# Reflection Cryptanalysis of PRINCE-like Ciphers

Hadi Soleimany[1], Céline Blondeau[1], Xiaoli Yu[2,3], Wenling Wu[2], Kaisa Nyberg[1], Huiling Zhang[2], Lei Zhang[2], Yanfeng Wang[2]

[1]Department of Information and Computer Science, Aalto University School of Science, Finland

[2]Institute of Software, Chinese Academy of Sciences, P. R. China

[3]Graduate University of Chinese Academy of Sciences, P. R. China

FSE 2013

Aalto University
School of Science

# Outline


1. Description of PRINCE-like Ciphers
2. Distinguishers
3. Key Recovery
4. Various Classes of $\alpha$-reflection
5. Conclusions

1. Description of PRINCE-like Ciphers
2. Distinguishers
3. Key Recovery
4. Various Classes of $\alpha$-reflection
5. Conclusions

# Description of PRINCE-like cipher

- Low-latency SPN block cipher was proposed at ASIACRYPT2012.

# Description of PRINCE-like cipher

- Low-latency SPN block cipher was proposed at ASIACRYPT2012.
- Based on the so-called FX construction

# Description of PRINCE-like cipher

- Low-latency SPN block cipher was proposed at ASIACRYPT2012.
- Based on the so-called FX construction
- The key is split into two parts of n bits $k = k_0||k_1$.

# Description of PRINCE-like cipher

- Low-latency SPN block cipher was proposed at ASIACRYPT2012.
- Based on the so-called FX construction
- The key is split into two parts of n bits $k = k_0 || k_1$.


- $k_0' = (k_0 \ggg 1) \oplus (k_0 \gg (n-1))$

# Description of PRINCE-like cipher

- Low-latency SPN block cipher was proposed at ASIACRYPT2012.
- Based on the so-called FX construction
- The key is split into two parts of n bits $k = k_0||k_1$.


- $k'_0 = (k_0 \ggg 1) \oplus (k_0 \gg (n-1))$
- With a property called $\alpha$-reflection:

$$D(k_0||k'_0||k_1)() = E(k'_0||k_0||k_1 \oplus \alpha)()$$

# Description of PRINCE-like cipher

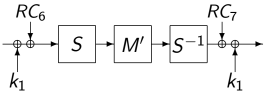
- Low-latency SPN block cipher was proposed at ASIACRYPT2012.
- Based on the so-called FX construction
- The key is split into two parts of n bits $k = k_0||k_1$.


- $k'_0 = (k_0 \ggg 1) \oplus (k_0 \gg (n-1))$
- With a property called $\alpha$-reflection:

$$D(k_0||k'_0||k_1)() = E(k'_0||k_0||k_1 \oplus \alpha)()$$

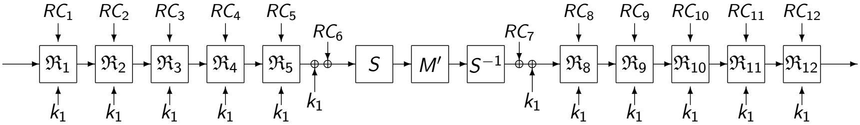
- Independently of the value of $\alpha$, the designers showed that PRINCE is secure against known attacks.

