Modeling differential trail search

Marine Minier – Loria, CARAMBA Team

Joint work with C. Prud’homme, P. Derbrez, S. Delaune, P. Huynh, V. Mollimard

Codes by P. Huynh, S. Delaune and C. Prud’homme

Slides by M. Simard
RoadMap

• Introduction to differential cryptanalysis

• How to model that? With what?
  • Step 1
  • Step 2
  • Results

• Conclusion
Introduction

Thank you to Marc Simard for wonderful slides!
How to Cipher in symmetric key cryptography?

- Stream Ciphers

- Block Ciphers
  - Repeat rounds many many times
  - Feistel (as DES): 1 round
  - SPN (as AES): 1 round
SPN Example

Cryptography: Theory and Practice
Stinson, CRC Press, 1995

Key Schedule

Round 1
Round 2
Round 3
Final Round
Substitution-Permutation Network (SPN)

Elementary Operations

Linear Operation

Bits Permutation
XOR
S-box

Linear
Non Linear
### XOR

**Linear Operation**

<table>
<thead>
<tr>
<th>A</th>
<th>B</th>
<th>A $\oplus$ B</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
</tbody>
</table>

$\forall A \in \mathbb{F}_2$, 

$$A \oplus A = 0$$
XOR
Linear Operation

<table>
<thead>
<tr>
<th>A</th>
<th>B</th>
<th>A ⊕ B</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
</tbody>
</table>

\[
\begin{array}{ccc}
1 & \rightarrow & 1 \\
0 & \rightarrow & 0 \\
0 & \rightarrow & 1 \\
1 & \rightarrow & 0 \\
\end{array}
\]
S-box
(substitution box)

Non Linear Operation

Describes a random permutation from $\mathbb{F}_2^n$ to $\mathbb{F}_2^n$

4-bit S-box Example:

<table>
<thead>
<tr>
<th>x</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>a</th>
<th>b</th>
<th>c</th>
<th>d</th>
<th>e</th>
<th>f</th>
</tr>
</thead>
<tbody>
<tr>
<td>S[x]</td>
<td>c</td>
<td>6</td>
<td>9</td>
<td>0</td>
<td>1</td>
<td>a</td>
<td>2</td>
<td>b</td>
<td>3</td>
<td>8</td>
<td>5</td>
<td>d</td>
<td>4</td>
<td>e</td>
<td>7</td>
<td>f</td>
</tr>
</tbody>
</table>
Cryptanalysis

We look for the **plaintext**, or better the **used key**

- Linear Cryptanalysis
  - Known Plaintext Attacks
- Differential Cryptanalysis
  - Chosen Plaintext Attacks
Differential Cryptanalysis
Elementary Principle

We associated at each pair of differences $\Delta x \rightarrow \Delta y$ a probability $p$

$p (\Delta x \rightarrow \Delta y)$ is the probability to get the difference $\Delta y$ as output knowing that the input difference is $\Delta x$
Linear operations:
- $L(x) \oplus L(x') = L(x \oplus x') = L(\Delta x)$
- with probability 1!

Non-linear operations:
- S-boxes
- DDT
\[ \forall (\Delta x, \Delta y) \in (\mathbb{F}_2^n)^2 \text{ at all couples } (x, x') \text{ having difference } \Delta x, \]

\[ p(\Delta x \rightarrow \Delta y) = \frac{\# \{ (x, x') \in (\mathbb{F}_2^n)^2 \text{ with } S[x] \oplus S[x'] = \Delta y \}}{\# \{ (x, x') \in (\mathbb{F}_2^n)^2 \text{ with } x \oplus x' = \Delta x \}} = 2^n \]

Thus, \( p(0110 \rightarrow 1110) \neq 0 \).
# Differential Distribution Table (DDT)

