

The background features a large, semi-transparent watermark of the National Technical University of Singapore (NTU) crest. The crest is a shield-shaped emblem containing a lion rampant, a gear, and two atomic symbols.

The Skinny Family of Tweakable Block Ciphers

Thomas Peyrin

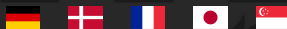
NTU - Singapore

ASK 2016

Nagoya, Japan - September 30, 2016

SKINNY website

C. Beierle, J. Jean, S. Kölbl, G. Leander, A. Moradi,
T. Peyrin, Y. Sasaki, P. Sasdrich and S.M. Sim
(CRYPTO 2016)



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

Any new cryptanalysis of SKINNY is welcome !

Outline

- 1 **The STK construction**
 - ▷ Block ciphers
 - ▷ The example of AES
 - ▷ TWEAKEY framework and the STK construction
- 2 **The Skinny tweakable block cipher**
- 3 **SKINNY security**
- 4 **SKINNY performances**
- 5 **Future works**

Outline

- ① **The STK construction**
 - ▷ Block ciphers
 - ▷ The example of AES
 - ▷ TWEAKEY framework and the STK construction
- ② The Skinny tweakable block cipher
- ③ SKINNY security
- ④ SKINNY performances
- ⑤ Future works

Outline

① The STK construction

- ▷ Block ciphers
- ▷ The example of AES
- ▷ TWEAKEY framework and the STK construction

② The Skinny tweakable block cipher

③ SKINNY security

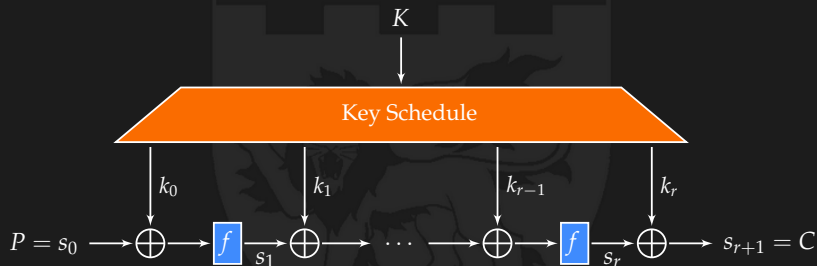
④ SKINNY performances

⑤ Future works

Iterated block ciphers

An iterated block cipher is composed of two parts :

- ▷ an **internal permutation** f repeated r times (also named round function)
- ▷ a **key schedule** that generates $r + 1$ subkeys $K \rightarrow (k_0, \dots, k_r)$



For a compression function, the key schedule is also named the message expansion

Iterated block ciphers

An iterated block cipher is composed of two parts :

- ▷ an **internal permutation** f repeated r times (also named round function)
- ▷ a **key schedule** that generates $r + 1$ subkeys $K \rightarrow (k_0, \dots, k_r)$



For a compression function, the key schedule is also named the message expansion

Permutations

We know how to design a good permutation :

▷ **Feistel network**

DES, SHA-2

▷ **Substitution-Permutation network (SPN)**

AES, Keccak (SHA-3)

Many recent primitives try to use only permutations to avoid the key schedule (sponge functions, Grøstl, LED)

Outline

① The STK construction

- ▷ Block ciphers
- ▷ The example of AES
- ▷ TWEAKEY framework and the STK construction

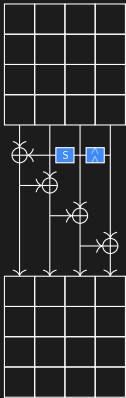
② The Skinny tweakable block cipher

③ SKINNY security

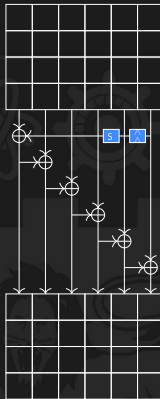
④ SKINNY performances

⑤ Future works

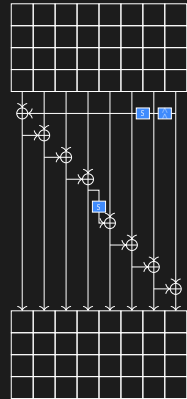
The AES key schedules



AES-128



AES-192

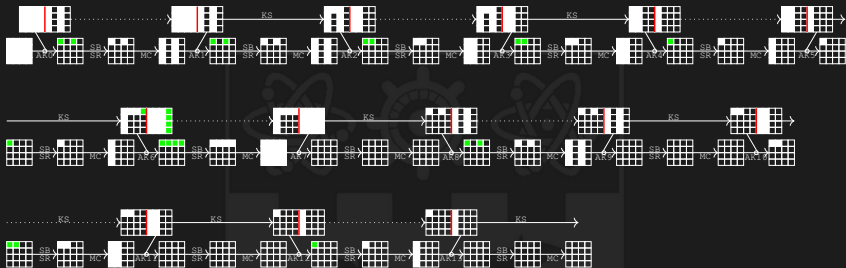


AES-256

Rationale :

