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

Université de Rennes 1 - Crypto Seminar

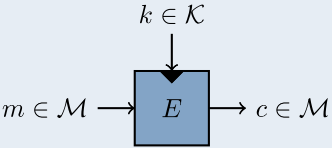
June 3, 2016

Plan

Plan

Block Cipher

Primitive



Three variables:

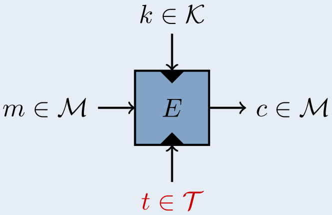
- A secret key k form the set of all keys $\mathcal{K}$
- A plaintext from the set $\mathcal{M}$
- Its corresponding ciphertext: $c = E_k(m)$

Properties

- For every key k, E_k is a permutation over $\mathcal{M}$
- For a fixed unknown key k and a given set $\{(m_i, E_k(m_i))\}$, recovering k should be hard
- For $k \xleftarrow{\$} \mathcal{K}$ drawn uniformly at random from $\mathcal{K}$, E_k should be indistinguishable from a random permutation

Tweakable Block Cipher

Primitive



Four variables:

- A secret key k form the set of all keys $\mathcal{K}$
- A tweak input t form the set of all tweaks $\mathcal{T}$
- A plaintext from the set $\mathcal{M}$
- Its corresponding ciphertext: $c = E_k^t(m)$

Properties

- For every key k and every tweak t, E_k^t is a permutation over $\mathcal{M}$

Tweakable Block Cipher

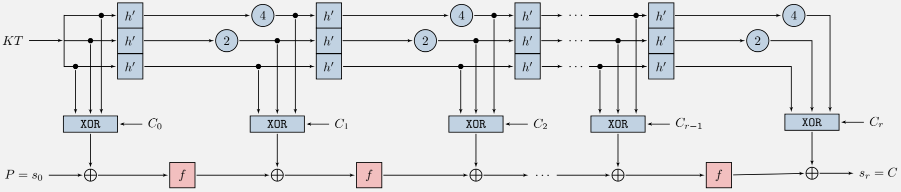
- Having a tweakable block cipher has many applications:
  - Authenticated encryption
  - Disk/memory encryption
  - Hashing: block counter as tweak for HAIFA-like CF
- There are have been many proposed constructions
- Most of which rely on a block cipher, and generically introduce the tweak (XEX, XTS, etc.)
- Very few direct constructions: Hasty Pudding Cipher, Threefish, 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
- Fully linear scheduling (h': cell permutation)
- Provide bounds in terms of number of active Sboxes in related-key/related-tweak
- **Trick:** linear code due to small field multiplications (2 and 4) to bound the number of cancellations in the XORs
- This allows the usage of automated tools to find bounds

Example of the TK3 construction: $|KT| = |K| + |T| = 3 \cdot |P|$



Plan

SKINNY: Specifications

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

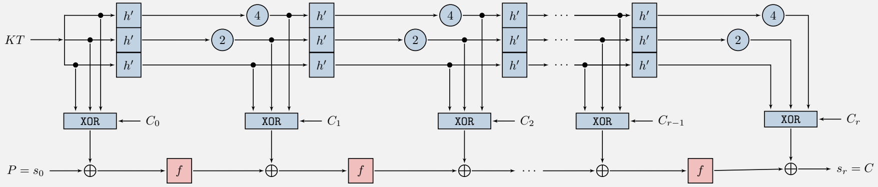
Comparison: SKINNY-64-128 has 36 rounds, SIMON-64-128 has 44 rounds.

