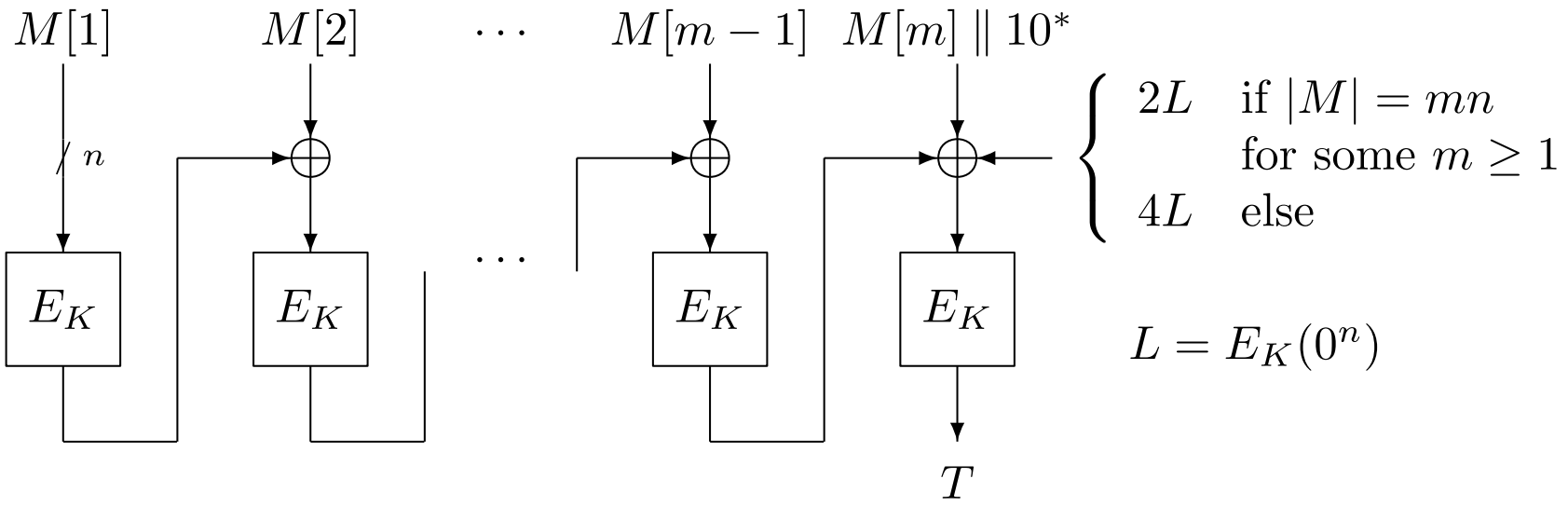
$$\mathbf{Adv}^{\mathrm{prf}}_{\mathrm{CMAC}[\mathrm{AES}]}(\mathcal{A}) \leq \mathbf{Adv}^{\mathrm{prp}}_{\mathrm{AES}}(\mathcal{A}') + \frac{4\sigma^2}{2^{128}}$$

- If E = Rijndael-256

$$\mathbf{Adv}^{\mathrm{prf}}_{\mathrm{CMAC}[\text{Rijndael-256}]}(\mathcal{A}) \leq \mathbf{Adv}^{\mathrm{prp}}_{\text{Rijndael-256}}(\mathcal{A}') + \frac{4\sigma^2}{2^{256}}$$

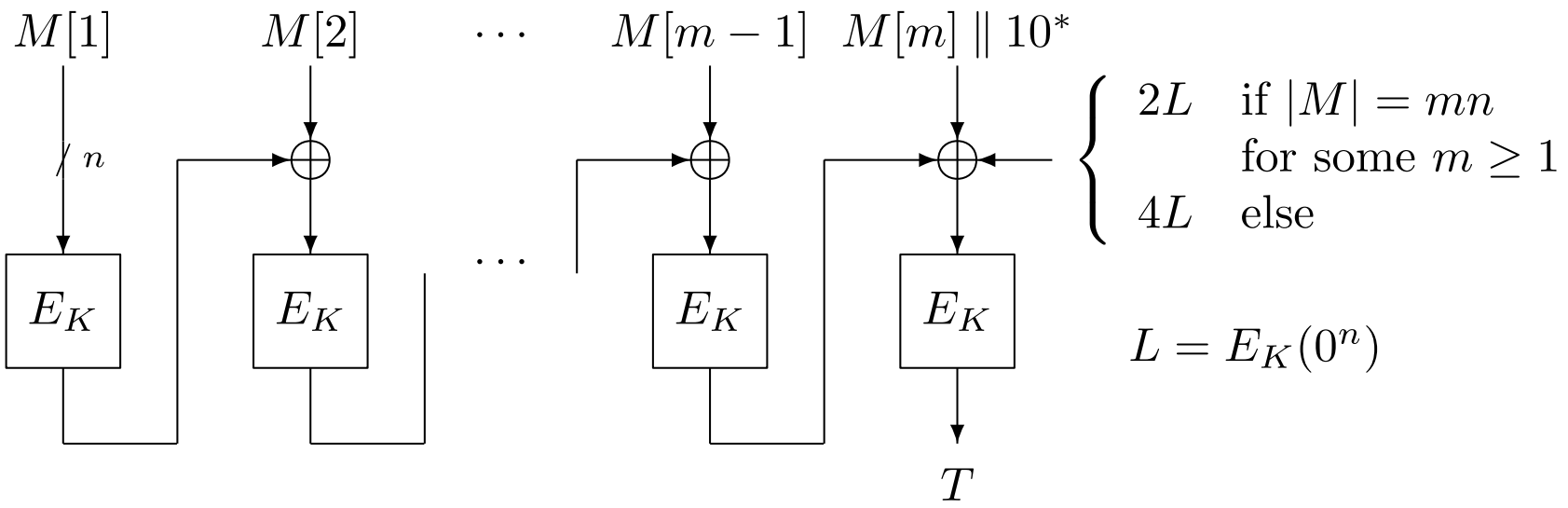
CMAC with AES

- $E = \text{AES}, n = 128$
- $2L$ and $4L$ are computed over $\text{GF}(2^{128})$



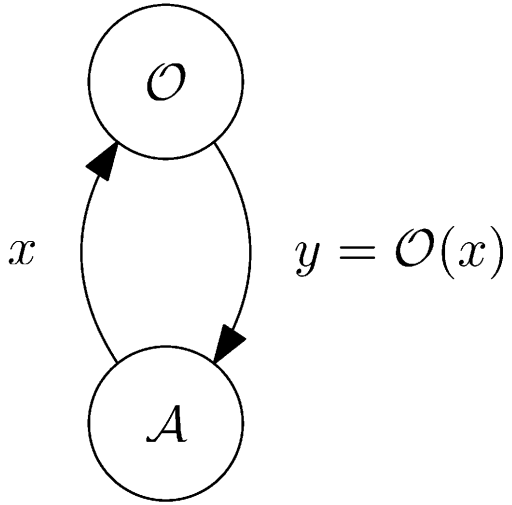
CMAC with Rijndael-256

- E = Rindael-256, $n = 256$
- $2L$ and $4L$ are computed over GF(2^{256})



