NIST Workshop on the Requirements for an Accordion Cipher Mode 2024

Efficient Instances of Docked Double Decker With AES, and Application to Authenticated Encryption

Christoph Dobraunig[1], Krystian Matusiewicz[1], Bart Mennink[2], Alexander Tereschenko[1]

[1] Intel, [2] Radboud University

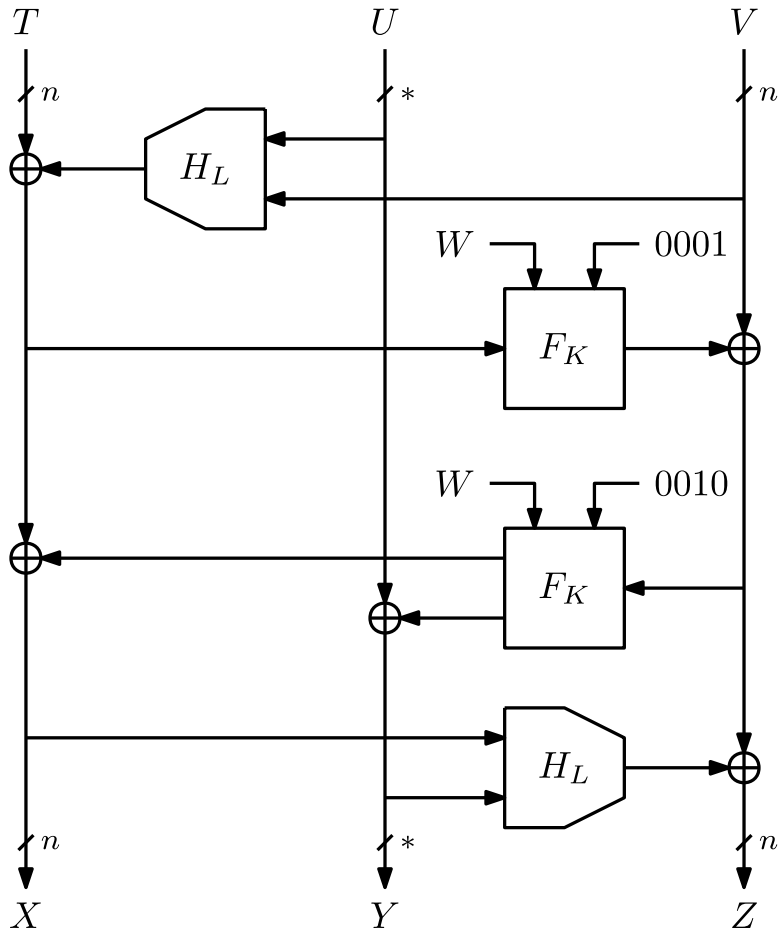
Notices & Disclaimers

- Performance varies by use, configuration and other factors. Learn more at www.Intel.com/PerformanceIndex.
- No product or component can be absolutely secure. Your costs and results may vary. Results have been estimated or simulated.
- Intel technologies may require enabled hardware, software or service activation.
- Intel does not control or audit third-party data. You should consult other sources to evaluate accuracy.
- These materials are provided “as is.” Intel disclaims all express and implied warranties, including without limitation, the implied warranties of merchantability, fitness for a particular purpose, and non-infringement, as well as any warranty arising from course of performance, course of dealing, or usage in trade.
- Intel, the Intel logo, and other Intel marks are trademarks of Intel Corporation or its subsidiaries. Other names and brands may be claimed as the property of others.

Overview

- The docked double decker
- 3 instances
  - ddd-AES
  - ddd-AES+
  - bbb-ddd-AES
- Design rationale
- Practical implications

The Docked Double Decker [GDM19]



- Building Blocks
  - F_K: stream cipher
  - H_L: universal hash
- Construction
  - Feistel-like structure
  - Outer lanes of fixed size
  - Inner lane of variable size

Security of the Docked Double Decker [GDM19]

- Generic security
  - Assume
    - H_L is ε-XOR-universal
    - F_K is PRF-secure
  - Adversary makes q queries and at most q_W queries per tweak W
  - Docked double decker is designed to be secure up to approximately

$$\sum_{W \in \{0,1\}^w} \binom{q_W}{2} \epsilon + \mathbf{Adv}_F^{\mathrm{prf}}(2q)$$