# Description of PRINCE-like Cipher



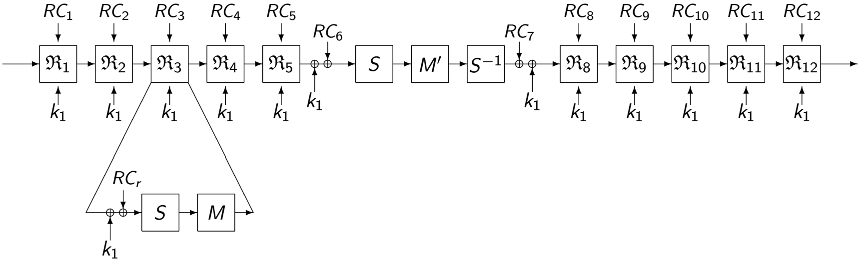

The 2 midmost rounds

# Description of PRINCE-like Cipher



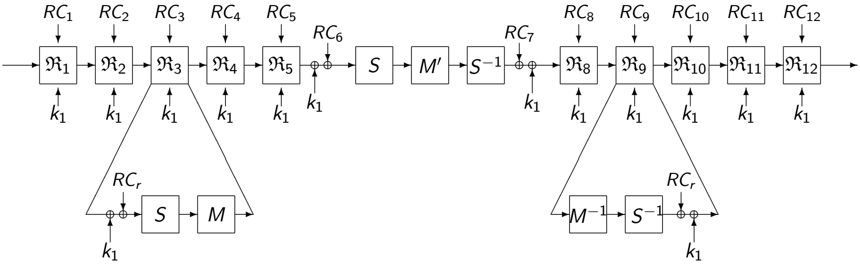

Total 12 rounds

# Description of PRINCE-like Cipher



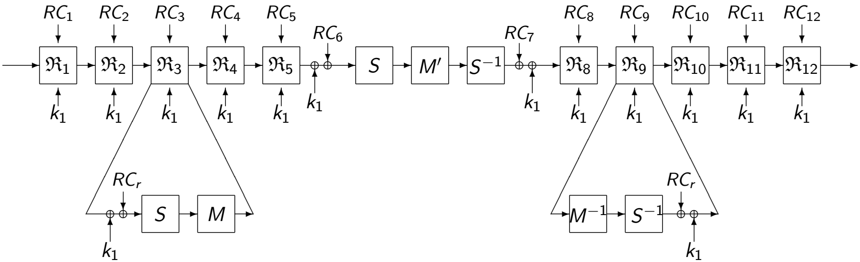

The first rounds

# Description of PRINCE-like Cipher




The last rounds

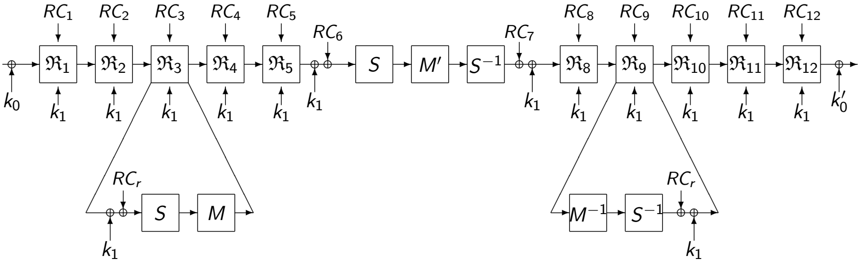
# Description of PRINCE-like Cipher




Related constants:

$$RC_{2R-r+1} = RC_r \oplus \alpha, \text{ for all } r = 1, \ldots, 2R$$

# Description of PRINCE-like Cipher




The whitening key

# Description of PRINCE

- PRINCE-like cipher with $n = 64$.
- Constant is defined as $\alpha = 0xc0ac29b7c97c50dd$.
- The $S$-layer is a non-linear layer where each nibble is processed by the same Sbox.

# Description of PRINCE

- $M'$ is an involutory $64 \times 64$ block diagonal matrix $(\hat{M}_0, \hat{M}_1, \hat{M}_1, \hat{M}_0)$.

# Description of PRINCE

- $M'$ is an involutory $64 \times 64$ block diagonal matrix $(\hat{M}_0, \hat{M}_1, \hat{M}_1, \hat{M}_0)$.

$$\hat{M}_0 = \begin{pmatrix} M_0 & M_1 & M_2 & M_3 \\ M_1 & M_2 & M_3 & M_0 \\ M_2 & M_3 & M_0 & M_1 \\ M_3 & M_0 & M_1 & M_2 \end{pmatrix}, \quad \hat{M}_1 = \begin{pmatrix} M_1 & M_2 & M_3 & M_0 \\ M_2 & M_3 & M_0 & M_1 \\ M_3 & M_0 & M_1 & M_2 \\ M_0 & M_1 & M_2 & M_3 \end{pmatrix}.$$

# Description of PRINCE

- $M'$ is an involutory $64 \times 64$ block diagonal matrix $(\hat{M}_0, \hat{M}_1, \hat{M}_1, \hat{M}_0)$.

$$\hat{M}_0 = \begin{pmatrix} M_0 & M_1 & M_2 & M_3 \\ M_1 & M_2 & M_3 & M_0 \\ M_2 & M_3 & M_0 & M_1 \\ M_3 & M_0 & M_1 & M_2 \end{pmatrix}, \quad \hat{M}_1 = \begin{pmatrix} M_1 & M_2 & M_3 & M_0 \\ M_2 & M_3 & M_0 & M_1 \\ M_3 & M_0 & M_1 & M_2 \\ M_0 & M_1 & M_2 & M_3 \end{pmatrix}.$$

- The second linear matrix $M$ for PRINCE is obtained by composition of $M'$ and a permutation $SR$ of nibbles by setting $M = SR \circ M'$.

