OMD

A Compression Function Mode of Operation for Authenticated Encryption

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)***

Outline

- Authenticated Encryption
  - Nonce-based Authenticated Encryption with Associated Data
  - The Security Goal(s)
- OMD:
  - Description
  - Security Analysis
  - Performance
- Conclusion

Authenticated Encryption

Privacy (Confidentiality) + Integrity(Authenticity)

Authenticated Encryption

Privacy (Confidentiality) + Integrity(Authenticity)

Privacy-Only Encryption Schemes

- **Probabilistic**
- **IV-based**
- **Nonce-based**
- **Deterministic**

Authenticated Encryption

Privacy (Confidentiality) + Integrity(Authenticity)

Privacy-<u>Only</u> Encryption Schemes

- ❖ Probabilistic
- ❖ IV-based
- ❖ Nonce-based
- ❖ Deterministic

Message Authentication Schemes

- ❖ Deterministic (MAC)
- ❖ (Randomized) IV-based
- ❖ (Counter) Nonce-based

Authenticated Encryption

Privacy (Confidentiality) + Integrity(Authenticity)

Privacy-Only Encryption Schemes

- Probabilistic
- IV-based
- Nonce-based
- Deterministic

Message Authentication Schemes

- Deterministic (MAC)
- (Randomized) IV-based
- (Counter) Nonce-based

Formalizations:

Indistinguishability and Non-malleability notions (IND-CPA, IND-CCA1, IND-CCA2, NM-CCA, PRP)

Unforgeability and PRF

Authenticated Encryption

Privacy (Confidentiality) + Integrity(Authenticity)

Privacy-Only Encryption Schemes

- ❖ Probabilistic
- ❖ IV-based
- ❖ Nonce-based
- ❖ Deterministic

Message Authentication Schemes

- ❖ Deterministic (MAC)
- ❖ (Randomized) IV-based
- ❖ (Counter) Nonce-based

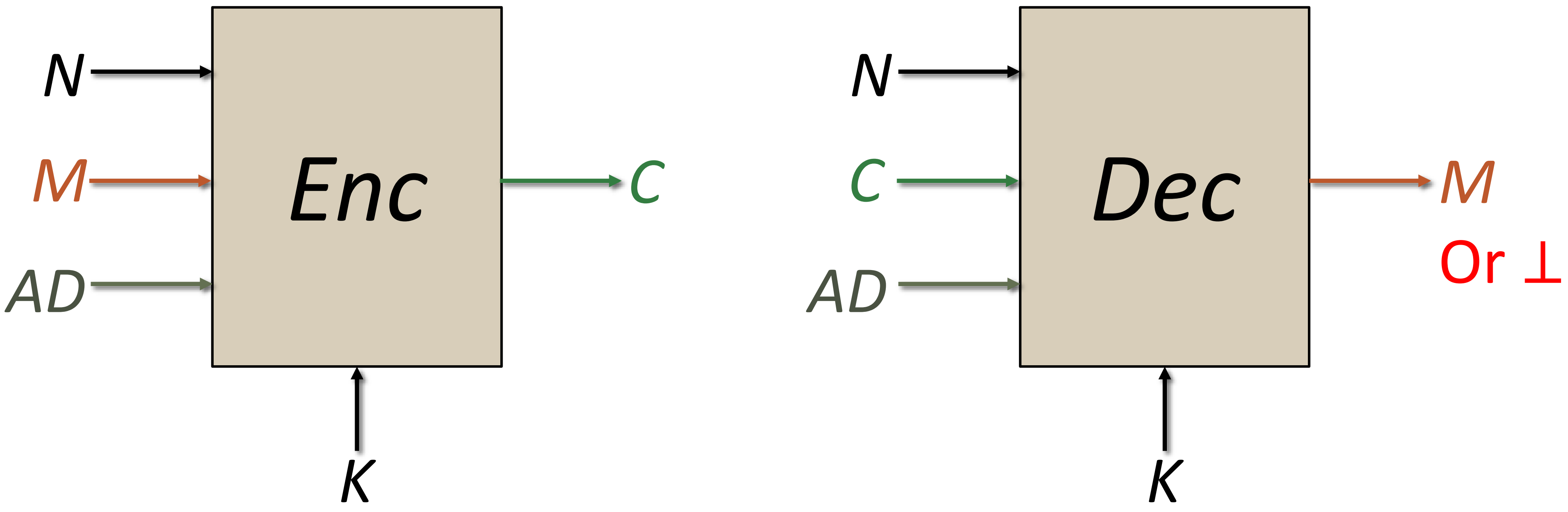
Formalizations:

Indistinguishability and Non-malleability notions (IND-CPA, IND-CCA1, IND-CCA2, NM-CCA, PRP)

Unforgeability and PRF

Authenticated Encryption?

Nonce-based Authenticated Encryption with Associated Data



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

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

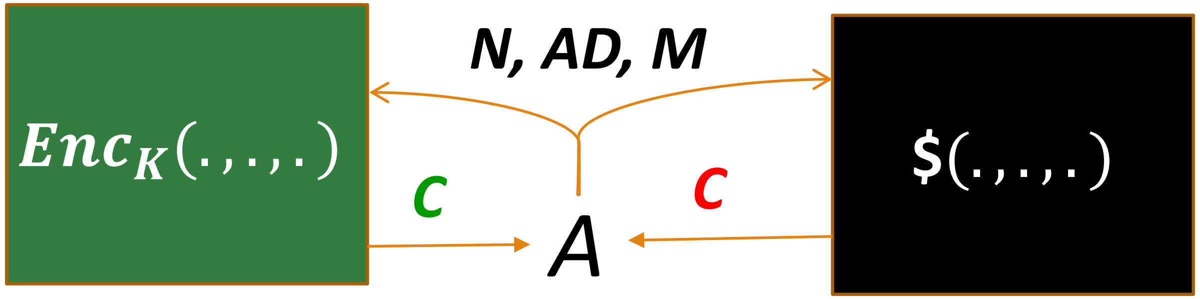
***AD*: Associated data** that needs to be authenticated, but must not be encrypted

***C*: Ciphertext**

***K*: Secret Key**

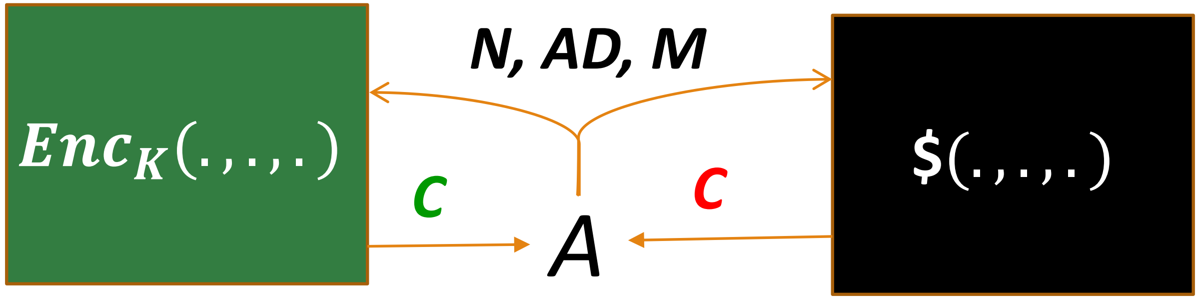
The Security Goal(s)

The Security Goal(s)

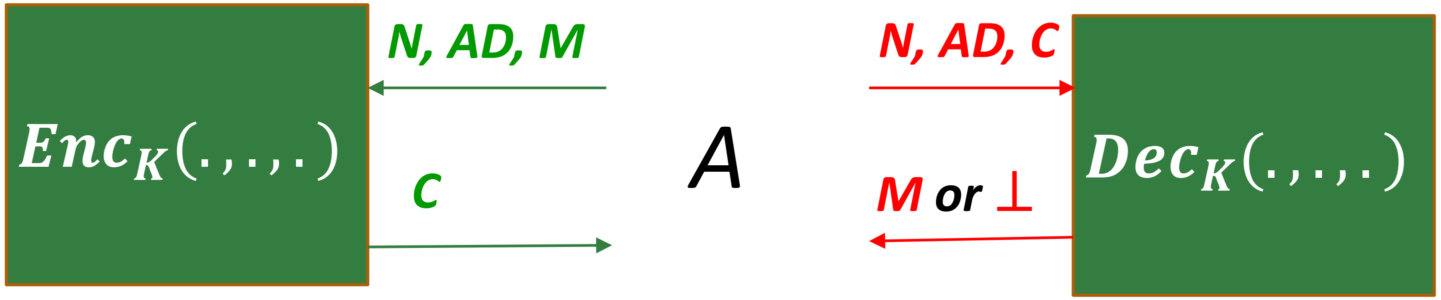


$$\mathbf{Adv}_{\Pi}^{\mathrm{priv}}(A) = \Pr\left[A^{\boldsymbol{Enc_K}(.,.,.)} \Rightarrow 1\right] - \Pr\left[A^{\$(.,.,.)} \Rightarrow 1\right]$$

The Security Goal(s)



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



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

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 OMD Mode of Operation

- OMD stands for Offset Merkle–Damgård.
- OMD is a mode of operation that converts a compression function to a nonce-based AEAD.

