Structural attacks on block ciphers

Sondre Rønjom
NSM/UiB

September 2, 2017

1. Preliminaries
2. Subspaces in block ciphers
3. From subspace trails to invariant subspaces in Simpira
4. Zero-difference cryptanalysis of AES

Block ciphers

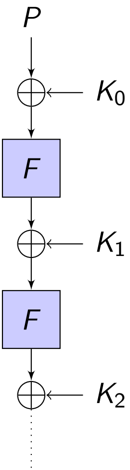


Figure: Typical Design

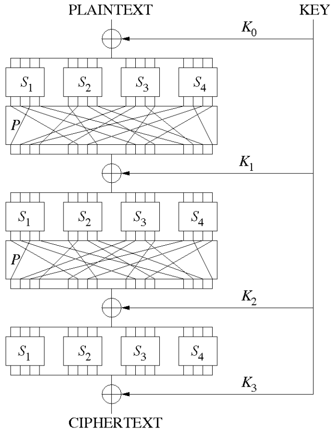


Figure: Classical SPN

Block ciphers as family of permutations

Block ciphers

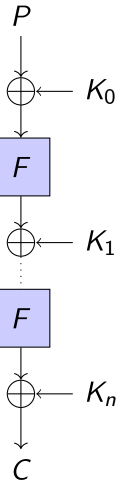
A block cipher defines a map

$$\mathcal{E} : \mathcal{P} \times \mathcal{K} \to \mathcal{C}$$

that takes plaintexts and keys to ciphertexts.

Set of permutations

1. fixing a key $K \in \mathcal{K}$ defines a permutation
$$\mathcal{E}_K : \mathcal{P} \to \mathcal{C}$$
2. fixing all keys defines a set
$$E = \{\mathcal{E}_0, \mathcal{E}_1, \ldots, \mathcal{E}_{|\mathcal{K}|-1}\}$$



Block ciphers as family of permutations

Block ciphers

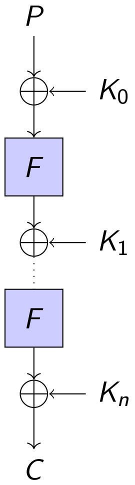
A block cipher defines a map

$$\mathcal{E} : \mathcal{P} \times \mathcal{K} \to \mathcal{C}$$

that takes plaintexts and keys to ciphertexts.

Set of permutations

1. fixing a key $K \in \mathcal{K}$ defines a permutation
$$\mathcal{E}_K : \mathcal{P} \to \mathcal{C}$$
2. fixing all keys defines a set
$$E = \{\mathcal{E}_0, \mathcal{E}_1, \ldots, \mathcal{E}_{|\mathcal{K}|-1}\}$$

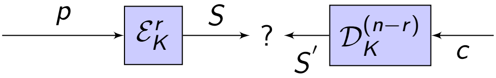


Is the block cipher sufficiently generic ?

Distinguishers and property testing

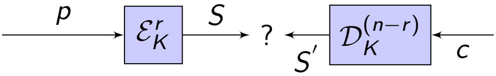
Is there a property that distinguishes one or a class of few from the many ?

Distinguisher to key recovery



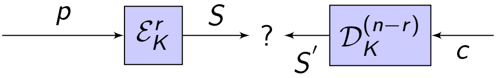
- distinguisher for r out of n rounds of the cipher
- guess enough key bytes in decryption direction
- verify key guess in the middle using distinguisher

Distinguisher to key recovery



- distinguisher for r out of n rounds of the cipher
- guess enough key bytes in decryption direction
- verify key guess in the middle using distinguisher

Distinguisher to key recovery



- distinguisher for r out of n rounds of the cipher
- guess enough key bytes in decryption direction
- verify key guess in the middle using distinguisher

Subspace attacks

Subspace cryptanalysis

Basic exploitation

Plaintexts or ciphertexts stay inside linear and affine subspaces for many rounds (form of truncated differentials)

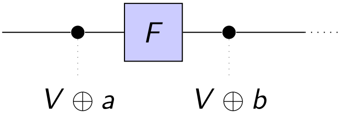
Brief overview

- *A Cryptanalysis of PRINTcipher: The Invariant Subspace Attack*(CRYPTO'11)
- *A Generic Approach to Invariant Subspace Attacks: Cryptanalysis of Robin, iSCREAM and Zorro*, (EC'15)
- *Subspace Trail Cryptanalysis and its Applications to AES* (FSE '17)
- related to superbox cryptanalysis and truncated differentials
- ...active research area

Some notation

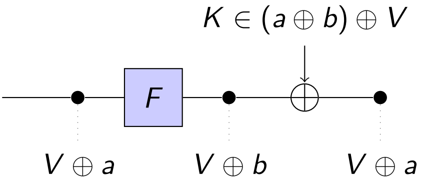
- $\mathbb{F}^n$ is n-dimensional space over field $\mathbb{F}$
- let V be a subspace of $\mathbb{F}^n$
- Let F be a function on $\mathbb{F}^n$ (a permutation)
- $S = F(V) = \{F(v), \mid v \in V\}$
- cosets : $V \oplus a = \{v \oplus a \,|\, v \in V\}$ for $V \subseteq \mathbb{F}^n$