## 4-bit S-box Example

### Differential Distribution Table

<table>
<thead>
<tr>
<th>Δy</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>a</th>
<th>b</th>
<th>c</th>
<th>d</th>
<th>e</th>
<th>f</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>16</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>2</td>
<td>4</td>
<td>0</td>
<td>4</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>6</td>
<td>2</td>
<td>2</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>3</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>4</td>
<td>2</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>4</td>
</tr>
<tr>
<td>4</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>6</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>4</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>5</td>
<td>0</td>
<td>4</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>4</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td>6</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>4</td>
<td>0</td>
<td>4</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>7</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>4</td>
</tr>
<tr>
<td>8</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>4</td>
<td>0</td>
<td>4</td>
<td>2</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>9</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>4</td>
<td>2</td>
<td>0</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>a</td>
<td>0</td>
<td>2</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>6</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>4</td>
</tr>
<tr>
<td>b</td>
<td>0</td>
<td>0</td>
<td>8</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td>c</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>6</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>d</td>
<td>0</td>
<td>4</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>4</td>
<td>2</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td>e</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>4</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>6</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>f</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>6</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>4</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>2</td>
</tr>
</tbody>
</table>

### Table obtained with:

<table>
<thead>
<tr>
<th>x</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
</tr>
</thead>
<tbody>
<tr>
<td>S[x]</td>
<td>e</td>
<td>4</td>
<td>d</td>
<td>1</td>
<td>2</td>
<td>f</td>
<td>b</td>
<td>8</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>x</th>
<th>8</th>
<th>9</th>
<th>a</th>
<th>b</th>
<th>c</th>
<th>d</th>
<th>e</th>
<th>f</th>
</tr>
</thead>
<tbody>
<tr>
<td>S[x]</td>
<td>3</td>
<td>a</td>
<td>6</td>
<td>c</td>
<td>5</td>
<td>9</td>
<td>0</td>
<td>7</td>
</tr>
</tbody>
</table>

### Diagram

\[
p(1010 \rightarrow 1000) = \frac{6}{16}
\]
Differential Trail Search
Looking for the best differential characteristic

\[ \begin{align*}
  p_{1} & : (1011 \rightarrow 010) \\
  p_{2} & : (0100 \rightarrow 0101) \\
  p_{3} & : (0100 \rightarrow 0101) \\
  p_{4} & : (0100 \rightarrow 0101) \\
  p_{5} & : (0100 \rightarrow 0101)
\end{align*} \]

Probability to obtain with an input difference: \(\text{0000 1011 0000 0000}\), last difference before the last round: \(\text{0000 0110 0000 0110}\)

\[ \frac{27}{1024} \]
Differential Trail Search

Last round

We can attack bits 5 to 8 and 13 to 16 of $K_5$ chosen such that $\Delta x = 0000 1011 0000 0000 \rightarrow 0000 0110 0000 0110$. The differential characteristic with the best proba:

$$p(0000 1011 0000 0000 \rightarrow 0000 0110 0000 0110) = \frac{27}{1024}$$

We retain the subkey with the highest number of occurrences of couples $(\tilde{y}, \tilde{y}')$ coherent with the best differential characteristic after ciphering.
What are we doing?

Know and improve existing attacks

Create new attacks

Why?

To be convinced about the security of current schemes

To elaborate new secure schemes
Cryptanalysis Problem

Modeling

Problem MILP
Mixed Integer Linear Programming

Problem SAT
Boolean Satisfiability

Problem CP
Constraint Programming

Resolution

MILP Solver
Gurobi

SAT Solver
MiniZinc

CP Solver
Choco
How to model?

Here are my slides and there are less, less…
What scheme?

The SKINNY Family of Block Ciphers and its Low-Latency Variant MANTIS
Beierle, Jean, Kölbl, Leander, Moradi, Peyrin, Sasaki, Sasdrich & Sim
CRYPTO 2016

SKINNY
2 versions: SKINNY-64 and SKINNY-128
Key size variable
32 to 56 rounds

SC: Sboxes
AC/ART: Add Constants/Add Round Tweakey
Round Tweakey is like a Subkey

How to model?
Non linear part
Each cell, apply S
Linear Part
Round function

Loria
How to model?

• Two steps
  • Step 1, abstract cell differences δx with Boolean variables Δx in {0,1}
  • Find the path with the minimal weight
    • Active S-box means ΔSx = 1!
    • because less active S-box = better proba!
  • Then go to Step 2!

