The SKINNY Family of Block Ciphers

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

NIST Lightweight Cryptography Workshop 2016
Overview

Goals:
• Lightest tweakable block cipher with scalable security
• Suitable for most lightweight applications
• Perform and share full security analysis
• Efficient software/hardware implementations in many scenarios

Results:
• SKINNY family of lightweight (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 in both single-key and related-key
• Efficient and competitive software/hardware implementations
  • Round-based SKINNY-64-128: 1696 GE
  • CTR mode @ Skylake (avx2): 2.63 c/B
Tweakable Block Cipher

\[ P \xrightarrow{TBC} C \]

\[ K \quad T \]

- tweakable block cipher has many applications:
  - Authenticated encryption
  - Disk/memory encryption
  - Hashing: block counter as tweak for HAIFA-like CF
  - (More: \ldots)
- Several block cipher modes: XEX, XPX, XTS, etc.
- Very few direct constructions: Hasty Pudding Cipher, Threefish, Mercy, BLAKE2
Hardness of Key Schedule Design

• We know how to design a good permutation
  • Feistel
  • Substitution-Permutation Network (SPN)

• Designing key (and tweak) schedule is hard
  • AES key schedule is hard to analyze and very different from round function
  • Many recent primitives try to use only permutations to avoid the key schedule

• Designing good schedule for tweak and key is even harder
TWEAKEY [Asiacrypt’14]

Tweak and key are treated the same way

**Superposition-Tweakey (STK)**
- Fully linear scheduling ($h'$: cell permutation)
- Provide bounds in terms of number of active Sboxes in related-key/related-tweak (RK/RT)
- Trick: linear code due to small field multiplications to bound the number of cancellations in the XORs
Specification
SKINNY: General Design Strategy

- Start from weak crypto components, but providing very efficient implementations
  - Opposed to AES: strong Sbox and diffusion → only 10 rounds
  - Similar to SIMON: only AND/XOR/ROT → 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: Specification Overview

Specifications
• SKINNY has a state of either 64 bit \( (s = 4) \) or 128 bits \( (s = 8) \).
• Internal state \( IS \) : viewed as a \( 4 \times 4 \) matrix of \( s \)-bit elements, i.e. \( |IS| = n = 16s \in \{64,128\} \).
• The tweakey size can be \( n, 2n \) or \( 3n \).

Number of rounds

<table>
<thead>
<tr>
<th>Block size ( n )</th>
<th>Tweakey size</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>( n )</td>
</tr>
<tr>
<td>64</td>
<td>32</td>
</tr>
<tr>
<td>128</td>
<td>40</td>
</tr>
</tbody>
</table>

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
- **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 S-box

$S_4$: 4-bit Sbox for SKINNY-64*

- Almost PICCOLO Sbox [SIH$^+$11]
- Implementation: 4 NOR and 4 XOR
- Hardware cost: 12 GE

Properties

- Maximal diff. probability: $2^{-2}$
- Maximal abs. linear bias: $2^{-2}$
- $\deg(S_4) = \deg(S_4^{-1}) = 3$
- One fixed point: $S_4(0xF) = 0xF$
- Branch number: 2
SKINNY: 8-Bit S-box

\[ S_8: 8\text{-bit Sbox for SKINNY-128-}^* \]
- Generalize the \( S_4 \) construction
- Implementation: 8 NOR and 8 XOR
- Hardware cost: 24 GE

**Properties**
- Maximal diff. probability: \( 2^{-2} \)
- Maximal abs. linear bias: \( 2^{-2} \)
- \( \deg(S_8) = \deg(S_8^{-1}) = 6 \)
- One fixed point: \( S_8(0xFF) = 0xFF \)
- Branch number: 2
SKINNY: Round Constant

6-bit constant generated with LFSR

- \( c_0 = rc_3 || rc_2 || rc_1 || rc_0 \)
- \( c_1 = 0 || 0 || rc_5 || rc_4 \)
- \( c_2 = 0x2 \)

Criterion for the choice of constants

- Placement of \( c_0 \), \( c_1 \) and \( c_2 \) has been chosen to maximize the constants diffusion after application of forward/backward linear layer.
- Prevent spreading of symmetries, fixed points and more generally subspaces.
SKINNY: Tweakey Schedule

- $P_T$ is 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
SKINNY: Tweakey Schedule

- $P_T$ is 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
SKINNY: MixColumns

MixColumns

- Matrix multiplication performed as in the MixColumns of the AES
- However:
  - The matrix $M$ is binary
  - It has branch number 2: $M \times (0, \alpha, 0, 0)^\top = (0, 0, \alpha, 0)^\top$

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

- $M$ has branching number 2, but good differential paths avoided by a careful choice of $M$
- Fast diffusion (6 rounds forward and backward)
SKINNY: Choice of Each Component

• Informally: Minimize number of operations, maximize security

• Many new components, selected incrementally:
  • Sboxes
  • ShiftRows+MixColumns
  • TWEAKEY Permutation $P_T$

• Selection based on two independent estimations:
  • Security (manual analysis and MILP)
  • Implementation efficiency (hardware/software)
Security
Security Overview

