NTT

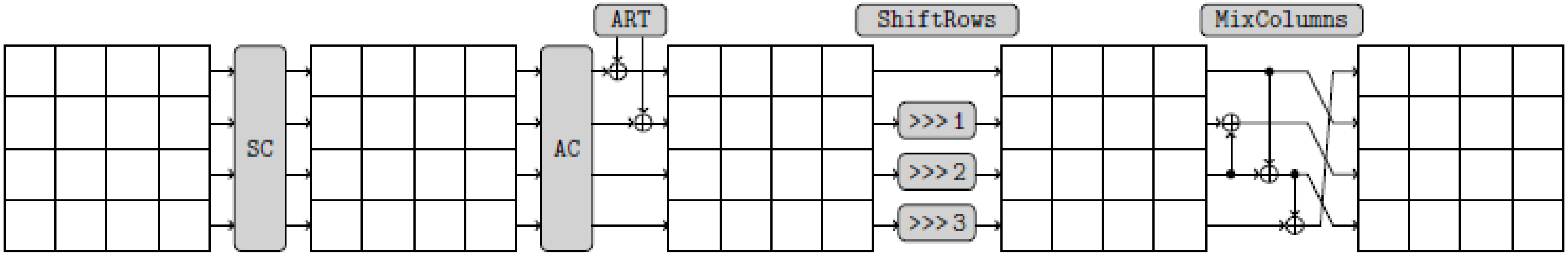
Innovative R&D by NTT

3rd SKINNY Breaking Competition

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

Eurocrypt 2018 Rump Session@ Tel Aviv 01/May/2018

SKINNY Overview



- Lightweight tweakable block cipher
- 64 or 128-bit block, various tweakey sizes: n, $2n$, and $3n$ bits
- Aiming an alternative of SIMON (designed by NSA)
- Perform and share full security analysis: guarantee against differential/linear cryptanalysis (both single and related-key)

Paper, Specifications, Results and Updates are available at :

https://sites.google.com/site/skinnycipher/

Previous Competition

2016-2017 competition

- **Goal**: attack 18 rounds or more for SKINNY-64-128
- **Result**: The winner attacked 23 rounds

Previous Competition

2016-2017 competition

Goal: attack 18 rounds or more for SKINNY-64-128

Result: The winner attacked 23 rounds

2017-2018 competition

Goal: attack 24 rounds or more for SKINNY-64-128

Result:

Previous Competition

2016-2017 competition

Goal: attack 18 rounds or more for SKINNY-64-128

Result: The winner attacked 23 rounds

2017-2018 competition

Goal: attack 24 rounds or more for SKINNY-64-128

Result: No winner

Previous Competition

2016-2017 competition

Goal: attack 18 rounds or more for SKINNY-64-128

Result: The winner attacked 23 rounds

2017-2018 competition

Goal: attack 24 rounds or more for SKINNY-64-128

Result: No winner

2018-2019 competition

Previous Competition

2016-2017 competition

Goal: attack 18 rounds or more for SKINNY-64-128

Result: The winner attacked 23 rounds

2017-2018 competition

Goal: attack 24 rounds or more for SKINNY-64-128

Result: No winner

2018-2019 competition

low data & **practical complexity**

New Direction of the Competition

Rules

We give sets of 2^{20} plaintext-ciphertexts encrypted under a 128-bit key for

- Skinny-64-128 reduced to r rounds, $4 \leq r \leq 18$
- Skinny-128-128 reduced to r rounds, $4 \leq r \leq 20$

Your goal is to recover the secret key.

Deadline: *Feb 2019*

You can find a C code to read the challenge file in the correct format and to verify your results.

