The 23rd Annual International Conference on Information Security and Cryptology

ICISC 2020

December 2 (Wed) ~ December 4 (Fri), 2020 | Virtual Conference

Hosted by
Korea Institute of Information Security and Cryptology (KIISC)
National Security Research Institute (NSR)

Korea Institute of Information Security & Cryptology

A New Non-random Property of 4.5-Round PRINCE

Bolin Wang, Chan Song, Wenling Wu, Lei Zhang

TCA Laboratory, SKLCS, Institute of Software, Chinese Academy of Sciences

Introduction(1/2)

- PRINCE is a low-latency block cipher structured as a substitution-permutation network (SPN).
- Invariant subspace attack was one of the new cryptanalytic methods. The subspace trail cryptanalysis is a generalization of invariant subspace attack.

Introduction(2/2)

- So far, two subspace trails that exist with probability 1 are known for 2.5 rounds of PRINCE.
- We propose a new non-random property for 4.5 rounds of PRINCE based on subspace trail with certain probability, which is independent of the secret key, the details of the Linear layer and of the S-Box layer.

Table of Contents

Part Ⅰ

PRINCE and its Subspace Trail

PRINCE

- High-level description of PRINCE:
- Lightweight cipher with a state size of 64 bits, organized in a 4×4 matrix (every cell represents a nibble)
- Based on the so called *FX construction*:

$$FX_{k_1,k_0,k_0'} = k_0' \oplus F_{k_1}(\cdot \oplus k_0)$$

- 128 bits $k \equiv (k_0||k_1)$:

$$(k_0||k_0'||k_1) = (k_0||(k_0 \ggg 1) \oplus (k_0 \ll 63)||k_1)$$

PRINCEcore

- 10 Rounds $R_i(\cdot)$:

$$R_i(x) = RC_i \oplus k_1 \oplus SR \circ M' \circ S\text{–}Box(x)$$

- 2 Middle Rounds:

$$S\text{–}Box^{-1} \circ M' \circ S\text{–}Box(\cdot)$$

- α-Reflection property:

$$D_{(k_0||k_0'||k_1)}(\cdot) = E_{(k_0'||k_0||k_1 \oplus \alpha)}(\cdot)$$

Subspace Trail

Appeared at FSE 2017.

Definition

Let $(V_1, V_2, \cdots, V_{r+1})$ denote a set of $r+1$ subspaces with $\dim(V_i) \leq \dim(V_{i+1})$. If for each $i = 1,2,\cdots,r$ and for each $a_i \in V_i^{\perp}$, there exist (unique) $a_{i+1} \in V_{i+1}^{\perp}$ such that $F(V_i \oplus a_i) \subseteq V_{i+1} \oplus a_{i+1}$, then $(V_1, V_2, \cdots, V_{r+1})$ is a **subspace trail** of length r for the function F.

Subspaces of PRINCE

- Column subspaces C_i;

$$C_i = \langle e[4 \cdot i], e[4 \cdot i + 1], e[4 \cdot i + 2], e[4 \cdot i + 3] \rangle$$

- Diagonal subspaces D_i;

$$D_i = SR(C_i)$$

- Inverse-diagonal subspaces ID_i;

$$ID_i = SR^{-1}(C_i)$$

- Mixed subspaces M_i;

$$M_i = M'(D_i)$$

- Inverse-mixed subspaces IM_i;

$$IM_i = M'(ID_i)$$

Subspace Trails for 2.5 rounds of PRINCE (1/2)

- Consider the middle rounds (1.5) and one round before:

$$R^{(2.5)}(\cdot) = M' \circ S\text{–}Box \circ R \circ ARK(\cdot).$$

- For each $a \in C_I^{\perp}$, there exists unique $b \in M_I^{\perp}$ such that

$$R^{(1+1.5)}(C_I \oplus a) = M_I \oplus b.$$

$$C_I \oplus a \xrightarrow{R \circ ARK(\cdot)} D_I \oplus b \xrightarrow{M' \circ S\text{–}Box(\cdot)} M_I \oplus c$$

Subspace Trails for 2.5 rounds of PRINCE (2/2)

- Consider the middle rounds and the linear part of the next round:

$$R^{(2.5)}(\cdot) = M' \circ SR^{-1} \circ ARK(\cdot) \circ super\text{–}SBox \circ ARK(\cdot).$$

- For each $a \in C_I^{\perp}$, there exists unique $b \in IM_I^{\perp}$ such that

$$R^{(2+0.5)}(C_I \oplus a) = IM_I \oplus b.$$

$$C_I \oplus a \xrightarrow{super-SBox \circ ARK(\cdot)} C_I \oplus b \xrightarrow{M' \circ SR^{-1} \circ ARK(\cdot)} IM_I \oplus c$$

Part II

Two 4.5-round Subspace Trails

Proposition

For any D_I and C_J, we have that

$$Prob(x \in C_J | x \in D_I) = 2^{-16|I|+4|I|\cdot|J|}.$$

Compute the probabilities of intersection of D_I and C_J, D_J and C_Q.

