Security Proofs of Oribatida

Arghya Bhattarcharjee[1] Eik List[2] Cuauthemoc Mancillas-Lopéz[3]
Mridul Nandi[1]

[1]ISI Kolkata, India

[2]Bauhaus-Universität Weimar, Germany

[3]CINVESTAV-IPN, Mexico

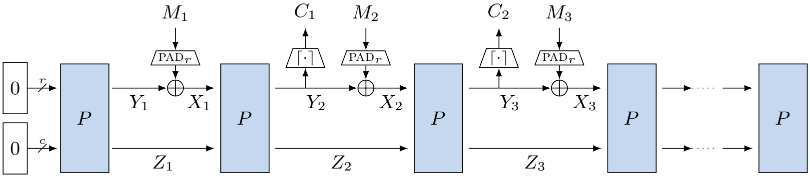
NIST Lightweight Workshop
Fall 2019

Section 1

Motivation

Permutation-based AE

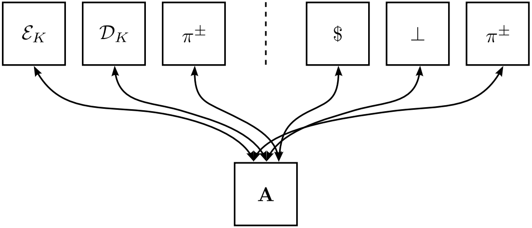
- Introduced by Bertoni et al. [BDPVA07]
- General constructions: Sponge [BDPVA07], Duplex [BDPA11]
- Many AE Schemes: Ascon [DEMS16], Keyak [BDP+16], Farfalle, NORX [AJN14], . . . ,



Security Model

nAE Security

- Ideal-permutation model
- $q_c/\sigma_c = \#$ Construction queries/blocks
- $q_e/\sigma_e = \#$ Construction encryption queries/blocks
- $q_d/\sigma_d = \#$ Construction decryption queries/blocks
- $q_p = \#$ Primitive queries



Bounds

Types:

- Inner-keyed, outer-keyed, full-keyed, suffix-keyed sponge
- SpongeWrap [BDPA11] and MonkeyDuplex [BDPVA12]

Large Corpus on Analysis:

- Keyed sponges [ADMA15, BDPA08, BDPA11, DMA17, GPT15, JLM14, MRV15, DM19, NY16]
- Bound by [DM19]:

$$\mathbf{Adv}_{\Pi}^{\mathsf{PRF}}(\mathbf{A}) = O\left(\frac{q_c^2 + q_c q_p}{2^c}\right) + \mathbf{Adv}_{\Pi}^{\mathsf{kp}}(\mathbf{A}')$$

- Improvements seem hard $\implies$ novel design approaches needed

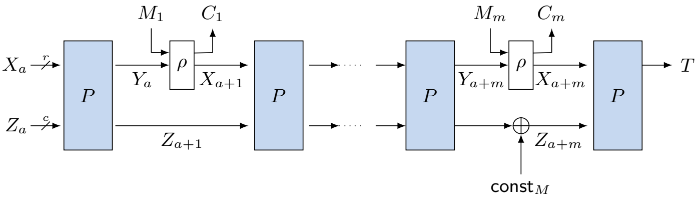
---

kp = key-prediction, $q_c = \#$construction queries (online), $q_p = \#$primitive queries (offline)

Beetle

[CDNY18a]

- Added transform ρ
- Permutation-input X_i and output block C_i differ



$$O\left(\frac{rq_p + r\sigma}{2^c} + \frac{q_v + q_p}{2^r} + \frac{\sigma^2 + q_p^2}{2^n}\right)$$

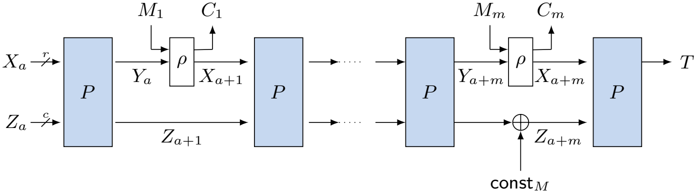
INT-RUP Security
[ABL+14]

