DoveMAC

Tony Grochow[1] Eik List[1] Mridul Nandi[2]

[1]Bauhaus-Universität Weimar, Germany

[2]Indian Statistical Institute, Kolkata, India

Nov 2020

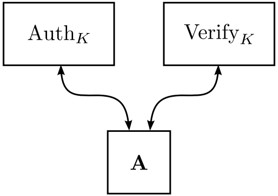
Section 1

Motivation

Message Authentication Codes

- Goal: Data authentication via unforgeable authentication tags
- Stateful, randomized, nonce-based, or **stateless deterministic** (our focus)

MAC security

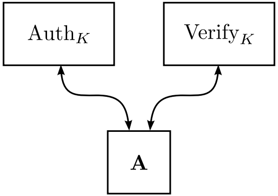


$$\mathbf{Adv}_F^{\mathsf{MAC}}(\mathbf{A}) \stackrel{\mathsf{def}}{=} \Pr_{K \twoheadleftarrow \mathcal{K}} [\mathbf{A}\ \text{forges}]$$

Message Authentication Codes

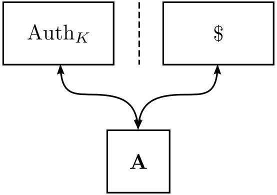
MAC and PRF Security

MAC security



$$\mathbf{Adv}_F^{\mathsf{MAC}}(\mathbf{A}) \stackrel{\text{def}}{=} \Pr_{K \twoheadleftarrow \mathcal{K}}[\mathbf{A} \text{ forges}]$$

PRF security



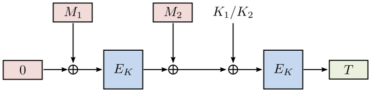
$$\mathbf{Adv}_F^{\mathsf{PRF}}(\mathbf{A}) \stackrel{\text{def}}{=} \underset{\mathbf{A}}{\Delta}(F_K; \$)$$

$\Delta_{\mathbf{A}}(X; Y) := \left| \Pr\left[\mathbf{A}^X \Rightarrow 1\right] - \Pr\left[\mathbf{A}^Y \Rightarrow 1\right] \right|$ over random choice of keys, oracles X and Y, and coins of $\mathbf{A}$ if any.

$\$$ returns $|F_K(M)|$ uniform random bits on any input M.

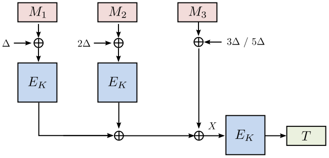
Block-cipher-based MACs

Sequential



CMAC [Dwo16]

Parallel



PMAC [BR02]

- Various Standards: CMAC [Dwo16], OMAC [IK03], f9 [ETS01], PMAC [BR02] ...

Tweakable Block Ciphers (TBCs) for MACs

TBCs [LRW02]:

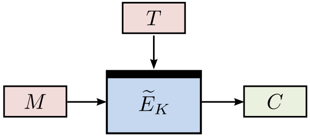
- Keyed families of permutations

$$\widetilde{E} : \mathbb{F}_2^k \times \mathbb{F}_2^t \times \mathbb{F}_2^n \to \mathbb{F}_2^n$$

- Additional public tweak T

(Not only) For MACs, tweaks are useful for:

- Domain separation $\implies$ security
- Additional message input $\implies$ efficiency



Constructions:

- PMAC_TBC1k/PMAC_TBC3k [Nai15]
- HaT [CLS17]
- ZMAC [IMPS17]
- Hashes in TBC-based AE schemes

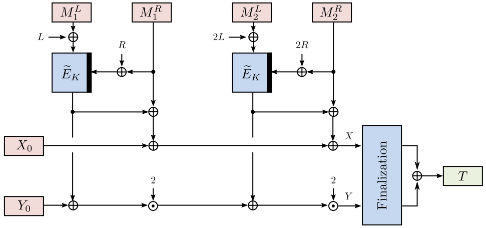
TBC-based Parallel MACs: ZMAC [IMPS17]

Combines:

- + High security: $(n+t)/2$ bits
- + Parallelizable
- + High efficiency: $n+t$ bits per primitive call

