# Yet Another Lightweight Block Cipher

Christof Beierle, Jérémy Jean, Gregor Leander, Amir Moradi, **Thomas Peyrin**, Yu Sasaki, Pascal Sasdrich, Siang Meng Sim

# Simon and its (bigger) brothers

Many lightweight block-ciphers have been proposed recently (PRESENT, KATAN, LED, PICCOLO, TWINE, …), all offering very similar performance with security guarantees

**Simon** came with **no security guarantee** (nor any crypt-analysis), but with an **impressive performance** for many platforms

Because of its performance, SIMON is a natural favorite for NIST and/or ISO standardization

**We need an academic competitor to Simon !**

# What is **Skinny** ?

**Skinny** is a **tweakable block cipher** with following goals:

- **SW/HW performances equivalent to Simon**
- **With security proofs regarding differential/linear attacks**
- Flexible key/tweak/block sizes

# **Skinny** design

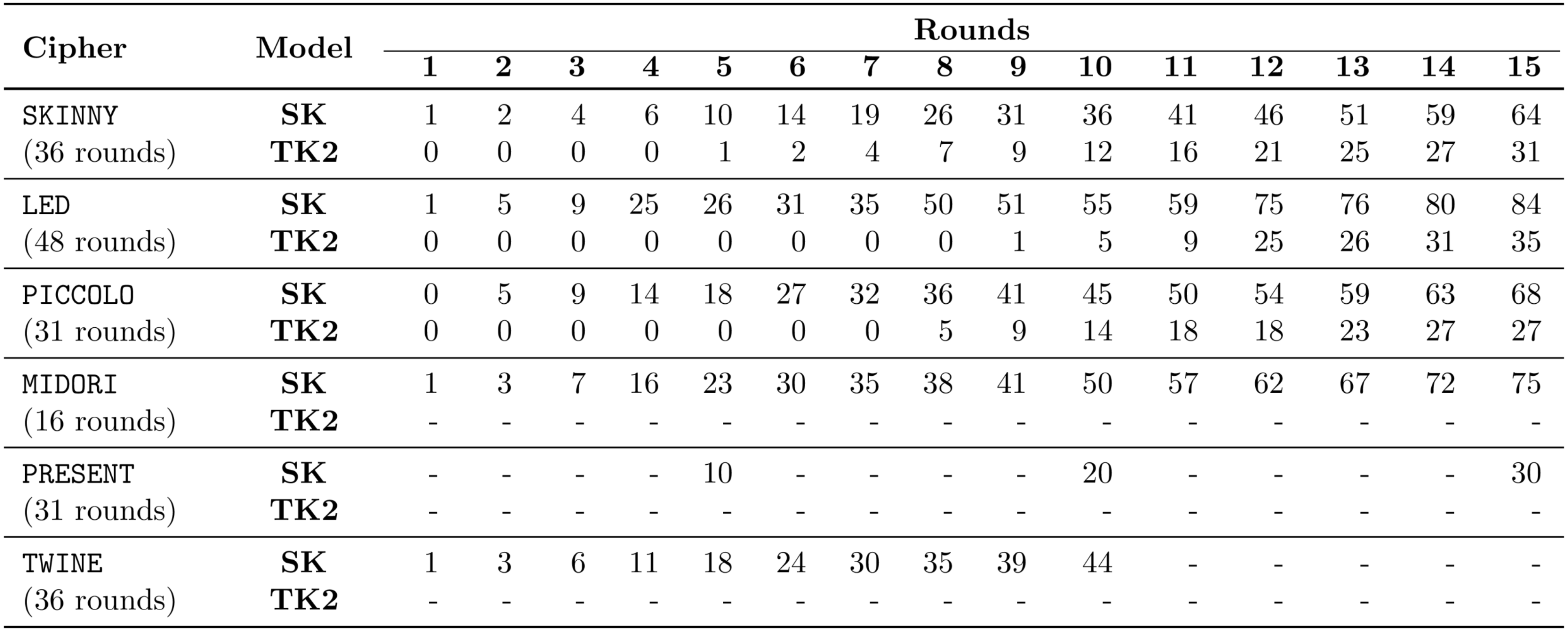
## **AES-like design**

**But**:

- Subtweakey added only to half of the state
- Constants reduced to very minimum (LFSR produced)
- Sbox is very light (almost PICCOLO Sbox)
- Mixcolumns extremely light (binary matrix with **only three XORs**)
- Tweakey schedule uses new LFSR based tweak separation
- Order of operations is SB – AK – ShR –MC, with no whitening key

