OMD version 2.0

Reza Reyhanitabar

Design Team:
Simon Cogliani, Diana Maimut, David Naccache (*ENS, France*)
Rodrigo Portella do Canto (Paris II - *Panthéon-Assas University, France*)
Reza Reyhanitabar, Serge Vaudenay, Damian Vizár *(EPFL, Switzerland)*

CAESAR candidate OMD

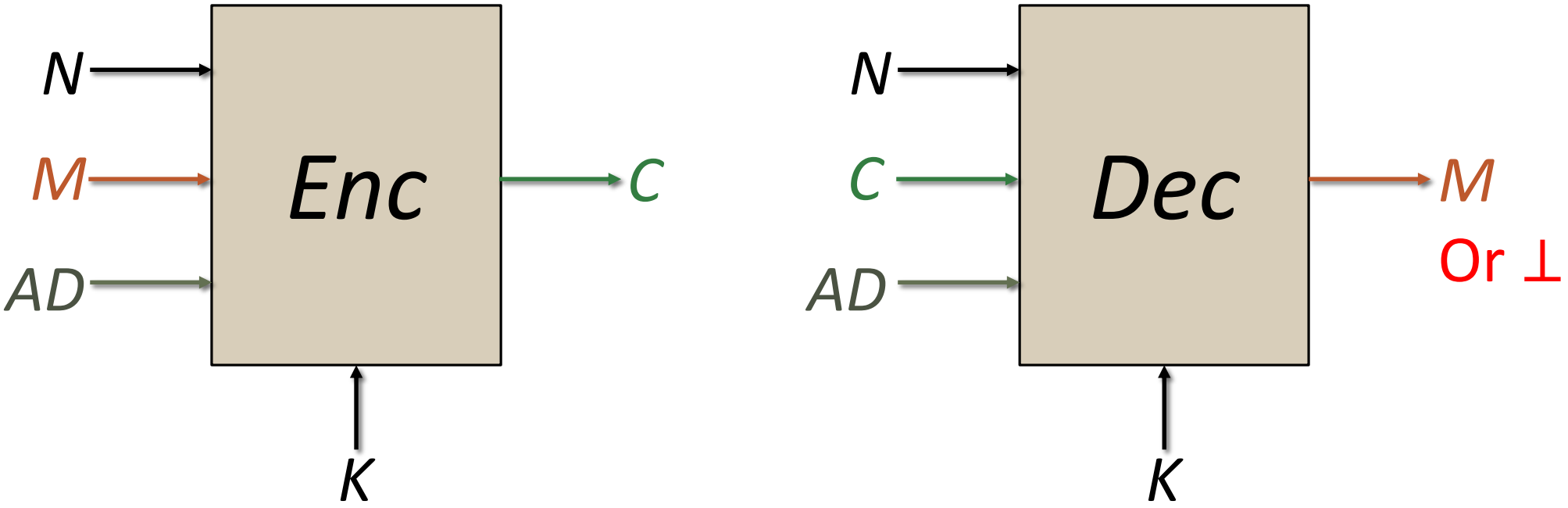
- **OMD stands for Offset Merkle–Damgård**

Compression function-based mode of operation for AEAED

- **Notable Features:**
  - **High security level**
    - **127-bit security using sha-256**
    - **255-bit security using sha-512**
  - **Provable security (based on a well-studied standard security assumption)**

    If the compression function keyed via its message input is PRF then OMD is a secure AEAD.

Nonce-based Authenticated Encryption with Associated Data



***N*: Nonce** (public message number)

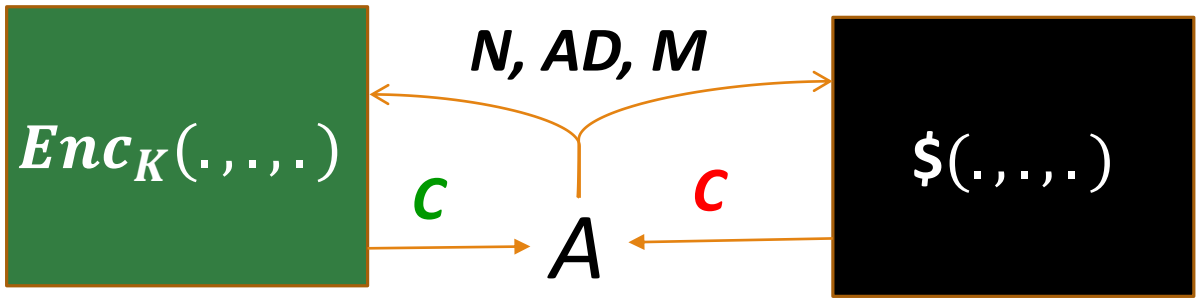
***M*: Plaintext** that needs to be encrypted and authenticated