1 Description of PRINCE-like Ciphers

2 Distinguishers

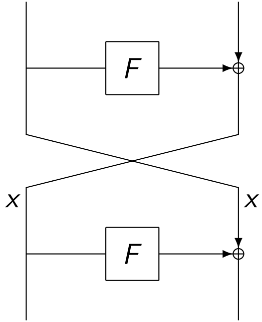
3 Key Recovery

4 Various Classes of $\alpha$-reflection

5 Conclusions

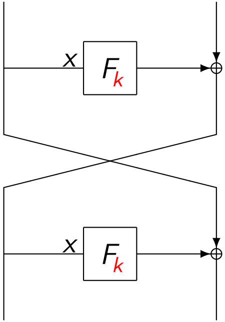
# Previous Works: Reflection Attack

- It has been applied on some ciphers and hash functions with Feistel construction (Kara 2008, Bouillaguet et al. 2010).



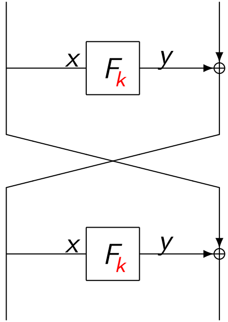
# Previous Works: Reflection Attack

- It has been applied on some ciphers and hash functions with Feistel construction (Kara 2008, Bouillaguet et al. 2010).



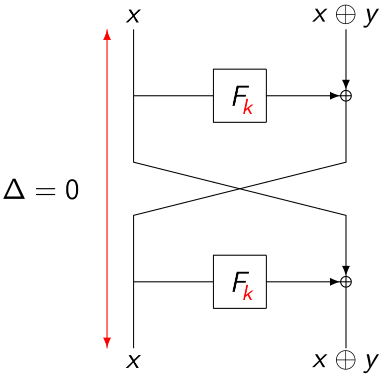
# Previous Works: Reflection Attack

- It has been applied on some ciphers and hash functions with Feistel construction (Kara 2008, Bouillaguet et al. 2010).



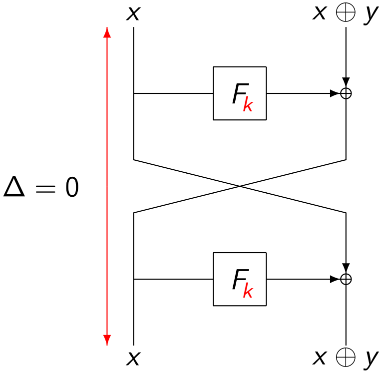
# Previous Works: Reflection Attack

- It has been applied on some ciphers and hash functions with Feistel construction (Kara 2008, Bouillaguet et al. 2010).



# Previous Works: Reflection Attack

- It has been applied on some ciphers and hash functions with Feistel construction (Kara 2008, Bouillaguet et al. 2010).




**This work**

Using probabilistic reflection property instead of deterministic approach.

# Fixed Points

**Definition**

Let $f : A \rightarrow A$ be a function on a set $A$. A point $x \in A$ is called a fixed point of the function $f$ if and only if $f(x) = x$.

# Fixed Points

## Definition

Let $f : A \to A$ be a function on a set $A$. A point $x \in A$ is called a fixed point of the function $f$ if and only if $f(x) = x$.

## Lemma

*Let $f : \mathbb{F}_2^n \to \mathbb{F}_2^n$ be a linear involution. Then the number of fixed points of $f$ is greater than or equal to $2^{n/2}$.*

# Fixed Points

## Definition

Let $f : A \to A$ be a function on a set $A$. A point $x \in A$ is called a fixed point of the function $f$ if and only if $f(x) = x$.

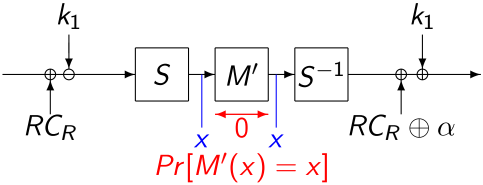
## Lemma

*Let $f : \mathbb{F}_2^n \to \mathbb{F}_2^n$ be a linear involution. Then the number of fixed points of $f$ is greater than or equal to $2^{n/2}$.*

## Idea

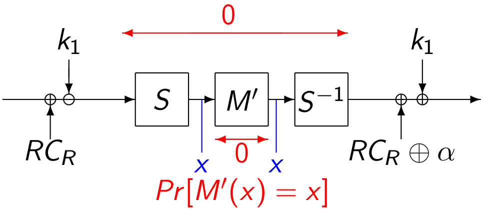
Take advantage of $\alpha$-reflection property and the fact that always fixed points exist in midmost rounds of PRINCE-like ciphers.

