Practical low data-complexity subspace-trail cryptanalysis of round-reduced PRINCE

Lorenzo Grassi and Christian Rechberger

December, 2016

Introduction

One of the most analyzed lightweight block-cipher is PRINCE [**BCG+12**], which inspired follow-up designs as QARMA, MANTIS, Midori, ...

To encourage cryptanalysis, “The PRINCE Challenge” was organized with the goal to find *practical* attacks.

Introduction

In this paper:

- *Truncated Differential Attack* for 4 rounds of PRINCE
  - Co-Winner of the *Third* PRINCE Challenge;
  - data complexity of 8 CP/CC and computational cost of 2^{18} E;
  - *practically verified*;
- Analysis of PRINCE-like structure - Equivalent Variant of PRINCE.

Table of Contents

Part I

PRINCE and its Subspace Trail

PRINCE

High-level description of PRINCE:

- *lightweight cipher* with state size of 64 bits, organized in a 4×4 matrix (every cell represents a nibble);
- based on the so called *FX construction*:

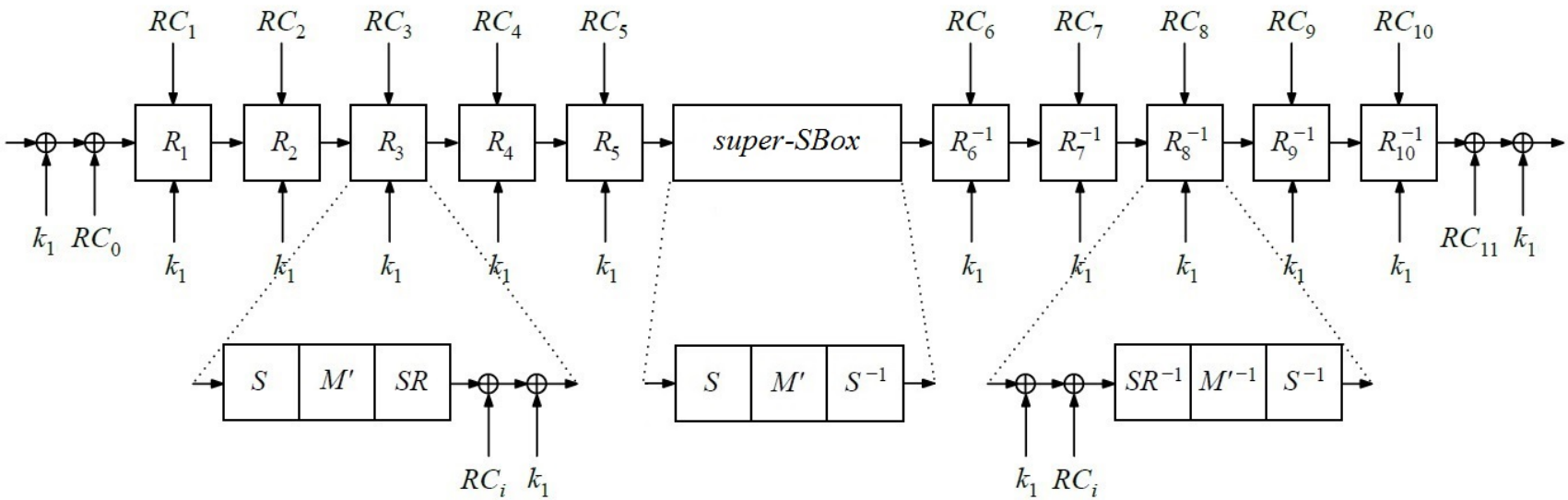
$$FX_{k_1,k_0,k_0'}(\cdot) = k_0' \oplus F_{k_1}(\cdot \oplus k_0);$$

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

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

- core cipher “PRINCEcore” is a *substitution-permutation network*.

PRINCEcore



"PRINCEcore" composed of 12 Rounds:

- 10 Rounds $R_i(\cdot)$:

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

- 2 Middle Rounds: $\text{S-Box}^{-1} \circ M' \circ \text{S-Box}(\cdot)$

PRINCE - The Reflection Property

Since:

- $M' = M'^{-1}$,
- $RC_i \oplus RC_{11-i} = constant$,

PRINCE has the α-reflection property:

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

Follows-up designs - QARMA, MANTIS, Midori, ... - were inspired by PRINCE.

PRINCE - The Reflection Property

Since:

- $M' = M'^{-1}$,
- $RC_i \oplus RC_{11-i} = constant$,

PRINCE has the α-reflection property:

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

Follows-up designs - QARMA, MANTIS, Midori, ... - were inspired by PRINCE.

Subspace Trail

Appeared at FSE 2017 [**GRR17**] - Allows to describe some key-recovery attacks in an easier and more formal way.

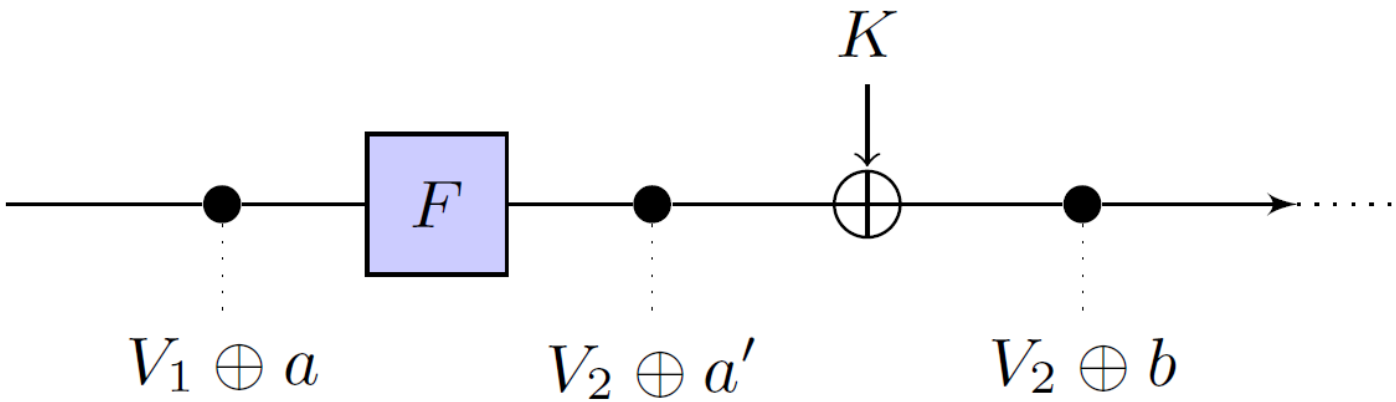
Definition

Let $(V_0, V_1, ..., V_r)$ denote a set of $r+1$ subspaces with $\dim(V_i) \leq \dim(V_{i+1})$. If for each $i = 0, ..., r-1$ and for each $a_i \in V_i^{\perp}$, there exists (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 $(V_0, V_1, ..., V_r)$ is a subspace trail of length r for the function F.