- Correct authenticated decryption:
  Buffer entire plaintext until verification $\implies$ latency, storage
- Errors in resource-constrained environments $\implies$ Robustness desirable
- Andreeva et al. [ABL+14]:
  - PA1, PA2 notions for Privacy under release of unverified plaintext
  - INT-RUP for Integrity
  - PA2 unachievable for online schemes
  - INT-RUP achievable

INT-RUP Security

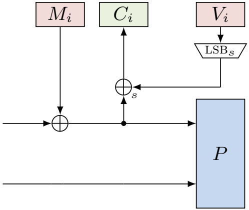
Beetle

- Bound of Beetle does not hold in INT-RUP
- Attack in $O(q_d q_p / 2^c)$
- Problem: #Offline primitive queries q_p



Idea: Ciphertext Masking

- Dynamic mask from earlier capacity (random permutation outputs)
- INT-RUP security: $O(q_d^2/2^c)$
- Only #Online construction queries q_d relevant

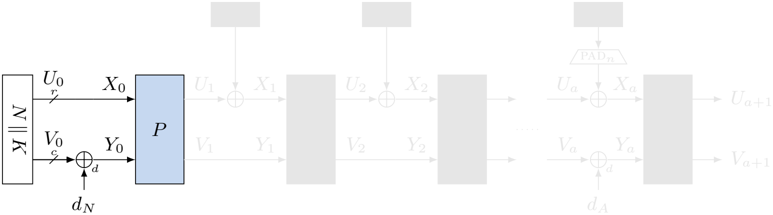


Section 2

Oribatida

- Nonce and key concatenated
- Domain separation

$$d_N = \begin{cases} 5 & \text{if } |A| + |M| > 0 \\ 9 & \text{otherwise.} \end{cases}$$

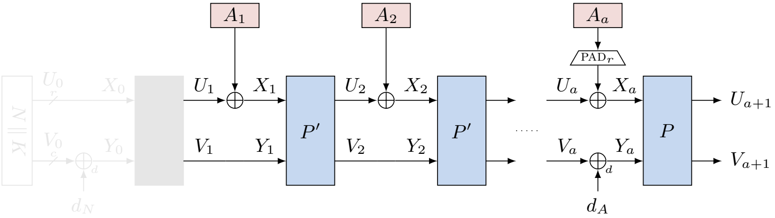


Oribatida

Associated-data Processing

- Absorbed in the rate
- Round-reduced permutation for intermediate blocks
- Always wrapped by full permutation calls
- Domain separation

$$d_A = \begin{cases} 4 & \text{if } |M| = 0 \wedge |A| \bmod r \equiv 0 \\ 6 & \text{if } |M| = 0 \wedge |A| \bmod r > 0 \\ 12 & \text{if } |M| > 0 \wedge |A| \bmod r \equiv 0 \\ 14 & \text{if } |M| > 0 \wedge |A| \bmod r > 0. \end{cases}$$