Theorem

Let $I, J, Q \subseteq \{0,1,2,3\}$ where $0 < |I| \le 3$, $0 < |J| \le 3$, $0 < |Q| \le 3$. For any I, J and Q, we have that $R^{m_1}(C_I \oplus a) = M_Q \oplus b$ with probability $2^{-16|I|+4|I|\cdot|J|} \cdot 2^{-16|J|+4|J|\cdot|Q|}$, where the input and output of second round needs to consider the intersection of D_I and C_J, D_J and C_Q respectively. Equivalently:

$$\mathrm{Prob}\left(R^{m_1}(x) \oplus R^{m_1}(y) \in M_Q \middle| x \oplus y \in C_I\right) = 2^{-16|I|+4|I|\cdot|J|} \cdot 2^{-16|J|+4|J|\cdot|Q|},$$

$$C_I \oplus a \xrightarrow{R(\cdot)} D_I \oplus b \xrightarrow{R(\cdot)} C_Q \oplus c \xrightarrow{R(\cdot)} D_Q \oplus d \xrightarrow{\Lambda(\cdot)} M_Q \oplus e$$

where $m_1 = 2 + 1 + 1.5$, $\Lambda(\cdot) = M' \circ S\text{-}Box$.

Theorem

Let $I, J, Q \subseteq \{0,1,2,3\}$ where $0 < |I| \leq 3$, $0 < |J| \leq 3$, $0 < |Q| \leq 3$. For any I, J and Q, we have that$R^{m_2}(C_I \oplus a) = IM_Q \oplus b$ with probability $2^{-16|I|+4|I|\cdot|J|} \cdot 2^{-16|J|+4|J|\cdot|Q|}$, where the input and output of second round needs to consider th e intersection of D_I and C_J, D_J and C_Q respectively. Equivalently:

$$\mathrm{Prob}\left(R^{m_2}(x) \oplus R^{m_2}(y) \in IM_Q \middle| x \oplus y \in C_I\right) = 2^{-16|I|+4|I|\cdot|J|} \cdot 2^{-16|J|+4|J|\cdot|Q|},$$

$$C_I \oplus a \xrightarrow{R(\cdot)} D_I \oplus b \xrightarrow{R(\cdot)} C_Q \oplus c \xrightarrow{\Gamma_1(\cdot)} C_Q \oplus d \xrightarrow{\Gamma_2(\cdot)} IM_Q \oplus e$$

where $m_2 = 2 + 2 + 0.5, \Gamma_1(\cdot) = super\text{–}SBox \circ ARK(\cdot), \Gamma_2(\cdot) = M' \circ SR^{-1} \circ ARK(\cdot)$.

Part III

Structural Property of 4.5-round PRINCE

Using the first 4.5-round subspace trail, given $C_I \oplus a$ (i.e. an arbitrary coset of C_I), consider all the 2^{16} plaintexts and the corresponding ciphertexts after 4.5 rounds that is $(p^i, c^i = R^{2+1+1.5}(p^i))$ for $i = 0, \ldots, 2^{16} - 1$ where $p^i \in C_I \oplus a$.

Theorem

For certain fixed Q, let n be the number of different pairs of ciphertexts (c^i, c^j) for $i \neq j$ such that $c^i \oplus c^j \in M_Q$

$$n := |\{(p^i, c^i), (p^j, c^j) | \forall p^i, p^j \in C_I \oplus a, p^i < p^j \text{ and } c^i \oplus c^j \in M_Q\}|.$$

The number n is a multiple of 8, that is $\exists n' \in \mathbb{N}$ such that $n = 8 \cdot n'$,

Using the second 4.5-round subspace trail, given $C_I \oplus a$ (i.e. an arbitrary coset of C_I), consider all the 2^{16} plaintexts and the corresponding ciphertexts after 4.5 rounds that is $(p^i, c^i = R^{2+2+0.5}(p^i))$ for $i = 0, \ldots, 2^{16} - 1$ where $p^i \in C_I \oplus a$.

Theorem

For certain fixed Q, let n be the number of different pairs of ciphertexts (c^i, c^j) for $i \neq j$ such that $c^i \oplus c^j \in IM_Q$

$$n := |\{(p^i, c^i), (p^j, c^j) | \forall p^i, p^j \in C_I \oplus a, p^i < p^j \text{ and } c^i \oplus c^j \in IM_Q\}|.$$

The number n is a multiple of 8, that is $\exists n' \in \mathbb{N}$ such that $n = 8 \cdot n'$,

“$<$” in the above two Theorems means the partial order.

