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

$$\begin{tikzcd} P \arrow[r, "E_K"] \arrow[r, bend right, "E_{K\oplus\Delta}"'] & C \end{tikzcd}$$

PICARO

Gilles Piret, Thomas Roche and Claude Carlet
PICARO - A Block Cipher Allowing Efficient Higher-Order Side-Channel Resistance,
ACNS 2012.

Background

Objective

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

All countermeasures have a high performance overhead

$\rightarrow$ 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

$\rightarrow$ 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

PICARO

Focus on the Sbox, with special care to:

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

PICARO

Focus on the Sbox, with special care to:

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

$$\begin{aligned} S : GF(2^4) \times GF(2^4) &\rightarrow GF(2^4) \times GF(2^4) \\ (x, y) &\mapsto (xy, (x^3 + \mathtt{0x02})(y^3 + \mathtt{0x04})) \end{aligned}$$

Claude Carlet
Relating Three Nonlinearity Parameters of Vectorial Functions and Building APN functions from Bent Functions,
Designs, Codes and Cryptography 2011.

PICARO

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 $GF(2^4)$

$$\begin{aligned} S : GF(2^4) \times GF(2^4) &\rightarrow GF(2^4) \times GF(2^4) \\ (x, y) &\mapsto (xy, (x^3 + \mathtt{0x02})(y^3 + \mathtt{0x04})) \end{aligned}$$

Claude Carlet
Relating Three Nonlinearity Parameters of Vectorial Functions and Building APN functions from Bent Functions,
Designs, Codes and Cryptography 2011.

PICARO

Focus on the Sbox, with special care to:

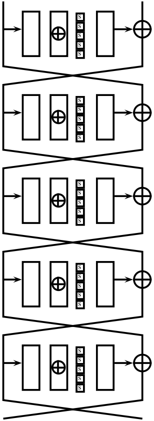
- non-linearity $nl = 94$
- maximal differential probability $\delta = 4/2^8$
- algebraic degree $d = 4$
- ease to mask 4 non-linear operations in $GF(2^4)$

$$
\begin{aligned}
S : GF(2^4) \times GF(2^4) &\rightarrow GF(2^4) \times GF(2^4) \\
(x, y) &\mapsto (xy, (x^3 + \mathtt{0x02})(y^3 + \mathtt{0x04}))
\end{aligned}
$$

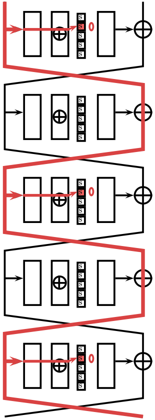
Claude Carlet
Relating Three Nonlinearity Parameters of Vectorial Functions and Building APN functions from Bent Functions,
Designs, Codes and Cryptography 2011.

Non-Bijective

Round Function: Possible Threat



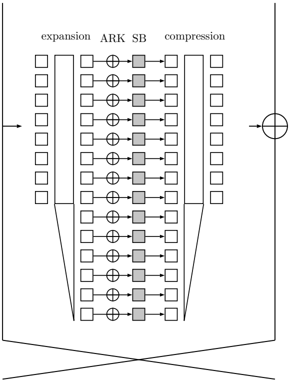
Round Function: Possible Threat



- 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



12 rounds

- 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:

$$G = \begin{pmatrix} Id_8 & \mathscr{G} \end{pmatrix}$$

with $\mathscr{G} = \begin{pmatrix} \texttt{01} & \texttt{01} & \texttt{0A} & \texttt{01} & \texttt{09} & \texttt{0C} \\ \texttt{05} & \texttt{01} & \texttt{01} & \texttt{0A} & \texttt{01} & \texttt{09} \\ \texttt{06} & \texttt{05} & \texttt{01} & \texttt{01} & \texttt{0A} & \texttt{01} \\ \texttt{0C} & \texttt{06} & \texttt{05} & \texttt{01} & \texttt{01} & \texttt{0A} \\ \texttt{09} & \texttt{0C} & \texttt{06} & \texttt{05} & \texttt{01} & \texttt{01} \\ \texttt{01} & \texttt{09} & \texttt{0C} & \texttt{06} & \texttt{05} & \texttt{01} \\ \texttt{0A} & \texttt{01} & \texttt{09} & \texttt{0C} & \texttt{06} & \texttt{05} \\ \texttt{01} & \texttt{0A} & \texttt{01} & \texttt{09} & \texttt{0C} & \texttt{06} \end{pmatrix}$