***AD*: Associated data** that needs to be authenticated, but must not be encrypted

***C*: Ciphertext**

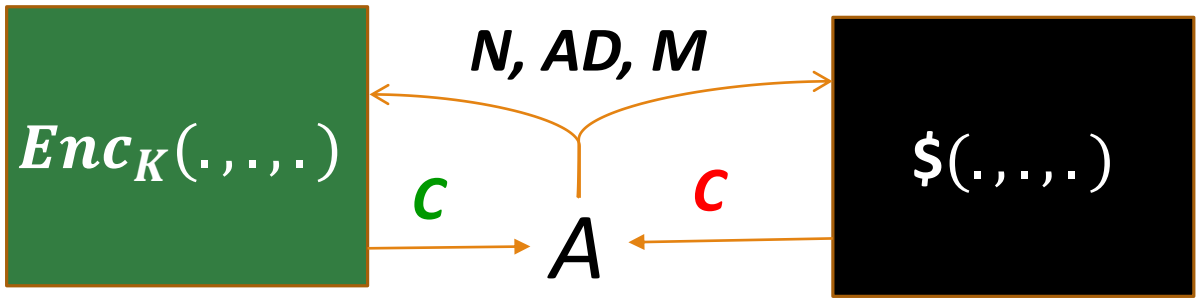
***K*: Secret Key**

The Security Goal(s)

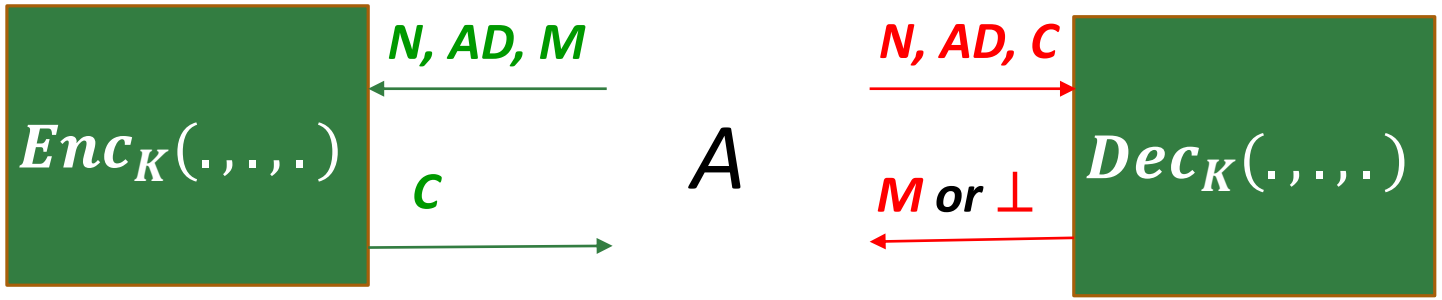


$$\mathbf{Adv}_{\Pi}^{\text{priv}}(A)=\Pr\left[A^{Enc_K(.,.,.)} \Rightarrow 1\right] - \Pr\left[A^{\$(.,.,.)} \Rightarrow 1\right]$$

The Security Goal(s)



