The SKINNY Family of Lightweight Tweakable Block Ciphers

Jérémy Jean

joint work with:

Christof Beierle   Stefan Kölbl   Gregor Leander   Amir Moradi
Thomas Peyrin   Yu Sasaki   Pascal Sasdrich   Siang Meng Sim

CRYPTO 2016

August 17, 2016

Goals and Results

Goals

- Alternative to NSA-designed SIMON block cipher [BSS+13]
- Construct a lightweight (tweakable) block cipher
- Achieve scalable security
- Suitable for most lightweight applications
- Perform and share full security analysis
- Efficient software/hardware implementations in many scenarios

Goals and Results

Goals

- Alternative to NSA-designed SIMON block cipher [BSS+13]
- Construct a lightweight (tweakable) block cipher
- Achieve scalable security
- Suitable for most lightweight applications
- Perform and share full security analysis
- Efficient software/hardware implementations in many scenarios

Results

- SKINNY family of lightweight (tweakable) block ciphers
- Generalize the STK construction from TWEAKEY framework [JNP14]
- Block sizes n: 64 and 128 bits
- Various key+tweak sizes: n, $2n$ and $3n$ bits
- Security guarantees for differential/linear cryptanalysis in both single-key (SK) and related-key (RK) models
- Efficient and competitive software/hardware implementations
  - Round-based SKINNY-64-128: 1696 GE
  - CTR mode @ Skylake (avx2): 2.63 c/B

Tweakable Block Cipher

- Having a tweakable block cipher has many applications:
  - Authenticated encryption
  - Disk/memory encryption
  - Hashing: block counter as tweak for HAIFA-like CF
  - (More...)
- There are have been several proposed constructions, most of which rely on a block cipher, and generically introduce the tweak (XEX, XPX, XTS, etc.)
- Very few direct constructions: Hasty Pudding Cipher, Threefish, Mercy, BLAKE2
- TWEAKEY framework [JNP14]: as a designer, key and tweak seem like they have to be handled in the same way by the primitive, with a ''tweakey schedule''

TWEAKEY Framework [JNP14]

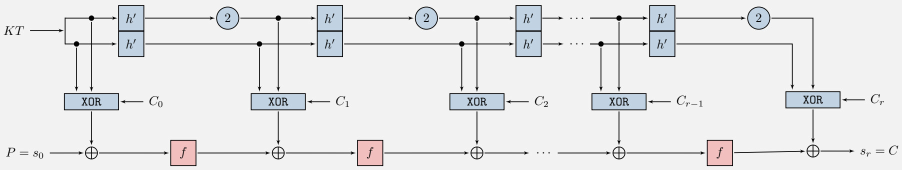
High-Level Overview

- Bring key and tweak schedules together
- Extend key-alternating strategy

Superposition-Tweakey (STK)

- Fully linear scheduling (h': cell permutation)
- Provide bounds in terms of number of active Sboxes in related-key/related-tweak (RK/RT)
- **Trick:** linear code due to small field multiplications to bound the number of cancellations in the XORs
- Allows usage of automated tools to find bounds (even for RK/RT)

Example of the TK2 construction: $|KT| = |K| + |T| = 2 \cdot |P|$



SKINNY: General Design Strategy

- Start from weak crypto components, but providing very efficient implementations
  - Opposed to AES: strong Sbox and diffusion $\Rightarrow$ only 10 rounds
  - Similar to SIMON: only AND/XOR/ROT $\Rightarrow$ many rounds
- Reuse AES well-understood design strategy
- Remove all operations not strictly necessary to security

SKINNY: Similarities and Differences with the AES

Similarities

Design

- Key-alternating cipher
- 4×4 internal state
- AES-like SPN round function

Security

- Diffusion achieved by SR+MC
- Bounds on # of active Sboxes
- Design resistant against lin. and diff. cryptanalysis

Differences

Design

- More rounds
- Linear TWEAKEY schedule
- Non-optimal diffusion matrix (binary, branch number: 2)

Security

- Related-key/related-tweak security claimed
- **SK bounds** harder to prove than AES (non MDS) $\rightarrow$ MILP
- Simpler MILP modeling (RK/RT)