But:

- Needs relatively much memory
- May be a obstracle for microcontrollers or constrained environments



ZMAC [IMPS17]

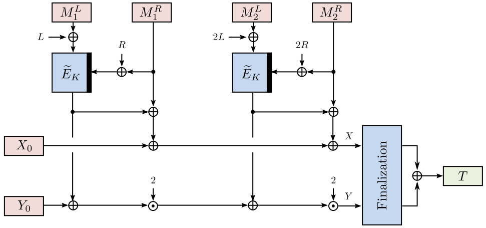
TBC-based Parallel MACs: ZMAC [IMPS17]

Combines:

+ High security: $(n+t)/2$ bits
+ Parallelizable
+ High efficiency: $n+t$ bits per primitive call

But:

- Needs relatively much memory
- May be a obstracle for microcontrollers or constrained environments

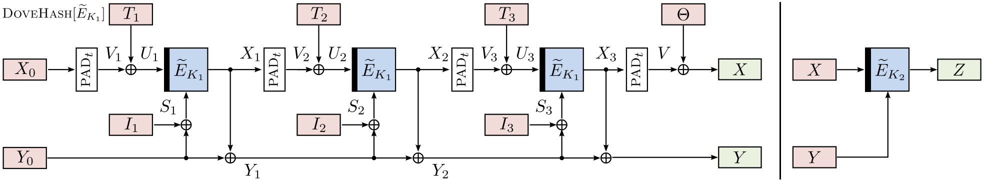


ZMAC [IMPS17]

Can we keep the **high rate** and **high security** of ZMAC but **reduce** its state **size**?

Section 2

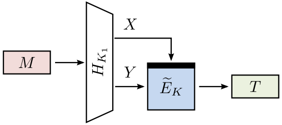
DoveMAC



- Processes $(n+t)$-bit/TBC call
- Top: t bits, extended or truncated after each call
- Bottom: n bits
- TBC output feed-forward to bottom lane after each call
- Checksum $\Theta = \sum_{i=1}^{m} T_i$ needed for beyond-birthday security

DoveMAC

Finalization



- Instance of Hash-as-Tweak (HaT) [CLS17] or its generalization Hash-then-TBC (HtTBC) [LN17]
- Easily extendable to variable-output-length PRF
- n-bit-secure if hash function H optimal
- Single-key version easily obtainable: reserve one tweak domain bit

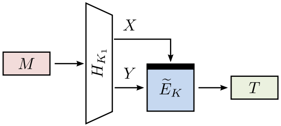
Section 3

Proof Sketch

Proof Sketch: PRF Security of DoveMAC

Steps:

1. Replace primitives with ideal tweakable permutations
2. Reduce to Hash-then-TBC
3. Upper bound collision probability of DoveHash
4. Upper bound truncated-almost universality of DoveHash

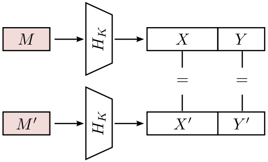


Proof Sketch: Notions

Definition 1 (Collision Probability)

Collision among at most q pairwise distinct messages $M \neq M'$ of at most m b-bit blocks each and σ b-bit blocks in total:

$$\mathsf{coll}_H(b, q, m, \sigma) \stackrel{\mathsf{def}}{=} \Pr_{\substack{K \twoheadleftarrow \mathcal{K} \\ M \neq M'}} \left[H_K(M) = H_K\left(M'\right) \right] .$$

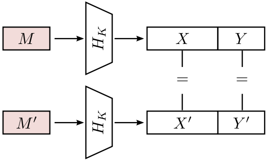


Proof Sketch: Notions

Definition 1 (Collision Probability)

Collision among at most q pairwise distinct messages $M \neq M'$ of at most m b-bit blocks each and σ b-bit blocks in total:

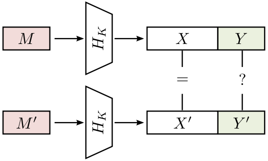
$$\mathsf{coll}_H(b, q, m, \sigma) \stackrel{\mathsf{def}}{=} \Pr_{\substack{K \twoheadleftarrow \mathcal{K} \\ M \neq M'}} \left[H_K(M) = H_K\left(M'\right) \right].$$



