ZMAC^+ – An Efficient Variable-output-length Variant of ZMAC

Eik List[1] Mridul Nandi[2]

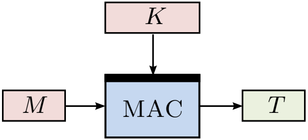
[1]Bauhaus-Universität Weimar, Weimar, Germany
[2]Indian Statistical Institute, Kolkata, India

FSE
March 2018

Section 1

Motivation

Message Authentication Codes

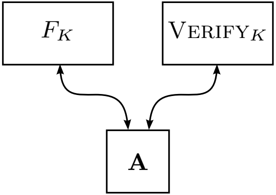


- Goal: Unforgeable authentication tags
- Stateful, randomized, nonce-based, or **stateless deterministic** (focus)
- Standards: CMAC [Dwo16], OMAC [IK03], f9 [ETS01], ...

Message Authentication Codes

MAC and PRF Security

MAC Security

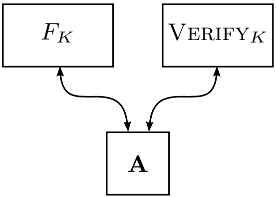


$$\mathbf{Adv}_F^{\mathrm{MAC}}(\mathbf{A}) \stackrel{\mathsf{def}}{=} \Pr_{K \twoheadleftarrow \mathcal{K}}[\mathbf{A} \text{ forges}]$$

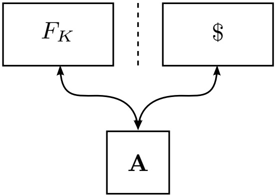
Message Authentication Codes

MAC and PRF Security

MAC Security



PRF Security



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

$$\mathbf{Adv}_F^{\mathrm{PRF}}(\mathbf{A}) \stackrel{\text{def}}{=} \Delta_{\mathbf{A}}(F_K; \$)$$

$\Delta_{\mathbf{A}}(X;Y) := \left| \Pr\left[\mathbf{A}^X \Rightarrow 1\right] - \Pr\left[\mathbf{A}^Y \Rightarrow 1\right] \right|$ 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.

Desirable Properties

Security

- High security

Desirable Properties

Security

- High security

Efficiency

- High rate
- Parallelizability
- Single key
- Single primitive

Desirable Properties

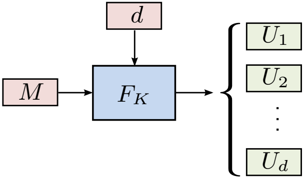
Security	Efficiency	Functionality

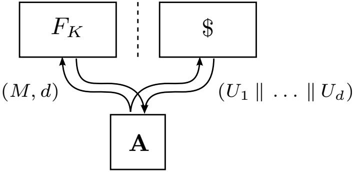
- High security

- High rate
- Parallelizability
- Single key
- Single primitive

- Variable output lengths

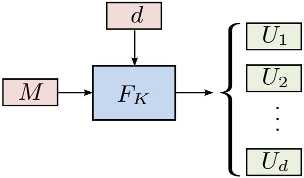
Variable-output-length PRFs

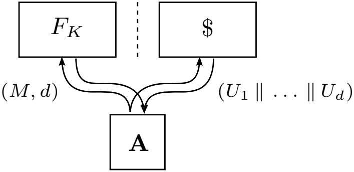




$$\mathbf{Adv}_F^{\mathrm{VOLPRF}}(\mathbf{A}) \stackrel{\mathsf{def}}{=} \underset{\mathbf{A}}{\Delta}(F_K; \$)$$

Variable-output-length PRFs



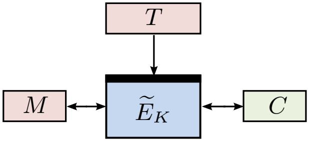


$$\mathbf{Adv}_F^{\mathrm{VOLPRF}}(\mathbf{A}) \stackrel{\mathsf{def}}{=} \underset{\mathbf{A}}{\Delta}(F_K; \$)$$

Examples:

- SHAKE [Dwo15]
- Farfalle [BDP+16]
- (all stream ciphers)

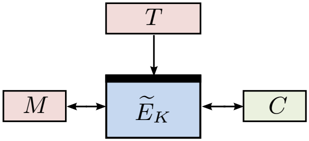
Tweakable Block Ciphers (TBCs) for MACs



TBCs [LRW02]:

- Keyed families of permutations
  $\widetilde{E} : \{0,1\}^k \times \{0,1\}^t \times \{0,1\}^n \to \{0,1\}^n$
- Additional public input tweak T

Tweakable Block Ciphers (TBCs) for MACs



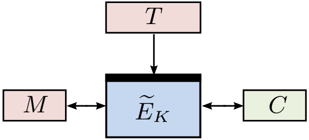
TBCs [LRW02]:

- Keyed families of permutations
  $\widetilde{E} : \{0,1\}^k \times \{0,1\}^t \times \{0,1\}^n \to \{0,1\}^n$
- Additional public input tweak T

Security Improvement over BCs:

- Tweak for domain separation

Tweakable Block Ciphers (TBCs) for MACs



TBCs [LRW02]:

- Keyed families of permutations
  $\widetilde{E} : \{0,1\}^k \times \{0,1\}^t \times \{0,1\}^n \to \{0,1\}^n$
- Additional public input tweak T

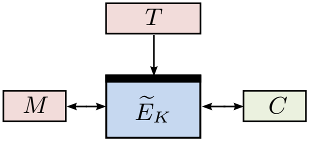
Security Improvement over BCs:

- Tweak for domain separation

Efficiency Improvement over BCs:

- Tweak for message processing

Tweakable Block Ciphers (TBCs) for MACs



TBCs [LRW02]:

- Keyed families of permutations
  $\widetilde{E} : \{0,1\}^k \times \{0,1\}^t \times \{0,1\}^n \to \{0,1\}^n$
- Additional public input tweak T

Security Improvement over BCs:

- Tweak for domain separation

Efficiency Improvement over BCs:

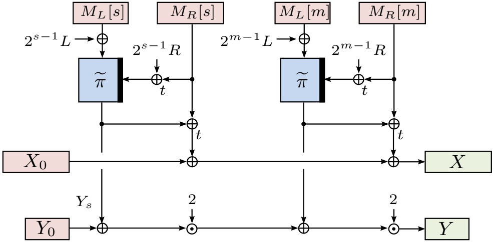
- Tweak for message processing

Recent existing TBC-based MACs w/ high security:

- PMAC_TBC1K/PMAC_TBC3K [Nai15]
- HaT [CLS17]
- ZMAC [IMPS17]

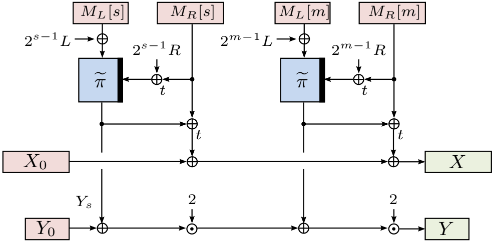
Good Candidate: ZMAC

[IMPS17]



Good Candidate: ZMAC

[IMPS17]

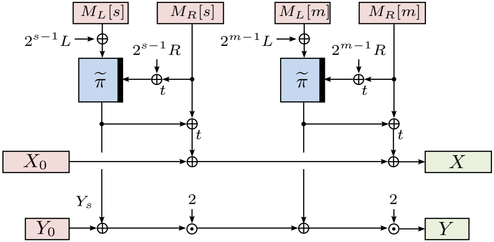


Efficiency:

- Fully parallelizable
- High rate: $(n + t)/n$
- TBC-based single-key, single-primitive

Good Candidate: ZMAC

[IMPS17]

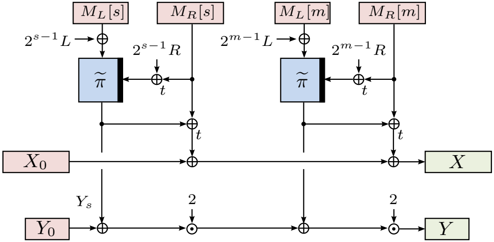


Efficiency:

- Fully parallelizable
- High rate: $(n+t)/n$
- TBC-based single-key, single-primitive

BBB-Security: ε-almost-universal (AU) for $\varepsilon \leq \frac{4}{2^{n+\min(n,t)}}$

Good Candidate: ZMAC
[IMPS17]



Efficiency:

- Fully parallelizable
- High rate: $(n+t)/n$
- TBC-based single-key, single-primitive

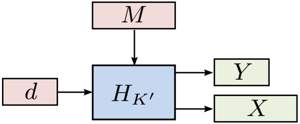
BBB-Security: ε-almost-universal (AU) for $\varepsilon \leq \frac{4}{2^{n+\min(n,t)}}$

Functionality: Can we obtain a variable-output-length PRF?

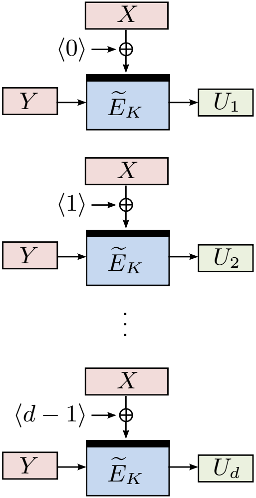
Section 2

Hash-then-TBC and ZMAC^{+}

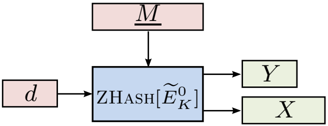
Hash-then-TBC (HtTBC)



- TBC-based VOLPRF
- Fully parallelizable
- Input $(Y, X) \in \{0,1\}^n \times \{0,1\}^t$
  Output of universal hash function H
- Inputs: (M, d)
- $d = $ #Output blocks $(U_1, \ldots, U_d)$

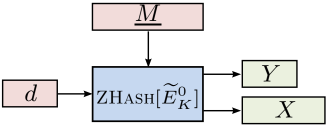


ZMAC$^+$ = ZHASH + HTTBC



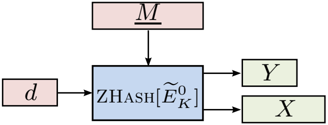
- Injective encoding and padding of message and output length: $M \leftarrow \underline{M} \parallel 1 \parallel 0^* \parallel \langle d \rangle_n$

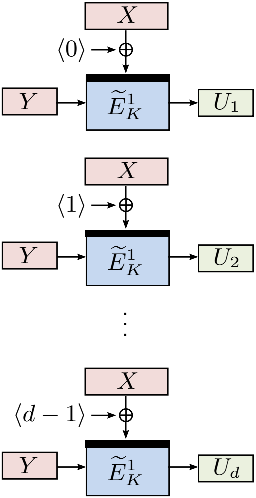
ZMAC$^+$ = ZHASH + HTTBC



- Injective encoding and padding of message and output length: $M \leftarrow \underline{M} \,\|\, 1 \,\|\, 0^* \,\|\, \langle d \rangle_n$
- Single keyed primitive $\widetilde{E}_K$:
  - $\widetilde{E}_K^0$ in ZHASH
  - $\widetilde{E}_K^1$ in HTTBC
  - $\widetilde{E}_K^2$ to derive L and R

ZMAC$^+$ = ZHash + HtTBC





- Injective encoding and padding of message and output length:
  $M \leftarrow \underline{M} \,\|\, 1 \,\|\, 0^* \,\|\, \langle d \rangle_n$
- Single keyed primitive $\widetilde{E}_K$:
  - $\widetilde{E}_K^0$ in ZHash
  - $\widetilde{E}_K^1$ in HtTBC
  - $\widetilde{E}_K^2$ to derive L and R
- Bound of $O(q/2^n + q(q+\sigma)/2^{n+\min(n,t)})$
  Eliminates term $O(\sigma^2/2^{n+\min(n,t)})$

---

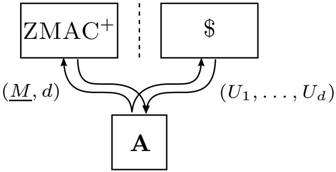
q = #queries; σ = sum of #blocks of all messages

Section 3

Security Analysis

VOLPRF Security of HtTBC

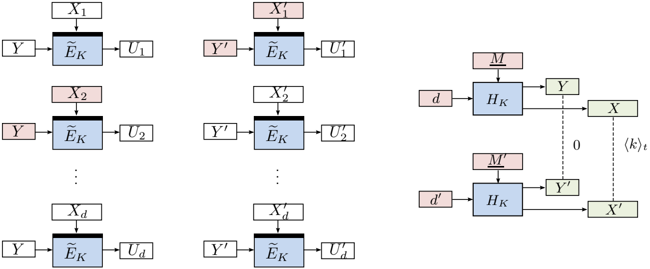
Proof Strategy



- H-coefficient technique [CS14, Pat08]
- Ideal world: U_i uniformly independently at random
- Replace $\widetilde{E}_K^{0/1/2}$ by independent uniform random permutations $\widetilde{\pi}^{0/1/2}$
- 2 bad events $\implies$ 2 requirements for H

VOLPRF Security of Hash-then-TBC

bad_1

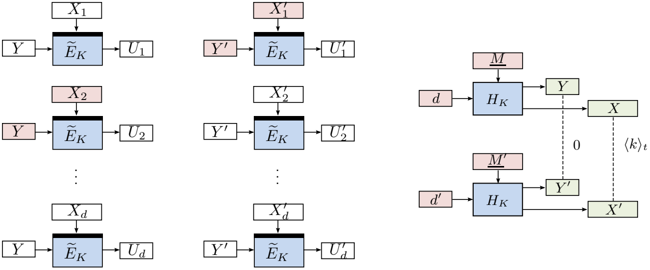


- bad_1: Collision of tweaks and inputs to $\widetilde{E}_K$ of HtTBC:

$$\exists k, k' : (Y, X \oplus \langle k-1 \rangle_t) = (Y', X' \oplus \langle k'-1 \rangle_t).$$

VOLPRF Security of Hash-then-TBC

bad_1



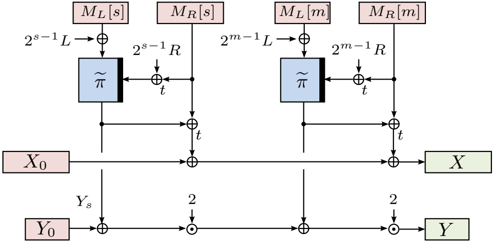
- bad_1: Collision of tweaks and inputs to $\widetilde{E}_K$ of HtTBC:

$$\exists k, k' : (Y, X \oplus \langle k-1 \rangle_t) = (Y', X' \oplus \langle k'-1 \rangle_t).$$