Award for Competition 2017-2018

Award Categories

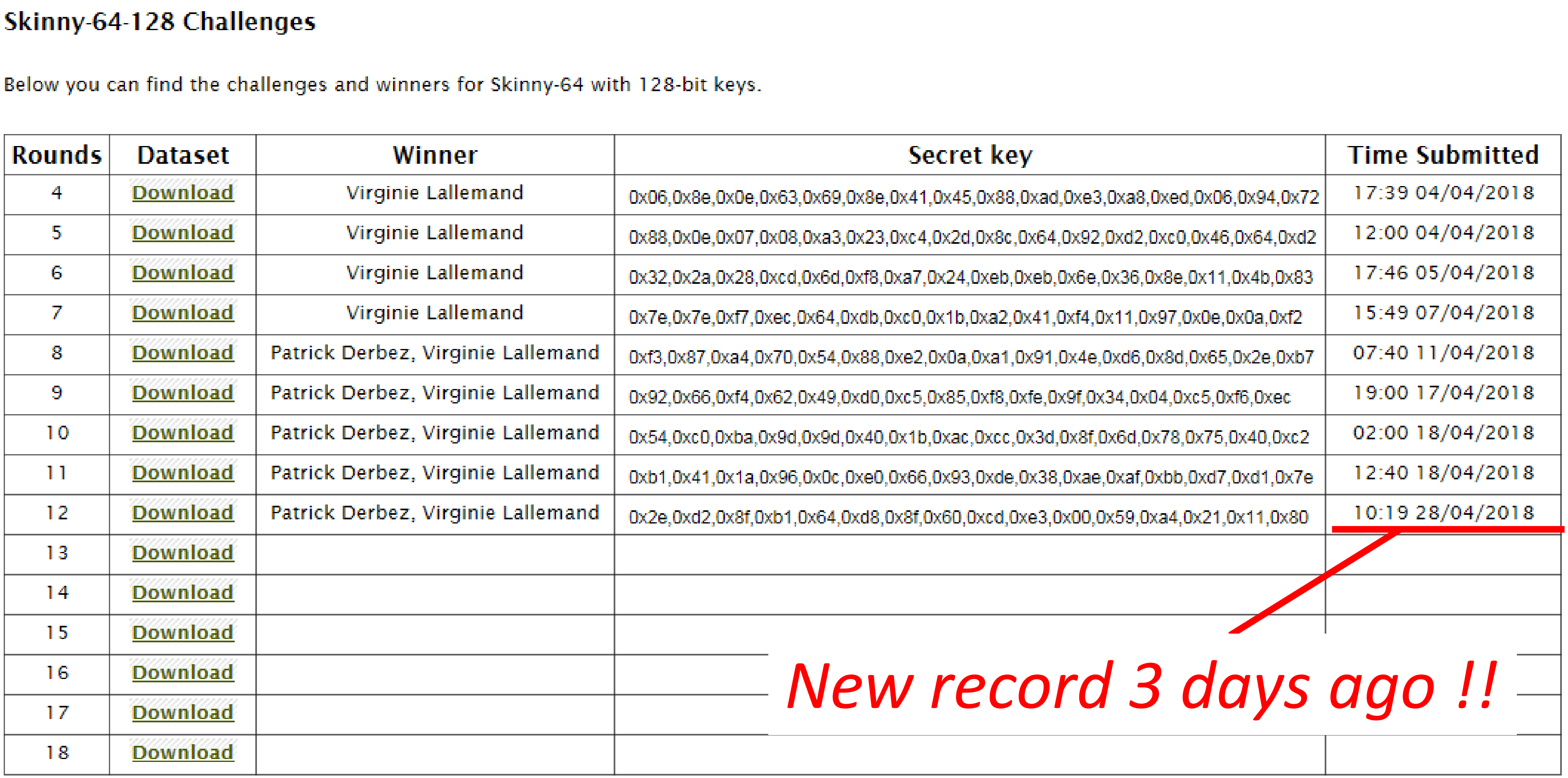
- Number of attacked rounds for Skinny-64-128
- Number of attacked rounds for Skinny-128-128
- Most interesting cryptanalysis

We will award with prizes from the designers home countries

Possible/Impossible Approaches

- No Chosen-Plaintext Attack
  - No differential cryptanalysis
  - No impossible differential cryptanalysis
  - No (amplified)boomerang/rectangle attacks
  - No integral attacks
  - No cube attacks
- Known Plaintext Attacks
  - Linear cryptanalysis
  - (classical) Meet-in-the-Middle attacks