Definition 2 (Truncated Almost-Universality)

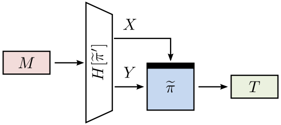
$H : \mathcal{K} \times \mathcal{M} \to \mathbb{F}_2^t \times \mathbb{F}_2^n$ is (t, n, ϵ)-truncated-AU if for all $M \neq M'$:

$$\sum_{\Delta \in \mathbb{F}_2^n} \Pr_{K \twoheadleftarrow \mathcal{K}} \left[H_K(M) \oplus H_K(M') = (0^t, \Delta) \right] \leq \epsilon.$$



Proof Sketch: (1) Ideal Primitive

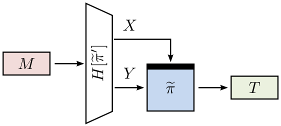
- Replace primitives with ideal tweakable permutations:
  From $\underbrace{\widetilde{E}_{K_1}, \widetilde{E}_{K_2}}$ from $K_1, K_2 \twoheadleftarrow \mathcal{K}$
  $\implies \widetilde{\pi}, \widetilde{\pi}' \twoheadleftarrow \mathsf{Perm}(\mathbb{F}_2^t, \mathbb{F}_2^n)$



$$\mathbf{Adv}^{\mathsf{PRF}}_{\mathsf{DoveMAC}\left[\widetilde{E}_{K_1}, \widetilde{E}_{K_2}\right]}(\mathbf{A}) \leq \mathbf{Adv}^{\mathsf{PRF}}_{\mathsf{DoveMAC}\left[\widetilde{\pi}, \widetilde{\pi}'\right]}(\mathbf{A}') + (\sigma + q) \cdot \mathbf{Adv}^{\mathsf{TPRP}}_{\widetilde{E}_K}(\mathbf{A}'') \,.$$

Proof Sketch: (2) Reduce to HtTBC

$$\mathbf{Adv}^{\mathsf{PRF}}_{\mathsf{DoveMAC}\left[\widetilde{\pi},\widetilde{\pi}'\right]}(\mathbf{A}) \leq \mathbf{Adv}^{\mathsf{PRF}}_{\mathsf{HtTBC}\left[\widetilde{\pi}',\mathsf{DoveHash}\left[\widetilde{\pi}\right]\right]}(\mathbf{A}')$$



Theorem 3 (PRF Security of HtTBC [LN17])

Let H denote DoveHash$[\widetilde{\pi}]$. Assume that

$$\mathsf{coll}_H(n+t, q, m, \sigma) \leq \epsilon_1 \, ,$$

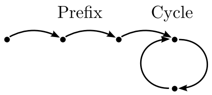
and H is (t, n, ϵ_2)-tAU. Let $\mathbf{A}$ be a PRF adversary against HtTBC$[\widetilde{\pi}', H]$ that makes at most q queries consisting at most m $(t+n)$-bit blocks after padding each, that sum to at most σ $(t+n)$-bit blocks in total. Then

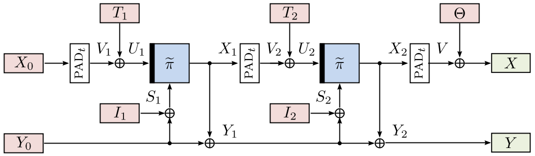
$$\mathbf{Adv}^{\mathsf{PRF}}_{\mathsf{HtTBC}[\widetilde{\pi}',\mathsf{DoveHash}[\widetilde{\pi}]]}(\mathbf{A}) \leq \epsilon_1 + \frac{\binom{q}{2} \cdot \epsilon_2}{2^n} \, .$$

Proof Sketch: (3) Upper Bounding The Collision Probability

Structure Graphs [BPR05]

