RSAConference2016

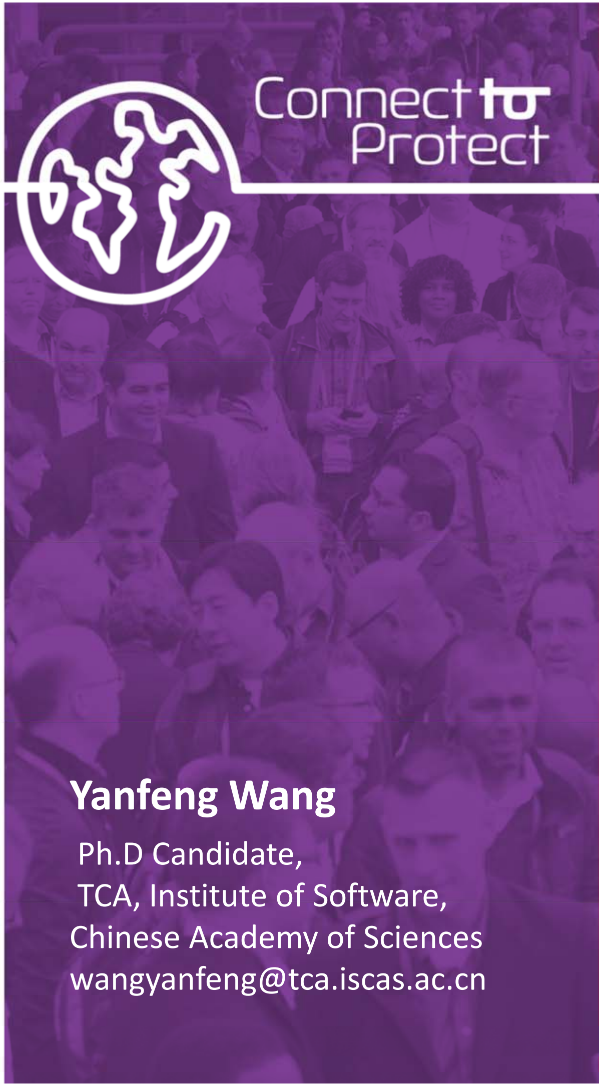
San Francisco | February 29 – March 4 | Moscone Center

SESSION ID: CRYP-F01

New Observations On Piccolo Block Cipher

Yanfeng Wang and Wenling Wu

Connect to Protect



Yanfeng Wang

Ph.D Candidate,
TCA, Institute of Software,
Chinese Academy of Sciences
wangyanfeng@tca.iscas.ac.cn

#RSAC

Outline

- Introduction
- Description of Piccolo
- Linear-Reflection Weak Keys of Piccolo
- New Observations on Piccolo-128
- Conclusion

Outline

- **Introduction**
- Description of Piccolo
- Linear-Reflection Weak Keys of Piccolo
- New Observations on Piccolo-128
- Conclusion

Introduction

- New lightweight block ciphers with very simple key-schedules or even without key-schedule, have been proposed.
- Avoiding MITM(Meet-in-the-Middle) attacks, related-key differential attack and key bits leakage are three main goals in the design of key schedules.
- However, the choice of round constants makes no influence on the security of block ciphers against the above three attacks.

Introduction

- Related attacks: slide cryptanalysis, probabilistic slide cryptanalysis(FSE 2014) and invariant subspace attack(CRYPTO 2011).
- All attacks can be prevented by a careful choice of round constants.
- In this paper, we take the Piccolo block cipher as a target cipher to reveal some new design principles on round constants.

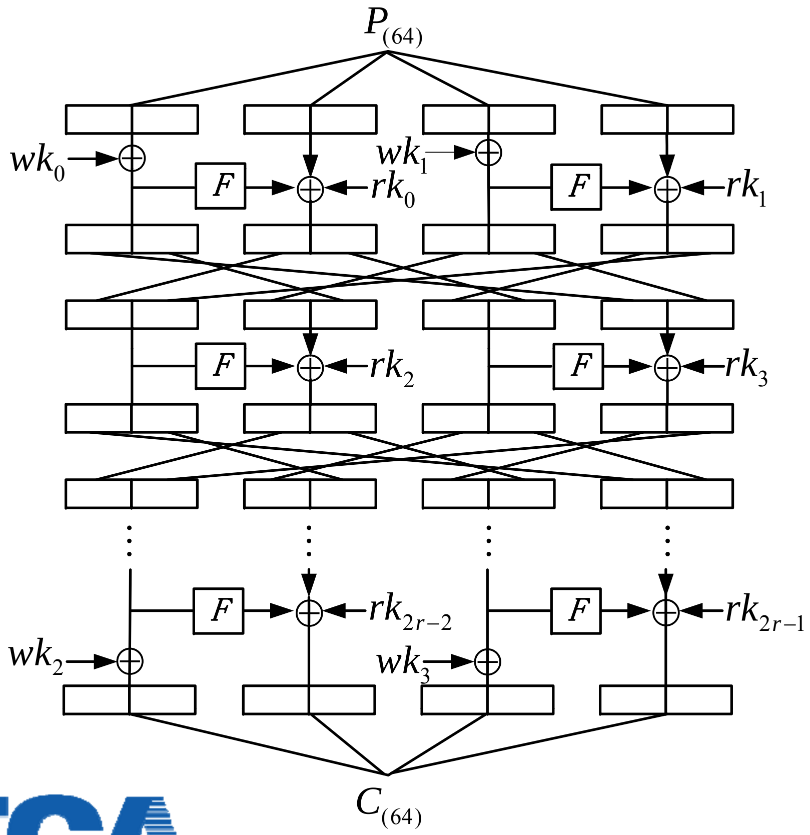
Outline

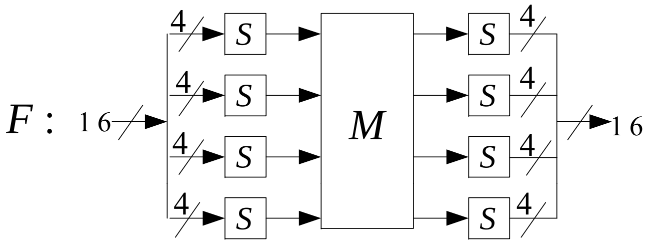
- Introduction
- **Description of Piccolo**
- Linear-Reflection Weak Keys of Piccolo
- New Observations on Piccolo-128
- Conclusion