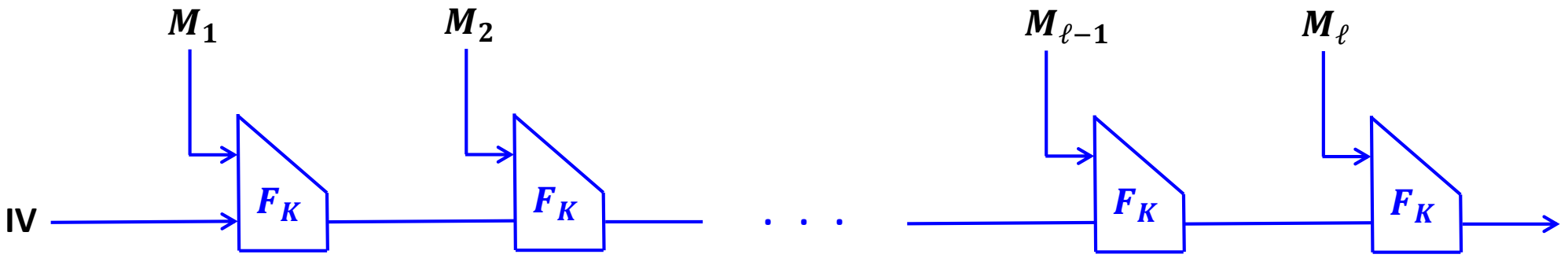
$$\mathbf{Adv}_{\Pi}^{\text{priv}}(A)=\Pr\left[A^{Enc_K(.,.,.)} \Rightarrow 1\right] - \Pr\left[A^{\$(.,.,.)} \Rightarrow 1\right]$$



$$\mathbf{Adv}_{\Pi}^{\text{auth}}(A)=\Pr\left[A^{Enc_K(.,.,.),\, Dec_K(.,.,.)} \text{ forges}\right]$$

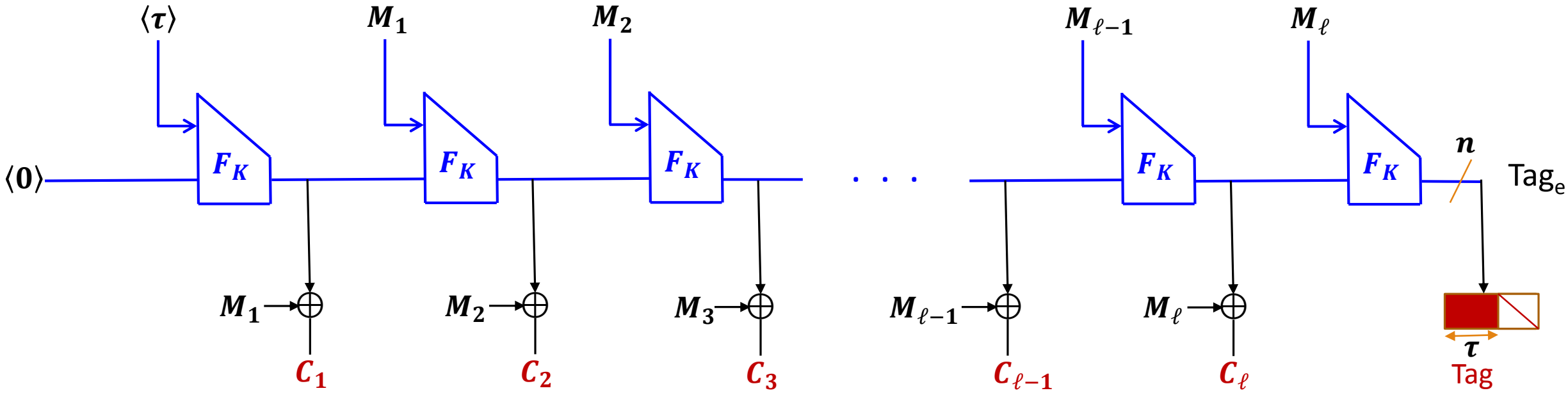
A forges if: $\exists (N, AD, C)$ *such that* $Dec_K(N, AD, C) \neq \perp$ **AND** *no previous query* $Enc_K(N, AD, M)$ *returned* C