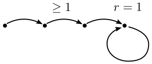
- Vertices $\mathcal{V}$: State values $v_i = B_i = (U_i, S_i)$
- Edges $\mathcal{E}$: transitions $(v_i, v_{i+1}, \lambda_i)$
- Labels Λ: $\lambda_i = (T_i, I_i)$
- Walk: Sequence of vertices $\mathbf{v} = (v_0, \ldots, v_m)$



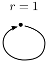


Proof Sketch: (3) Upper Bounding The Collision Probability

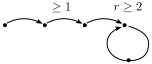
Bad structure graphs in a message M:



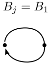
$$\Pr[\mathsf{bad}_1] \leq \frac{m}{2^n - m}$$



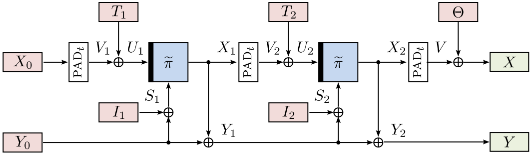
$$\Pr[\mathsf{bad}_2] \leq \frac{m}{2^n - m}$$



$$\Pr[\mathsf{bad}_3] \leq \frac{2^{\max(0, n-t)} \binom{m}{2}}{(2^n - m)^2}$$



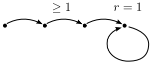
$$\Pr[\mathsf{bad}_4] \leq \frac{2^{\max(0, n-t)} \binom{m}{2}}{(2^n - m)^2}$$



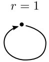
$m, \sigma < 2^{n-2}$

Proof Sketch: (3) Upper Bounding The Collision Probability

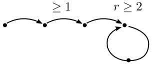
Bad structure graphs in a message M:



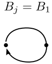
$$\Pr[\mathsf{bad}_1] \leq \frac{m}{2^n - m}$$



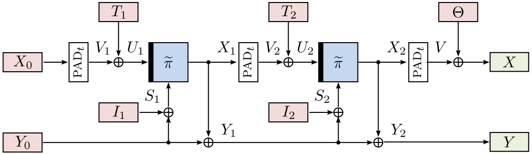
$$\Pr[\mathsf{bad}_2] \leq \frac{m}{2^n - m}$$



$$\Pr[\mathsf{bad}_3] \leq \frac{2^{\max(0, n-t)} \binom{m}{2}}{(2^n - m)^2}$$



$$\Pr[\mathsf{bad}_4] \leq \frac{2^{\max(0, n-t)} \binom{m}{2}}{(2^n - m)^2}$$



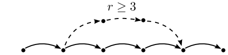
$$\Pr[\mathsf{bad}] \leq \sum_{i=1}^{q} 2 \cdot \frac{m}{2^n - \sigma} + 2 \cdot \frac{2^{\max(0, n-t)} \cdot \binom{m}{2}}{(2^n - \sigma)^2}$$

$$\leq \frac{4\sigma}{2^n} + \frac{4qm^2}{2^{n + \min(n,t)}}$$

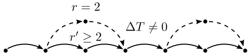
$m, \sigma < 2^{n-2}$

Proof Sketch: (3) Upper Bounding The Collision Probability

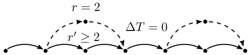
Good structure graphs of messages M and M':



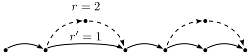
$$\Pr[\mathsf{good}_1] \leq \frac{2^{\max(0,n-t)}\binom{m}{2}}{(2^n - 2m)^2}$$



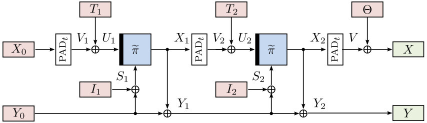
$$\Pr[\mathsf{good}_2] \leq \frac{2^{\max(0,n-t)}\binom{m}{2}}{(2^n - 2m)^2}$$



$$\Pr[\mathsf{good}_3] \leq \frac{2^{\max(0,n-t)}\binom{m}{2}}{(2^n - 2m)^2}$$



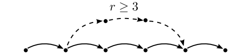
$$\Pr[\mathsf{good}_4] \leq \frac{2^{\max(0,n-t)}\binom{m}{2}}{(2^n - 2m)^2}$$