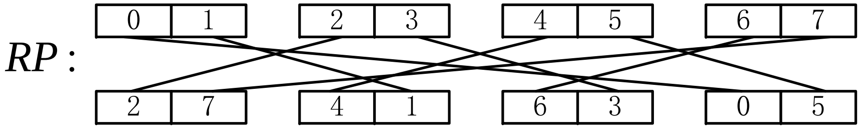
Description of Piccolo

- A lightweight block cipher proposed in CHES 2011 by SONY.
  - Structure : GFN
  - Block size : 64-bit
  - Key length : 80-/128-bit
  - Number of rounds: 25/31
- Encryption Algorithm
- Key Schedule Algorithm

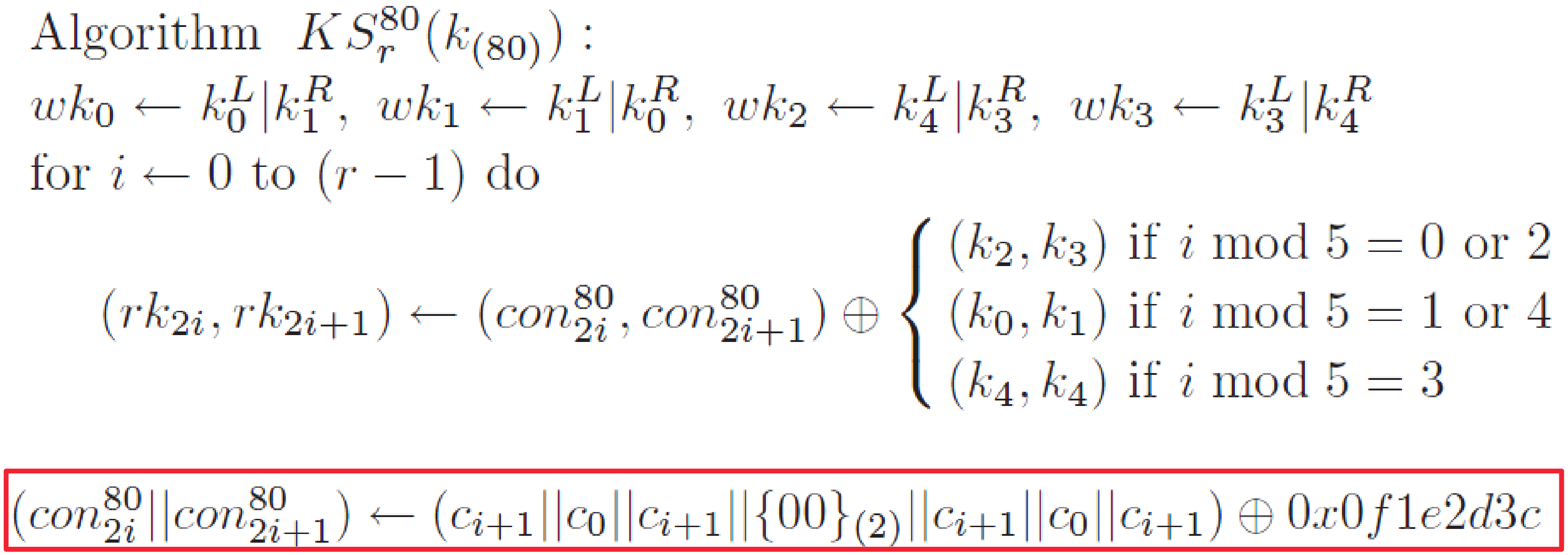
Encryption Algorithm







Key Schedule Algorithm



```
Algorithm $KS_r^{80}(k_{(80)})$ :
$wk_0 \leftarrow k_0^L|k_1^R,\ wk_1 \leftarrow k_1^L|k_0^R,\ wk_2 \leftarrow k_4^L|k_3^R,\ wk_3 \leftarrow k_3^L|k_4^R$
for $i \leftarrow 0$ to $(r-1)$ do
    $(rk_{2i}, rk_{2i+1}) \leftarrow (con_{2i}^{80}, con_{2i+1}^{80}) \oplus \begin{cases} (k_2, k_3) \text{ if } i \bmod 5 = 0 \text{ or } 2 \\ (k_0, k_1) \text{ if } i \bmod 5 = 1 \text{ or } 4 \\ (k_4, k_4) \text{ if } i \bmod 5 = 3 \end{cases}$
```

$$\boxed{(con_{2i}^{80}||con_{2i+1}^{80}) \leftarrow (c_{i+1}||c_0||c_{i+1}||\{00\}_{(2)}||c_{i+1}||c_0||c_{i+1}) \oplus 0x0f1e2d3c}$$

Key Schedule Algorithm

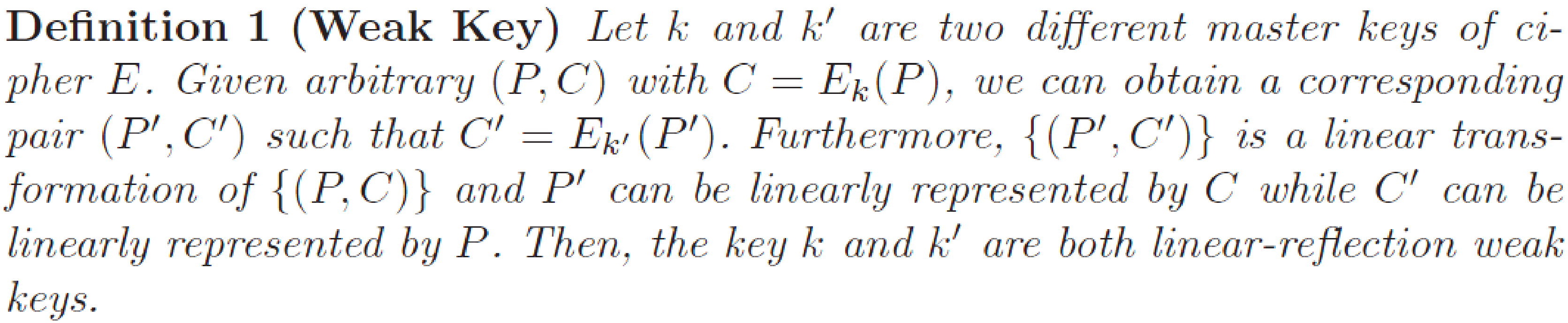
```
Algorithm $KS_r^{128}(k_{(128)})$ :
$wk_0 \leftarrow k_0^L | k_1^R,\ wk_1 \leftarrow k_1^L | k_0^R,\ wk_2 \leftarrow k_4^L | k_7^R,\ wk_3 \leftarrow k_7^L | k_4^R$
for $i \leftarrow 0$ to $(2r - 1)$ do
    if $(i + 2) \bmod 8 = 0$ then
        $(k_0, k_1, k_2, k_3, k_4, k_5, k_6, k_7) \leftarrow (k_2, k_1, k_6, k_7, k_0, k_3, k_4, k_5)$
    $rk_i \leftarrow k_{(i+2) \bmod 8} \oplus con_i^{128}$
```

$$\boxed{(con_{2i}^{128} || con_{2i+1}^{128}) \leftarrow (c_{i+1} || c_0 || c_{i+1} || \{00\}_{(2)} || c_{i+1} || c_0 || c_{i+1}) \oplus 0x6547a98b}$$