Keys Leading to Colliding Ciphertexts

Preliminary Remarks

Sbox Property

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

Preliminary Remarks

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

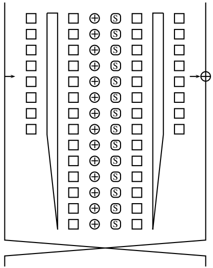
Preliminary Remarks

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

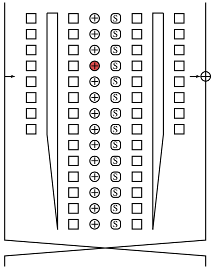
Preliminary Remarks

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

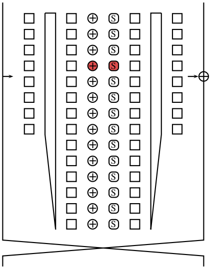
Preliminary Remarks

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

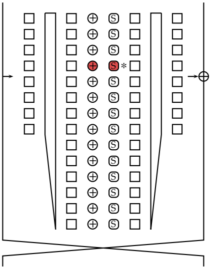
Preliminary Remarks

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

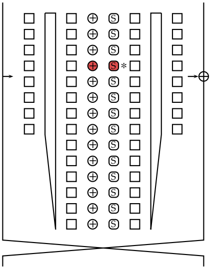
Preliminary Remarks

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?

Keys Leading to Colliding Ciphertexts

Question:
Can we find a master key difference Δ 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 Δ 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:

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

$\rightarrow$ 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

$$\begin{cases} \kappa^1 = K \\ \kappa^i = T(\kappa^{i-1}) \ggg \theta(i) & \text{for } i = 2, \cdots, 12 \end{cases}$$

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

where θ is defined by:

i	2	3	4	5	6	7	8	9	10	11	12
$\theta(i)$	1	15	1	15	1	52	1	15	1	15	1

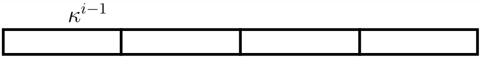
k^i = first 112 bits of κ^i

Key Schedule

$$\kappa^i = T(\kappa^{i-1}) \ggg \theta(i)$$

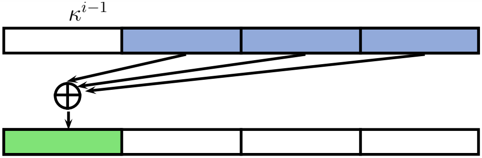
Key Schedule

$$\kappa^i = T(\kappa^{i-1}) \ggg \theta(i)$$



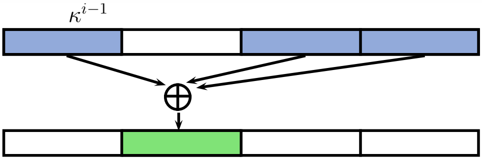
Key Schedule

$$\kappa^{i} = T(\kappa^{i-1}) \ggg \theta(i)$$



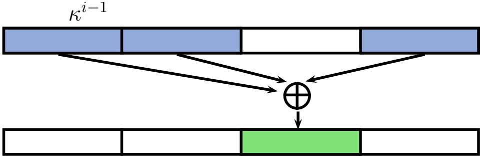
Key Schedule

$$\kappa^i = T(\kappa^{i-1}) \ggg \theta(i)$$



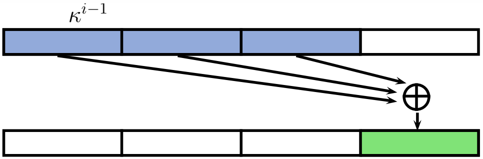
Key Schedule

$$\kappa^i = T(\kappa^{i-1}) \ggg \theta(i)$$



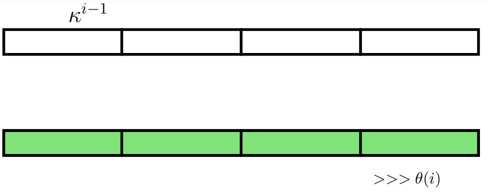
Key Schedule

$\kappa^i = T(\kappa^{i-1}) \ggg \theta(i)$



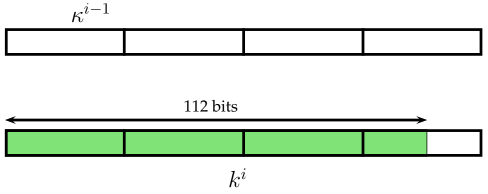
Key Schedule

$$\kappa^i = T(\kappa^{i-1}) \ggg \theta(i)$$



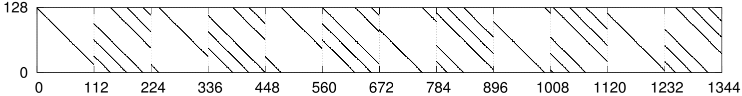
Key Schedule

$$\kappa^i = T(\kappa^{i-1}) \ggg \theta(i)$$



Keys Leading to Colliding Ciphertexts

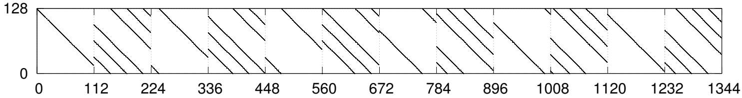
Key Schedule totally linear over $GF(2)$ $\Leftrightarrow$ linear code



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

Keys Leading to Colliding Ciphertexts

Key Schedule totally linear over $GF(2)$ $\Leftrightarrow$ 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})

$\rightarrow$**Codewords of weight** ≤ 18 **obtained by exhausting all master keys of weight** ≤ 4

Keys Leading to Colliding Ciphertexts

Minimum distance 18

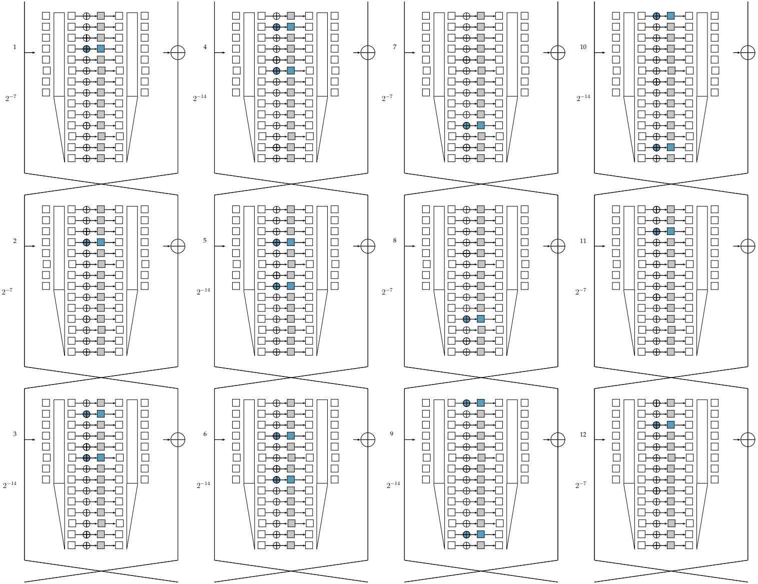
8 words/master key differences reaching that minimum:

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

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

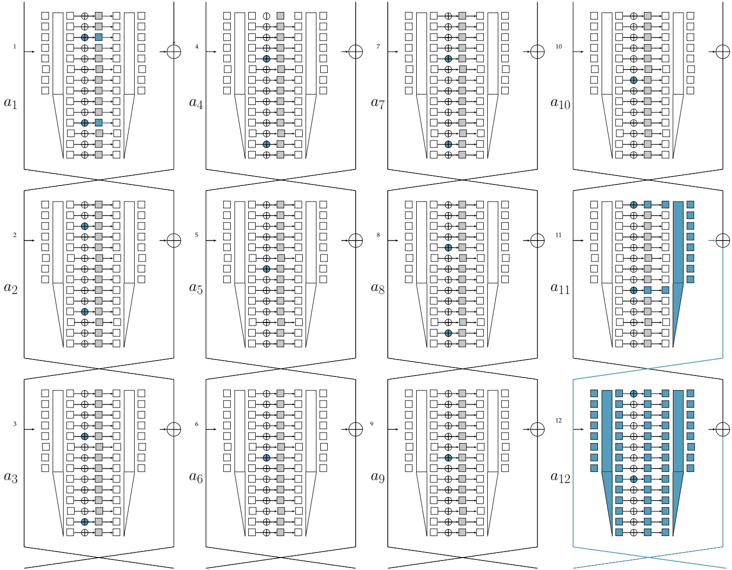
$\rightarrow$ Ciphertexts collide with probability $2^{-18\times 7} = 2^{-126}$

Distinguisher



Related-Key Attack

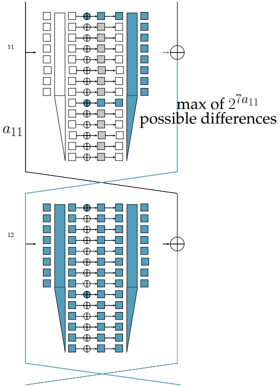
Idea: Mounting a 2R-attack



Properties

Ciphertext Filter

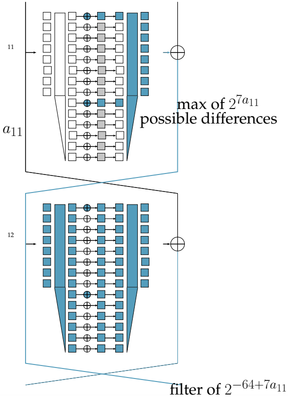
For a plaintext and a pair of keys following the characteristic, only $2^{7\times a_{11}}$ differences are possible out of 2^{64} for the right half of the ciphertext



Properties

Ciphertext Filter

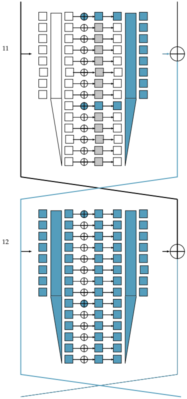
For a plaintext and a pair of keys following the characteristic, only $2^{7 \times a_{11}}$ differences are possible out of 2^{64} for the right half of the ciphertext



Properties

Compression Function Property (for values and differences)

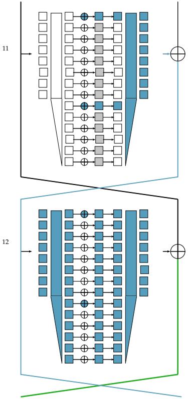
The knowledge of the output of the compression function and of any 6 bytes of the input is sufficient to uniquely determine all input bits



Properties

Compression Function Property (for values and differences)

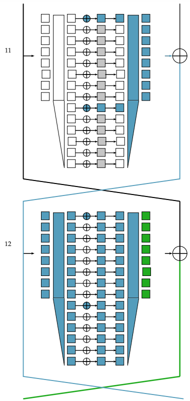
The knowledge of the output of the compression function and of any 6 bytes of the input is sufficient to uniquely determine all input bits



Properties

Compression Function Property (for values and differences)

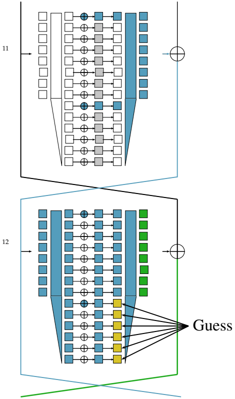
The knowledge of the output of the compression function and of any 6 bytes of the input is sufficient to uniquely determine all input bits



