State of the Art in Lightweight Cryptography

Alex Biryukov   Léo Perrin
firstname.lastname@uni.lu

University of Luxembourg

FSE 14 Rump Session
(04 March 2014)

ECRYPT... $\rightarrow$ **A**CRYPT

http://cryptolux.org/index.php/Lightweight_Cryptography

Published a new lightweight primitive? Drop us a mail!
Published a new attack on a lightweight primitive? Drop us a mail!
Published new implementation results? Drop us a mail!

Work in progress, so any feedback is welcome!

https://www.cryptolux.org/index.php/Lightweight_Block_Ciphers

	al.		64				• 3-subsets MitM (full cipher)[19]	0.13 µm	688	25.1	0.292	ECRYPT[4]
LBlock	Wu et al.	ACNS 11[20]	64	80	Feistel	32	• Impossible differential (21 rounds)[21] • Related key impossible differential (22 rounds)[22] • Integral attack (22 rounds)[23]	0.18 µm	1320	200	--	Specification[20]
LED	Guo et al.	CHES 11[24]	64	64	SPN	32	• Ad Hoc (12 rounds of LED-64, 32 rounds of LED-128)[25]	0.18 µm	966	5.1	--	Specification[24]
				128		48			1265	3.4	--	Specification[24]
mCrypton	Lim et al.	ISA 06[26]	64	64	SPN	12	• MitM[27] 7-rounds mCrytpon-64/96/128 • MitM[27] 8- and 9-rounds mCrytpon-128	0.13µm	2420[note 2]	482.3	--	Specification[26]
				96					2681[note 2]	--	--	
				128					2949[note 2]	--	--	
Piccolo	Shibutani et al.	CHES 11[28]	64	80	GFS	25	• Biclique (full Piccolo-80; 28-round Piccolo-128)[29] • Related-key impossible diff[30], 14-rounds Piccolo-80, 21-rounds Piccolo-128	--	683 / 1136	14.8 / 237.04	-- / --	Specification[28]
				128		31		--	758 / 1196	12.12 / 193.9	-- / --	
PRESENT	Bogdanov et al.	CHES 07[31]	64	80	SPN	31	• Statistical saturation[32], up to 24-rounds	0.18 µm	1075 / 1570	11.7 / 200	1.4 / 2.78	Poschmann's PhD Thesis[33]
				128					1391 / 1884	11.45 / 200	-- / 3.67	
PRINCE	Borghoff et al.	ASIACRYPT 12[34]	64	128	SPN	10	• Reflection attack[35], 6 rounds • Sieve-in-the-Middle[36],	0.09 µm / 0.13 µm	3286 / 3491	529.9 / 533.3	4.5 / 5.8	Specification[34]

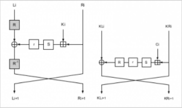
https://www.cryptolux.org/index.php/Lightweight_Block_Ciphers

It has been an inspiration for the AES competition finalist RC6. This algorithm is patented by RSA security.

SEA

[edit]

- Article: *SEA: A Scalable Encryption Algorithm for Small Embedded Applications*, Smart Card Research and Advanced Applications 06[40]
- Authors: Francois-Xavier Standaert, Gilles Piret, Neil Gershenfeld, and Jean-Jacques Quisquater
- Target: Software and Hardware



The RC5 round function.

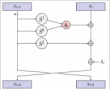
SEA is a block cipher which can have an arbitrary block size n (as long as n=6b for some b), word size w and number of rounds n_r. A complete description of the algorithm (round function and update of the key) is given on the figure on the right which comes from the original paper[40]. It is based on the following operations:

- Bitwise XOR
- Application of a S-box S. Interestingly, S is a 3x3 S-box.
- Rotation of the words in a vector of words
- Bit rotation inside a word
- Addition modulo 2^b

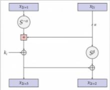
SIMON and SPECK

[edit]

- Article: *The SIMON and SPECK Families of Lightweight Block Ciphers*, eprint.iacr.org, 2013, 404
- Authors: Ray Beaulieu, Douglas Shors, Jason Smith, Stefan Treatman-Clark, Bryan Weeks, and Louis Wingers (NSA)
- Target: Hardware (SIMON) and software (SPECK)



Round function of SIMON



Round function of SPECK

These ciphers have been designed by the American National Security Agency (NSA). They are both Feistel networks with two branches but differ by the design of their Feistel function. They are both almost ARX construction, meaning that they rely on Addition, word Rotation and Xor, although SIMON uses And gates instead of additions. Both perform exceptionally well in both hardware and software, although SIMON is supposed to be more hardware-oriented and SPECK more software-oriented. Unlike all other ciphers' specification, no security analysis whatsoever is provided.

SIMON

[edit]

Hardware-oriented, this blockcipher relies only on the following operations: and, rotation, xor. It is a classical Feistel network where the Feistel function consists in applying basic operations on the branch, xoring the in subkey and then xoring the result with the other branch.