Specifications: Overview

Specifications

- SKINNY has a state of either 64 bit ($s = 4$) or 128 bits ($s = 8$).
- Internal state IS: viewed as a 4×4 matrix of s-bit elements.
  $\Rightarrow |IS| = n = 16s \in \{64, 128\}$.
- The tweakey size can be n, $2n$ or $3n$.

$$IS = \begin{bmatrix} m_0 & m_1 & m_2 & m_3 \\ m_4 & m_5 & m_6 & m_7 \\ m_8 & m_9 & m_{10} & m_{11} \\ m_{12} & m_{13} & m_{14} & m_{15} \end{bmatrix}$$

Number of Rounds

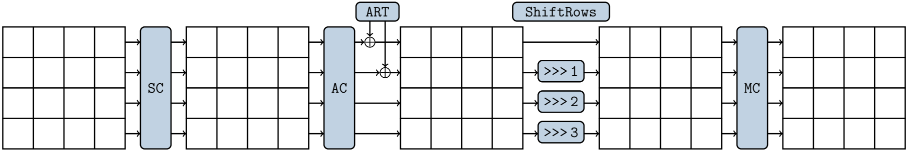
	Tweakey size		
Block size n	n	$2n$	$3n$
64	32	36	40
128	40	48	56

Comparison: SKINNY-64-128 has 36 rounds, SIMON-64-128 has 44 rounds.

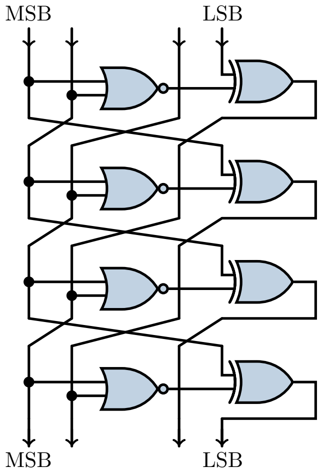
SKINNY Round Function

AES-like Round Function

- **SubCells (SC)**: Application of a s-bit Sbox to all 16 cells
- **AddConstants (AC)**: Inject round constants in the state
- **AddRoundTweakey (ART)**: Extract and inject the subtweakeys to half the state
- **ShiftRows (SR)**: Right-rotate Line i by i positions
- **MixColumns (MC)**: Multiply the state by a binary matrix



SKINNY **4-bit Sbox**



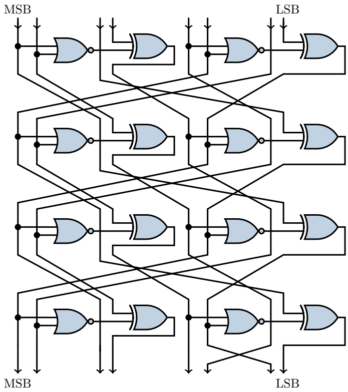
$\mathcal{S}_4$: 4-bit Sbox for SKINNY-64-*

- Almost PICCOLO Sbox [SIH+11]
- Implementation: 4 NOR and 4 XOR
- Hardware cost: 12 GE

Properties

- Maximal diff. probability: 2^{-2}
- Maximal abs. linear bias: 2^{-2}
- $\deg(\mathcal{S}_4) = \deg(\mathcal{S}_4^{-1}) = 3$
- One fixed point: $\mathcal{S}_4(0xF) = 0xF$
- Branch number: 2

SKINNY 8-bit Sbox



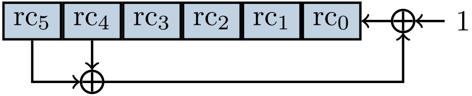
$\mathcal{S}_8$: 8-bit Sbox for SKINNY-128-*

- Generalize the $\mathcal{S}_4$ construction
- Implementation: 8 NOR and 8 XOR
- Hardware cost: 24 GE

Properties

- Maximal diff. probability: 2^{-2}
- Maximal abs. linear bias: 2^{-2}
- $\deg(\mathcal{S}_8) = \deg(\mathcal{S}_8^{-1}) = 6$
- One fixed point: $\mathcal{S}_8(\texttt{0xFF}) = \texttt{0xFF}$
- Branch number: 2

SKINNY Round Constants



6-bit LFSR

- The round constants are produced with a LFSR
- State: $(rc_5 || rc_4 || rc_3 || rc_2 || rc_1 || rc_0)$
- Initial value 0, clocked **before** injection
- Hardware cost: 1 XNOR