# Characteristic $\mathcal{I}_1$



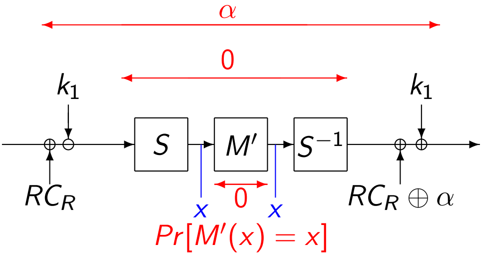

$$\mathcal{P}_{\mathcal{I}_1} = \mathcal{P}_{F_{M'}} = \frac{|F_{M'}|}{2^n}.$$

# Characteristic $\mathcal{I}_1$



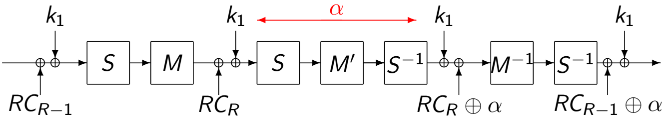

$$\mathcal{P}_{\mathcal{I}_1} = \mathcal{P}_{F_{M'}} = \frac{|F_{M'}|}{2^n}.$$

# Characteristic $\mathcal{I}_1$



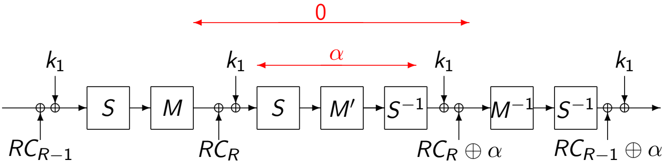

$$\mathcal{P}_{\mathcal{I}_1} = \mathcal{P}_{F_{M'}} = \frac{|F_{M'}|}{2^n}.$$

# Characteristic $\mathcal{I}_2$



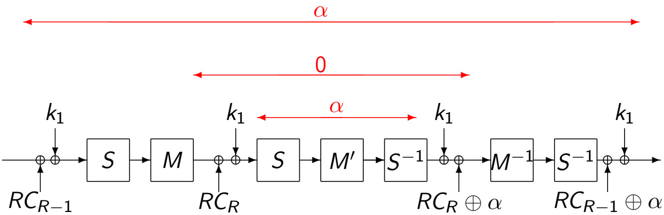

$$\mathcal{P}_{\mathcal{I}_2} = 2^{-n} \# \left\{ x \in \mathbb{F}_2^n \,|\, S^{-1}(M'(S(x))) \oplus x = \alpha \right\}.$$

# Characteristic $\mathcal{I}_2$



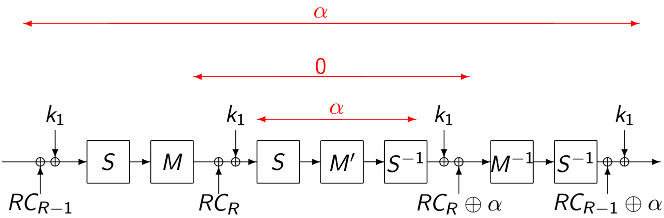

$$\mathcal{P}_{\mathcal{I}_2} = 2^{-n} \# \left\{ x \in \mathbb{F}_2^n \,|\, S^{-1}(M'(S(x))) \oplus x = \alpha \right\}.$$

# Characteristic $\mathcal{I}_2$



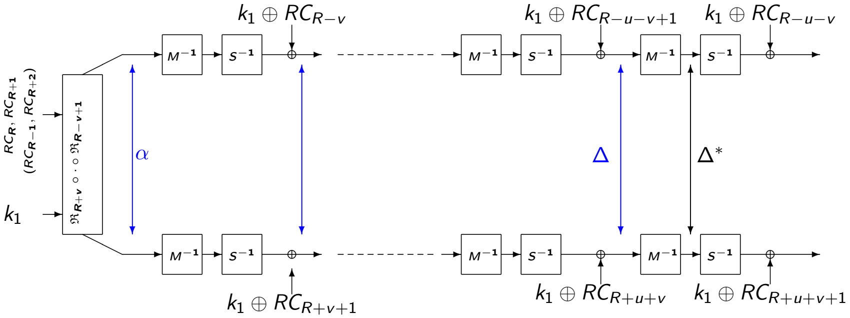

$$\mathcal{P}_{\mathcal{I}_2} = 2^{-n} \# \left\{ x \in \mathbb{F}_2^n \,|\, S^{-1}(M'(S(x))) \oplus x = \alpha \right\}.$$

# Characteristic $\mathcal{I}_2$




If $\mathcal{P}_{\mathcal{I}_2} = 0$ then we have impossible differential.