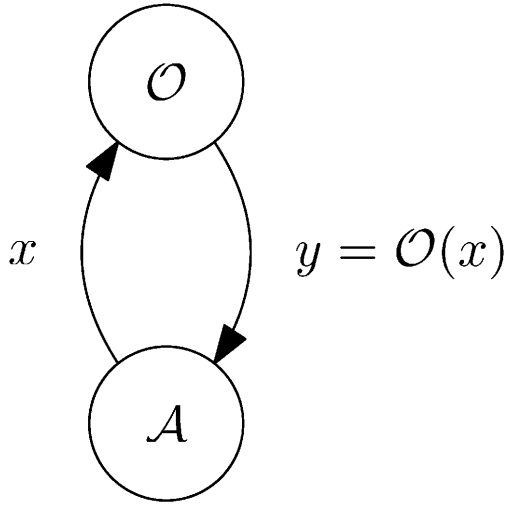
Quantum Attacks

Classical model



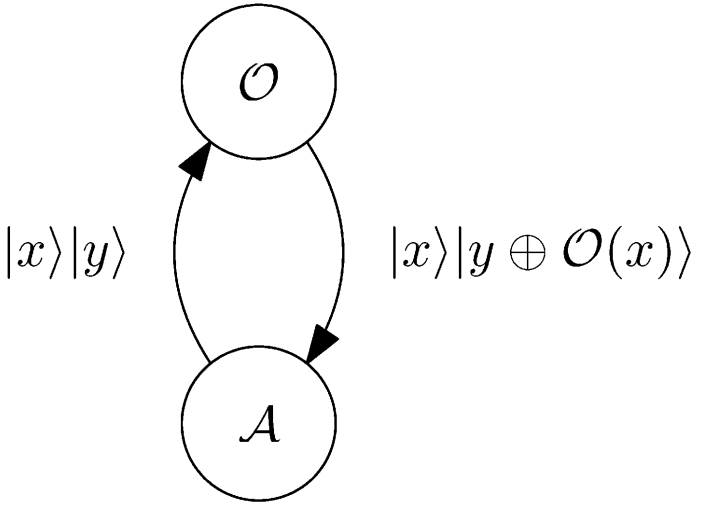
Classical computer

Q1 model



Quantum computer

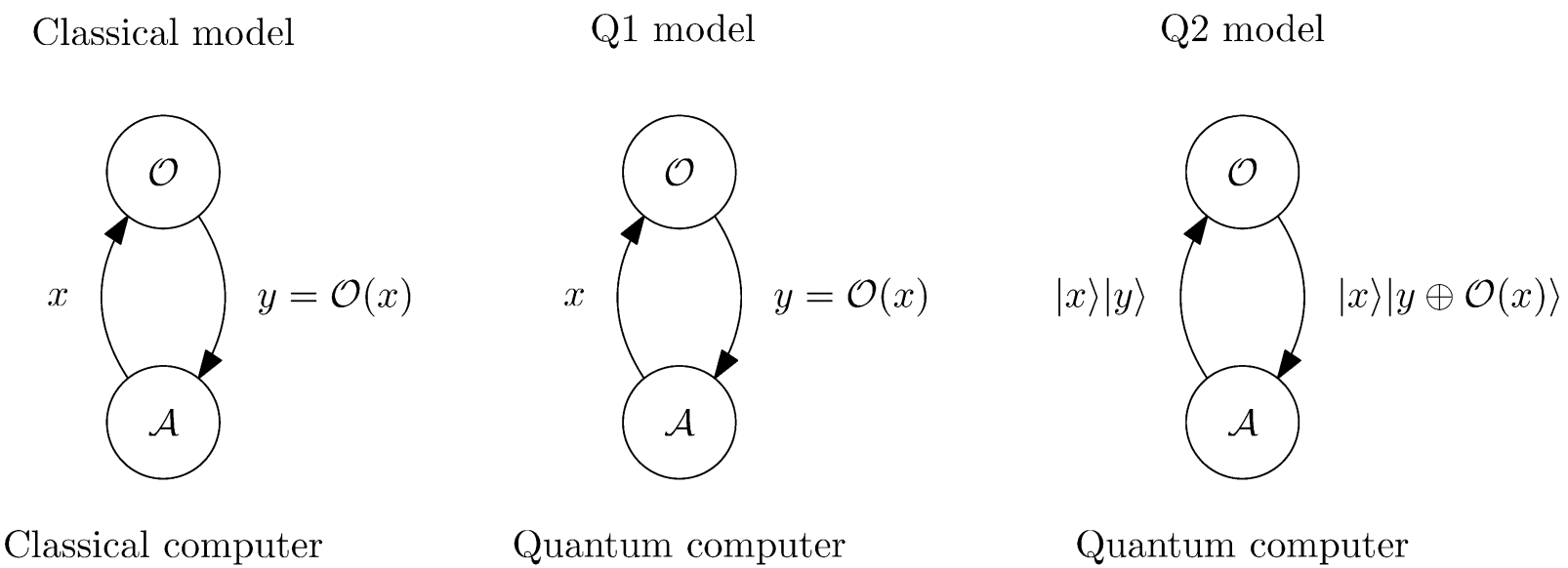
Q2 model



Quantum computer

Quantum Attacks

- CMAC is insecure in Q2 model [KLL+16, SS17]
  - A periodic function can be defined for CMAC, sufficient for existential forgery

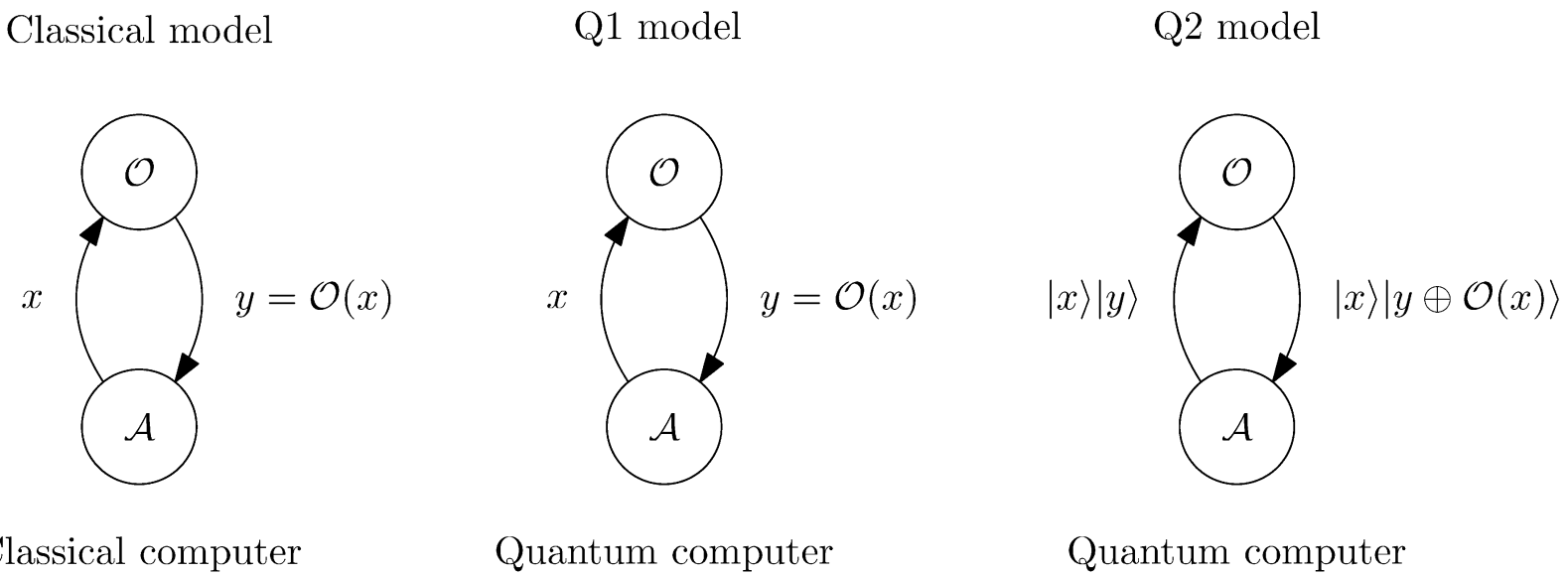


[KLL+16] Kaplan, Leurent, Leverrier, Naya-Plasencia. Breaking symmetric cryptosystems using quantum period finding. CRYPTO 2016.

