Related-Key Attack on Full-Round PICARO
SAC 2015

Anne Canteaut, Virginie Lallemand, María Naya-Plasencia

Inria, France

August 12th, 2015
Outline

1. PICARO
2. Keys Leading to Colliding Ciphertexts
3. Related-Key Attack
4. Conclusion
PICARO

Gilles Piret, Thomas Roche and Claude Carlet

Background

Objective

Build a cipher that would be easy to protect against side-channel attacks

All countermeasures have a high performance overhead

→ Start from the masking scheme, determine the parts that are hard to mask and then design the cipher accordingly
Background

Objective

Build a cipher that would be easy to protect against side-channel attacks

All countermeasures have a high performance overhead

→ Start from the masking scheme, determine the parts that are hard to mask and then design the cipher accordingly

PICARO is more efficient than AES when masked using Rivain-Prouff’s scheme
Focus on the Sbox, with special care to:

- non-linearity
- maximal differential probability
- algebraic degree
- ease to mask
Focus on the Sbox, with special care to:

- non-linearity
- maximal differential probability
- algebraic degree
- ease to mask

\[ S : GF(2^4) \times GF(2^4) \rightarrow GF(2^4) \times GF(2^4) \]
\[ (x, y) \mapsto (xy, (x^3 + 0x02)(y^3 + 0x04)) \]

Claude Carlet

*Relating Three Nonlinearity Parameters of Vectorial Functions and Building APN functions from Bent Functions, Designs, Codes and Cryptography 2011.*
Focus on the Sbox, with special care to:

- non-linearity $nl = 94$
- maximal differential probability $\delta = 4/2^8$
- algebraic degree $d = 4$
- ease to mask 4 non-linear operations in $GF(2^4)$

$$S : GF(2^4) \times GF(2^4) \rightarrow GF(2^4) \times GF(2^4)$$

$$(x, y) \mapsto (xy, (x^3 + 0x02)(y^3 + 0x04))$$

Claude Carlet

*Relating Three Nonlinearity Parameters of Vectorial Functions and Building APN functions from Bent Functions, Design, Codes and Cryptography 2011.*
Focus on the Sbox, with special care to:

- non-linearity $nl = 94$
- maximal differential probability $\delta = 4/2^8$
- algebraic degree $d = 4$
- ease to mask 4 non-linear operations in $GF(2^4)$

$$S : GF(2^4) \times GF(2^4) \rightarrow GF(2^4) \times GF(2^4)$$

$$(x, y) \mapsto (xy, (x^3 + 0x02)(y^3 + 0x04))$$

Claude Carlet

*Relating Three Nonlinearity Parameters of Vectorial Functions and Building APN functions from Bent Functions,*

 Designs, Codes and Cryptography 2011.

Non-Bijective
Round Function: Possible Threat

Possible to have only 1 round active out of 2 with only 1 active Sbox
Need to ensure a minimum number of active Sboxes per round
Round Function: Possible Threat

- Possible to have **only 1 round active out of 2** with **only 1 active Sbox**
- Need to ensure a **minimum** number of active Sboxes per round
Round Function

Solution Proposed: Expansion and Compression layers

- Expansion from 8 bytes to $8+6$ bytes
- Key addition
- Sbox layer
- Compression from $8+6$ bytes back to 8 bytes

MDS code $[8+6, 8, 7]$ of generator matrix:

$$G = \begin{pmatrix} \text{Id}_8 & \mathcal{G} \end{pmatrix}$$

with $\mathcal{G} = \begin{pmatrix}
01 & 01 & 0A & 01 & 09 & 0C \\
05 & 01 & 01 & 0A & 01 & 09 \\
06 & 05 & 01 & 01 & 0A & 01 \\
0C & 06 & 05 & 01 & 01 & 0A \\
09 & 0C & 06 & 05 & 01 & 01 \\
01 & 09 & 0C & 06 & 05 & 01 \\
0A & 01 & 09 & 0C & 06 & 05 \\
01 & 0A & 01 & 09 & 0C & 06
\end{pmatrix}$
Keys Leading to Colliding Ciphertexts
Preliminary Remarks

Sbox Property

Any entering difference has a probability of $2^{-7}$ of being cancelled
### Preliminary Remarks

<table>
<thead>
<tr>
<th><strong>Sbox Property</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Any entering difference has a probability of $2^{-7}$ of being cancelled</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Round Function Property</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Key addition is realised after the expansion and just before the Sbox layer</td>
</tr>
</tbody>
</table>
Preliminary Remarks

Sbox Property
Any entering difference has a probability of $2^{-7}$ of being cancelled.

