Lightweight Crytography at the University of Luxembourg (+ some open positions)

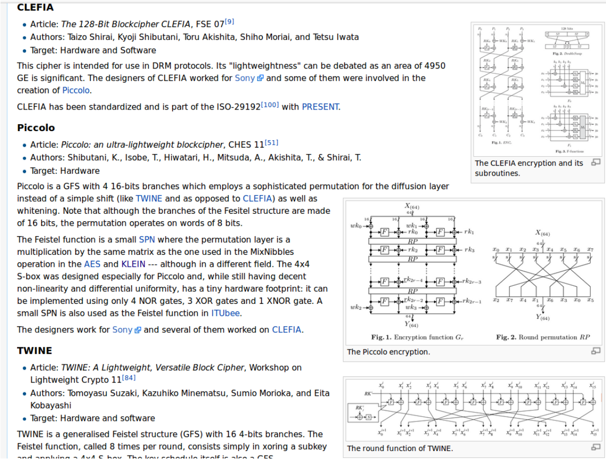
CryptoLUX Team[1]

[1] SnT, CSC, University of Luxembourg
https://cryptolux.org

March 7, 2017
Fast Software Encryption 2017

Thorough Review of LWC

- List of LW algorithms (BC but also SC, HF, AEAD schemes)
- Best attacks
- Full references
- **Will be updated soon!**



CLEFIA

- Article: *The 128-Bit Blockcipher CLEFIA*, FSE 07[9]
- Authors: Taizo Shirai, Kyoji Shibutani, Toru Akishita, Shiho Moriai, and Tetsu Iwata
- Target: Hardware and Software

This cipher is intended for use in DRM protocols. Its "lightweightness" can be debated as an area of 4950 GE is significant. The designers of CLEFIA worked for Sony and some of them were involved in the creation of Piccolo.

CLEFIA has been standardized and is part of the ISO-29192[100] with PRESENT.

The CLEFIA encryption and its subroutines.

Piccolo

- Article: *Piccolo: an ultra-lightweight blockcipher*, CHES 11[51]
- Authors: Shibutani, K., Isobe, T., Hiwatari, H., Mitsuda, A., Akishita, T., & Shirai, T.
- Target: Hardware

Piccolo is a GFS with 4 16-bits branches which employs a sophisticated permutation for the diffusion layer instead of a simple shift (like TWINE and as opposed to CLEFIA) as well as whitening. Note that although the branches of the Fesitel structure are made of 16 bits, the permutation operates on words of 8 bits.

The Feistel function is a small SPN where the permutation layer is a multiplication by the same matrix as the one used in the MixNibbles operation in the AES and KLEIN --- although in a different field. The 4x4 S-box was designed especially for Piccolo and, while still having decent non-linearity and differential uniformity, has a tiny hardware footprint: it can be implemented using only 4 NOR gates, 3 XOR gates and 1 XNOR gate. A small SPN is also used as the Feistel function in ITUbee.

The designers work for Sony and several of them worked on CLEFIA.

Fig. 1. Encryption function G_r
Fig. 2. Round permutation RP

The Piccolo encryption.

TWINE

- Article: *TWINE: A Lightweight, Versatile Block Cipher*, Workshop on Lightweight Crypto 11[84]
- Authors: Tomoyasu Suzaki, Kazuhiko Minematsu, Sumio Morioka, and Eita Kobayashi
- Target: Hardware and software

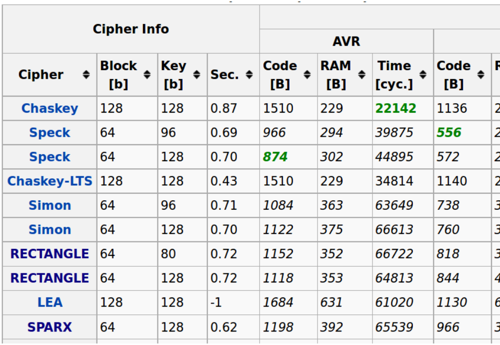
TWINE is a generalised Feistel structure (GFS) with 16 4-bits branches. The Feistel function, called 8 times per round, consists simply in xoring a subkey and applying a 4x4 S-box. The key schedule itself is also a GFS

The round function of TWINE.

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

FELICS Framework

- Fair Evaluation of LIghtweight Cryptographic Systems
- Open benchmarking tool for software implementations
- Block and Stream ciphers
- Ranking of the primitives
- **Send us your implementations!**



Cipher Info				AVR				
Cipher	Block [b]	Key [b]	Sec.	Code [B]	RAM [B]	Time [cyc.]	Code [B]	R
Chaskey	128	128	0.87	1510	229	**22142**	1136	2
Speck	64	96	0.69	*966*	*294*	*39875*	***556***	2
Speck	64	128	0.70	***874***	*302*	*44895*	*572*	2
Chaskey-LTS	128	128	0.43	1510	229	34814	1140	2
Simon	64	96	0.71	*1084*	*363*	*63649*	*738*	3
Simon	64	128	0.70	*1122*	*375*	*66613*	*760*	3
RECTANGLE	64	80	0.72	*1152*	*352*	*66722*	*818*	3
RECTANGLE	64	128	0.72	*1118*	*353*	*64813*	*844*	4
LEA	128	128	-1	*1684*	*631*	*61020*	*1130*	6
SPARX	64	128	0.62	*1198*	*392*	*65539*	*966*	3

https://www.cryptolux.org/index.php/FELICS[1]

[1] NIST'15, see also http://eprint.iacr.org/2015/209.pdf

SPARX

- Substitution-Permutation Addition Rotation Xor[2]
- First ARX-based BC designed for provable security against DC and LC
- **External analysis welcome!**

`https://www.cryptolux.org/index.php/SPARX`

[2] ASIACRYPT'16, see also `https://eprint.iacr.org/2016/984.pdf`

Conclusion for LWC

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

We are hiring!

- post-doc in real-world crypto/blockchain/ privacy
- post-doc in lightweight crypto and side-channel attacks (FDISC project)
- PhDs in applied crypto (PRIDE project)

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