Subspace Trail - Example



Example of Subspace Trail: $\forall a \in V_1^{\perp}$ there exists $b \in V_2^{\perp}$ s.t.

$$F(V_1 \oplus a) \subseteq V_2 \oplus b.$$

Subspaces for PRINCE

We define the following subspaces:

- *column space* $\mathcal{C}_i$;
- *diagonal space* $\mathcal{D}_i$;
- *inverse-diagonal space* $\mathcal{ID}_i$;
- *mixed space* $\mathcal{M}_i$;
- *inverse-mixed space* $\mathcal{IM}_i$.

The Column Space

Definition

The *column spaces* $\mathcal{C}_i$ for $i \in \{0, 1, 2, 3\}$ are defined as

$$\mathcal{C}_i = \langle e_{0,i}, e_{1,i}, e_{2,i}, e_{3,i} \rangle.$$

E.g. $\mathcal{C}_0$ corresponds to the symbolic matrix

$$\mathcal{C}_0 = \left\{ \begin{bmatrix} x & 0 & 0 & 0 \\ y & 0 & 0 & 0 \\ z & 0 & 0 & 0 \\ w & 0 & 0 & 0 \end{bmatrix} \;\middle|\; \forall x, y, w, z \in \mathbb{F}_{2^4} \right\} \equiv \begin{bmatrix} x & 0 & 0 & 0 \\ y & 0 & 0 & 0 \\ z & 0 & 0 & 0 \\ w & 0 & 0 & 0 \end{bmatrix}$$

The Column Space

Definition

The *column spaces* $\mathcal{C}_i$ for $i \in \{0, 1, 2, 3\}$ are defined as

$$\mathcal{C}_i = \langle e_{0,i}, e_{1,i}, e_{2,i}, e_{3,i} \rangle.$$

$\mathcal{C}_i$ is an *invariant subspace* for the middle-rounds:

$$\text{S-Box}^{-1} \circ M' \circ \text{S-Box}(\mathcal{C}_i \oplus a) = \mathcal{C}_i \oplus b.$$

The Diagonal and Inverse-Diagonal Space

Definition

The *diagonal spaces* $\mathcal{D}_i$ for $i \in \{0, 1, 2, 3\}$ and the *inverse-diagonal space* are defined as

$$\mathcal{D}_i = SR(\mathcal{C}_i), \qquad \mathcal{ID}_i = SR^{-1}(\mathcal{C}_i).$$

E.g. $\mathcal{D}_0$ corresponds to symbolic matrix

$$\mathcal{D}_0 \equiv \begin{bmatrix} x & 0 & 0 & 0 \\ 0 & 0 & 0 & y \\ 0 & 0 & z & 0 \\ 0 & w & 0 & 0 \end{bmatrix}$$

for all $x, y, w, z \in \mathbb{F}_{2^4}$.

The Mixed and Inverse-Mixed Space

Definition

The *i-th mixed spaces* $\mathcal{M}_i$ for $i \in \{0, 1, 2, 3\}$ and the *i-th inverse-mixed spaces* $\mathcal{IM}_i$ are defined as

$$\mathcal{M}_i = M'(\mathcal{D}_i), \qquad \mathcal{IM}_i = M'(\mathcal{ID}_i).$$

E.g. $\mathcal{M}_0$ corresponds to symbolic matrix

$$\mathcal{M}_0 \equiv \begin{bmatrix} \alpha_3(x) & \alpha_3(z) & \alpha_0(w) & \alpha_2(y) \\ \alpha_2(x) & \alpha_2(z) & \alpha_3(w) & \alpha_1(y) \\ \alpha_1(x) & \alpha_1(z) & \alpha_2(w) & \alpha_0(y) \\ \alpha_0(x) & \alpha_0(z) & \alpha_1(w) & \alpha_3(y) \end{bmatrix}$$

where $\alpha_i(\cdot) := \cdot \wedge (0x2^i \oplus 0xf)$, i.e. $\alpha_0(\cdot) = \cdot \wedge 0xe$, $\alpha_1(\cdot) = \cdot \wedge 0xd$, $\alpha_2(\cdot) = \cdot \wedge 0xb$ and $\alpha_3(\cdot) = \cdot \wedge 0x7$.

Subspace Trail for PRINCE (1/2)

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

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

For each $a \in \mathcal{C}_i^{\perp}$, there exists $b \in \mathcal{M}_i^{\perp}$ s.t.

$$R^{(2.5)}(\mathcal{C}_i \oplus a) = \mathcal{M}_i \oplus b$$

since

$$\mathcal{C}_i \oplus a \xrightarrow{R \circ ARK(\cdot)} \mathcal{D}_i \oplus d \xrightarrow{M' \circ \text{S-Box}} \mathcal{M}_i \oplus b.$$

Subspace Trail for PRINCE (1/2)

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

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

For each $a \in \mathcal{C}_i^{\perp}$, there exists $b \in \mathcal{M}_i^{\perp}$ s.t.

$$R^{(2.5)}(\mathcal{C}_i \oplus a) = \mathcal{M}_i \oplus b$$

since

$$\mathcal{C}_i \oplus a \xrightarrow{R \circ ARK(\cdot)} \mathcal{D}_i \oplus d \xrightarrow{M' \circ \text{S-Box}} \mathcal{M}_i \oplus b.$$

Subspace Trail for PRINCE (2/2)

Since $R^{(2.5)}(\mathcal{C}_i \oplus a) = \mathcal{M}_i \oplus b$:

Lemma

$$Prob(R^{(2.5)}(x) \oplus R^{(2.5)}(y) \in \mathcal{M}_i \mid x \oplus y \in \mathcal{C}_i) = 1.$$

Exploit this probability to set up the truncated differential attack on the 4 middle rounds of PRINCE.