# External Characteristic $\mathcal{P}_{\mathcal{C}_r}$



1 Description of PRINCE-like Ciphers

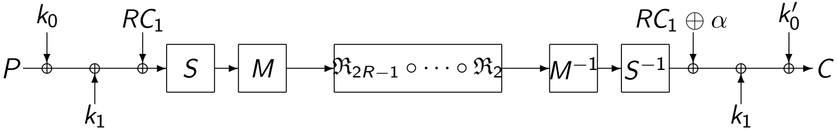
2 Distinguishers

3 Key Recovery

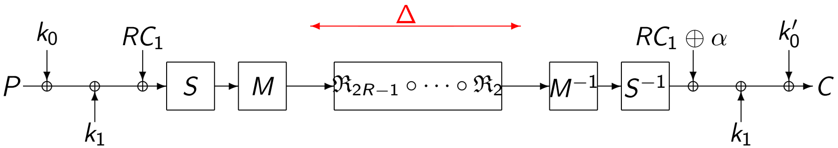
4 Various Classes of $\alpha$-reflection

5 Conclusions

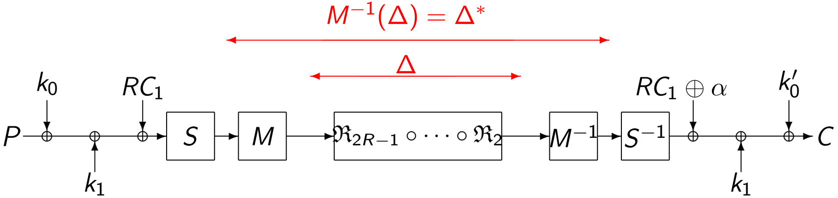
# Key Recovery



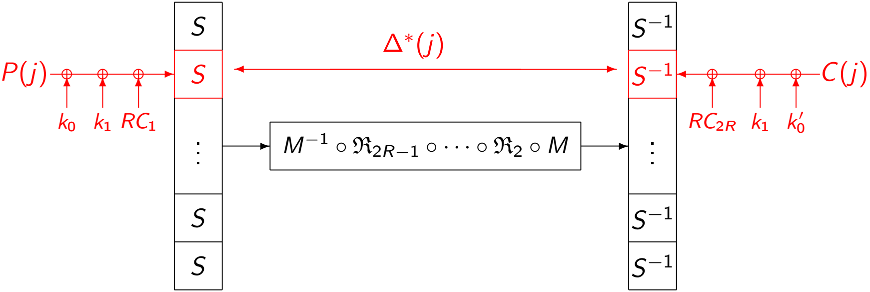
# Key Recovery



# Key Recovery



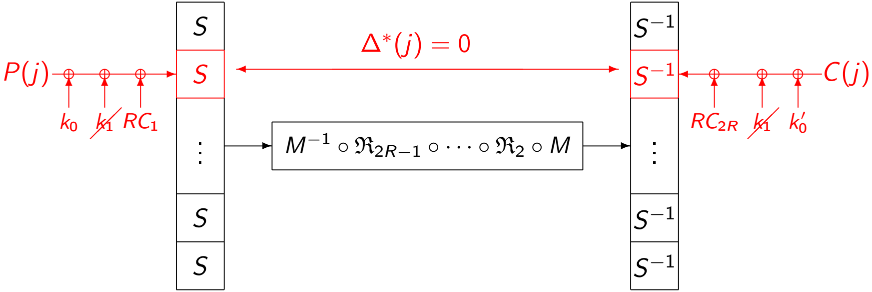
# Key Recovery Nibble by Nibble




$$\Delta^*(j) = S(P(j) \oplus k_0(j) \oplus k_1(j) \oplus RC_1(j))$$

$$\oplus S(C(j) \oplus k_0'(j) \oplus k_1(j) \oplus RC_{2R}(j))$$

# Key Recovery for Passive Nibble




$$P(j) \oplus k_0(j) \oplus C(j) \oplus k'_0(j) \oplus \alpha(j) = 0,$$

- The difference after passing through the S-boxes is still zero.
- The value of $k_1(j)$ need not be known.