- Implications
  - Birthday bound secure in n in general case
  - Security can significantly increase when tweaks are not used too often

Our Goals and Hurdles to Overcome

- Goals
  - Build upon widely used components (NIST standards)
    - AES [DR02, DR20]
    - Operations in binary extension fields, e.g., like GHash [MV04]
  - Efficient in parallel use of components
  - Birthday bound and beyond-birthday bound secure instances that fit NIST's accordion idea
- Hurdles
  - AES
    - Not a tweakable blockcipher
    - 128-bit blocksize
    - Typical stream cipher modes only give birthday-bound security

Universal Hash Function Instantiation

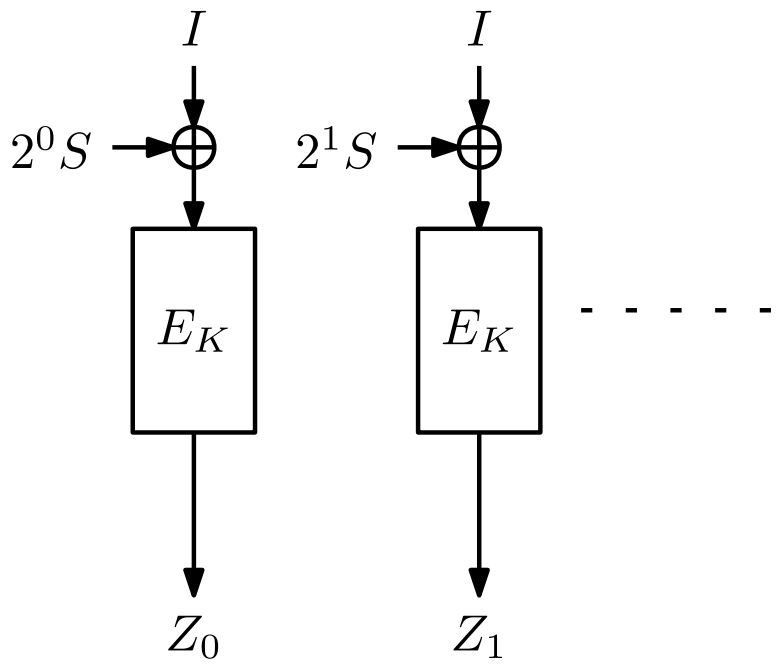
- Polyval [GLL17]
  - Operates on finite field $GF(2^{128})[x]/(x_{128} + x_{127} + x_{126} + x_{121} + 1)$
  - Defined as follows, for a padded message $(I_1, I_2, \ldots, I_s)$:

$$Polyval_L(I_1, I_2, \ldots, I_s) = \sum_{i=1}^{s} \left(L^{s-i+1} \cdot I_i \cdot x^{-128 \cdot (s-i+1)} \right)$$

  - We use zero padding with length extension
  - Polyval is ε-XOR-universal with $\varepsilon = \frac{m_{max}}{2^{128}}$ [GLL17]

Instantiation for Birthday Bound Secure ddd-AES

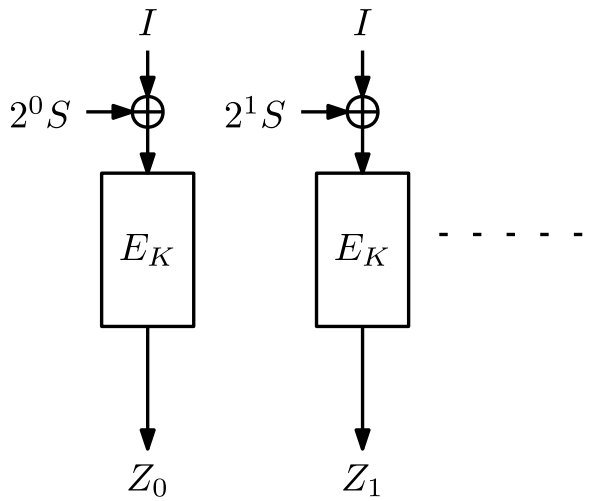
- XE-style [Rog04] tweakable blockcipher in counter mode
  - Let $S = E_K(B||W)$