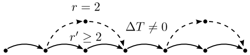
$m, \sigma < 2^{n-2}$

Proof Sketch: (3) Upper Bounding The Collision Probability

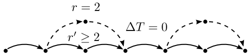
Good structure graphs of messages M and M':



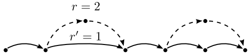
$$\Pr[\mathsf{good}_1] \leq \frac{2^{\max(0,n-t)} \binom{m}{2}}{(2^n - 2m)^2}$$



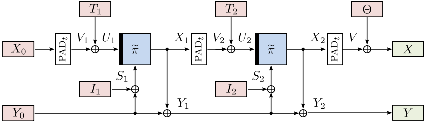
$$\Pr[\mathsf{good}_2] \leq \frac{2^{\max(0,n-t)} \binom{m}{2}}{(2^n - 2m)^2}$$



$$\Pr[\mathsf{good}_3] \leq \frac{2^{\max(0,n-t)} \binom{m}{2}}{(2^n - 2m)^2}$$



$$\Pr[\mathsf{good}_4] \leq \frac{2^{\max(0,n-t)} \binom{m}{2}}{(2^n - 2m)^2}$$



$$\Pr[\mathsf{good}] \leq \sum_{i=1}^{q} 4 \cdot \frac{2^{\max(0,n-t)} \binom{m}{2}}{(2^n - 2\sigma)^2} \leq \frac{4q^2m^2}{2^{n+\min(n,t)}}$$

$m, \sigma < 2^{n-2}$

Proof Sketch: (3) Upper Bounding The Collision Probability

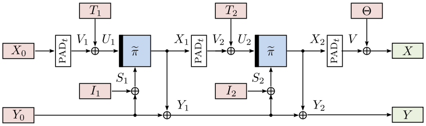
Lemma 4 (Collision Probability of DoveHash$[\widetilde{\pi}]$)

Let $\sigma < 2^{n-2}$. Then,

$$\mathsf{coll}_{\mathsf{DoveHash}[\widetilde{\pi}]}(t+n, q, m, \sigma) \leq \frac{4\sigma}{2^n} + \frac{4qm^2 + 4q^2m^2}{2^{n+\min(n,t)}}.$$

Proof Sketch: (4) Upper Bounding Truncated-AU Security

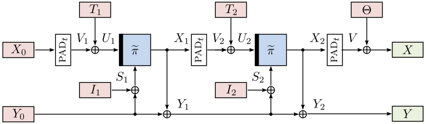
Bad walks: output loop or non-trivial output collision



$m, \sigma < 2^{n-2}$

Proof Sketch: (4) Upper Bounding Truncated-AU Security

Bad walks: output loop or non-trivial output collision



Collision of $X_i = X_j$ in M:

$$\Pr[\mathsf{bad}_1] \leq \frac{\binom{m}{2}}{2^n - 2m}$$

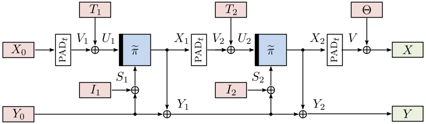
Collision $X_i = X'_j$ between M and M':

$$\Pr[\mathsf{bad}_2] \leq \frac{\binom{m}{2}}{2^n - 2m}$$

$m, \sigma < 2^{n-2}$

Proof Sketch: (4) Upper Bounding Truncated-AU Security

Bad walks: output loop or non-trivial output collision



Collision of $X_i = X_j$ in M:

$$\Pr[\mathsf{bad}_1] \le \frac{\binom{m}{2}}{2^n - 2m}$$

Collision $X_i = X'_j$ between M and M':

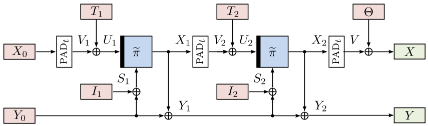
$$\Pr[\mathsf{bad}_2] \le \frac{\binom{m}{2}}{2^n - 2m}$$

$$\begin{aligned} \Pr[\mathsf{bad}] &\le \mathsf{coll}_{\mathsf{DoveHash}[\widetilde{\pi}]}(t+n, 2, m, 2m) + 2 \cdot \frac{\binom{m}{2}}{2^n - 2\sigma} \\ &\le \mathsf{coll}_{\mathsf{DoveHash}[\widetilde{\pi}]}(t+n, 2, m, 2m) + \frac{2m^2}{2^n}\,. \end{aligned}$$