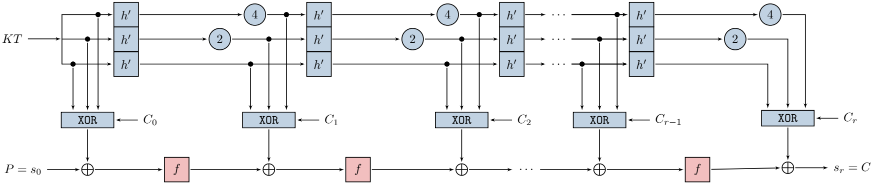
$s = 4$

$$\begin{bmatrix} rc_3||rc_2||rc_1||rc_0 & 0 & 0 & 0 \\ 0||\ \ 0||rc_5||rc_4 & 0 & 0 & 0 \\ \mathtt{0x2} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

$s = 8$

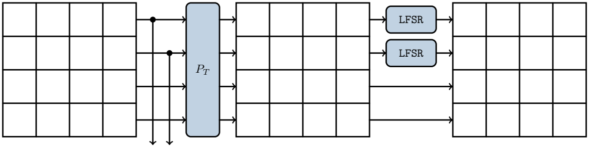
$$\begin{bmatrix} 0||\ \ 0||\ \ 0||\ \ 0||rc_3||rc_2||rc_1||rc_0 & 0 & 0 & 0 \\ 0||\ \ 0||\ \ 0||\ \ 0||\ \ 0||\ \ 0||rc_5||rc_4 & 0 & 0 & 0 \\ \mathtt{0x2} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

TWEAKEY Schedule in SKINNY



TWEAKEY Schedule

- Similar to the STK construction
- Subtweakey: first and second rows of all tweakey words are injected in the internal state
- Then, the tweakey words are updated independently:
  - The cells are reordered with a permutation P_T
  - Half the cells are individually updated with LFSRs (1 XOR each)



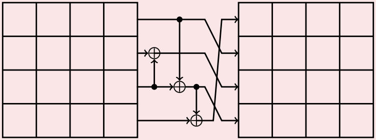
SKINNY **MixColumns**

MixColumns

- Matrix multiplication performed as in the MixColumns of the AES
- However:
  - The matrix $\mathbf{M}$ is binary
  - It has branch number 2: $\mathbf{M} \times (0, \alpha, 0, 0)^\top = (0, 0, \alpha, 0)^\top$

$$\mathbf{M} = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 \end{pmatrix}$$

Implementation Using 3 XORs



Design Choices

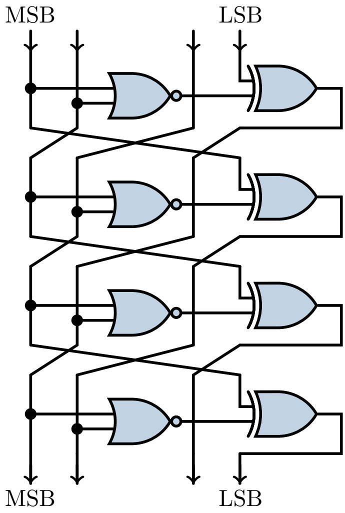
Criteria for Elementary Component Selection

- Informally: Minimize number of operations, maximize security
- Many new components, selected incrementally:
  - Sboxes
  - ShiftRows+MixColumns
  - TWEAKEY Permutation P_T
- Selection based on two independent estimations:
  - Security (manual analysis and MILP)
  - Implementation efficiency (hardware/software)

Hardware Area Estimation

- NOR/NAND gate: 1 GE
- OR/AND gate: 1.33 GE
- XOR/XNOR gate: 2.67 GE
- NOT gate: 0.67 GE
- One memory bit: 6 GE (using scan flip-flop)

Rationale: Selection of $\mathcal{S}_4$



Selection process

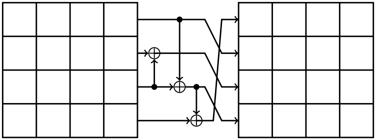
- Optimization for HW implementation
- Explore all permutations using an increasing number of instructions from $\{\text{NAND}, \text{NOR}, \text{XOR}, \text{NXOR}\}$
- Stop when reaching certain criterion $(p_{max}, \epsilon_{max}, \ldots)$
- **Result:** $\mathcal{S}_4$ with 4 NOR + 4 XOR
- Almost PICCOLO Sbox
- 12 GE with special 4-input gates