Invariant subspace attacks



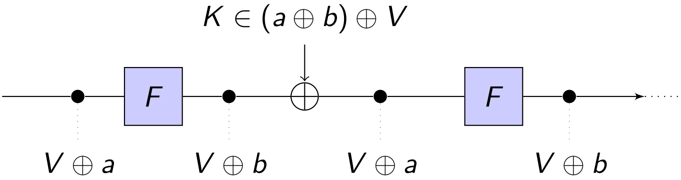
Consider a permutation formed by iterating a permutation F xored with a fixed round key K. Assume the round function maps a coset $V \oplus a$ to a coset $V \oplus b$

Invariant subspace attacks



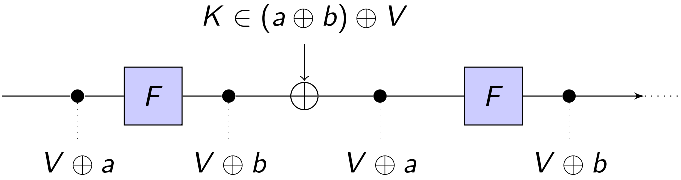
...and that the fixed round key K is in $V \oplus (a \oplus b)$.

Invariant subspace attacks



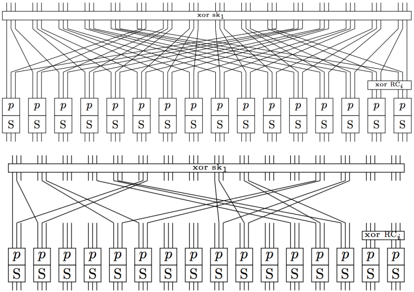
Then this process repeats itself.
Plaintexts in coset $V \oplus a$ are mapped to itself

Invariant subspace attacks



Confidentiality is broken: Density of weak keys $= 2^{n-\dim(V)}$

A Cryptanalysis of PRINTcipher: The Invariant Subspace Attack, [Leander+]



Inspecting components reveals invariant subspace for large class of keys

- block size $n = 48$
- Fixed key K in each round (used for key-dependent p and XOR)
- Round constant
- Finds 2^{52} weak keys out of 2^{80}

Subspace Trails

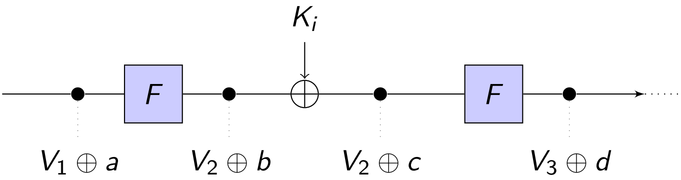


Figure: Subspace trail

Let R^m denote m applications of the round function F with fixed round keys K_i.

Subspace Trails

A (constant dimensional) generic subspace trail $(V_0, V_1, ..., V_m)$ is such that for each a, there exist a unique b such that

$$F(V_i \oplus a) = V_{i+1} \oplus b.$$

Subspace Trails

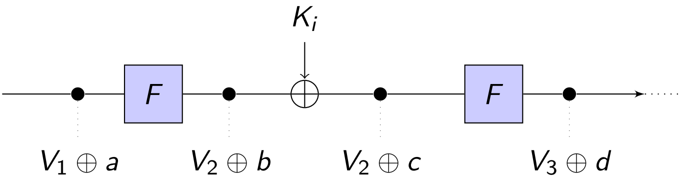


Figure: Subspace trail

Let R^m denote m applications of the round function F with fixed round keys K_i.

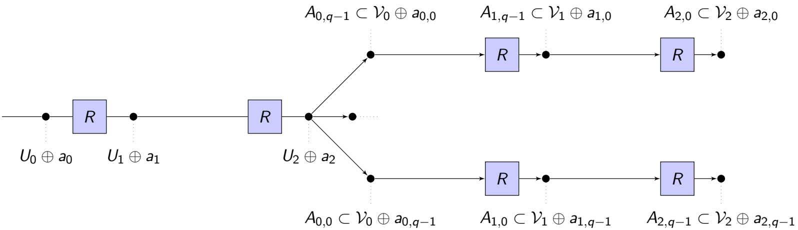
Subspace Trails

A (constant dimensional) generic subspace trail $(V_0, V_1, ..., V_m)$ is such that for each a, there exist a unique b such that

$$F(V_i \oplus a) = V_{i+1} \oplus b.$$

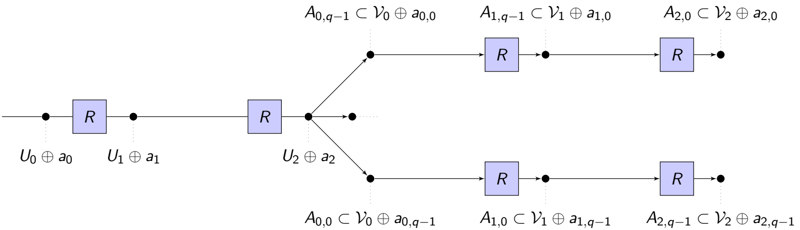
Connecting trails / Trail branching

- $U = (U_0, \ldots, U_m)$
- $V = (V_0, \ldots, V_n)$
- a_i, b_i random and fixed constants.
- $F^m(U_0 \oplus a_0) = U_m \oplus a_m$
- $F^n(V_0 \oplus b_0) = V_n \oplus b_n$.
- Endpoints of U and V correlate (intersect)