$m, \sigma < 2^{n-2}$

Proof Sketch: (4) Upper Bounding Truncated-AU Security

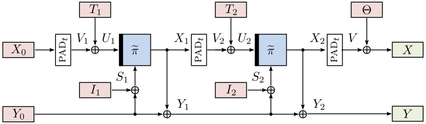
Good walks: collision in $X = X'$ without bad event



$m, \sigma < 2^{n-2}$

Proof Sketch: (4) Upper Bounding Truncated-AU Security

Good walks: collision in $X = X'$ without bad event



$\Delta\Theta \neq 0^t$:

$$\Pr[\text{good}_1] \leq \frac{2^{n-\min(t,n)}}{2^n - 2m}$$

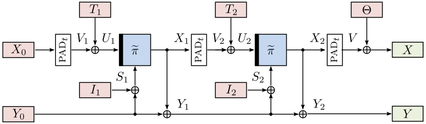
$\Delta\Theta = 0^t$:

$$\Pr[\text{good}_2] \leq \frac{2^{n-\min(t,n)}}{2^n - 2m}$$

$m, \sigma < 2^{n-2}$

Proof Sketch: (4) Upper Bounding Truncated-AU Security

Good walks: collision in $X = X'$ without bad event



$\Delta\Theta \neq 0^t$:

$$\Pr[\mathsf{good}_1] \leq \frac{2^{n-\min(t,n)}}{2^n - 2m}$$

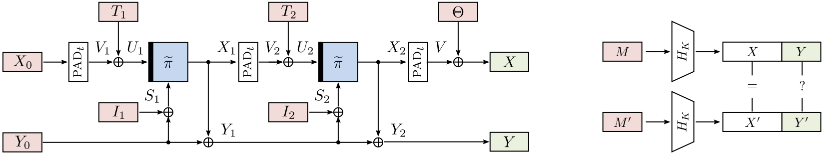
$\Delta\Theta = 0^t$:

$$\Pr[\mathsf{good}_2] \leq \frac{2^{n-\min(t,n)}}{2^n - 2m}$$

$$\Pr[X = X' | \neg\mathsf{bad}] \leq 2 \cdot \frac{2^{n-\min(n,t)}}{2^n - 2\sigma} \leq \frac{4}{2^{\min(n,t)}} .$$

$m, \sigma < 2^{n-2}$

Proof Sketch: (4) Upper Bounding Truncated-AU Security

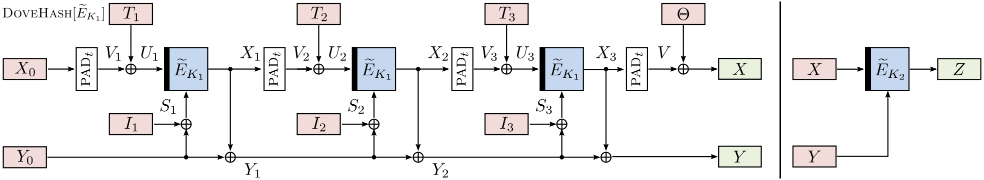


Lemma 5 (tAU Upper Bound of DoveHash$[\widetilde{\pi}]$)

Let $m, \sigma < 2^{n-2}$. Then, DoveHash$[\widetilde{\pi}]$ is (t, n, ϵ)-tAU for

$$\epsilon \leq \mathsf{coll}_{\mathsf{DoveHash}[\widetilde{\pi}]}(t+n, 2, m, 2m) + \frac{2m^2}{2^n} + \frac{4}{2^{\min(n,t)}} .$$

Proof Sketch: Summary



Theorem 6 (PRF Security of DoveMAC)