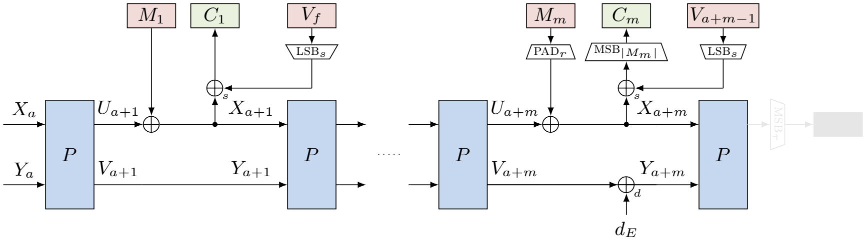


Oribatida

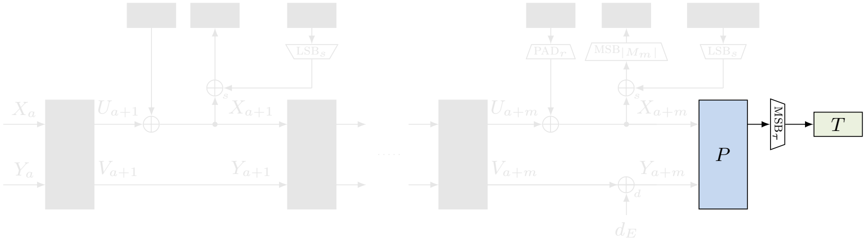
Encryption

- Absorbed in the rate
- Mask V_i: s lsb from previous capacity
- $V_f = V_0$ if no AD, and V_1 otherwise
- Domain separation

$$d_E = \begin{cases} 13 & \text{if } |M| \bmod r \equiv 0 \\ 15 & \text{if } |M| \bmod r \not\equiv 0 \end{cases}$$



- Outputs first τ bits
- Decryption analogously, only returns message if T valid



Oribatida

Variants

		Permutations					State size		
				Key	Nonce	Tag	Rate	Capacity	Mask
Rec.	Name	P	P'	(k)	(ν)	(τ)	(r)	(c)	(s)
1	Oribatida-256-64	SimP-256-4	SimP-256-2	128	128	128	128	128	64
2	Oribatida-192-96	SimP-192-4	SimP-192-2	128	64	96	96	96	96

Section 3

nAE Security

nAE Security

- H-coefficient technique [CS14, Pat08]
- Assumes: P, P' ideal (same) permutation

Bad events:

1. r-multi-collision on rate among encryption construction queries **or** in rate among primitive queries

$$\frac{\binom{\sigma}{r}}{2^{r(r-1)}} + \frac{\binom{q_p}{r}}{2^{r(r-1)}}$$

2. Collision of permutation in-/outputs in construction queries

$$2 \cdot \frac{\binom{\sigma}{2}}{2^n}$$

3. Collision of permutation in-/outputs between construction and primitive query

$$2 \cdot \left(\frac{\sigma_e \cdot q_p}{2^{c+s}} + \frac{r \cdot q_p}{2^{n-\tau}}\right)$$

4. Initial-state collision with primitive query

$$\frac{3q_p}{2^k} + \frac{q_c \cdot q_p}{2^{c+s}}$$

nAE Security (cont'd)

Interpolation probability of good transcripts:

$$\frac{\Pr[\Theta_{\mathsf{real}} = \tau]}{\Pr[\Theta_{\mathsf{ideal}} = \tau]} \leq 1 - \left(\frac{q_d}{2^{\tau}} + \frac{q_d(q_p + \sigma_e)}{2^{c+s}} + \frac{(\sigma_d + q_d) \cdot r}{2^{c+s}} \right)$$

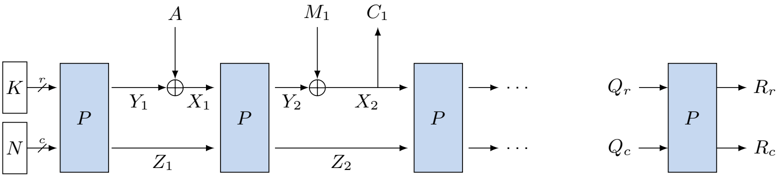
Bound:

$$\mathbf{Adv}^{\mathrm{NAE}}_{\Pi[\pi]_K}(\mathbf{A}) \leq \frac{\binom{\sigma}{r} + 2\binom{q_p}{r}}{2^{r(r-1)}} + \frac{\sigma^2}{2^n} + \frac{3q_p}{2^k} + \frac{r(q_d + \sigma_d) + 2\sigma_e q_p + q_p q_c + q_d(\sigma_e + q_p)}{2^{c+s}} + \frac{2rq_p}{2^{n-\tau}} + \frac{q_d}{2^{\tau}}$$