- ▷ XORs for inter-column diffusion, shift for inter-row diffusion, Sbox for non-linearity, counter to break symmetries
- ▷ quite different from the AES round function

Security issues with the AES key schedule



Related-key attacks on the full AES-256 and AES-192

- ▷ existence of 2-round **local collision** paths [BKN09]
- ▷ 14-round path with only 24 active Sboxes (5 in the key schedule, 19 in the internal state)
- ▷ later improved in [BK09] using boomerang technique (since very good small differential paths exist) :
key recovery attack with $2^{99.5}$ time and data
- ▷ harder to attack AES-192 and so far no attack on AES-128

Proven bounds for AES-128

Single-key model

Rounds	1	2	3	4	5	6	7	8	9	10
min	1	5	9	25	26	30	34	50	51	55

Related-key model (truncated differences)

Rounds	1	2	3	4	5	6	7	8	9	10
min	0	1	3	9	11	13	15	21	23	25

Related-key model (actual differences)

Rounds	1	2	3	4	5	6	7	8	9	10
min	0	1	5	13	17	?	?	?	?	?

Outline

① The STK construction

- ▷ Block ciphers
- ▷ The example of AES
- ▷ TWEAKEY framework and the STK construction

② The Skinny tweakable block cipher

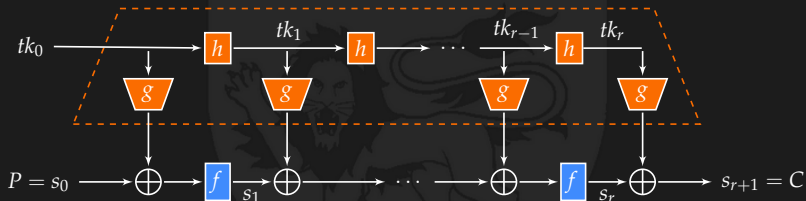
③ SKINNY security

④ SKINNY performances

⑤ Future works

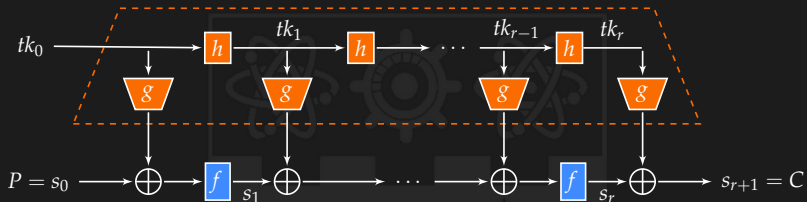
The TWEAKEY framework

The TWEAKEY framework rationale [ASIACRYPT'14]:
tweak and key should be treated the same way → **tweakey**



TWEAKEY generalizes the class of **key-alternating** ciphers

The TWEAKEY framework



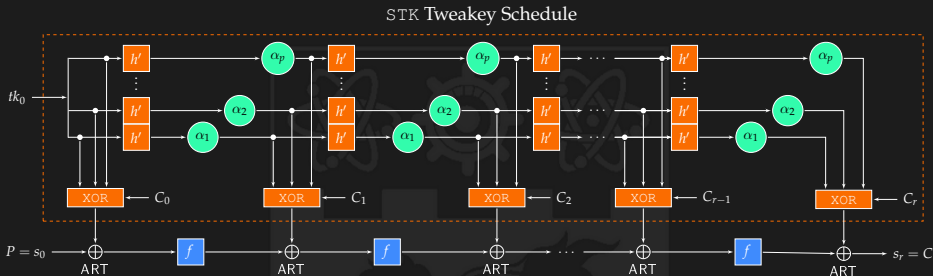
The main issue :

adding more tweakey state makes the security drop, or renders security hard to study, even for automated tools

Idea :

separate the tweakey material in several words, design a secure tweakey schedule for one word and then **superpose** them in a secure way