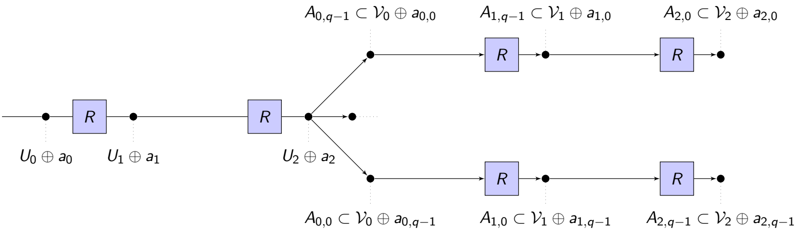
Connecting trails / Trail branching

- $U = (U_0, \ldots, U_m)$
- $V = (V_0, \ldots, V_n)$
- a_i, b_i random and fixed constants.
- $F^m(U_0 \oplus a_0) = U_m \oplus a_m$
- $F^n(V_0 \oplus b_0) = V_n \oplus b_n$.
- Endpoints of U and V correlate (intersect)

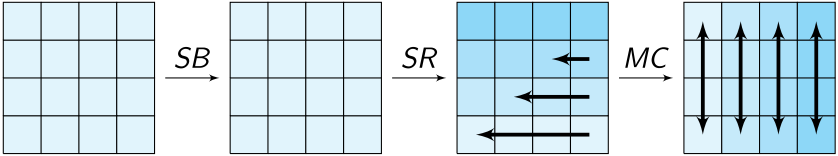


Connecting trails / Trail branching

- $U = (U_0, \ldots, U_m)$
- $V = (V_0, \ldots, V_n)$
- a_i, b_i random and fixed constants.
- $F^m(U_0 \oplus a_0) = U_m \oplus a_m$
- $F^n(V_0 \oplus b_0) = V_n \oplus b_n$.
- Endpoints of U and V correlate (intersect)



Subspace trails in AES



- block size 128 bit, typical key size $\in \{128, 256\}$, rounds $\in \{10, 14\}$
- internal state viewed as a 4×4 matrix states over $\mathbb{F}_{2^8}$
- rounds consist of fixed function F and addition of round keys
- $F = MC \circ SR \circ SB$

Diagonal Space

Let $e_{i,j}$ be the 4×4 matrix with a single 1 in position i, j (or as a vector of length 16 with a single 1 in position $4 \cdot j + i$).

Definition

(**Diagonal spaces**) The diagonal spaces $\mathcal{D}_i$ are defined as

$$\mathcal{D}_i =< e_{0,i}, e_{1,i+1}, e_{2,i+2}, e_{3,i+3} >$$

where $i + j$ is computed modulo 4. For instance, the diagonal space $\mathcal{D}_0$ corresponds to the symbolic matrix

$$\mathcal{D}_0 = \left\{ \begin{bmatrix} x_1 & 0 & 0 & 0 \\ 0 & x_2 & 0 & 0 \\ 0 & 0 & x_3 & 0 \\ 0 & 0 & 0 & x_4 \end{bmatrix} \middle| \forall x_1, x_2, x_3, x_4 \in \mathbb{F}_{2^8} \right\}.$$

Diagonal Space

Let $e_{i,j}$ be the 4×4 matrix with a single 1 in position i, j (or as a vector of length 16 with a single 1 in position $4 \cdot j + i$).

Definition

(**Diagonal spaces**) The diagonal spaces $\mathcal{D}_i$ are defined as

$$\mathcal{D}_i =< e_{0,i}, e_{1,i+1}, e_{2,i+2}, e_{3,i+3} >$$

where $i + j$ is computed modulo 4. For instance, the diagonal space $\mathcal{D}_0$ corresponds to the symbolic matrix

$$\mathcal{D}_0 = \left\{ \begin{bmatrix} x_1 & 0 & 0 & 0 \\ 0 & x_2 & 0 & 0 \\ 0 & 0 & x_3 & 0 \\ 0 & 0 & 0 & x_4 \end{bmatrix} \middle| \forall x_1, x_2, x_3, x_4 \in \mathbb{F}_{2^8} \right\}.$$

Column Space

Definition

(**Column spaces**) The column spaces $\mathcal{C}_i$ are defined as

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

For instance, the columns space $\mathcal{C}_0$ corresponds to the image of

$$\mathcal{C}_0 = \left\{ \begin{bmatrix} x_1 & 0 & 0 & 0 \\ x_2 & 0 & 0 & 0 \\ x_3 & 0 & 0 & 0 \\ x_4 & 0 & 0 & 0 \end{bmatrix} \middle| \forall x_1, x_2, x_3, x_4 \in \mathbb{F}_{2^8} \right\}.$$

Column Space

Definition

(**Column spaces**) The column spaces $\mathcal{C}_i$ are defined as

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

For instance, the columns space $\mathcal{C}_0$ corresponds to the image of

$$\mathcal{C}_0 = \left\{ \begin{bmatrix} x_1 & 0 & 0 & 0 \\ x_2 & 0 & 0 & 0 \\ x_3 & 0 & 0 & 0 \\ x_4 & 0 & 0 & 0 \end{bmatrix} \middle| \forall x_1, x_2, x_3, x_4 \in \mathbb{F}_{2^8} \right\}.$$

Mixed Space

Definition

(**Mixed spaces**) The ith mixed subspace $\mathcal{M}_i$ is defined as

$$\mathcal{M}_i = MC \circ SR(\mathcal{C}_i).$$

For instance, $\mathcal{M}_0$ corresponds to the image of

$$\mathcal{M}_0 = \left\{ \begin{bmatrix} \alpha \cdot x_1 & x_4 & x_3 & (\alpha+1) \cdot x_2 \\ x_1 & x_4 & (\alpha+1) \cdot x_3 & \alpha \cdot x_2 \\ x_1 & (\alpha+1) \cdot x_4 & \alpha \cdot x_3 & x_2 \\ (\alpha+1) \cdot x_1 & \alpha \cdot x_4 & x_3 & x_2 \end{bmatrix} \middle| \forall x_1, x_2, x_3, x_4 \in \mathbb{F}_{2^8} \right.$$

where α is the generator of the AES field.