Section 4

INT-RUP Security

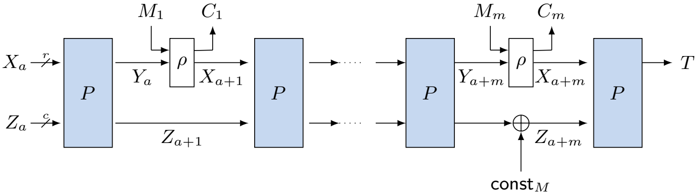
1. 1 encryption query $(N, A, M) \implies C$
2. q_d decryption queries $(N, A^i, C) \implies M^i$, with r bits fixed to constant
3. q_p primitive queries $Q^j \implies R^j$ with same r fixed bits
4. State collision when $q_d q_p \in O(2^n)$



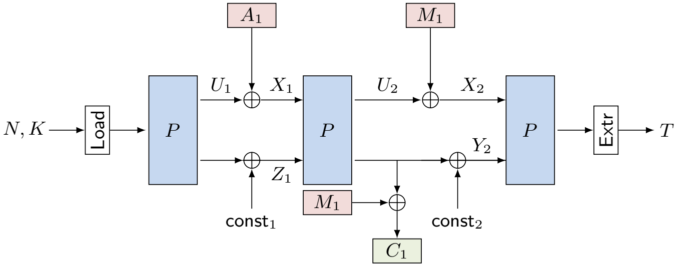
INT-RUP-Security

Attack on Beetle [CDNY18b]

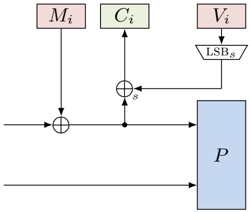
1. q_d encryption queries $(N, A^i, M) \implies C^i$, with r bits fixed to constant
2. q_d decryption queries $(N, A^i, {C'}^i) \implies {M'}^i$, with ${C'}^i = Y_2^i \oplus \text{shuffle}(Y_2^i)$ fixes first r bits
3. Again, q_p primitive queries with r bits fixed
4. State collision when $q_d q_p \in O(2^n)$



1. Encryption queries $(N, A, M_1) \implies (C_1, T)$
2. q_d decryption queries $(N, A, C_1^i) \implies M_1^i$
   capacity value Y_2 is fixed and known
3. Again, q_p primitive queries with Y_2 fixed
4. State collision when $q_d q_p \in O(2^n)$



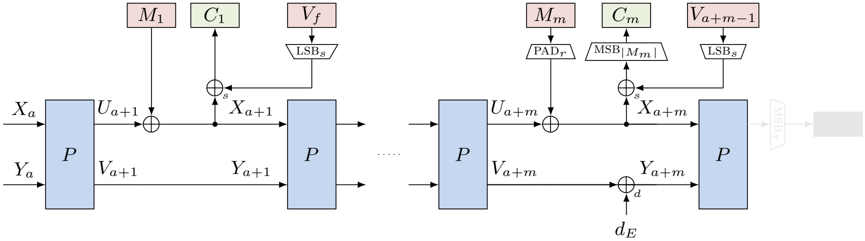
- $\mathbf{A}$ cannot fix the rate to a known constant
- Input to primitive oracle unknown



INT-RUP-Security

Best Attack

1. q_d encryption queries $(N^i, A^i, M) \implies C^i$
2. q_d decryption queries $(N, A^i, C'^i) \implies M'^i$
3. State collision in $V_2^i = V_2^j$ in $q_d^2 \in O(2^n)$



INT-RUP-Security

Bound

- H-coefficient technique [CS14, Pat08]
- Assumes: P, P' ideal (same) permutation

Bad events:

1. Non-trivial collision of permutation in/outputs in construction queries
2. Multi-collision between r tags
3. Non-trivial collision of permutation in/outputs between construction and primitive query
4. Initial-state collision with a primitive query
5. Multi-collision in the rate part of r primitive queries
6. Forgery in decryption queries if all blocks are old