[SS17] Santoli and Schaffner. Using Simon's algorithm to attack symmetric-key cryptographic primitives. Quant. Inf. Comput., 2017.

Quantum Attacks

- CMAC is insecure in Q2 model [KLL+16, SS17]
- However, in Q1 model, CMAC maintains provable security up to the birthday bound, assuming that the block cipher is secure in Q1 model



[KLL+16] Kaplan, Leurent, Leverrier, Naya-Plasencia. Breaking symmetric cryptosystems using quantum period finding. CRYPTO 2016.

[SS17] Santoli and Schaffner. Using Simon's algorithm to attack symmetric-key cryptographic primitives. Quant. Inf. Comput., 2017.

Security of CMAC in Q1 Model

- CMAC is insecure in Q2 model
- However, in Q1 model, CMAC maintains provable security up to the birthday bound, assuming that the block cipher is secure in Q1 model, following [MS17]

$$\mathbf{Adv}^{\text{q1-prf}}_{\text{CMAC}[E]}(\mathcal{A}) \leq \mathbf{Adv}^{\text{q1-prp}}_{E}(\mathcal{A}') + \frac{4\sigma^2}{2^n}$$

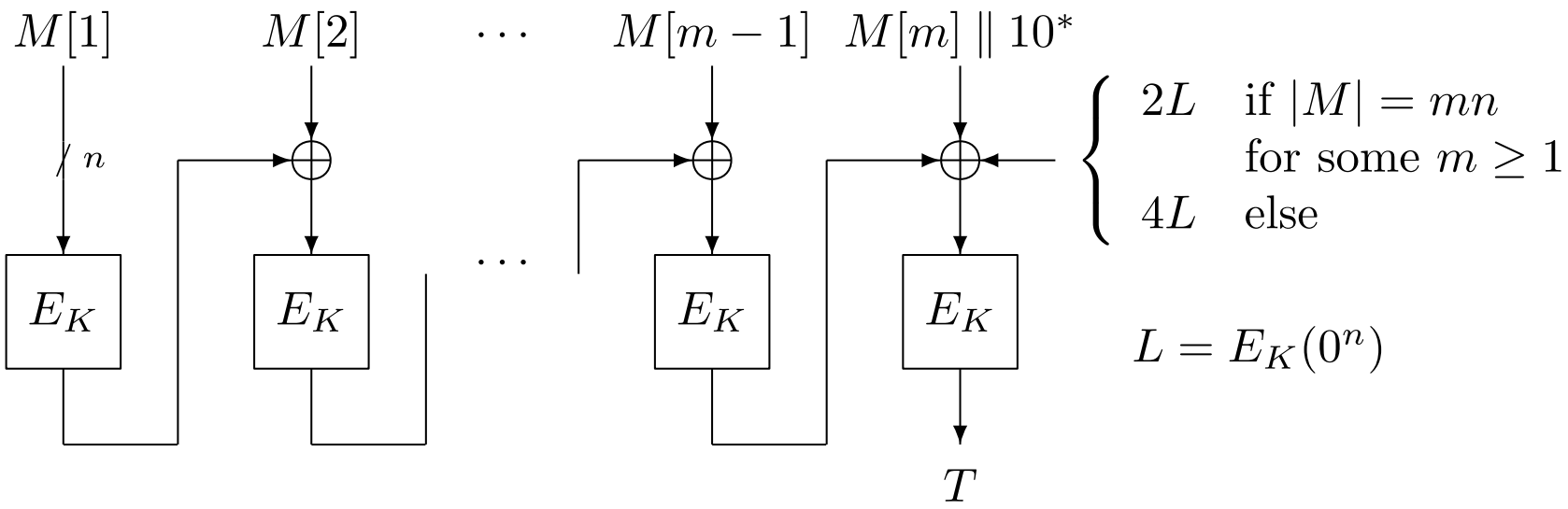
$$\mathbf{Adv}^{\text{q1-prf}}_{\text{CMAC}[\text{AES}]}(\mathcal{A}) \leq \mathbf{Adv}^{\text{q1-prp}}_{\text{AES}}(\mathcal{A}') + \frac{4\sigma^2}{2^{128}}$$

$$\mathbf{Adv}^{\text{q1-prf}}_{\text{CMAC}[\text{Rijndael-256}]}(\mathcal{A}) \leq \mathbf{Adv}^{\text{q1-prp}}_{\text{Rijndael-256}}(\mathcal{A}') + \frac{4\sigma^2}{2^{256}}$$

[MS17] Mennink and Szepieniec. XOR of PRPs in a Quantum World. PQCrypto 2017.

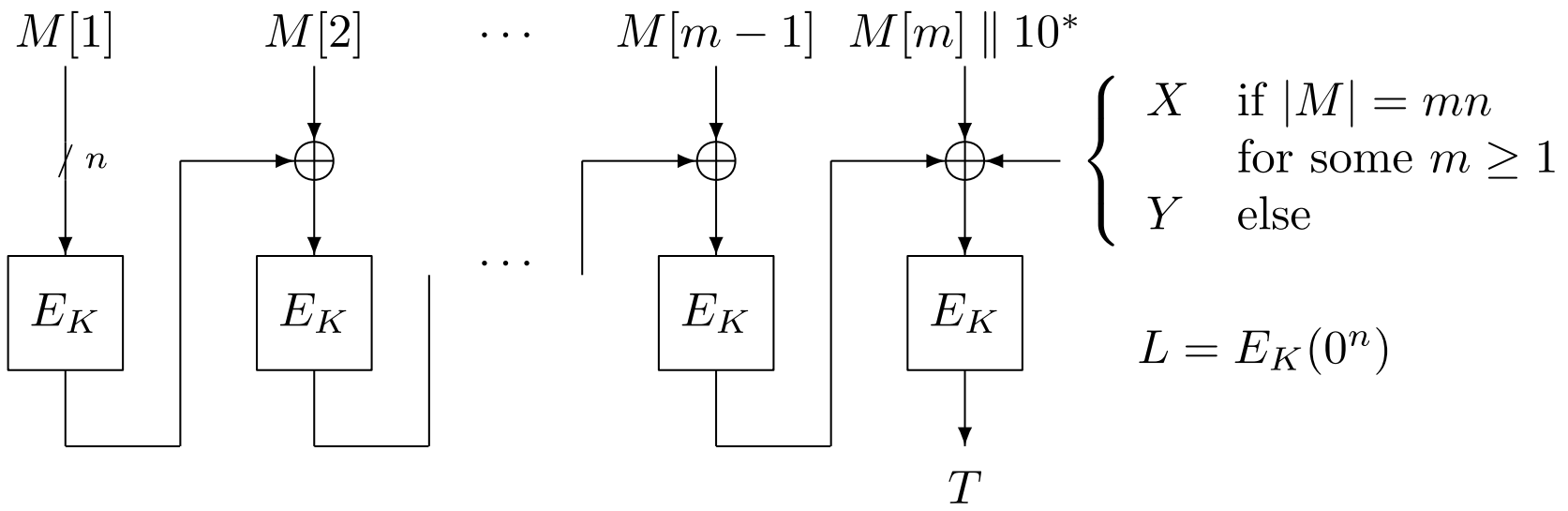
CMAC with Rijndael-256

- E = Rindael-256, $n = 256$
- $2L$ and $4L$ are computed over GF(2^{256})