The OMD Mode of Operation

- OMD stands for **Offset Merkle–Damgård**.
- OMD is **a mode of operation that converts a compression function to a nonce-based AEAD**.
- **Design rationale**:

The OMD Mode of Operation

- **OMD stands for Offset Merkle–Damgård.**
- **OMD is a mode of operation that converts a compression function to a nonce-based AEAD.**
- **<u>Design rationale</u>:**
  - **High security level (beyond the classical 64-bit security by AES-based designs).**

The OMD Mode of Operation

- OMD stands for **Offset Merkle–Damgård**.
- **OMD is a mode of operation that converts a compression function to a nonce-based AEAD.**
- **Design rationale:**
  - **High security level (beyond the classical 64-bit security by AES-based designs).**
  - **Provable security based on a well-studied standard property of a widely-used primitive.**

The OMD Mode of Operation

- OMD stands for Offset Merkle–Damgård.
- OMD is a mode of operation that converts a compression function to a nonce-based AEAD.
- Design rationale:
  - High security level (beyond the classical 64-bit security by AES-based designs).
  - Provable security based on a well-studied standard property of a widely-used primitive.
  - Simplicity (using only a single primitive).

The OMD Mode of Operation

- **OMD stands for Offset Merkle–Damgård.**
- **OMD is a mode of operation that converts a compression function to a nonce-based AEAD.**
- **Design rationale:**
  - **High security level (beyond the classical 64-bit security by AES-based designs).**
  - **Provable security based on a well-studied standard property of a widely-used primitive.**
  - **Simplicity (using only a single primitive).**
  - **Patent-freeness (avoid using any patented algorithms, such as PMAC, as a subroutine).**

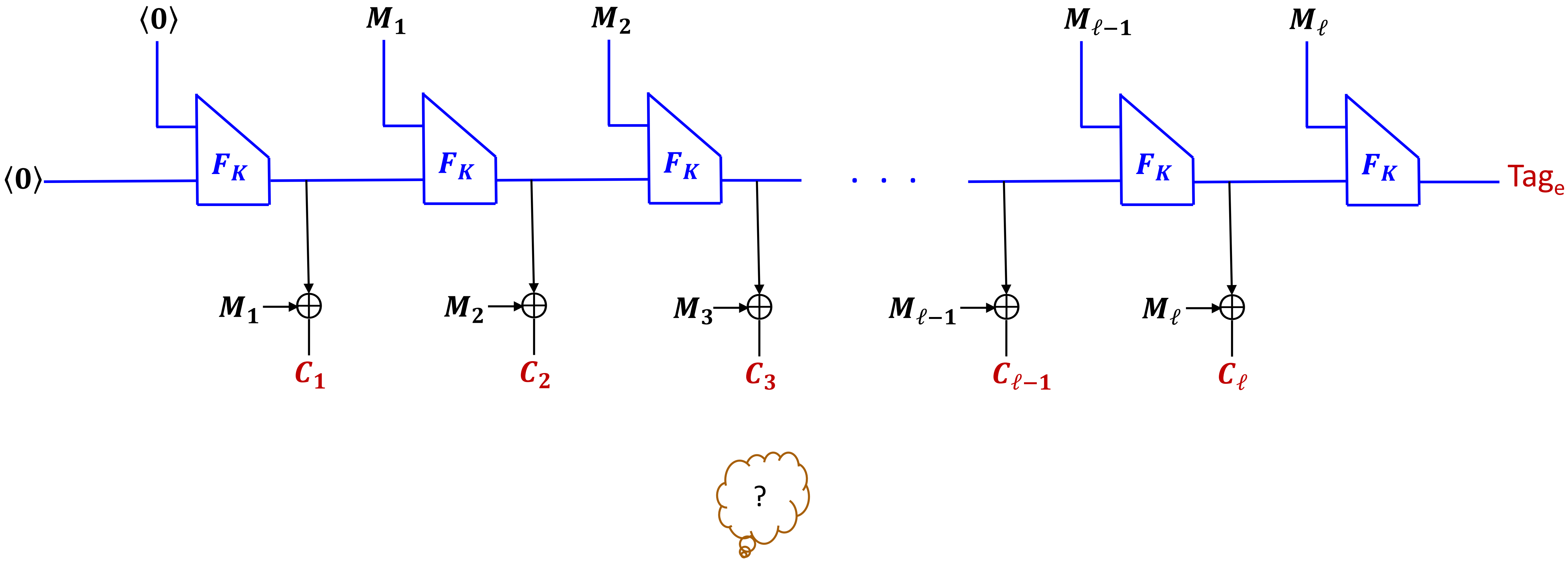
The OMD Mode of Operation

- OMD stands for **Offset Merkle–Damgård**.
- OMD is **a mode of operation that converts a compression function to a nonce-based AEAD**.
- **Design rationale:**
  - **High security level** (beyond the classical 64-bit security by AES-based designs).
  - **Provable security** based on a well-studied standard property of a widely-used primitive.
  - **Simplicity** (using only a single primitive).
  - **Patent-freeness** (avoid using any patented algorithms, such as PMAC, as a subroutine).
  - **Not being a blockcipher-based or permutation-based design** (**Don't Put All Your "Security" Eggs in One or Two Baskets!**)

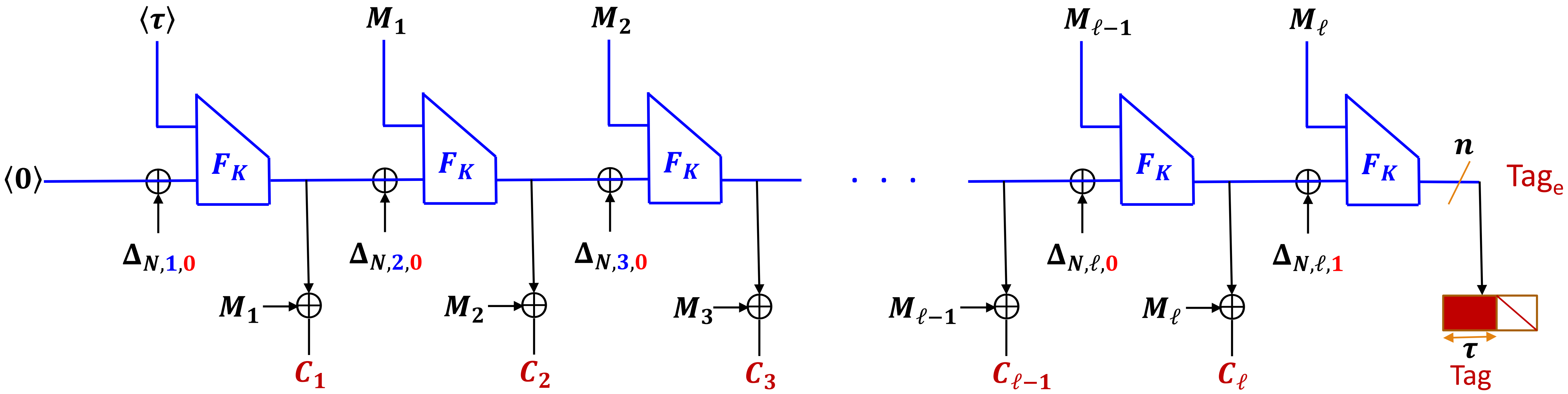
The OMD Mode of Operation

- OMD stands for **Offset Merkle–Damgård.**
- **OMD is a mode of operation that converts a compression function to a nonce-based AEAD.**
- **Design rationale:**
  - **High security level (beyond the classical 64-bit security by AES-based designs).**
  - **Provable security based on a well-studied standard property of a widely-used primitive.**
  - **Simplicity (using only a single primitive).**
  - **Patent-freeness (avoid using any patented algorithms, such as PMAC, as a subroutine).**
  - **Not being a blockcipher-based or permutation-based design (Don't Put All Your "Security" Eggs in One or Two Baskets!)**
  - **Acceptable performance, comparable with that of the standardized AES-GCM scheme.**

- **We Assume that: the keyed compression function F is a PRF.**
- **We know that: MD Preserves PRF.** (Bellare and Ristenpart, ICALP 2007)