Current Status for SKINNY-64-128



Skinny-64-128 Challenges

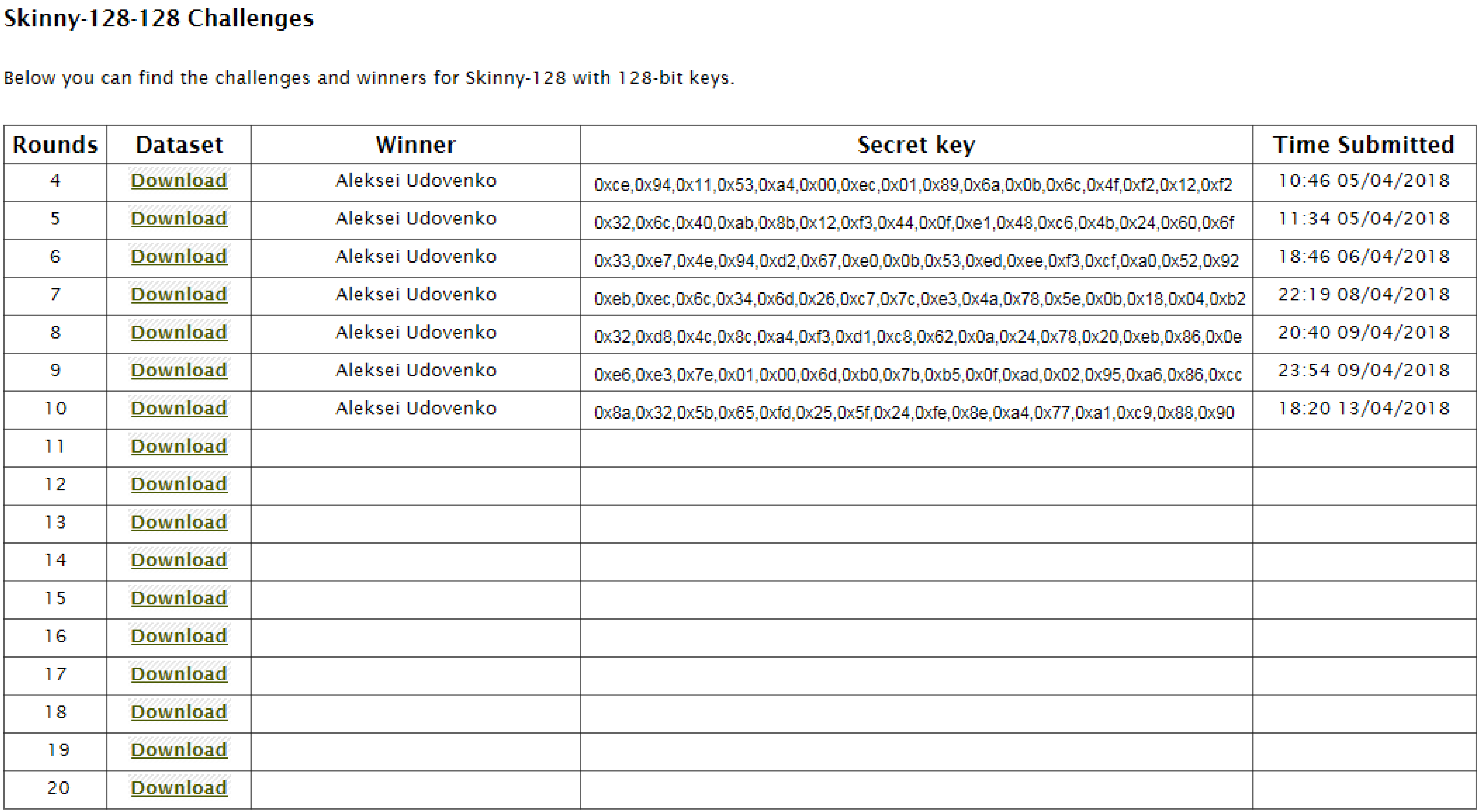
Below you can find the challenges and winners for Skinny-64 with 128-bit keys.

