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
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 $k = k_0 || k_1$. 

$$k_0 \rightarrow PRINCE_{core} \rightarrow k_0'$$
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 $k = k_0 || k_1$.

\[ k'_0 = (k_0 \gg 1) \oplus (k_0 \gg (n - 1)) \]
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 $k = k_0 || k_1$.

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

- 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 $k = k_0 || k_1$.

\[ k'_0 = (k_0 \gg 1) \oplus (k_0 \gg (n - 1)) \]

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.
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:

$$RC_{2R-r+1} = RC_r \oplus \alpha, \text{ for all } r = 1, \ldots, 2R$$
The whitening key
Description of PRINCE

- PRINCE-like cipher with $n = 64$.
- Constant is defined as $\alpha = \text{0xc0ac29b7c97c50dd}$.
- 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).

\[ \Delta = 0 \]
Previous Works: Reflection Attack

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

\[
\Delta = 0
\]

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 $f : A \rightarrow A$ 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 $f(x) = x$.

**Lemma**

Let $f : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^n$ 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 $f : A \rightarrow A$ 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 $f(x) = x$.

Lemma

Let $f : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^n$ 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 $I_1$

\[ Pr[M'(x) = x] \]

\[ P_{I_1} = P_{F_{M'}} = \frac{|F_{M'}|}{2^n}. \]
Characteristic $\mathcal{I}_1$

\[
Pr[M'(x) = x] = \mathcal{P}_{F_{M'}} = \frac{|F_{M'}|}{2^n}.
\]
Characteristic $I_1$

$Pr[M'(x) = x]$

$\mathcal{P}_{I_1} = \mathcal{P}_{F_{M'}} = \frac{|F_{M'}|}{2^n}.$
Characteristic $\mathcal{I}_2$

\[
\mathcal{P}_{\mathcal{I}_2} = 2^{-n} \# \{ x \in \mathbb{F}_2^n \mid S^{-1}(M'(S(x))) \oplus x = \alpha \}.
\]
\[ P_{I_2} = 2^{-n} \# \{ x \in \mathbb{F}_2^n | S^{-1}(W(M(S(x)))) \oplus x = \alpha \}. \]
Characteristic $\mathcal{I}_2$

\[ \mathcal{P}_{\mathcal{I}_2} = 2^{-n} \# \left\{ x \in \mathbb{F}_2^n \mid S^{-1}(S'(S(x)))) \oplus x = \alpha \right\}. \]
Characteristic $I_2$

If $P_{I_2} = 0$ then we have impossible differential.
External Characteristic $\mathcal{P}_{Cr}$
<table>
<thead>
<tr>
<th></th>
<th>Description of PRINCE-like Ciphers</th>
<th>Distinguishers</th>
<th>Key Recovery</th>
<th>Various Classes of $\alpha$-reflection</th>
<th>Conclusions</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Description of PRINCE-like Ciphers</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Distinguishers</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Key Recovery</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Various Classes of $\alpha$-reflection</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Conclusions</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Key Recovery

\[ P \rightarrow S \rightarrow M \rightarrow \mathcal{R}_{2R-1} \circ \cdots \circ \mathcal{R}_2 \rightarrow M^{-1} \rightarrow S^{-1} \]

\[RC_1 \oplus \alpha\]

\[c^?_{k_0'} \rightarrow C\]

\[k_0 \]

\[RC_1 \]

\[S\]

\[M\]

\[k_1\]
Key Recovery

\[
P \xrightarrow{k_0} \xrightarrow{RC_1} S \xrightarrow{k_1} M \xrightarrow{\mathcal{R}_{2R-1} \circ \cdots \circ \mathcal{R}_2} M^{-1} \xrightarrow{S^{-1}} RC_1 \oplus \alpha \xrightarrow{k'_0} C
\]
Key Recovery

\[ M^{-1}(\Delta) = \Delta^* \]

\[ \Delta \]

\[ \Delta = M^{-1}(\Delta) = \Delta^* \]

\[ k_0, k_1, k'_0, k'_1 \]

\[ P \rightarrow S \rightarrow M \rightarrow R_{2R-1} \circ \cdots \circ R_2 \rightarrow M^{-1} \rightarrow S^{-1} \rightarrow C \]
Key Recovery Nibble by Nibble

\[ \Delta^*(j) = S(P(j) \oplus k_0(j) \oplus k_1(j) \oplus RC_1(j)) \]
\[ \oplus S(C(j) \oplus k'_0(j) \oplus k_1(j) \oplus RC_2R(j)) \]
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 $\mathcal{P}_C$ of Characteristic

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

- Cancellation idea.
- Branch and Bound algorithm.