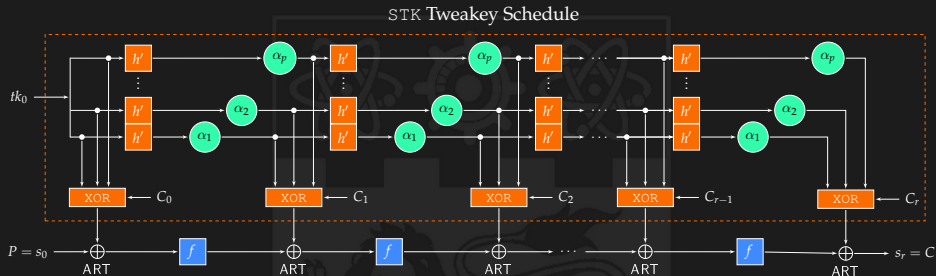
The STK construction (Superposition-TWEAKEY)



From the TWEAKEY framework to the STK construction :

- ▷ the tweakkey state update function h consists in the same subfunction h' applied to each tweakkey word
- ▷ the subtweakkey extraction function g consists in XORing all the words together
 - reduce the implementation overhead
 - reduce the area footprint by reusing code
 - **simplify the security analysis**

The STK construction (Superposition-TWEAKEY)



From the TWEAKEY framework to the STK construction :

- ▷ **problem** : **strong interaction** between the parallel branches of tweakey state
- ▷ **solution** : **differentiate** the parallel branches by simply using distinct small linear layers

Outline

- 1 **The STK construction**
 - ▷ Block ciphers
 - ▷ The example of AES
 - ▷ TWEAKEY framework and the STK construction
- 2 **The Skinny tweakable block cipher**
- 3 SKINNY security
- 4 SKINNY performances
- 5 Future works

SKINNY goals and results

Goals

- ▷ Provide an alternative to NSA-designed **SIMON** block cipher
- ▷ 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 (tweakable) block ciphers
- ▷ Block sizes n : 64 and 128 bits
- ▷ Various key+tweak sizes : n , $2n$ and $3n$ bits
- ▷ **Security guarantees** for differential/linear cryptanalysis (both single and related-key)
- ▷ **Efficient and competitive** software/hardware implementations
 - Round-based SKINNY-64-128 : **1696 GE** (SIMON : 1751 GE)
 - on Skylake (avx2) : **2.78 c/B** (SIMON : 1.81 c/B) for fixed-key

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
- ▷ Remove all operations not strictly necessary to security
- ▷ **Result : removing *any* operations from SKINNY results in an unsecure cipher**

SKINNY 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 tweakkey size can be n , $2n$ or $3n$.

Number of rounds

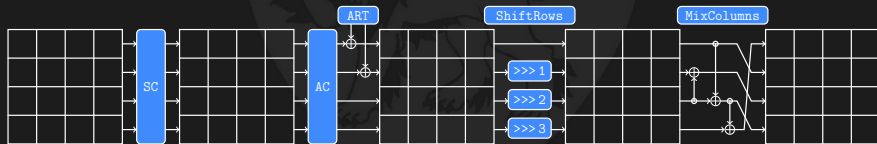
Block size n	Tweakkey size		
	n	$2n$	$3n$
64	32	36	40
128	40	48	56

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

SKINNY round function

AES-like round function

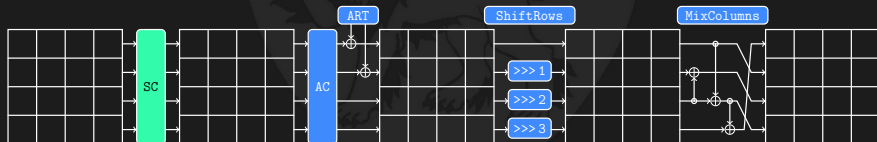
- ▷ **SubCells (SC)** : Application of a s -bit Sbox to all 16 cells
- ▷ **AddConstants (AC)** : Inject round constants in the state
- ▷ **AddRoundTweakey (ART)** : Extract and inject the subtweakeys to **half** the state
- ▷ **ShiftRows (SR)** : **Right**-rotate line i by i positions
- ▷ **MixColumns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