Mixed Space

Definition

(**Mixed spaces**) The ith mixed subspace $\mathcal{M}_i$ is defined as

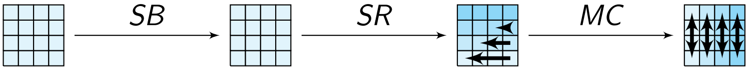
$$\mathcal{M}_i = MC \circ SR(\mathcal{C}_i).$$

For instance, $\mathcal{M}_0$ corresponds to the image of

$$\mathcal{M}_0 = \left\{ \begin{bmatrix} \alpha \cdot x_1 & x_4 & x_3 & (\alpha+1) \cdot x_2 \\ x_1 & x_4 & (\alpha+1) \cdot x_3 & \alpha \cdot x_2 \\ x_1 & (\alpha+1) \cdot x_4 & \alpha \cdot x_3 & x_2 \\ (\alpha+1) \cdot x_1 & \alpha \cdot x_4 & x_3 & x_2 \end{bmatrix} \middle| \forall x_1, x_2, x_3, x_4 \in \mathbb{F}_{2^8} \right.$$

where α is the generator of the AES field.

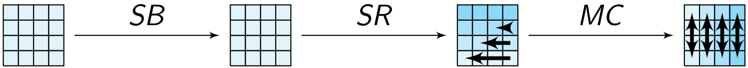
Subspace Trail Cryptanalysis and its Applications to AES[GRR17], FSE '17



For fixed $I, J \subset \{0,1,2,3\}$, $|I| + |J| \leq 4$

1. $R(\mathcal{D}_I \oplus a) = \mathcal{C}_I \oplus b$
2. $R(\mathcal{C}_I \oplus a) = \mathcal{M}_I \oplus b$
3. $R^2(\mathcal{C}_I \oplus a) = \mathcal{M}_I \oplus b$
4. $\mathcal{M}_I \cap \mathcal{D}_J = \{0\}$

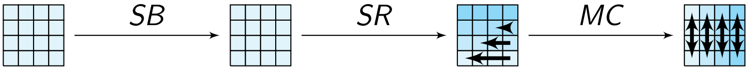
Subspace Trail Cryptanalysis and its Applications to AES[GRR17], FSE '17



For fixed $I, J \subset \{0,1,2,3\}$, $|I| + |J| \leq 4$

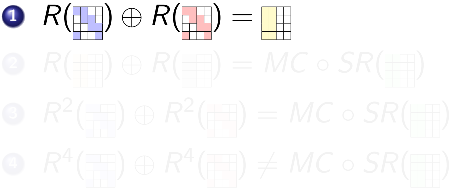
1. $R(\mathcal{D}_I \oplus a) = \mathcal{C}_I \oplus b$
2. $R(\mathcal{C}_I \oplus a) = \mathcal{M}_I \oplus b$
3. $R^2(\mathcal{C}_I \oplus a) = \mathcal{M}_I \oplus b$
4. $\mathcal{M}_I \cap \mathcal{D}_J = \{0\}$

Subspace Trail Cryptanalysis and its Applications to AES[GRR17], FSE '17

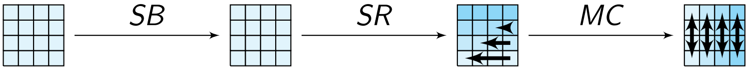


For fixed $I, J \subset \{0,1,2,3\}$, $|I| + |J| \leq 4$

1. $R(\mathcal{D}_I \oplus a) = \mathcal{C}_I \oplus b$
2. $R(\mathcal{C}_I \oplus a) = \mathcal{M}_I \oplus b$
3. $R^2(\mathcal{C}_I \oplus a) = \mathcal{M}_I \oplus b$
4. $\mathcal{M}_I \cap \mathcal{D}_J = \{0\}$

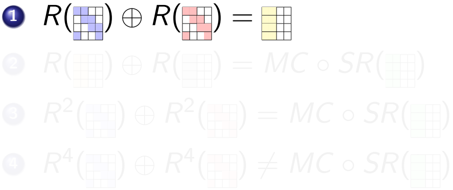


Subspace Trail Cryptanalysis and its Applications to AES[GRR17], FSE '17

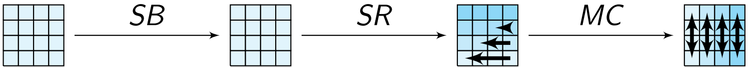


For fixed $I, J \subset \{0,1,2,3\}$, $|I| + |J| \leq 4$

1. $R(\mathcal{D}_I \oplus a) = \mathcal{C}_I \oplus b$
2. $R(\mathcal{C}_I \oplus a) = \mathcal{M}_I \oplus b$
3. $R^2(\mathcal{C}_I \oplus a) = \mathcal{M}_I \oplus b$
4. $\mathcal{M}_I \cap \mathcal{D}_J = \{0\}$