Properties

Compression Function Property (for values and differences)

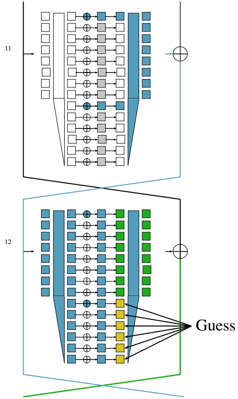
The knowledge of the output of the compression function and of any 6 bytes of the input is sufficient to uniquely determine all input bits



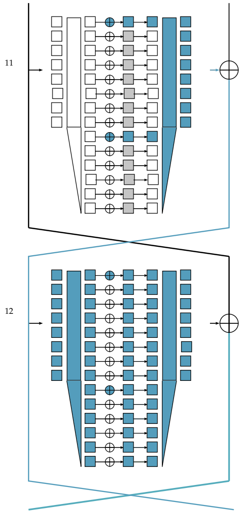
Properties

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

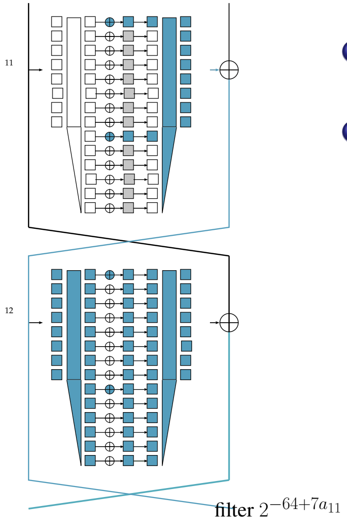


Basic Attack



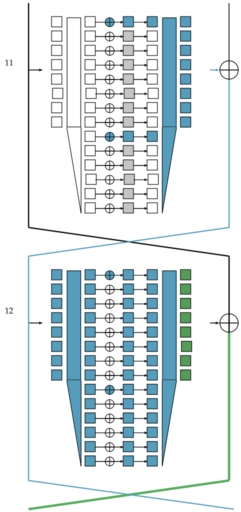
1. Ask for $2^{7a_1 \to a_{10}}$ messages encrypted with both K and $K \oplus \Delta$

Basic Attack



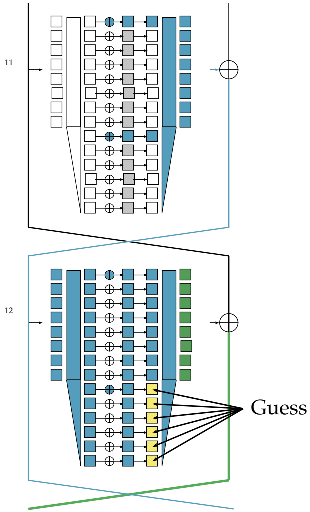
1. Ask for $2^{7a_1 \to a_{10}}$ messages encrypted with both K and $K \oplus \Delta$
2. Filter out the pairs without the correct ciphertext difference

Basic Attack



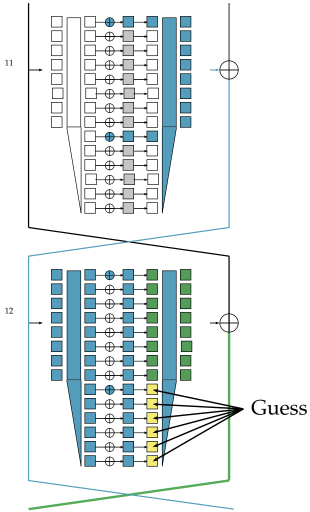
1. Ask for $2^{7a_1 \to a_{10}}$ messages encrypted with both K and $K \oplus \Delta$
2. Filter out the pairs without the correct ciphertext difference
3. Guess 6-byte differences and deduce whole *Comp* input difference