Part IV

Sketch of the Proof

Reduction to a Single Round (1/2)

Remember:

$$R^{(1+1.5)}(C_Q \oplus a) = M_Q \oplus b.$$

And for each x, y :

$$Prob(R^{(1+1.5)}(x) \oplus R^{(1+1.5)}(y) \in M_I | x \oplus y \in C_I) = 1.$$

Again, for one forward round, we have $R(C_I \oplus a) = D_I \oplus b.$

Since

$$C_I \oplus a \xrightarrow{R(\cdot)} D_I \oplus b \xrightarrow{R(\cdot)} C_Q \oplus c \xrightarrow{R^{1+1.5}(\cdot)} M_Q \oplus d,$$

We can focus on the second round $D_I \oplus b \xrightarrow{R(\cdot)} C_Q \oplus b$.

Reduction to a Single Round (2/2)

Given an arbitrary coset of D_I, consider all the 2^{16} plaintexts and the corresponding ciphertexts after 1 round, that is $(\hat{p}^i, \hat{c}^i)$ for $i = 0, \ldots, 2^{16} - 1$ where $\hat{c}^i = R(\hat{p}^i)$.

Lemma

For certain fixed I and Q, and assume $|I| = 1$, let n be the number of different pairs of ciphertexts $(\hat{c}^i, \hat{c}^j)$ for $i \neq j$ such that $\hat{c}^i \oplus \hat{c}^j \in C_Q$

$$n \coloneqq |\{(p^i, c^i), (p^j, c^j) | \forall p^i, p^j \in D_I \oplus a, p^i < p^j \text{ } and \text{ } c^i \oplus c^j \in C_Q\}|.$$

The number n is a multiple of 8, that is $\exists n' \in \mathbb{N}$ such that $n = 8 \cdot n'$

Sketch of the Proof

W.l.o.g. I= $\{0\}$.

Given $p^1, p^2 \in D_i \oplus a$, by definition of D_i, there exist $x, y, z, w \in F_{2^4}$ and $x', y', z', w' \in F_{2^4}$ such that:

$$p^1 = a \oplus \begin{bmatrix} x & 0 & 0 & 0 \\ 0 & 0 & 0 & y \\ 0 & 0 & z & 0 \\ 0 & w & 0 & 0 \end{bmatrix}, p^2 = a \oplus \begin{bmatrix} x' & 0 & 0 & 0 \\ 0 & 0 & 0 & y' \\ 0 & 0 & z' & 0 \\ 0 & w' & 0 & 0 \end{bmatrix},$$

For the following:

$$p^1 \equiv < x, y, z, w > \text{ and } p^2 \equiv < x', y', z', w' > .$$

Study the following cases:

- 3 variables are equal, e.g. $y = y'$, $z = z'$, $w = w'$, $x \neq x'$;
- 2 variables are equal, e.g. $y = y'$, $z = z'$, $x \neq x'$, $w \neq w'$;
- 1 variable is equal, e.g. $y = y'$, $x \neq x'$, $z \neq z'$, $w \neq w'$;
- All variables are different, e.g. $x \neq x'$, $y \neq y'$, $z \neq z'$, $w \neq w'$.

First Case:

If 3 variables are equal, then $R(p^1)\oplus R(p^2) \in D_0$ with prob. 1.

$$(R(p^1)\oplus R(p^2))_{0,0} = \alpha_3(S-Box(x\oplus a_{0,0})\oplus S-Box(x'\oplus a_{0,0})),$$
$$(R(p^1)\oplus R(p^2))_{1,3} = \alpha_2(S-Box(x\oplus a_{0,0})\oplus S-Box(x'\oplus a_{0,0})),$$
$$(R(p^1)\oplus R(p^2))_{2,2} = \alpha_1(S-Box(x\oplus a_{0,0})\oplus S-Box(x'\oplus a_{0,0})),$$
$$(R(p^1)\oplus R(p^2))_{3,1} = \alpha_0(S-Box(x\oplus a_{0,0})\oplus S-Box(x'\oplus a_{0,0})).$$

It is possible that p^1 and p^2 exist such that $R(p^1)\oplus R(p^2) \in C_Q$ for | Q | = 3.

$R(p^1)\oplus R(p^2) \in C_Q$ for | Q | = 3 if and only if one column of $R(p^1)\oplus R(p^2)$ is eq ual to zero.