• Step 2
  • Input the solutions of Step 1
  • Then try to instantiate cell differences δx to maximize the overall probability p

• How to do that?
Step 1
Step 1 (remember BOOLEAN): SC

• SC: SubCells: A 4-bit or an 8-bit S-box is applied to each cell of the state.
  • At cell level, use the DDT: $\delta_x \Rightarrow \delta_y$ with a certain probability

• For Step 1 really simple model
  • At Boolean Level: S-box is bijective!
  • Thus if $\Delta x=1$, then $\Delta y=1$ => active S-box
  • if $\Delta x=0$, then $\Delta y=0$ => inactive S-box
  • Thus Good news! No effect!

$\Delta x=\Delta y=1$

$\Delta x=\Delta y=0$
Step 1: AC and ART

- AddConstants: Round constants are XORed to the state
- AddRoundTweakey: The first and second rows of all tweakey arrays are extracted and XORed

- No differences are inserted through AC and ART (if yes, more tricky...)

- So, do nothing to model ;o)
Step 1: ShiftRows

- ShiftRows. The rows of the cipher state cell array are rotated to the right (not to the left as in the AES!)
  - By 1 for the first row
  - By 2 for the second
  - By 3 for the third

- So, at cell level: $\delta y[i+j \mod 4,j] = \delta x[i,j]$
- So, at boolean level: $\Delta y[i+j \mod 4,j] = \Delta x[i,j]$
Step 1: MixColumns

• MixColumns. Each column of the cipher internal state array is multiplied by the 4x4 binary matrix

\[
\begin{pmatrix}
1 & 0 & 1 & 1 \\
1 & 0 & 0 & 0 \\
0 & 1 & 1 & 0 \\
1 & 0 & 1 & 0 \\
\end{pmatrix}
\]

• Thus,

\[
\delta y_{0,j} = \delta x_{0,j} \oplus \delta x_{2,j} \oplus \delta x_{3,j}
\]
\[
\delta y_{1,j} = \delta x_{1,j}
\]
\[
\delta y_{2,j} = \delta x_{1,j} \oplus \delta x_{2,j}
\]
\[
\delta y_{3,j} = \delta x_{0,j} \oplus \delta x_{2,j}
\]

• Same for Boolean variables
• BUT $\oplus$ is not an available operation in the model, so...
Step 1: BUT the XOR?

Byte values

\[
\begin{align*}
\delta_A & \oplus \delta_B = \delta_C \\
\times & \oplus \times = \times \\
\times & \oplus \times = \times \\
\times & \oplus \times = \times \\
\end{align*}
\]

(white = 0, colored \(\neq 0\))

Boolean abstraction

\[
\begin{align*}
\Delta_A & \oplus \Delta_B = \Delta_C \\
\times & \oplus \times = \times \\
\times & \oplus \times = \times \\
\times & \oplus \times = \times \\
\end{align*}
\]

\[
\begin{array}{c|c|c|c|c|c|c|c|c|c}
\Delta_A & \Delta_B & \Delta_C \\
\hline
0 & 0 & 0 \\
0 & 1 & 1 \\
1 & 0 & 1 \\
1 & 1 & ? \\
\end{array}
\]

\[
\Delta_A + \Delta_B + \Delta_C \neq 1
\]
Step 2: Attacker models SK, TK1, TK2, TK3

- Tweakey framework instead key schedule

SK: no difference in the tweakey

TK1: differences in Lane 1

TK2: differences in Lane 1 and Lane 2

TK3: differences in Lane 1, 2 and 3

19/09/2022
Step 1: what we have

- 4 models we tested: 1 MILP, 1 MiniZinc, 1 CP, 1 Ad-Hoc (C++)

Step 1: 2 substeps
- First, Minimize
- Second, Enumerate
- ..\..\..\BOULOT\ASIACRYPT\TOOLS\MiniZinc-Step1\SK\SK-Step1.mzn