Part II

Truncated Differential Attack on 4 Rounds of PRINCE

Truncated Differential on 4-rounds PRINCE

We have just seen that

$$Prob(R^{(2.5)}(x) \oplus R^{(2.5)}(y) \in \mathcal{M}_i \mid x \oplus y \in \mathcal{C}_i) = 1.$$

Idea: recover the key using a *Truncated Differential Attack on the 4 central rounds*:

$$p^1, p^2 \xrightarrow{R(\cdot)} \xrightarrow{M' \circ \text{S-Box}(\cdot)} R^{(2.5)}(p^1), R^{(2.5)}(p^2)$$

$$R^{(2.5)}(p^1), R^{(2.5)}(p^2) \xleftarrow{\text{S-Box} \circ ARK(\cdot)} \xleftarrow{R(\cdot)} c^1, c^2.$$

Why Truncated Differential Attack?

- Given p^1, p^2 s.t. $p^1 \oplus p^2 \in \mathcal{C}_i$ and corresponding ciphertexts c^1, c^2, we are looking for keys k_1 and $\hat{k} \equiv k_1 \oplus k_0'$ s.t.

$$\text{S-Box}\big(k_1 \oplus R_{\hat{k}}(c^1)\big) \oplus \text{S-Box}\big(k_1 \oplus R_{\hat{k}}(c^2)\big) \in \mathcal{M}_i.$$

- Since $M'(\mathcal{M}_i) \equiv \mathcal{D}_i$ and since M' is linear:

$$M'(\text{S-Box}\big(k_1 \oplus R_{\hat{k}}(c^1)\big)) \oplus M'(\text{S-Box}\big(k_1 \oplus R_{\hat{k}}(c^2)\big)) \in \mathcal{D}_i.$$

- By definition of $\mathcal{D}_i$, we are looking for keys k_1 and $\hat{k}$ s.t. some nibbles of

$$M'(\text{S-Box}\big(k_1 \oplus R_{\hat{k}}(c^1)\big)) \oplus M'(\text{S-Box}\big(k_1 \oplus R_{\hat{k}}(c^2)\big))$$

are equal to zero (no condition on the others).

Why Truncated Differential Attack?

- Given p^1, p^2 s.t. $p^1 \oplus p^2 \in \mathcal{C}_i$ and corresponding ciphertexts c^1, c^2, we are looking for keys k_1 and $\hat{k} \equiv k_1 \oplus k_0'$ s.t.

$$\text{S-Box}\big(k_1 \oplus R_{\hat{k}}(c^1)\big) \oplus \text{S-Box}\big(k_1 \oplus R_{\hat{k}}(c^2)\big) \in \mathcal{M}_i.$$

- Since $M'(\mathcal{M}_i) \equiv \mathcal{D}_i$ and since M' is linear:

$$M'(\text{S-Box}\big(k_1 \oplus R_{\hat{k}}(c^1)\big)) \oplus M'(\text{S-Box}\big(k_1 \oplus R_{\hat{k}}(c^2)\big)) \in \mathcal{D}_i.$$

- By definition of $\mathcal{D}_i$, we are looking for keys k_1 and $\hat{k}$ s.t. some nibbles of

$$M'(\text{S-Box}\big(k_1 \oplus R_{\hat{k}}(c^1)\big)) \oplus M'(\text{S-Box}\big(k_1 \oplus R_{\hat{k}}(c^2)\big))$$

are equal to zero (no condition on the others).

Why Truncated Differential Attack?

- Given p^1, p^2 s.t. $p^1 \oplus p^2 \in \mathcal{C}_i$ and corresponding ciphertexts c^1, c^2, we are looking for keys k_1 and $\hat{k} \equiv k_1 \oplus k_0'$ s.t.

$$\text{S-Box}\big(k_1 \oplus R_{\hat{k}}(c^1)\big) \oplus \text{S-Box}\big(k_1 \oplus R_{\hat{k}}(c^2)\big) \in \mathcal{M}_i.$$

- Since $M'(\mathcal{M}_i) \equiv \mathcal{D}_i$ and since M' is linear:

$$M'(\text{S-Box}\big(k_1 \oplus R_{\hat{k}}(c^1)\big)) \oplus M'(\text{S-Box}\big(k_1 \oplus R_{\hat{k}}(c^2)\big)) \in \mathcal{D}_i.$$

- By definition of $\mathcal{D}_i$, we are looking for keys k_1 and $\hat{k}$ s.t. some nibbles of

$$M'(\text{S-Box}\big(k_1 \oplus R_{\hat{k}}(c^1)\big)) \oplus M'(\text{S-Box}\big(k_1 \oplus R_{\hat{k}}(c^2)\big))$$

  are equal to zero (no condition on the others).

Idea of the Attack

W.l.o.g. consider $\mathcal{M}_0$:

$$\mathcal{M}_0 \equiv \begin{bmatrix} \alpha_3(x) & \alpha_3(z) & \alpha_0(w) & \alpha_2(y) \\ \alpha_2(x) & \alpha_2(z) & \alpha_3(w) & \alpha_1(y) \\ \alpha_1(x) & \alpha_1(z) & \alpha_2(w) & \alpha_0(y) \\ \alpha_0(x) & \alpha_0(z) & \alpha_1(w) & \alpha_3(y) \end{bmatrix}.$$

For guessed keys $k_1, k_1 \oplus k_0'$, check if
$\text{S-Box}\big(k_1 \oplus R_{\hat{k}}(c^1)\big) \oplus \text{S-Box}\big(k_1 \oplus R_{\hat{k}}(c^2)\big) \in \mathcal{M}_0$ or not.