SPECK

[edit]

Software-oriented, this blockcipher relies only on the following operations: addition, rotation, xor (ARX construction). The Feistel structure is heavily tweaked in this one as both branches are modified during each round. Thus, it is hard to define a Feistel function in its case.

https://www.cryptolux.org/index.php/Lightweight_Authenticated_Encryption

- Article: The Hummingbird-2 lightweight authenticated encryption algorithm
- Authors: Engels, D., Saarinen, M. J. O., Schweitzer, P., & Smith, E. M.

Hummingbird-2 is, as its name indicates, a new iteration of the Hummingbird[13] primitive which was successfully attacked by Saarinen[14]. This cipher has an internal state which is initialized using the 64-bits IV. There is no key schedule: the same functions are applied to the internal state every time. At each clock, operations involving the key, the plain-text 16-bits block and the 128-bits internal state are performed to generate a block of ciphertext. Then, the same sort of operations are used to update the internal state using variables created during the cipher-text generation.

The only operations used are XOR, addition modulo 2^{16} and a non-linear function called f which is based on 4 different S-boxes.

Notes [edit]

1. ↑ It only supports encryption of messages of length 3x128 bits.
2. ↑ 2.0 2.1 To the best of our knowledge.
3. ↑ These figures correspond to the peaks of power consumption.

References [edit]

1. ↑ Whiting, D., Schneier, B., Lucks, S., & Muller, F. (2005). *Fast encryption and authentication in a single cryptographic primitive*. ECRYPT Stream Cipher Project Report, 27(200), 5. pdf at ssi.gouv.fr
2. ↑ 2.0 2.1 Bertoni, G., Daemen, J., Peeters, M., & Van Assche, G. (2012, January). *Duplexing the sponge: single-pass authenticated encryption and other applications*. In Selected Areas in Cryptography (pp. 320-337). Springer Berlin Heidelberg. pdf at eprint.iacr.org
3. ↑ Andreeva, E. and Bilgin, B. and Bogdanov, A. and Luykx, A. and Mennink, B. and Mouha, N. and Yasuda, K. 2013). *APE: Authenticated Permutation-Based Encryption for Lightweight Cryptography*. Cryptology ePrint Archive, Report 2013/791. pdf at eprint.iacr.org
4. ↑ 4.0 4.1 4.2 4.3 Bogdanov, A., Mendel, F., Regazzoni, F., Rijmen, V., & Tischhauser, E. (2013). *ALE: AES-based lightweight authenticated encryption*. Lecture Notes in Computer Science. pdf at dtu.dk
5. ↑ 5.0 5.1 Khovratovich, D., & Rechberger, C (2013). *The LOCAL attack: Cryptanalysis of the authenticated encryption scheme ALE*. pdf at eprint.iacr.org
6. ↑ 6.0 6.1 Wu, S., Wu, H., Huang, T., Wang, M., & Wu, W. (2013). *Leaked-State-Forgery Attack against the Authenticated Encryption Algorithm ALE*. In Advances in Cryptology-ASIACRYPT 2013 (pp. 377-404). Springer Berlin Heidelberg. pdf at springer.com
7. ↑ 7.0 7.1 Jakimoski, G., & Khajuria, S. (2012, January). *ASC-1: An authenticated encryption stream cipher*. In Selected Areas in Cryptography (pp. 356-372). Springer Berlin Heidelberg. pdf at springer.com
8. ↑ 8.0 8.1 8.2 Aumasson, J. P., Knellwolf, S., & Meier, W. (2012). *Heavy Quark for secure AEAD*. DIAC-Directions in Authenticated Ciphers, Sweden. pdf at 131002.net
9. ↑ 9.0 9.1 9.2 Bilgin, B., Bogdanov, A., Knežević, M., Mendel, F., & Wang, Q. (2013). *FIDES: lightweight authenticated cipher with side-channel resistance for constrained hardware*. In Cryptographic Hardware and Embedded Systems-CHES 2013 (pp. 142-158). Springer Berlin Heidelberg. pdf at kuleuven.be
10. ↑ 10.0 10.1 10.2 Engels, D., Saarinen, M. J. O., Schweitzer, P., & Smith, E. M. (2012). *The Hummingbird-2 lightweight authenticated encryption algorithm*. In RFID. Security and Privacy (pp. 19-31). Springer Berlin Heidelberg. pdf from rfid-cusp.org
11. ↑ Saarinen, M. J. O. (2013). *Related-key Attacks Against Full Hummingbird-2*. IACR Cryptology ePrint Archive, 2013, 70. pdf at eprint.iacr.org
12. ↑ 12.0 12.1 Biryukov, A. (2005). *A new 128-bit key stream cipher LEX*. eSTREAM, ECRYPT Stream Cipher Project, Report, 13, 2005. pdf at ecrypt.eu.org