Rounds	Dataset	Winner	Secret key	Time Submitted
4	Download	Virginie Lallemand	0x06,0x8e,0x0e,0x63,0x69,0x8e,0x41,0x45,0x88,0xad,0xe3,0xa8,0xed,0x06,0x94,0x72	17:39 04/04/2018
5	Download	Virginie Lallemand	0x88,0x0e,0x07,0x08,0xa3,0x23,0xc4,0x2d,0x8c,0x64,0x92,0xd2,0xc0,0x46,0x64,0xd2	12:00 04/04/2018
6	Download	Virginie Lallemand	0x32,0x2a,0x28,0xcd,0x6d,0xf8,0xa7,0x24,0xeb,0xeb,0x6e,0x36,0x8e,0x11,0x4b,0x83	17:46 05/04/2018
7	Download	Virginie Lallemand	0x7e,0x7e,0xf7,0xec,0x64,0xdb,0xc0,0x1b,0xa2,0x41,0xf4,0x11,0x97,0x0e,0x0a,0xf2	15:49 07/04/2018
8	Download	Patrick Derbez, Virginie Lallemand	0xf3,0x87,0xa4,0x70,0x54,0x88,0xe2,0x0a,0xa1,0x91,0x4e,0xd6,0x8d,0x65,0x2e,0xb7	07:40 11/04/2018
9	Download	Patrick Derbez, Virginie Lallemand	0x92,0x66,0xf4,0x62,0x49,0xd0,0xc5,0x85,0xf8,0xfe,0x9f,0x34,0x04,0xc5,0xf6,0xec	19:00 17/04/2018
10	Download	Patrick Derbez, Virginie Lallemand	0x54,0xc0,0xba,0x9d,0x9d,0x40,0x1b,0xac,0xcc,0x3d,0x8f,0x6d,0x78,0x75,0x40,0xc2	02:00 18/04/2018
11	Download	Patrick Derbez, Virginie Lallemand	0xb1,0x41,0x1a,0x96,0x0c,0xe0,0x66,0x93,0xde,0x38,0xae,0xaf,0xbb,0xd7,0xd1,0x7e	12:40 18/04/2018
12	Download	Patrick Derbez, Virginie Lallemand	0x2e,0xd2,0x8f,0xb1,0x64,0xd8,0x8f,0x60,0xcd,0xe3,0x00,0x59,0xa4,0x21,0x11,0x80	10:19 28/04/2018
13	Download			
14	Download			
15	Download			
16	Download			
17	Download			
18	Download			

New record 3 days ago !!

https://sites.google.com/site/skinnycipher/

Current Status for SKINNY-128-128



Skinny-128-128 Challenges

Below you can find the challenges and winners for Skinny-128 with 128-bit keys.

Rounds	Dataset	Winner	Secret key	Time Submitted
4	Download	Aleksei Udovenko	0xce,0x94,0x11,0x53,0xa4,0x00,0xec,0x01,0x89,0x6a,0x0b,0x6c,0x4f,0xf2,0x12,0xf2	10:46 05/04/2018
5	Download	Aleksei Udovenko	0x32,0x6c,0x40,0xab,0x8b,0x12,0xf3,0x44,0x0f,0xe1,0x48,0xc6,0x4b,0x24,0x60,0x6f	11:34 05/04/2018
6	Download	Aleksei Udovenko	0x33,0xe7,0x4e,0x94,0xd2,0x67,0xe0,0x0b,0x53,0xed,0xee,0xf3,0xcf,0xa0,0x52,0x92	18:46 06/04/2018
7	Download	Aleksei Udovenko	0xeb,0xec,0x6c,0x34,0x6d,0x26,0xc7,0x7c,0xe3,0x4a,0x78,0x5e,0x0b,0x18,0x04,0xb2	22:19 08/04/2018
8	Download	Aleksei Udovenko	0x32,0xd8,0x4c,0x8c,0xa4,0xf3,0xd1,0xc8,0x62,0x0a,0x24,0x78,0x20,0xeb,0x86,0x0e	20:40 09/04/2018
9	Download	Aleksei Udovenko	0xe6,0xe3,0x7e,0x01,0x00,0x6d,0xb0,0x7b,0xb5,0x0f,0xad,0x02,0x95,0xa6,0x86,0xcc	23:54 09/04/2018
10	Download	Aleksei Udovenko	0x8a,0x32,0x5b,0x65,0xfd,0x25,0x5f,0x24,0xfe,0x8e,0xa4,0x77,0xa1,0xc9,0x88,0x90	18:20 13/04/2018
11	Download			
12	Download			
13	Download			
14	Download			
15	Download			
16	Download			
17	Download			
18	Download			
19	Download			
20	Download			

https://sites.google.com/site/skinnycipher/

Summary

- Competition is actively studied.

Summary

- Competition is actively studied.

Join the competition!!

Summary

- Competition is actively studied.

  Join the competition!!

- We have not yet received any submission for most interesting cryptanalysis award.

Summary

- Competition is actively studied.

Join the competition!!

- We have not yet received any submission for most interesting cryptanalysis award.

We do not know how they got broken.

Summary

- Competition is actively studied.

  Join the competition!!

- We have not yet received any submission for most interesting cryptanalysis award.

  We do not know how they got broken.

- Most interesting cryptanalysis prize can be won by any teams, not necessary be first to break the particular round.

Summary

- Competition is actively studied.

Join the competition!!

- We have not yet received any submission for most interesting cryptanalysis award.

We do not know how they got broken.

- Most interesting cryptanalysis prize can be won by any teams, not necessary be first to break the particular round.

Join the competition from 4-round attacks!!