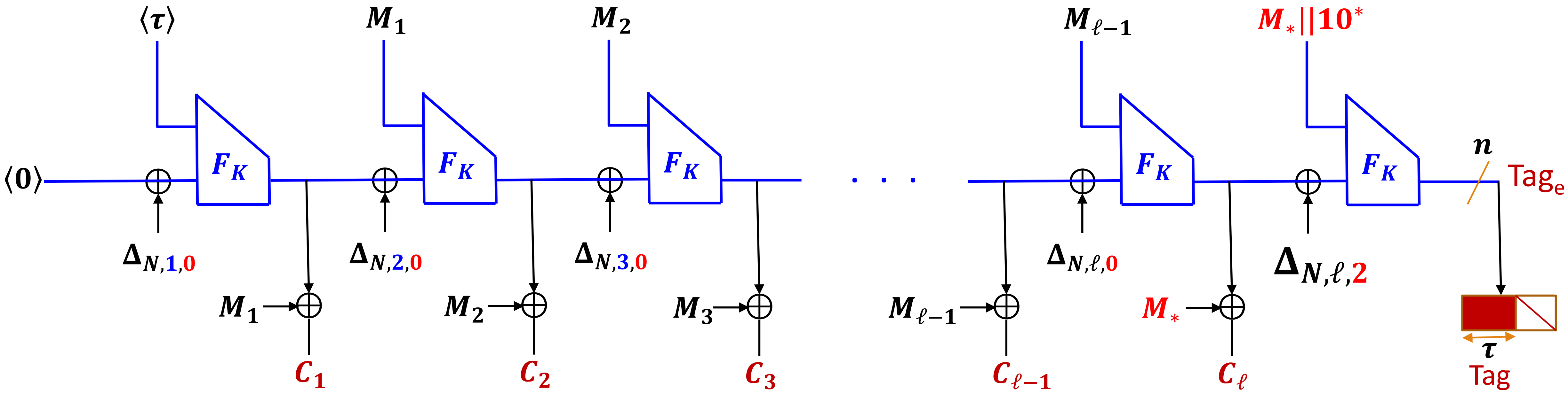


Toward making an AE out of the MD iteration



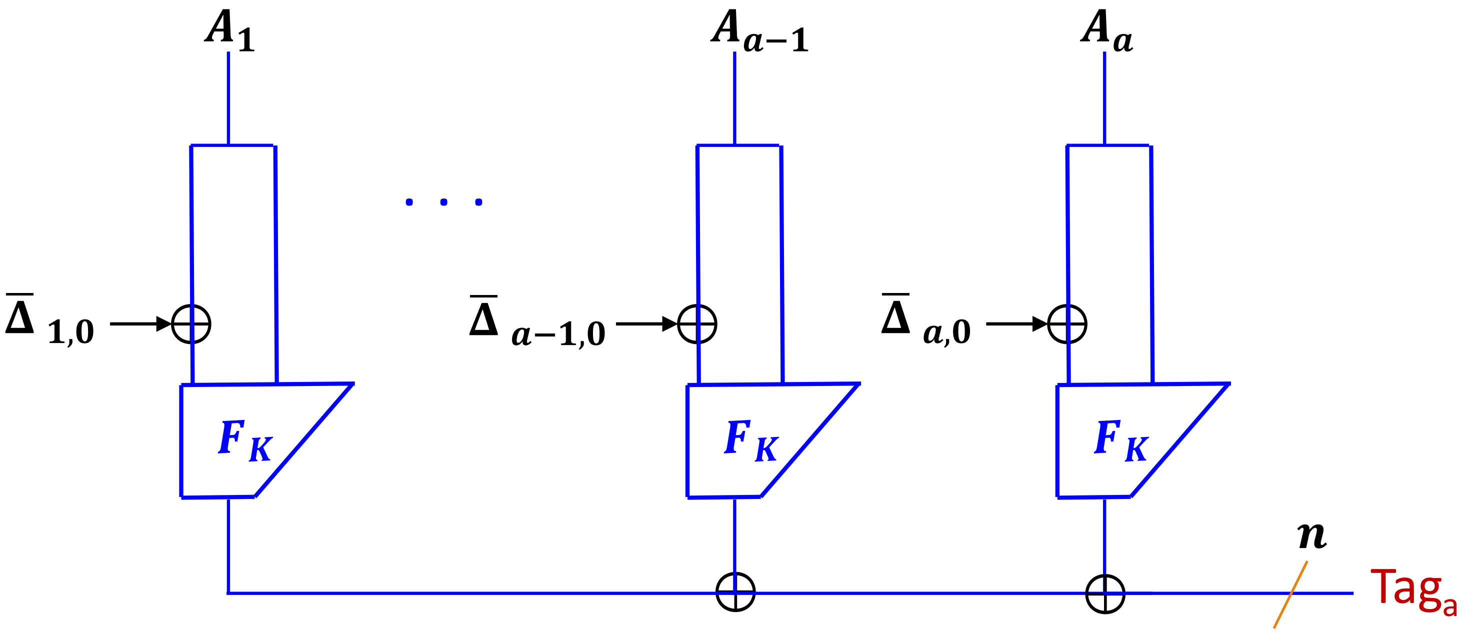
OMD: A Secure Nonce-based AE Algorithm

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

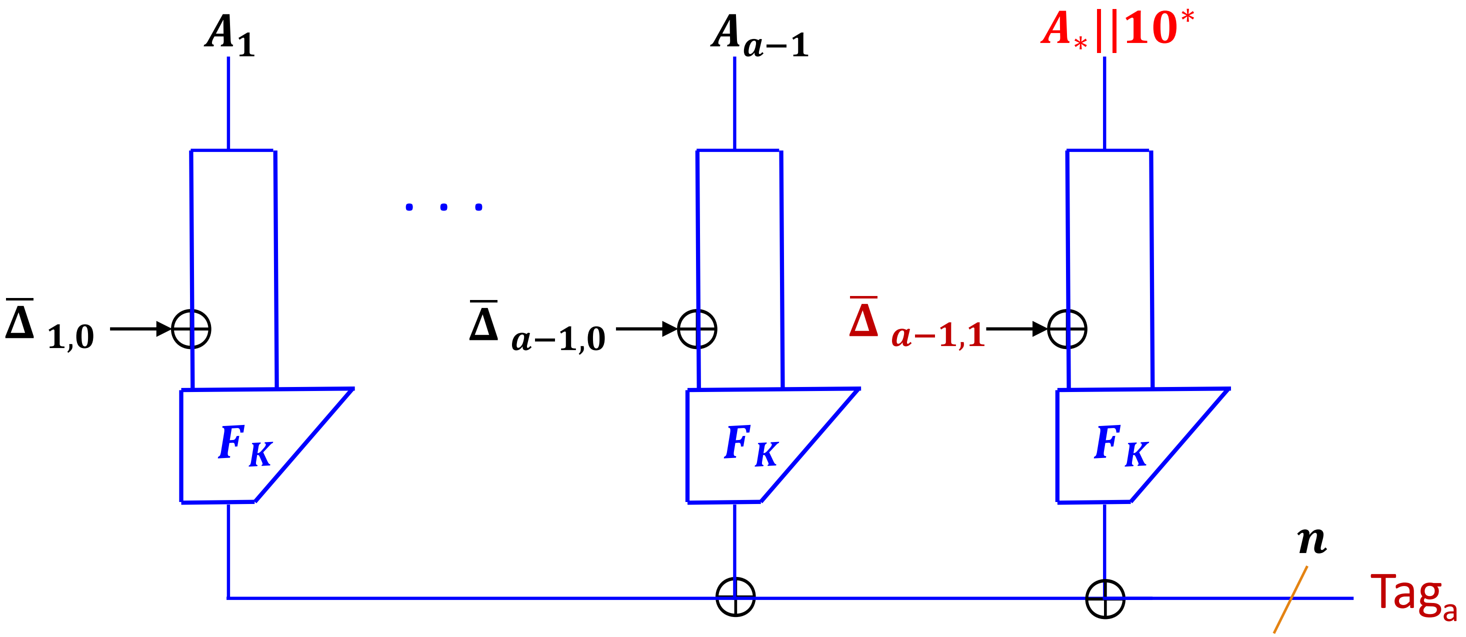


OMD: A Secure Nonce-based AE Algorithm

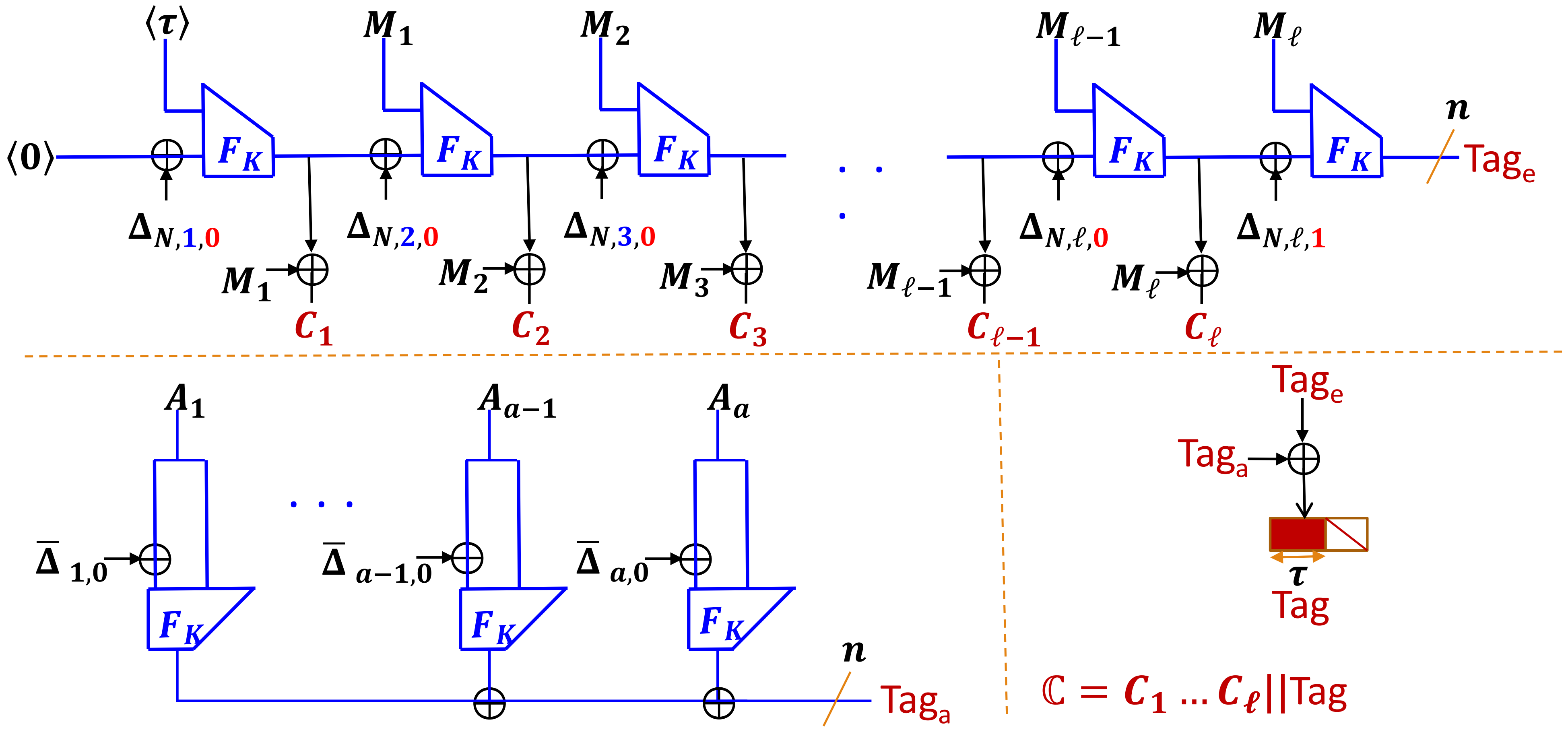
(Encrypting a message whose length is not a multiple of the block length)



Handling Associated Data when the length of the data is a multiple of the input length.



Handling Associated Data when the length of the data is not a multiple of the input length.