Outline

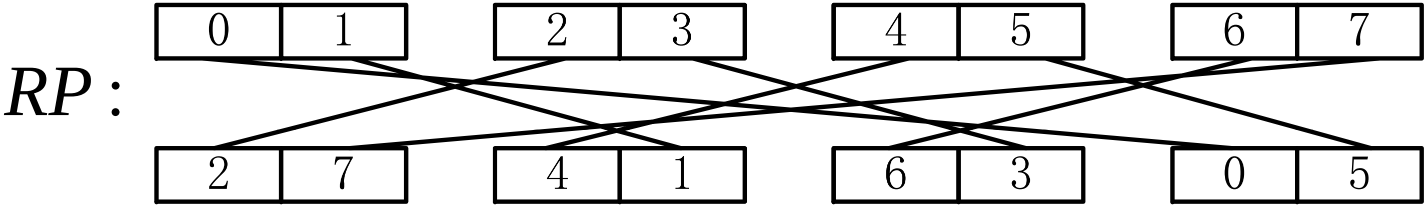
- Introduction
- Description of Piccolo
- **Linear-Reflection Weak Keys of Piccolo**
- New Observations on Piccolo-128
- Conclusion

Linear-Reflection Weak Keys of Piccolo



Definition 1 (Weak Key) *Let k and k' are two different master keys of cipher E. Given arbitrary (P, C) with $C = E_k(P)$, we can obtain a corresponding pair (P', C') such that $C' = E_{k'}(P')$. Furthermore, $\{(P', C')\}$ is a linear transformation of $\{(P, C)\}$ and P' can be linearly represented by C while C' can be linearly represented by P. Then, the key k and k' are both linear-reflection weak keys.*

Linear-Reflection Weak Keys of Piccolo



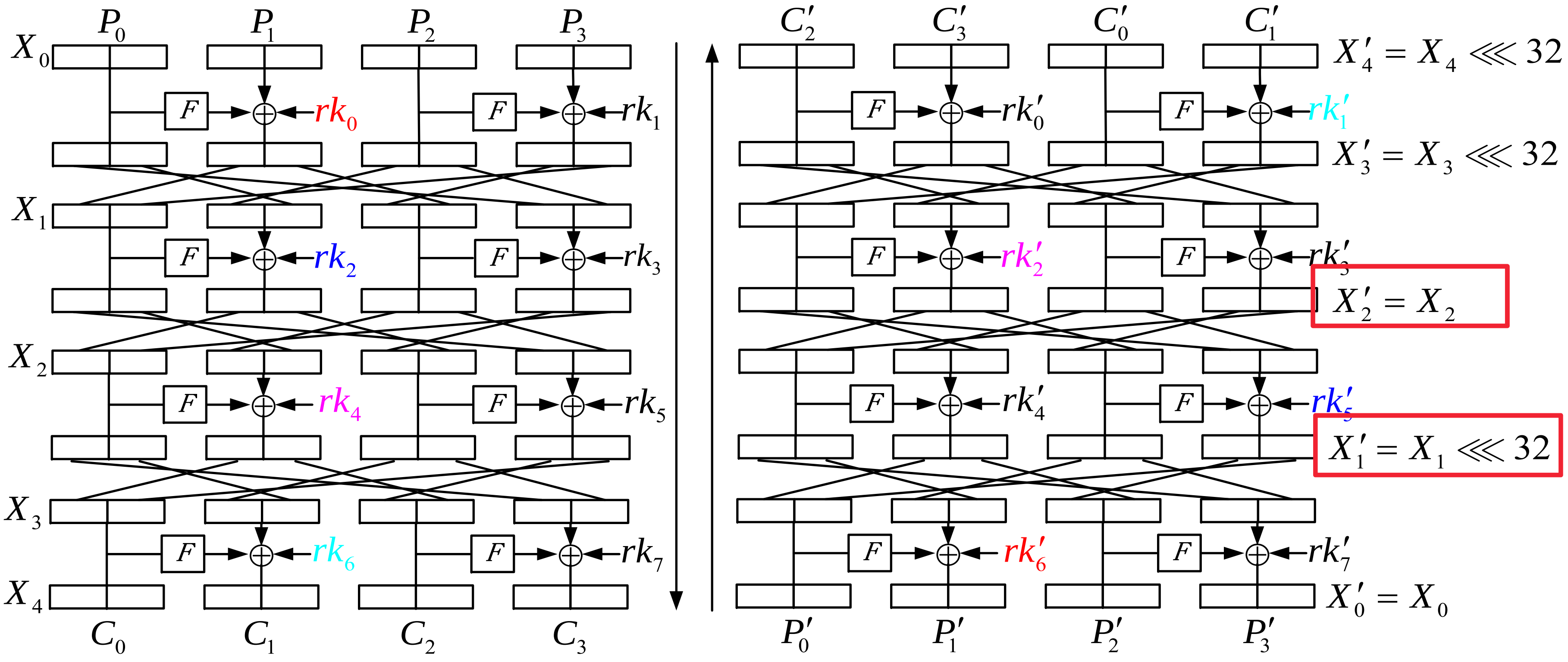
Observation 1 (Property of RP) *The permutation RP used in Piccolo has some relationships with its inverse RP^{-1}:*

1. *If the input of permutation RP is $X_{(64)}$ and the corresponding output is denoted by $(Y_{1(32)}, Y_{2(32)})$, then the output of RP^{-1} with the same input will be $(Y_{2(32)}, Y_{1(32)})$.*
2. *$RP^2 = (RP^{-1})^2 = (RP^2)^{-1}$. The fact reveals that RP^2 is self-inverse and the period of permutation RP is 4.*