- $\Pr[\mathsf{bad}_1]$ upper bounded by max. differential prob. of certain differences:

$$\Pr\left[\mathsf{bad}_1\right] \leq \sum_{k=0}^{d+d'-1} \Pr_{K \twoheadleftarrow \mathcal{K}} \left[H_K\left(M\right) \oplus H_K\left(M'\right) = (0, \langle k \rangle_t) \right].$$

DP Analysis of ZHash



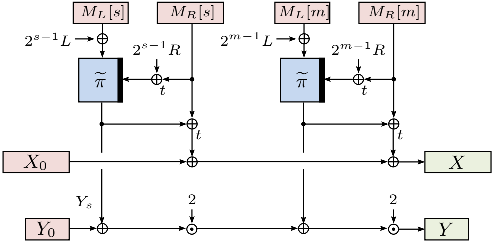
Theorem 1

For distinct $(\underline{M}, d)$ and $(\underline{M}', d')$ with at most m and m' $(n+t)$-bit blocks, $1 \leq m \leq m' < 2^{\min\{n,(n+t)/2\}-3}$, it holds that

$$\sum_{k=0}^{d+d'-2} \mathsf{DP}_H\left[M, M', (0^n, \langle k \rangle_t)\right] \leq \begin{cases} \frac{2(d+d')}{2^n} & \text{if } C1, \\ \frac{2(m+m'+1)}{2^{n+t}} + \frac{4(d+d')}{2^{n+\min\{n,t\}}} & \text{oth.} \end{cases}$$

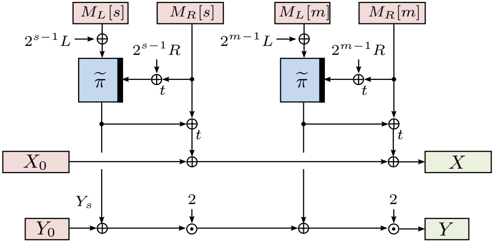
where $C1 \stackrel{\text{def}}{=} M$, M' have equal length and differ in exactly 1 block

Rationale



- $\mathsf{DP}_H\left[M, M', (0^n, \langle k \rangle_t)\right]$ is lengthy

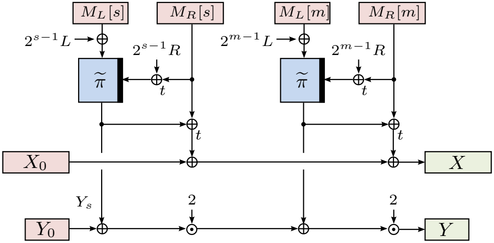
Rationale



- $\mathsf{DP}_H\,[M, M', (0^n, \langle k \rangle_t)]$ is lengthy

- Why not consider ε-AXU of ZHASH?
  $\Longrightarrow$ "not guaranteed to be small" in C1 [IMPS17]
  (when M, M' have equal length and differ in 1 block)

Rationale

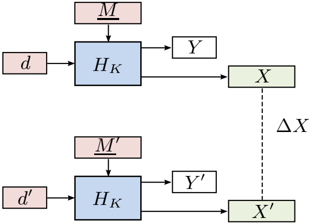


- $\mathsf{DP}_H\,[M, M', (0^n, \langle k \rangle_t)]$ is lengthy

- Why not consider ε-AXU of ZHASH?
  $\Longrightarrow$ "not guaranteed to be small" in C1 [IMPS17]
  (when M, M' have equal length and differ in 1 block)

- Why not abstract away $\widetilde{E}_K^{T_i}(S_i)$ as a XT$[\widetilde{\pi}, H_L]$ permutation?
  $\Longrightarrow$ Would give $\sigma^2/2^{n+\min(n,t)}$ term

Truncated-AXU

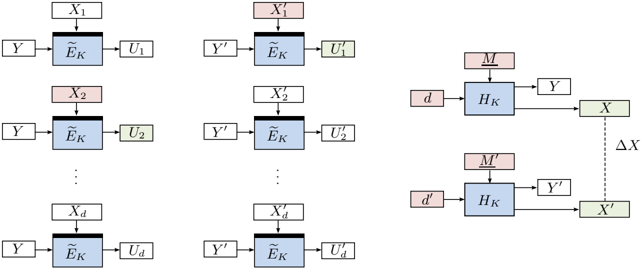


H is (n, t, ε)-truncated AXU (tAXU) iff:

$$\max_{\Delta X} \sum_{\Delta Y} \Pr_{K \twoheadleftarrow \mathcal{K}} \left[H_K(M) \oplus H_K\left(M'\right) = (\Delta Y, \Delta X) \right] \leq \varepsilon.$$

VOLPRF Security of Hash-then-TBC (Cont'd)

bad$_2$

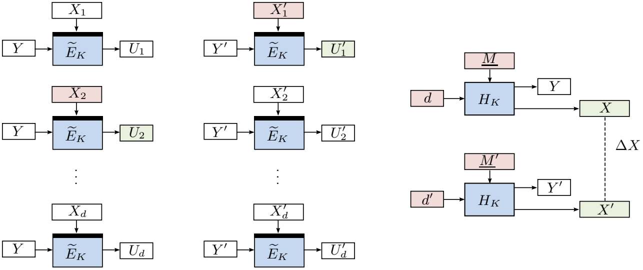


- bad$_2$: Collision of tweaks and outputs from $\widetilde{E}_K$ of $\mathrm{H{\scriptsize T}TBC}$:

$$\mathsf{bad}_2 \stackrel{\text{def}}{=} \exists k, k' : (X \oplus \langle k-1 \rangle_t, U_k) = (X' \oplus \langle k'-1 \rangle_t, U'_{k'}).$$

VOLPRF Security of Hash-then-TBC (Cont'd)

bad_2



- bad_2: Collision of tweaks and outputs from $\widetilde{E}_K$ of $\textsc{HtTBC}$:

$$\mathsf{bad}_2 \stackrel{\text{def}}{=} \exists k, k' : (X \oplus \langle k-1 \rangle_t, U_k) = (X' \oplus \langle k'-1 \rangle_t, U'_{k'}).$$

- Assume that H is (n, t, ε)-tAXU:

$$\Pr[\mathsf{bad}_2] \leq d \cdot d' \cdot \varepsilon \cdot \Pr\left[U_k = U'_{k'}\right] \leq \frac{dd'\varepsilon}{2^n} \implies \frac{2{\sigma'}^2\varepsilon}{2^n}$$

$\sigma' = \sum_{i=1}^{q} d^i$

Full Bound over q Queries

Details in Paper

- (n, t, ε)-tAXU:

$$\varepsilon \leq \frac{2(m + m' + 1)}{2^{n+\min\{n,t\}}} + \frac{4}{2^{\min\{n,t\}}}.$$

Full Bound over q Queries

Details in Paper

- (n, t, ε)-tAXU:

$$\varepsilon \leq \frac{2(m + m' + 1)}{2^{n+\min\{n,t\}}} + \frac{4}{2^{\min\{n,t\}}}.$$

- DP:

$$\frac{2\sigma'}{2^n} + \frac{2(q-1)\sigma + q^2 + 4(q-1)\sigma'}{2^{n+\min\{n,t\}}}$$