SKINNY: Specifications

General Overview

- SKINNY follows the TWEAKEY framework, however:
  - It generalizes the STK construction (three tweakey words TK_i)
  - Only half the tweakey state is extracted and injected in the internal state
  - The field multiplications are replaced by a LFSR
- The round function f is an AES-like SPN
- The round constants C_i are produced by a LFSR

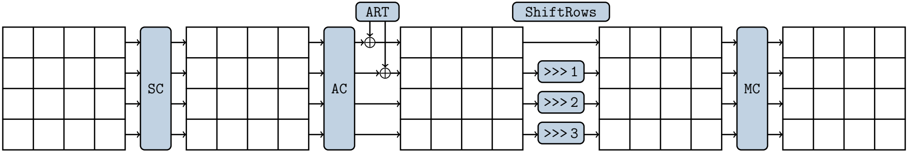
STK Construction



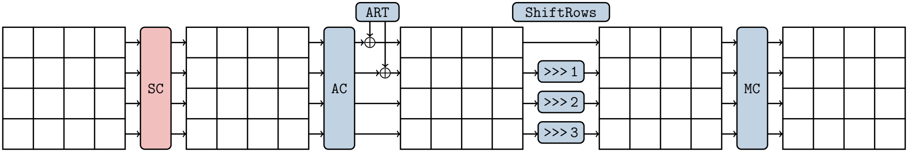
Round Function

AES-like Round Function

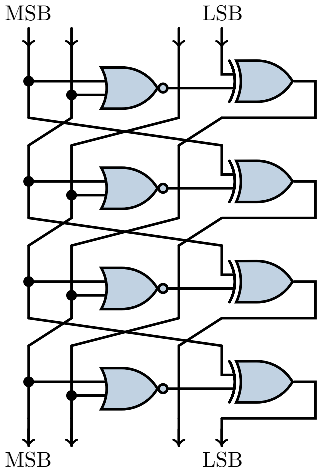
- **SubCells (SC)**: Application of a s-bit Sbox to all 16 cells
- **AddConstants (AC)**: Inject round constants in the state
- **AddRoundTweakey (ART)**: Extract and inject the subtweakeys to half the state
- **ShiftRows (SR)**: Right-rotate line i by i positions
- **MixColumns (MC)**: Multiply the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



Round Function



4-bit Sbox



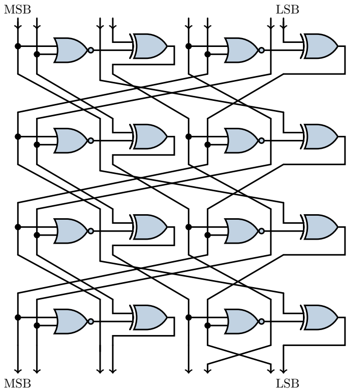
$\mathcal{S}_4$: 4-bit Sbox for SKINNY-64-*

- 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

8-bit Sbox



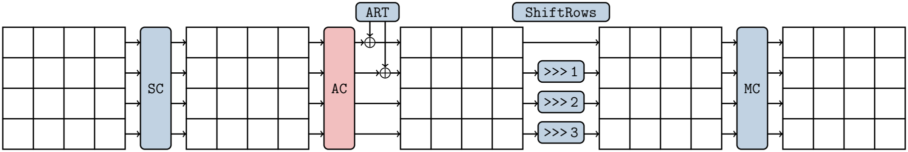
$\mathcal{S}_8$: 8-bit Sbox for SKINNY-128-*

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

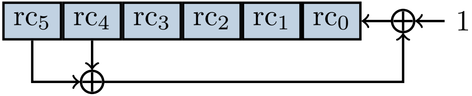
Properties

- 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

Round Function



Round Constants



6-bit LFSR

- The round constants are produced with a LFSR
- State: $(\mathrm{rc}_5 \| \mathrm{rc}_4 \| \mathrm{rc}_3 \| \mathrm{rc}_2 \| \mathrm{rc}_1 \| \mathrm{rc}_0)$
- Initial value 0, clocked **before** injection
- Hardware cost: 1 XNOR

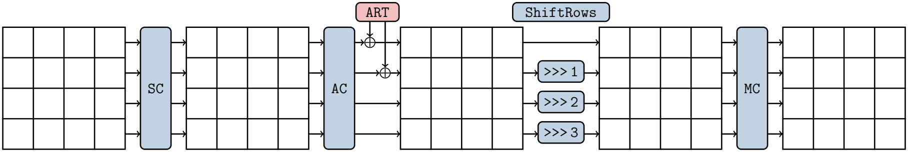
$s = 4$

$$\begin{bmatrix} \mathrm{rc}_3 \| \mathrm{rc}_2 \| \mathrm{rc}_1 \| \mathrm{rc}_0 & 0 & 0 & 0 \\ 0 \| \quad 0 \| \mathrm{rc}_5 \| \mathrm{rc}_4 & 0 & 0 & 0 \\ \mathtt{0x2} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