1 Description of PRINCE-like Ciphers

2 Distinguishers

3 Key Recovery

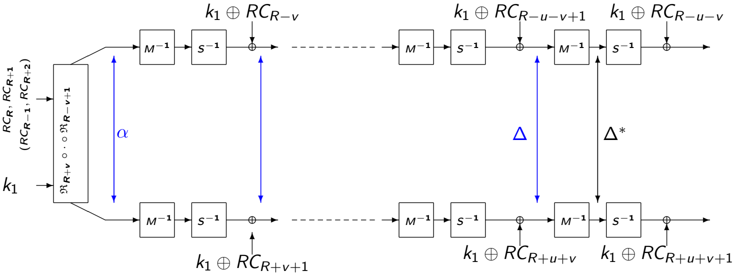
4 Various Classes of $\alpha$-reflection

5 Conclusions

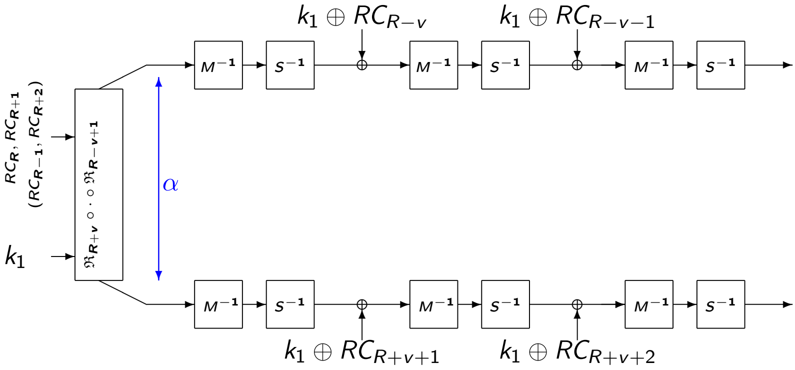
# Maximizing Probability $\mathcal{P}_\mathcal{C}$ of Characteristic

To maximize $\mathcal{P}_\mathcal{C}$ we can either use

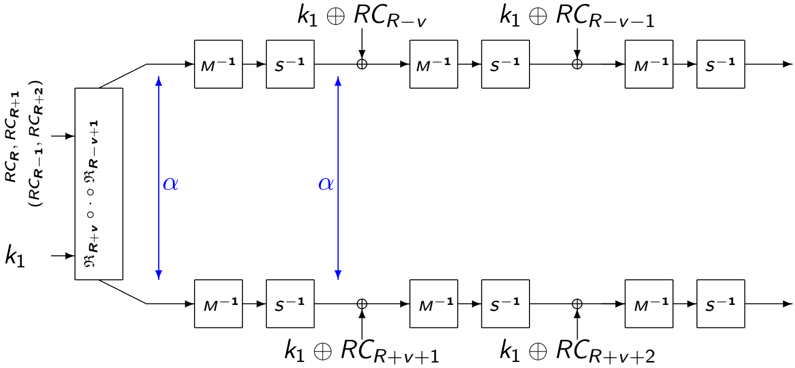
- Cancellation idea.
- Branch and Bound algorithm.



# Cancellation Idea

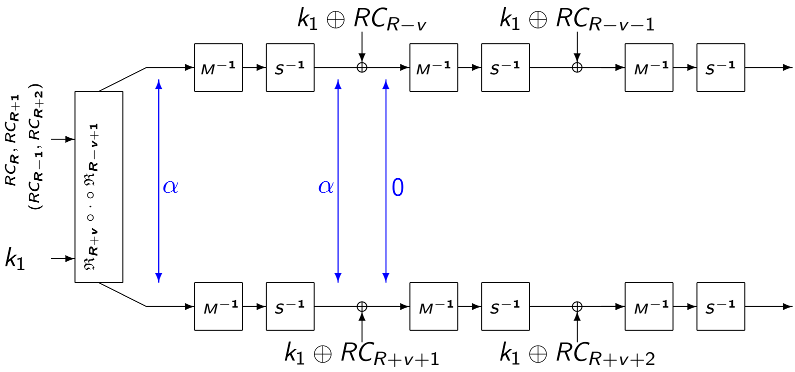


# Cancellation Idea

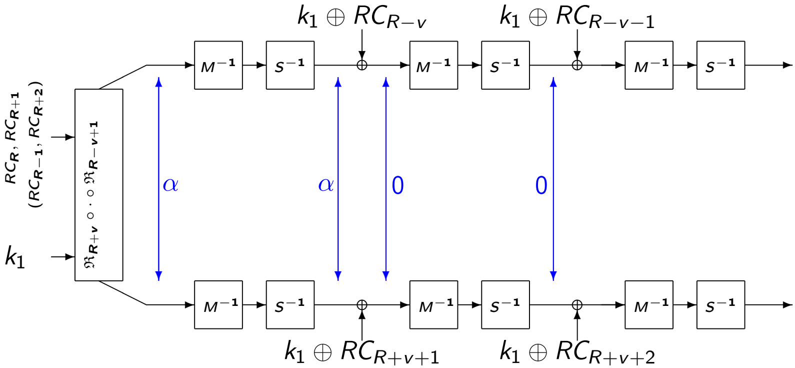



With $\mathcal{P} = \Pr_{\mathbf{X}}\left[S(\mathbf{X}) \oplus S(\mathbf{X} \oplus \alpha) = M^{-1}(\alpha)\right]$