Full Bound over q Queries

Details in Paper

- (n, t, ε)-tAXU:

$$\varepsilon \leq \frac{2(m + m' + 1)}{2^{n+\min\{n,t\}}} + \frac{4}{2^{\min\{n,t\}}}.$$

- DP:

$$\frac{2\sigma'}{2^n} + \frac{2(q-1)\sigma + q^2 + 4(q-1)\sigma')}{2^{n+\min\{n,t\}}}$$

- VOLPRF bound for $\mathbf{A}$ with q queries of at most $m \leq 2^{\min\{n,t\}-3}$ $(n+t)$-bit blocks each and at most σ blocks in total, and whose output lengths d^i sum up to at most σ':

$$\mathbf{Adv}^{\mathrm{VOLPRF}}_{\mathrm{ZMAC}^{+}[\widetilde{\pi}]}(\mathbf{A}) \leq \frac{(\sigma')^2}{2^n} \cdot \left(\frac{4m+2}{2^{n+\min\{n,t\}}} + \frac{4}{2^{\min\{n,t\}}} \right) + \frac{2\sigma'}{2^n} + \frac{2(q-1)\sigma + q^2 + 4(q-1)\sigma'}{2^{n+\min\{n,t\}}}$$

Full Bound over q Queries

Details in Paper

- (n, t, ε)-tAXU:

$$\varepsilon \leq \frac{2(m + m' + 1)}{2^{n+\min\{n,t\}}} + \frac{4}{2^{\min\{n,t\}}}.$$

- DP:

$$\frac{2\sigma'}{2^n} + \frac{2(q-1)\sigma + q^2 + 4(q-1)\sigma')}{2^{n+\min\{n,t\}}}$$

- VOLPRF bound for $\mathbf{A}$ with q queries of at most $m \leq 2^{\min\{n,t\}-3}$ $(n+t)$-bit blocks each and at most σ blocks in total, and whose output lengths d^i sum up to at most σ':

$$\mathbf{Adv}^{\mathrm{VOLPRF}}_{\mathrm{ZMAC}^+[\widetilde{\pi}]}(\mathbf{A}) \leq \frac{(\sigma')^2}{2^n} \cdot \left(\frac{4m+2}{2^{n+\min\{n,t\}}} + \frac{4}{2^{\min\{n,t\}}} \right) + \frac{2\sigma'}{2^n} + \frac{2(q-1)\sigma + q^2 + 4(q-1)\sigma'}{2^{n+\min\{n,t\}}}$$

- No $\sigma^2 / 2^{2n}$ term

Section 4

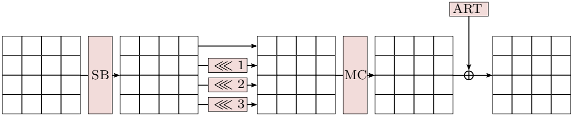
Potential Instantiations and Summary

Suitable Instantiations

- Desirable:
  - Efficient round function + efficient tweak schedule
  - $t \geq n$

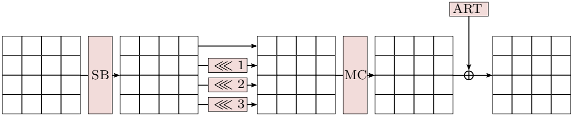
Suitable Instantiations

- Desirable:
  - Efficient round function + efficient tweak schedule
  - $t \geq n$
- Deoxys-BC-256/Deoxys-BC-384 [JNP14]: AES-NI

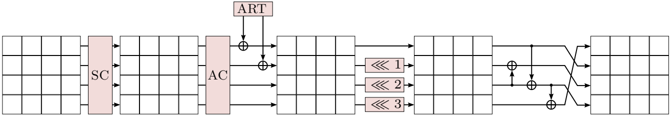


Suitable Instantiations

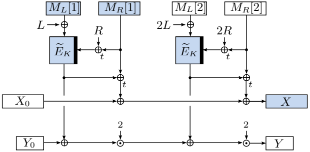
- Desirable:
  - Efficient round function + efficient tweak schedule
  - $t \geq n$
- Deoxys-BC-256/Deoxys-BC-384 [JNP14]: AES-NI

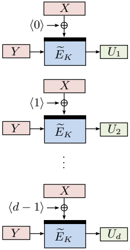


- Skinny-64/128 and Skinny-128/256 [BJK+16]: Lighter



Potential Instantiations





- n-bit outputs: Same performance as ZMAC
- Long outputs: $+1$ (parallelizable) Call to TBC
- Ongoing work: optimized implementation

	Output length	
TBC $\widetilde{E}_K$	n bit	$\|M\|$ bit
Deoxys-BC-256	0.62	1.49
Deoxys-BC-384	0.61	1.60
Skinny-128/256	2.08	6.20
Skinny-128/384	1.62	6.42

Estimated performance in cycles/byte on Intel Skylake with AES-NI.

Summary

- Proposed $\mathrm{ZMAC}^+ = \mathrm{ZH}\textsc{ash} + \mathrm{H}\textsc{t}\mathrm{TBC}$
- Variable-output-length PRF
- Eliminated $\sigma^2/2^{2n}$ in security bound with few domains in tweak
    - $\mathbb{ZHASH}$ needed block index in tweak i [IMPS17]
- Single primitive, single key

Questions?

References I

Guido Bertoni, Joan Daemen, Michaël Peeters, Gilles Van Assche, and Ronny Van Keer.
Farfalle: Parallel Permutation-based Cryptography.
IACR Cryptology ePrint Archive, 2016:1188, 2016.

Christof Beierle, Jérémy Jean, Stefan Kölbl, Gregor Leander, Amir Moradi, Thomas Peyrin, Yu Sasaki, Pascal Sasdrich, and Siang Meng Sim.
The SKINNY Family of Block Ciphers and Its Low-Latency Variant MANTIS.
In Matthew Robshaw and Jonathan Katz, editors, *CRYPTO II*, volume 9815 of *Lecture Notes in Computer Science*, pages 123–153. Springer, 2016.

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

Shan Chen and John P. Steinberger.
Tight Security Bounds for Key-Alternating Ciphers.
In Phong Q. Nguyen and Elisabeth Oswald, editors, *EUROCRYPT*, volume 8441 of *Lecture Notes in Computer Science*, pages 327–350. Springer, 2014.

Morris J Dworkin.
SHA-3 Standard: Permutation-based Hash and Extendable-output Functions.
Federal Inf. Process. Stds. (NIST FIPS)-202, 2015.

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

References II

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, December 2001.
http://www.etsi.org/deliver/etsi_ts/135200_135299/135201/04.01.00_60/ts_135201v040100p.pdf.

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

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.
Full version at https://eprint.iacr.org/2017/535.

Jérémy Jean, Ivica Nikolic, and Thomas Peyrin.
Tweaks and Keys for Block Ciphers: The TWEAKEY Framework.
In Palash Sarkar and Tetsu Iwata, editors, *ASIACRYPT (2)*, volume 8874 of *Lecture Notes in Computer Science*, pages 274–288, 2014.

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

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 *Lecture Notes in Computer Science*, pages 167–182. Springer, 2015.

Jacques Patarin.
The "Coefficients H" Technique.
In Roberto Maria Avanzi, Liam Keliher, and Francesco Sica, editors, *SAC*, volume 5381 of *Lecture Notes in Computer Science*, pages 328–345. Springer, 2008.