OMD: A Secure Nonce-based AEAD Algorithm

(The Case shown: encrypting a message and associated data whose lengths are a multiple of the block length and input length, respectively.)

Security Analysis

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

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

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 message blocks in any query

n: the output length of the compression function in bits

τ: the tag length

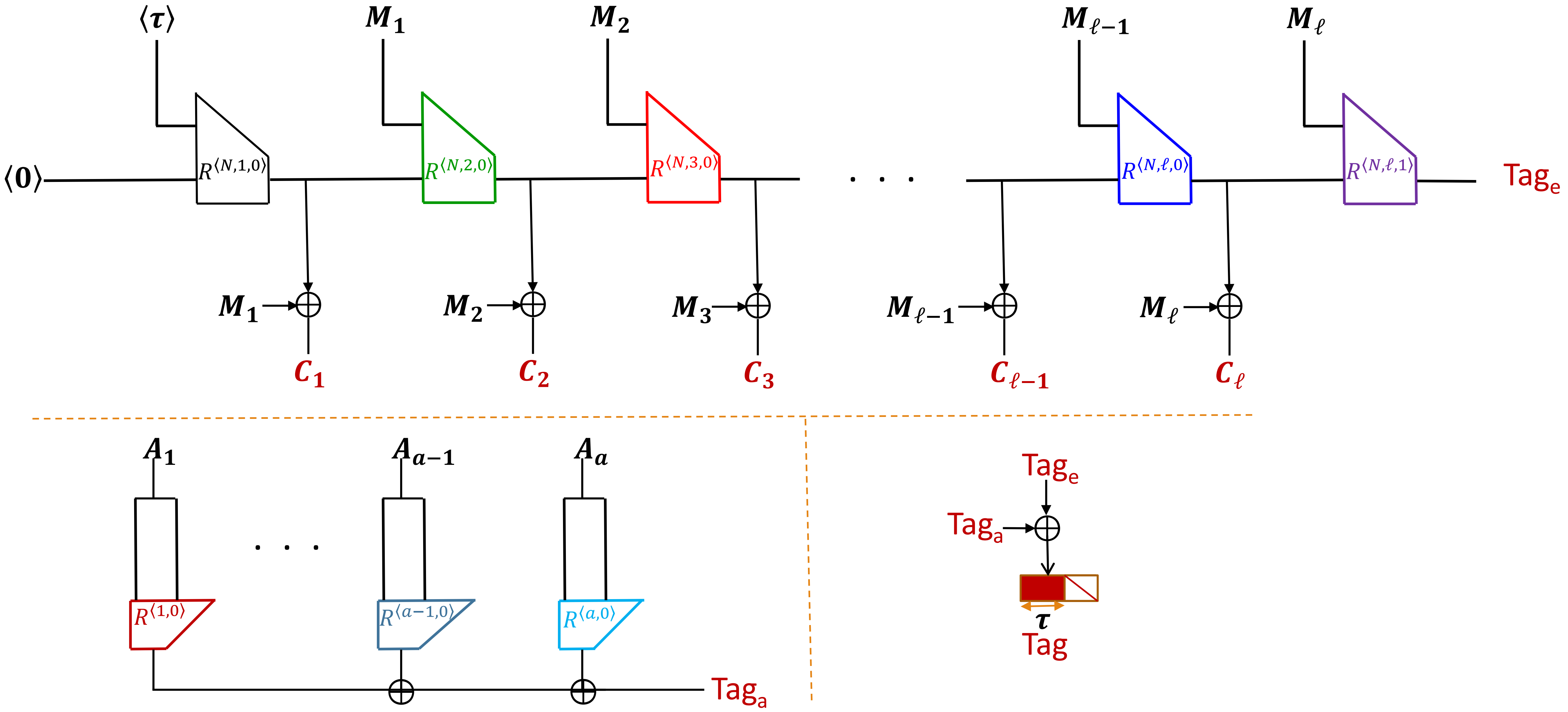
$t' = t + cn\sigma$

Modular, Simple Proof:

- **Step 1:** (**Idealized**) **Generalized OMD** **using a tweakable random function**