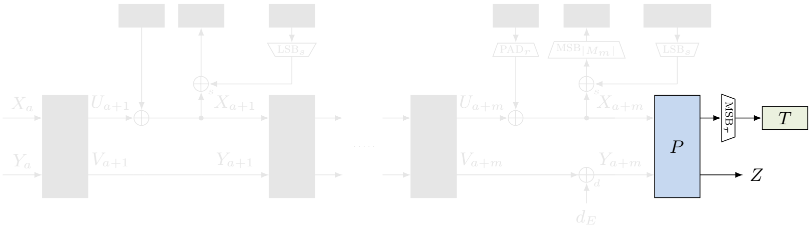
$$\mathbf{Adv}^{\text{INT-RUP}}_{\Pi[\pi]_K}(\mathbf{A}) \leq \frac{\sigma_e^2}{2^n} + \frac{4\sigma_e\sigma_d + 4\sigma q_p + q_c q_p + q_p + r(\sigma_d + q_d)}{2^{c+s}} + \frac{q_d^2 + \binom{q_d+q_v}{2}}{2^c} + \frac{\binom{q_e}{r}}{2^{\tau(r-1)}} + \frac{3rq_p}{2^{n-\tau}} + \frac{3q_p}{2^k} + \frac{2\binom{q_p}{r}}{2^{r(r-1)}} + \frac{2q_v}{2^\tau}.$$

Section 5

Tweaks

Observation by Rohit and Sarkar

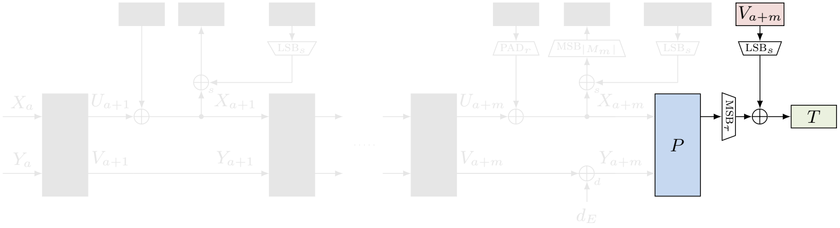
- Guess final permutation output $Z \implies$ recover state
- Only effective for our secondary proposal Oribatida-192
  Not for our primary proposal Oribatida-256
- nAE analysis used to have one incorrect denominator: $q_p/2^{c+s}$ $\implies q_p/2^{n-\tau}$
- Covered in final workshop submission



Possible Tweaks

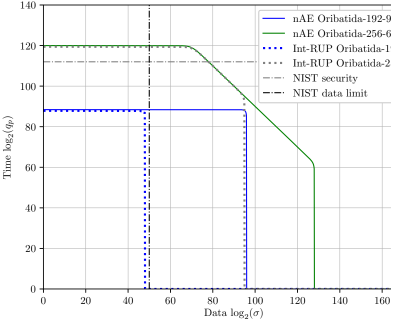
- Simple: Restrict tags to 64 bits for Oribatida-192
- Better: Mask the tag like ciphertext outputs before.
- Increases the relevant term from

$$\frac{3rq_p}{2^{n-\tau}} \quad \text{to} \quad \frac{3rq_p}{2^{n-\tau+s}}$$

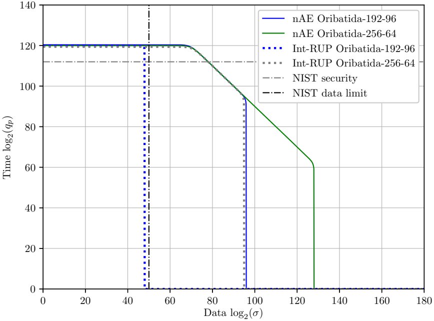


Possible Tweaks

Current Security



With Tag Masking



For $q_c = 2^{50}$

Section 6

Features

Implementation

Hardware Implementation on *Virtex 7 FPGA*

Table: LUTs = lookup tables; AD = associated data; Enc. = encryption; Dec. = decryption.