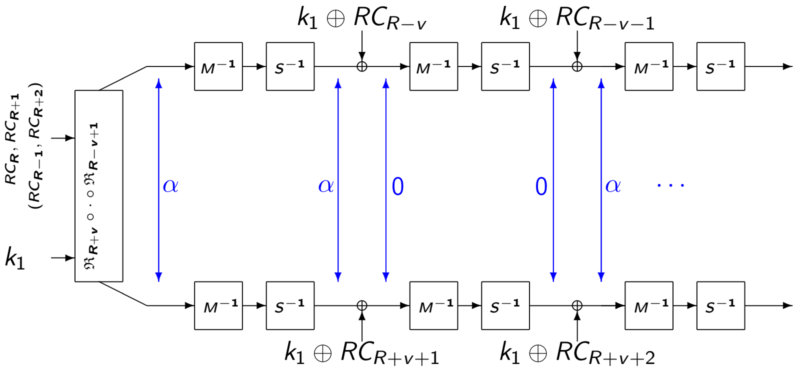
# Cancellation Idea



# Cancellation Idea



# Cancellation Idea




With $\mathcal{P} = \Pr_{\mathbf{X}}\left[S(\mathbf{X}) \oplus S(\mathbf{X} \oplus \alpha) = M^{-1}(\alpha)\right]$ there is an iterative characteristic over four rounds of a PRINCE-like cipher.

# Best $\alpha$ with Cancellation Idea on 12 rounds

| $\alpha$ | $\Delta^*$ | $w(\Delta^*)$ | $\mathcal{P}_{\mathcal{C}_4}$ | Data Compl. | Time Compl. |
|---|---|---|---|---|---|
| 0x8400400800000000 | 0x8800400400000000 | 4 | $2^{-22}$ | $2^{57.95}$ | $2^{71.37}$ |
| 0x8040000040800000 | 0x8080000040400000 | 4 | $2^{-22}$ | $2^{57.95}$ | $2^{71.37}$ |
| 0x0000408000008040 | 0x0000404000008080 | 4 | $2^{-22}$ | $2^{57.95}$ | $2^{71.37}$ |
| 0x0000000048008004 | 0x0000000044008008 | 4 | $2^{-22}$ | $2^{57.95}$ | $2^{71.37}$ |
| 0x0000440040040000 | 0x0000440040040000 | 4 | $2^{-24}$ | $2^{60.27}$ | $2^{73.69}$ |
| 0x8008000000008800 | 0x8008000000008800 | 4 | $2^{-24}$ | $2^{60.27}$ | $2^{73.69}$ |

# Examples of $\alpha$ with Branch and Bound Algorithm on 12 Rounds

| $\alpha$ | $\Delta^*$ | $w(\Delta^*)$ | $\mathcal{P}_{\mathcal{C}_4}$ | Data Compl. | Time Compl. |
|---|---|---|---|---|---|
| 0x0108088088010018 | 0x0000001008000495 | 5 | $2^{-26}$ | $2^{62.78}$ | $2^{80.2}$ |
| 0x0088188080018010 | 0x00000100c09d0008 | 5 | $2^{-26}$ | $2^{62.78}$ | $2^{80.2}$ |
| 0x0108088088010018 | 0x000000100800d8cc | 6 | $2^{-26}$ | $2^{62.83}$ | $2^{84.25}$ |
| 0x0001111011010011 | 0x1101100110000100 | 7 | $2^{-28}$ | $2^{63.45}(a = 32)$ | $2^{88.87}$ |

# Number of non-zero nibbles of $\alpha$

**Observation**

The best results so far have been obtained for $\alpha$ with a small number of non-zero nibbles.

# Number of non-zero nibbles of $\alpha$

**Observation**

The best results so far have been obtained for $\alpha$ with a small number of non-zero nibbles.

**Question**

Would $\alpha$ with many non-zero nibbles guarantee security against reflection attacks?