Let $\widetilde{\pi}, \widetilde{\pi}' \twoheadleftarrow \widetilde{\mathrm{Perm}}(\mathcal{T}, \mathcal{B})$. Let $\mathbf{A}$ be a PRF adversary on DoveMAC$[\widetilde{\pi}, \widetilde{\pi}']$ s.t. $\mathbf{A}$ asks at most q queries that consist of at most $m < 2^{n-2}$ $(t+n)$-bit blocks after padding each, and that sum to at most $\sigma < 2^{n-2}$ $(t+n)$-bit blocks in total. Then

$$\mathbf{Adv}^{\mathsf{PRF}}_{\mathsf{DoveMAC}[\widetilde{\pi}, \widetilde{\pi}']}(\mathbf{A}) \leq \frac{4\sigma}{2^n} + \frac{q^2 m^2}{2^{2n}} + \frac{2q^2 + 4qm^2 + 4q^2 m^2}{2^{n+\min(n,t)}}.$$

Section 4

Implementation

Implementation

Table: Rounded inverse throughputs in cycles/byte and RAM storage (bytes).

	Message length (bytes)												
	ATmega 2560							ATmega 328p					RAM
Scheme	64	128	256	512	1 024	2 048	4 096	64	128	256	512	1 024	(bytes)
DoveMAC[Skinny-64-128]	760	616	544	508	490	481	476	758	614	542	506	488	176
ZMAC1[Skinny-64-128]	1 013	757	630	566	534	518	510	1 009	755	627	564	532	236

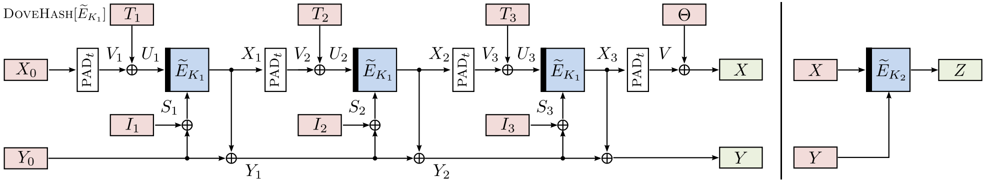
- Instantiation with Skinny-64-128 [BJK+16]
- Widespread 8-bit Atmel microcontrollers
- Comparison with ZMAC1 (ZHash [IMPS17] with HtTBC as finalization [Nai18])
- Base: Skinny AVR implementation by [BJK+16, rwe18] for both

Code available at `https://github.com/medsec/dovemac`

Section 5

Summary

Summary

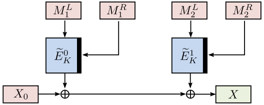


- Sequential TBC-based MAC
- High rate: $(n+t)$ bits/TBC call
- High security: $\min(n, (n+t)/2)$ bits without nonces
- Lower state size than ZMAC

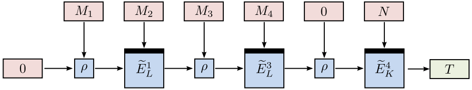
- Easily extendable to variable-output-length PRF with Hash-then-TBC
- 2 keys, but single-key version easily obtainable by using tweak bit as domain

Limitations

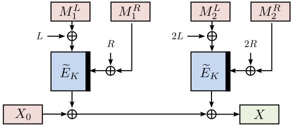
- Has grown complex
- Simpler and smaller high-rate schemes (as part of AE schemes) appeared since
- But: Nonce essential for high security



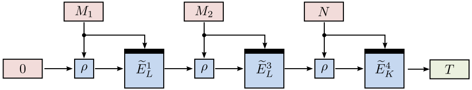
iZOCB-Hash [BGIM19]



Romulus [IKMP19, IKMP20]



iZOTR-Hash [BGIM19]



AE-TLR [GKP20]

Questions?

Bibliography I

Zhenzhen Bao, Jian Guo, Tetsu Iwata, and Kazuhiko Minematsu.
ZOCB and ZOTR: Tweakable Blockcipher Modes for Authenticated Encryption with Full Absorption.
IACR Trans. Symmetric Cryptol., 2019(2):1–54, 2019.

Christof Beierle, Jérémy Jean, Stefan Kölbl, Gregor Leander, Amir Moradi, Thomas Peyrin, Yu Sasaki, Pascal Sasdrich, and Siang Meng Sim.
SKINNY family of block ciphers – Implementations, 2016.
https://sites.google.com/site/skinnycipher/implementation.