Section 5

Backup Slides

VOLPRF Security of Hash-then-TBC

[CS14, Pat08]

Lemma 2 (H-coefficient Technique)

Assume, the set of attainable transcripts is partitioned into two disjoint sets $\textsc{GoodT}$ and $\textsc{BadT}$. Further assume, there exist $\epsilon_1, \epsilon_2 \geq 0$ such that for any transcript $\tau \in \textsc{GoodT}$, it holds that

$$\frac{\Pr[\Theta_{\text{real}} = \tau]}{\Pr[\Theta_{\text{ideal}} = \tau]} \geq 1 - \epsilon_1, \quad \text{and} \quad \Pr[\Theta_{\text{ideal}} \in \textsc{BadT}] \leq \epsilon_2.$$

Then, for all adversaries $\mathbf{A}$, it holds that $\Delta_{\mathbf{A}}(\mathcal{O}_{\text{real}}; \mathcal{O}_{\text{ideal}}) \leq \epsilon_1 + \epsilon_2$.

- Bad Transcripts: $\epsilon_2 \leq \Pr[\text{bad}_1] + \Pr[\text{bad}_2]$
- Good Transcripts: $\epsilon_1 = 0$

VOLPRF Security of Hash-then-TBC (Cont'd)

Theorem 3

Let H be (n, t, ε)-tAXU and $L \twoheadleftarrow \mathcal{L}$ and H and $\widetilde{\pi} \twoheadleftarrow \widetilde{\mathsf{Perm}}(\mathcal{T}', \{0,1\}^n)$ independent. Then, for any VOLPRF adversary $\mathbf{A}$ on $\mathrm{H}\textsc{t}\mathrm{TBC}[\widetilde{\pi}, H_L]$ that makes at most q queries whose output lengths d^i sum up to at most σ' blocks in total, it holds that $\mathbf{Adv}^{\mathrm{VOLPRF}}_{\mathrm{H}\textsc{t}\mathrm{TBC}[\widetilde{\pi}, H_L]}(\mathbf{A})$ is at most

$$\frac{(\sigma')^2 \varepsilon}{2^n} + \max_{M^1, \ldots, M^q} \sum_{i<j}^{q} \sum_{k=0}^{d^i + d^j - 2} \mathsf{DP}_{H_L}\left[M^i, M^j, (0^n, \langle k \rangle_t)\right].$$

VOLPRF Security of Hash-then-TBC (Cont'd)

Theorem 3

Let H be (n, t, ε)-tAXU and $L \twoheadleftarrow \mathcal{L}$ and H and $\widetilde{\pi} \twoheadleftarrow \widetilde{\mathsf{Perm}}(\mathcal{T}', \{0,1\}^n)$ independent. Then, for any VOLPRF adversary $\mathbf{A}$ on $\mathrm{H{\scriptsize T}TBC}[\widetilde{\pi}, H_L]$ that makes at most q queries whose output lengths d^i sum up to at most σ' blocks in total, it holds that $\mathbf{Adv}^{\mathrm{VOLPRF}}_{\mathrm{H{\scriptsize T}TBC}[\widetilde{\pi}, H_L]}(\mathbf{A})$ is at most

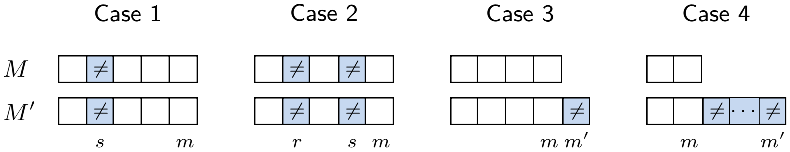
$$\frac{(\sigma')^2 \varepsilon}{2^n} + \max_{M^1, \ldots, M^q} \sum_{i<j}^{q} \sum_{k=0}^{d^i + d^j - 2} \mathsf{DP}_{H_L}\left[M^i, M^j, (0^n, \langle k \rangle_t)\right].$$

For single-block outputs:

- ϵ_2-AU suffices instead of DP: $\Pr[\mathsf{bad}_1] \leq \binom{q}{2} \varepsilon_2$

$$\mathbf{Adv}^{\mathrm{PRF}}_{\mathrm{H{\scriptsize T}TBC}[\widetilde{\pi}, H_L]}(\mathbf{A}) \leq \binom{q}{2} \cdot \left(\frac{2\varepsilon}{2^n} + \varepsilon_2\right).$$

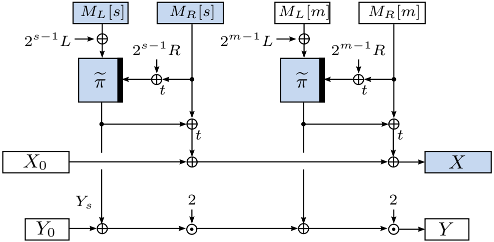
DP Analysis of ZHash (Cont'd)



- Two scenarios with same four cases each
  - $t \leq n$
  - $t > n$
- Focus on $t \leq n$ in the following
- Focus also on fixed $(0, \langle k \rangle_t)$ and consider different k later

DP Analysis of ZHash (Cont'd)

Case 1



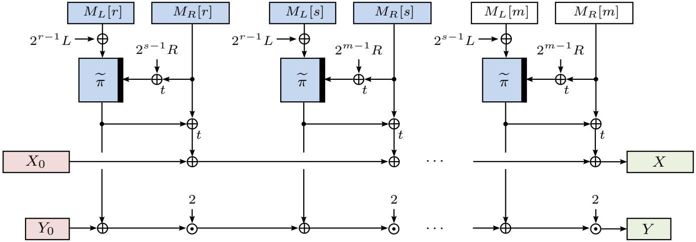
$$\Pr\begin{bmatrix}\Delta X_s = \langle k \rangle_t \\ \Delta Y_s = 0\end{bmatrix} = \Pr\begin{bmatrix}\mathrm{MSB}_t(\Delta Y_s \oplus \Delta M_R[s]) = \langle k \rangle_t \\ \Delta Y_s = 0\end{bmatrix}$$

- $\Delta Y_s = 0 \implies \Delta M_R[s] = \langle k \rangle_t$
- If $k = 0 \implies \Delta Y_s = 0$ impossible
- If $k \neq 0 \implies Y_s$ and Y'_s independent:

$$\Pr\left[(\Delta Y, \Delta X) = (0, \langle k \rangle_t)\right] \leq \frac{1}{2^n}$$

DP Analysis of ZHash (Cont'd)

Case 2



- There exist (at least) two blocks r, s: $M_r \neq M'_r$ and $M_s \neq M'_s$

$$\Delta X = \Delta X_r \oplus \Delta X_s \oplus \Delta_1, \qquad \Delta_1 \stackrel{\text{def}}{=} \langle k \rangle_t \oplus \bigoplus_{1 \leq i \leq m, i \notin \{r,s\}} \Delta X_i,$$
$$\Delta Y = \lambda_r \cdot \Delta Y_r \oplus \lambda_s \cdot \Delta Y_s \oplus \Delta_2, \qquad \Delta_2 \stackrel{\text{def}}{=} 0 \oplus \bigoplus_{1 \leq i \leq m, i \notin \{r,s\}} \lambda_i \cdot \Delta Y_i.$$

