Does Lightweight Cryptography Imply Slight Security?

Orr Dunkelman

Computer Science Department
University of Haifa

7th March, 2014
Outline

1. Introduction
   - Lightweight Cryptography
   - Lightweight Cryptography Primitives

2. The Path to Security

3. A Few Examples
   - The MISTY1 to KASUMI Transition
   - The AES to LED Transition
   - The KTANTAN Block Cipher
   - ZORRO

4. Conclusions/Discussions
Lightweight Cryptography

- Targets constrained environments.
- Tries to reduce the computational efforts needed to obtain security.
- Optimization targets: size, power, energy, time, code size, RAM/ROM consumption, etc.
Lightweight Cryptography

- Targets constrained environments.
- Tries to reduce the computational efforts needed to obtain security.
- Optimization targets: size, power, energy, time, code size, RAM/ROM consumption, etc.

Why now?
Constrained environments today are different than constrained environments 10 years ago.

- Ubiquitous computing – RFID tags, sensor networks.
- Low-end devices (8-bit platforms).
- Stream ciphers do not enjoy the same “foundations” as block ciphers.
- Failure of previous solutions (KeeLoq, Mifare) to meet required security targets.
- Good research direction...
Some Lightweight Primitives

<table>
<thead>
<tr>
<th>Block Ciphers</th>
<th>Stream Ciphers</th>
<th>Hash Functions</th>
<th>MACs</th>
</tr>
</thead>
<tbody>
<tr>
<td>HIGHT</td>
<td>Grain</td>
<td>H-PRESENT</td>
<td>SQUASH</td>
</tr>
<tr>
<td>mCrypton</td>
<td>Trivium</td>
<td>PHOTON</td>
<td></td>
</tr>
<tr>
<td>DESL</td>
<td>Mickey</td>
<td>QUARK</td>
<td></td>
</tr>
<tr>
<td>PRESENT</td>
<td>F-FCSR-H</td>
<td>Armadillo</td>
<td></td>
</tr>
<tr>
<td>KATAN</td>
<td>WG-7</td>
<td>SpongeNT</td>
<td></td>
</tr>
<tr>
<td>KTANTAN</td>
<td>CAZAD</td>
<td>GLOUN</td>
<td></td>
</tr>
<tr>
<td>PRINTcipher</td>
<td></td>
<td>Keccak-f*</td>
<td></td>
</tr>
<tr>
<td>SEA</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Klein</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>LBlock</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>GOST</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ZORRO</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>TWINE</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>LED</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PRINCE</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Simon</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Speck</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## Some Lightweight Primitives

<table>
<thead>
<tr>
<th>Block Ciphers</th>
<th>Stream Ciphers</th>
<th>Hash Functions</th>
<th>MACs</th>
</tr>
</thead>
<tbody>
<tr>
<td>HIGHT</td>
<td>Grain</td>
<td>H-PRESENT</td>
<td>SQUASH</td>
</tr>
<tr>
<td>mCrypton</td>
<td>Trivium</td>
<td>PHOTON</td>
<td></td>
</tr>
<tr>
<td>DESL</td>
<td>Mickey</td>
<td>QUARK</td>
<td></td>
</tr>
<tr>
<td>PRESENT</td>
<td>F-FCSR-H</td>
<td>Armadillo</td>
<td></td>
</tr>
<tr>
<td>KATAN</td>
<td>WG-7</td>
<td>SpongeNT</td>
<td></td>
</tr>
<tr>
<td>KTANTAN</td>
<td>CAZAD</td>
<td>GLOUN</td>
<td></td>
</tr>
<tr>
<td>PRINTcipher</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SEA</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Klein</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>LBlock</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>GOST</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ZORRO</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>TWINE</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>LED</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PRINCE</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Simon</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Speck</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Security Challenges

- Lightweight ⇒ pick the point on the security/performance curve with as little security margins as possible.
- Use best-of-the-art approaches:
  - Count the number of active S-boxes (wide trail),
  - Scale-down “known” ciphers (Misty1 → KASUMI, AES → LED, Zorro, DES → DESL, . . . )
  - Use “secure structures” (GFNs/AIDS-like/etc.)
Security Challenges