The MD Construction



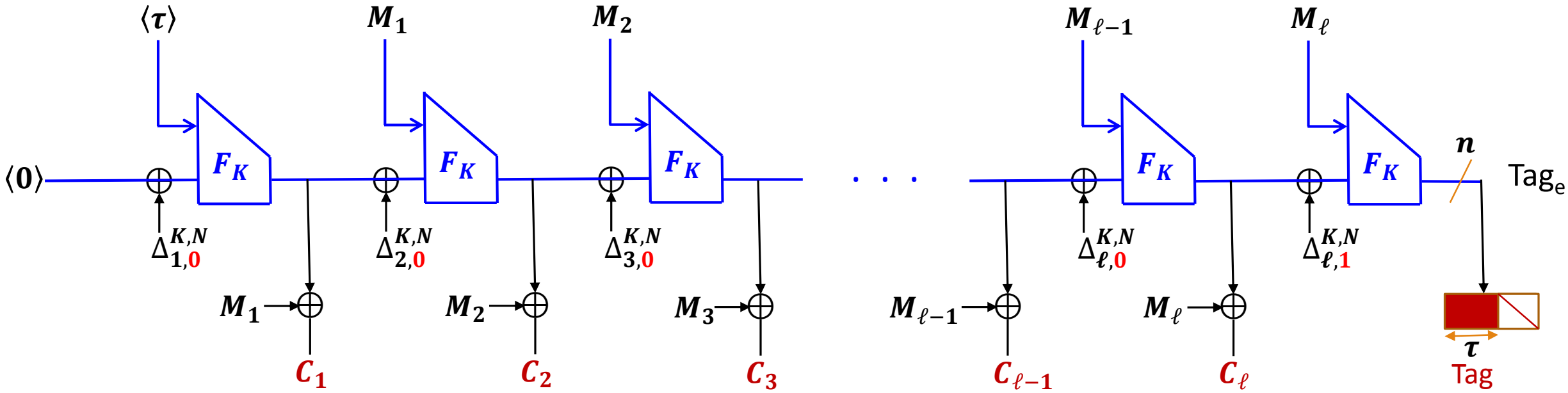
- **Assumption: the keyed compression function F is a PRF**
- **MD Preserves PRF** (Bellare and Ristenpart, ICALP 2007)

OMD: Making a nonce-based AE Scheme based on the MD construction



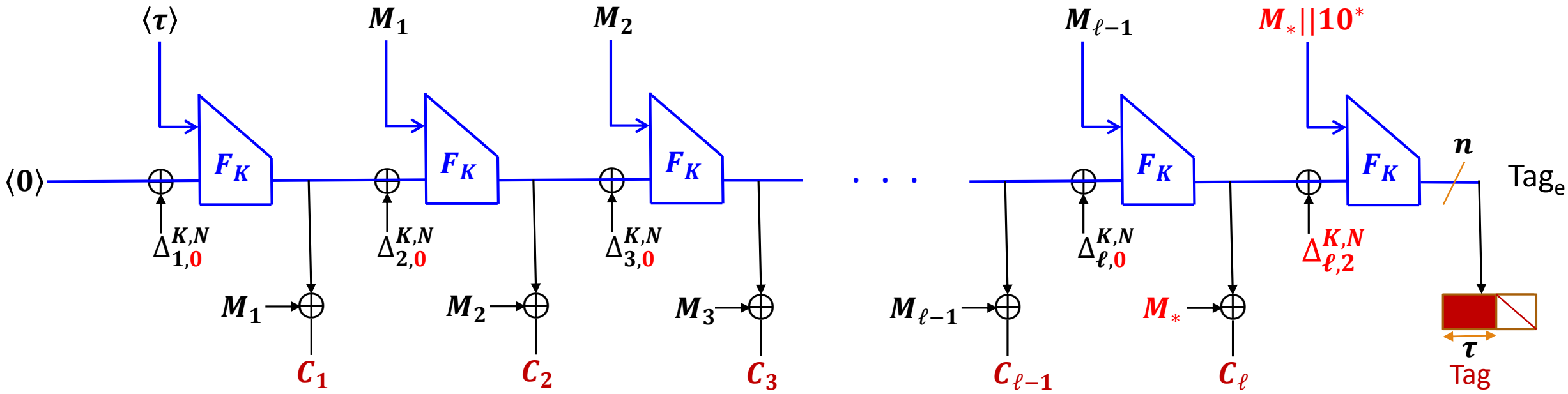
Encrypting a message whose length is a multiple of the block length