Lessons learnt:
- MinZinc and CP are too slow
- When you deviate from the optimal, MILP becomes too slow too
- Only the Ad-Hoc model is able to provide us what we want
- In TK1 (when differences are authorized also in the key), SKINNY-128 with 14 rounds:
  - 3 solutions for optimal value $v = 45$
  - 897 solutions for $v = v + 5 = 50$
  - 137 019 solutions for $v = v + 10 = 55$
  - 7 241 601 solutions for $v = 59$
Step 2
Where we are now

• With Step 1, we have the differential trails of minimal weights with Boolean variables

• Now, let us try to instantiate those trails to maximize the overall probability $p$

• Some trails could not be instantiated: they are called non-consistent BUT some are instantiable, we are looking for those trails

• So, take as input all the Step 1 solutions
Step 2: model each SKINNY transformation

• With $\delta x$ variables with integer domains

• SC: SubCells. An S-box

• If, there is an active S-box, model the DDT:
  • $(\delta x, \delta y, -10.\log_2 (p(\delta x \rightarrow \delta y)))$ under a table constraint
  • To discard negative value and keep only integer value

  • Objective function becomes: Minimize $\sum(-10.\log_2 (p(\delta x \rightarrow \delta y)))$
Step 2: model each SKINNY transformation

• AC and ART: no effect in differential cryptanalysis

• ShiftRows: Direct implementation, just shift to the right

• MixColumns: Direct implementation, just XOR through table constraint

• The XOR is implemented through a table constraint
Step 2: all in 1! Only CP!

Minimize $Obj_{Step2} = \sum_{r=1}^{n} \sum_{i=1}^{4} \sum_{j=1}^{4} P_{r,i,j}$ subject to $20 \times n \leq \sum_{r=1}^{n} \sum_{i=1}^{4} \sum_{j=1}^{4} P_{r,i,j} \leq \min(70 \times n, O^*)$

$\delta X_{r,i,j} \in 0..255$, $\delta S_{B, r,i,j} \in 0..255$, $Pr_{r,i,j} \in \{0, 20, \ldots, 70\}$,

$$\begin{cases} 
\delta X_{r,i,j} = 0 \land \delta S_{B, r,i,j} = 0 \land P_{r,i,j} = 0 & \text{if } \Delta X_{r,i,j} = 0 \\
\delta X_{r,i,j} \geq 1 \land \delta S_{B, r,i,j} \geq 1 \land P_{r,i,j} \geq 20 & \text{otherwise}
\end{cases}$$

$\delta S_{B, 0,j} = \delta X_{r+1,1,j}$

MixColumns First Row

MixColumns Second Row

$$\begin{cases} 
\delta S_{B, 2, (2+j)\%4} = \delta X_{r+1,2,j} & \text{if } \Delta S_{B, 1, (3+j)\%4} = 0 \\
\delta S_{B, 1, (3+j)\%4} = \delta X_{r+1,2,j} & \text{if } \Delta S_{B, 2, (2+j)\%4} = 0 \\
\delta S_{B, 1, (3+j)\%4} = \delta S_{B, 2, (2+j)\%4} & \text{if } \Delta X_{r+1,2,j} = 0 \\
\text{TABLE}(\langle \delta S_{B, 1, (3+j)\%4}, \delta S_{B, 2, (2+j)\%4}, \delta X_{r+1,2,j} \rangle : \langle \text{XOR} \rangle) & \text{otherwise}
\end{cases}$$

$\langle \text{XOR} \rangle$ encodes $\oplus$ relation and $\langle \text{SBox} \rangle$ the S-box constraint.
Results
SKINNY-64: few seconds!