Round Function Property
Key addition is realised after the expansion and just before the Sbox layer.

→ Main Idea: Introduce a difference in the key and cancel it immediately.
Preliminary Remarks

Sbox Property

Any entering difference has a probability of $2^{-7}$ of being cancelled.

Round Function Property

Key addition is realised after the expansion and just before the Sbox layer.

→ Main Idea: Introduce a difference in the key and cancel it immediately.
Preliminary Remarks

**Sbox Property**

Any entering difference has a probability of $2^{-7}$ of being cancelled.

**Round Function Property**

Key addition is realised after the expansion and just before the Sbox layer.

→ Main Idea: Introduce a difference in the key and cancel it immediately.
Preliminary Remarks

**Sbox Property**
Any entering difference has a probability of $2^{-7}$ of being cancelled

**Round Function Property**
Key addition is realised after the expansion and just before the Sbox layer

→ Main Idea: Introduce a difference in the key and cancel it immediately
Preliminary Remarks

Sbox Property

Any entering difference has a probability of $2^{-7}$ of being cancelled.

Round Function Property

Key addition is realised after the expansion and just before the Sbox layer.

→ Main Idea: Introduce a difference in the key and cancel it immediately.

How far can we go?
Question:
Can we find a master key difference $\Delta$ such that for random $(P, K)$ we have with high probability $E_K(P) = E_{K \oplus \Delta}(P)$?

To cancel all the key differences, we can afford a maximum of $s$ Sbox cancellations, with $s$ satisfying:

$$2^{-7s} > 2^{-128}$$
Keys Leading to Colliding Ciphertexts

Question:
Can we find a master key difference $\Delta$ such that for random $(P, K)$ we have with high probability $E_K(P) = E_{K \oplus \Delta}(P)$?

To cancel all the key differences, we can afford a maximum of $s$ Sbox cancellations, with $s$ satisfying:

$$2^{-7s} > 2^{-128}$$

→ Find a Master Key difference that activates less than 18 bytes in the subkeys
Key Schedule

- Master key $K$ of 128 bits
- 12 round-keys $k^i$ of 112 bits

\[
\begin{align*}
\kappa^1 &= K \\
\kappa^i &= T(\kappa^{i-1}) \gg \theta(i) \quad \text{for } i = 2, \ldots, 12
\end{align*}
\]

\[
\begin{pmatrix}
T(K)^{(1)} \\
T(K)^{(2)} \\
T(K)^{(3)} \\
T(K)^{(4)}
\end{pmatrix} = \begin{pmatrix}
0 & 1 & 1 & 1 \\
1 & 0 & 1 & 1 \\
1 & 1 & 0 & 1 \\
1 & 1 & 1 & 0
\end{pmatrix} \times \begin{pmatrix}
K^{(1)} \\
K^{(2)} \\
K^{(3)} \\
K^{(4)}
\end{pmatrix}
\]

where $\theta$ is defined by:

<table>
<thead>
<tr>
<th>$i$</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>10</th>
<th>11</th>
<th>12</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\theta(i)$</td>
<td>1</td>
<td>15</td>
<td>1</td>
<td>15</td>
<td>1</td>
<td>52</td>
<td>1</td>
<td>15</td>
<td>1</td>
<td>15</td>
<td>1</td>
</tr>
</tbody>
</table>

$k^i =$ first 112 bits of $\kappa^i$
Key Schedule

\[ \kappa^i = T(\kappa^{i-1}) \gg \theta(i) \]
Key Schedule

\[ \kappa_i = T(\kappa_{i-1}^{i-1}) \gg \theta(i) \]
Keys Leading to Colliding Ciphertexts