  - Stream cipher (and thus ddd-AES) aims for $2^{n/2}$ PRF security

ddd-AES$^+$ for Variable Length Tweaks

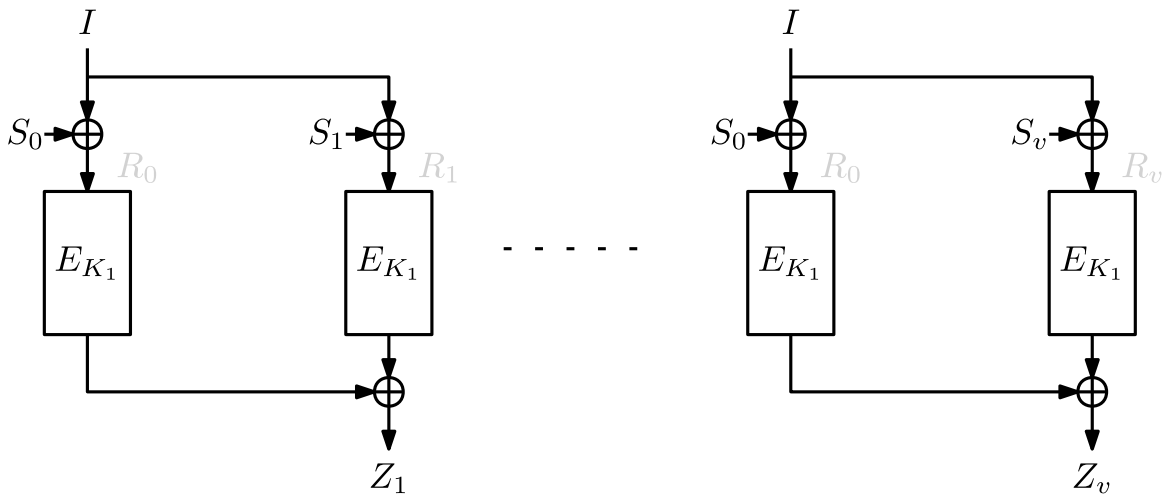
- XE-style [Rog04] tweakable blockcipher in counter mode
  - Pad B, W into $(W_0, W_1, \ldots, W_{l-1}||B'||0^*)$ with $B' = B \oplus 1000$
  - Let $S = E_K(W_0||0) \oplus E_K(W_1||1) \oplus \cdots \oplus E_K\left(W_{l-1}||B'||0^*||(l-1)\right)$



  - Stream cipher (and thus ddd-AES$^+$) aims for $2^{n/2}$ PRF security

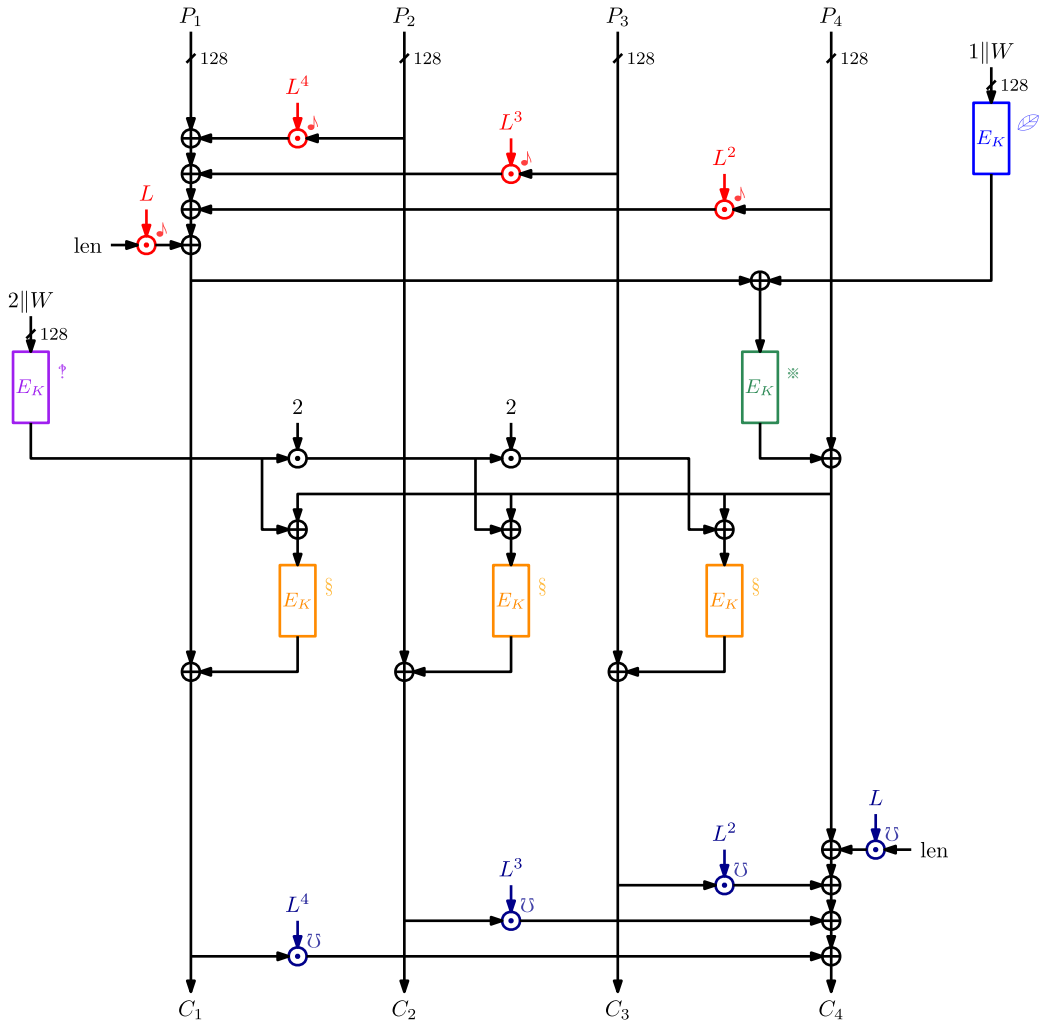
Instance Beyond Birthday Bound Secure bbb-ddd-AES