- Lightweight ⇒ pick the point on the security/performance curve with as little security margins as possible.
- Use best-of-the-art approaches:
  - Count the number of active S-boxes (wide trail),
  - Scale-down “known” ciphers (Misty1 → KASUMI, AES → LED, Zorro, DES → DESL, . . .)
  - Use “secure structures” (GFNs/AES-like/etc.)
  - Ignore related-key attacks...
Security Challenges

- Lightweight ⇒ pick the point on the security/performance curve with as little security margins as possible.
- Use best-of-the-art approaches:
  - Count the number of active S-boxes (wide trail),
  - Scale-down “known” ciphers (Misty1 → KASUMI, AES → LED, Zorro, DES → DESL, . . . )
  - Use “secure structures” (GFNs/AES-like/etc.)
  - Ignore related-key attacks...
- Use provable approaches:
  - Even-Mansour (1-Key/Multiple Key)
Security Challenges

- Lightweight ⇒ pick the point on the security/performance curve with as little security margins as possible.
- Use best-of-the-art approaches:
  - Count the number of active S-boxes (wide trail),
  - Scale-down “known” ciphers (Misty1 → KASUMI, AES→ LED, Zorro, DES→ DESL, . . .)
  - Use “secure structures” (GFNs/AES-like/etc.)
  - Ignore related-key attacks...
- Use provable approaches:
  - Even-Mansour (1-Key/Multiple Key)

- As usual . . . pray.
MISTY1

- Introduced by Matsui in 1997.
- 64-bit block, 128-bit key.
- Recursive structure — 8 Feistel rounds, each round function is a 3-round Feistel function.
- Each of these semi-round functions is a 3-round Feistel on its own.
- Uses 7-bit and 9-bit S-boxes for maximal nonlinearity.
- Every two rounds there is an $FL$-layer.
- Cryptrec-approved, NESSIE-portfolio, RFC, ISO.
- Predecessor of KASUMI.
KASUMI

\[
\begin{align*}
&\Gamma KC_1 \rightarrow KO_1, KL_1 \rightarrow FL1 \rightarrow FO1 \\
&\Gamma KO_2, KL_2 \rightarrow FL2 \\
&\Gamma KL_3 \rightarrow KO_3, KL_3 \rightarrow FO3 \\
&\Gamma KO_4, KL_4 \rightarrow FL4 \\
&\Gamma KL_5 \rightarrow KO_5, KL_5 \rightarrow FO5 \\
&\Gamma KO_6, KL_6 \rightarrow FL6 \\
&\Gamma KL_7 \rightarrow KO_7, KL_7 \rightarrow FO7 \\
&\Gamma KO_8, KL_8 \rightarrow FL8 \\
&\Gamma KL_9 \rightarrow KO_9, KL_9 \rightarrow FO9 \\
\end{align*}
\]

\[
\begin{align*}
&\Gamma FO_1, KL_1 \rightarrow FO1 \\
&\Gamma FO_2 \rightarrow FL2 \\
&\Gamma FO_3 \rightarrow FL3 \\
&\Gamma FO_4 \rightarrow FL4 \\
&\Gamma FO_5 \rightarrow FL5 \\
&\Gamma FO_6 \rightarrow FL6 \\
&\Gamma FO_7 \rightarrow FL7 \\
&\Gamma FO_8 \rightarrow FL8 \\
&\Gamma FO_9 \rightarrow FL9 \\
\end{align*}
\]

KASUMI

KA S U M I
KASUMI — Changes from MISTY1

- Done by ETSI’s SAGE group to fit mobile handsets.
- $FL$ functions to be moved from datapath to round-path.
- One key addition reduced from the $FO$ function.
- Extra $S7$ in $FI$ (=>$FO$ can no longer be divided into 4 parallel functions, but only 2).
KASUMI — Changes from MISTY1

- Done by ETSI’s SAGE group to fit mobile handsets.
- $FL$ functions to be moved from datapath to round-path.
- One key addition reduced from the $FO$ function.
- Extra $S7$ in $FI$ ($\Rightarrow$ $FO$ can no longer be divided into 4 parallel functions, but only 2).
- Key schedule changed significantly.
KASUMI vs. MISTY1

- In the single-key model: KASUMI ≈ MISTY1:
  - 6-Round Misty1 [JL12]: $2^{52.5}$ CPs, $2^{112.4}$ time.
  - 6-Round KASUMI [K12]: $2^{55}$ CPs, $2^{100}$ time.
- In the related-key model: MISTY1 ≫ KASUMI.
  - Practical key recovery attack against the full KASUMI ([DKS10]).
  - MISTY1: not even close (without FL, [DK13]).
The LED Block Cipher

- Introduced by [G+11].
- 64-bit block with 64-bit key (LED-64) or 128-bit key (LED-128).
- LED-64: 8-Step 1-Key Even-Mansour.
- LED-128: 12-Step 2-Key Even-Mansour.
- The "public permutation": 4-round unkeyed AES-like construction.
The LED Block Cipher (cont.)