Mihir Bellare, Krzysztof Pietrzak, and Phillip Rogaway.
Improved Security Analyses for CBC MACs.
In Victor Shoup, editor, *CRYPTO*, volume 3621 of *LNCS*, pages 527–545. Springer, 2005.

John Black and Phillip Rogaway.
A Block-Cipher Mode of Operation for Parallelizable Message Authentication.
In Lars R. Knudsen, editor, *EUROCRYPT*, volume 2332 of *LNCS*, pages 384–397. Springer, 2002.

Benoít Cogliati, Jooyoung Lee, and Yannick Seurin.
New Constructions of MACs from (Tweakable) Block Ciphers.
In *IACR Transactions on Symmetric Cryptology*, volume 2/2017, pages 27–58, 2017.

Morris J Dworkin.
NIST Special Publication 800-38B: Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication.
Technical report, NIST, 2016.
https://doi.org/10.6028/NIST.SP.800-38B, first version May 2005.

ETSI (European Telecommunications Standards Institute.
3GPP TS 35.201 Specification of the 3GPP confidentiality and integrity algorithm. Document 1: f8 and f9 specifications (version 4.1.0 Release 4).
Technical report, ETSI, December 2001.
http://www.etsi.org/deliver/etsi_ts/135200_135299/135201/04.01.00_60/ts_135201v040100p.pdf.

Bibliography II

Chun Guo, Mustafa Khairallah, and Thomas Peyrin.
Aet-lr: Rate-1 leakage-resilient aead based on the romulus family.
In *Submission to NIST Lightweight Cryptography Workshop*, 2020.

Tetsu Iwata and Kaoru Kurosawa.
OMAC: One-Key CBC MAC.
In Thomas Johansson, editor, *FSE*, volume 2887 of *LNCS*, pages 129–153. Springer, 2003.

Tetsu Iwata, Mustafa Khairallah, Kazuhiko Minematsu, and Thomas Peyrin.
Romulus v1.2.
https://csrc.nist.gov/CSRC/media/Projects/lightweight-cryptography/documents/round-2/spec-doc-rnd2/Romulus-spec-round2.pdf, Mar 29 2019.
2nd-round Submission to the NIST Lightweight competition.

Tetsu Iwata, Mustafa Khairallah, Kazuhiko Minematsu, and Thomas Peyrin.
Duel of the Titans: The Romulus and Remus Families of Lightweight AEAD Algorithms.
IACR Trans. Symmetric Cryptol., 2020(1):43–120, 2020.

Tetsu Iwata, Kazuhiko Minematsu, Thomas Peyrin, and Yannick Seurin.
ZMAC: A Fast Tweakable Block Cipher Mode for Highly Secure Message Authentication.
In Jonathan Katz and Hovav Shacham, editors, *CRYPTO, Part III*, volume 10403 of *LNCS*, pages 34–65. Springer, 2017.

Eik List and Mridul Nandi.
ZMAC+ - An Efficient Variable-output-length Variant of ZMAC.
IACR Transactions of Symmetric Cryptology, 2017(4):306–325, 2017.

Moses Liskov, Ronald L. Rivest, and David Wagner.
Tweakable Block Ciphers.
In Moti Yung, editor, *CRYPTO*, volume 2442 of *LNCS*, pages 31–46. Springer, 2002.

Bibliography III

Yusuke Naito.
Full PRF-Secure Message Authentication Code Based on Tweakable Block Cipher.
In Man Ho Au and Atsuko Miyaji, editors, *ProvSec*, volume 9451 of *LNCS*, pages 167–182. Springer, 2015.

Yusuke Naito.
On the Efficiency of ZMAC-Type Modes.
In Jan Camenisch and Panos Papadimitratos, editors, *CANS*, volume 11124 of *LNCS*, pages 190–210. Springer, 2018.

rweather.
SKINNY-C (Implementation for Arduino), Apr 8 2018.
https://github.com/rweather/skinny-c, last access 2018-11-23.