Given a text t, *how to check if t belongs in $\mathcal{M}_0$?*

- Working independently on each nibble of t;
- For each column, exploiting the relationships that hold among the nibbles of t.

Idea of the Attack

W.l.o.g. consider $\mathcal{M}_0$:

$$\mathcal{M}_0 \equiv \begin{bmatrix} \alpha_3(x) & \alpha_3(z) & \alpha_0(w) & \alpha_2(y) \\ \alpha_2(x) & \alpha_2(z) & \alpha_3(w) & \alpha_1(y) \\ \alpha_1(x) & \alpha_1(z) & \alpha_2(w) & \alpha_0(y) \\ \alpha_0(x) & \alpha_0(z) & \alpha_1(w) & \alpha_3(y) \end{bmatrix}.$$

For guessed keys $k_1, k_1 \oplus k_0'$, check if
$\text{S-Box}\big(k_1 \oplus R_{\hat{k}}(c^1)\big) \oplus \text{S-Box}\big(k_1 \oplus R_{\hat{k}}(c^2)\big) \in \mathcal{M}_0$ or not.

Given a text t, *how to check if t belongs in $\mathcal{M}_0$?*

- Working independently on each nibble of t;
- For each column, exploiting the relationships that hold among the nibbles of t.

Idea of the Attack (1/2)

W.l.o.g. consider $\mathcal{M}_0$:

$$\mathcal{M}_0 \equiv \begin{bmatrix} \alpha_3(x) & \alpha_3(z) & \alpha_0(w) & \alpha_2(y) \\ \alpha_2(x) & \alpha_2(z) & \alpha_3(w) & \alpha_1(y) \\ \alpha_1(x) & \alpha_1(z) & \alpha_2(w) & \alpha_0(y) \\ \alpha_0(x) & \alpha_0(z) & \alpha_1(w) & \alpha_3(y) \end{bmatrix}.$$

If $t \in \mathcal{M}_0$, then

$$t_{0,0} \wedge 0\text{x}8 = 0,$$
$$t_{1,0} \wedge 0\text{x}4 = 0,$$
$$\ldots$$

Work independently on each nibble.

Idea of the Attack (2/2)

W.l.o.g. consider $\mathcal{M}_0$:

$$\mathcal{M}_0 \equiv \begin{bmatrix} \alpha_3(x) & \alpha_3(z) & \alpha_0(w) & \alpha_2(y) \\ \alpha_2(x) & \alpha_2(z) & \alpha_3(w) & \alpha_1(y) \\ \alpha_1(x) & \alpha_1(z) & \alpha_2(w) & \alpha_0(y) \\ \alpha_0(x) & \alpha_0(z) & \alpha_1(w) & \alpha_3(y) \end{bmatrix}.$$

If $t \in \mathcal{M}_0$, then

$$t_{0,0} \wedge 0\text{x}b = t_{1,0} \wedge 0\text{x}7,$$
$$t_{2,0} \wedge 0\text{x}b = t_{1,0} \wedge 0\text{x}d,$$
$$\ldots$$

Exploit the relationships among the nibbles.

Attack on 4 Rounds

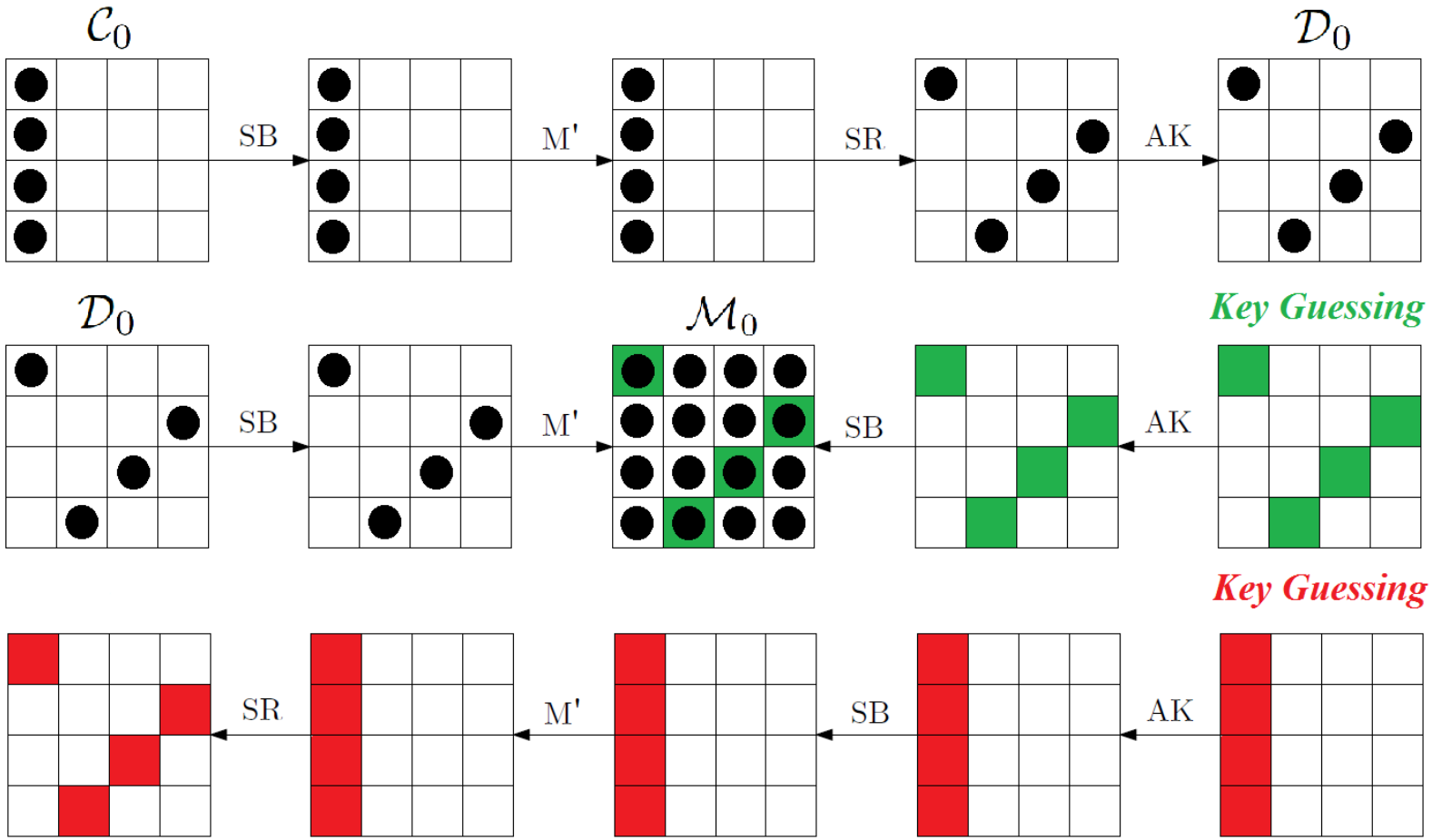
Working independently on each column, two steps of the attack