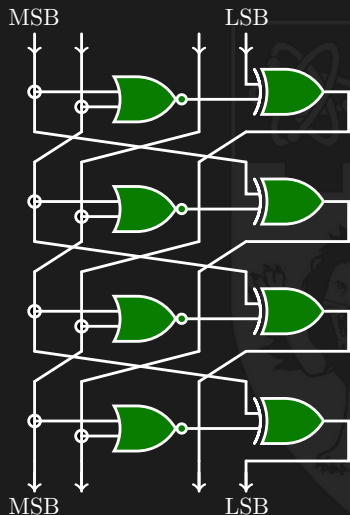
SKINNY round function

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



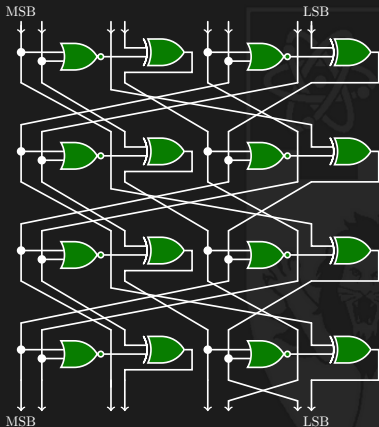
\mathcal{S}_4 : 4-bit Sbox for SKINNY-64-*

- ▷ Almost PICCOLO Sbox
- ▷ 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

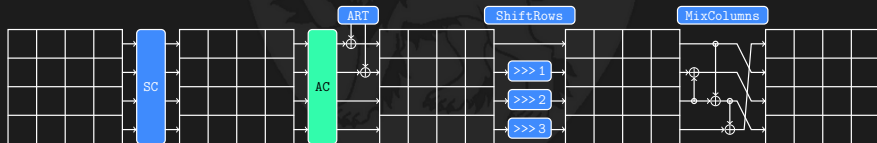
Properties

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

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 constants addition

We update the constant state with a **cheap LFSR** :

$$(rc_5 || rc_4 || rc_3 || rc_2 || rc_1 || rc_0) \rightarrow (rc_4 || rc_3 || rc_2 || rc_1 || rc_0 || rc_5 \oplus rc_4 \oplus 1)$$

We XOR the following constant matrix to the state :

$$\begin{bmatrix} c_0 & 0 & 0 & 0 \\ c_1 & 0 & 0 & 0 \\ c_2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} \quad \begin{aligned} c_0 &= (rc_3 || rc_2 || rc_1 || rc_0) \\ c_1 &= (0 || 0 || rc_5 || rc_4) \\ c_2 &= 0_{x2} \end{aligned}$$

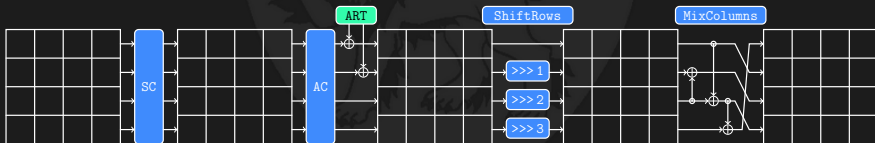
Criterion for the choice of constants :

- ▷ placement of c_0 , c_1 and c_2 has been chosen to maximise the constants diffusion after application of forward/backward linear layer
- ▷ prevent spreading of symmetries, fixed points and more generally subspaces

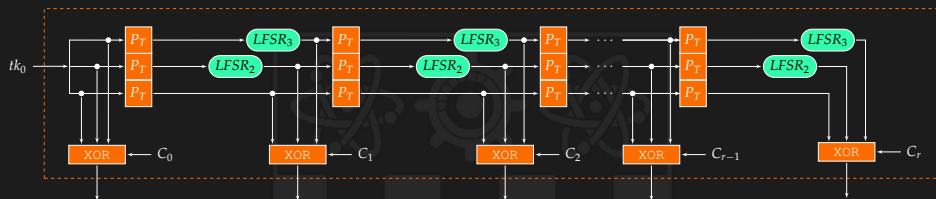
SKINNY round function

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



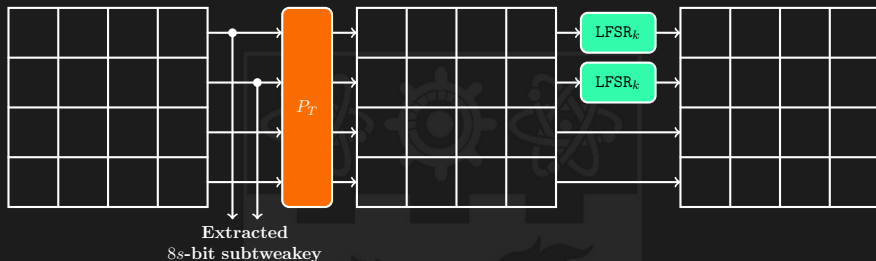
The SKINNY tweakey schedule



In details :