	LUTs	FF	#Slices	Frequency (MHz)	Cycles		Throughput (Mbps)	
					AD	Message	AD	Message
SimP								
SimP-256	495	340	148	580.51	69	137	1 076.88	542.37
SimP-192	383	259	122	581.98	53	105	1 054.15	532.10
Oribatida-256-64								
Enc. and Dec.	940	599	298	554.16	68	138	1 043.12	514.00
Enc. only	805	595	253	560.71	68	138	1 055.45	520.08

Oribatida– Features

- **Lightweight:** Permutation-based, no additional subkeys
- **Cross-platform:** SimP permutation only AND, rotation, XOR, no S-boxes
  State can be split according to platform needs
- **Well-known Components:** Duplex, Simon in SimP
- **High nAE-Security** as for Beetle:

$$\frac{r\sigma}{2^c} + \frac{\sigma^2 + q_p^2}{2^n} + \frac{q_p}{2^c}$$

- **Int-RUP-robust:** Limits damage if messages may leak

Questions?

Bibliography I

Elena Andreeva, Andrey Bogdanov, Atul Luykx, Bart Mennink, Nicky Mouha, and Kan Yasuda.
How to Securely Release Unverified Plaintext in Authenticated Encryption.
In Palash Sarkar and Tetsu Iwata, editors, *ASIACRYPT I*, volume 8873 of *LNCS*, pages 105–125. Springer, 2014.

Elena Andreeva, Joan Daemen, Bart Mennink, and Gilles Van Assche.
Security of Keyed Sponge Constructions Using a Modular Proof Approach.
In Gregor Leander, editor, *FSE*, volume 9054 of *LNCS*, pages 364–384. Springer, 2015.

Riham AlTawy, Guang Gong, Morgan He, Ashwin Jha, Kalikinkar Mandal, Mridul Nandi, and Raghvendra Rohit.
SpoC: An Authenticated Cipher.
Technical report, Feb 24 2019.
First-round submission to the NIST Lightweight Cryptography Competition.

Jean-Philippe Aumasson, Philipp Jovanovic, and Samuel Neves.
NORX: Parallel and Scalable AEAD.
In Miroslaw Kutylowski and Jaideep Vaidya, editors, *ESORICS II*, volume 8713 of *LNCS*, pages 19–36. Springer, 2014.

Farzaneh Abed, Eik List, Stefan Lucks, and Jakob Wenzel.
Differential Cryptanalysis of Round-Reduced Simon and Speck.
In Carlos Cid and Christian Rechberger, editors, *FSE*, volume 8540 of *LNCS*, pages 525–545. Springer, 2014.

Guido Bertoni, Joan Daemen, Michaël Peeters, Gilles van Assche, and Ronny van Keer.
Keyak v2.
2016.
Submission to the CAESAR competition.

Guido Bertoni, Joan Daemen, Michaël Peeters, and Gilles Van Assche.
On the Indifferentiability of the Sponge Construction.
In Nigel P. Smart, editor, *EUROCRYPT*, volume 4965 of *LNCS*, pages 181–197. Springer, 2008.

Bibliography II

Guido Bertoni, Joan Daemen, Michaël Peeters, and Gilles Van Assche.
Duplexing the Sponge: Single-Pass Authenticated Encryption and Other Applications.
In Ali Miri and Serge Vaudenay, editors, *SAC*, volume 7118 of *LNCS*, pages 320–337. Springer, 2011.

Guido Bertoni, Joan Daemen, Michaël Peeters, and Gilles Van Assche.
Sponge functions.
In *ECRYPT hash workshop*, volume 2007. Citeseer, 2007.

Guido Bertoni, Joan Daemen, Michaël Peeters, and Gilles Van Assche.
Permutation-based encryption, authentication and authenticated encryption.
Directions in Authenticated Ciphers, 2012.

Ray Beaulieu, Douglas Shors, Jason Smith, Stefan Treatman-Clark, Bryan Weeks, and Louis Wingers.
The SIMON and SPECK Families of Lightweight Block Ciphers.
IACR Cryptology ePrint Archive, 2013:404, 2013.