- 48-round (12-step LED-128) offer security against differential, linear, meet-in-the-middle, ...
The LED Block Cipher (cont.)

- No related-key issues/weakness in key schedule.
The LED Block Cipher (cont.)

- 48-round (12-step LED-128) offer security against differential, linear, meet-in-the-middle, ... 
- No related-key issues/weakness in key schedule. 
- As long as the 8-Step 1-Key Even-Mansour secure (LED-64) or 5-Step 1-Key Even-Mansour secure (LED-128).
## Results on LED (Single-Key)

<table>
<thead>
<tr>
<th>Source</th>
<th>Cipher</th>
<th>Steps</th>
<th>Time</th>
<th>Data</th>
<th>Memory</th>
</tr>
</thead>
<tbody>
<tr>
<td>[IS12]</td>
<td>LED-64</td>
<td>2</td>
<td>$2^{56}$</td>
<td>$2^8$ CP</td>
<td>$2^8$</td>
</tr>
<tr>
<td>[D+14]</td>
<td>LED-64</td>
<td>2</td>
<td>$2^{48}$</td>
<td>$2^{16}$ CP</td>
<td>$2^{17}$</td>
</tr>
<tr>
<td>[D+14]</td>
<td>LED-64</td>
<td>2</td>
<td>$2^{48}$</td>
<td>$2^{48}$ KP</td>
<td>$2^{48}$</td>
</tr>
<tr>
<td>[D+13]</td>
<td>LED-64</td>
<td>3</td>
<td>$2^{60.2}$</td>
<td>$2^{49}$ KP</td>
<td>$2^{60}$</td>
</tr>
<tr>
<td>[IS12]</td>
<td>LED-128</td>
<td>4</td>
<td>$2^{112}$</td>
<td>$2^{16}$ CP</td>
<td>$2^{19}$</td>
</tr>
<tr>
<td>[M+12]</td>
<td>LED-128</td>
<td>4</td>
<td>$2^{96}$</td>
<td>$2^{64}$ KP</td>
<td>$2^{64}$</td>
</tr>
<tr>
<td>[NWW13]</td>
<td>LED-128</td>
<td>4</td>
<td>$2^{96}$</td>
<td>$2^{32}$ KP</td>
<td>$2^{32}$</td>
</tr>
<tr>
<td>[NWW13]</td>
<td>LED-128</td>
<td>6</td>
<td>$2^{124.4}$</td>
<td>$2^{59}$ KP</td>
<td>$2^{59}$</td>
</tr>
<tr>
<td>[D+13]</td>
<td>LED-128</td>
<td>6</td>
<td>$2^{124.5}$</td>
<td>$2^{45}$ KP</td>
<td>$2^{60}$</td>
</tr>
<tr>
<td>[D+13]</td>
<td>LED-128</td>
<td>8</td>
<td>$2^{123.8}$</td>
<td>$2^{49}$ KP</td>
<td>$2^{60}$</td>
</tr>
</tbody>
</table>
Related-Key Attacks on LED-64 [M+12]

- Find iterative characteristic $\Delta \rightarrow \Delta$ through $P_i$.
- Set key difference to $\Delta$, plaintext difference to 0 ...
Related-Key Attacks on LED-64 [M+12]

- Find iterative characteristic $\Delta \rightarrow \Delta$ through $P_i$.
- Set key difference to $\Delta$, plaintext difference to 0 . . .
- 3-Step immediate related-key attack on LED-64, can be extended to 4-Step.
- 6-Step immediate related-key attack on LED-128.
The KTANTAN Block Ciphers [DDK09]