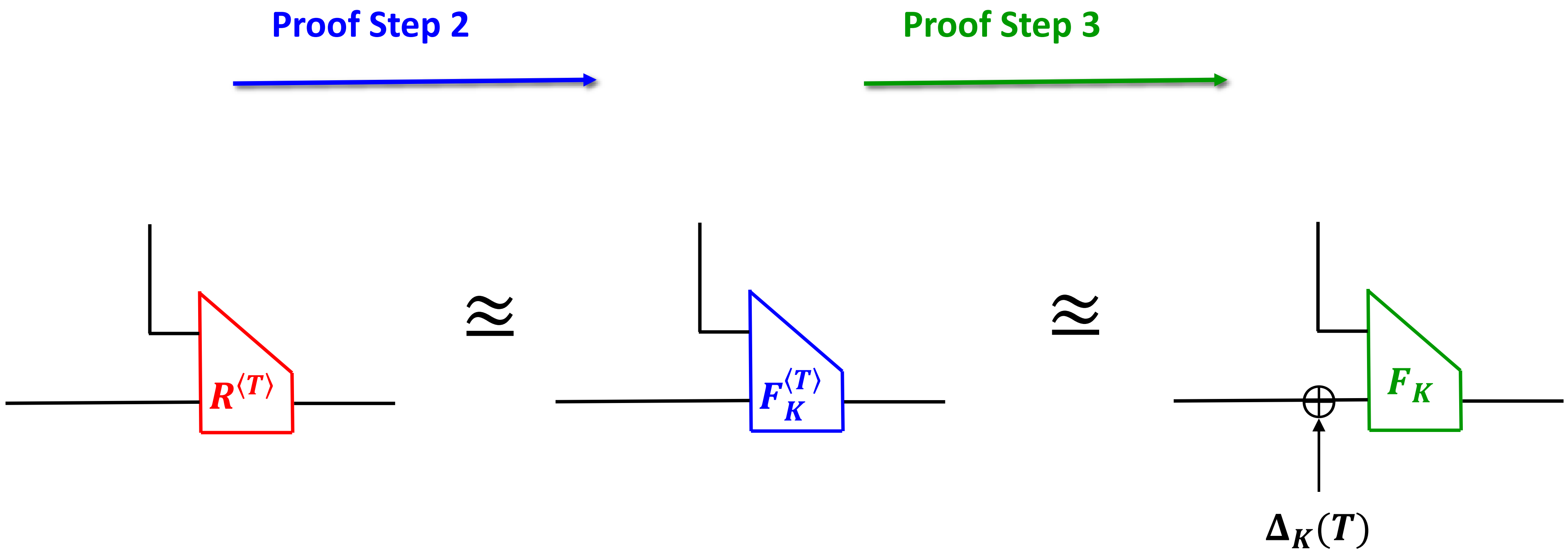
- **Step 2:** Realization of the tweakable random function **using a tweakble PRF**

- **Step 3:** Instantiation of the tweakable PRF **using a PRF**



Proof Step 1: Generalized OMD (G-OMD)

Each call to the tweakable random function uses a new distinct tweak.



The XE method
(Rogaway, ASIACRYPT 2004):

Cause of $\frac{3\sigma^2}{2^n}$ *in the security bounds*

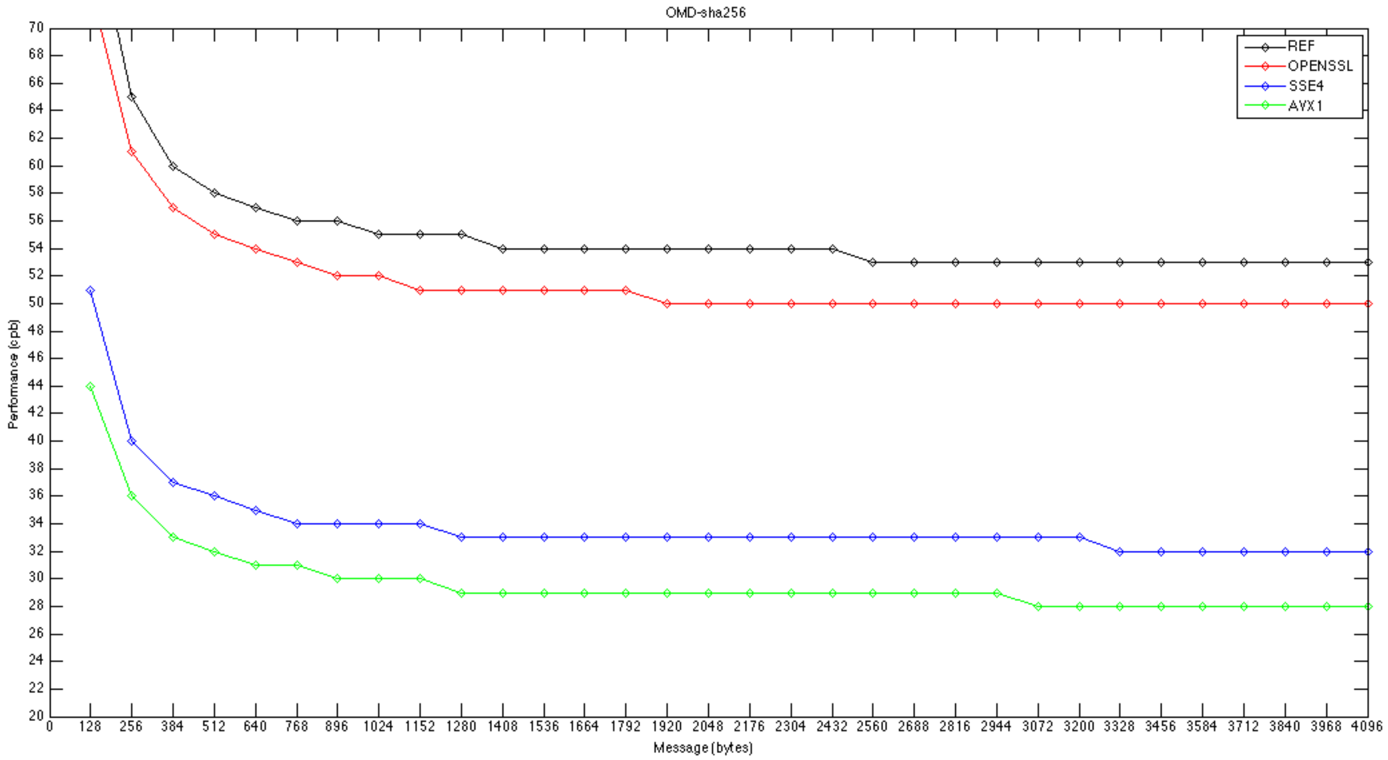
Performance

- We have done some preliminary performance measurements on Intel Core i5-2415M.

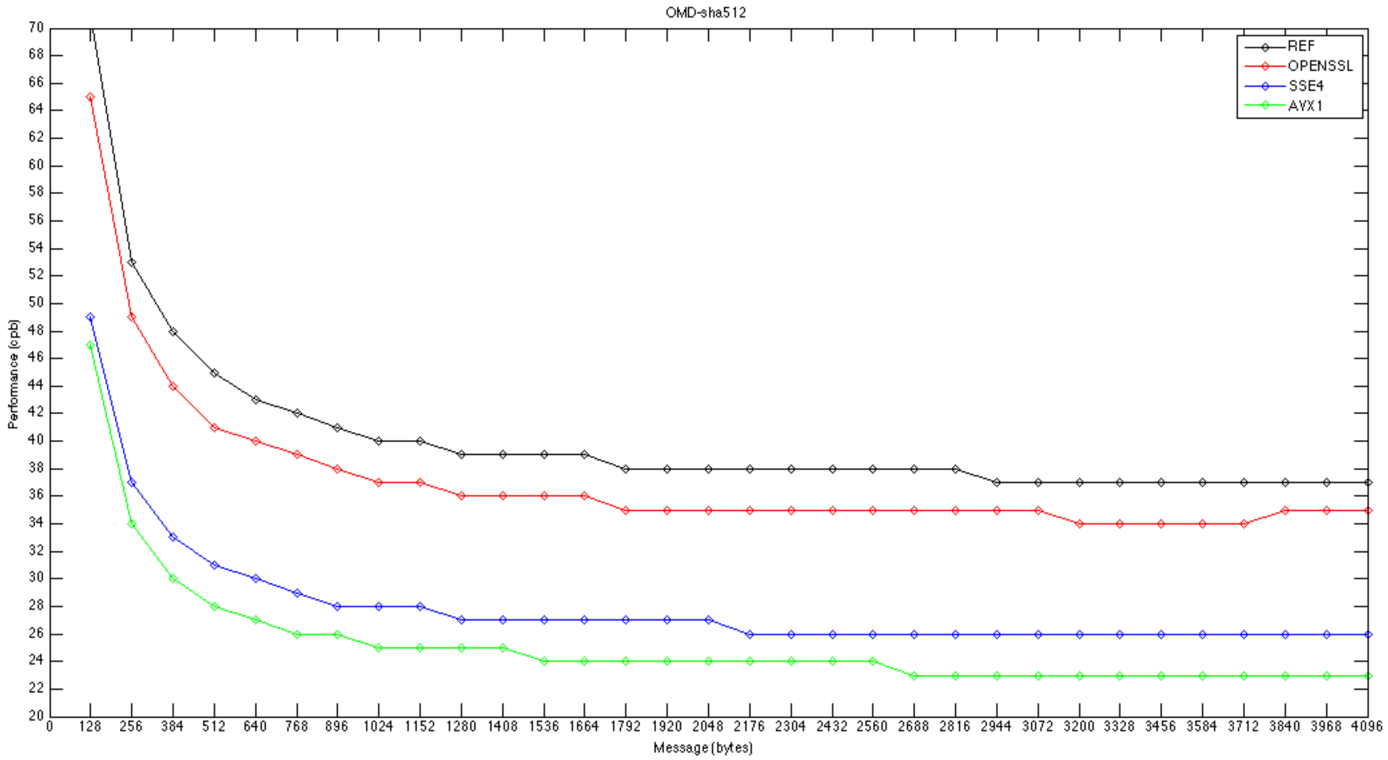
- The results show that OMD-sha256 and OMD-sha512 have reasonable software performance comparable to AES-GCM (while providing much higher security levels).

