The Skinny competition

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

NTU - Singapore

FSE 2017 rump session

Tokyo, Japan - March 7, 2017

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 !**

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
- ▷ 64 or 128-bit block, various tweakey 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 : 1539 GE (SIMON : 1751 GE)
  - ○ on Skylake (avx2) : 2.78 c/B (SIMON : 1.81 c/B) for fixed-key

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 :

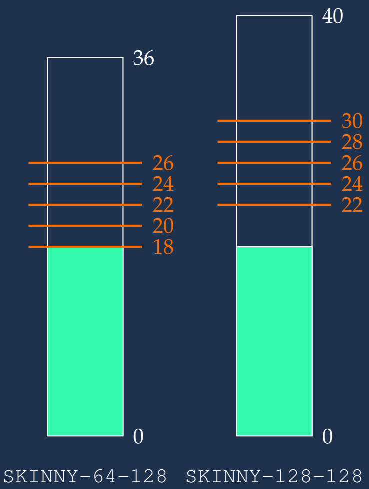
- ▷ SKINNY-64-128 has **36** rounds
- ▷ SKINNY-128-128 has **40** rounds

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

The SKINNY competition categories

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

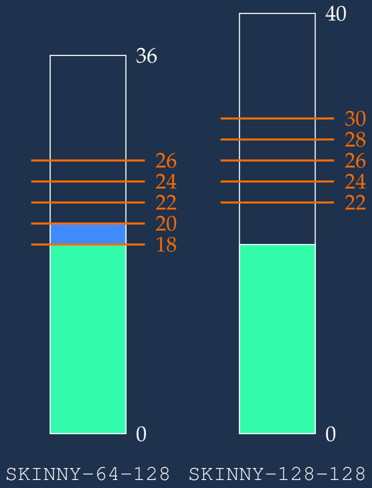
1. 26 rounds of SKINNY-64-128 or
   30 rounds of SKINNY-128-128
2. 24 rounds of SKINNY-64-128 or
   28 rounds of SKINNY-128-128
3. 22 rounds of SKINNY-64-128 or
   26 rounds of SKINNY-128-128
4. 20 rounds of SKINNY-64-128 or
   24 rounds of SKINNY-128-128
5. 18 rounds of SKINNY-64-128 or
   22 rounds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



The SKINNY competition categories

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

- *Related-Key Impossible-Differential Attack on Reduced-Round SKINNY* by R. Ankele, S. Banik, A. Chakraborti, E. List, F. Mendel, S.M. Sim and G. Wang

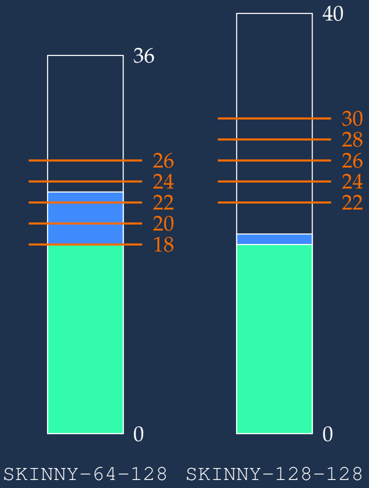


The SKINNY competition categories

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

- *Related-Key Impossible-Differential Attack on Reduced-Round SKINNY* by R. Ankele, S. Banik, A. Chakraborti, E. List, F. Mendel, S.M. Sim and G. Wang

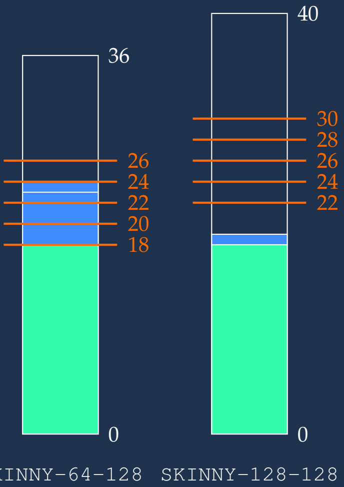
- *Security Analysis of SKINNY under Related-Tweakey Settings* by G. Liu, M. Ghosh and L. Song



The SKINNY competition categories

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

- *Related-Key Impossible-Differential Attack on Reduced-Round SKINNY* by R. Ankele, S. Banik, A. Chakraborti, E. List, F. Mendel, S.M. Sim and G. Wang
- *Security Analysis of SKINNY under Related-Tweakey Settings* by G. Liu, M. Ghosh and L. Song
- *Cryptanalysis of Reduced round SKINNY Block Cipher* by S. Sadeghi, T. Mohammadi, and N. Bagheri



The winners

1+2= 3 gifts *Related-Key Impossible-Differential Attack on Reduced-Round SKINNY* by R. Ankele, S. Banik, A. Chakraborti, E. List, F. Mendel, S.M. Sim and G. Wang

3 gifts *Security Analysis of SKINNY under Related-Tweakey Settings* by G. Liu, M. Ghosh and L. Song

4 gifts *Cryptanalysis of Reduced round SKINNY Block Cipher* by S. Sadeghi, T. Mohammadi, and N. Bagheri