Jean-Sébastien Coron, Yevgeniy Dodis, Avradip Mandal, and Yannick Seurin.
A Domain Extender for the Ideal Cipher.
In Daniele Micciancio, editor, *TCC*, volume 5978 of *LNCS*, pages 273–289. Springer, 2010.
Full version at https://eprint.iacr.org/2009/356.

Avik Chakraborti, Nilanjan Datta, Mridul Nandi, and Kan Yasuda.
Beetle Family of Lightweight and Secure Authenticated Encryption Ciphers.
IACR Trans. Cryptogr. Hardw. Embed. Syst., 2018(2):218–241, 2018.
Updated version at https://eprint.iacr.org/2018/805.

Avik Chakraborti, Nilanjan Datta, Mridul Nandi, and Kan Yasuda.
Beetle Family of Lightweight and Secure Authenticated Encryption Ciphers.
Cryptology ePrint Archive, Report 2018/805, 2018.

Bibliography III

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 *LNCS*, pages 327–350. Springer, 2014.
Full version at https://eprint.iacr.org/2013/222.

Huaifeng Chen and Xiaoyun Wang.
Improved Linear Hull Attack on Round-Reduced Simon with Dynamic Key-Guessing Techniques.
In Thomas Peyrin, editor, *FSE*, volume 9783 of *LNCS*, pages 428–449. Springer, 2016.

Christoph Dobraunig, Maria Eichlseder, Florian Mendel, and Martin Schläffer.
Ascon v1.2 Submission to the CAESAR Competition.
September 15 2016.
Submission to the CAESAR competition.

Christoph Dobraunig and Bart Mennink.
Security of the Suffix Keyed Sponge.
Cryptology ePrint Archive, Report 2019/573, 2019.

Joan Daemen, Bart Mennink, and Gilles Van Assche.
Full-State Keyed Duplex with Built-In Multi-user Support.
In Tsuyoshi Takagi and Thomas Peyrin, editors, *ASIACRYPT II*, volume 10625 of *LNCS*, pages 606–637. Springer, 2017.

Peter Gaži, Krzysztof Pietrzak, and Stefano Tessaro.
The Exact PRF Security of Truncation: Tight Bounds for Keyed Sponges and Truncated CBC.
In Rosario Gennaro and Matthew Robshaw, editors, *CRYPTO I*, volume 9215 of *LNCS*, pages 368–387. Springer, 2015.

Philipp Jovanovic, Atul Luykx, and Bart Mennink.
Beyond $2^{c/2}$ Security in Sponge-Based Authenticated Encryption Modes.
In Palash Sarkar and Tetsu Iwata, editors, *ASIACRYPT I*, volume 8873 of *LNCS*, pages 85–104. Springer, 2014.

Bibliography IV

Zhengbin Liu, Yongqiang Li, and Mingsheng Wang.
Optimal Differential Trails in SIMON-like Ciphers.
IACR Trans. Symmetric Cryptol., 2017(1):358–379, 2017.

Bart Mennink, Reza Reyhanitabar, and Damian Vizár.
Security of full-state keyed sponge and duplex: Applications to authenticated encryption.
In Tetsu Iwata and Jung Hee Cheon, editors, *ASIACRYPT II*, volume 9453 of *LNCS*, pages 465–489. Springer, 2015.

Yusuke Naito and Kan Yasuda.
New Bounds for Keyed Sponges with Extendable Output: Independence Between Capacity and Message Length.
In Thomas Peyrin, editor, *FSE*, volume 9783 of *LNCS*, pages 3–22. Springer, 2016.

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

Håvard Raddum.
Algebraic Analysis of the Simon Block Cipher Family.
In Kristin E. Lauter and Francisco Rodríguez-Henríquez, editors, *LATINCRYPT*, volume 9230 of *LNCS*, pages 157–169. Springer, 2015.