- ▷ P_T will simply be a permutation of the nibbles positions :
 $P_T = [9, 15, 8, 13, 10, 14, 12, 11, 0, 1, 2, 3, 4, 5, 6, 7]$
- ▷ nibbles in the top two rows of the k -th tweakey word are updated with $LFSR_k$
- ▷ no whitening key
- ▷ very simple transformations : linear and lightweight

The SKINNY tweakey schedule



In details :

- ▷ P_T will simply be a **permutation of the nibbles positions** :
 $P_T = [9, 15, 8, 13, 10, 14, 12, 11, 0, 1, 2, 3, 4, 5, 6, 7]$
- ▷ nibbles in the **top two rows** of the k -th tweakey word are updated with $LFSR_k$
- ▷ **no whitening key**
- ▷ very simple transformations : **linear and lightweight**

The permutations P_T in SKINNY tweakey schedule

$$P_T = [9, 15, 8, 13, 10, 14, 12, 11, 0, 1, 2, 3, 4, 5, 6, 7]$$

Criterion for the choice of permutation P_T :

- ▷ maximize the bounds on the number of active Sboxes in the related-tweakey model
- ▷ both halves of the tweakey states will be equally mixed to the cipher internal state
- ▷ P_T consist of a single cycle
- ▷ subtweakeys size is only half of the cipher internal state size to save XOR gates

The LFSRs in SKINNY tweakey schedule

s	TK	LFSR
4	TK2	$(x_3 x_2 x_1 x_0) \rightarrow (x_2 x_1 x_0 x_3 \oplus x_2)$
	TK3	$(x_3 x_2 x_1 x_0) \rightarrow (x_0 \oplus x_3 x_3 x_2 x_1)$
8	TK2	$(x_7 x_6 x_5 x_4 x_3 x_2 x_1 x_0) \rightarrow$ $(x_6 x_5 x_4 x_3 x_2 x_1 x_0 x_7 \oplus x_5)$
	TK3	$(x_7 x_6 x_5 x_4 x_3 x_2 x_1 x_0) \rightarrow$ $(x_0 \oplus x_6 x_7 x_6 x_5 x_4 x_3 x_2 x_1)$

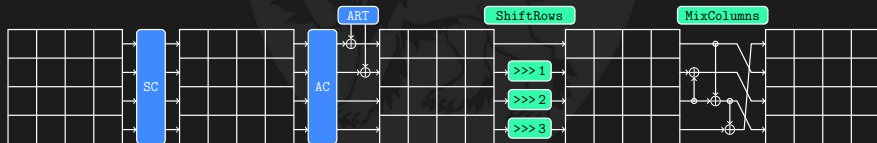
Criterion for the choice of LFSRs :

- ▷ for a given cell position, a single **cancellation can only happen every 30 rounds** for TK2, same with two cancellations for TK3
- ▷ cheapest possible LFSRs choice

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 linear diffusion layer

Best candidate found :

apply right-shiftrows and multiply each 4-bit slice with matrix :

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

Criterion for the choice of linear diffusion layer :

- ▷ **cheap cheap cheap** : at most 3 XORs
- ▷ M has branching number 2, but good differential paths avoided by a careful choice of M
- ▷ **maximize the bounds on the number of active Sboxes in the single and related-tweakey model**
- ▷ fast diffusion (6 rounds forward and backward) and fast tweakey diffusion (only one round forward and backward)

Outline

- 1 **The STK construction**
 - ▷ Block ciphers
 - ▷ The example of AES
 - ▷ TWEAKEY framework and the STK construction
- 2 **The Skinny tweakable block cipher**
- 3 **SKINNY security**
- 4 **SKINNY performances**
- 5 **Future works**

Overview of SKINNY security

Claims

- ▷ Security against known classes of attacks
- ▷ Security in the **related-key model**
- ▷ No guarantees for known or chosen key
- ▷ No claim for related-cipher security
(the constants do not encode the cipher parameters)

Attack vectors considered

- ▷ **Differential/Linear cryptanalysis**
- ▷ Integral attack
- ▷ Division property
- ▷ Meet-in-the-middle attack
- ▷ Impossible differential attack
- ▷ Invariant subspace attack
- ▷ Slide attack
- ▷ Algebraic attack