SKINNY-**128-***

Similar selection intractable for the 8-bit Sbox ($\mathcal{S}_8$)
$\Rightarrow$ reuse structure of $\mathcal{S}_4$

Rationale: Selection of $\mathbf{M}$

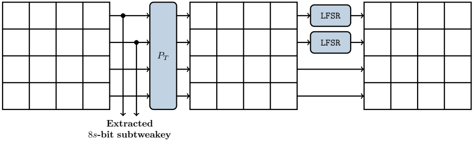
$$\mathbf{M} = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 \end{pmatrix}$$

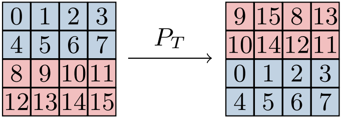


Selection (for fixed ShiftRows)

- **Implementation-wise requirements:**
  - Binary matrix: implementations using only XOR (no shifts)
  - Restricted to (invertible) matrices using at most 3 XORs
- **Security-wise requirements:**
  - Full diffusion (enc/dec) in 5 or 6 rounds
  - One subkey XORed to half the state affects the whole state after one round forwards and backwards
- **Number of candidates:** 24 matrices (all 6-round full diffusion)
- Choose $\mathbf{M}$ maximizing the number of active Sboxes for 12+ rounds

Rationale: TWEAKEY Schedule





Selection

- **Security-wise requirements:**
  - Follow the STK construction
  - Linear and independent updates for each tweakey state TK_i
  - P_T ensures full tweakey state is used every 2 rounds
  - LFSR updates verify the TWEAKEY constraints (cancellations)
- **Implementation-wise requirements:**
  - XOR only half the tweakey state (two lines): save about 85 GE for 64-bit blocks for round-based implementations
  - Ultra light LFSR: only 1 XOR
  - Nibble-wise permutation P_T
- **Number of candidates:** 5040 permutations $\times$ 6 pairs of lines $= 30240$
- Sort using Sbox counting (MILP), then pick best one

Theoretical Performances of SKINNY and Others

Cipher	Rounds	#operations per bit without KS	#operations per bit with KS	Round-based area estimation
SKINNY-64-128	36	**117**	**139.5**	**8.68**
SIMON-64-128	44	88	154	**8.68**
PRESENT-64-128	31	147.2	161.8	**12.43**
PICCOLO-64-128	31	162.75	162.75	**12.35**
SKINNY-128-128	40	130	130	**7.01**
SIMON-128-128	72	136	204	**7.34**
NOEKEON-128-128	16	100	200	**30.36**
AES-128-128	10	202.5	248.1	**59.12**

Example of SKINNY-64-128 (more in the paper)

- 1R: $(4\ \text{NOR} + 4\ \text{XOR})/4$ [SB] $+ (3\ \text{XOR})/4$ [MC] $+ (32\ \text{XOR})/64$ [ART]
- That is (per bit per round): 1 NOR + 2.25 XOR
- #operations per bit (without KS): $(1 + 2.25) \times 36 = 117$
- #operations per bit per round in KS only (TK2): $(8\ \text{XOR})/64$ [LFSR] $+ (32\ \text{XOR})/64$ $[TK_1 \oplus TK_2] = 0.625$
- RB area estimation: $1 \times 1 + (2.25 + 0.625) \times 2.67 = 8.68$
- **Very low number of operations per plaintext bit.**

Security Analysis: Overview

Claims

- Security against known classes of attacks
- Security in the related-key/related-tweak model

Attack Vectors Considered

- Differential/Linear cryptanalysis
- Integral attack [DKR97]
- Division property [Tod15, BC16]
- Meet-in-the-middle attack [DS08, DKS10, DFJ13]
- Impossible differential attack [Knu98]
- Invariant subspace attack [LMR15]
- Slide attack [BW99, BW00]
- Algebraic attack

ASIC Implementations

Preliminaries

- ASIC: Application-Specific Integrated Circuit
- Synthesis: Synopsys Design Compiler version A-2007.12-SP1
- UMCL18G212T3 standard cell library [Vir04]
  - UMC L180 0.18μm 1P6M logic process
  - Typical voltage of 1.8 V