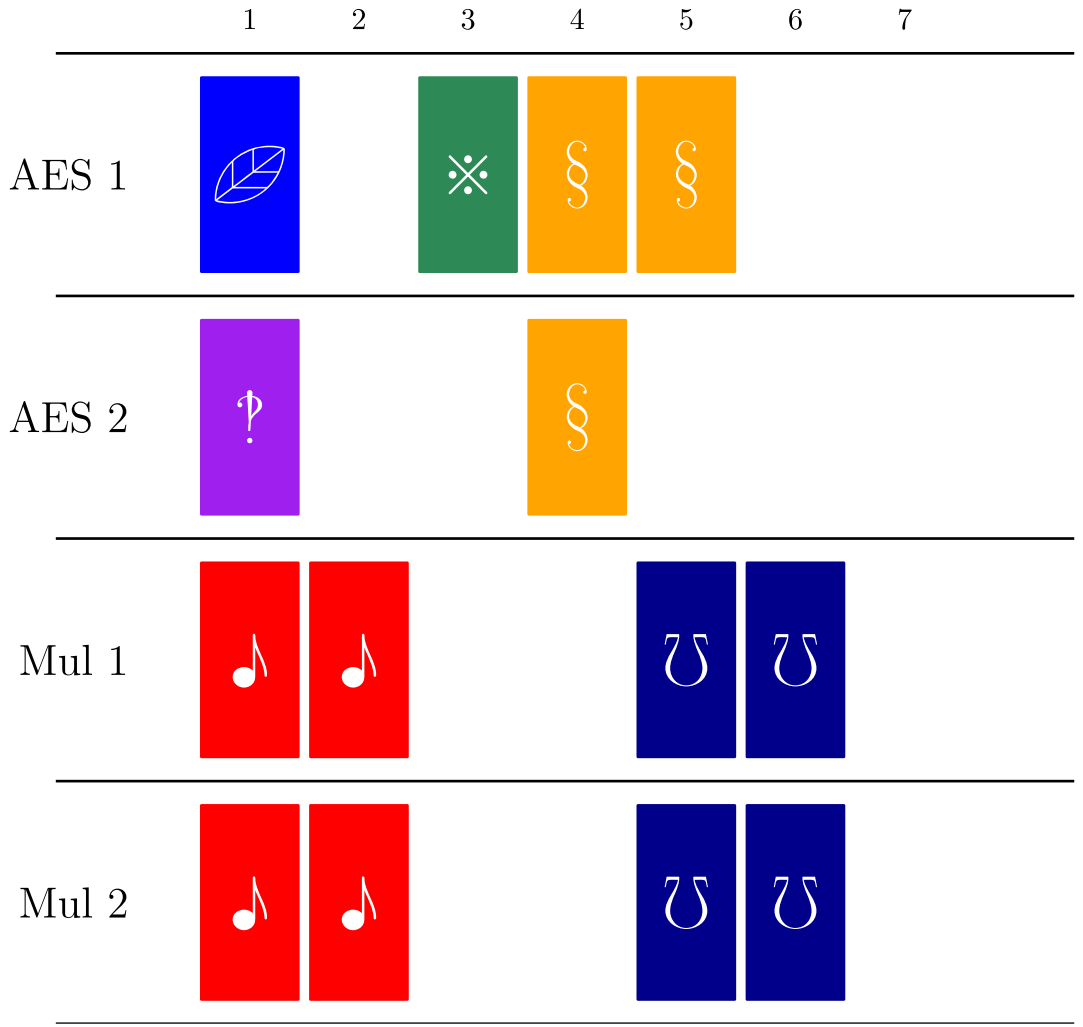
- $\widetilde{XORP}$ PRF in counter mode
  - $\widetilde{XORP}$: $XORP$ as in CENC [Iwa06] extended to include tweak
    - New and comes with separate security proof
    - Let $S_j = E_{K_2}(B||W||c||j)$