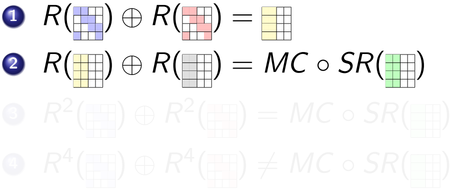


Subspace Trail Cryptanalysis and its Applications to AES[GRR17], FSE '17

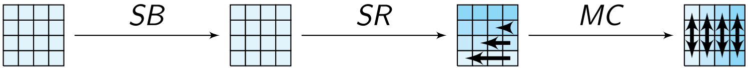


For fixed $I, J \subset \{0,1,2,3\}$, $|I| + |J| \leq 4$

1. $R(\mathcal{D}_I \oplus a) = \mathcal{C}_I \oplus b$
2. $R(\mathcal{C}_I \oplus a) = \mathcal{M}_I \oplus b$
3. $R^2(\mathcal{C}_I \oplus a) = \mathcal{M}_I \oplus b$
4. $\mathcal{M}_I \cap \mathcal{D}_J = \{0\}$

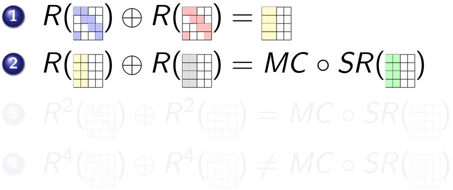


Subspace Trail Cryptanalysis and its Applications to AES[GRR17], FSE '17

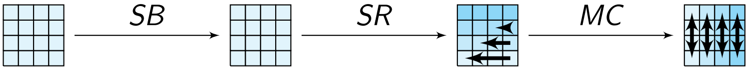


For fixed $I, J \subset \{0,1,2,3\}$, $|I| + |J| \leq 4$

1. $R(\mathcal{D}_I \oplus a) = \mathcal{C}_I \oplus b$
2. $R(\mathcal{C}_I \oplus a) = \mathcal{M}_I \oplus b$
3. $R^2(\mathcal{C}_I \oplus a) = \mathcal{M}_I \oplus b$
4. $\mathcal{M}_I \cap \mathcal{D}_J = \{0\}$

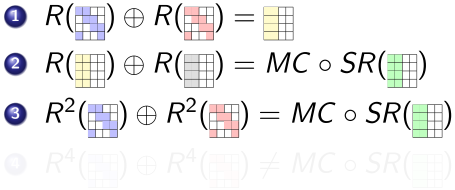


Subspace Trail Cryptanalysis and its Applications to AES[GRR17], FSE '17

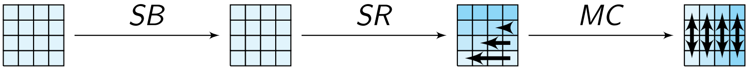


For fixed $I, J \subset \{0,1,2,3\}$, $|I| + |J| \leq 4$

1. $R(\mathcal{D}_I \oplus a) = \mathcal{C}_I \oplus b$
2. $R(\mathcal{C}_I \oplus a) = \mathcal{M}_I \oplus b$
3. $R^2(\mathcal{C}_I \oplus a) = \mathcal{M}_I \oplus b$
4. $\mathcal{M}_I \cap \mathcal{D}_J = \{0\}$

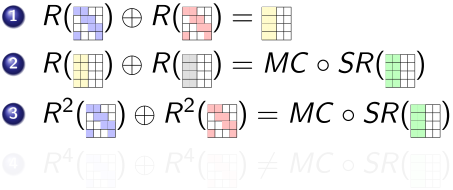


Subspace Trail Cryptanalysis and its Applications to AES[GRR17], FSE '17

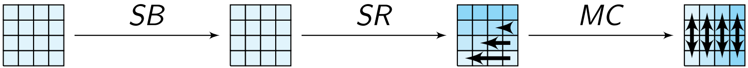


For fixed $I, J \subset \{0, 1, 2, 3\}$, $|I| + |J| \leq 4$

1. $R(\mathcal{D}_I \oplus a) = \mathcal{C}_I \oplus b$
2. $R(\mathcal{C}_I \oplus a) = \mathcal{M}_I \oplus b$
3. $R^2(\mathcal{C}_I \oplus a) = \mathcal{M}_I \oplus b$
4. $\mathcal{M}_I \cap \mathcal{D}_J = \{0\}$

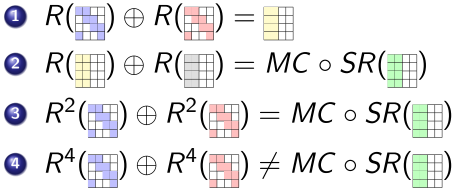


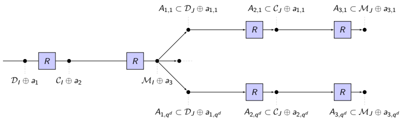
Subspace Trail Cryptanalysis and its Applications to AES[GRR17], FSE '17