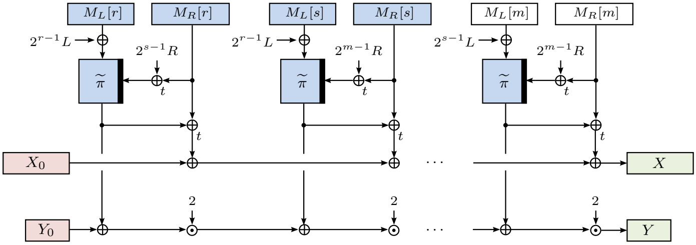
- Substitute $\Delta_3 = \Delta_1 \oplus \Delta M_R[r] \oplus \Delta M_R[s]$:

$$\Pr\begin{bmatrix}\Delta X = \langle k \rangle_t \\ \Delta Y = 0\end{bmatrix} = \Pr\begin{bmatrix}\mathrm{MSB}_t(\Delta Y_r \oplus \Delta Y_s) = \Delta_3 \\ \lambda_r \cdot \Delta Y_r \oplus \lambda_s \cdot \Delta Y_s = \Delta_2\end{bmatrix}$$

$\lambda_r = 2^{m+1-r}$, $\lambda_r = 2^{m+1-r}$

DP Analysis of ZHash (Cont'd)

Case 2



- Over all n-bit Δ_4 that yield t-bit differences Δ_3:

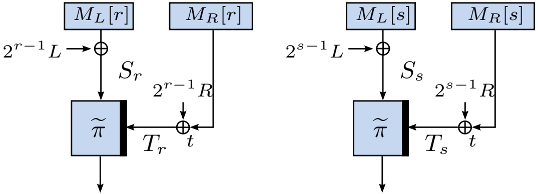
$$\Pr\left[\begin{matrix}\Delta X = \langle k \rangle, \\ \Delta Y = 0\end{matrix}\right] \leq \max_{\substack{\Delta_3 \in \{0,1\}^t \\ \Delta_2 \in \{0,1\}^n}} \sum_{\substack{\Delta_4 \in \{0,1\}^n \\ \mathrm{MSB}_t(\Delta_4) = \Delta_3}} \Pr\left[\begin{matrix}\Delta Y_r \oplus \Delta Y_s = \Delta_4, \\ \lambda_r \cdot \Delta Y_r \oplus \lambda_s \cdot \Delta Y_s = \Delta_2\end{matrix}\right]$$

- Cannot assume ΔY_r and ΔY_s are independent

$\lambda_r = 2^{m+1-r}$, $\lambda_r = 2^{m+1-r}$

DP Analysis of ZHash (Cont'd)

Case 2



- Event STColl(r): $\exists i \in \{1, \ldots, m\}, i \neq r : (S_i, T_i) = (S_r, T_r)$ or $(S'_i, T'_i) = (S_r, T_r)$

$$\Pr[\mathsf{STColl}(r)] \leq \frac{(m+1) + (m'+1) - 1}{2^{n+t}} \leq \frac{(m+m'+1)}{2^{n+t}}$$

- Similar for (S_s, T_s)
- $\mathsf{STColl}(r, s) = \mathsf{STColl}(r) \vee \mathsf{STColl}(s)$:

$$\Pr[\mathsf{STColl}(r, s)] \leq \frac{2(m+m'+1)}{2^{n+\min\{n,t\}}}$$

DP Analysis of ZHash (Cont'd)

Case 2

- If (S_r, T_r) fresh $\implies$ ΔY_r sampled from $2^n - (m + m' + 1)$ values
- If (S_s, T_s) fresh $\implies$ ΔY_s sampled from $2^n - (m + m' + 1)$ values

$$\Pr[E] \overset{\textsf{def}}{=} \max_{\substack{\Delta_3 \in \{0,1\}^t \\ \Delta_2 \in \{0,1\}^n}} \sum_{\substack{\Delta_4 \in \{0,1\}^n \\ \mathrm{MSB}_t(\Delta_4) = \Delta_3}} \Pr\left[\begin{matrix} \Delta Y_r \oplus \Delta Y_s = \Delta_4, \\ \lambda_r \cdot \Delta Y_r \oplus \lambda_s \cdot \Delta Y_s = \Delta_2 \end{matrix}\right]$$

$$\Pr[E | \neg \mathsf{STColl}(r, s)] \leq 2^{n-t} \cdot \frac{1}{(2^n - (m + m' + 1))^2} \leq \frac{4}{2^{n+t}}$$

since we assume $m, m' < 2^{n-2}$

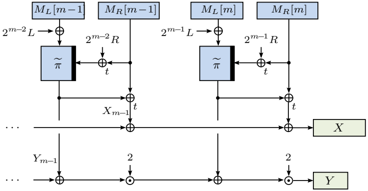
- It follows

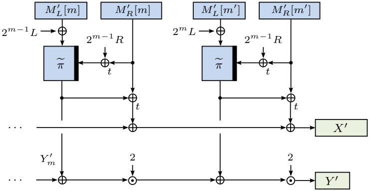
$$\Pr\left[\begin{matrix} \Delta X = \langle k \rangle_t \\ \Delta Y = 0 \end{matrix}\right] \leq \Pr\left[E | \neg \mathsf{STColl}(r, s)\right] + \Pr\left[\mathsf{STColl}(r, s)\right]$$

$$\leq \frac{4}{2^{n+t}} + \frac{2(m + m' + 1)}{2^{n+t}}$$

DP Analysis of ZHash (Cont'd)

Case 3





- M' is one block longer than M: $m' = m + 1$
- Padding and length encoding ensures $m > 0$
- The chaining indices are shifted

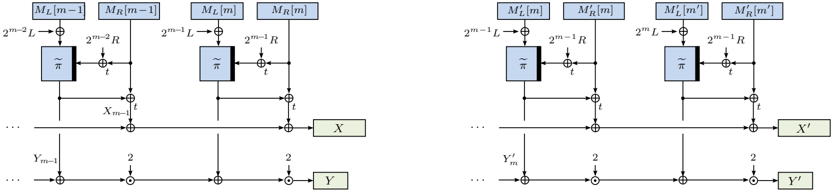
$$Y = \sum_{i=1}^{m} \mathbf{2^{m+1-i}} Y_i \qquad \text{whereas} \qquad Y' = \sum_{i=1}^{m+1} \mathbf{2^{m+2-i}} Y'_i$$

- Simply shift blocks by one? $\Longrightarrow$ factors of masks L, R **not** shifted:

$$S_i = M_L[i] \oplus 2^{i-1} L \qquad S'_i = M'_L[i] \oplus 2^{i-1} L$$

DP Analysis of ZHash (Cont'd)

Case 3



- Goal:

$$\Pr[E] \stackrel{\text{def}}{=} \max_{\substack{\Delta_1 \in \{0,1\}^t \\ \Delta_2 \in \{0,1\}^n}} \sum_{\substack{\Delta_3 \in \{0,1\}^n \\ \mathrm{MSB}_t(\Delta_3) = \Delta_1}} \Pr\begin{bmatrix} Y'_{m+1} \oplus Y'_m \oplus Y_m = \Delta_3 \\ 2\left(Y'_{m+1} \oplus 2Y'_m \oplus Y_m\right) = \Delta_2 \end{bmatrix}$$

- Substitute $A = Y'_{m+1} \oplus Y_m,\ B = Y'_m$:

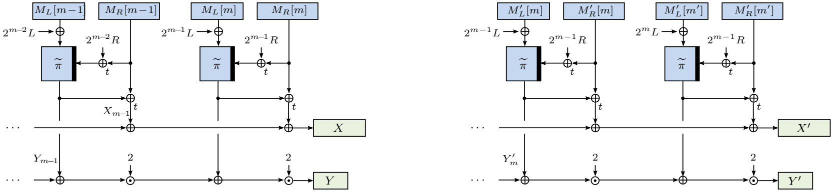
$$\Pr\begin{bmatrix} A \oplus B = \Delta_3 \\ A \oplus 2B = \Delta_4 \end{bmatrix}$$

- Unique solution (A, B) in $\mathbb{F}_{2^n}$:

$$B = 3^{-1}(\Delta_3 \oplus \Delta_4) \qquad A = \Delta_3 \oplus B$$

DP Analysis of ZHash (Cont'd)

Case 3



- Similar approach as in Case 2:
  Boolean variable $\mathsf{STColl}'(m+1)$ for M'_{m+1} is fresh:

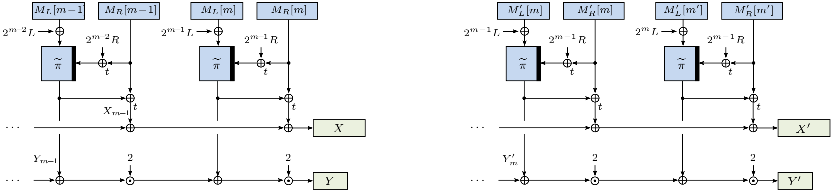
$$\Pr\left[\begin{matrix} A \oplus B = \Delta_3 \\ A \oplus 2B = \Delta_4 \end{matrix}\right] \leq \Pr\left[\begin{matrix} A \oplus B = \Delta_3 \\ A \oplus 2B = \Delta_4 \end{matrix} \middle| \neg\mathsf{STColl}'(m+1)\right] + \Pr\left[\mathsf{STColl}'(m+1)\right]$$

- It holds

$$\Pr\left[\mathsf{STColl}'(m+1)\right] \leq \frac{m + m' + 1}{2^{n+t}}.$$

DP Analysis of ZHash (Cont'd)

Case 3



- Otherwise, Y'_{m+1} is randomly chosen from $2^n - (m + m' + 1)$ values
- Choice of Y'_{m+1} (only in A) independent from Y'_m (only in B):

$$\Pr\left[\begin{matrix} B = 3^{-1}(\Delta_3 \oplus \Delta_4) \\ A = B \oplus \Delta_3 \end{matrix}\right] \le \frac{1}{2^n} \cdot \frac{1}{2^n - (m + m' + 1)} \le \frac{2}{2^{2n}}$$

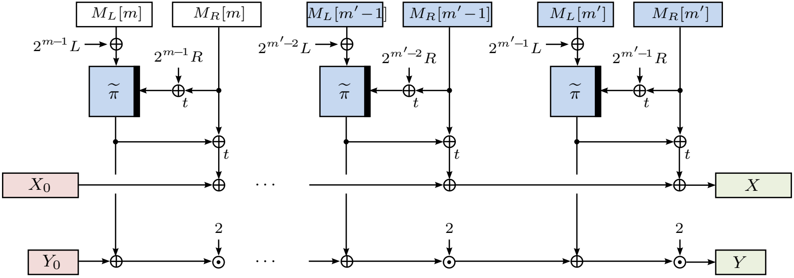
- Summing over 2^{n-t} t-bit values:

$$\Pr\left[\begin{matrix} \Delta X = \langle k \rangle_t \\ \Delta Y = 0 \end{matrix}\right] \le \Pr\left[E \middle| \neg \mathsf{STColl}'(m+1)\right] + \Pr\left[\mathsf{STColl}'(m+1)\right]$$

$$\le \frac{2}{2^{n+t}} + \frac{m + m' + 1}{2^{n+t}}$$

DP Analysis of ZHash (Cont'd)

Case 4



- M' exceeds M by ≥ 2 blocks
- Similar strategy as in Case 2, with block indices $m+1$, $m+2$:

$$\Pr\left[\begin{array}{c}\Delta X = \langle k \rangle_t \\ \Delta Y = 0\end{array}\right] \leq \Pr\left[\, E \middle| \neg\mathsf{STColl}'(m'-1, m')\right] + \Pr\left[\mathsf{STColl}'(m'-1, m')\right]$$

$$\leq \frac{4}{2^{n+t}} + \frac{2(m+m'+1)}{2^{n+t}}$$

- Note: same bound for all cases but C1
- We can handle C1 with care when bounding over q queries

DP Analysis of ZHash (Cont'd)

From 2 to q queries: Case 1

- Same strategy for scenario $t > n$
- Case 1: For each $M_R[s]$ and fixed k, there is at most one $M'_R[s]$ with $\Delta M_R[s] = \langle k \rangle_t$

$$\max_{\underline{M}^1,\ldots,\underline{M}^q} \sum_{i<j}^{q} \sum_{k=0}^{d^i+d^j-2} \mathsf{DP}_{\textsc{ZHash}[\widetilde{\pi}]} \left[\left(\underline{M}^i, d^i \right), \left(\underline{M}^j, d^j \right), (0^n, \langle k \rangle_t) \right]$$

$$\leq \max_{\underline{M}^1,\ldots,\underline{M}^q} \sum_{i=1}^{q} \sum_{k=0}^{2(d^i-1)} \frac{1}{2^n} \leq \max_{\underline{M}^1,\ldots,\underline{M}^q} \sum_{i=1}^{q} \frac{2d^i}{2^n} \leq \underline{\underline{\frac{2\sigma'}{2^n}}}$$

$\sigma' = \sum_{i=1}^{q} d^i$

DP Analysis of ZHash (Cont'd)

From 2 to q queries: Cases 2-4

$$
\begin{aligned}
&\sum_{i<j}^{q} \left(\frac{2(m^i + m^j + 1)}{2^{n+\min\{n,t\}}} + \frac{4(d^i + d^j)}{2^{n+\min\{n,t\}}} \right) \\
\leq\ & \frac{2(q-1)\sigma}{2^{n+\min\{n,t\}}} + \sum_{i<j}^{q} \left(\frac{2}{2^{n+\min\{n,t\}}} + \frac{4(d^i + d^j)}{2^{n+\min\{n,t\}}} \right) \\
\leq\ & \underline{\underline{\frac{2(q-1)\sigma + q^2 + 4(q-1)\sigma'}{2^{n+\min\{n,t\}}}}}
\end{aligned}
$$

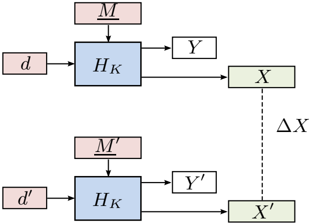
$\sum_{i<j}^{q}(m^i + m^j) = (q-1)\sigma$ and $\sum_{i<j}^{q}(d^i + d^j) = (q-1)\sigma'$