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

List of attacks 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

<table>
<thead>
<tr>
<th>Cipher</th>
<th>Single-Key (SK)</th>
<th>Related-Key (RK)</th>
</tr>
</thead>
<tbody>
<tr>
<td>SKINNY-64-128</td>
<td>8/36 = 22%</td>
<td>15/36 = 42%</td>
</tr>
<tr>
<td>SIMON-64-128</td>
<td>19/44 = 43%</td>
<td>no bound known</td>
</tr>
<tr>
<td>SKINNY-128-128</td>
<td>15/40 = 37%</td>
<td>19/40 = 47%</td>
</tr>
<tr>
<td>SIMON-128-128</td>
<td>41/72 = 53%</td>
<td>no bound known</td>
</tr>
<tr>
<td>AES-128</td>
<td>4/10 = 40%</td>
<td>6/10 = 60%</td>
</tr>
<tr>
<td>NEOKEON-128</td>
<td>12/16 = 75%</td>
<td>12/16 = 75%</td>
</tr>
</tbody>
</table>
Performance
### Theoretical Performance of SKINNY

<table>
<thead>
<tr>
<th>Cipher</th>
<th>Rounds</th>
<th>#operations per bit without KS</th>
<th>#operations per bit with KS</th>
<th>Round based area estimation</th>
</tr>
</thead>
<tbody>
<tr>
<td>SKINNY-64-128</td>
<td>36</td>
<td>117</td>
<td>139.5</td>
<td>8.68</td>
</tr>
<tr>
<td>SIMON-64-128</td>
<td>44</td>
<td>88</td>
<td>154</td>
<td>8.68</td>
</tr>
<tr>
<td>PRESENT-64-128</td>
<td>31</td>
<td>147.2</td>
<td>161.8</td>
<td>12.43</td>
</tr>
<tr>
<td>PICCOLO-64-128</td>
<td>31</td>
<td>162.75</td>
<td>162.75</td>
<td>12.35</td>
</tr>
<tr>
<td>SKINNY-128-128</td>
<td>40</td>
<td>130</td>
<td>130</td>
<td>7.01</td>
</tr>
<tr>
<td>SIMON-128-128</td>
<td>72</td>
<td>136</td>
<td>204</td>
<td>7.04</td>
</tr>
<tr>
<td>NEOKEON-128-128</td>
<td>16</td>
<td>100</td>
<td>200</td>
<td>30.36</td>
</tr>
<tr>
<td>AES-128-128</td>
<td>10</td>
<td>202.5</td>
<td>248.1</td>
<td>59.12</td>
</tr>
</tbody>
</table>

**Example of SKINNY-64-128 (more in the paper)**
- 1R : (4 NOR + 4 XOR)=4 [SB] + (3 XOR)=4 [MC] + (32 XOR)=64 [ART]
- That is (per bit per round) : 1 NOR + 2.25 XOR
- #operations per bit (without KS) : (1 + 2:25) 36 = 117
- Very low number of operations per plaintext bit
- Challenge : do better
ASIC Implementations

Preliminaries

• ASIC: Application-Specific Integrated Circuit
• Synthesis: Synopsys Design Compiler version A-2007.12-SP1
• UMCL18G212T3 standard cell library [Vir04]
  • UMC L180 0.18m 1P6M logic process
  • Typical voltage of 1.8 V

Four scenarios

• Round-based implementations
  ⇒ most important target for our design choices
• Fully unrolled implementations (see full version)
• Serial implementations (see full version)
  • Bit-serial
  • Nibble- or byte-serial
• Threshold implementations (see full version)
## Round-Based Implementation Results

<table>
<thead>
<tr>
<th></th>
<th>Area (GE)</th>
<th>Delay (ns)</th>
<th>Throughput @100KHz (Kbit/s)</th>
<th>Throughput @maximum (Mbit/s)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>SKINNY-64-128</strong></td>
<td>1696</td>
<td>1.87</td>
<td>177.78</td>
<td>951.11</td>
</tr>
<tr>
<td><strong>SKINNY-128-128</strong></td>
<td>2391</td>
<td>2.89</td>
<td>320.00</td>
<td>1107.20</td>
</tr>
<tr>
<td><strong>SKINNY-128-256</strong></td>
<td>3312</td>
<td>2.89</td>
<td>266.67</td>
<td>922.67</td>
</tr>
<tr>
<td><strong>SIMON-64-128</strong></td>
<td>1751</td>
<td>1.60</td>
<td>145.45</td>
<td>870</td>
</tr>
<tr>
<td><strong>SIMON-128-128</strong></td>
<td>2342</td>
<td>1.60</td>
<td>188.24</td>
<td>1145</td>
</tr>
<tr>
<td><strong>SIMON-128-256</strong></td>
<td>3419</td>
<td>1.60</td>
<td>177.78</td>
<td>1081</td>
</tr>
<tr>
<td><strong>LED-64-64</strong></td>
<td>2695</td>
<td>-</td>
<td>198.9</td>
<td>-</td>
</tr>
<tr>
<td><strong>LED-64-128</strong></td>
<td>3036</td>
<td>-</td>
<td>133.0</td>
<td>-</td>
</tr>
<tr>
<td><strong>PRESENT-64-128</strong></td>
<td>1884</td>
<td>-</td>
<td>200.00</td>
<td>-</td>
</tr>
<tr>
<td><strong>PICCOLO-64-128</strong></td>
<td>1773</td>
<td>-</td>
<td>193.94</td>
<td>-</td>
</tr>
</tbody>
</table>
SKINNY: in a nutshell

• New very lightweight family of tweakable block cipher ⇒ Almost as light as possible
• Alternative to SIMON family of block ciphers
• Very efficient implementations (both SW and HW)
• SK and RK/RT security guarantees
Final Remarks

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

SKINNY competition:

• breaking contest of reduced-round versions of SKINNY-64-128 and SKINNY-64-128
• small gifts for improving the current best attack
• deadline for submission 1st of March 2017
• details are available at the web page

Thank you for your attention!!