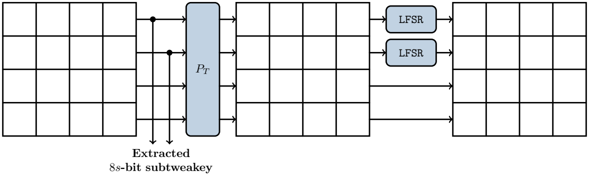
$s = 8$

$$\begin{bmatrix} 0 \| \quad 0 \| \quad 0 \| \quad 0 \| \mathrm{rc}_3 \| \mathrm{rc}_2 \| \mathrm{rc}_1 \| \mathrm{rc}_0 & 0 & 0 & 0 \\ 0 \| \quad 0 \| \quad 0 \| \quad 0 \| \quad 0 \| \quad 0 \| \mathrm{rc}_5 \| \mathrm{rc}_4 & 0 & 0 & 0 \\ \mathtt{0x2} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

Round Function

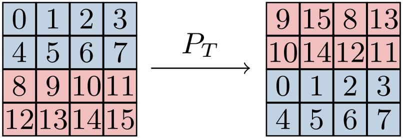


Add Round Tweakey and TWEAKEY schedule



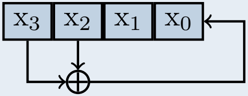
TWEAKEY Schedule

- Similar to the STK construction
- Subtweakey: first and second rows of all tweakey words are injected in the internal state
- Then, the tweakey words $TK2$ and $TK3$ are updated independently:
  - The cells are reordered with a permutation P_T
  - Each cell is individually updated with an LFSR

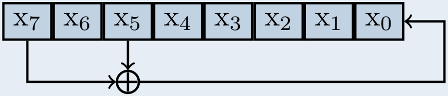


Add Round Tweakey and TWEAKEY schedule

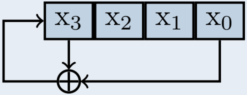
LFSR for $TK2$ when $s = 4$



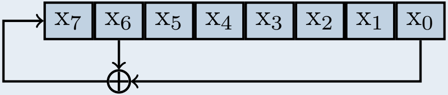
LFSR for $TK2$ when $s = 8$



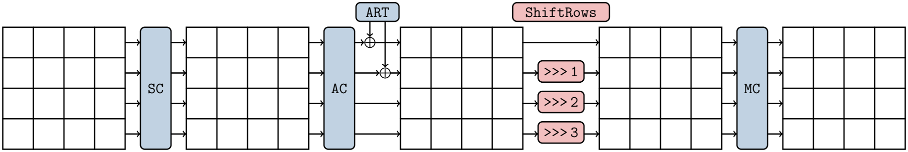
LFSR for $TK3$ when $s = 4$



LFSR for $TK3$ when $s = 8$

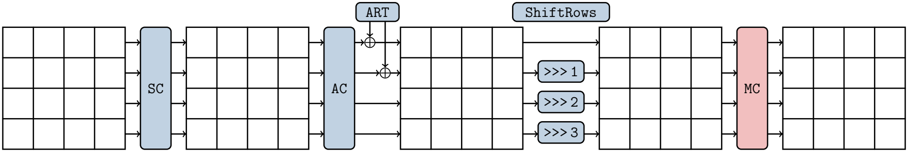


ShiftRows



- Similar to the ShiftRows in the AES
- However, the lines are rotated to the right

MixColumns



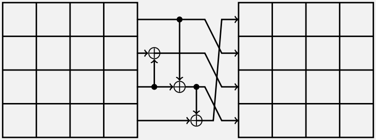
MixColumns

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



Plan

Rationale

General Goals

- Cipher well-suited for most lightweight applications
- Efficient hardware implementation
- Do not waste **any** operations: only keep vital components
- Removing any operations from SKINNY results in an unsecure cipher
- Good micro-controllers performances as second criteria

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)

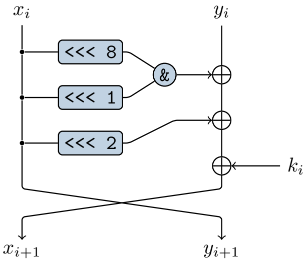
Hardware Implementations

- **Low-latency**: one cipher call takes one cycle
- **Round-based**: one round takes one cycle
- **Bit-serial**: the datapath is reduced to a single bit

Generalities: Feistel or SPN?