OMD: Making a nonce-based AE Scheme based on the MD construction

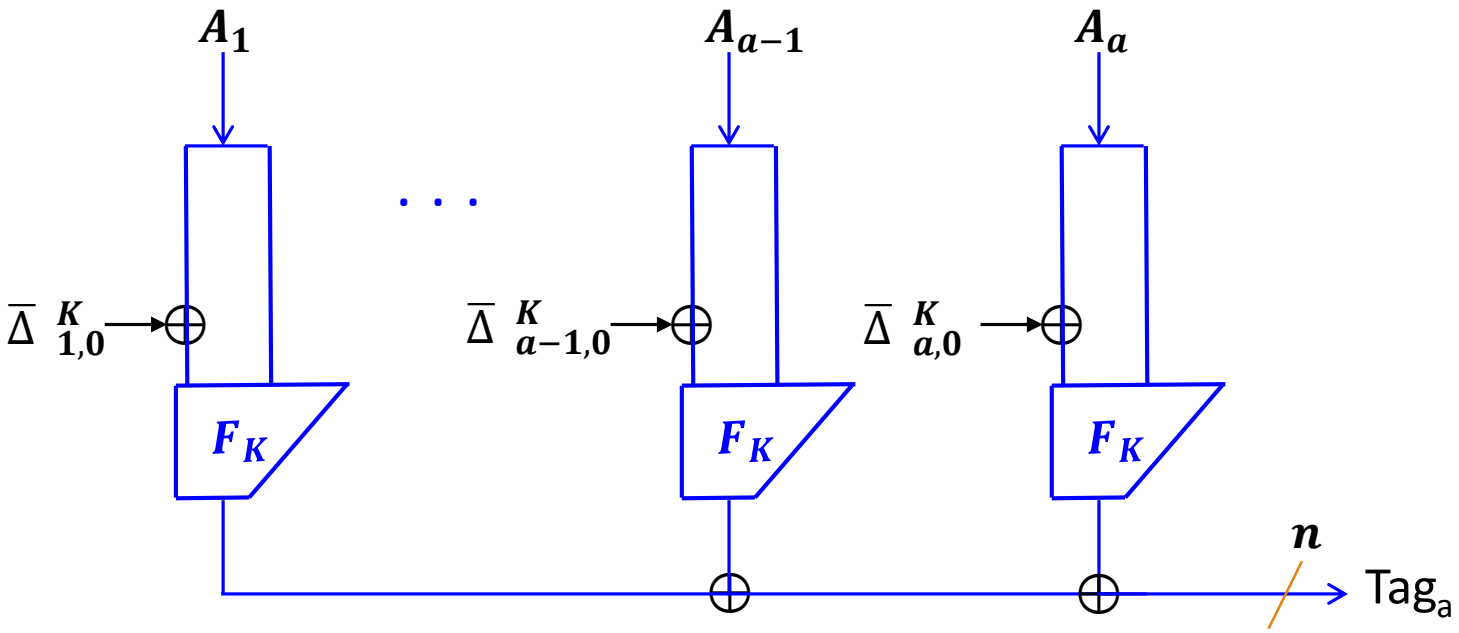


Encrypting a message whose length is a multiple of the block length

OMD: Making a nonce-based AE Scheme based on the MD construction

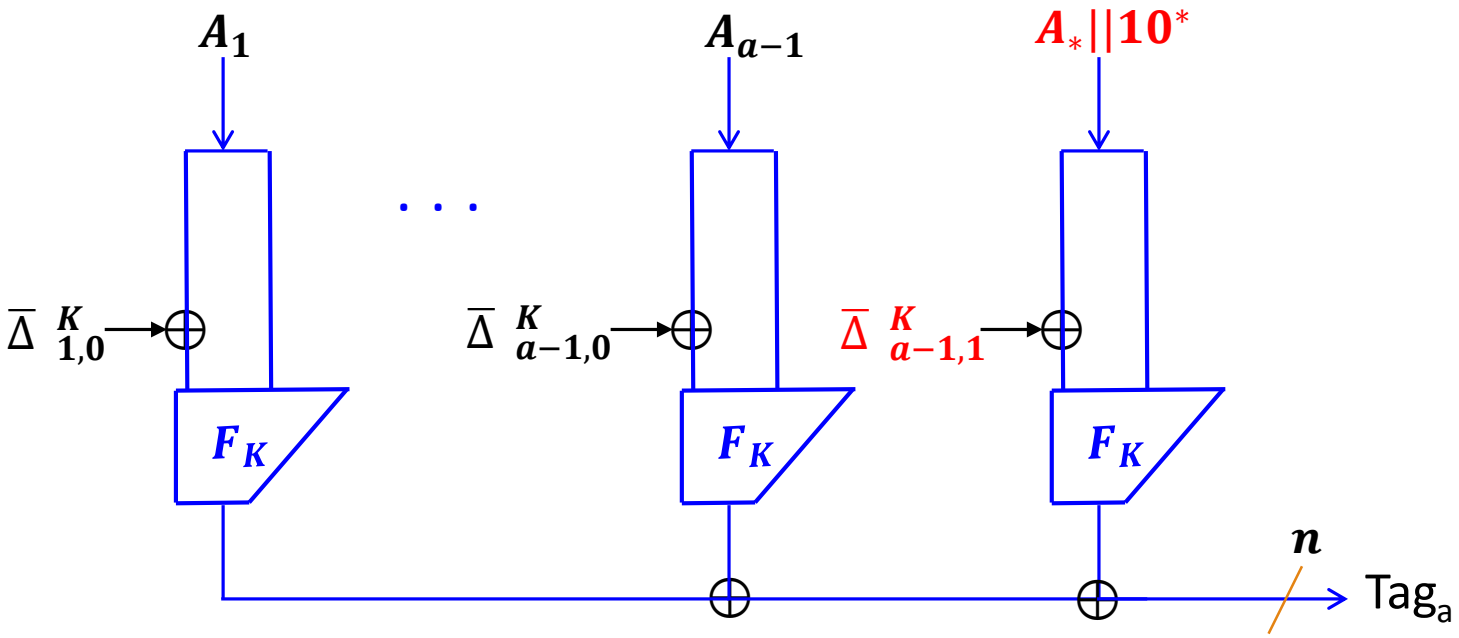


