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.

<table>
<thead>
<tr>
<th>Rounds</th>
<th>Dataset</th>
<th>Winner</th>
<th>Secret key</th>
<th>Time Submitted</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>Download</td>
<td>Virginie Lallemand</td>
<td>0x06,0x8e,0x0e,0x63,0x69,0x8e,0x41,0x45,0x88,0xad,0xe3,0xa8,0xed,0x06,0x94,0x72</td>
<td>17:39 04/04/2018</td>
</tr>
<tr>
<td>5</td>
<td>Download</td>
<td>Virginie Lallemand</td>
<td>0x88,0x0e,0x07,0x08,0xa3,0x23,0xc4,0x2d,0x8c,0x64,0x92,0xd2,0x00,0x46,0x64,0xd2</td>
<td>12:00 04/04/2018</td>
</tr>
<tr>
<td>6</td>
<td>Download</td>
<td>Virginie Lallemand</td>
<td>0x32,0x2a,0x23,0xcd,0x6d,0xf8,0xa7,0x24,0xeb,0xeb,0x6e,0x36,0x8e,0x11,0x4b,0x83</td>
<td>17:46 05/04/2018</td>
</tr>
<tr>
<td>7</td>
<td>Download</td>
<td>Virginie Lallemand</td>
<td>0x7e,0x7e,0xf7,0xec,0x64,0xcb,0xc0,0x1b,0xa2,0x41,0xf4,0x11,0x97,0x0e,0x0a,0xf2</td>
<td>15:49 07/04/2018</td>
</tr>
<tr>
<td>8</td>
<td>Download</td>
<td>Patrick Derbez, Virginie Lallemand</td>
<td>0xf3,0x87,0xa4,0x70,0x54,0x88,0xe2,0x0a,0xa1,0x91,0x4e,0x66,0x6d,0x65,0xc2,0xeb7</td>
<td>07:40 11/04/2018</td>
</tr>
<tr>
<td>9</td>
<td>Download</td>
<td>Patrick Derbez, Virginie Lallemand</td>
<td>0x92,0x66,0x14,0x62,0x49,0xd0,0xc5,0x85,0x78,0x6e,0x34,0x04,0xc5,0xd6,0xec</td>
<td>19:00 17/04/2018</td>
</tr>
<tr>
<td>10</td>
<td>Download</td>
<td>Patrick Derbez, Virginie Lallemand</td>
<td>0x54,0xc0,0xba,0x9d,0x40,0x1b,0xac,0xcc,0x3d,0xf8,0x6d,0x73,0x75,0x40,0xc2</td>
<td>02:00 18/04/2018</td>
</tr>
<tr>
<td>11</td>
<td>Download</td>
<td>Patrick Derbez, Virginie Lallemand</td>
<td>0xb1,0x41,0x1a,0x96,0xc0,0xe0,0x66,0x93,0xde,0x38,0xae,0xaf,0xbb,0xd7,0xd1,0x7e</td>
<td>12:40 18/04/2018</td>
</tr>
<tr>
<td>12</td>
<td>Download</td>
<td>Patrick Derbez, Virginie Lallemand</td>
<td>0xe,0xd2,0x8f,0xb1,0x64,0xd8,0x8f,0xd6,0xcd,0xe3,0xo0,0x59,0xa4,0x21,0x11,0x80</td>
<td>10:19 28/04/2018</td>
</tr>
<tr>
<td>13</td>
<td>Download</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>14</td>
<td>Download</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>15</td>
<td>Download</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>16</td>
<td>Download</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>17</td>
<td>Download</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>18</td>
<td>Download</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

New record 3 days ago!!

[https://sites.google.com/site/skinnycipher/](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.

<table>
<thead>
<tr>
<th>Rounds</th>
<th>Dataset</th>
<th>Winner</th>
<th>Secret key</th>
<th>Time Submitted</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>Download</td>
<td>Aleksei Udovenko</td>
<td>0xce,0x94,0x11,0x53,0xa4,0x00,0xec,0x01,0x89,0x6a,0x0b,0x6c,0x4f,0xf2,0x12,0xf2</td>
<td>10:46 05/04/2018</td>
</tr>
<tr>
<td>5</td>
<td>Download</td>
<td>Aleksei Udovenko</td>
<td>0x32,0x6c,0x40,0xab,0x6b,0x12,0xf3,0x44,0x0f,0xe1,0x48,0xc6,0x4b,0x24,0x60,0x6f</td>
<td>11:34 05/04/2018</td>
</tr>
<tr>
<td>6</td>
<td>Download</td>
<td>Aleksei Udovenko</td>
<td>0x33,0xe7,0x4e,0x94,0xc2,0xe7,0xe0,0x0b,0x53,0xed,0xe0,0xf3,0xcf,0xa0,0x52,0x92</td>
<td>18:46 06/04/2018</td>
</tr>
<tr>
<td>7</td>
<td>Download</td>
<td>Aleksei Udovenko</td>
<td>0xeb,0xec,0x6c,0x34,0x6d,0x26,0xc7,0xe3,0x4a,0x78,0xe5,0x0b,0x18,0xe4,0xb2</td>
<td>22:19 08/04/2018</td>
</tr>
<tr>
<td>8</td>
<td>Download</td>
<td>Aleksei Udovenko</td>
<td>0x32,0xd8,0x4c,0x8c,0xa4,0xf3,0xda,0x62,0x0a,0x24,0x78,0x20,0xeb,0x86,0xe0</td>
<td>20:40 09/04/2018</td>
</tr>
<tr>
<td>9</td>
<td>Download</td>
<td>Aleksei Udovenko</td>
<td>0xe6,0xe3,0x7e,0x01,0xc0,0x6d,0xb0,0x7b,0xb5,0x0f,0xad,0x02,0x95,0xa6,0x86,0xcc</td>
<td>23:54 09/04/2018</td>
</tr>
<tr>
<td>10</td>
<td>Download</td>
<td>Aleksei Udovenko</td>
<td>0x8a,0x32,0x5b,0x65,0xfd,0x25,0x5f,0x24,0x1e,0x8e,0xa4,0x77,0xa1,0xc9,0x88,0x90</td>
<td>18:20 13/04/2018</td>
</tr>
<tr>
<td>11</td>
<td>Download</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>Download</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>13</td>
<td>Download</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>14</td>
<td>Download</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>15</td>
<td>Download</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>16</td>
<td>Download</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>17</td>
<td>Download</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>18</td>
<td>Download</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>19</td>
<td>Download</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>20</td>
<td>Download</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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.  
  \textit{Join the competition!!}

• We have not yet received any submission for most interesting cryptanalysis award.  
  \textit{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!!