- KTANTAN has 3 flavors: KTANTAN-32, KTANTAN-48, KTANTAN-64.
- Block size: 32/48/64 bits.
- Key size: 80 bits.
- KATAN-\(n\) and KTANTAN-\(n\) are the same up to key schedule.
- In KTANTAN, the key is burnt into the device and cannot be changed.
General Structure of KATAN/KTANTAN

\[ L_2 \xrightarrow{\oplus} L_1 \xrightarrow{\ominus} \ominus \xrightarrow{\ominus} k_a \]

\[ IR \xrightarrow{\ominus} k_b \]

Orr Dunkelman
The KTANTAN Block Ciphers — Key Schedule

- Main problem — related-key and slide attacks.
- Solution A — two round functions, prevents slide attacks.
- Solution B — divide the key into 5 words of 16 bits, pick bits in a nonlinear manner.
The KTANTAN Block Ciphers — Key Schedule

- Main problem — related-key and slide attacks.
- Solution A — two round functions, prevents slide attacks.
- Solution B — divide the key into 5 words of 16 bits, pick bits in a nonlinear manner.
- Specifically, let $K = w_4||w_3||w_2||w_1||w_0$, $T = T_7 \ldots T_0$ be the round-counter LFSR, set:

$$a_i = MUX16to1(w_i, T_7T_6T_5T_4)$$

$$k_a = \overline{T_3} \cdot \overline{T_2} \cdot (a_0) \oplus (T_3 \lor T_2) \cdot \overline{T_3} \cdot T_2 \cdot (a_4)$$

$$\oplus (T_3 \lor \overline{T_2}) \cdot MUX4to1(a_3a_2a_1a_0, \overline{T_1T_0})$$

$$k_b = \overline{T_3} \cdot T_2 \cdot (a_4) \oplus (T_3 \lor \overline{T_2}) \cdot MUX4to1(a_3a_2a_1a_0, \overline{T_1T_0})$$
Security Analysis — Differential Cryptanalysis

- Computer-aided search for the various round combinations and all block sizes.
- KATAN32: Best 42-round characteristic has probability $2^{-11}$.
- KATAN48: Best 43-round characteristic has probability $2^{-18}$.
- KATAN64: Best 37-round characteristic has probability $2^{-20}$. 
Security Analysis — Differential Cryptanalysis

- Computer-aided search for the various round combinations and all block sizes.
- KATAN32: Best 42-round characteristic has probability $2^{-11}$.
- KATAN48: Best 43-round characteristic has probability $2^{-18}$.
- KATAN64: Best 37-round characteristic has probability $2^{-20}$.
- This also proves that all the differential-based attacks fail (boomerang, rectangle).
Related-Key Differentials in KATAN

- No good methodology for that.
Related-Key Differentials in KATAN

- No good methodology for that.
- In KATAN32 — each key bit difference must enter (at least) two linear operations and two non-linear ones.
- Hence, an active bit induces probability of $2^{-2}$, and cancels four other bits (or probability of $2^{-4}$ and 6).
Related-Key Differentials in KATAN

- No good methodology for that.
- In KATAN32 — each key bit difference must enter (at least) two linear operations and two non-linear ones.
- Hence, an active bit induces probability of $2^{-2}$, and cancels four other bits (or probability of $2^{-4}$ and 6).
- So if there are 76 key bits active — there are at least 16 quintuples, each with probability $2^{-2}$. 
Related-Key Differentials in KATAN

- No good methodology for that.
- In KATAN32 — each key bit difference must enter (at least) two linear operations and two non-linear ones.
- Hence, an active bit induces probability of $2^{-2}$, and cancels four other bits (or probability of $2^{-4}$ and 6).
- So if there are 76 key bits active — there are at least 16 quintuples, each with probability $2^{-2}$.
- The key expansion is linear, so check minimal hamming weight in the code.
- Our analysis, so far revealed 72 as the lower bound.
Attacks on the KTANTAN Family

**BR10** Meet in the middle attacks
- Data: 2–3 KPs, Time: $\approx 2^{75}$, Memory: $O(1)$.

**A11** Related-key attacks
- Data: A few pairs of RK CPs (with 2–4 keys), Time: $2^{30}$, Memory: $O(1)$.

**W+11** Meet in the middle attacks
- Data: 4 CPs, Time: $\approx 2^{73}/2^{74}/2^{75}$, Memory: $O(1)$.
What Went Wrong?