Comparing Simon, Skinny and others

Ratio of rounds required for Diff/Lin resistance

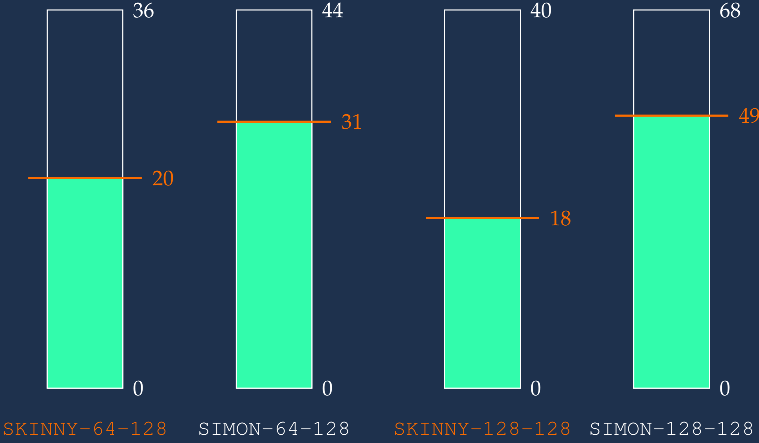
Cipher	Single Key (SK)	Related Key (RK)
SKINNY-64-128	8/36 = 22%	15/36 = 42%
SIMON-64-128	19/44 = 43%	no bound known
SKINNY-128-128	15/40 = 37%	19/40 = 47%
SIMON-128-128	37/68 = 54%	no bound known
AES-128	4/10 = 40%	6/10 = 60%

Ratio of attacked rounds

Cipher	Single Key (SK)	Related Key (RK)
SKINNY-64-128	20/36 = 55%	24/36 = 66%
SIMON-64-128	31/44 = 70%	? $\geq$ 70%
SKINNY-128-128	18/40 = 45%	21/40 = 52%
SIMON-128-128	49/68 = 72%	? $\geq$ 72%
AES-128	7/10 = 70%	7/10 = 70%

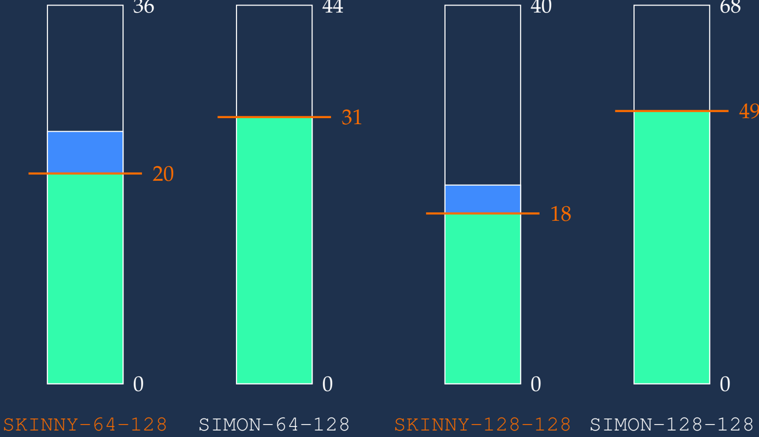
Comparing Simon and Skinny (single-key)

Ratio of attacked rounds (single-key)



Comparing Simon and Skinny (related-key)

Ratio of attacked rounds (related-key)

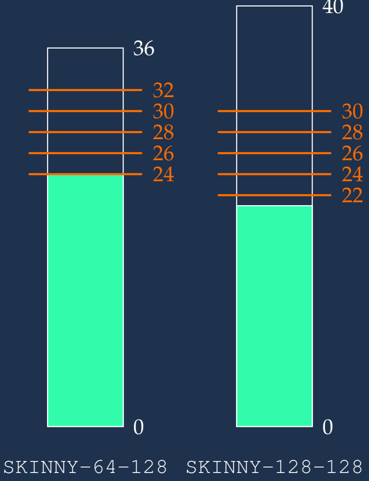


The Skinny 17/18 competition

The SKINNY competition 17/18 categories

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

1. 32 rounds of SKINNY-64-128 or
   30 rounds of SKINNY-128-128
2. 30 rounds of SKINNY-64-128 or
   28 rounds of SKINNY-128-128
3. 28 rounds of SKINNY-64-128 or
   26 rounds of SKINNY-128-128
4. 26 rounds of SKINNY-64-128 or
   24 rounds of SKINNY-128-128
5. 24 rounds of SKINNY-64-128 or
   22 rounds of SKINNY-128-128



The SKINNY competition 17/18 categories

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

1. 32 rounds of `SKINNY-64-128` or
   30 rounds of `SKINNY-128-128`
   gets **5 presents** (one from each country : 🇩🇪 🇩🇰 🇫🇷 🇯🇵 🇸🇬)
2. 30 rounds of `SKINNY-64-128` or
   28 rounds of `SKINNY-128-128`
   gets **4 presents** from 4 different countries (chosen by the winner)
3. 28 rounds of `SKINNY-64-128` or
   26 rounds of `SKINNY-128-128`
   gets **3 presents** from 3 different countries (chosen by the winner)
4. 26 rounds of `SKINNY-64-128` or
   24 rounds of `SKINNY-128-128`
   gets **2 presents** from 2 different countries (chosen by the winner)
5. 24 rounds of `SKINNY-64-128` or
   22 rounds of `SKINNY-128-128`
   gets **1 present** (country chosen by the winner)

The SKINNY competition 17/18 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
- winners to be announced / gifts to be given during FSE'18

Submitting to the `SKINNY` competition

When :

- **start :** now !
- **end :** deadline for submission **1st of February 2018**

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

Thank you !