Announcing the SKINNY cryptanalysis competition

Thomas Peyrin

NTU - Singapore

ASK 2016

Nagoya, Japan - September 28, 2016

A new family of lightweight tweakable block ciphers

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 !

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 :

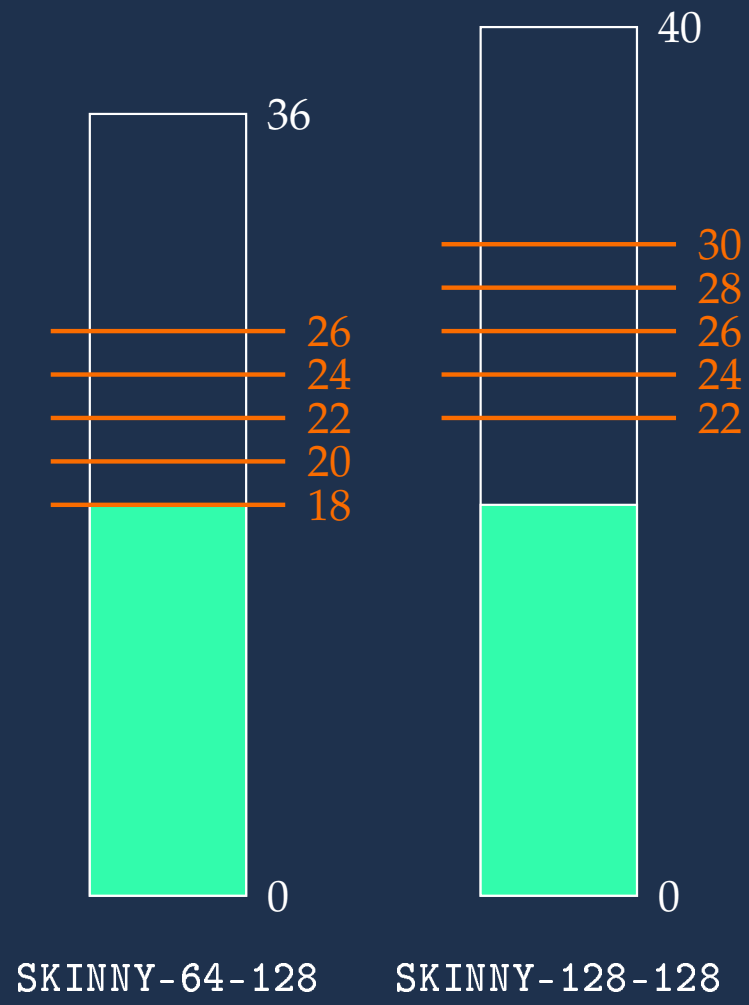
- SKINNY-64-128 has **36** rounds
  ... current best attack reaches **18** rounds only
- SKINNY-128-128 has **40** rounds
  ... current best attack reaches **18** rounds only

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)