SIMON

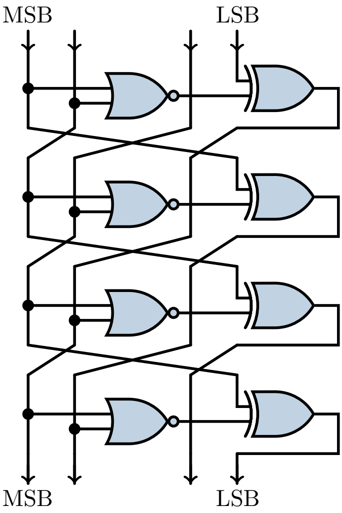
- Balanced Feistel Network
- Very small number of operations
- Highly scalable
- Difficult to analyze



SKINNY

- AES-like SP Network
- Very small number of operations
- Tweakable block cipher
- Less scalable than SIMON
- Easier to analyze, even for related-key/related-tweak security
- No whitening key

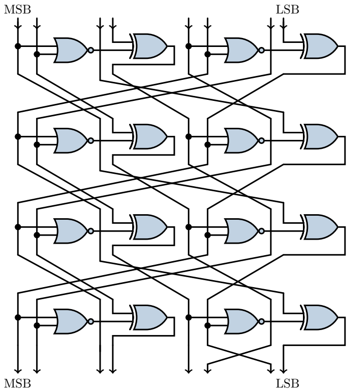
Rationale: Selection of $\mathcal{S}_4$



Selection process

- Optimization for hardware implementation
- Explore all permutations using an increasing number of instructions from {NAND, NOR, XOR, 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

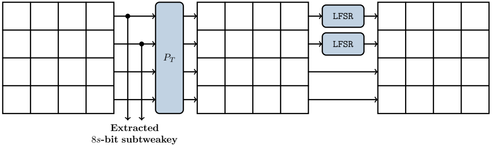
Rationale: Selection of $\mathcal{S}_8$



Selection process

- Full search infeasible (space too large)
- We reuse the structure of $\mathcal{S}_4$
- With 1 NOR/XOR per iteration:
  - Check all bit permutations
  - 8+ iterations needed
  - But: asymmetric degree $\mathcal{S}_4/\mathcal{S}_4^{-1}$
- With 2 NOR/XOR per iteration:
  - Same simplified search
  - 4+ iterations needed
  - Symmetric algebraic degree
  - Swap two bits: $3 \to 1$ fixed point

Rationale: Tweakey Schedule



0	1	2	3
4	5	6	7
8	9	10	11
12	13	14	15

$\xrightarrow{P_T}$

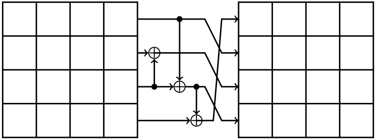
9	15	8	13
10	14	12	11
0	1	2	3
4	5	6	7

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
  - Light LFSR: only 1 XOR
  - Nibble-wise permutation P_T
- **Number of candidates**: 5040 permutations $\times$ 6 pairs of lines $= 30240$
- Reduce to 4 candidates by maximizing the number of active Sboxes for 12+ rounds $\Rightarrow$ Pick the first one as P_T (XOR 2 first lines)

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
  - Good differential and linear bounds
  - 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

Comparing Differential Bounds for SKINNY-64-128

Cipher	Model	Rounds															
		1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**
SKINNY	**SK**	1	2	5	8	12	16	26	36	41	46	51	55	58	61	66	75
(36 rounds)	**TK2**	0	0	0	0	1	2	3	6	9	12	16	21	25	31	35	40