- The key schedule.
What Went Wrong?

- The key schedule.
- The bits which are chosen as the key are not “well distributed”.
- For example, bit 32 of the key, does not enter the first 218 rounds...
- Other bits which are not that common also appear.
- This can be used in several ways (MitM, RK differentials).
Zorro block cipher [G+13]

- Lightweight block cipher that targets side channel security.
- 128-bit block, 128-bit key.
- Single-key iterated Even-Mansour construction.
- 24 rounds, every four rounds the key is XOREd to the state.
- Based on the AES
The ZORRO Block Cipher (cont.)

\[ \begin{align*}
\oplus \quad 4R \\
K 
\end{align*} \]

\[ \begin{align*}
\oplus \quad 4R \\
K 
\end{align*} \]

\[ \begin{align*}
\oplus \quad 4R \\
K 
\end{align*} \]

\[ \begin{align*}
\oplus \quad 4R \\
K 
\end{align*} \]

\[ \begin{align*}
\oplus \quad 4R \\
K 
\end{align*} \]

\[ \begin{align*}
\oplus \quad 4R \\
K 
\end{align*} \]
The ZORRO Round Function
Interesting Properties of Zorro [W+13]

- S-boxes are used only in the first row.
Interesting Properties of Zorro [W+13]

- S-boxes are used only in the first row.
- Circulant matrices have interesting properties when raised to the power. Namely,

\[
\begin{pmatrix}
2 & 3 & 1 & 1 \\
1 & 2 & 3 & 1 \\
1 & 1 & 2 & 3 \\
3 & 1 & 1 & 2
\end{pmatrix}^4 = 
\begin{pmatrix}
1 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 \\
0 & 0 & 1 & 0 \\
0 & 0 & 0 & 1
\end{pmatrix}
\]
Interesting Properties of Zorro [W+13]

- S-boxes are used only in the first row.
- Circulant matrices have interesting properties when raised to the power. Namely,

\[
\begin{pmatrix}
2 & 3 & 1 & 1 \\
1 & 2 & 3 & 1 \\
1 & 1 & 2 & 3 \\
3 & 1 & 1 & 2 \\
\end{pmatrix}^4 = \begin{pmatrix}
1 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 \\
0 & 0 & 1 & 0 \\
0 & 0 & 0 & 1 \\
\end{pmatrix}
\]

- So what?
Differential/Linear Properties of Zorro [W+13]

- Consider differences/masks of the form:

\[
\begin{pmatrix}
  a & a & a & a \\
  b & b & b & b \\
  c & c & c & c \\
  d & d & d & d \\
\end{pmatrix}
\]

- The equality of different columns remains, up to the S-boxes.
Differential/Linear Properties of Zorro [W+13]

- Consider differences/masks of the form:

\[
\begin{pmatrix}
a & a & a & a \\
b & b & b & b \\
c & c & c & c \\
d & d & d & d \\
\end{pmatrix}
\]

- The equality of different columns remains, up to the S-boxes.
- Which are applied only to the first row.
Differential/Linear Properties of Zorro \([W+13]\)

- Consider differences/masks of the form:

\[
\begin{pmatrix}
a & a & a & a \\
b & b & b & b \\
c & c & c & c \\
d & d & d & d
\end{pmatrix}
\]

- The equality of different columns remains, up to the S-boxes.
- Which are applied only to the first row.
- So let’s try to not activate it...
Differential/Linear Properties of Zorro (cont.)

\[
\begin{pmatrix}
0 \\
a \\
b
\end{pmatrix}
\] \xrightarrow{SB}
\[
\begin{pmatrix}
0 \\
a \\
b
\end{pmatrix}
\]
\xrightarrow{MC}
\[
\begin{pmatrix}
0 \\
c \\
d \\
e
\end{pmatrix}
\] \xrightarrow{SB}
\[
\begin{pmatrix}
0 \\
c \\
d \\
e
\end{pmatrix}
\]
\xrightarrow{MC}
\[
\begin{pmatrix}
0 \\
f \\
0 \\
g
\end{pmatrix}
\] \xrightarrow{SB}

\[
\begin{pmatrix}
0 \\
f \\
0 \\
g
\end{pmatrix}
\] \xrightarrow{MC}
\[
\begin{pmatrix}
h \\
i \\
j \\
k
\end{pmatrix}
\] \xrightarrow{SB}
\[
\begin{pmatrix}
h \\
i \\
j \\
k
\end{pmatrix}
\] \xrightarrow{MC}
\[
\begin{pmatrix}
0 \\
a \\
0 \\
b
\end{pmatrix}
\] \xrightarrow{AK}
\[
\begin{pmatrix}
0 \\
a \\
0 \\
b
\end{pmatrix}
\]
Implications \([W+13]\)