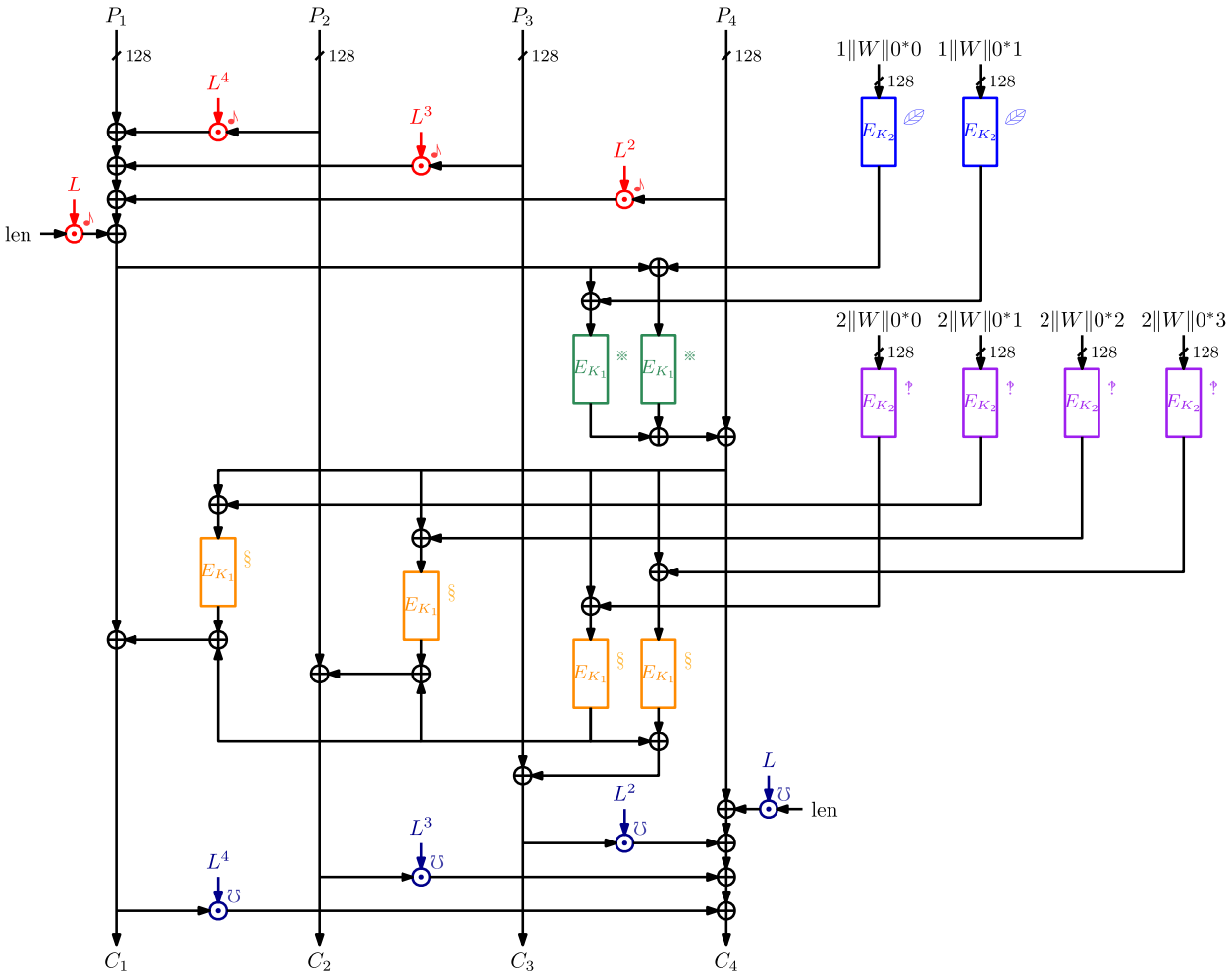
  - Stream cipher (and thus bbb-ddd-AES) aims for $2^{2n/3}$ PRF security when tweaks are not reused too often