Second Case:

W.l.o.g. consider $p^1 \equiv < x, y, z, w >$ and $p^2 \equiv < x', y, z, w' >$.

$$R(p^1) \oplus R(p^2) \in C_Q \text{ if and only if } R(\hat{p}^1) \oplus R(\hat{p}^2) \in C_Q$$

where $\hat{p}^1 \equiv < x', y, z, w >$, $\hat{p}^2 \equiv < x, y, z, w' >$, for all $y, z \in F_{2^4}$.

It is sufficient to compute $R(p^1) \oplus R(p^2) = R(\hat{p}^1) \oplus R(\hat{p}^2)$.

Given p^1 and p^2, is it possible that x, x', w, w' exist such that $R(p^1) \oplus R(p^2) \in C_Q$ for $|\, Q \,| = 3$?

Second Case:

Compute and analyze the first column (the others are analogous):

$$(R(p^1)\oplus R(p^2))_{\cdot,0} = \begin{bmatrix} \alpha_3(S-Box(x\oplus a_{0,0})\oplus S-Box(x'\oplus a_{0,0})) \\ \alpha_2(S-Box(w\oplus a_{3,1})\oplus S-Box(w'\oplus a_{3,1})) \\ 0 \\ 0 \end{bmatrix}$$

Third Case:

W.l.o.g. consider $p^1 \equiv < x, y, z, w >$ and $p^2 \equiv < x', y, z', w' >$.

$$R(p^1) \oplus R(p^2) \in C_Q \text{ if and only if } R(\hat{p}^1) \oplus R(\hat{p}^2) \in C_Q \text{ where}$$

$$p^1 \equiv \langle x', y, z, w \rangle \text{ and } p^2 \equiv \langle x, y, z', w' \rangle$$

$$p^1 \equiv \langle x, y, z', w \rangle \text{ and } p^2 \equiv \langle x', y, z, w' \rangle$$

$$p^1 \equiv \langle x, y, z, w' \rangle \text{ and } p^2 \equiv \langle x', y, z', w \rangle$$

for each $y \in F_{2^4}$.

Forth Case:

W.l.o.g. consider $p^1 \equiv < x, y, z, w >$ and $p^2 \equiv < x', y', z', w' >$.

$R(p^1) \oplus R(p^2) \in C_Q$ if and only if $R(\hat{p}^1) \oplus R(\hat{p}^2) \in C_Q$ where

$p^1 \equiv \langle x', y, z, w \rangle$ and $p^2 \equiv \langle x, y', z', w' \rangle$

$p^1 \equiv \langle x, y', z, w \rangle$ and $p^2 \equiv \langle x', y, z', w' \rangle$

$p^1 \equiv \langle x, y, z', w \rangle$ and $p^2 \equiv \langle x', y', z, w' \rangle$

$p^1 \equiv \langle x, y, z, w' \rangle$ and $p^2 \equiv \langle x', y', z', w \rangle$

$p^1 \equiv \langle x', y', z, w \rangle$ and $p^2 \equiv \langle x, y, z', w' \rangle$

$p^1 \equiv \langle x', y, z', w \rangle$ and $p^2 \equiv \langle x, y', z, w' \rangle$

$p^1 \equiv \langle x', y, z, w' \rangle$ and $p^2 \equiv \langle x, y', z', w \rangle$

Conclusion:

$$n \coloneqq |\{(p^i, c^i), (p^j, c^j) | \forall p^i, p^j \in D_I \oplus a, p^i < p^j \ and \ c^i \oplus c^j \in C_Q\}|.$$

Given a coset of D_i, we analyze the number of collisions in the same coset of C_Q after one round.

Since $|\mathrm{Q}| = 3$, there exist $n_1, n_2, n_3, n_4 \in N$ such that the total number of collisions n is equal to $n = 2^{12} \cdot n_1 + 2^9 \cdot n_2 + 2^6 \cdot n_3 + 8 \cdot n_4 = 8 \cdot (2^9 \cdot n_1 + 2^6 \cdot n_2 + 2^3 \cdot n_3 + n_4)$, i.e. it is a multiple of 8.

Part V

Open Problems

- Set up a 6-round Secret-Key Distinguisher for PRINCE indepen dent of the secret key;
- Set up a key recovery attack that exploits this 4.5-round secret key distinguisher;
- Apply “similar” distinguisher to other constructions.

Thanks for your attention!

Questions?

Comments?

Partial Order of the Plaintexts

Definition

Given two different texts t^1 and t^2, we say that $t^1 \leq t^2$ if $t^1 = t^2$ or if there exists $i, j \in \{0,1,2,3\}$ such that

(1) $t^1_{k,l} = t^2_{k,l}$ for all $k, l \in \{0,1,2,3\}$ with $k + 4 \cdot l < i + 4 \cdot j$;

(2) $t^1_{i,j} < t^2_{i,j}$.