Four scenarios

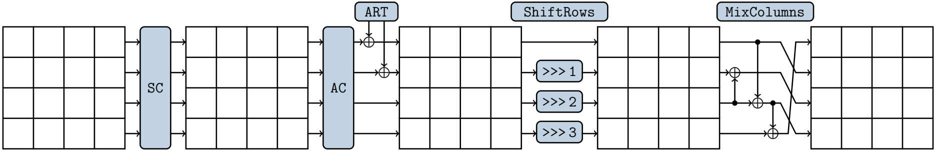
- Round-based implementations
  $\Rightarrow$ most important target for our design choices
- Fully unrolled implementations (see full version)
- Serial implementations (see full version)
  - Bit-serial
  - Nibble- or byte-serial
- Threshold implementations (see full version)

Round-Based Implementation Results

	Area	Delay	Throughput @100KHz	Throughput @maximum
	GE	ns	KBit/s	MBit/s
SKINNY-64-128	**1696**	1.87	177.78	951.11
SKINNY-128-128	2391	2.89	320.00	1107.20
SKINNY-128-256	3312	2.89	266.67	922.67
SIMON-64-128	**1751**	1.60	145.45	870
SIMON-128-128	2342	1.60	188.24	1145
SIMON-128-256	3419	1.60	177.78	1081
LED-64-64	2695	-	198.9	-
LED-64-128	3036	-	133.0	-
PRESENT-64-128	1884	-	200.00	-
PICCOLO-64-128	1773	-	193.94	-

SKINNY in a Nutshell

- New very lightweight family of tweakable block cipher
  $\Rightarrow$ Almost as light as possible
- Alternative to SIMON family of block ciphers
- Very efficient implementations (both SW and HW)
- SK and RK/RT security garantees



More in the Full Version

- Complete description of all design choices
- Security analysis
  - Detailed analysis of many known classes of attacks
- All implementation results
  - ASIC: Bit/Nibble-serial, Low-latency, Threshold
  - FPGA (Virtex 7)
  - Micro-controllers (ATmega644)
  - Software (bit-sliced, CTR mode)
- Low-latency tweakable block cipher: MANTIS
  - Similar to PRINCE, but including a tweak input
  - Useful for memory encryption

The End.

Paper, Specifications, Results and Updates available at:
https://sites.google.com/site/skinnycipher/

The End.

Paper, Specifications, Results and Updates available at:
https://sites.google.com/site/skinnycipher/

Thank you for your attention!

Backup Slides

Differential/Linear Cryptanalysis

- We adapt the number of rounds to get resistance (+ margin):
  - SKINNY-64-64/128/192 has 32/36/40 rounds
  - SKINNY-128-128/256/384 40/48/56 rounds
- As a result, for all SKINNY variants:
  - **SK** security reached in less than 40% of the rounds
  - **TK2** security reached in 40 – 45% of the rounds

Comparison with Other 64/128 and 128/128 Ciphers

Cipher	Single Key (SK)	Related Key (RK)
SKINNY-64-128	8/36 = 22%	15/36 = 42%
SIMON-64-128	19/44 = 43%	no bound known
SKINNY-128-128	15/40 = 37%	19/40 = 47%
SIMON-128-128	41/72 = 57%	no bound known
AES-128	4/10 = 40%	6/10 = 60%
NOEKEON-128	12/16 = 75%	12/16 = 75%

Unrolled Implementations

	Area	Delay	Throughput @100KHz	Throughput @maximum
	GE	ns	KBit/s	MBit/s
SKINNY-64-128	17454	51.59	6400.00	1240.55
SKINNY-128-128	32415	97.53	12800.00	1307.06
SKINNY-128-256	46014	119.57	12800.00	1070.50
LED-64-128	111496	-	-	-
PRESENT-64-128	56722	-	-	-
PICCOLO-64-128	25668	-	-	-

Notes

- One encryption in one cycle $\Rightarrow$ best throughput
- Long critical path $\Rightarrow$ long delays
- Very few academic unrolled implementations

Serial Implementations (nibble- or byte-wise)