Notes for SKINNY

- **SK** corresponds to the single-key model
- The **TK2** model corresponds to the related-key/related-tweak model (difference possible in the two tweakey words TK_1 and TK_2)
- The values give lower bounds on the number of active Sboxes for up to 16 rounds
- They may not be tight (can only be bigger)
- Produced using MILP optimization
- The bounds are for differential characteristics

Comparing Differential Bounds for SKINNY-64-128

Cipher	Model	Rounds															
		1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**
SKINNY	**SK**	1	2	5	8	12	16	26	36	41	46	51	55	58	61	66	75
(36 rounds)	**TK2**	0	0	0	0	1	2	3	6	9	12	16	21	25	31	35	40
LED	**SK**	1	5	9	25	26	30	34	50	51	55	59	75	76	80	84	100
(48 rounds)	**TK2**	0	0	0	0	0	0	0	0	1	5	9	25	26	30	34	50

Comparison with LED [GPPR11]

- The bounds for LED are tight
- LED has a strong diffusion in **SK**: it reaches more active Sboxes than SKINNY (same as AES)
- However, in **TK2**, LED provides less active Sboxes for 16+ rounds
- The LED round function is much heavier than that SKINNY

Comparing Differential Bounds for SKINNY-64-128

Cipher	Model	Rounds															
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
SKINNY	SK	1	2	5	8	12	16	26	36	41	46	51	55	58	61	66	75
(36 rounds)	TK2	0	0	0	0	1	2	3	6	9	12	16	21	25	31	35	40
PICCOLO	SK	0	5	9	14	18	27	32	36	41	45	50	54	59	63	68	72
(31 rounds)	TK2	0	0	0	0	0	0	0	5	9	14	18	18	23	27	27	32

Comparison with PICCOLO [SIH+11]

- The bounds are quite similar
- We estimate the number of active Sboxes from the number of active F-functions given in [SIH+11].
- However, SKINNY does not use an MDS matrix as PICCOLO

Comparing Differential Bounds for SKINNY-64-128

Cipher	Model	Rounds															
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
SKINNY	SK	1	2	5	8	12	16	26	36	41	46	51	55	58	61	66	75
(36 rounds)	TK2	0	0	0	0	1	2	3	6	9	12	16	21	25	31	35	40
MIDORI	SK	1	3	7	16	23	30	35	38	41	50	57	62	67	72	75	84
(16 rounds)	TK2	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-

Comparison with MIDORI [BBI+15]

- Broken
- No related-key bounds are known for MIDORI
- The diffusion of MIDORI is better than the one of SKINNY
- The round function of SKINNY is lighter

Comparing Differential Bounds for SKINNY-64-128

Cipher	Model	Rounds															
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
SKINNY	SK	1	2	5	8	12	16	26	36	41	46	51	55	58	61	66	75
(36 rounds)	TK2	0	0	0	0	1	2	3	6	9	12	16	21	25	31	35	40
PRESENT	SK	-	-	-	-	10	-	-	-	-	20	-	-	-	-	30	-
(31 rounds)	TK2	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-

Comparison with PRESENT [BKL+07]

- The bounds for PRESENT are tight
- No related-key bounds are known for PRESENT

Comparing Differential Bounds for SKINNY-64-128

Cipher	Model	Rounds															
		1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**
SKINNY	**SK**	1	2	5	8	12	16	26	36	41	46	51	55	58	61	66	75
(36 rounds)	**TK2**	0	0	0	0	1	2	3	6	9	12	16	21	25	31	35	40
TWINE	**SK**	0	1	2	3	4	6	8	11	14	18	22	24	27	30	32	-
(36 rounds)	**TK2**	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-

Comparison with TWINE [SMMK13]

- **SK** bounds are taken from the specifications [SMMK13]
- No correct related-key bounds are known for TWINE (the designers claim 6 Sboxes for 2R, but a characteristic with 0 Sbox exists)

Theoretical Performances of SKINNY-64-128

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: $1 \times 1 + (2.25 + 0.625) \times 2.67 = 8.68$

Plan

Security Analysis: Overview

Claims

- Security against known classes of attacks
- Security in the related-key model
- No garantees for known or chosen key
- No claim for related-cipher security (the constant does not encode the cipher parameters)