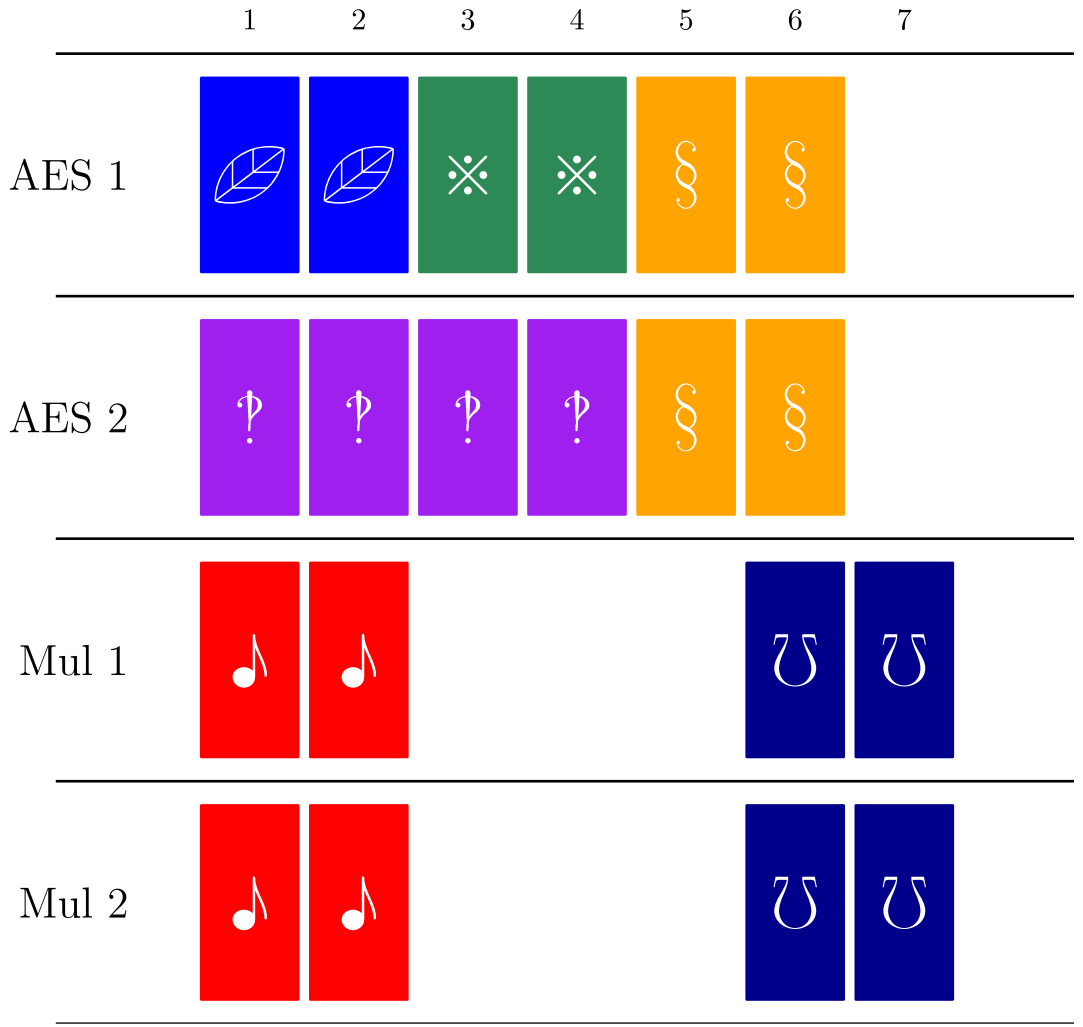
Design Rationale: ddd-AES with 512-bit blocks