	Area	Delay	Clock Cycles	Throughput @100KHz	Throughput @maximum
	GE	ns	#	KBit/s	MBit/s
SKINNY-64-128	1399	0.95	788	8.12	85.49
SKINNY-128-128	1840	1.03	872	14.68	142.51
SKINNY-128-256	2655	0.95	1040	12.31	129.55
SIMON-64-128	1000	-	-	16.7	-
SIMON-128-128	1317	-	-	22.9	-
SIMON-128-256	1883	-	-	21.1	-
LED-64-128	1265	-	1872	3.4	-
PRESENT-64-128	1391	-	559	11.45	-
PICCOLO-64-128	1773	-	528	12.12	-

Notes

- The datapath is either on 4 bits (nibble) or 8 bits (byte)

Bit-Serial Implementations

	Area	Delay	Clock Cycles	Throughput @100KHz	Throughput @maximum
	GE	ns	#	KBit/s	MBit/s
SKINNY-64-128	1172	1.06	3152	2.27	22.06
SKINNY-128-128	1481	1.05	6976	1.83	17.47
SKINNY-128-256	2125	0.89	8320	1.53	17.29
SIMON-64-128	958	-	-	4.2	-
SIMON-128-128	1234	-	-	2.9	-
SIMON-128-256	1782	-	-	2.6	-

Notes

- The datapath is reduced to a single bit
- SIMONcan use regular flip-flops (4.67 GE)
- SKINNYhas to use (some) scan flip-flops (6 GE)
- So far, the possibility of implementing an SPN cipher in a bit-serial way is an unique feature of SKINNY

Bibliography I

Christina Boura and Anne Canteaut.
Another View of the Division Property.
CRYPTO 2016. LNCS, Springer, to appear, 2016.

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

Alex Biryukov and David Wagner.
Slide Attacks.
In Lars R. Knudsen, editor, FSE'99, volume 1636 of LNCS, pages 245--259. Springer, March 1999.

Alex Biryukov and David Wagner.
Advanced Slide Attacks.
In Bart Preneel, editor, EUROCRYPT 2000, volume 1807 of LNCS, pages 589--606. Springer, May 2000.

Patrick Derbez, Pierre-Alain Fouque, and Jérémy Jean.
Improved Key Recovery Attacks on Reduced-Round AES in the Single-Key Setting.
In Thomas Johansson and Phong Q. Nguyen, editors, EUROCRYPT 2013, volume 7881 of LNCS, pages 371--387. Springer, May 2013.

Joan Daemen, Lars R. Knudsen, and Vincent Rijmen.
The Block Cipher Square.
In Eli Biham, editor, FSE'97, volume 1267 of LNCS, pages 149--165. Springer, January 1997.

Orr Dunkelman, Nathan Keller, and Adi Shamir.
Improved Single-Key Attacks on 8-Round AES-192 and AES-256.
In Masayuki Abe, editor, ASIACRYPT 2010, volume 6477 of LNCS, pages 158--176. Springer, December 2010.

Bibliography II

Hüseyin Demirci and Ali Aydin Selçuk.
A Meet-in-the-Middle Attack on 8-Round AES.
In Kaisa Nyberg, editor, FSE 2008, volume 5086 of LNCS, pages 116--126. Springer, February 2008.

Jérémy Jean, Ivica Nikolic, and Thomas Peyrin.
Tweaks and Keys for Block Ciphers: The TWEAKEY Framework.
LNCS, pages 274--288. Springer, December 2014.

Lars Knudsen.
DEAL - A 128-bit Block Cipher.
In NIST AES Proposal, 1998.

Gregor Leander, Brice Minaud, and Sondre Rønjom.
A Generic Approach to Invariant Subspace Attacks: Cryptanalysis of Robin, iSCREAM and Zorro.
LNCS, pages 254--283. Springer, 2015.

Kyoji Shibutani, Takanori Isobe, Harunaga Hiwatari, Atsushi Mitsuda, Toru Akishita, and Taizo Shirai.
Piccolo: An Ultra-Lightweight Blockcipher.
In Bart Preneel and Tsuyoshi Takagi, editors, CHES 2011, volume 6917 of LNCS, pages 342--357. Springer, September / October 2011.

Yosuke Todo.
Structural Evaluation by Generalized Integral Property.
LNCS, pages 287--314. Springer, 2015.

Virtual Silicon Inc.
0.18 μm VIP Standard Cell Library Tape Out Ready, Part Number: UMCL18G212T3, Process: UMC Logic 0.18 μm Generic II Technology: 0.18μm, July 2004.