Limits: full code book = $2^{64}$ thus $Pr < 2^{-64}$

<table>
<thead>
<tr>
<th></th>
<th>Nb Rounds</th>
<th>$Obj_{step1}$</th>
<th>Nb sol. Step 1</th>
<th>Step 2 time</th>
<th>Best $Pr$</th>
</tr>
</thead>
<tbody>
<tr>
<td>SK</td>
<td>7</td>
<td>26</td>
<td>2</td>
<td>1s</td>
<td>$2^{-52}$ &lt; $2^{-64}$</td>
</tr>
<tr>
<td>SK</td>
<td>8</td>
<td>36</td>
<td>17</td>
<td>1s</td>
<td>$2^{-64}$</td>
</tr>
<tr>
<td>TK1</td>
<td>10</td>
<td>23</td>
<td>1</td>
<td>1s</td>
<td>$2^{-46}$ = $2^{-64}$</td>
</tr>
<tr>
<td>TK1</td>
<td>11</td>
<td>32</td>
<td>2</td>
<td>1s</td>
<td>$2^{-64}$</td>
</tr>
<tr>
<td>TK2</td>
<td>13</td>
<td>25 $\rightarrow$ 27</td>
<td>10</td>
<td>1s</td>
<td>$2^{-55}$ &lt; $2^{-64}$</td>
</tr>
<tr>
<td>TK2</td>
<td>14</td>
<td>31</td>
<td>1</td>
<td>1s</td>
<td>$2^{-64}$</td>
</tr>
<tr>
<td>TK3</td>
<td>15</td>
<td>24 $\rightarrow$ 26</td>
<td>46</td>
<td>2s</td>
<td>$2^{-54}$ = $2^{-64}$</td>
</tr>
<tr>
<td>TK3</td>
<td>16</td>
<td>27 $\rightarrow$ 31</td>
<td>87</td>
<td>4s</td>
<td>$2^{-64}$</td>
</tr>
<tr>
<td>TK3</td>
<td>17</td>
<td>31</td>
<td>2</td>
<td>1s</td>
<td>$2^{-64}$ &lt; $2^{-64}$</td>
</tr>
</tbody>
</table>
SKINNY-128: push the limits!