- More optimized implementations and performance measurements will be available through the CAESAR website .

Timing Measurements for some different implementations of **OMD-sha256**

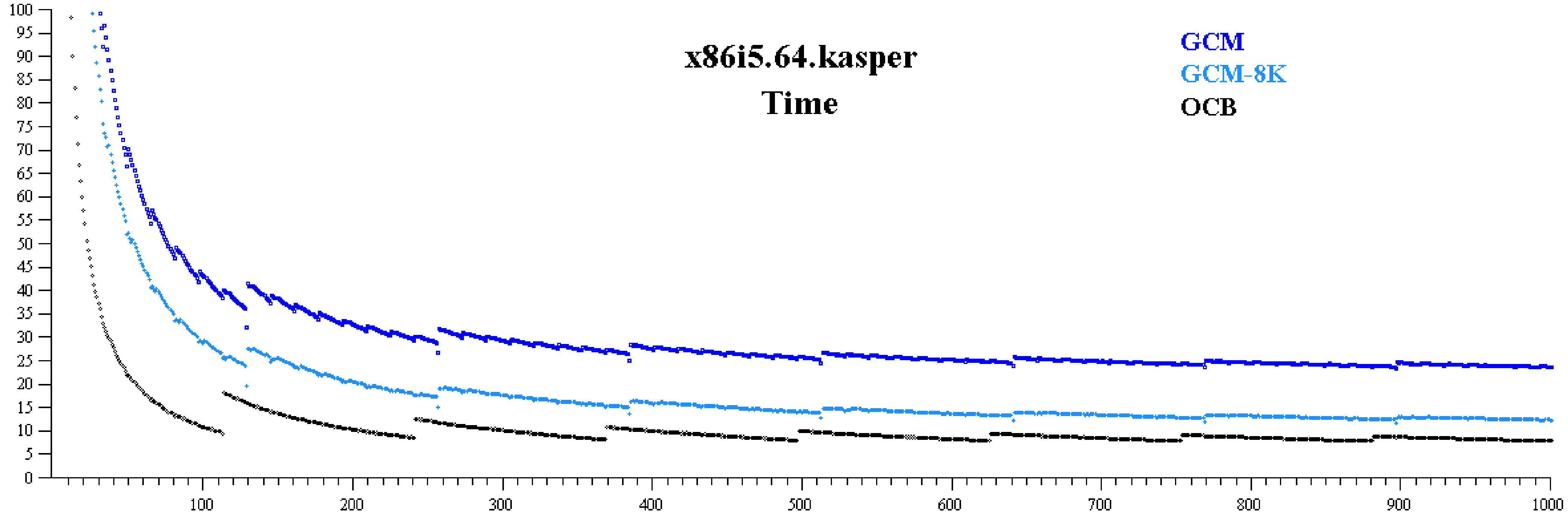


Timing Measurements for some different implementations of **OMD-sha512**



Performance of GCM and OCB (without AES-NI)

Source: http://www.cs.ucdavis.edu/~rogaway/ocb/index.html



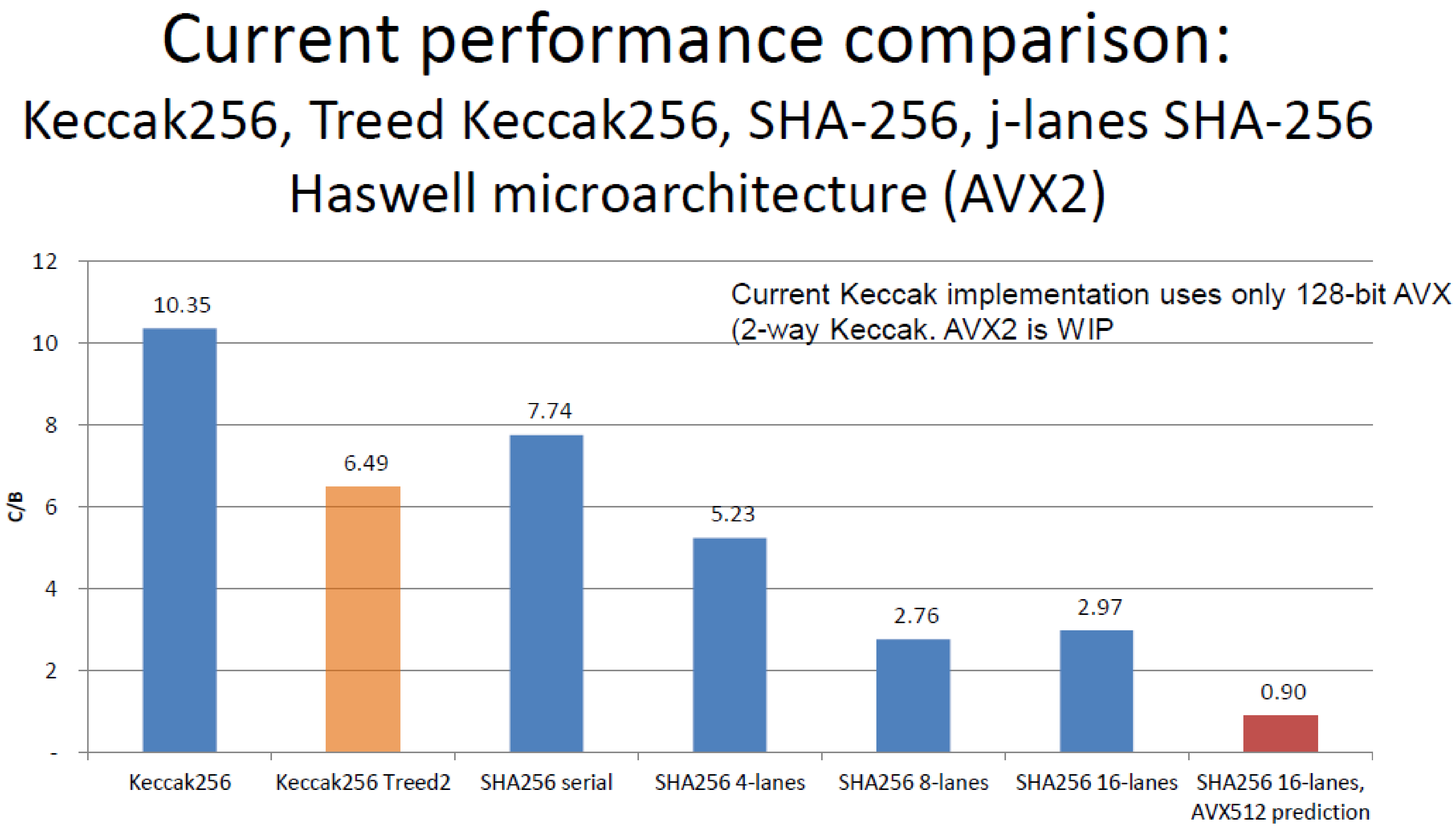
Performance and Security Comparison

Performance (rate) measurements are in “**cycles per byte**” (**cpb**).