1. recover 4 nibbles of the final key $k'_0 \oplus k_1$ and 4 nibbles of the key k_1 working independently on each nibble;

2. using the knowledge of the nibbles just found, recover the rest of the key by exploiting the relationships among the nibbles.

The attack can be set up in other different ways: *the previous one requires the minimum data complexity* (the computational cost is still very competitive).

1st Step - Work Independently on each Nibble



Red: Guessed Nibbles of $k_1 \oplus k_0'$ - *Green*: Guessed Nibbles of k_1

Attack on 4 Rounds

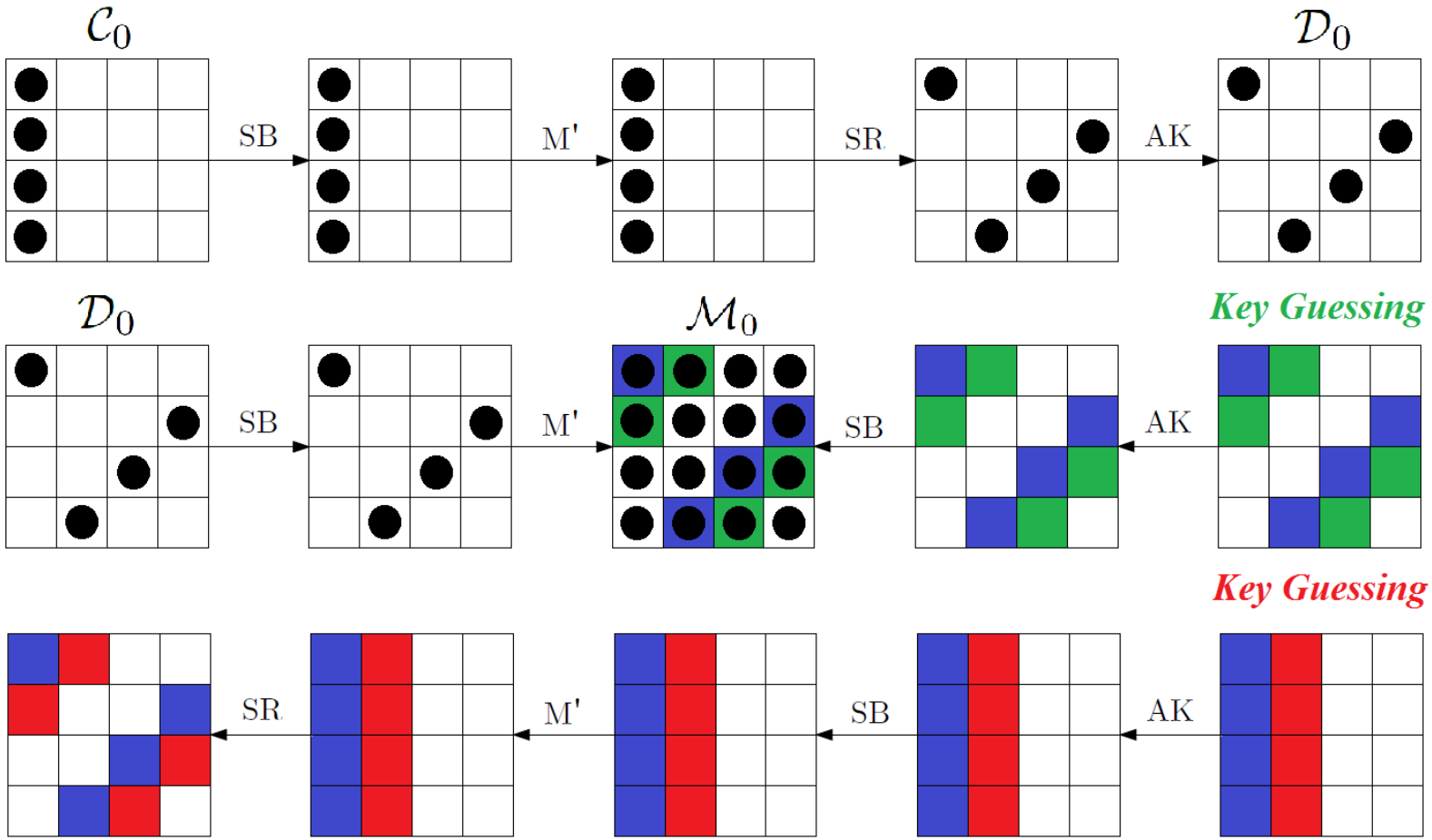
Working independently on each column, two steps of the attack

1. recover 4 nibbles of the final key $k'_0 \oplus k_1$ and 4 nibbles of the key k_1 working independently on each nibble;

2. using the knowledge of the nibbles just found, recover the rest of the key by exploiting the relationships among the nibbles.