Lemma 4

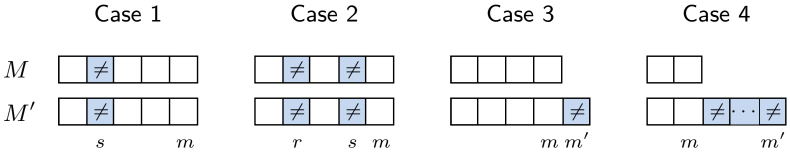
Let $\widetilde{\pi} \twoheadleftarrow \widetilde{\mathsf{Perm}}(\mathcal{T}', \{0,1\}^n)$. Given q pairwise distinct tuples $(\underline{M}^i, d^i) \in \mathcal{M} \times \mathcal{D}$, where each $\underline{M}^i$ consists of less than $2^{\min\{n,t\}-3}$ blocks of $(n+t)$ bit each, and of at most σ blocks in total, and whose output lengths $\sum_{i=1}^{q} d^i \leq \sigma'$. Then, it holds that

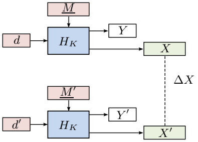
$$\max_{\underline{M}^1,\ldots,\underline{M}^q} \sum_{i<j}^{q} \sum_{k=0}^{d^i+d^j-2} \mathsf{DP}_{\text{ZHASH}[\widetilde{\pi}]}\left[\left(\underline{M}^i, d^i\right), \left(\underline{M}^j, d^j\right), (0^n, \langle k \rangle_t)\right]$$
$$\leq \frac{2\sigma'}{2^n} + \frac{2(q-1)\sigma + q^2 + 4(q-1)\sigma'}{2^{n+\min\{n,t\}}}.$$

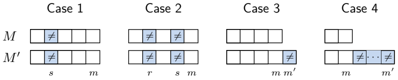
(n, t, ε)-tAXU Analysis of ZHash



- Goal: Fix any $\nabla X \in \{0,1\}^t$, probability $\Delta X \stackrel{\text{def}}{=} X \oplus X' \stackrel{?}{=} \nabla X$
- Same two scenarios ($t \leq n$ and $t > n$), same four cases each:







- Consider block $M_s \neq M'_s$:

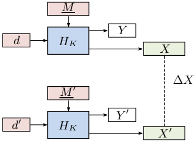
$$\Pr[E] \overset{\mathsf{def}}{=} \sum_{\nabla Y \in \{0,1\}^n} \max_{\nabla X \in \{0,1\}^t} \Pr \begin{bmatrix} \Delta X = \nabla X \\ \Delta Y = \nabla Y \end{bmatrix}$$

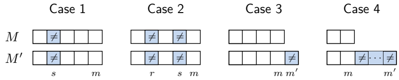
$$\begin{aligned} \Pr[E] &\leq \Pr\left[E \middle| \neg \mathsf{STColl}(s) \right] + \Pr\left[\mathsf{STColl}(s) \right] \\ &\leq \frac{1}{2^n - (m + m' + 1)} + \frac{(m + m' + 1)}{2^{n+t}} \\ &\leq \frac{2}{2^t} + \frac{m + m' + 1}{2^{n+t}} \end{aligned}$$

- Case 3 similar: uses $\mathsf{STColl}'(m + 1)$

(n, t, ε)-tAXU Analysis of ZHash (Cont'd)

Cases 2-4





- At least two blocks r, s exist: $M_r \neq M'_r$, $M_s \neq M'_s$
- We fix the smallest such r, s:

$$\Pr[E] \stackrel{\text{def}}{=} \sum_{\nabla Y \in \{0,1\}^n} \max_{\nabla X \in \{0,1\}^t} \Pr\begin{bmatrix} \Delta X = \nabla X \\ \Delta Y = \nabla Y \end{bmatrix}$$

$$\begin{aligned}\Pr[E] &\leq \Pr\left[E \mid \neg \mathsf{STColl}(r,s)\right] + \Pr\left[\mathsf{STColl}(r,s)\right] \\ &\leq 2^n \cdot \frac{4}{2^{n+t}} + \frac{2(m+m'+1)}{2^{n+t}} \\ &\leq \frac{4}{2^t} + \frac{2(m+m'+1)}{2^{n+t}}\end{aligned}$$

- Case 4 similar: uses $\mathsf{STColl}'(m'-1, m')$
- Scenario $t > n$ similar

(n, t, ε)-tAXU Analysis of ZHash (Cont'd)

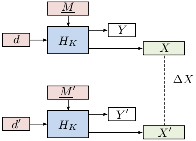
Theorem 5

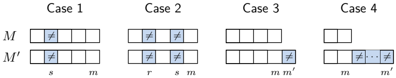
Let $\widetilde{\pi} \twoheadleftarrow \widetilde{\mathsf{Perm}}(\mathcal{T}', \{0,1\}^n)$. For distinct inputs $(\underline{M}, d)$ and $(\underline{M}', d')$ of at most m and m' $(n+t)$-bit blocks, respectively, with $1 \leq m \leq m' < 2^{\min\{n,t\}-3}$, $\mathrm{ZH{\small ASH}}[\widetilde{\pi}]$ is (n, t, ε)-tAXU for

$$\varepsilon \leq \frac{2(m + m' + 1)}{2^{n+\min\{n,t\}}} + \frac{4}{2^{\min\{n,t\}}}.$$

(n, t, ε)-tAXU Analysis of ZHash (Cont'd)

Case 1





- Consider block $M_s \neq M'_s$:

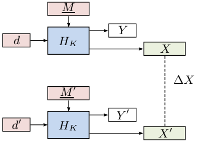
$$\Pr[E] \stackrel{\text{def}}{=} \sum_{\nabla Y \in \{0,1\}^n} \max_{\nabla X \in \{0,1\}^t} \Pr\begin{bmatrix} \Delta X = \nabla X \\ \Delta Y = \nabla Y \end{bmatrix}$$

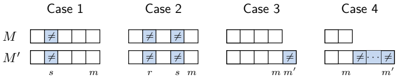
$$\begin{aligned} \Pr[E] &\leq \Pr\left[E \middle| \neg \mathsf{STColl}(s)\right] + \Pr\left[\mathsf{STColl}(s)\right] \\ &\leq \frac{1}{2^n - (m + m' + 1)} + \frac{(m + m' + 1)}{2^{n+t}} \\ &\leq \frac{2}{2^t} + \frac{m + m' + 1}{2^{n+t}} \end{aligned}$$

- Case 3 similar: uses $\mathsf{STColl}'(m + 1)$

(n, t, ε)-tAXU Analysis of ZHash (Cont'd)

Cases 2-4





- At least two blocks r, s exist: $M_r \neq M'_r$, $M_s \neq M'_s$
- We fix the smallest such r, s:

$$\Pr[E] \stackrel{\text{def}}{=} \sum_{\nabla Y \in \{0,1\}^n} \max_{\nabla X \in \{0,1\}^t} \Pr\begin{bmatrix} \Delta X = \nabla X \\ \Delta Y = \nabla Y \end{bmatrix}$$

$$\begin{aligned} \Pr[E] &\leq \Pr\left[E \middle| \neg \mathsf{STColl}(r, s)\right] + \Pr\left[\mathsf{STColl}(r, s)\right] \\ &\leq 2^n \cdot \frac{4}{2^{n+t}} + \frac{2(m + m' + 1)}{2^{n+t}} \\ &\leq \frac{4}{2^t} + \frac{2(m + m' + 1)}{2^{n+t}} \end{aligned}$$

- Case 4 similar: uses $\mathsf{STColl}'(m' - 1, m')$
- Scenario $t > n$ similar