- Using the iterative characteristic it is possible to devise:
  - Differential attack (20-round characteristic, \(2^{-108.3}\) probability, 4-R attack, \(2^{112.4}\) CPs, \(2^{112.4}\) time).
  - Linear distinguisher (24-round characteristic, \(2^{-52.62}\) bias, 0-R attack, \(2^{105.3}\) KPs).
Our Improvements — Linear Attack

- Distinguisher $\implies$ key recovery transformation.
- 20-round linear characteristic
- 4-round attack
- Immediate attack — $2^{90}$ KPs and time
- With some more improvements can be reduced...
Our Improvements — A Different Mask

We can also change the mask a bit, to obtain characteristics with 2 active S-boxes every two rounds:

\[
\begin{pmatrix}
0 & 0 \\
X_1 & X_3 \\
X_2 & X_2 \\
X_3 & X_1
\end{pmatrix}
\xrightarrow{SB}
\begin{pmatrix}
0 & 0 \\
X_1 & X_3 \\
X_2 & X_2 \\
X_3 & X_1
\end{pmatrix}
\xrightarrow{SR}
\begin{pmatrix}
0 & 0 \\
X_3 & X_1 \\
X_2 & X_2 \\
X_1 & X_3
\end{pmatrix}
\xrightarrow{MC}
\begin{pmatrix}
c' & 0 \\
0 & 0
\end{pmatrix}
\]

\[
\begin{pmatrix}
c' \\
a' \\
d \\
b'
\end{pmatrix}
\xrightarrow{SB}
\begin{pmatrix}
c' \\
a' \\
d \\
b'
\end{pmatrix}
\xrightarrow{SR}
\begin{pmatrix}
c' \\
a' \\
d \\
b'
\end{pmatrix}
\xrightarrow{MC}
\begin{pmatrix}
0 & 0 \\
x_1 & x_3 \\
x_2 & x_2 \\
x_3 & x_1
\end{pmatrix}
\]
A Different Mask (cont.)

- The different mask has 2 active S-boxes/2 rounds, rather than 4 active S-boxes/4 rounds.
A Different Mask (cont.)

- The different mask has 2 active S-boxes/2 rounds, rather than 4 active S-boxes/4 rounds.
- The gain is not in the probability, but rather in the key recovery phase.

<table>
<thead>
<tr>
<th>Attack</th>
<th>Complexity</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Data</td>
</tr>
<tr>
<td>Differential</td>
<td>$2^{95}$ CPs</td>
</tr>
<tr>
<td>Linear</td>
<td>$2^{83.3}$ KPs</td>
</tr>
</tbody>
</table>

Joint work with Ahiya Bar-On, Itai Dinur, Nathan Keller, Boaz Tsaban, and Adi Shamir
What Went Wrong?

- Too few active S-boxes.
What Went Wrong?

- Too few active S-boxes.
- Circulant matrices, which are good for implementation, may have undesirable security properties.
- Adding the key a few times — may cause some security problems.
How much are we willing to pay for security in lightweight schemes?
Conclusions/Discussions

- How much are we willing to pay for security in lightweight schemes?
- What is the target for lightweight schemes optimization?
Conclusions/Discussions

» How much are we willing to pay for security in lightweight schemes?
» What is the target for lightweight schemes optimization?
» Scale-down or “innovate”?
Conclusions/Discussions

- How much are we willing to pay for security in lightweight schemes?
- What is the target for lightweight schemes optimization?
- Scale-down or “innovate”?
- Related-key attacks? Weak key schedules? How? Why? What?
Conclusions/Discussions

- How much are we willing to pay for security in lightweight schemes?
- What is the target for lightweight schemes optimization?
- Scale-down or “innovate”? Why?
- Related-key attacks? Weak key schedules? How? Why? What?
- Side channel? Yes? No?
Questions?

Thank you for your attention!