Attack Vectors Considered

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

Differential/Linear Cryptanalysis

Model	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
SK	1	2	5	8	12	16	26	**36**	41	46	51	55	58	61	**66**	75	82	88	92	96
TK1	0	0	1	2	3	6	10	13	16	23	**32**	38	41	45	49	54	59	62	**66**	70
TK2	0	0	0	0	1	2	3	6	9	12	16	21	25	31	**35**	40	43	47	52	57
TK3	0	0	0	0	0	0	1	2	3	6	10	13	16	19	24	27	31	**35**	43	45
SK Lin	1	2	5	8	13	19	25	**32**	38	43	48	52	55	58	**64**	70	76	80	85	90

Model	21	22	23	24	25	26	27	28	29	30
SK	102	108	(114)	(116)	(124)	(132)	(136)	(136)	(148)	(158)
TK1	75	79	83	85	88	95	102	(108)	(112)	(120)
TK2	59	**64**	67	72	75	82	85	88	92	96
TK3	48	51	55	58	60	**65**	72	77	81	85
SK Lin	96	102	107	(110)	(118)	(122)	(128)	(136)	(141)	(143)

Differential/Linear Cryptanalysis

- With a Sbox with local property 2^{-2}, we need $n/2$ active Sboxes to achieve n-bit security:
  - SKINNY-64-$\star$ $\Rightarrow$ 32 Sboxes required
  - SKINNY-128-$\star$ $\Rightarrow$ 64 Sboxes required
- Then, we adapt the number of rounds:
  - SKINNY-64-64/128/192 has 32/36/40 rounds
  - SKINNY-128-128/256/384 40/48/56 rounds
- Hence, for all SKINNY variants:
  - **SK** security reached in less than 40% of the rounds
  - **TK2** security reached in $40-45\%$ of the rounds
- In comparison, for SIMON:
  - SIMON-64-128/**SK**: best attack on $19/44 = 43\%$ of the rounds
  - SIMON-128-128/**SK**: best attack on $41/72 = 57\%$ of the rounds
  - Nothing known so far for **TK2** security

Plan

ASIC Implementations

Preliminaries

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

Three scenarios

- Round-based implementations
  $\Rightarrow$ most important target for our design choices
- Fully unrolled implementations
- Serial implementations
- Threshold implementations

Round-Based Implementations

	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	-

Round-Based Implementations: Details

SKINNY-**64-128**
▪ Round function (907 GE) ▪ Register: 384 GE ▪ Sbox: 192 GE ▪ MC: 123 GE ▪ Logic: 166 GE ▪ Constants: 42 GE ▪ Key schedule (789 GE) ▪ Register: 768 GE ▪ Logic: 21 GE
Total: 1696 GE

SIMON-**64-128**
▪ Main register: 384 GE ▪ Key register: 768 GE ▪ Logic: 599 GE
Total: 1703 GE

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 ⇒ best throughput
- Long critical path ⇒ 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	966	-	1248	5.1	-
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
- SIMON can use regular flip-flops (4.67 GE)
- SKINNY has 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

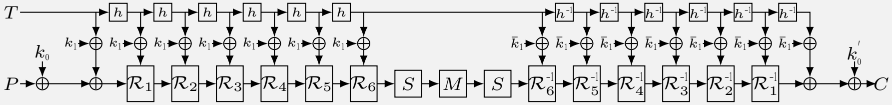
Plan

Low-Latency Variant of SKINNY: MANTIS

High-Level Description

- Low-latency block cipher similar to PRINCE... with a tweak!
- Put together **already-known components**:
  - PRINCE: α-reflection property: $\mathsf{Dec}_k(x) = \mathsf{Enc}_{k\oplus\alpha}(x)$
  - PRINCE: FX construction
  - MIDORI: low circuit-depth Sbox Sb_0
  - MIDORI: more general ShiftRows permutation
  - PRINCE: Suboptimal binary diffusion matrix (branching 4)
  - TWEAKEY: one-word tweakey schedule following STK construction

MANTIS



MANTIS: Main Features and Security Claims

Achievements

- Low-latency tweakable block cipher
- Main proposal: MANTIS_7 (total of 16 Sbox layers)
- Small hardware overhead in comparison to PRINCE (price of the tweak input and its security)