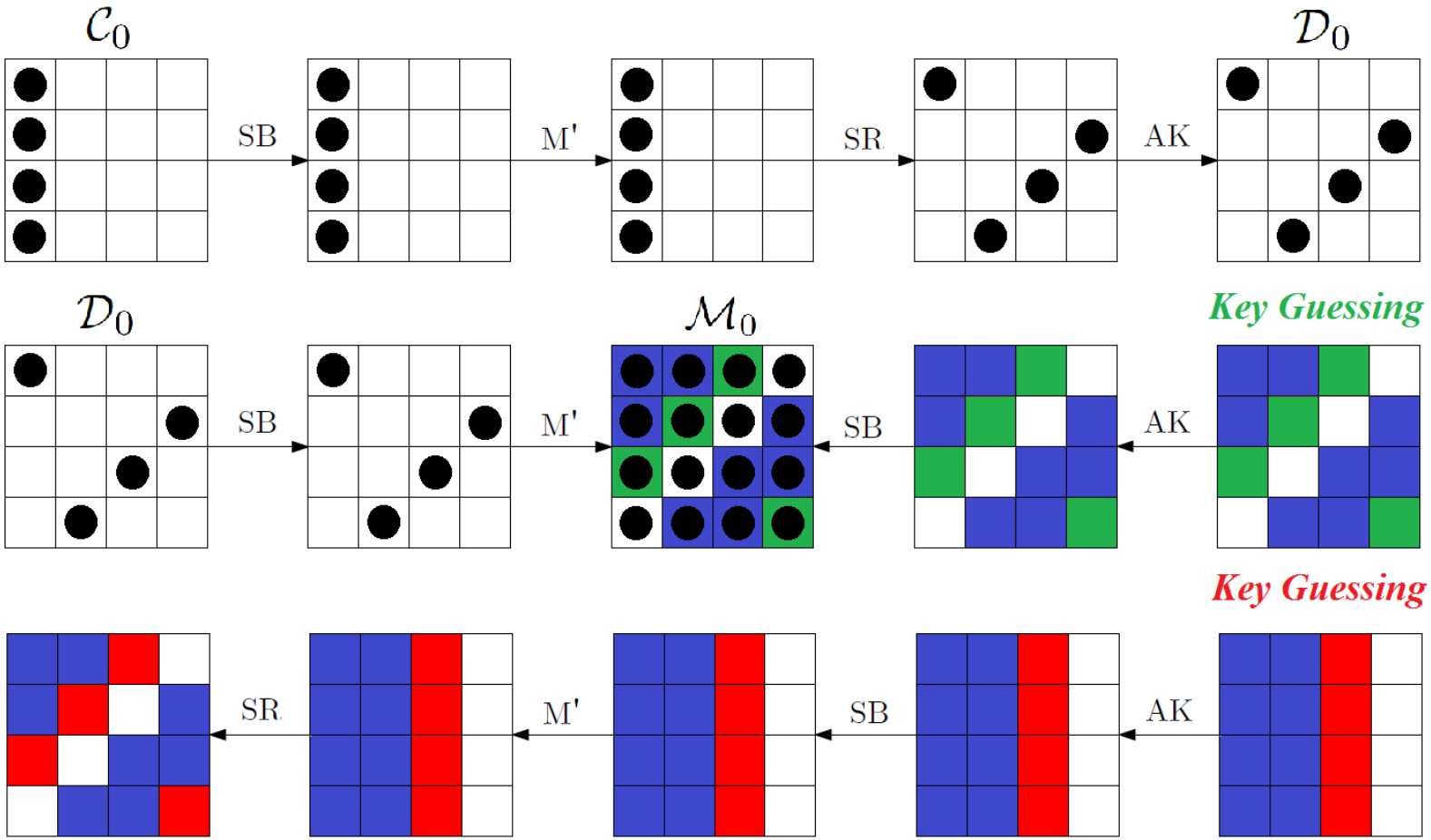
The attack can be set up in other different ways: *the previous one requires the minimum data complexity* (the computational cost is still very competitive).

2nd Step - Exploit Relationships among the Nibbles



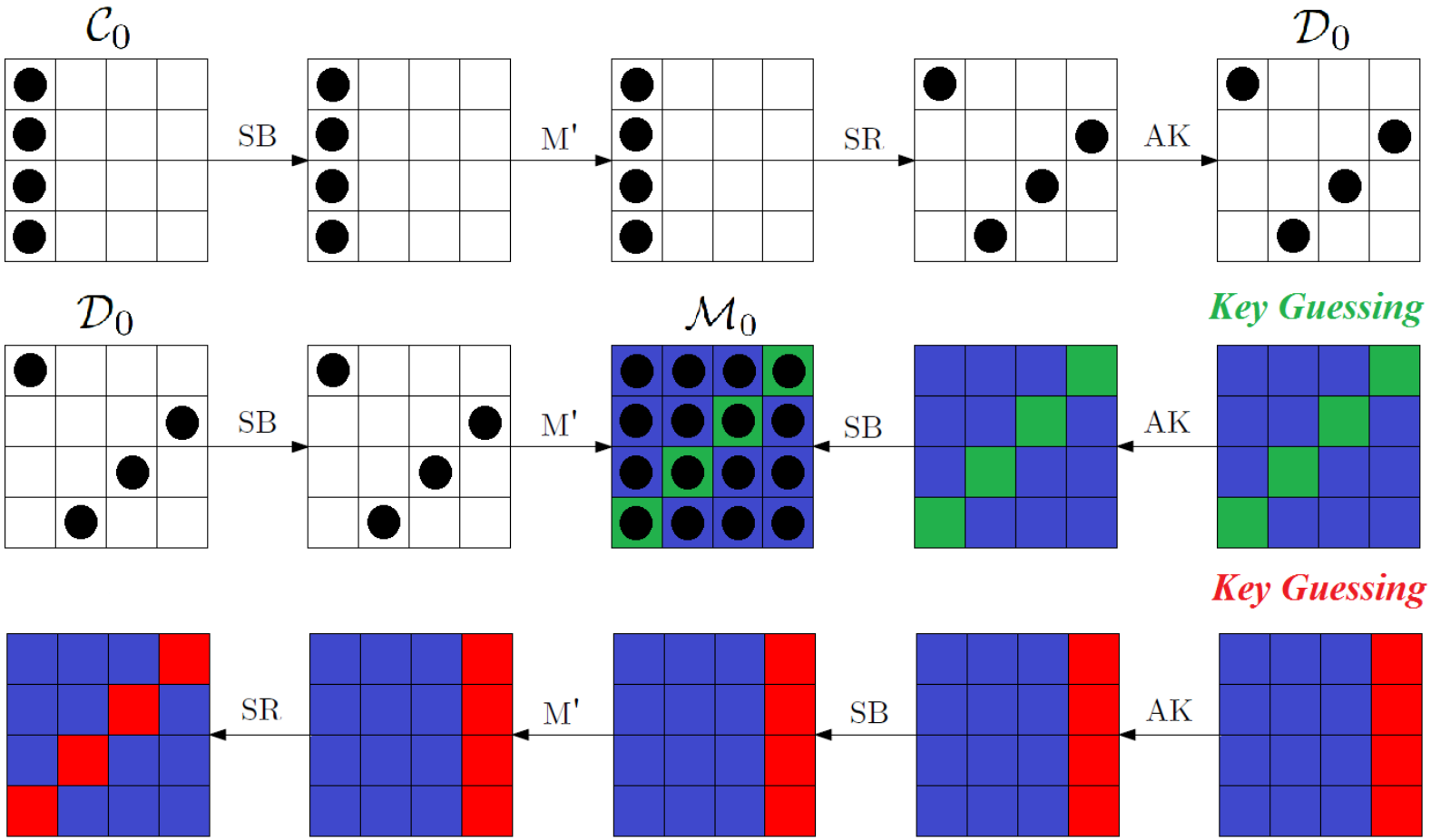
Red: Guessed Nibbles of $k_1 \oplus k_0'$ - *Green*: Guessed Nibbles of k_1 - *Blue*: *Known* Nibbles of k_1 and $k_1 \oplus k_0'$