Encrypting a message whose length is not a multiple of the block length



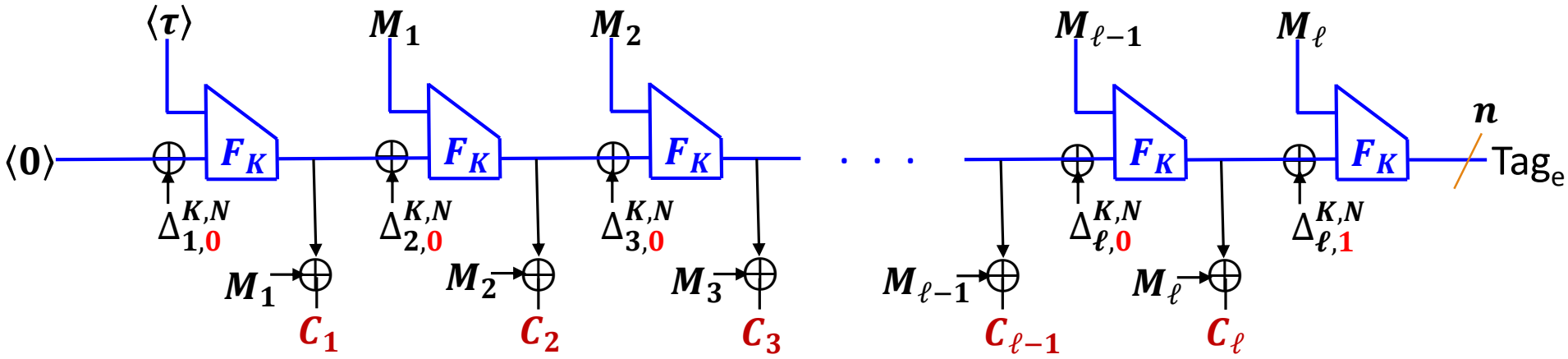
Handling Associated Data in OMD

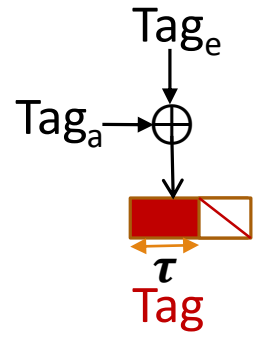
when the length of the data is a multiple of the input length.