Linear-Reflection Weak Keys of Piccolo

$$P \xrightarrow{k} C$$

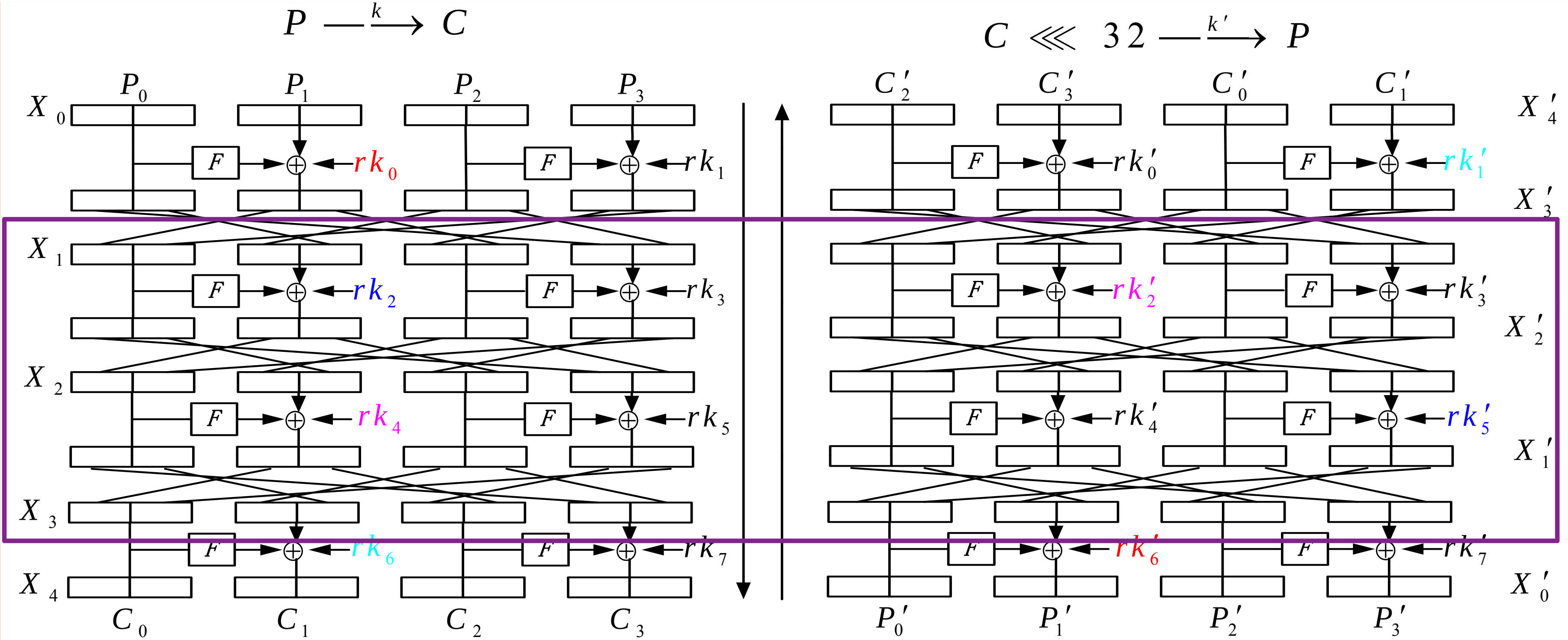
$$C \lll 32 \xrightarrow{k'} P$$



Linear-Reflection Weak Keys of Piccolo

$$\begin{cases} rk_0 = rk'_6 \\ rk_1 = rk'_7 \\ rk_2 = rk'_5 \\ rk_3 = rk'_4 \\ rk_4 = rk'_2 \\ rk_5 = rk'_3 \\ rk_6 = rk'_1 \\ rk_7 = rk'_0 \end{cases} \Rightarrow \begin{cases} P \xrightarrow{k} C \\ C \lll 32 \xrightarrow{k'} P \end{cases}$$