\[ k_1 \oplus R_{C_{R-v}} \]

\[ k_1 \oplus R_{C_{R-u-v+1}} \]

\[ k_1 \oplus R_{C_{R-u-v}} \]

\[ M^{-1} \rightarrow S^{-1} \rightarrow \alpha \rightarrow M^{-1} \rightarrow S^{-1} \rightarrow M^{-1} \rightarrow S^{-1} \rightarrow M^{-1} \rightarrow S^{-1} \]

\[ \Delta \]

\[ \Delta^* \]
Cancellation Idea

\[ k_1 \oplus R_{C_{R-v}} \]

\[ k_1 \oplus R_{C_{R-v-1}} \]

\[ \alpha \]

\[ R_{C_{R-1}, R_{C_{R+1}}} \]

\[ M^{-1} S^{-1} \]

\[ M^{-1} S^{-1} \]

\[ M^{-1} S^{-1} \]

\[ M^{-1} S^{-1} \]

\[ M^{-1} S^{-1} \]

\[ M^{-1} S^{-1} \]
Cancellation Idea

\[
\begin{align*}
\text{With } \mathcal{P} &= \Pr_X \left[ S(X) \oplus S(X \oplus \alpha) = M^{-1}(\alpha) \right]
\end{align*}
\]
Cancellation Idea
Cancellation Idea

\[ R^R \cdot k_1 \oplus R^{C_{R-v}} \]

\[ M^{-1} \rightarrow S^{-1} \rightarrow M^{-1} \rightarrow S^{-1} \rightarrow M^{-1} \rightarrow S^{-1} \]

\[ k_1 \oplus R^{C_{R-v-1}} \]
With $\mathcal{P} = \Pr_X \left[ S(X) \oplus S(X \oplus \alpha) = M^{-1}(\alpha) \right]$ there is an iterative characteristic over four rounds of a PRINCE-like cipher.
### Best $\alpha$ with Cancellation Idea on 12 rounds

<table>
<thead>
<tr>
<th>$\alpha$</th>
<th>$\Delta^*$</th>
<th>$\nu(\Delta^*)$</th>
<th>$\mathcal{P}_{C_4}$</th>
<th>Data Compl.</th>
<th>Time Compl.</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x8400400800000000</td>
<td>0x8800400400000000</td>
<td>4</td>
<td>$2^{-22}$</td>
<td>257.95</td>
<td>271.37</td>
</tr>
<tr>
<td>0x8040000040800000</td>
<td>0x8080000040400000</td>
<td>4</td>
<td>$2^{-22}$</td>
<td>257.95</td>
<td>271.37</td>
</tr>
<tr>
<td>0x0000408000008040</td>
<td>0x0000404000008080</td>
<td>4</td>
<td>$2^{-22}$</td>
<td>257.95</td>
<td>271.37</td>
</tr>
<tr>
<td>0x0000000048008004</td>
<td>0x0000000044008008</td>
<td>4</td>
<td>$2^{-22}$</td>
<td>257.95</td>
<td>271.37</td>
</tr>
<tr>
<td>0x0000440040040000</td>
<td>0x0000440040040000</td>
<td>4</td>
<td>$2^{-24}$</td>
<td>260.27</td>
<td>273.69</td>
</tr>
<tr>
<td>0x8008000000008800</td>
<td>0x8008000000008800</td>
<td>4</td>
<td>$2^{-24}$</td>
<td>260.27</td>
<td>273.69</td>
</tr>
</tbody>
</table>
Examples of $\alpha$ with Branch and Bound Algorithm on 12 Rounds

<table>
<thead>
<tr>
<th>$\alpha$</th>
<th>$\Delta^*$</th>
<th>$w(\Delta^*)$</th>
<th>$P_{c_4}$</th>
<th>Data Compl.</th>
<th>Time Compl.</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x0108088088010018</td>
<td>0x0000001008000495</td>
<td>5</td>
<td>2$^{-26}$</td>
<td>262.78</td>
<td>2$^{80.2}$</td>
</tr>
<tr>
<td>0x008818808018010</td>
<td>0x00000100c09d0008</td>
<td>5</td>
<td>2$^{-26}$</td>
<td>262.78</td>
<td>2$^{80.2}$</td>
</tr>
<tr>
<td>0x0108088088010018</td>
<td>0x000000100800d8cc</td>
<td>6</td>
<td>2$^{-26}$</td>
<td>262.83</td>
<td>2$^{84.25}$</td>
</tr>
<tr>
<td>0x0001111011010011</td>
<td>0x1101100110000100</td>
<td>7</td>
<td>2$^{-28}$</td>
<td>263.45$^{(a = 32)}$</td>
<td>2$^{88.87}$</td>
</tr>
</tbody>
</table>
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?

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

$$\alpha = \begin{bmatrix} 0x7 & 0x1 & 0xc & 0xb \\ 0x9 & 0x5 & 0x9 & 0x3 \\ 0x9 & 0xa & 0x5 & 0x9 \\ 0x3 & 0x6 & 0x8 & 0xd \end{bmatrix}, \quad M^{-1}(\alpha) = \begin{bmatrix} 0x7 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0xb \\ 0 & 0 & 0xd & 0 \\ 0 & 0x9 & 0 & 0 \end{bmatrix}.$$
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 $R_{R-2} \circ \cdots \circ R_{R+3}$, the following truncated characteristic:

$$Y_{R+3}^O \oplus X_{R-2}^I = \begin{bmatrix} * & 0 & 0 & 0 \\ * & 0 & 0 & * \\ * & 0 & * & 0 \\ * & * & 0 & 0 \end{bmatrix} \oplus \alpha,$$

holds with probability $P_{F_{M'}} = \frac{|F_{M'}|}{2^n} = 2^{-32}$. 
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!