2nd Step - Exploit Relationships among the Nibbles



Red: Guessed Nibbles of $k_1 \oplus k_0'$ - *Green*: Guessed Nibbles of k_1 - *Blue*: *Known* Nibbles of k_1 and $k_1 \oplus k_0'$

2nd Step - Exploit Relationships among the Nibbles



Red: Guessed Nibbles of $k_1 \oplus k_0'$ - *Green*: Guessed Nibbles of k_1 - *Blue*: *Known* Nibbles of k_1 and $k_1 \oplus k_0'$

Attack on 4 Rounds

Working independently on each column, two steps of the attack

1. recover 4 nibbles of the final key $k'_0 \oplus k_1$ and 4 nibbles of the key k_1 working independently on each nibble;

2. using the knowledge of the nibbles just found, recover the rest of the key by exploiting the relationships among the nibbles.

The attack can be set up in other different ways: *the previous one requires the minimum data complexity* (the computational cost is still very competitive).

Final Result

Table: *Attacks on 4-round PRINCE*. Our attack is in bold.

Technique	Data (CP)	Comp. (E)	Memory
Trunc. Diff.	$\mathbf{8 = 2^3}$	$\mathbf{2^{18.25}}$	**small**
Bit-pattern Integral	$48 = 2^{5.6}$	2^{22}	small
(Pre-Computed) Integral	$64 = 2^6$	$2^{7.4}$	small
Integral	$160 = 2^{7.32}$	$2^{9.32}$	small
Diff. / Logic	2^{10}	5 sec	$\ll 2^{27}$
Differential	2^{32}	$2^{56.26}$	2^{48}

Table created using “Cryptanalysis Zoo” by IAIK, TU Graz - see
`http://cryptanalysiszoo.iaik.tugraz.at/Mw`

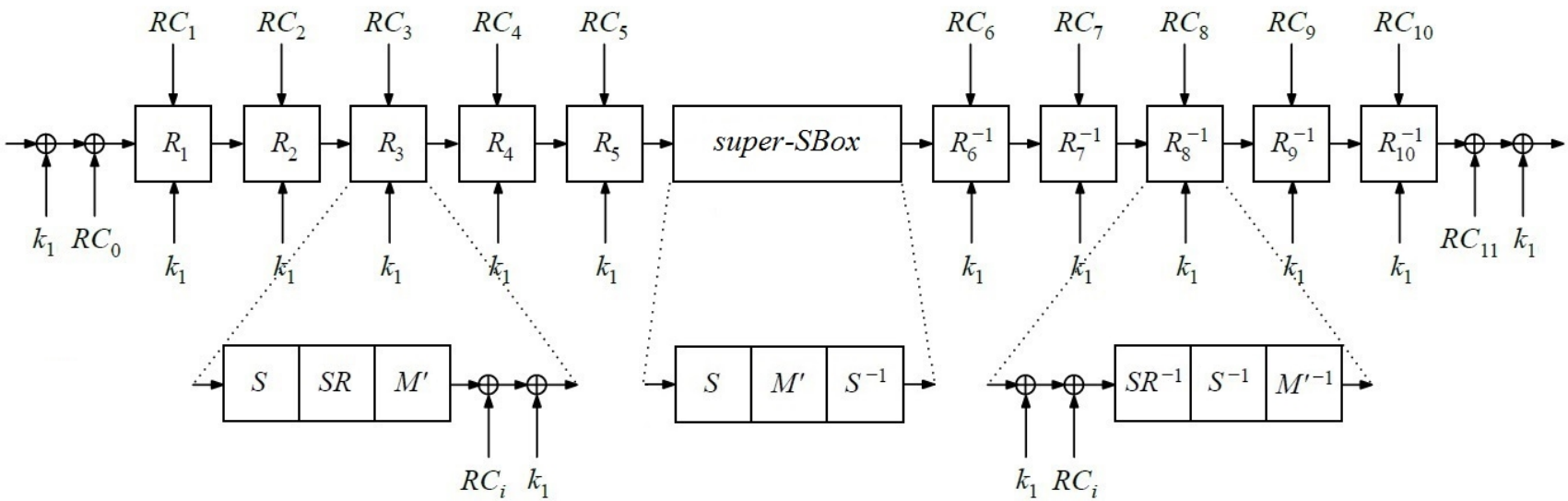
Part III

Equivalent Variant of PRINCE

The Linear Component of PRINCE Round

A round of PRINCE is similar to one round of AES.
However the *SR* operation is computed **after** the *M′* one and not before.