# Number of non-zero nibbles of $\alpha$

## Observation

The best results so far have been obtained for $\alpha$ with a small number of non-zero nibbles.

## Question

Would $\alpha$ with many non-zero nibbles guarantee security against reflection attacks?

$$\alpha = \begin{bmatrix} \texttt{0x7} & \texttt{0x1} & \texttt{0xc} & \texttt{0xb} \\ \texttt{0x9} & \texttt{0x5} & \texttt{0x9} & \texttt{0x3} \\ \texttt{0x9} & \texttt{0xa} & \texttt{0x5} & \texttt{0x9} \\ \texttt{0x3} & \texttt{0x6} & \texttt{0x8} & \texttt{0xd} \end{bmatrix},$$

# Number of non-zero nibbles of $\alpha$

**Observation**

The best results so far have been obtained for $\alpha$ with a small number of non-zero nibbles.

**Question**

Would $\alpha$ with many non-zero nibbles guarantee security against reflection attacks?

$$\alpha = \begin{bmatrix} \texttt{0x7} & \texttt{0x1} & \texttt{0xc} & \texttt{0xb} \\ \texttt{0x9} & \texttt{0x5} & \texttt{0x9} & \texttt{0x3} \\ \texttt{0x9} & \texttt{0xa} & \texttt{0x5} & \texttt{0x9} \\ \texttt{0x3} & \texttt{0x6} & \texttt{0x8} & \texttt{0xd} \end{bmatrix}, \quad M^{-1}(\alpha) = \begin{bmatrix} \texttt{0x7} & 0 & 0 & 0 \\ 0 & 0 & 0 & \texttt{0xb} \\ 0 & 0 & \texttt{0xd} & 0 \\ 0 & \texttt{0x9} & 0 & 0 \end{bmatrix}.$$

# Truncated Attack

Assume $\alpha$ is such that $M^{-1}(\alpha) = \begin{bmatrix} * & 0 & 0 & 0 \\ 0 & 0 & 0 & * \\ 0 & 0 & * & 0 \\ 0 & * & 0 & 0 \end{bmatrix}$ where $*$ can be any arbitrary value. For six rounds $\mathfrak{R}_{R-2} \circ \cdots \circ \mathfrak{R}_{R+3}$, the following truncated characteristic:

$$Y^O_{R+3} \oplus X^I_{R-2} = \begin{bmatrix} * & 0 & 0 & 0 \\ * & 0 & 0 & * \\ * & 0 & * & 0 \\ * & * & 0 & 0 \end{bmatrix} \oplus \alpha,$$

holds with probability $\mathcal{P}_{F_{M'}} = \frac{|F_{M'}|}{2^n} = 2^{-32}$.

# Truncated Attack

Similar characteristics can be obtained for $\alpha$ such that:

$$M^{-1}(\alpha) = \begin{bmatrix} 0 & * & 0 & 0 \\ * & 0 & 0 & 0 \\ 0 & 0 & 0 & * \\ 0 & 0 & * & 0 \end{bmatrix} \text{ or } M^{-1}(\alpha) = \begin{bmatrix} 0 & 0 & * & 0 \\ 0 & * & 0 & 0 \\ * & 0 & 0 & 0 \\ 0 & 0 & 0 & * \end{bmatrix} \text{ or }$$

$$M^{-1}(\alpha) = \begin{bmatrix} 0 & 0 & 0 & * \\ 0 & 0 & * & 0 \\ 0 & * & 0 & 0 \\ * & 0 & 0 & 0 \end{bmatrix}.$$

- This truncated characteristic over six rounds exists for $4 \times (2^{16} - 1) \approx 2^{18}$ values of $\alpha$,
- Key recovery attack on 8 rounds can be done by data complexity $2^{35.8}$ and time complexity of $2^{96.8}$ memory accesses in addition of $2^{88}$ full encryption.

1 Description of PRINCE-like Ciphers

2 Distinguishers

3 Key Recovery

4 Various Classes of $\alpha$-reflection

5 Conclusions

# Conclusions

- We introduced new generic distinguishers on PRINCE-like ciphers.
- The security of PRINCE-like ciphers depends strongly on the choice of the value of $\alpha$.
- We identified special classes of $\alpha$ for which 4, 6, 8 or 10 rounds can be distinguished from random.
- The weakest class allows an efficient key-recovery attack on 12 rounds of the cipher.
- Our best attack on PRINCE with original $\alpha$ breaks a reduced 6-round version.
- New design criteria for the selection of the value of $\alpha$ for PRINCE-like ciphers are obtained.

Thanks for your attention!