# Bounds on the number of active Sboxes

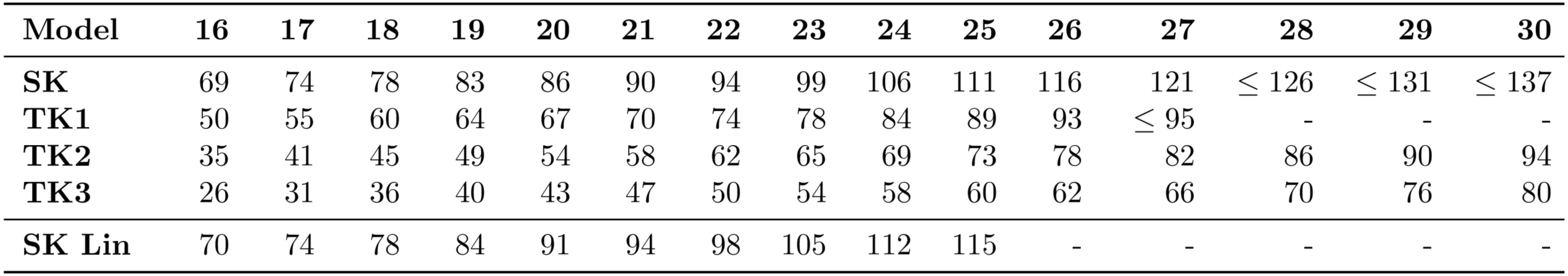
With so weak internal components, it is very unlikely that we obtain good security … especially in related-key model



| Cipher | Model | Rounds | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** | **9** | **10** | **11** | **12** | **13** | **14** | **15** |
| SKINNY | **SK** | 1 | 2 | 4 | 6 | 10 | 14 | 19 | 26 | 31 | 36 | 41 | 46 | 51 | 59 | 64 |
| (36 rounds) | **TK2** | 0 | 0 | 0 | 0 | 1 | 2 | 4 | 7 | 9 | 12 | 16 | 21 | 25 | 27 | 31 |
| LED | **SK** | 1 | 5 | 9 | 25 | 26 | 31 | 35 | 50 | 51 | 55 | 59 | 75 | 76 | 80 | 84 |
| (48 rounds) | **TK2** | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 5 | 9 | 25 | 26 | 31 | 35 |
| PICCOLO | **SK** | 0 | 5 | 9 | 14 | 18 | 27 | 32 | 36 | 41 | 45 | 50 | 54 | 59 | 63 | 68 |
| (31 rounds) | **TK2** | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 5 | 9 | 14 | 18 | 18 | 23 | 27 | 27 |
| MIDORI | **SK** | 1 | 3 | 7 | 16 | 23 | 30 | 35 | 38 | 41 | 50 | 57 | 62 | 67 | 72 | 75 |
| (16 rounds) | **TK2** | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - |
| PRESENT | **SK** | - | - | - | - | 10 | - | - | - | - | 20 | - | - | - | - | 30 |
| (31 rounds) | **TK2** | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - |
| TWINE | **SK** | 1 | 3 | 6 | 11 | 18 | 24 | 30 | 35 | 39 | 44 | - | - | - | - | - |
| (36 rounds) | **TK2** | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - |

# Bounds on the number of active Sboxes

With so weak internal components, it is very unlikely that we obtain good security … especially in related-key model



| Model | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **SK** | 69 | 74 | 78 | 83 | 86 | 90 | 94 | 99 | 106 | 111 | 116 | 121 | $\leq 126$ | $\leq 131$ | $\leq 137$ |
| **TK1** | 50 | 55 | 60 | 64 | 67 | 70 | 74 | 78 | 84 | 89 | 93 | $\leq 95$ | - | - | - |
| **TK2** | 35 | 41 | 45 | 49 | 54 | 58 | 62 | 65 | 69 | 73 | 78 | 82 | 86 | 90 | 94 |
| **TK3** | 26 | 31 | 36 | 40 | 43 | 47 | 50 | 54 | 58 | 60 | 62 | 66 | 70 | 76 | 80 |
| **SK Lin** | 70 | 74 | 78 | 84 | 91 | 94 | 98 | 105 | 112 | 115 | - | - | - | - | - |

# Bounds on the number of active Sboxes

**Because Simon is an &RX design**:

- it is very hard to get bounds on the best differential paths
- impossible as of today for 128-bit block versions
- impossible as of today in the related-key model

# Performances

## Round-based ASIC implementations:

| | Area | Throughput @100KHz |
|---|---|---|
| SKINNY-64-128 | 1691 | 177.78 |
| SIMON-64-128 | 1751 | 145.45 |
| SKINNY-128-128 | 2382 | 320.00 |
| SIMON-128-128 | 2342 | 188.24 |
| SKINNY-128-256 | 3302 | 266.67 |
| SIMON-128-256 | 3419 | 177.78 |

## Bitslice implementations:

| | Westmere | Ivy Bridge | Haswell | | Skylake | |
|---|---|---|---|---|---|---|
| Instruction Set | sse4 | sse4 | sse4 | avx2 | sse4 | avx2 |
| SKINNY-64-128 | 5.6 | 4.8 | 4.9 | 2.5 | 4.6 | 2.1 |
| SIMON-64-128 | 6.9 | 5.9 | 5.8 | 3.0 | 5.4 | 2.7 |

# Challenge: can you do better ?

## Number of bitwise operations per plaintext bit

| **Cipher** | **nb. of op** |
|---|---|
| SKINNY-64-128 | **139.5** |
| SIMON-64-128 | **154** |
| PRESENT-128 | 161.8 |
| PICCOLO-128 | 162.75 |
| KATAN-64-80 | 797.8 |
| SKINNY-128-256 | **186** |
| SIMON-128-256 | **252** |
| AES-128 | 248.1 |
| AES-256 | 411.2 |