Key Schedule

\[ \kappa^i = T(\kappa^{i-1}) \gg \theta(i) \]
Key Schedule

\[ \kappa^i = T(\kappa^{i-1}) \gg \theta(i) \]
\[ \kappa_i = T(\kappa_{i-1}) \gg \theta(i) \]
Key Schedule

\[
\kappa_i = T(\kappa_{i-1}) \gg \theta(i)
\]
Key Schedule

\[ \kappa^i = T(\kappa^{i-1}) \gg \theta(i) \]
Key Schedule

\[ \kappa^i = T(\kappa^{i-1}) \gg \theta(i) \]
Keys Leading to Colliding Ciphertexts

Key Schedule totally linear over $GF(2) \iff$ linear code

First approximation: look for low-weight codewords (in bits)
Keys Leading to Colliding Ciphertexts

Key Schedule totally linear over $GF(2) \iff$ linear code

First approximation: look for low-weight codewords (in bits)

Remark: Each master key bit flipped results in a minimum of 4 bits flipped in the odd round subkeys ($k_1, k_3, k_5, k_7, k_9, k_{11}$)

→ Codewords of weight $\leq 18$ obtained by exhausting all master keys of weight $\leq 4$
Keys Leading to Colliding Ciphertexts

Minimum distance 18

8 words/master key differences reaching that minimum:

<table>
<thead>
<tr>
<th>config.</th>
<th>$K$</th>
<th>$k^1$</th>
<th>$k^2$</th>
<th>$k^3$</th>
<th>$k^4$</th>
<th>$k^5$</th>
<th>$k^6$</th>
<th>$k^7$</th>
<th>$k^8$</th>
<th>$k^9$</th>
<th>$k^{10}$</th>
<th>$k^{11}$</th>
<th>$k^{12}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>27, 123</td>
<td>27</td>
<td>28</td>
<td>11, 43</td>
<td>12, 44</td>
<td>27, 59</td>
<td>28, 60</td>
<td>80</td>
<td>81</td>
<td>0, 96</td>
<td>1, 97</td>
<td>16</td>
<td>17</td>
</tr>
<tr>
<td>2</td>
<td>28, 124</td>
<td>28</td>
<td>29</td>
<td>12, 44</td>
<td>13, 45</td>
<td>28, 60</td>
<td>29, 61</td>
<td>81</td>
<td>82</td>
<td>1, 97</td>
<td>2, 98</td>
<td>17</td>
<td>18</td>
</tr>
<tr>
<td>3</td>
<td>29, 125</td>
<td>29</td>
<td>30</td>
<td>13, 45</td>
<td>14, 46</td>
<td>29, 61</td>
<td>30, 62</td>
<td>82</td>
<td>83</td>
<td>2, 98</td>
<td>3, 99</td>
<td>18</td>
<td>19</td>
</tr>
<tr>
<td>4</td>
<td>30, 126</td>
<td>30</td>
<td>31</td>
<td>14, 46</td>
<td>15, 47</td>
<td>30, 62</td>
<td>31, 63</td>
<td>83</td>
<td>84</td>
<td>3, 99</td>
<td>4, 100</td>
<td>19</td>
<td>20</td>
</tr>
<tr>
<td>5</td>
<td>91, 123</td>
<td>91</td>
<td>92</td>
<td>11, 107</td>
<td>12, 108</td>
<td>27</td>
<td>28</td>
<td>48, 80</td>
<td>49, 81</td>
<td>64, 96</td>
<td>65, 97</td>
<td>80</td>
<td>81</td>
</tr>
<tr>
<td>6</td>
<td>92, 124</td>
<td>92</td>
<td>93</td>
<td>12, 108</td>
<td>13, 109</td>
<td>28</td>
<td>29</td>
<td>49, 81</td>
<td>50, 82</td>
<td>65, 97</td>
<td>66, 98</td>
<td>81</td>
<td>82</td>
</tr>
<tr>
<td>7</td>
<td>93, 125</td>
<td>93</td>
<td>94</td>
<td>13, 109</td>
<td>14, 110</td>
<td>29</td>
<td>30</td>
<td>50, 82</td>
<td>51, 83</td>
<td>66, 98</td>
<td>67, 99</td>
<td>82</td>
<td>83</td>
</tr>
<tr>
<td>8</td>
<td>94, 126</td>
<td>94</td>
<td>95</td>
<td>14, 110</td>
<td>15, 111</td>
<td>30</td>
<td>31</td>
<td>51, 83</td>
<td>52, 84</td>
<td>67, 99</td>
<td>68, 100</td>
<td>83</td>
<td>84</td>
</tr>
</tbody>
</table>