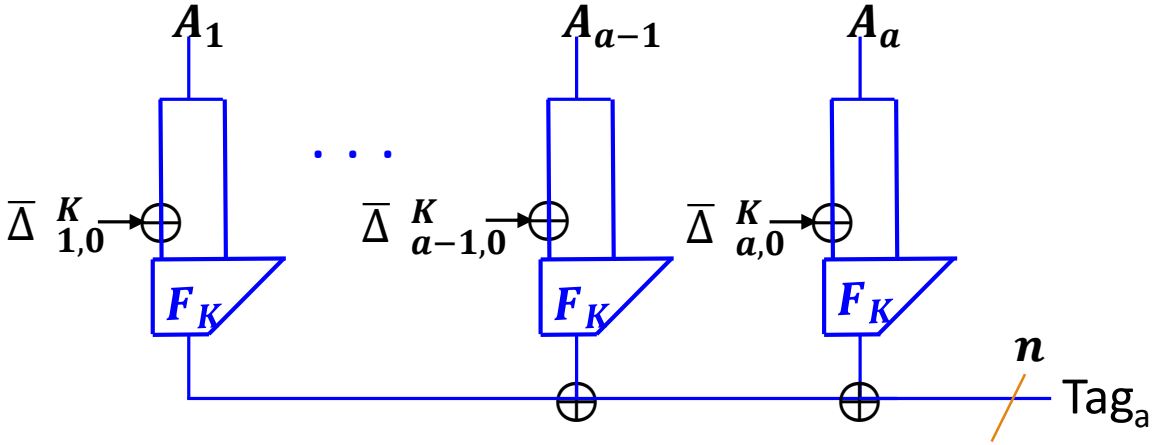


Handling Associated Data in OMD

when the length of the data is <u>not</u> a multiple of the input length.







OMD

A Secure Nonce-based AE Algorithm that integrates a modified MD pass with XOR MAC

Computing the Masking Sequence: OMD version 1

$$\Delta_{0,0}^{K,N} = F_K(N \parallel 10^{n-1-|N|}, 0^m), \qquad \bar{\Delta}_{0,0}^{K} = 0^n$$

$$L_* = F_K(0^n, 0^m)$$

$$L(0) = 4 \cdot L_*$$
for $i \geq 1$ $\quad L(i) = 2 \cdot L(i-1)$

---

for $i \geq 1$:

$$\Delta_{i,0}^{K,N} = \Delta_{i-1,0}^{K,N} \oplus L(\mathrm{ntz}(i))$$
$$\Delta_{i,1}^{K,N} = \Delta_{i,0}^{K,N} \oplus 2 \cdot L_*$$
$$\Delta_{i,2}^{K,N} = \Delta_{i,0}^{K,N} \oplus 2 \cdot L_*$$
$$\bar{\Delta}_{i,0}^{K} = \bar{\Delta}_{i-1,0}^{K} \oplus L(\mathrm{ntz}(i))$$

for $i \geq 0$:

$$\bar{\Delta}_{i,1}^{K} = \bar{\Delta}_{i,0}^{K} \oplus L_*$$

Computing the Masking Sequence: OMD version 2

$$\Delta_{0,0}^{K,N} = F_K(N \parallel 10^{n-1-|N|}, 0^m), \qquad \overline{\Delta}_{0,0}^{K} = 0^n$$

$$L_* = F_K(0^n, <\tau>_m)$$

$$L(0) = 4 \cdot L_*$$
for $i \geq 1$ $\quad L(i) = 2 \cdot L(i-1)$

---

for $i \geq 1$:

$$\Delta_{i,0}^{K,N} = \Delta_{i-1,0}^{K,N} \oplus L(\mathrm{ntz}(i))$$
$$\Delta_{i,1}^{K,N} = \Delta_{i,0}^{K,N} \oplus 2 \cdot L_*$$
$$\Delta_{i,2}^{K,N} = \Delta_{i,0}^{K,N} \oplus 2 \cdot L_*$$
$$\overline{\Delta}_{i,0}^{K} = \overline{\Delta}_{i-1,0}^{K} \oplus L(\mathrm{ntz}(i))$$

for $i \geq 0$:

$$\overline{\Delta}_{i,1}^{K} = \overline{\Delta}_{i,0}^{K} \oplus L_*$$

Security

$$\mathbf{Adv}^{\text{priv}}_{\text{p-OMD}[F,\tau]}(t, \sigma_e, \ell_{max}) = \mathbf{Adv}^{prf}_{F}(t', 2\sigma_e) + \frac{\mathbf{3\sigma_e^2}}{\mathbf{2^n}}$$

$$\mathbf{Adv}^{\text{auth}}_{\text{p-OMD}[F,\tau]}(t, q_v, \sigma, \ell_{max}) = \mathbf{Adv}^{prf}_{F}(t', 2\sigma) + \frac{\mathbf{3\sigma^2}}{\mathbf{2^n}} + \frac{q_v \ell_{max}}{2^n} + \frac{q_v}{2^\tau}$$