Linear-Reflection Weak Keys of Piccolo

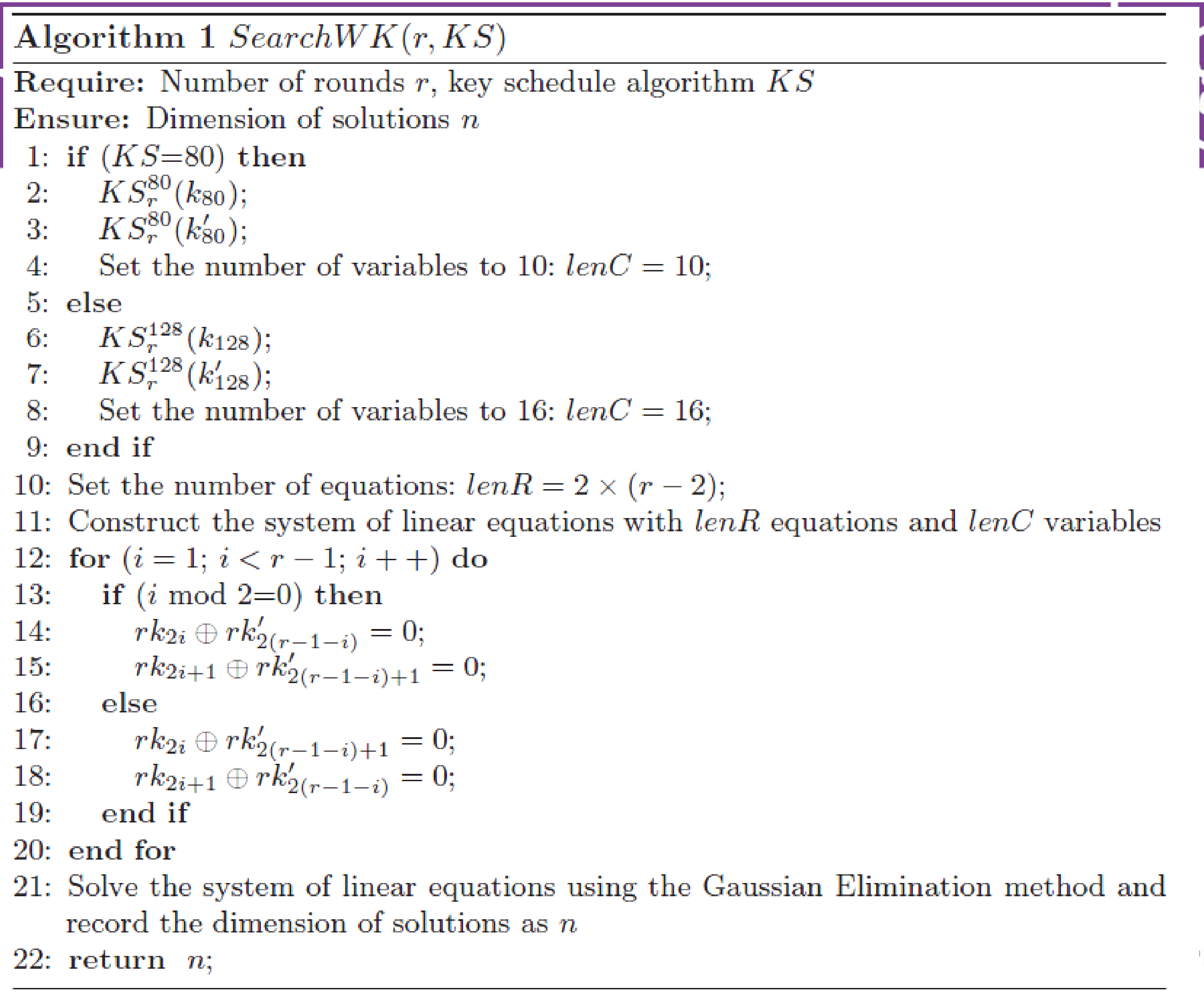

$P \xrightarrow{k} C$
$C \lll 32 \xrightarrow{k'} P$
P_0 P_1 P_2 P_3
X_0 X_1 X_2 X_3 X_4
F
rk_0 rk_1 rk_2 rk_3 rk_4 rk_5 rk_6 rk_7
C_0 C_1 C_2 C_3
C'_2 C'_3 C'_0 C'_1
X'_4 X'_3 X'_2 X'_1 X'_0
rk'_0 rk'_1 rk'_2 rk'_3 rk'_4 rk'_5 rk'_6 rk'_7
P'_0 P'_1 P'_2 P'_3

TCA

Linear-Reflection Weak Keys of Piccolo

$$\begin{cases} rk_0 = rk'_6 \\ rk_1 = rk'_7 \\ rk_2 = rk'_5 \\ rk_3 = rk'_4 \\ rk_4 = rk'_2 \\ rk_5 = rk'_3 \\ rk_6 = rk'_1 \\ rk_7 = rk'_0 \end{cases} \Rightarrow \begin{cases} rk_2 = rk'_5 \\ rk_3 = rk'_4 \\ rk_4 = rk'_2 \\ rk_5 = rk'_3 \end{cases}$$

Search



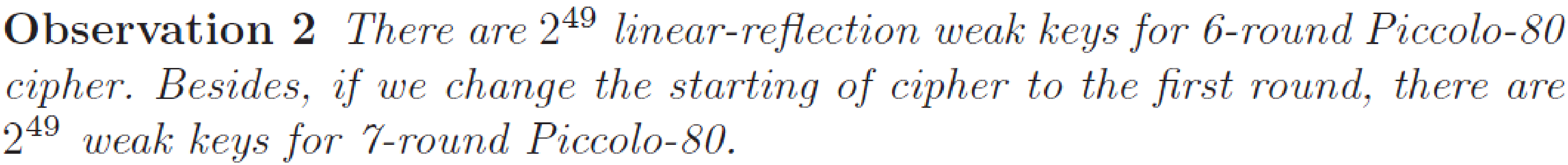
Algorithm 1 $SearchWK(r, KS)$

Require: Number of rounds r, key schedule algorithm KS

Ensure: Dimension of solutions n

```
if ($KS$=80) then
    $KS_r^{80}(k_{80})$;
    $KS_r^{80}(k'_{80})$;
    Set the number of variables to 10: $lenC = 10$;
else
    $KS_r^{128}(k_{128})$;
    $KS_r^{128}(k'_{128})$;
    Set the number of variables to 16: $lenC = 16$;
end if
Set the number of equations: $lenR = 2 \times (r - 2)$;
Construct the system of linear equations with $lenR$ equations and $lenC$ variables
for ($i = 1; i < r - 1; i++$) do
    if ($i$ mod 2=0) then
        $rk_{2i} \oplus rk'_{2(r-1-i)} = 0$;
        $rk_{2i+1} \oplus rk'_{2(r-1-i)+1} = 0$;
    else
        $rk_{2i} \oplus rk'_{2(r-1-i)+1} = 0$;
        $rk_{2i+1} \oplus rk'_{2(r-1-i)} = 0$;
    end if
end for
Solve the system of linear equations using the Gaussian Elimination method and
    record the dimension of solutions as $n$
return $n$;
```

Weak Keys of Piccolo-80



Observation 2 *There are 2^{49} linear-reflection weak keys for 6-round Piccolo-80 cipher. Besides, if we change the starting of cipher to the first round, there are 2^{49} weak keys for 7-round Piccolo-80.*

$$\begin{cases} k_0 \oplus k_1' = 0x2623 \\ k_1 \oplus k_0' = 0x022a \\ k_2 \oplus k_4' = 0x380e \\ k_3 \oplus k_4' = 0x1c07 \\ k_4 \oplus k_3' = 0x0e29 \\ k_4 \oplus k_2' = 0x2a20 \\ k_0 \oplus k_0' = 0x380e \\ k_1 \oplus k_1' = 0x1c07 \end{cases}$$

Weak Keys of Piccolo-80

$$(P_0, P_1, P_2, P_3) \xrightarrow{k} (C_0, C_1, C_2, C_3)$$

$$(P'_0, P'_1, P'_2, P'_3) \xrightarrow{k'} (C'_0, C'_1, C'_2, C'_3)$$

$$k = (x, x \oplus 0x3a24, y \oplus 0x380e, y \oplus 0x1c07, z)$$

$$k' = (x \oplus 0x380e, x \oplus 0x2623, z \oplus 0x2a20, z \oplus 0x0e29, y)$$

$$\begin{aligned} P' &= \left(C_2, C_3 \oplus k_3 \oplus 0x353a \oplus k'_2 \oplus 0x071c, C_0, C_1 \oplus k_2 \oplus 0x3f12 \oplus k'_3 \oplus 0x293d\right) \\ &= (C_2, C_3 \oplus y \oplus z \oplus 0x0401, C_0, C_1 \oplus y \oplus z \oplus 0x2008), \\ C' &= \left(P_0, P_1 \oplus k_2 \oplus 0x071c \oplus k'_2 \oplus 0x3f12, P_2, P_3 \oplus k_3 \oplus 0x293d \oplus k'_3 \oplus 0x353a\right) \\ &= (P_0, P_1 \oplus y \oplus z \oplus 0x2a20, P_2, P_3 \oplus y \oplus z \oplus 0x0e29). \end{aligned}$$

Weak Keys of Piccolo-128

Observation 3 *There are 2^{17} weak keys for 10-round Piccolo-128 cipher.*

$$\begin{aligned}
k_4 \oplus k_5' &= 0xf8c1 \\
k_5 \oplus k_4' &= 0x8cdc \\
k_6 \oplus k_6' &= 0x5816 \\
k_7 \oplus k_1' &= 0x2c0b \\
k_2 \oplus k_5' &= 0xf0c3 \\
k_1 \oplus k_4' &= 0xe4c6 \\
k_6 \oplus k_0' &= 0x1806 \\
k_7 \oplus k_3' &= 0x0c03
\end{aligned}$$

$$\begin{aligned}
k_0 \oplus k_7' &= 0xe8c5 \\
k_3 \oplus k_6' &= 0xfcc0 \\
k_4 \oplus k_2' &= 0x1806 \\
k_5 \oplus k_1' &= 0x0c03 \\
k_6 \oplus k_7' &= 0x80df \\
k_1 \oplus k_6' &= 0xf4c2 \\
k_4 \oplus k_4' &= 0x5816 \\
k_5 \oplus k_5' &= 0x2c0b
\end{aligned}$$