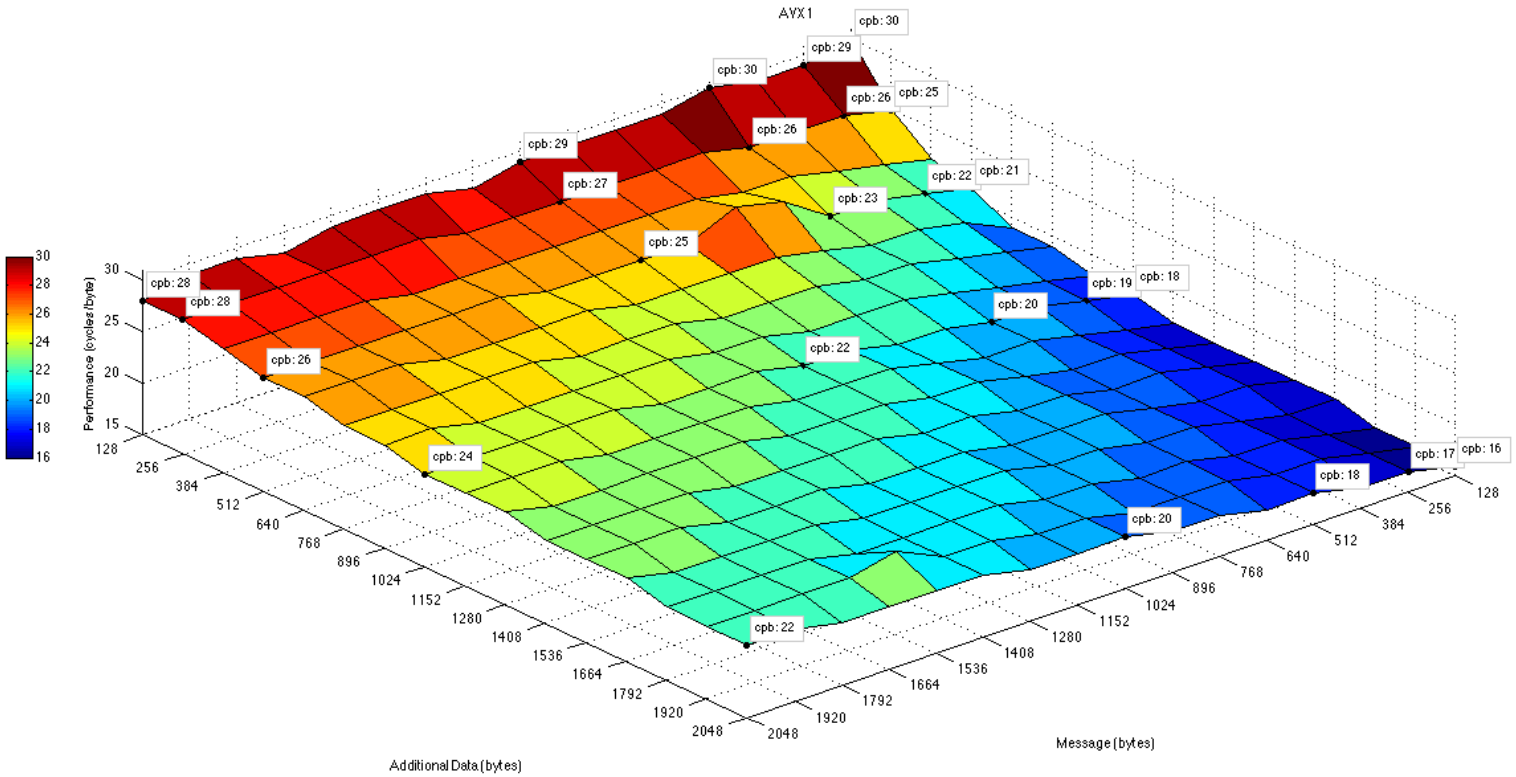
	Message length (bytes)	**AES-OCB** cpb	**AES-GCM** cpb	**OMD-sha256** cpb	**OMD-sha512** cpb
Without **AES-NI** and **Intel SHA Extensions**	128	16.14	32.31	44.56	45.93
	256	11.94	27.12	36.37	34.11
	512	9.84	24.61	32.28	28.11
	1024	8.80	23.36	30.34	25.18
	4096	**8.05**	**22.40**	**28.77**	**23.28**
With **AES-NI** and **Intel SHA Extensions**	4096	**1.48**	**4.17**	**2.87 (Projected)**	**N/A**
	Security	**64 bits**	**64 bits**	**127 bits**	**255 bits**

More recent results on performance of SHA-256 presented at the SHA3 2014 Workshop by Shay Gueron

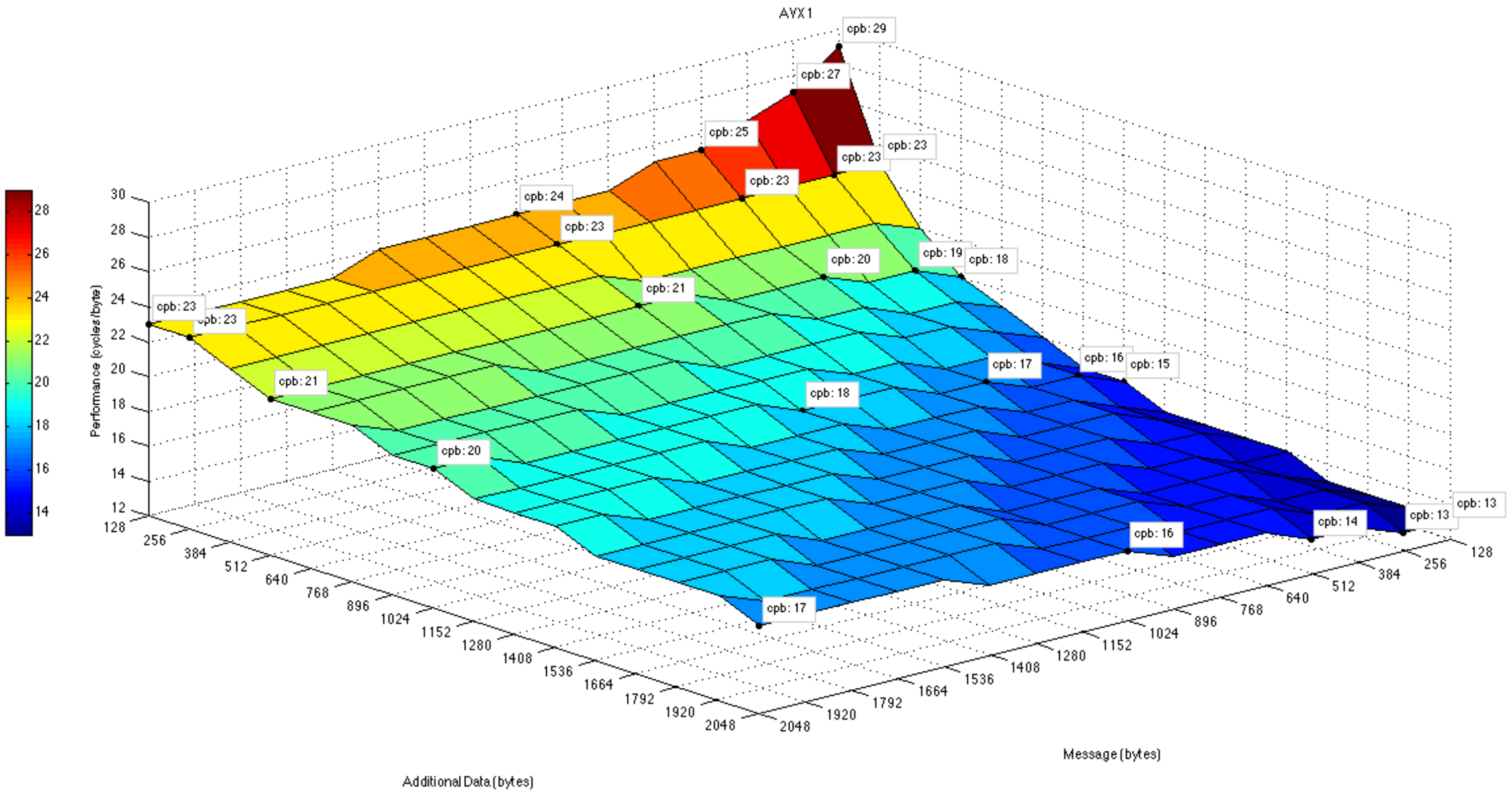
OMD-sha256 performs about 3 times slower than SHA-256, so we expect about 2.7 cpb for OMD-sha256.



OMD-sha256 Performance with Associated Data



OMD-sha512 Performance with Associated Data



OMD offers:

- ✓ **High security level** beyond the classical 64-bit security by AES-based designs (e.g. 127 bits for OMD-sha256 and 255 bits for OMD-sha512).
- ✓ **Provable security** based on a well-studied standard property of a widely-used primitive.
- ✓ **Simplicity.**
- ✓ **Patent-freeness** (does not use any patented algorithm structures; such as, PMAC or OCB as a subroutine).
- ✓ **Not relying on a blockcipher or ideal permutation** (**Don't Put All Your "Security" Eggs in One or Two Baskets!**)
- ✓ **Acceptable performance**, comparable with that of the standardized AES-GCM scheme.
  - ❖ On **future processors with Intel SHA Extensions**, OMD-sha256 will offer an appealing combination of **high performance (about 3 cpb)** <u>and</u> **high security level (127 bits)**.