σ_e: total number of calls to the compression function in encryption queries

σ: total number of calls to the compression function in all (encryption and verification) queries

q_v: the number of decryption (verification) queries

ℓ_{max}: the maximum number of internal calls to the compression function in any query

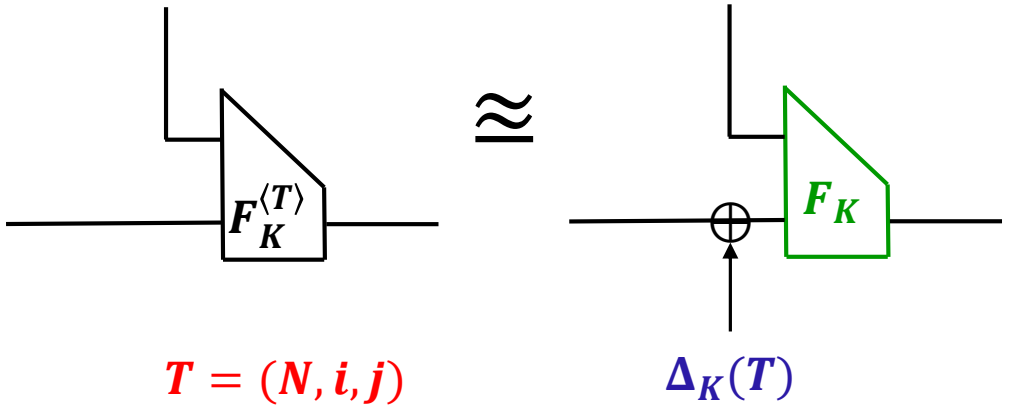
n: the output length of the compression function in bits

τ: the tag length

$t' = t + cn\sigma$

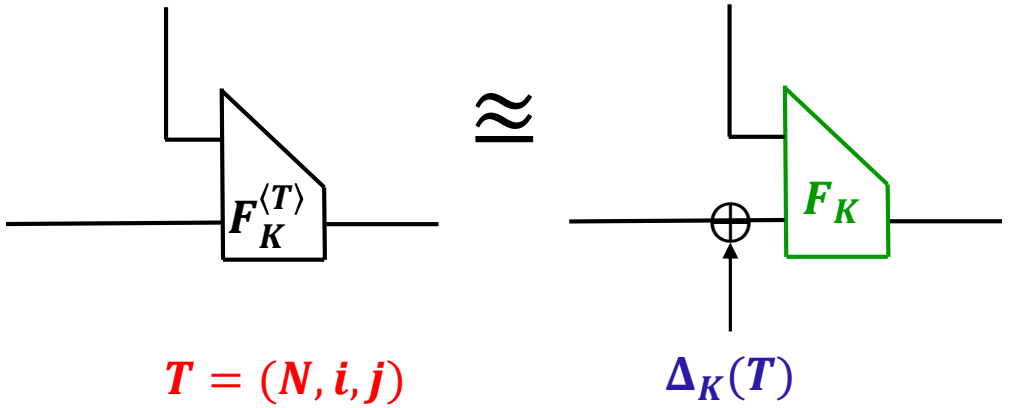
We used the XE method to make a tweak able-PRF out of a PRF.

This is the cause of the birthday-type term $\left(\frac{3\sigma^2}{2^n}\right)$ in the security bounds



We used the XE method to make a tweak able-PRF out of a PRF.

This is the cause of the birthday-type term $\left(\frac{3\sigma^2}{2^n}\right)$ *in the security bounds*



Using a native tweakable-and-keyed compression function (i.e. one with dedicated tweak and key inputs) this term can be avoided.

Any such functions?

- *Allocating some part of the input for tweak may be an option but this limits the parameters' sizes compared to the original OMD*
- *The TWEAKEY Framework* (Jean, Nikolić, and Peyrin, ASIACRYPT 2014) *seems a promising way toward designing an efficient TWEAKEY Compression Function.*

Conclusion

- **OMD v2** is *a new version of OMD with a minor tweak*
- ***OMD v2** has the same performance as OMD v1*
- ***OMD v2** has the same security bounds as OMD v1*
- ***OMD v2** is NOT susceptible to the tag-length variation misusing attacks,* *posted on the CAESAR mailing list* on 25 April 2014 by the Ascon team.

Thanks!

Questions?