For fixed $I, J \subset \{0,1,2,3\}$, $|I| + |J| \leq 4$

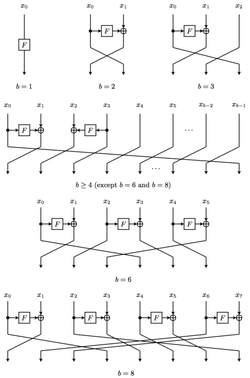
1. $R(\mathcal{D}_I \oplus a) = \mathcal{C}_I \oplus b$
2. $R(\mathcal{C}_I \oplus a) = \mathcal{M}_I \oplus b$
3. $R^2(\mathcal{C}_I \oplus a) = \mathcal{M}_I \oplus b$
4. $\mathcal{M}_I \cap \mathcal{D}_J = \{0\}$





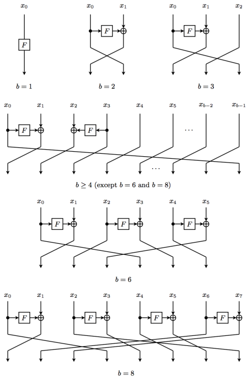
Attack on Simpira

Simpira (now Simpira v1)



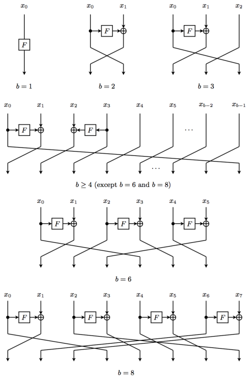
- *Simpira: A Family of Efficient Permutations Using the AES Round Function*, [GM16]
- a family of cryptographic permutations supporting $128 \times b$ bits
- designed to achieve high throughput on all modern 64-bit processors
- uses only one building block, AES (Intel/AMD/ARM native instructions)
- Generalized Feistel Structure
- Claim: no structural distinguishers with complexity below 2^{128}.

Simpira (now Simpira v1)



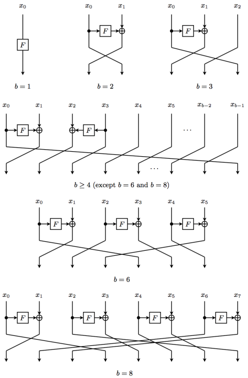
- *Simpira: A Family of Efficient Permutations Using the AES Round Function*, [GM16]
- a family of cryptographic permutations supporting $128 \times b$ bits
- designed to achieve high throughput on all modern 64-bit processors
- uses only one building block, AES (Intel/AMD/ARM native instructions)
- Generalized Feistel Structure
- Claim: no structural distinguishers with complexity below 2^{128}.

Simpira (now Simpira v1)



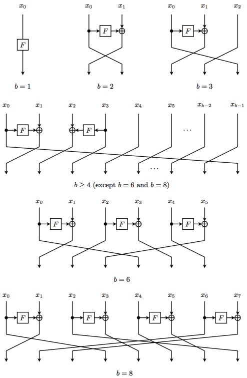
- *Simpira: A Family of Efficient Permutations Using the AES Round Function*, [GM16]
- a family of cryptographic permutations supporting $128 \times b$ bits
- designed to achieve high throughput on all modern 64-bit processors
- uses only one building block, AES (Intel/AMD/ARM native instructions)
- Generalized Feistel Structure
- Claim: no structural distinguishers with complexity below 2^{128}.

Simpira (now Simpira v1)



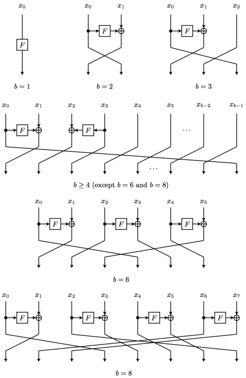
- *Simpira: A Family of Efficient Permutations Using the AES Round Function*, [GM16]
- a family of cryptographic permutations supporting $128 \times b$ bits
- designed to achieve high throughput on all modern 64-bit processors
- uses only one building block, AES (Intel/AMD/ARM native instructions)
- Generalized Feistel Structure
- Claim: no structural distinguishers with complexity below 2^{128}.

Simpira (now Simpira v1)



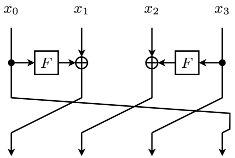
- *Simpira: A Family of Efficient Permutations Using the AES Round Function*, [GM16]
- a family of cryptographic permutations supporting $128 \times b$ bits
- designed to achieve high throughput on all modern 64-bit processors
- uses only one building block, AES (Intel/AMD/ARM native instructions)
- Generalized Feistel Structure
- Claim: no structural distinguishers with complexity below 2^{128}.

Simpira (now Simpira v1)



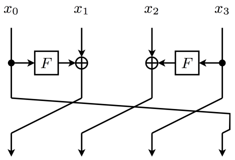
- *Simpira: A Family of Efficient Permutations Using the AES Round Function*, [GM16]
- a family of cryptographic permutations supporting $128 \times b$ bits
- designed to achieve high throughput on all modern 64-bit processors
- uses only one building block, AES (Intel/AMD/ARM native instructions)
- Generalized Feistel Structure
- Claim: no structural distinguishers with complexity below 2^{128}.

Simpira with $b = 4$



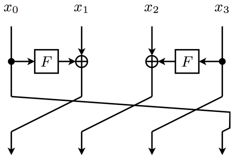
- 512 bit permutation
- $f(x)$: one AES round minus constants
- F-function: $F_i^t(x) = f(f(x) + k_{t,i})$
- Different constants in each new F-function
- Iterated for many rounds (not important)
- Suitable for a wide range of applications.