Byte distance: minimum of 18 active bytes
30 words/master key differences reaching that minimum

$\rightarrow$ Ciphertexts collide with probability $2^{-18 \times 7} = 2^{-126}$
Distinguisher
Related-Key Attack
Idea: Mounting a 2R-attack
For a plaintext and a pair of keys following the characteristic, only $2^7 \times a_{11}$ differences are possible out of $2^{64}$ for the right half of the ciphertext.
Ciphertext Filter

For a plaintext and a pair of keys following the characteristic, only $2^{7 \times a_{11}}$ differences are possible out of $2^{64}$ for the right half of the ciphertext.
Properties

Compression Function Property (for values and differences)

The knowledge of the output of the compression function and of any 6 bytes of the input is sufficient to uniquely determine all input bits.
Properties

Compression Function Property (for values and differences)

The knowledge of the output of the compression function and of any 6 bytes of the input is sufficient to uniquely determine all input bits.
Properties

Compression Function Property (for values and differences)

The knowledge of the output of the compression function and of any 6 bytes of the input is sufficient to uniquely determine all input bits.
Properties

Compression Function Property (for values and differences)

The knowledge of the output of the compression function and of any 6 bytes of the input is sufficient to uniquely determine all input bits.
Properties

Compression Function Property (for values and differences)

The knowledge of the output of the compression function and of any 6 bytes of the input is sufficient to uniquely determine all input bits

![Diagram showing the compression function property for related-key attacks on PICARO]
Basic Attack

1. Ask for $2^{7a_1 \to a_{10}}$ messages encrypted with both $K$ and $K \oplus \Delta$
Basic Attack

1. Ask for $2^{7a_1 \rightarrow a_{10}}$ messages encrypted with both $K$ and $K \oplus \Delta$

2. Filter out the pairs without the correct ciphertext difference

filter $2^{-64+7a_{11}}$
Basic Attack

1. Ask for $2^{7a_1 \rightarrow a_{10}}$ messages encrypted with both $K$ and $K \oplus \Delta$

2. Filter out the pairs without the correct ciphertext difference

3. Guess 6-byte differences and deduce the whole $Comp$ input difference
**Basic Attack**

1. Ask for $2^{7a_1 \rightarrow a_{10}}$ messages encrypted with both $K$ and $K \oplus \Delta$

2. Filter out the pairs without the correct ciphertext difference

3. Guess 6-byte differences and deduce whole $Comp$ input difference
Basic Attack

1. Ask for $2^{7a_1 \rightarrow a_{10}}$ messages encrypted with both $K$ and $K \oplus \Delta$.
2. Filter out the pairs without the correct ciphertext difference.
3. Guess 6-byte differences and deduce whole $Comp$ input difference.
Basic Attack

1. Ask for $2^{7a_1 \rightarrow a_{10}}$ messages encrypted with both $K$ and $K \oplus \Delta$
2. Filter out the pairs without the correct ciphertext difference
3. Guess 6-byte differences and deduce whole $Comp$ input difference
Basic Attack

1. Ask for $2^{7a_1\rightarrow a_{10}}$ messages encrypted with both $K$ and $K \oplus \Delta$

2. Filter out the pairs without the correct ciphertext difference

3. Guess 6-byte differences and deduce whole $Comp$ input difference
Basic Attack

1. Ask for $2^{7a_1 \rightarrow a_{10}}$ messages encrypted with both $K$ and $K \oplus \Delta$
2. Filter out the pairs without the correct ciphertext difference
3. Guess 6-byte differences and deduce whole Comp input difference
4. Compute expansion function in differences and add $\Delta$
Basic Attack

1. Ask for $2^{7a_1 \rightarrow a_{10}}$ messages encrypted with both $K$ and $K \oplus \Delta$
2. Filter out the pairs without the correct ciphertext difference
3. Guess 6-byte differences and deduce whole $Comp$ input difference
4. Compute expansion function in differences and add $\Delta$
5. Check the DDT and deduce values
Related-Key Attack