Comparing differential/linear bounds

- ▷ 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 has 40/48/56 rounds
- ▷ As a result, for all SKINNY variants :
 - **SK** security reached in 20 – 40% of the rounds
 - **TK2** security reached in 40 – 50% 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%

Outline

- ① **The STK construction**
 - ▷ Block ciphers
 - ▷ The example of AES
 - ▷ TWEAKEY framework and the STK construction
- ② **The Skinny tweakable block cipher**
- ③ **SKINNY security**
- ④ **SKINNY performances**
- ⑤ **Future works**

Theoretical performances of SKINNY

Cipher	Rounds	#operations per bit		Round-based area estimation
		without KS	with KS	
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)

- ▷ $1R : (4 \text{ NOR} + 4 \text{ XOR})/4 \text{ [SB]} + (3 \text{ XOR})/4 \text{ [MC]} + (32 \text{ XOR})/64 \text{ [ART]}$
- ▷ That is (per bit per round) : $1 \text{ NOR} + 2.25 \text{ XOR}$
- ▷ #operations per bit (without KS) : $(1 + 2.25) \times 36 = 117$
- ▷ **Very low number of operations per plaintext bit**
- ▷ **Challenge : do better**

Round-based ASIC implementation results

	Area	Delay	Through. @100KHz	Through. @max
	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-64-128	3036	-	133.0	-
PRESENT-64-128	1884	-	200.00	-
PICCOLO-64-128	1773	-	193.94	-

Round-based ASIC implementation results

	Area	Delay	Through. @100KHz	Through. @max
	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-64-128	3036	-	133.0	-
PRESENT-64-128	1884	-	200.00	-
PICCOLO-64-128	1773	-	193.94	-

Outline

- ① **The STK construction**
 - ▷ Block ciphers
 - ▷ The example of AES
 - ▷ TWEAKEY framework and the STK construction
- ② **The Skinny tweakable block cipher**
- ③ **SKINNY security**
- ④ **SKINNY performances**
- ⑤ **Future works**

SKINNY for Authenticated Encryption ?

Plug SKINNY-128-128 in the Deoxys nonce-respecting AE mode

- ▷ similar to TAE or OCB3
- ▷ full 128-bit (not birthday) security, independent of #data
- ▷ no long initialization required : fast for short inputs
- ▷ only $m + 1$ calls for m message blocks : fast for short inputs

Performance estimations of serial implementations

- ▷ computed serially, the main extra cost of the mode comes from the counter and checksum states
(about $(128 + 32) * 6GE = 960 GE$)
- ▷ SKINNY-128-128 can fit it 1481 GE, thus we can hope for a serial implementation of about 2500 GE
(throughput about 19 Mbit/s)

SKINNY for Authenticated Encryption ?

Plug SKINNY-128-128 in the Deoxys nonce-respecting AE mode

- ▷ similar to TAE or OCB3
- ▷ full 128-bit (not birthday) security, independent of #data
- ▷ no long initialization required : fast for short inputs
- ▷ only $m + 1$ calls for m message blocks : fast for short inputs

Performance estimations of round-based implementations

- ▷ computed round-based, the main extra cost of the mode comes from the counter and checksum states
(about $(128 + 32) * (6GE + 2.67GE) = 1387$ GE)
- ▷ SKINNY-128-128 can fit it 2391 GE, thus we can hope for a round-based implementation of about 3800 GE
(throughput about 1100 Mbit/s)

SKINNY for Authenticated Encryption ?

Plug SKINNY-128-128 in the Deoxys nonce-respecting AE mode

- ▷ similar to TAE or OCB3
- ▷ full 128-bit (not birthday) security, independent of #data
- ▷ no long initialization required : fast for short inputs
- ▷ only $m + 1$ calls for m message blocks : fast for short inputs

SKINNY would be a good lightweight candidate for the CAESAR competition (with good software speed, about $3c/B$)

Open problems for SKINNY

Open problems for SKINNY

- ▷ tighter bounds for SKINNY ?
- ▷ other proofs for SKINNY ?
(MitM, impossible differential, etc.)
- ▷ improved cryptanalysis ?