What happens if we change the order of these two operations?



Consequences (1/2)

PRINCE would be less secure!

If round of PRINCE equal to the AES one:

$$R^i(x) = RC_i \oplus k_1 \oplus M' \circ SR \circ \text{S-Box}(x),$$

then it is possible to construct a subspace trail that covers 3.5 rounds (instead of 2.5 as before):

$$\mathcal{ID}_i \oplus a \xrightarrow{R \circ ARK(\cdot)} \mathcal{C}_i \oplus b \xrightarrow{super\text{-}SBox(\cdot)} \mathcal{C}_i \oplus c \xrightarrow{M' \circ SR^{-1} \circ ARK(\cdot)} \mathcal{IM}_i \oplus d.$$

It follows that...

Consequences (1/2)

PRINCE would be less secure!

If round of PRINCE equal to the AES one:

$$R^i(x) = RC_i \oplus k_1 \oplus M' \circ SR \circ \text{S-Box}(x),$$

then it is possible to construct a subspace trail that covers 3.5 rounds (instead of 2.5 as before):

$$\mathcal{ID}_i \oplus a \xrightarrow{R \circ ARK(\cdot)} \mathcal{C}_i \oplus b \xrightarrow{\textit{super-SBox}(\cdot)} \mathcal{C}_i \oplus c \xrightarrow{M' \circ SR^{-1} \circ ARK(\cdot)} \mathcal{IM}_i \oplus d.$$

It follows that...

Consequences (2/2)

By practical tests and theoretical considerations:

- the number of active S-Box over 4 consecutive rounds is (at least) 12 instead of 16 (original PRINCE);
- (previous) truncated differential attack works on 5 rounds instead of 4 (original PRINCE);
- the balance property holds for 5.5 rounds instead of 4.5 (original PRINCE);
- no difference for Meet-in-the-Middle attacks.

The positions of the SR and of the M' influence the security of the cipher!

Consequences (2/2)

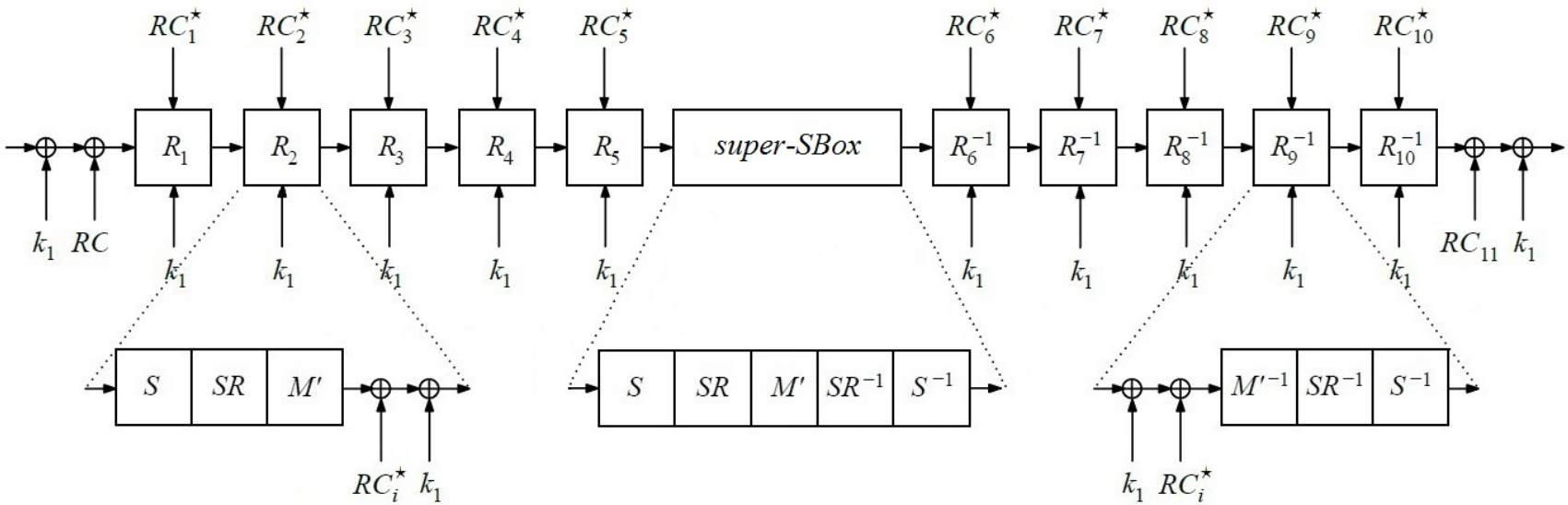
By practical tests and theoretical considerations:

- the number of active S-Box over 4 consecutive rounds is (at least) 12 instead of 16 (original PRINCE);
- (previous) truncated differential attack works on 5 rounds instead of 4 (original PRINCE);
- the balance property holds for 5.5 rounds instead of 4.5 (original PRINCE);
- no difference for Meet-in-the-Middle attacks.

The positions of the SR and of the M' influence the security of the cipher!

Equivalent Variant of PRINCE

To fix the problem, change also the middle-rounds as follows:



Keep in mind when design ciphers inspired by PRINCE!

Part IV

Conclusions

Conclusions

- Subspace Trail Cryptanalysis of PRINCE.
- Truncated Differential Attack on 4 rounds of PRINCE: *Co-Winner* of the *Third* PRINCE Challenge.
- Equivalent Version of PRINCE: Same analysis can be applied in a natural way to other PRINCE-like ciphers. *Keep in mind when design ciphers inspired by PRINCE!*

Thanks for your attention!

Questions?

Comments?

References I

L. Grassi and C. Rechberger and S. Rønjom,
New Insights on AES-Like SPN Ciphers
FSE 2017

J. Borghoff and A. Canteaut and T. Güneysu and E. B. Kavun and M. Knezevic and L. R. Knudsen and G. Leander and V. Nikov and C. Paar and C. Rechberger and P. Rombouts and S. S. Thomsen and T. Yalçin,
PRINCE - A Low-Latency Block Cipher for Pervasive Computing Applications
ASIACRYPT 2012