Limits: full code book = $2^{128}$ thus $Pr < 2^{-128}$

<table>
<thead>
<tr>
<th>Nb Rounds</th>
<th>Obj</th>
<th>Nb sol.</th>
<th>Step 1</th>
<th>Step 2 time</th>
<th>Best $Pr$</th>
</tr>
</thead>
<tbody>
<tr>
<td>SK</td>
<td>9</td>
<td>41 → 43</td>
<td>52</td>
<td>16s</td>
<td>$2^{-86}$</td>
</tr>
<tr>
<td>SK</td>
<td>9</td>
<td>46 → 48</td>
<td>48</td>
<td>11s</td>
<td>$2^{-96}$</td>
</tr>
<tr>
<td>SK</td>
<td>11</td>
<td>51 → 52</td>
<td>15</td>
<td>4s</td>
<td>$2^{-104}$</td>
</tr>
<tr>
<td>SK</td>
<td>12</td>
<td>55 → 56</td>
<td>11</td>
<td>6s</td>
<td>$2^{-112}$</td>
</tr>
<tr>
<td>SK</td>
<td>13</td>
<td>58 → 61</td>
<td>18</td>
<td>2m27s</td>
<td>$2^{-123}$</td>
</tr>
<tr>
<td>SK</td>
<td>14</td>
<td>61 → 63</td>
<td>6</td>
<td>21s</td>
<td>$\leq 2^{-128}$</td>
</tr>
<tr>
<td>TK1</td>
<td>8</td>
<td>13 → 16</td>
<td>14</td>
<td>4s</td>
<td>$2^{-33}$</td>
</tr>
<tr>
<td>TK1</td>
<td>9</td>
<td>16 → 20</td>
<td>6</td>
<td>3s</td>
<td>$2^{-41}$</td>
</tr>
<tr>
<td>TK1</td>
<td>10</td>
<td>23 → 27</td>
<td>6</td>
<td>4s</td>
<td>$2^{-55}$</td>
</tr>
<tr>
<td>TK1</td>
<td>11</td>
<td>32 → 36</td>
<td>531</td>
<td>37s</td>
<td>$2^{-74}$</td>
</tr>
<tr>
<td>TK1</td>
<td>12</td>
<td>38 → 46</td>
<td>186 482</td>
<td>213m</td>
<td>$2^{-93}$</td>
</tr>
<tr>
<td>TK1</td>
<td>13</td>
<td>41 → 53</td>
<td>2 385 482</td>
<td>2 days</td>
<td>$2^{-106.2}$</td>
</tr>
<tr>
<td>TK1</td>
<td>14</td>
<td>45 → 59</td>
<td>11 518 612</td>
<td>20 days</td>
<td>$2^{-120}$</td>
</tr>
<tr>
<td>TK1</td>
<td>15</td>
<td>49 → 63</td>
<td>7 542 053</td>
<td>25 days</td>
<td>$2^{-128}$</td>
</tr>
<tr>
<td>TK2</td>
<td>9</td>
<td>9 → 10</td>
<td>7</td>
<td>3s</td>
<td>$2^{-297}$</td>
</tr>
<tr>
<td>TK2</td>
<td>10</td>
<td>12 → 17</td>
<td>132</td>
<td>11s</td>
<td>$2^{-34.4}$</td>
</tr>
<tr>
<td>TK2</td>
<td>11</td>
<td>16 → 25</td>
<td>4203</td>
<td>6m</td>
<td>$2^{-51.4}$</td>
</tr>
<tr>
<td>TK2</td>
<td>12</td>
<td>21 → 35</td>
<td>1 922 762</td>
<td>512m</td>
<td>$2^{-70.4}$</td>
</tr>
<tr>
<td>TK2</td>
<td>19</td>
<td>52 → 63</td>
<td>772 163</td>
<td>280m</td>
<td>$\leq 2^{-128}$</td>
</tr>
<tr>
<td>TK3</td>
<td>10</td>
<td>6</td>
<td>3</td>
<td>3s</td>
<td>$2^{-12}$</td>
</tr>
<tr>
<td>TK3</td>
<td>11</td>
<td>10</td>
<td>3</td>
<td>10s</td>
<td>$2^{-21}$</td>
</tr>
<tr>
<td>TK3</td>
<td>12</td>
<td>13 → 17</td>
<td>373</td>
<td>1h</td>
<td>$2^{-38.7}$</td>
</tr>
<tr>
<td>TK3</td>
<td>13</td>
<td>16 → 25</td>
<td>34 638</td>
<td>85h</td>
<td>$2^{-51.4}$</td>
</tr>
<tr>
<td>TK3</td>
<td>23</td>
<td>55 → 63</td>
<td>47 068</td>
<td>11h</td>
<td>$2^{-128}$</td>
</tr>
</tbody>
</table>

SK 14 rounds, Few minutes (vs 15 days before)!

But 25 days for TK1 and TK2 the holy Grail even with 128 threads and a different model...

The best TK2 solution has 15 rounds and a probability of $2^{-124.2}$ BUT maybe not optimal...

TK3 only results with 1 active byte in each lane
Conclusion

All those results were accepted to ACNS 2021
Or partly available: https://hal.archives-ouvertes.fr/hal-03040548

Part of the ANR Decrypt project

Results on AES and Rijndael [AI 20, Africacrypt 22]
Results on Boomerang attacks (SKINNY, WARP, Rijndael…) [FSE 21, FSE 22, submitted]
Results on Division property on TRIVIUM [SAC 21]
Dedicated tool: TAGADA [CP 21]
Dedicated constraint: AbstractXOR [CP 20]
And because I love that

• The best TK1 differential characteristic on 14 rounds with a probability of $2^{-120}$

Thank You for your attention!
Bibliography

**Cryptography: Theory and Practice**  
Stinson  
CRC Press, 1995

**Modern Cryptanalysis : Techniques for Advanced Code Breaking**  
Swenson  
Wiley, 2008

**The SKINNY Family of Block Ciphers and its Low-Latency Variant MANTIS**  
Beierle, Jean, Kölbl, Leander, Moradi, Peyrin, Sasaki, Sasdrich & Sim  
*CRYPTO 2016*

**MILP Modeling for (Large) S-boxes to Optimize Probability of Differential Characteristics**  
Abdelkhalek, Sasaki, Todo, Tolba & Youssef  
*ToSC 2017*