Weak Keys of Piccolo-128

$$\begin{aligned} k = (&x \oplus 0x781e, x \oplus 0xbcd0, x \oplus 0x0802, x \oplus 0xb4d2,\\ &x, x \oplus 0xd4ca, x \oplus 0x1004, x \oplus 0xf4c2) \end{aligned}$$

$$\begin{aligned} k' = (&x \oplus 0x0802, x \oplus 0xd8c9, x \oplus 0x1806, x \oplus 0xf8c1,\\ &x \oplus 0x5816, x \oplus 0xf8c1, x \oplus 0x4812, x \oplus 0x90db) \end{aligned}$$

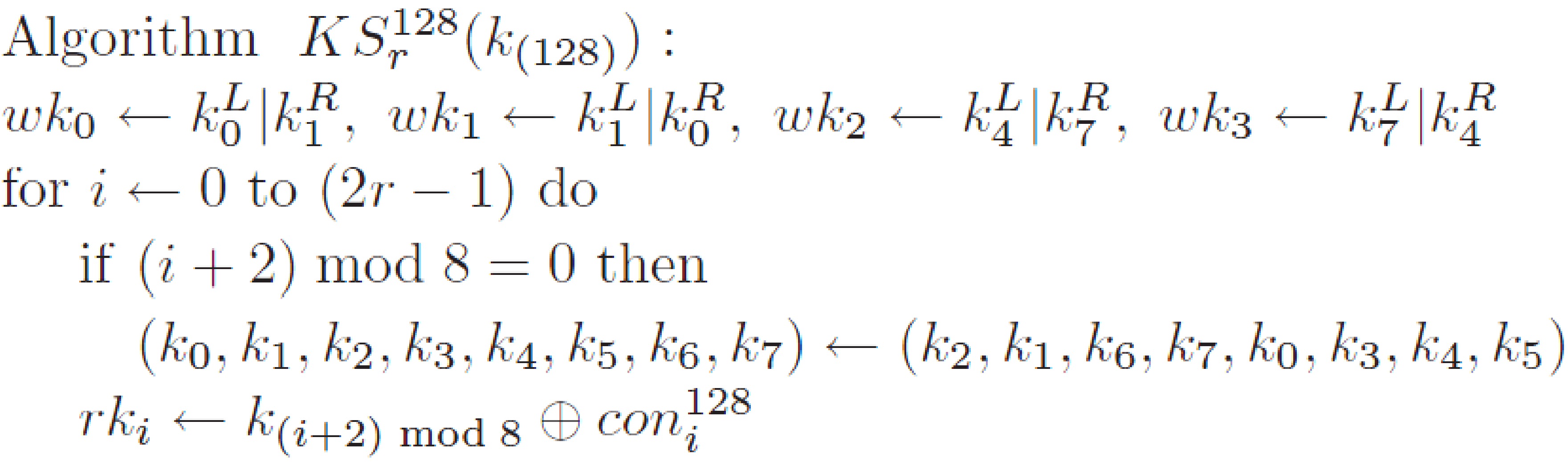
$$\begin{aligned} P' &= \left(C_2, C_3 \oplus k_7 \oplus 0x8181 \oplus k'_2 \oplus 0x6d45, C_0, C_1 \oplus k_2 \oplus 0x3553 \oplus k'_3 \oplus 0xad8a\right)\\ &= (C_2, C_3, C_0, C_1 \oplus 0x681a),\\ C' &= \left(P_0, P_1 \oplus k_2 \oplus 0x6d45 \oplus k'_2 \oplus 0x3553, P_2, P_3 \oplus k_3 \oplus 0xad8a \oplus k'_7 \oplus 0x8181\right)\\ &= (P_0, P_1 \oplus 0x4812, P_2, P_3 \oplus 0x0802). \end{aligned}$$

Outline

- Introduction
- Description of Piccolo
- Linear-Reflection Weak Keys of Piccolo
- **New Observations on Piccolo-128**
- Conclusion

New Observations on Piccolo-128

- Key Schedule Algorithm

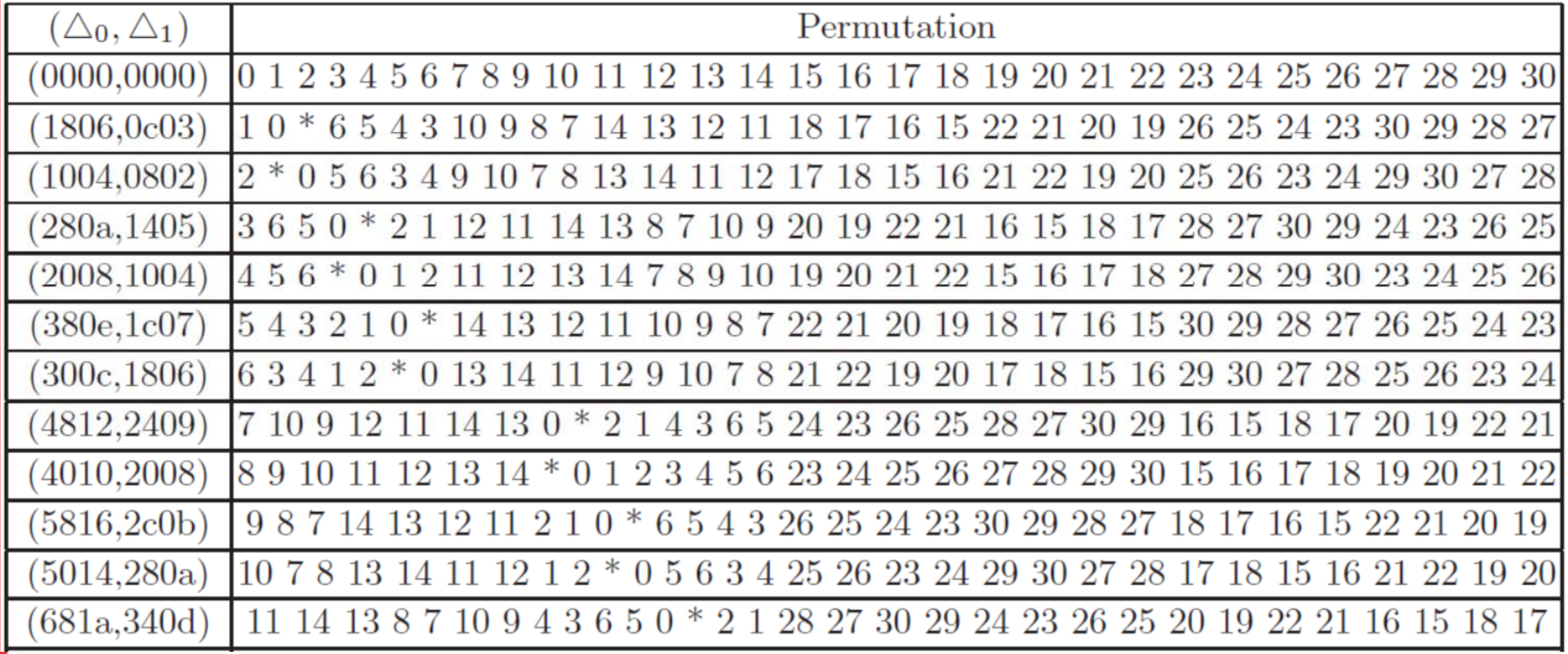


```
Algorithm $KS_r^{128}(k_{(128)})$ :
$wk_0 \leftarrow k_0^L|k_1^R,\ wk_1 \leftarrow k_1^L|k_0^R,\ wk_2 \leftarrow k_4^L|k_7^R,\ wk_3 \leftarrow k_7^L|k_4^R$
for $i \leftarrow 0$ to $(2r-1)$ do
    if $(i+2) \bmod 8 = 0$ then
        $(k_0, k_1, k_2, k_3, k_4, k_5, k_6, k_7) \leftarrow (k_2, k_1, k_6, k_7, k_0, k_3, k_4, k_5)$
    $rk_i \leftarrow k_{(i+2) \bmod 8} \oplus con_i^{128}$
```