Simpira with $b = 4$



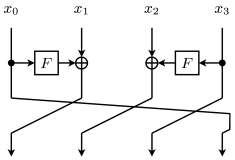
- 512 bit permutation
- $f(x)$: one AES round minus constants
- F-function: $F_i^t(x) = f(f(x) + k_{t,i})$
- Different constants in each new F-function
- Iterated for many rounds (not important)
- Suitable for a wide range of applications.

Simpira with $b = 4$



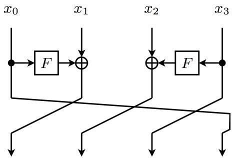
- 512 bit permutation
- $f(x)$: one AES round minus constants
- F-function: $F_i^t(x) = f(f(x) + k_{t,i})$
- Different constants in each new F-function
- Iterated for many rounds (not important)
- Suitable for a wide range of applications.

Simpira with $b = 4$



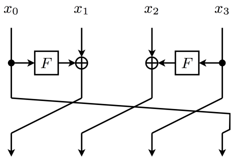
- 512 bit permutation
- $f(x)$: one AES round minus constants
- F-function: $F_i^t(x) = f(f(x) + k_{t,i})$
- Different constants in each new F-function
- Iterated for many rounds (not important)
- Suitable for a wide range of applications.

Simpira with $b = 4$



- 512 bit permutation
- $f(x)$: one AES round minus constants
- F-function: $F_i^t(x) = f(f(x) + k_{t,i})$
- Different constants in each new F-function
- Iterated for many rounds (not important)
- Suitable for a wide range of applications.

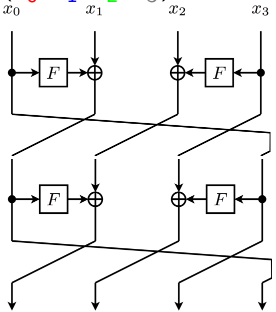
Simpira with $b = 4$



- 512 bit permutation
- $f(x)$: one AES round minus constants
- F-function: $F_i^t(x) = f(f(x) + k_{t,i})$
- Different constants in each new F-function
- Iterated for many rounds (not important)
- Suitable for a wide range of applications.

Initial observation for two rounds

$(x_0^t, x_1^t, x_2^t, x_3^t)$



- $F_i^t(x) = f(f(x) + k_{t,i})$ where $k_{t,i} \in \mathcal{C}_{0,1}$
- $(x_0^t, x_1^t, x_2^t, x_3^t) \in \mathbb{F}_{2^8}^{4\times 4\times 4}$

$$S_{t+1} = (x_0^{t+1}, x_1^{t+1}, x_2^{t+1}, x_3^{t+1})$$
$$= (F_1^t(x_0^t) \oplus x_1^t, F_2^t(x_3^t) \oplus x_2^t, x_3^t, x_0^t)$$
$$S_{t+2} = (x_0^{t+2}, x_1^{t+2}, x_2^{t+2}, x_3^{t+2})$$
$$= (F_1^{t+1}(x_0^{t+1}) \oplus x_1^{t+1}, F_2^{t+1}(x_3^{t+1}) \oplus x_2^{t+1}, x_3^{t+1}, x_0^{t+1})$$

$$x_3^{t+1} = x_0^t, x_2^{t+1} = x_3^t, x_0^{t+1} = F_1^t(x_0^t) \oplus x_1^t$$

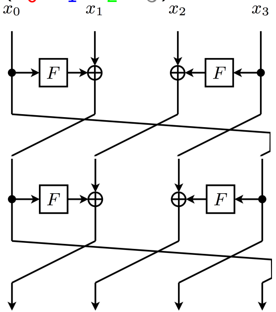
$(x_0^{t+2}, F_2^{t+1}(x_0^t) \oplus x_3^t, x_0^t, F_1^t(x_0^t) \oplus x_1^t))$

Structure

$$(a, b, c, d) \xrightarrow{R^2} (z, F_1(a) \oplus d, a, F_2(a) \oplus b).$$

Initial observation for two rounds

$(x_0^t, x_1^t, x_2^t, x_3^t)$



- $F_i^t(x) = f(f(x) + k_{t,i})$ where $k_{t,i} \in \mathcal{C}_{0,1}$
- $(x_0^t, x_1^t, x_2^t, x_3^t) \in \mathbb{F}_{2^8}^{4\times 4\times 4}$

$$\begin{aligned} S_{t+1} &= (x_0^{t+1}, x_1^{t+1}, x_2^{t+1}, x_3^{t+1}) \\ &= (F_1^t(x_0^t) \oplus x_1^t, F_2^t(x_3^t) \oplus x_2^t, x_3^t, x_0^t) \end{aligned}$$

$$\begin{aligned} S_{t+2} &= (x_0^{t+2}, x_1^{t+2}, x_2^{t+2}, x_3^{t+2}) \\ &= (F_1^{t+1}(x_0^{t+1}) \oplus x_1^{t+1}, F_2^{t+1}(x_3^{t+1}) \oplus x_2^{t+1}, x_3^{t+1}, x_0^{t+1}) \end{aligned}$$