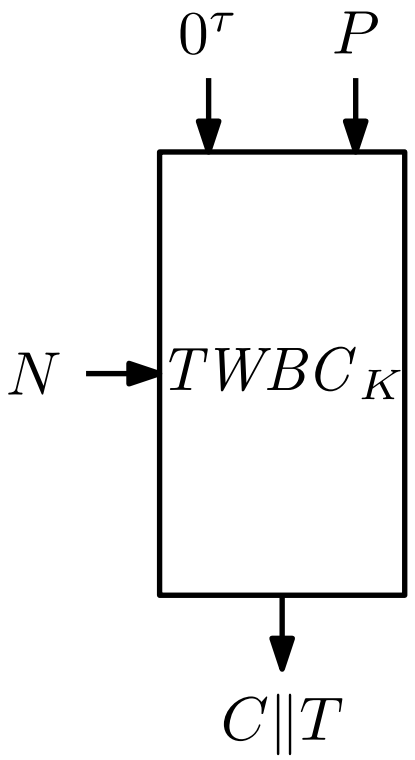


Design Rationale: bbb-ddd-AES with 512-bit blocks



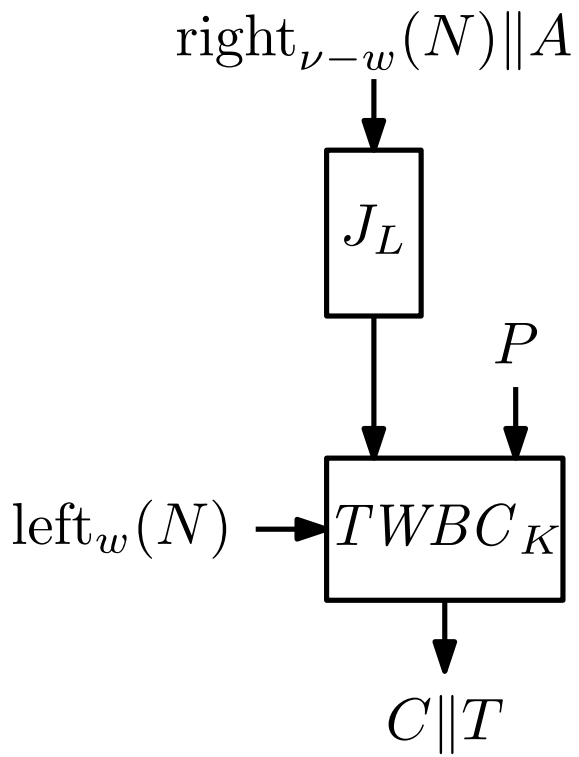


Basic Authenticated Encryption



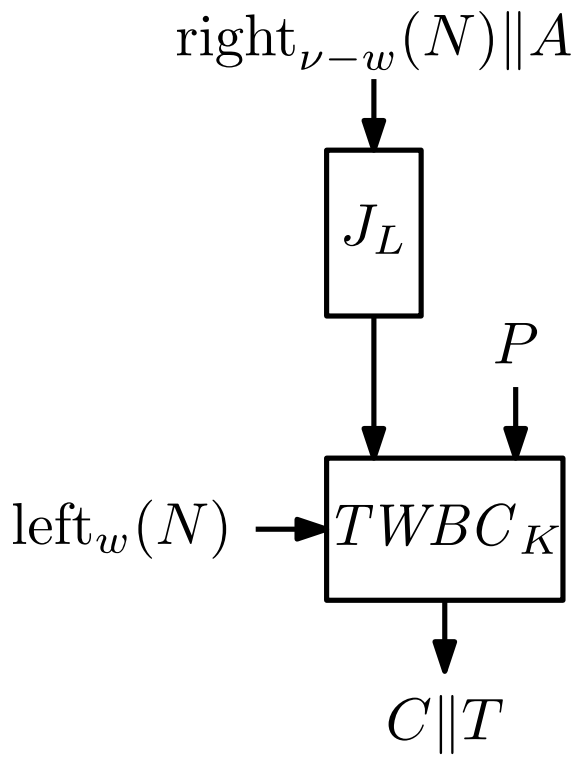
- Robust AE [HKR15]
  - Encryption:
    - Prepend τ zeros to P
    - Evaluate with $TWBC_K$ to obtain $C||T$
  - Decryption:
    - Decrypt $C||T$ using $TWBC_K^{-1}$
    - If the result starts with τ zeros: output P
- Limitations in our context
  - No associated data (ddd-AES$^+$ okay)