CMAC with Rijndael-256

- Let $X = 2L$ and $Y = 4L$



CMAC with Rijndael-256

- Conditions on X and Y
  - For any c, if L is chosen uniformly at random,

$$\begin{cases} \Pr[X = c] \leq \epsilon \\ \Pr[Y = c] \leq \epsilon \\ \Pr[X \oplus Y = c] \leq \epsilon \\ \Pr[X \oplus L = c] \leq \epsilon \\ \Pr[Y \oplus L = c] \leq \epsilon \\ \Pr[X \oplus Y \oplus L = c] \leq \epsilon \end{cases}$$

- These six conditions are necessary and sufficient for CMAC to be secure [Iwa03]

[Iwa03] Tetsu Iwata. Six conditions in OMAC-family are tight, Rump session talk at FSE 2003.

CMAC with Rijndael-256

- With $X = 2L$ and $Y = 4L$,

$$\begin{cases} \Pr[X = c] \leq \epsilon \\ \Pr[Y = c] \leq \epsilon \\ \Pr[X \oplus Y = c] \leq \epsilon \\ \Pr[X \oplus L = c] \leq \epsilon \\ \Pr[Y \oplus L = c] \leq \epsilon \\ \Pr[X \oplus Y \oplus L = c] \leq \epsilon \end{cases} \Rightarrow \begin{cases} \Pr[2L = c] \leq \epsilon \\ \Pr[4L = c] \leq \epsilon \\ \Pr[6L = c] \leq \epsilon \\ \Pr[3L = c] \leq \epsilon \\ \Pr[5L = c] \leq \epsilon \\ \Pr[7L = c] \leq \epsilon \end{cases}$$

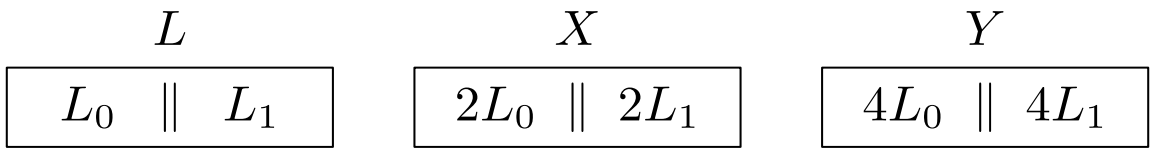
where $\epsilon = 1/2^n$

CMAC with Rijndael-256

- $X = 2L$ and $Y = 4L$ over GF(2^{256}) give $\epsilon = 1/2^{256}$ and work fine
  - Natural option for CMAC with Rijndael-256
- There are many other options that work

CMAC with Rijndael-256

- $L = E_K(0^{256}) = L_0 \parallel L_1 \in \{0,1\}^{128} \times \{0,1\}^{128}$
- $X = 2L_0 \parallel 2L_1$, $Y = 4L_0 \parallel 4L_1$ over GF(2^{128})
- This gives $\epsilon = 1/2^{256}$ and works



$$\begin{cases} \Pr[2L = c] \leq \epsilon \\ \Pr[4L = c] \leq \epsilon \\ \Pr[6L = c] \leq \epsilon \\ \Pr[3L = c] \leq \epsilon \\ \Pr[5L = c] \leq \epsilon \\ \Pr[7L = c] \leq \epsilon \end{cases}$$

CMAC with Rijndael-256

- $L = E_K(0^{256}) = L_0 \parallel L_1 \in \{0,1\}^{128} \times \{0,1\}^{128}$
- $X = 2L_0 \parallel 2L_1$, $Y = 4L_0 \parallel 4L_1$ over GF(2^{128})
- This gives $\epsilon = 1/2^{256}$ and works

L	X	Y
$L_0 \parallel L_1$	$2L_0 \parallel 2L_1$	$4L_0 \parallel 4L_1$

$$\begin{cases} \Pr[2L = c] \leq \epsilon \\ \Pr[4L = c] \leq \epsilon \\ \Pr[6L = c] \leq \epsilon \\ \Pr[3L = c] \leq \epsilon \\ \Pr[5L = c] \leq \epsilon \\ \Pr[7L = c] \leq \epsilon \end{cases}$$

- L can be broken into smaller words
- $L = L_0 \parallel L_1 \parallel L_2 \parallel L_3 \in (\{0,1\}^{64})^4$
- $X = 2L_0 \parallel 2L_1 \parallel 2L_2 \parallel 2L_3$, $Y = 4L_0 \parallel 4L_1 \parallel 4L_2 \parallel 4L_3$ over GF(2^{64})
- This gives $\epsilon = 1/2^{256}$ and works

CMAC with Rijndael-256

- Consider the case that L is broken into 64-bit words
  - $L = L_0 \parallel L_1 \parallel L_2 \parallel L_3 \in (\{0,1\}^{64})^4$
- Let $L_{[0..3]} = L_0 \oplus L_1 \oplus L_2 \oplus L_3$
- $X = L_1 \parallel L_2 \parallel L_3 \parallel L_{[0..3]}$, $Y = L_2 \parallel L_3 \parallel L_{[0..3]} \parallel L_0$
- This works, using only XOR and word shift

CMAC with Rijndael-256

$$\begin{cases} X = L_1 \parallel L_2 \parallel L_3 \parallel L_{[0..3]} \\ Y = L_2 \parallel L_3 \parallel L_{[0..3]} \parallel L_0 \end{cases}$$

$$\begin{cases} X = \begin{bmatrix} L_0 & L_1 & L_2 & L_3 \end{bmatrix} \cdot M_X \\ Y = \begin{bmatrix} L_0 & L_1 & L_2 & L_3 \end{bmatrix} \cdot M_Y \end{cases}$$

$$\text{where} \quad M_X = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{bmatrix} \quad \text{and} \quad M_Y = \begin{bmatrix} 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 \end{bmatrix}$$