Security Claims for MANTIS_7

- Secret key and chosen tweaks: $126 - n$ bits of security for 2^n pairs of chosen plaintexts
- No security claimed for related keys: as in PRINCE, there exists a probability one related-key distinguisher
- Same claims as PRINCE, but also related-tweak security
- **Low-data claims:** No attacks against MANTIS_{5+} with less than 2^{30} chosen plaintexts or with less than 2^{40} known plaintexts

Application to Memory Encryption

Current Commercial Solutions

- SecureBlue++ (IBM) - No public documentation
- SGX (Intel) - Ciphertext expansion

Shortcomings and Design Challenges

- **Natural solution:** dedicated TBC in ECB mode
  - No initialization overhead
  - Tweak input is the memory address
- However, current solutions present drawbacks:
  - Very few TBC candidates
  - Generic TBC constructions are not an option (bad latency)
  - Known dedicated TBC: latency far from the best achievable in BC
  - Decryption overhead

MANTIS **Rationale: Choice of h**

TWEAKEY Permutation Selection

- Consider the subsest of 8! permutations of the type below
- Filter the TWEAKEY permutation candidates so that 16 Sboxes are active for 5 rounds for related tweaks (**RT**)
- Then, pick h that maximizes the bounds for MANTIS_r for $r \geq 6$
- This makes MANTIS_5 just at the 2^{-64} security bound
- Therefore: MANTIS_7 has 4 additional rounds

Bounds for MANTIS_r **(using MILP)**

	MANTIS_2	MANTIS_3	MANTIS_4	MANTIS_5	MANTIS_6	MANTIS_7	MANTIS_8
RT	6	12	20	**34**	44	50	56
Linear	14	32	46	62	70	76	82

0	1	2	3
4	5	6	7
8	9	10	11
12	13	14	15

$\xrightarrow{h}$

6	5	4	15
0	1	2	3
7	12	13	4
8	9	10	11

MANTIS: Unrolled Implementations

Minimizing Area (Enc+Dec)

	Area (GE)	Delay (ns)
MANTIS_5	8577	21.73
MANTIS_6	9861	22.83
MANTIS_7	11205	25.08
MANTIS_8	12546	27.22

Implementation for Shortest Delay (Enc+Dec)

	Area (GE)	Delay (ns)
MANTIS_5	13410	9.00
MANTIS_6	15256	10.50
MANTIS_7	16899	12.00
MANTIS_8	18586	13.50
PRINCE	22040	8.00

Plan

Conclusion

Paper, Specifications, Results and Updates available at:
https://sites.google.com/site/skinnycipher/
(will be available soon)

Figures of this talk will soon be available at:
https://www.iacr.org/authors/tikz/

Thank you for your attention!

Plan

Bibliography I

Subhadeep Banik, Andrey Bogdanov, Takanori Isobe, Kyoji Shibutani, Harunaga Hiwatari, Toru Akishita, and Francesco Regazzoni.
Midori: A Block Cipher for Low Energy.
LNCS, pages 411--436. Springer, December 2015.

Andrey Bogdanov, Lars R. Knudsen, Gregor Leander, Christof Paar, Axel Poschmann, Matthew J. B. Robshaw, Yannick Seurin, and C. Vikkelsoe.
PRESENT: An Ultra-Lightweight Block Cipher.
In Pascal Paillier and Ingrid Verbauwhede, editors, CHES 2007, volume 4727 of LNCS, pages 450--466. Springer, September 2007.

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.

Jian Guo, Thomas Peyrin, Axel Poschmann, and Matthew J. B. Robshaw.
The LED Block Cipher.
In Bart Preneel and Tsuyoshi Takagi, editors, CHES 2011, volume 6917 of LNCS, pages 326--341. Springer, September / October 2011.

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.

Tomoyasu Suzaki, Kazuhiko Minematsu, Sumio Morioka, and Eita Kobayashi.
TWINE: A Lightweight Block Cipher for Multiple Platforms.
In Lars R. Knudsen and Huapeng Wu, editors, SAC 2012, volume 7707 of LNCS, pages 339--354. Springer, August 2013.

Bibliography III

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.