Advanced Authenticated Encryption with Associated Data (aaa)



- Building blocks
  - $TWBC_K$: tweakable wide blockcipher
  - J_L: universal hash
- Rationale
  - N partially entered into tweak
  - Rest of N and A hashed into τ -bit string

aaa: Security



- Nonce-respecting setting
  - $left_w(N)$ unique for each encryption query
  - Security analysis relies on fact that tweak to $TWBC_K$ is always new
- Random nonce setting
  - N is random for each encryption query
  - Security analysis relies on multicollision bound on the left w bits of the nonce
- Nonce-misusing setting
  - Birthday bound security

bbb-ddd-AES Example: Memory Encryption

- Assume advantage $\leq 2^{-32}$

- AES-XTS
  - 4 Terabyte of RAM (2^{40} lines) encrypted with one key
  - Write each line 2^{6} times

- bbb-ddd-AES
  - 4 Exabyte of RAM (2^{60} lines) encrypted with one key
  - Write each line 2^{11} times
  - And, e.g., 2^{20} lines 2^{30} times

aaa-bbb-ddd-AES Example: TLS

- AES-GCM
  - $2^{24.5}$ records of size up to $2^{14} + 1$ octets
  - Advantage below 2^{-57}

- aaa-bbb-ddd-AES
  - 2^{51} records of size up to $2^{14} + 1$ octets
  - Advantage below 2^{-57}
  - Plus other benefits like nonce-misuse resistance

Conclusion

- Introduced ddd-AES, ddd-AES+, and bbb-ddd-AES
- Schemes come with security reduction to AES
- Also introduced authenticated encryption mode aaa for TWBCs
- Paper at https://eprint.iacr.org/2024/084

Bibliography

Bibliography

- [DR02] Joan Daemen and Vincent Rijmen. The Design of Rijndael: AES - The Advanced Encryption Standard. Information Security and Cryptography. Springer, 2002.
- [DR20] Joan Daemen and Vincent Rijmen. The Design of Rijndael - The Advanced Encryption Standard (AES), Second Edition. Information Security and Cryptography. Springer, 2020.
- [GDM19] AIdo Gunsing, Joan Daemen, and Bart Mennink. Deck-Based Wide Block Cipher Modes and an Exposition of the Blinded Keyed Hashing Model. IACR Trans. Symmetric Cryptol., 2019(4):1–22, 2019.
- [GLL17] Shay Gueron, Adam Langley, and Yehuda Lindell. AES-GCM-SIV: Specification and Analysis. Cryptology ePrint Archive, Report 2017/168, 2017. http://eprint.iacr.org/2017/168.

Bibliography

- [DR02] Viet Tung Hoang, Ted Krovetz, and Phillip Rogaway. Robust Authenticated-Encryption AEZ and the Problem That It Solves. In Elisabeth Oswald and Marc Fischlin, editors, Advances in Cryptology - EUROCRYPT 2015, Proceedings, Part I, volume 9056 of Lecture Notes in Computer Science, pages 15–44. Springer, 2015.
- [Iwa06] Tetsu Iwata. New Blockcipher Modes of Operation with Beyond the Birthday Bound Security. In Matthew J. B. Robshaw, editor, FSE 2006, Revised Selected Papers, volume 4047 of Lecture Notes in Computer Science, pages 310–327. Springer, 2006.
- [MV04] David A. McGrew and John Viega. The Security and Performance of the Galois/Counter Mode (GCM) of Operation. In Anne Canteaut and Kapalee Viswanathan, editors, INDOCRYPT 2004, December 20-22, 2004, Proceedings, volume 3348 of Lecture Notes in Computer Science, pages 343–355. Springer, 2004.
- [Rog04] Phillip Rogaway. Efficient Instantiations of Tweakable Blockciphers and Refinements to Modes OCB and PMAC. In Pil Joong Lee, editor, Advances in Cryptology - ASIACRYPT 2004, Proceedings, volume 3329 of Lecture Notes in Computer Science, pages 16–31. Springer, 2004


intel