CMAC with Rijndael-256

X	M_X
Y	M_Y
$X \oplus Y$	$M_X \oplus M_Y$
$X \oplus L$	$M_X \oplus I$
$Y \oplus L$	$M_Y \oplus I$
$X \oplus Y \oplus L$	$M_X \oplus M_Y \oplus I$

$$\begin{cases} \Pr[X = c] \leq \epsilon \\ \Pr[Y = c] \leq \epsilon \\ \Pr[X \oplus Y = c] \leq \epsilon \\ \Pr[X \oplus L = c] \leq \epsilon \\ \Pr[Y \oplus L = c] \leq \epsilon \\ \Pr[X \oplus Y \oplus L = c] \leq \epsilon \end{cases}$$

$$M_X \begin{bmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{bmatrix} \quad M_Y \begin{bmatrix} 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 \end{bmatrix} \quad M_X \oplus M_Y \begin{bmatrix} 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 \end{bmatrix} \quad M_X \oplus L \begin{bmatrix} 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \quad M_Y \oplus L \begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 \end{bmatrix} \quad M_X \oplus M_Y \oplus L \begin{bmatrix} 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 \end{bmatrix}$$

- All six matrices are full rank
- For each condition, one value of L satisfies the equality, $\epsilon = 1/2^{256}$

CMAC with Rijndael-256

- More options

$$L = L_0 \parallel L_1 \parallel L_2 \parallel L_3 \in \{0,1\}^{256}, L_i \in \{0,1\}^{64}, L_{[a,b]} = L_a \oplus L_b$$

$$\begin{cases} X = L_2 \parallel L_{[2,3]} \parallel L_1 \parallel L_0 \\ Y = L_3 \parallel L_2 \parallel L_{[0,1]} \parallel L_1 \end{cases}$$

CMAC with Rijndael-256

- More options

$$L = L_0 \parallel L_1 \parallel \cdots \parallel L_7 \in \{0,1\}^{256}, L_i \in \{0,1\}^{32}$$

$$\begin{cases} X = L_1 \parallel L_2 \parallel L_3 \parallel L_{[0..3]} \parallel L_5 \parallel L_6 \parallel L_7 \parallel L_{[4..7]} \\ Y = L_2 \parallel L_3 \parallel L_{[0..3]} \parallel L_0 \parallel L_6 \parallel L_7 \parallel L_{[4..7]} \parallel L_4 \end{cases}$$

$$\begin{cases} X = L_2 \parallel L_{[2,3]} \parallel L_1 \parallel L_0 \parallel L_6 \parallel L_{[6,7]} \parallel L_5 \parallel L_4 \\ Y = L_3 \parallel L_2 \parallel L_{[0,1]} \parallel L_1 \parallel L_7 \parallel L_6 \parallel L_{[4,5]} \parallel L_5 \end{cases}$$

$$\begin{cases} X = L_1 \parallel L_2 \parallel L_3 \parallel L_4 \parallel L_5 \parallel L_6 \parallel L_7 \parallel L_{[0,1]} \\ Y = L_2 \parallel L_3 \parallel L_4 \parallel L_5 \parallel L_6 \parallel L_7 \parallel L_{[0,1]} \parallel L_{[1,2]} \end{cases}$$

CMAC with Rijndael-256

- It can be naturally defined
- The security follows from existing works
  - Birthday bound secure in the classical setting (128-bit secure)
  - Birthday bound secure in the Q1 setting (128-bit secure, assuming that Rijndael-256 is Q1 secure)
  - Insecure in the Q2 setting (irrelevant to the security of Rijndael-256)
- Using $X = 2L$ and $Y = 4L$ over $\mathrm{GF}(2^{256})$ works fine, but the definition of the mask could be explored

Outline

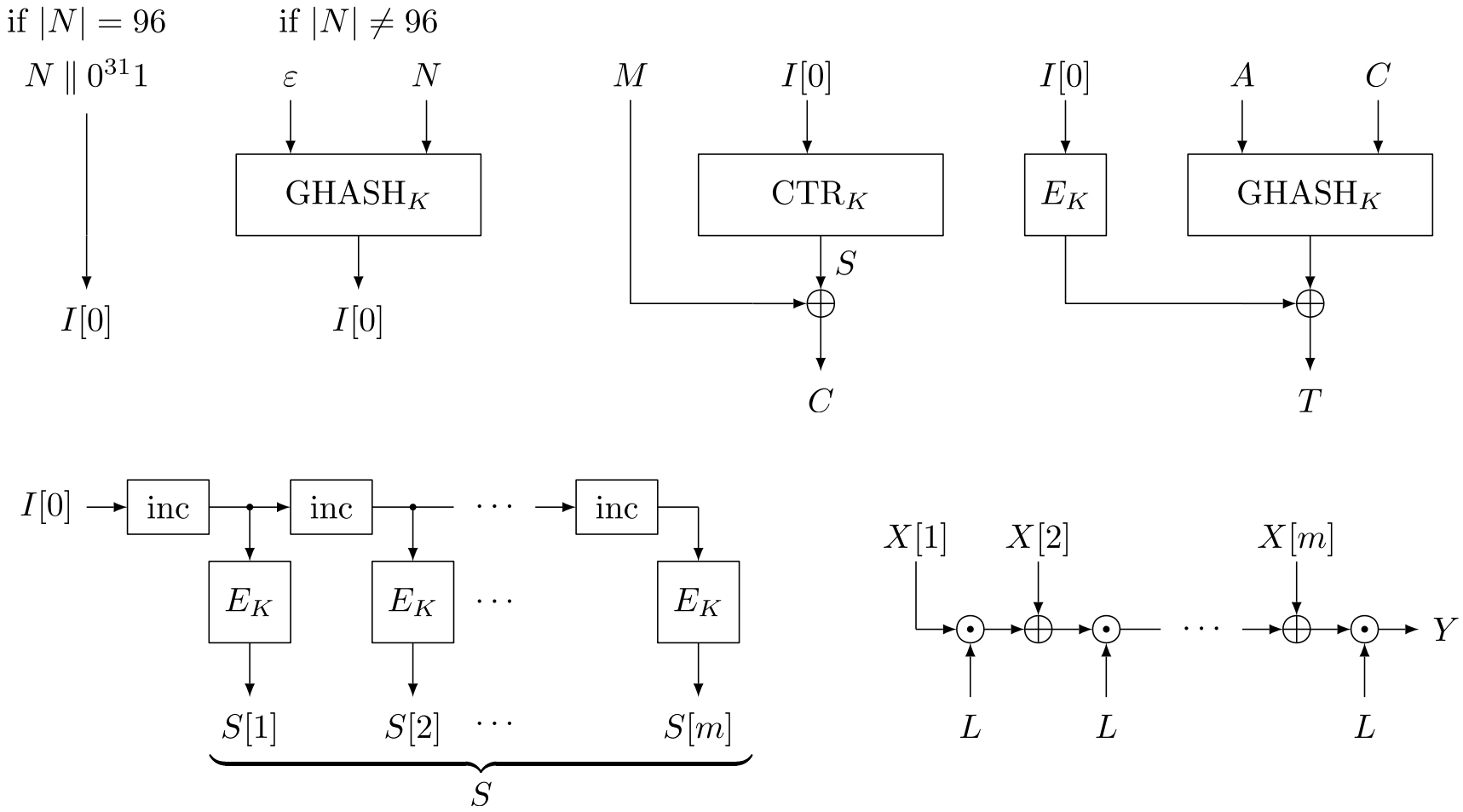
- AES-CMAC and Rijndael-256-CMAC
- AES-GCM and Rijndael-256-GCM

AES-GCM, Rijndael-256-GCM

- GCM, Galois/Counter Mode, an authenticated encryption with associated data (AEAD) scheme for 128-bit block ciphers
- Designed by McGrew and Viega in 2004 [MV04]
- Selected as the NIST recommended authenticated encryption mode in 2007 in NIST SP 800-38D
- Widely used in practice
  - ISO/IEC 19772, IEEE P1619.1, NSA Suite B, IETF IPsec, SSH, SSL,...