Nonce-Misuse Resistance?

OMD, as submitted to CAESAR, is not aimed to be misuse resistant <u>because</u> we want to have an online encryption process!

It has some weak level of misuse resistance (e.g. authenticity of the message is preserved) but <u>we do not claim any security beyond nonce reuse.</u>

Nonce-Misuse Resistance?

Can an online AEAD provide any useful privacy after nonce is reused?

I have posted a note answering this question negatively to the Google discussion group of CAESAR titled "Carefull with Misuse-Resistance of Online AEAD Schemes".

Nonce-Misuse Resistance?

“Misuse Resistant variants of the OMD Authenticated Encryption Scheme” can be found in our paper in <u>ProvSec 2014</u>.

These variants, as expected, are <u>two-pass</u> unlike OMD which is one-pass.

Thanks!

Questions?

References:

1. Bellare, M.: New Proofs for NMAC and HMAC: Security Without Collision-Resistance. IACR Cryptology ePrint Archive 2006, 43 (2006)

2. Bellare, M., Desai, A., Jokipii, E., Rogaway, P.: A Concrete Security Treatment of Symmetric Encryption. In: FOCS. pp. 394–403 (1997)

3. Bellare, M., Namprempre, C.: Authenticated Encryption: Relations among Notions and Analysis of the Generic Composition Paradigm. In: Okamoto, T. (ed.) ASIACRYPT 2000. LNCS, vol. 1976, pp. 531–545. Springer (2000)

4. Bellare, M., Namprempre, C.: Authenticated Encryption: Relations among Notions and Analysis of the Generic Composition Paradigm. J. Cryptology 21(4), 469–491 (2008)

5. Bellare, M., Rogaway, P.: Encode-Then-Encipher Encryption: How to Exploit Nonces or Redundancy in Plaintexts for Efficient Cryptography. In: Okamoto, T. (ed.) ASIACRYPT 2000. LNCS, vol. 1976, pp. 317–330. Springer (2000)

6. Bernstein, D.J.: Cryptographic competitions: CAESAR. http://competitions.cr.yp.to

7. Canvel, B., Hiltgen, A.P., Vaudenay, S., Vuagnoux, M.: Password Interception ina SSL/TLS Channel. In: Boneh, D. (ed.) CRYPTO 2003. LNCS, vol. 2729, pp. 583–599. Springer (2003)

8. Chakraborty, D., Sarkar, P.: A General Construction of Tweakable Block Ciphers and Different Modes of Operations. IEEE Transactions on Information Theory 54(5), 1991–2006 (2008)

9. Fleischmann, E., Forler, C., Lucks, S.: McOE: A Family of Almost Foolproof On-Line Authenticated Encryption Schemes. In: Canteaut, A. (ed.) FSE. LNCS, vol. 7549, pp. 196–215. Springer (2012)

References…

10. Guilford, J., Cote, D., Gopal, V.: Fast SHA512 Implementations on Intelr Architecture Processors (Nov 2012), http://www.intel.com/content/www/us/en/intelligent-systems/intel-technology/fast-sha512-implementations-ia-processors-paper.html

11. Guilford, J., Yap, K., Gopal, V.: Fast SHA-256 Implementations on Intelr Architecture Processors (May 2012), http://www.intel.com/content/www/us/en/intelligent-systems/intel-technology/sha-256-implementations-paper.html

12. Gulley, S., Gopal, V., Yap, K., Feghali, W., Guilford, J., Wolrich, G.: Intelr SHA Extensions: New Instructions Supporting the Secure Hash Algorithm on Inter Architecture Processors (Jul 2013), https://software.intel.com/sites/default/files/article/402097/intel-sha-extensions-white-paper.pdf

13. Iwata, T.: New Blockcipher Modes of Operation with Beyond the Birthday Bound Security. In: Robshaw, M.J.B. (ed.) FSE. Lecture Notes in Computer Science, vol. 4047, pp. 310–327. Springer (2006)

14. Iwata, T.: Authenticated Encryption Mode for Beyond the Birthday Bound Security.In: Vaudenay, S. (ed.) AFRICACRYPT. Lecture Notes in Computer Science, vol. 5023, pp. 125–142. Springer (2008)

15. Katz, J., Yung, M.: Unforgeable Encryption and Chosen Ciphertext Secure Modes of Operation. In: Schneier, B. (ed.) FSE 2000. LNCS, vol. 1978, pp. 284–299. Springer (2001)

16. Krovetz, T., Rogaway, P.: The Software Performance of Authenticated-Encryption Modes. In: Joux, A. (ed.) FSE 2011. LNCS, vol. 6733, pp. 306–327. Springer (2011)

17. Landecker, W., Shrimpton, T., Terashima, R.S.: Tweakable Blockciphers with Beyond Birthday-Bound Security. In: Safavi-Naini, R., Canetti, R. (eds.) CRYPTO. Lecture Notes in Computer Science, vol. 7417, pp. 14–30. Springer (2012)

18. Lefranc, D., Painchault, P., Rouat, V., Mayer, E.: A Generic Method to Design Modes of Operation Beyond the Birthday Bound. In: Adams, C.M., Miri, A., Wiener, M.J. (eds.) Selected Areas in Cryptography. Lecture Notes in Computer Science, vol. 4876, pp. 328–343. Springer (2007)

References…

19. Namprempre, C., Rogaway, P., Shrimpton, T.: Reconsidering Generic Composition. In: Nguyen, P.Q., Oswald, E. (eds.) EUROCRYPT. Lecture Notes in Computer Science, vol. 8441, pp. 257–274. Springer (2014)

20. Rogaway, P.: Authenticated-Encryption with Associated-Data. In: ACM Conference on Computer and Communications Security. pp. 98–107 (2002)

21. Rogaway, P.: Efficient Instantiations of Tweakable Blockciphers and Refinements to Modes OCB and PMAC. In: ASIACRYPT. pp. 16–31 (2004)

22. Rogaway, P.: Nonce-Based Symmetric Encryption. In: Roy, B.K., Meier, W. (eds.) FSE. LNCS, vol. 3017, pp. 348–359. Springer (2004)

23. Rogaway, P., Bellare, M., Black, J., Krovetz, T.: OCB: A Block-Cipher Mode of Operation for Efficient Authenticated Encryption. In: ACM Conference on Computer and Communications Security. pp. 196–205 (2001)

24. Rogaway, P., Shrimpton, T.: A Provable-Security Treatment of the Key-Wrap Problem. In: EUROCRYPT. pp. 373–390 (2006)

25. Vaudenay, S.: Security Flaws Induced by CBC Padding - Applications to SSL, IPSEC, WTLS ... In: Knudsen, L.R. (ed.) EUROCRYPT 2002. LNCS, vol. 2332, pp. 534–546. Springer (2002)

Appendix: Criteria for the Masking Function $\Delta_K(T)$

The masking function $\Delta_K(T) = \Delta_K(\alpha, i, j)$ outputs an n-bit mask such that the following two properties hold for any fixed string $H \in \{0,1\}^n$:

1. $\Pr[\Delta_K(\alpha, i, j) = H] \le 2^{-n}$ for any (α, i, j)
2. $\Pr[\Delta_K(\alpha, i, j) \oplus \Delta_K(\alpha', i', j') = H] \le 2^{-n}$ for $(\alpha, i, j) \neq (\alpha', i', j')$

where the probabilities are taken over random selection of the key.

Appendix: Computing the Masking Function

There are different ways to compute the masking values to satisfy these criteria. In OMD, we use the method proposed by Krovetz and Rogaway in FSE 2011 [16].

Initialization:
$\varDelta_{N,0,0} = F_K(N||10^{n-1-|N|}, 0^m)$; $\bar{\varDelta}_{0,0} = 0^n$; $L_* = F_K(0^n, 0^m)$; $L(0) = 4 \cdot L_*$, and $L(i) = 2 \cdot L(i-1)$ for $i \geq 1$.

Masking sequence for processing the message:
For $i \geq 1$: $\varDelta_{N,i,0} = \varDelta_{N,i-1,0} \oplus L(\mathtt{ntz}(i))$; $\varDelta_{N,i,1} = \varDelta_{N,i,0} \oplus 2 \cdot L_*$; and $\varDelta_{N,i,2} = \varDelta_{N,i,0} \oplus 3 \cdot L_*$.

Masking sequence for processing the associated data:
$\bar{\varDelta}_{i,0} = \bar{\varDelta}_{i-1,0} \oplus L(\mathtt{ntz}(i))$ for $i \geq 1$; and $\bar{\varDelta}_{i,1} = \bar{\varDelta}_{i,0} \oplus L_*$ for $i \geq 0$.