Basic Attack

1. Ask for $2^{7a_1 \rightarrow a_{10}}$ messages encrypted with both $K$ and $K \oplus \Delta$
2. Filter out the pairs without the correct ciphertext difference
3. Guess 6-byte differences and deduce whole $Comp$ input difference
4. Compute expansion function in differences and add $\Delta$
5. Check the DDT and deduce values
**Basic Attack**

1. Ask for $2^{7a_1 \rightarrow a_{10}}$ messages encrypted with both $K$ and $K \oplus \Delta$
2. Filter out the pairs without the correct ciphertext difference
3. Guess 6-byte differences and deduce whole $Comp$ input difference
4. Compute expansion function in differences and add $\Delta$
5. Check the DDT and deduce values
6. With ciphertext value, deduce $k^{12}$
Basic Attack

1. Ask for $2^{7a_1 \rightarrow a_{10}}$ messages encrypted with both $K$ and $K \oplus \Delta$
2. Filter out the pairs without the correct ciphertext difference
3. Guess 6-byte differences and deduce whole Comp input difference
4. Compute expansion function in differences and add $\Delta$
5. Check the DDT and deduce values
6. With ciphertext value, deduce $k^{12}$
7. Use previous rounds to filter out keys
Basic Attack

1. Ask for $2^{7a_1 \rightarrow a_{10}}$ messages encrypted with both $K$ and $K \oplus \Delta$
2. Filter out the pairs without the correct ciphertext difference
3. Guess 6-byte differences and deduce whole Comp input difference
4. Compute expansion function in differences and add $\Delta$
5. Check the DDT and deduce values
6. With ciphertext value, deduce $k_{12}^{12}$
7. Use previous rounds to filter out keys
Improvement: Structure-like Technique

Let the first round-key difference spreads freely and cancel it with a plaintext difference introduced in right hand plaintext half

Encrypt the $2^{8a_1}$ messages $P \oplus \delta$ under the keys $K$ and under $K \oplus \Delta$ where the $\delta$ covers all the possible differences at the output of the compression function
**Related-Key Attack**

**Improvement: Structure-like Technique**

Let the first round-key difference spreads freely and cancel it with a plaintext difference introduced in right hand plaintext half.

Encrypt the $2^{8a_1}$ messages $P \oplus \delta$ under the keys $K$ and under $K \oplus \Delta$ where the $\delta$ covers all the possible differences at the output of the compression function.

\[ 2^{8a_1} + 2^{8a_1} = 2^{8a_1+1} \] encryptions
give \[ 2^{8a_1} \times 2^{8a_1} \times 2^{-8a_1} = 2^{8a_1} \] pairs that pass the first round conditions

\[ \rightarrow 2^{7 \times a_2 \rightarrow 10 + 1} \] encryptions in total (vs $2^{7 \times a_1 \rightarrow 10 + 1}$)
Choosing Parameters

Memory:

\[ 2^{8 \times a_1 + 1} \]

Data:

\[ 2^{7 \times a_2 \rightarrow 10 + 1} \]

Time:

\[ 2^{7 \times a_2 \rightarrow 10 + 1} + 2^{7 \times a_1 \rightarrow 11} - 18.58 \]

<table>
<thead>
<tr>
<th>( a_2 \rightarrow 10 )</th>
<th>( a_1 \rightarrow 11 )</th>
<th>Memory</th>
<th>Data</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>14</td>
<td>18</td>
<td>( 2^{17} )</td>
<td>( 2^{99} )</td>
<td>( 2^{107.4} )</td>
</tr>
<tr>
<td>15</td>
<td>17</td>
<td>( 2^{9} )</td>
<td>( 2^{106} )</td>
<td>( 2^{106} )</td>
</tr>
</tbody>
</table>
Conclusion
While the designers targeted resistance against related-key attacks, we have shown a full-round cryptanalysis of PICARO under this model.

The main weakness exploited here (and one that should be fixed) is the small diffusion of its key schedule, which turns out to be devastating when combined with the non-bijective Sboxes.
Thank you for your attention