[MV04] David A. McGrew and John Viega. The Security and Performance of the Galois/Counter Mode (GCM) of Operation. Cryptology ePrint Archive: Report 2004/193 (full version of INDOCRYPT 2004).

Overview of GCM



Security Analysis

- [Ferguson, ’05]
  - Forgery attacks when the tag is short
- [Joux, ’06]
  - Key recovery attacks on GCM (nonce reuse), forgery
  - Attacks on the draft NIST version of GCM
- [Handschuh, Preneel, ’08]
  - A weak key, forgery attacks
- [Saarinen, ’12]
  - Many weak keys, forgery attacks (cycling attack)
- [Procter, Cid, ’15]
  - Generalization weak key classes and of the cycling attack

Provable Security

- [McGrew, Viega, '04]
  - Initial provable security proof
- [Iwata, Ohashi, Minematsu, '12]
  - Pointed out a gap in the proof of [McGrew, Viega '04]
  - Corrected proofs
    - separating the case for $|N| = 96$ and $|N| \neq 96$, with security bounds containing 2^{22} for the latter
- [Niwa, Ohashi, Minematsu, Iwata, '15]
  - Improved provable security bound for $|N| \neq 96$, reducing 2^{22} to 2^5
- [Hoang, Tessaro, Thiruvengadam, '18]
  - Multi-user security in the ideal cipher model

Provable Security Bounds in [IOM12] and [NOMI15]

$$[\mathrm{IOM12}] \quad |N| = 96, \quad \mathbf{Adv}^{\mathrm{priv}}_{\mathrm{GCM}[E,\tau]}(\mathcal{A}) \leq \mathbf{Adv}^{\mathrm{prp}}_{E}(\mathcal{A}') + \frac{0.5(\sigma + q + 1)^2}{2^n}$$

$$[\mathrm{IOM12}] \quad |N| \neq 96, \quad \mathbf{Adv}^{\mathrm{priv}}_{\mathrm{GCM}[E,\tau]}(\mathcal{A}) \leq \mathbf{Adv}^{\mathrm{prp}}_{E}(\mathcal{A}') + \frac{0.5(\sigma + q + 1)^2}{2^n} + \frac{2^{22} q(\sigma + q)(\ell_N + 1)}{2^n}$$

$$[\mathrm{NOMI15}] \quad |N| \neq 96, \quad \mathbf{Adv}^{\mathrm{priv}}_{\mathrm{GCM}[E,\tau]}(\mathcal{A}) \leq \mathbf{Adv}^{\mathrm{prp}}_{E}(\mathcal{A}') + \frac{0.5(\sigma + q + 1)^2}{2^n} + \frac{2^{5} q(\sigma + q)(\ell_N + 1)}{2^n}$$

Provable Security Bounds in [IOM12] and [NOMI15]

$$\text{[IOM12]}\quad |N| = 96,\quad \mathbf{Adv}^{\text{auth}}_{\text{GCM}[E,\tau]}(\mathcal{A}) \le \mathbf{Adv}^{\text{prp}}_{E}(\mathcal{A}') + \frac{0.5(\sigma + q + q' + 1)^2}{2^n} + \frac{q'(\ell_A + 1)}{2^\tau}$$

$$\text{[IOM12]}\quad |N| \neq 96,\quad \mathbf{Adv}^{\text{auth}}_{\text{GCM}[E,\tau]}(\mathcal{A}) \le \mathbf{Adv}^{\text{prp}}_{E}(\mathcal{A}') + \frac{0.5(\sigma + q + q' + 1)^2}{2^n} + \frac{2^{22}(q + q')(\sigma + q + 1)(\ell_N + 1)}{2^n} + \frac{q'(\ell_A + 1)}{2^\tau}$$

$$\text{[NOMI15]}\quad |N| \neq 96,\quad \mathbf{Adv}^{\text{auth}}_{\text{GCM}[E,\tau]}(\mathcal{A}) \le \mathbf{Adv}^{\text{prp}}_{E}(\mathcal{A}') + \frac{0.5(\sigma + q + q' + 1)^2}{2^n} + \frac{2^{5}(q + q')(\sigma + q + 1)(\ell_N + 1)}{2^n} + \frac{q'(\ell_A + 1)}{2^\tau}$$

Provable Security Bounds in [IOM12] and [NOMI15]

- These bounds cover $E = \mathrm{AES}$ $(n = 128)$
- For AES:

$$[\mathrm{IOM12}] \quad |N| = 96, \quad \mathbf{Adv}^{\mathrm{priv}}_{\mathrm{GCM}[\mathrm{AES},\tau]}(\mathcal{A}) \leq \mathbf{Adv}^{\mathrm{prp}}_{\mathrm{AES}}(\mathcal{A}') + \frac{0.5(\sigma + q + 1)^2}{2^{128}}$$

$$[\mathrm{NOMI15}] \quad |N| \neq 96, \quad \mathbf{Adv}^{\mathrm{priv}}_{\mathrm{GCM}[\mathrm{AES},\tau]}(\mathcal{A}) \leq \mathbf{Adv}^{\mathrm{prp}}_{\mathrm{AES}}(\mathcal{A}') + \frac{0.5(\sigma + q + 1)^2}{2^{128}} + \frac{2^5 q(\sigma + q)(\ell_N + 1)}{2^{128}}$$

$$[\mathrm{IOM12}] \quad |N| = 96, \quad \mathbf{Adv}^{\mathrm{auth}}_{\mathrm{GCM}[\mathrm{AES},\tau]}(\mathcal{A}) \leq \mathbf{Adv}^{\mathrm{prp}}_{\mathrm{AES}}(\mathcal{A}') + \frac{0.5(\sigma + q + q' + 1)^2}{2^{128}} + \frac{q'(\ell_A + 1)}{2^{\tau}}$$

$$[\mathrm{NOMI15}] \quad |N| \neq 96, \quad \mathbf{Adv}^{\mathrm{auth}}_{\mathrm{GCM}[\mathrm{AES},\tau]}(\mathcal{A}) \leq \mathbf{Adv}^{\mathrm{prp}}_{\mathrm{AES}}(\mathcal{A}') + \frac{0.5(\sigma + q + q' + 1)^2}{2^{128}} + \frac{2^5 (q + q')(\sigma + q + 1)(\ell_N + 1)}{2^{128}} + \frac{q'(\ell_A + 1)}{2^{\tau}}$$

- Also valid in Q1 setting

Provable Security Bounds in [IOM12] and [NOMI15]

- For Rijdael-256:

$$[\mathrm{IOM12}]\quad |N| = 96,\quad \mathbf{Adv}^{\mathrm{priv}}_{\mathrm{GCM[Rijndael\text{-}256},\tau]}(\mathcal{A}) \leq \mathbf{Adv}^{\mathrm{prp}}_{\mathrm{Rijndael\text{-}256}}(\mathcal{A}') + \frac{0.5(\sigma + q + 1)^2}{2^{256}}$$