Basic Attack



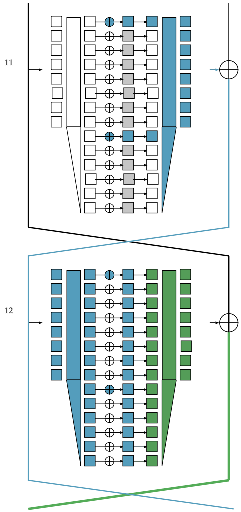
1. Ask for $2^{7a_1 \to a_{10}}$ messages encrypted with both K and $K \oplus \Delta$
2. Filter out the pairs without the correct ciphertext difference
3. Guess 6-byte differences and deduce whole *Comp* input difference

Basic Attack



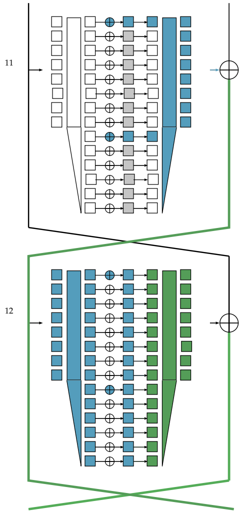
1. Ask for $2^{7a_1 \to a_{10}}$ messages encrypted with both K and $K \oplus \Delta$
2. Filter out the pairs without the correct ciphertext difference
3. Guess 6-byte differences and deduce whole *Comp* input difference

Basic Attack



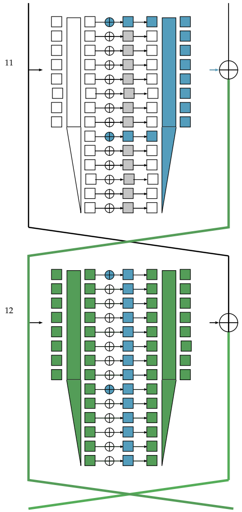
1. Ask for $2^{7a_1 \to a_{10}}$ messages encrypted with both K and $K \oplus \Delta$
2. Filter out the pairs without the correct ciphertext difference
3. Guess 6-byte differences and deduce whole *Comp* input difference

Basic Attack



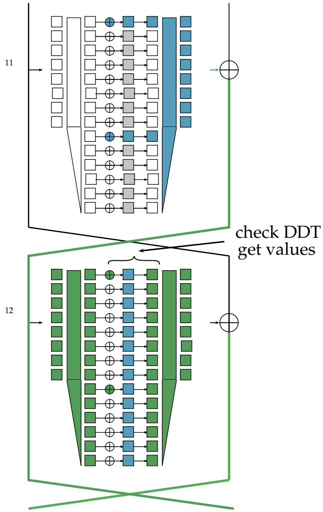
1. Ask for $2^{7a_1 \to a_{10}}$ messages encrypted with both K and $K \oplus \Delta$
2. Filter out the pairs without the correct ciphertext difference
3. Guess 6-byte differences and deduce whole *Comp* input difference

Basic Attack



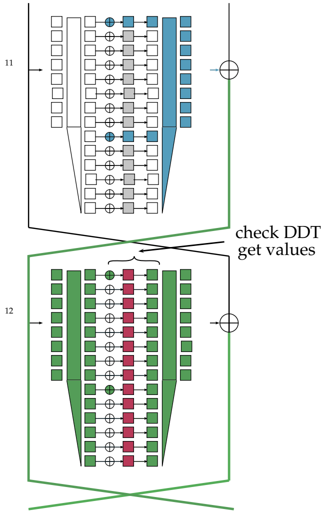
1. Ask for $2^{7a_1 \to a_{10}}$ messages encrypted with both K and $K \oplus \Delta$
2. Filter out the pairs without the correct ciphertext difference
3. Guess 6-byte differences and deduce whole *Comp* input difference
4. Compute expansion function in differences and add Δ