New Observations on Piccolo-128

- 128bit master key is noted by (even,odd)
  - (k_0,k_2,k_4,k_6)→even
  - (k_1,k_3,k_5,k_7)→odd
- Similarity between different keys
  - For a fixed (even,odd), there exist 31 different keys such that the round keys for 30 rounds are equal to that under (even,odd).

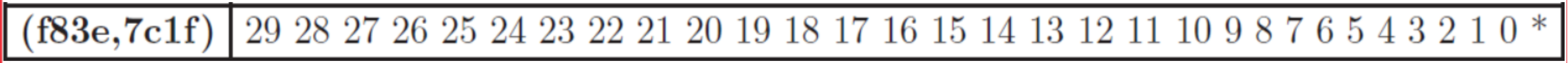
New Observations on Piccolo-128



$(\triangle_0, \triangle_1)$	Permutation
(0000,0000)	0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30
(1806,0c03)	1 0 * 6 5 4 3 10 9 8 7 14 13 12 11 18 17 16 15 22 21 20 19 26 25 24 23 30 29 28 27
(1004,0802)	2 * 0 5 6 3 4 9 10 7 8 13 14 11 12 17 18 15 16 21 22 19 20 25 26 23 24 29 30 27 28
(280a,1405)	3 6 5 0 * 2 1 12 11 14 13 8 7 10 9 20 19 22 21 16 15 18 17 28 27 30 29 24 23 26 25
(2008,1004)	4 5 6 * 0 1 2 11 12 13 14 7 8 9 10 19 20 21 22 15 16 17 18 27 28 29 30 23 24 25 26
(380e,1c07)	5 4 3 2 1 0 * 14 13 12 11 10 9 8 7 22 21 20 19 18 17 16 15 30 29 28 27 26 25 24 23
(300c,1806)	6 3 4 1 2 * 0 13 14 11 12 9 10 7 8 21 22 19 20 17 18 15 16 29 30 27 28 25 26 23 24
(4812,2409)	7 10 9 12 11 14 13 0 * 2 1 4 3 6 5 24 23 26 25 28 27 30 29 16 15 18 17 20 19 22 21
(4010,2008)	8 9 10 11 12 13 14 * 0 1 2 3 4 5 6 23 24 25 26 27 28 29 30 15 16 17 18 19 20 21 22
(5816,2c0b)	9 8 7 14 13 12 11 2 1 0 * 6 5 4 3 26 25 24 23 30 29 28 27 18 17 16 15 22 21 20 19
(5014,280a)	10 7 8 13 14 11 12 1 2 * 0 5 6 3 4 25 26 23 24 29 30 27 28 17 18 15 16 21 22 19 20
(681a,340d)	11 14 13 8 7 10 9 4 3 6 5 0 * 2 1 28 27 30 29 24 23 26 25 20 19 22 21 16 15 18 17

New Observations on Piccolo-128

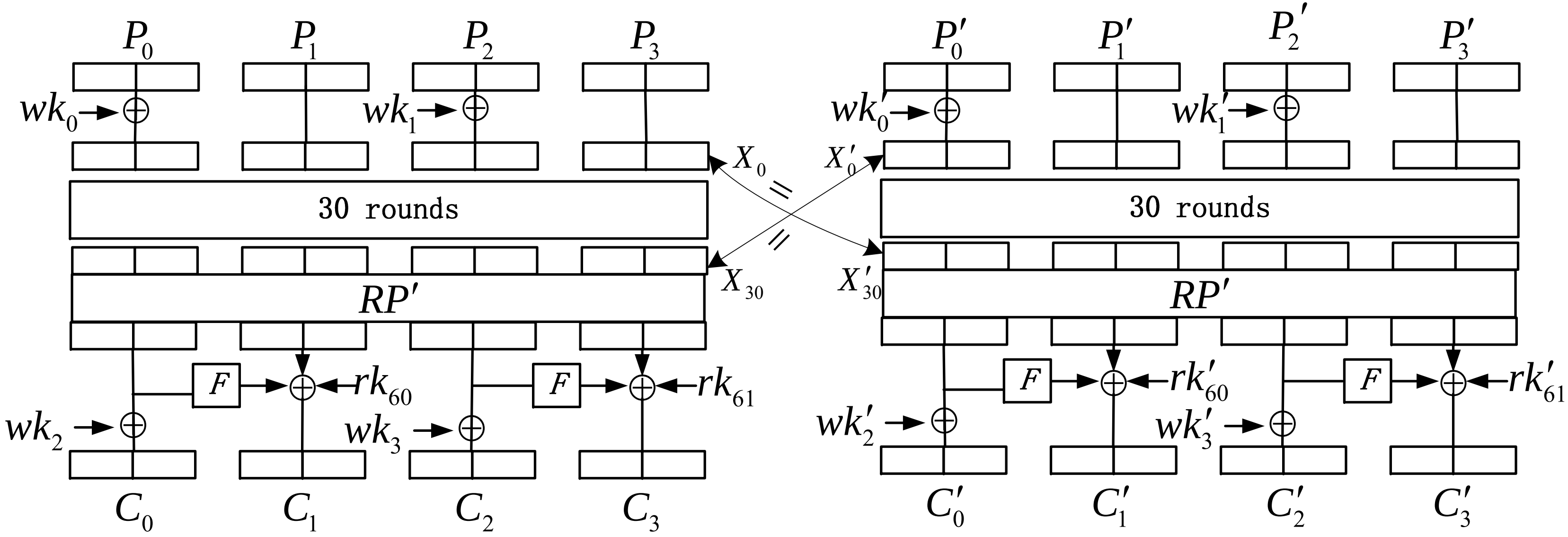
- **RP should not be allowed to be self-inverse.**