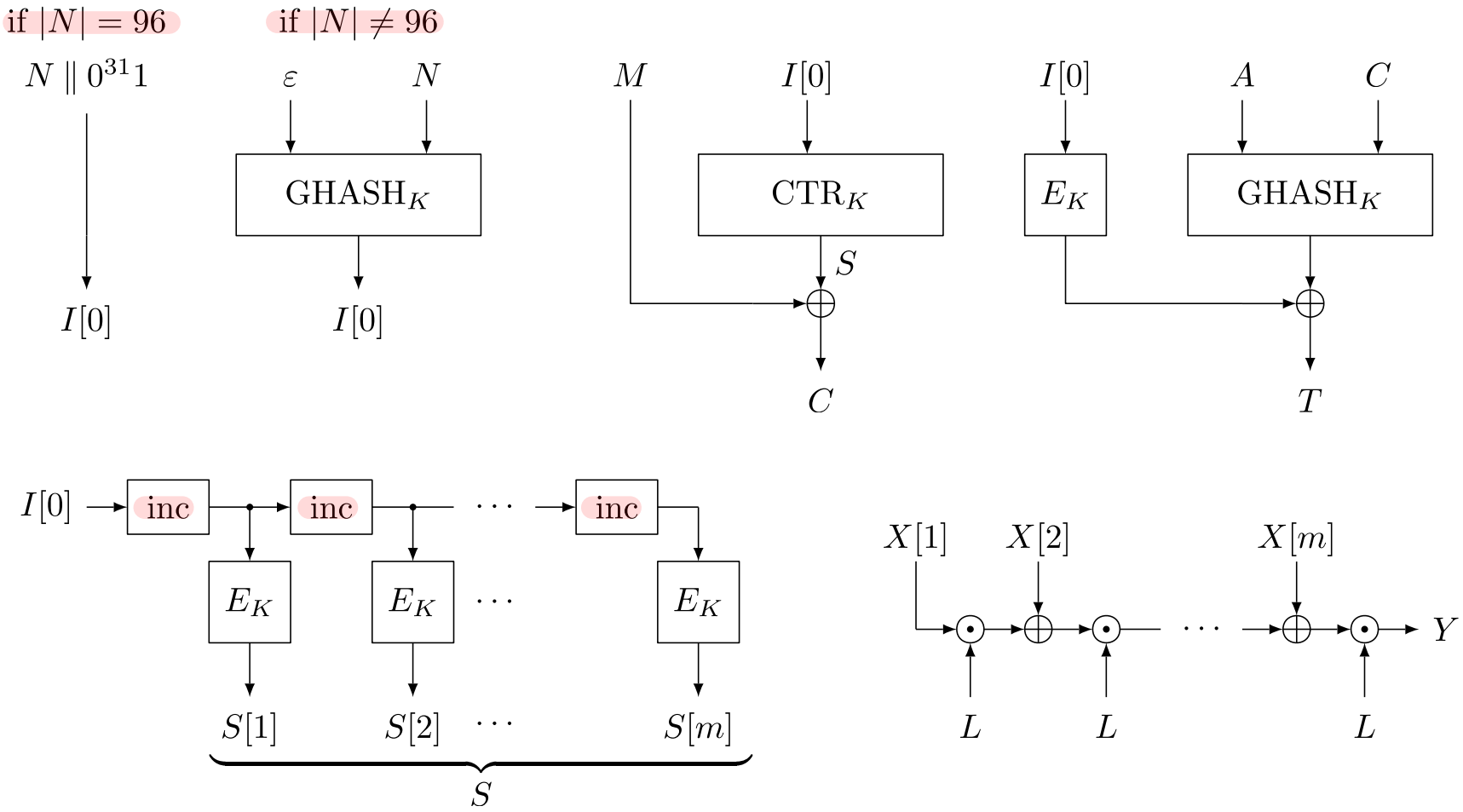
$$[\mathrm{NOMI15}]\ |N| \neq 96,\quad \mathbf{Adv}^{\mathrm{priv}}_{\mathrm{GCM[Rijndael\text{-}256},\tau]}(\mathcal{A}) \leq \mathbf{Adv}^{\mathrm{prp}}_{\mathrm{Rijndael\text{-}256}}(\mathcal{A}') + \frac{0.5(\sigma + q + 1)^2}{2^{256}} + \frac{2^5 q(\sigma + q)(\ell_N + 1)}{2^{256}}$$

$$[\mathrm{IOM12}]\quad |N| = 96,\quad \mathbf{Adv}^{\mathrm{auth}}_{\mathrm{GCM[Rijndael\text{-}256},\tau]}(\mathcal{A}) \leq \mathbf{Adv}^{\mathrm{prp}}_{\mathrm{Rijndael\text{-}256}}(\mathcal{A}') + \frac{0.5(\sigma + q + q' + 1)^2}{2^{256}} + \frac{q'(\ell_A + 1)}{2^{\tau}}$$

$$[\mathrm{NOMI15}]\ |N| \neq 96,\quad \mathbf{Adv}^{\mathrm{auth}}_{\mathrm{GCM[Rijndael\text{-}256},\tau]}(\mathcal{A}) \leq \mathbf{Adv}^{\mathrm{prp}}_{\mathrm{Rijndael\text{-}256}}(\mathcal{A}') + \frac{0.5(\sigma + q + q' + 1)^2}{2^{256}} + \frac{2^5 (q + q')(\sigma + q + 1)(\ell_N + 1)}{2^{256}} + \frac{q'(\ell_A + 1)}{2^{\tau}}$$

- 96 is used as an absolute value, and inc increments the last 32 bits

Overview of GCM



How Do We Define Rijndael-256-GCM?

- [SP 800-38D] is for a 128-bit block cipher
- [MV04] covers an n-bit block cipher with $n \geq 64$ (the main focus seems to be $n = 128$ and 64)
  - $I[0] = N \parallel 0^{31}1$ if $|N| = n - 32$, $I[0] = \mathrm{GHASH}_L(\varepsilon, N)$ otherwise
  - inc increments the last 32 bits
  - Input of GHASH:
    $X[1], \ldots, X[m] = A[1] \parallel \cdots \parallel A[a]0^* \parallel C[1] \parallel \cdots \parallel C[c]0^* \parallel \mathrm{len}_{n/2}(A) \parallel \mathrm{len}_{n/2}(C)$
  - $Y = X[1]L^m \oplus X[2]L^{m-1} \oplus \cdots \oplus X[m]L$ over $\mathrm{GF}(2^n)$
  - With $n = 256$, the generation of $I[0]$ depends on whether $|N| = 224$ or not
  - One plaintext length is limited to $2^{32} - 2$ blocks (in a 256-bit block), not enough

How Do We Define Rijndael-256-GCM?