Zejun Xiang, Wentao Zhang, Zhenzhen Bao, and Dongdai Lin.
Applying MILP Method to Searching Integral Distinguishers Based on Division Property for 6 Lightweight Block Ciphers.
In Jung Hee Cheon and Tsuyoshi Takagi, editors, *ASIACRYPT I*, volume 10031 of *LNCS*, pages 648–678, 2016.

Section 7

Supporting Slides

Int-RUP Security

- H-coefficient technique [CS14, Pat08]
- Assumes: P, P' ideal (same) permutation

Bad events:

1. r-multi-collision on rate among encryption construction queries **or** in rate among primitive queries

$$\frac{\binom{\sigma}{r}}{2^{r(r-1)}} + \frac{\binom{q_p}{r}}{2^{r(r-1)}}$$

2. Collision of permutation in-/outputs in construction queries

$$2 \cdot \frac{\binom{\sigma}{2}}{2^n}$$

3. Collision of permutation in-/outputs between construction and primitive query

$$2 \cdot \left(\frac{\sigma_e \cdot q_p}{2^{c+s}} + \frac{r \cdot q_p}{2^{n-\tau}} \right)$$

4. Initial-state collision with primitive query

$$\frac{3q_p}{2^k} + \frac{q_c \cdot q_p}{2^{c+s}}$$

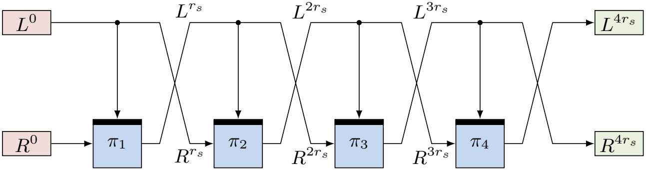
Section 8

Permutation

SimP

Ψ_r Domain extender [CDMS10]:

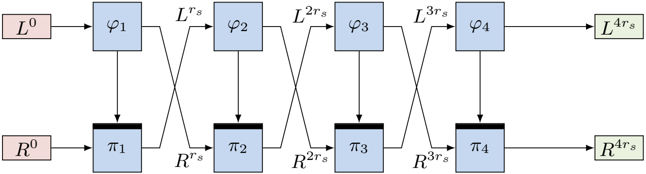
- Swap halves after each step
- Indifferentiable $O(q^2/2^n)$



SimP

Φ_r:

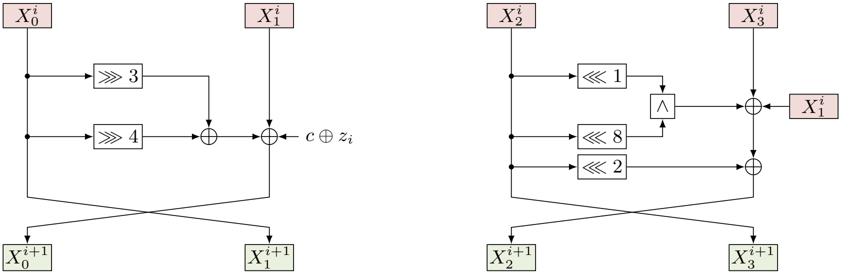
- Key-update permutation φ_i for other branch



SimP

Instantiation of Φ:

- Simon [BSS$^+$13]
- Lightweight: only 3 rotations, 3 XORs, 1 AND
- Intense analysis [ALLW14, CW16, LLW17, Rad15, XZBL16]
- Original round and rotation constants



- 4-word state: Simon round-function + Simon key-update function
- Half #rounds of full Simon-96-96/-128-128 per step
- Each bit passes full Simon

Variant	Word size (w)	#Steps (θ)	#Rounds/Step (r_s)
SimP-192-2	48	2	26
SimP-192-4	48	4	26
SimP-256-2	64	2	34
SimP-256-4	64	4	34

SimP

Analysis

- Round-reduced for intermediate blocks of AD
- Need only differentials
- Always wrapped by full steps