Basic Attack



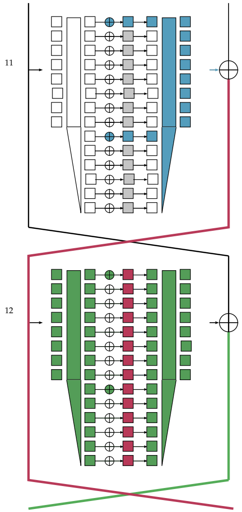
1. Ask for $2^{7a_1 \to a_{10}}$ messages encrypted with both K and $K \oplus \Delta$
2. Filter out the pairs without the correct ciphertext difference
3. Guess 6-byte differences and deduce whole *Comp* input difference
4. Compute expansion function in differences and add Δ
5. Check the DDT and deduce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

Basic Attack



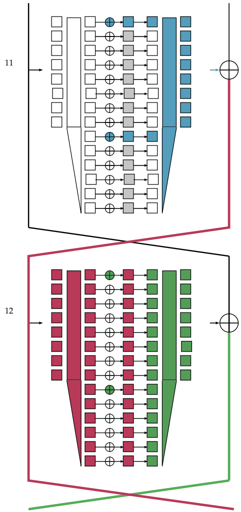
1. Ask for $2^{7a_1 \to a_{10}}$ messages encrypted with both K and $K \oplus \Delta$
2. Filter out the pairs without the correct ciphertext difference
3. Guess 6-byte differences and deduce whole *Comp* input difference
4. Compute expansion function in differences and add Δ
5. Check the DDT and deduce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

Basic Attack



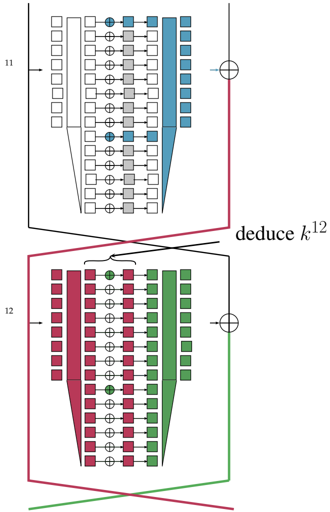
1. Ask for $2^{7a_1 \to a_{10}}$ messages encrypted with both K and $K \oplus \Delta$
2. Filter out the pairs without the correct ciphertext difference
3. Guess 6-byte differences and deduce whole *Comp* input difference
4. Compute expansion function in differences and add Δ
5. Check the DDT and deduce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

Basic Attack



1. Ask for $2^{7a_1 \to a_{10}}$ 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 Δ
5. Check the DDT and deduce values
6. With ciphertext value, deduce k^{12}
7. Use previous rounds to filter out keys

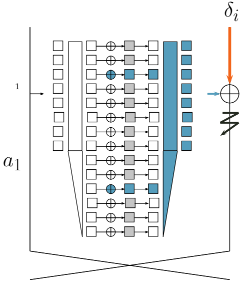
Basic Attack



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 Δ
5. Check the DDT and deduce values
6. With ciphertext value, deduce k^{12}
7. Use previous rounds to filter out keys

Improvement: Structure-like Technique

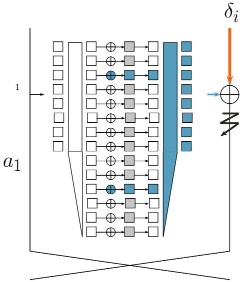
Let the first round-key difference spreads freely and cancel it with a plaintext difference introduced in right hand plaintext half



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

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 δ 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

$$\rightarrow 2^{7 \times a_{2\rightarrow 10}+1} \text{ encryptions in total (vs } 2^{7 \times a_{1\rightarrow 10}+1} \text{)}$$

Choosing Parameters

Memory:

$$2^{8\times a_1+1}$$

Data:

$$2^{7\times a_{2\to 10}+1}$$

Time:

$$2^{7\times a_{2\to 10}+1}+2^{7\times a_{1\to 11}-18.58}$$

$a_{2\to 10}$	$a_{1\to 11}$	Memory	Data	Time
14	18	2^{17}	2^{99}	$2^{107.4}$
15	17	2^{9}	2^{106}	2^{106}

Conclusion

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