The SKINNY cryptanalysis competition

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

SKINNY has several versions :

- ▷ SKINNY-64-128 has **36** rounds
- ▷ SKINNY-128-128 has **40** rounds

The SKINNY cryptanalysis competition

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

SKINNY has several versions :

- ▷ SKINNY-64-128 has **36** rounds
... current best attack reaches **18** rounds only
- ▷ SKINNY-128-128 has **40** rounds
... current best attack reaches **18** rounds only

The SKINNY cryptanalysis competition

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

SKINNY has several versions :

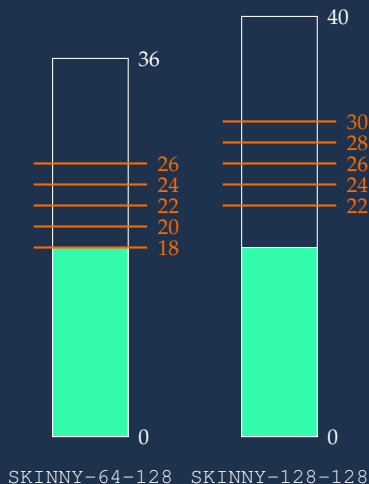
- ▷ SKINNY-64-128 has **36** rounds
... current best attack reaches **18** rounds only
- ▷ SKINNY-128-128 has **40** rounds
... current best attack reaches **18** rounds only

To motivate further cryptanalysis on SKINNY, we propose several (**very**) **reduced versions** for a cryptanalysis competition

The SKINNY competition categories






We propose **5 categories**, best cryptanalysis for :

- ① 26 rounds of SKINNY-64-128 or
30 rounds of SKINNY-128-128
- ② 24 rounds of SKINNY-64-128 or
28 rounds of SKINNY-128-128
- ③ 22 rounds of SKINNY-64-128 or
26 rounds of SKINNY-128-128
- ④ 20 rounds of SKINNY-64-128 or
24 rounds of SKINNY-128-128
- ⑤ 18 rounds of SKINNY-64-128 or
22 rounds of SKINNY-128-128



The SKINNY competition categories

We propose **5 categories**, best cryptanalysis for :

- 1 26 rounds of SKINNY-64-128 or
30 rounds of SKINNY-128-128
gets **5 presents** (one from each country :     )
- 2 24 rounds of SKINNY-64-128 or
28 rounds of SKINNY-128-128
gets **4 presents** from 4 different countries (chosen by the winner)
- 3 22 rounds of SKINNY-64-128 or
26 rounds of SKINNY-128-128
gets **3 presents** from 3 different countries (chosen by the winner)
- 4 20 rounds of SKINNY-64-128 or
24 rounds of SKINNY-128-128
gets **2 presents** from 2 different countries (chosen by the winner)
- 5 18 rounds of SKINNY-64-128 or
22 rounds of SKINNY-128-128
gets **1 present** (country chosen by the winner)

The SKINNY competition rules

- ▷ **the SKINNY designers will judge the best attack submitted after the deadline**, but main criterion will be : final complexity (computations, data and memory), application to other SKINNY versions, novelty, attack model, etc.
- ▷ **types of attacks :**
 - single-key and related-key attacks qualify for the competition
 - we will decide separately if accelerated brute force (e.g. biclique attacks) qualifies for the competition
 - related-cipher attacks do not qualify for the competition
 - tweak is allowed for of up to 64 bits for SKINNY-64-128 (but in that case, security bound is 2^k where k is the key size)
- ▷ attacks from the SKINNY document count as already existing attacks
- ▷ if some attacks are similar, the first submitted has priority

The SKINNY competition rules

- ▷ **the SKINNY designers will judge the best attack submitted after the deadline**, but main criterion will be : final complexity (computations, data and memory), application to other SKINNY versions, novelty, attack model, etc.
- ▷ **types of attacks :**
 - single-key and related-key attacks qualify for the competition
 - we will decide separately if accelerated brute force (e.g. biclique attacks) qualifies for the competition
 - related-cipher attacks do not qualify for the competition
 - tweak is allowed for of up to 64 bits for SKINNY-64-128 (but in that case, security bound is 2^k where k is the key size)
- ▷ attacks from the SKINNY document count as already existing attacks
- ▷ if some attacks are similar, the first submitted has priority
- ▷ gov. agencies **can** participate to the competition (please send us your full address for prizes delivery)

Submitting to the SKINNY competition

When :

- ▷ **start** : now !
- ▷ **end** : deadline for submission **1st of March 2017**

Attacks are to be submitted to skinny@googlegroups.com
(state in the submission from which countries you want the gift)



Thank you!