(f83e,7c1f)	29 28 27 26 25 24 23 22 21 20 19 18 17 16 15 14 13 12 11 10 9 8 7 6 5 4 3 2 1 0 *

New Observations on Piccolo-128

Observation 4 *If we replace the RP in Piccolo-128 by a self-inverse permutation RP', there exists 2^{32} weak keys for the full round new cipher and they can be parted into 2^{31} pairs (k, k') such that the decryption under k' can be represented by a non-linear function of the encryption under k and the degree of the non-linear function is equal to the degree of F function in Piccolo.*



New Observations on Piccolo-128

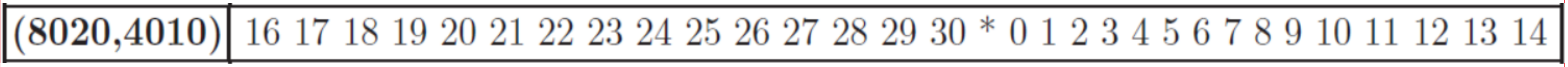
$$P' = RP'(C_0 \oplus (e^L \| o^R), F(C_0 \oplus (e^L \| o^R)) \oplus C_1 \oplus e \oplus 0x9d79,$$
$$C_2 \oplus (o^L \| e^R), F(C_2 \oplus (o^L \| e^R)) \oplus C_3 \oplus o \oplus 0xd594)$$
$$\oplus (e'^L \| o'^R, 0, o'^L \| e'^R, 0),$$

$$C' = (P_0^* \oplus (e'^L \| o'^R), F(P_0^* \oplus (e'^L \| o'^R)) \oplus P_1^* \oplus e' \oplus 0x9d79,$$
$$P_2^* \oplus (o'^L \| e'^R), F(P_2^* \oplus (o'^L \| e'^R)) \oplus P_3^* \oplus o' \oplus 0xd594),$$

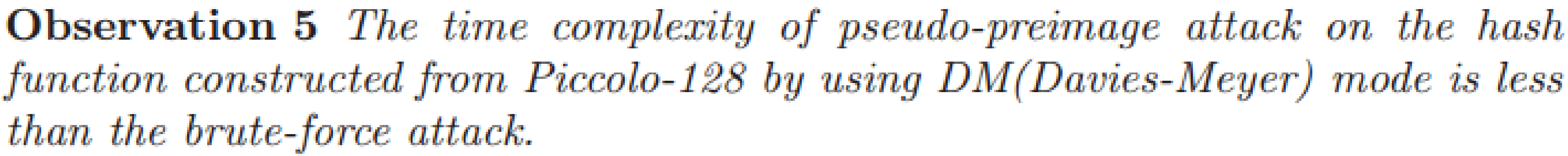
$$where \quad P^* = RP'((P_0, P_1, P_2, P_3) \oplus (e^L \| o^R, 0, o^L \| e^R, 0)).$$

New Observations on Piccolo-128

- **Security of hash function based on full-round Piccolo-128 is insufficient.**



(8020,4010)	16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 * 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14



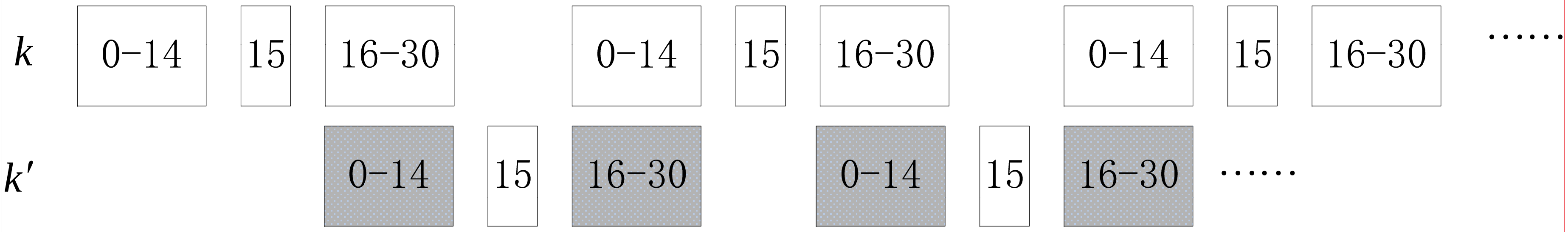
Observation 5 *The time complexity of pseudo-preimage attack on the hash function constructed from Piccolo-128 by using DM(Davies-Meyer) mode is less than the brute-force attack.*

New Observations on Piccolo-128

- DM mode:

Let $M_{i\text{-}1}$, $H_{i\text{-}1}$ and H_i be the input message , the input chaining value, and the output; the new chaining value H_i is computed as:

$$H_i = E_{M_{i-1}}(H_{i-1}) \oplus H_{i-1}.$$



k 0–14 15 16–30 0–14 15 16–30 0–14 15 16–30 ……

k' 0–14 15 16–30 0–14 15 16–30 ……

Outline

- Introduction
- Description of Piccolo
- Linear-Reflection Weak Keys of Piccolo
- New Observations on Piccolo-128
- **Conclusion**

Conclusion

- Evaluate the security of Piccolo block cipher from the known and chosen key respective.
- Define linear-reflection weak keys.
  - For one weak key k, we can find another related weak key k’ such that the cipher with k’ can be completely determined by the cipher under k.
  - 7-round Piccolo-80 (Observation 2)
  - 10-round Piccolo-128 (Observation 3)

Conclusion

- Summarize some interesting characteristics of key schedule algorithm for Piccolo-128.
  - RP should not be allowed to be self-inverse (Observation 4)
  - Security of hash function based on full-round Piccolo-128 is insufficient (Observation 5)
- We expect that the results of our paper may guide the design of round constants for some simple key schedules.

Thanks For Your Attention!