- [MV04]
  - $I[0] = N \parallel 0^{31}1$ if $|N| = n - 32$, $I[0] = \mathrm{GHASH}_L(\varepsilon, N)$ otherwise
  - inc increments the last 32 bits
- [IOM12, NOMI15]
  - $I[0] = N \parallel 0^{31}1$ if $|N| = 96$, $I[0] = \mathrm{GHASH}_L(\varepsilon, N)$ otherwise
  - inc increments the last 32 bits
- [AY12]
  - $I[0] = N \parallel 0^{31}1$ if $|N| = 3n/4$, $I[0] = \mathrm{GHASH}_L(\varepsilon, N)$ otherwise
  - inc increments the least $n/4$ bits
  - The parameter choice of [AY12] allows 192-bit nonces and inc works on 64 bits for $n = 256$

[AY12] Aoki, Yasuda. The Security and Performance of "GCM" when Short Multiplications Are Used Instead. Inscrypt 2012

Provable Security Bounds in [IOM12] and [NOMI15]

- For Rijdael-256:

$$[\text{IOM12}]\quad |N| = 96,\quad \mathbf{Adv}^{\text{priv}}_{\text{GCM[Rijndael-256},\tau]}(\mathcal{A}) \leq \mathbf{Adv}^{\text{prp}}_{\text{Rijndael-256}}(\mathcal{A}') + \frac{0.5(\sigma + q + 1)^2}{2^{256}}$$

$$[\text{NOMI15}]\ |N| \neq 96,\quad \mathbf{Adv}^{\text{priv}}_{\text{GCM[Rijndael-256},\tau]}(\mathcal{A}) \leq \mathbf{Adv}^{\text{prp}}_{\text{Rijndael-256}}(\mathcal{A}') + \frac{0.5(\sigma + q + 1)^2}{2^{256}} + \frac{2^5 q(\sigma + q)(\ell_N + 1)}{2^{256}}$$

$$[\text{IOM12}]\quad |N| = 96,\quad \mathbf{Adv}^{\text{auth}}_{\text{GCM[Rijndael-256},\tau]}(\mathcal{A}) \leq \mathbf{Adv}^{\text{prp}}_{\text{Rijndael-256}}(\mathcal{A}') + \frac{0.5(\sigma + q + q' + 1)^2}{2^{256}} + \frac{q'(\ell_A + 1)}{2^{\tau}}$$

$$[\text{NOMI15}]\ |N| \neq 96,\quad \mathbf{Adv}^{\text{auth}}_{\text{GCM[Rijndael-256},\tau]}(\mathcal{A}) \leq \mathbf{Adv}^{\text{prp}}_{\text{Rijndael-256}}(\mathcal{A}') + \frac{0.5(\sigma + q + q' + 1)^2}{2^{256}} + \frac{2^5(q + q')(\sigma + q + 1)(\ell_N + 1)}{2^{256}} + \frac{q'(\ell_A + 1)}{2^{\tau}}$$

- 96 can be changed to 192. Changing inc to increment the last 64 bits does not affect [IOM12], $|N| = 192$, but [NOMI15] bounds should be reviewed

GHASH in Rijndael-256-GCM

- A naïve definition of GHASH works in $\mathrm{GF}(2^{256})$
- $X[1], \ldots, X[m] = A[1] \| \cdots \| A[a]0^* \| C[1] \| \cdots \| C[c]0^* \| \mathrm{len}_{128}(A) \| \mathrm{len}_{128}(C)$
- $Y = X[1]L^m \oplus X[2]L^{m-1} \oplus \cdots \oplus X[m]L$ over $\mathrm{GF}(2^{256})$

- [AY12] proposes to use a multiplication over $\mathrm{GF}(2^{64})$ to define GHASH over 128-bit blocks
  - Called GCM/2+
  - Can be used to define GHASH over 256-bit blocks based on a multiplication over $\mathrm{GF}(2^{128})$, needs modification to other places, but achieves 128-bit security
  - [Procter, Cid, '15] shows the analysis of weak key classes

[AY12] Aoki, Yasuda. The Security and Performance of "GCM" when Short Multiplications Are Used Instead. Inscrypt 2012.

GHASH in Rijndael-256-GCM

- GHASH over $\{0,1\}^{256}$ blocks based on GF(2^{128}) multiplication
- $L = E_K(0^{256}) = L_0 \parallel L_1 \in \{0,1\}^{128} \times \{0,1\}^{128}$
- $X[1], \ldots, X[m] = A[1] \parallel \cdots \parallel A[a]0^* \parallel C[1] \parallel \cdots \parallel C[c]0^* \parallel \mathrm{len}_{128}(A) \parallel \mathrm{len}_{128}(C)$
  - Break into 128-bit blocks
- $Y_0 = X[1]L_0^m \oplus X[2]L_0^{m-1} \oplus \cdots \oplus X[m]L_0$
  $Y_1 = X[1]L_1^m \oplus X[2]L_1^{m-1} \oplus \cdots \oplus X[m]L_1$
  over GF(2^{128})
- $Y = Y_0 \parallel Y_1$

- ϵ-almost XOR universal hash function with $\epsilon = \ell^2/2^{256}$

GHASH in Rijndael-256-GCM

- Focusing on the case $|N|$ fixed, with Rijdael-256,

$$[\text{IOM12}] \quad \mathbf{Adv}^{\text{priv}}_{\text{GCM}[\text{AES},\tau]}(\mathcal{A}) \leq \mathbf{Adv}^{\text{prp}}_{\text{AES}}(\mathcal{A}') + \frac{0.5(\sigma+q+1)^2}{2^{128}}$$

$$\Longrightarrow \quad \mathbf{Adv}^{\text{priv}}_{\text{GCM}[\text{AES},\tau]}(\mathcal{A}) \leq \mathbf{Adv}^{\text{prp}}_{\text{AES}}(\mathcal{A}') + \frac{0.5(\sigma+q+1)^2}{2^{128}} \qquad (\text{unaffected})$$

$$[\text{IOM12}] \quad \mathbf{Adv}^{\text{auth}}_{\text{GCM}[\text{AES},\tau]}(\mathcal{A}) \leq \mathbf{Adv}^{\text{prp}}_{\text{AES}}(\mathcal{A}') + \frac{0.5(\sigma+q+q'+1)^2}{2^{128}} + \frac{q'(\ell_A+1)}{2^{\tau}}$$

$$\Longrightarrow \quad \mathbf{Adv}^{\text{auth}}_{\text{GCM}[\text{AES},\tau]}(\mathcal{A}) \leq \mathbf{Adv}^{\text{prp}}_{\text{AES}}(\mathcal{A}') + \frac{0.5(\sigma+q+q'+1)^2}{2^{128}} + \frac{q'(\ell_A+1)^2}{2^{\tau}}$$

- The bound is still good when $\tau = 256$

GCM with Rijndael-256

- GCM with Rijndael-256 can be defined naively, but the several parameter choices can be reviewed
  - Whether $|N| = 192$ or not, or whether $|N| = 224$ or not, fixed length, or if other lengths are allowed
  - Whether ctr works on the last 32 bits, or 64 bits, or other length
    - Affects the maximum number of plaintext blocks
  - The provable security bounds in [IOM12], $|N| = 192$, is unaffected by the length of inc, but it affects the bounds in [NOMI15], $|N| \neq 192$
- Use of a 256-bit output universal hash function defined over GF(2^{128}) could be explored more

Summary

- Rijndael-256-CMAC can be naturally defined
- The security follows from existing works
- Using $X = 2L$ and $Y = 4L$ over GF(2^{256}) works fine, but the definition of the mask could be explored

- Rijndael-256-GCM can also be defined naturally, but several parameter choices can be reviewed
  - The nonce length
  - The inc function
- Use of a 256-bit output universal hash function defined over GF(2^{128}) could be explored more