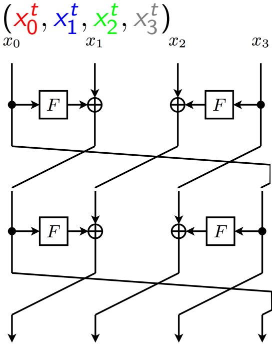
$$x_3^{t+1} = x_0^t, x_2^{t+1} = x_3^t, x_0^{t+1} = F_1^t(x_0^t) \oplus x_1^t$$

$(x_0^{t+2}, F_2^{t+1}(x_0^t) \oplus x_3^t, x_0^t, F_1^t(x_0^t) \oplus x_1^t))$

Structure

$$(a, b, c, d) \xrightarrow{R^2} (z, F_1(a) \oplus d, a, F_2(a) \oplus b).$$

Initial observation for two rounds



- $F_i^t(x) = f(f(x) + k_{t,i})$ where $k_{t,i} \in \mathcal{C}_{0,1}$
- $(x_0^t, x_1^t, x_2^t, x_3^t) \in \mathbb{F}_{2^8}^{4\times 4\times 4}$

$$
\begin{aligned}
S_{t+1} =& (x_0^{t+1}, x_1^{t+1}, x_2^{t+1}, x_3^{t+1}) \\
=& (F_1^t(x_0^t) \oplus x_1^t, F_2^t(x_3^t) \oplus x_2^t, x_3^t, x_0^t) \\
S_{t+2} =& (x_0^{t+2}, x_1^{t+2}, x_2^{t+2}, x_3^{t+2}) \\
=& (F_1^{t+1}(x_0^{t+1}) \oplus x_1^{t+1}, F_2^{t+1}(x_3^{t+1}) \oplus x_2^{t+1}, x_3^{t+1}, x_0^{t+1})
\end{aligned}
$$

$x_3^{t+1} = x_0^t, x_2^{t+1} = x_3^t, x_0^{t+1} = F_1^t(x_0^t) \oplus x_1^t$

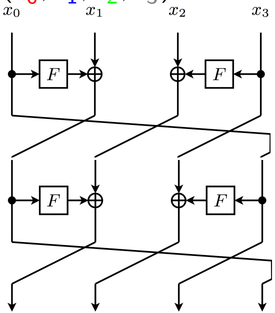
$(x_0^{t+2}, F_2^{t+1}(x_0^t) \oplus x_3^t, x_0^t, F_1^t(x_0^t) \oplus x_1^t))$

Structure

$$(a, b, c, d) \xrightarrow{R^2} (z, F_1(a) \oplus d, a, F_2(a) \oplus b).$$

Initial observation for two rounds

$(x_0^t, x_1^t, x_2^t, x_3^t)$



- $F_i^t(x) = f(f(x) + k_{t,i})$ where $k_{t,i} \in \mathcal{C}_{0,1}$
- $(x_0^t, x_1^t, x_2^t, x_3^t) \in \mathbb{F}_{2^8}^{4\times 4\times 4}$

$$
\begin{aligned}
S_{t+1} &= (x_0^{t+1}, x_1^{t+1}, x_2^{t+1}, x_3^{t+1}) \\
&= (F_1^t(x_0^t) \oplus x_1^t, F_2^t(x_3^t) \oplus x_2^t, x_3^t, x_0^t) \\
S_{t+2} &= (x_0^{t+2}, x_1^{t+2}, x_2^{t+2}, x_3^{t+2}) \\
&= (F_1^{t+1}(x_0^{t+1}) \oplus x_1^{t+1}, F_2^{t+1}(x_3^{t+1}) \oplus x_2^{t+1}, x_3^{t+1}, x_0^{t+1})
\end{aligned}
$$

$$x_3^{t+1} = x_0^t, x_2^{t+1} = x_3^t, x_0^{t+1} = F_1^t(x_0^t) \oplus x_1^t$$

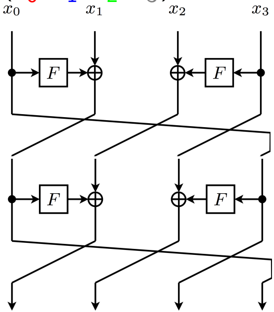
$(x_0^{t+2}, F_2^{t+1}(x_0^t) \oplus x_3^t, x_0^t, F_1^t(x_0^t) \oplus x_1^t))$

Structure

$$(a, b, c, d) \xrightarrow{R^2} (z, F_1(a) \oplus d, a, F_2(a) \oplus b).$$

Initial observation for two rounds

$(x_0^t, x_1^t, x_2^t, x_3^t)$



- $F_i^t(x) = f(f(x) + k_{t,i})$ where $k_{t,i} \in \mathcal{C}_{0,1}$
- $(x_0^t, x_1^t, x_2^t, x_3^t) \in \mathbb{F}_{2^8}^{4\times 4\times 4}$

$$S_{t+1} = (x_0^{t+1}, x_1^{t+1}, x_2^{t+1}, x_3^{t+1})$$
$$= (F_1^t(x_0^t) \oplus x_1^t, F_2^t(x_3^t) \oplus x_2^t, x_3^t, x_0^t)$$
$$S_{t+2} = (x_0^{t+2}, x_1^{t+2}, x_2^{t+2}, x_3^{t+2})$$
$$= (F_1^{t+1}(x_0^{t+1}) \oplus x_1^{t+1}, F_2^{t+1}(x_3^{t+1}) \oplus x_2^{t+1}, x_3^{t+1}, x_0^{t+1})$$

$$x_3^{t+1} = x_0^t, x_2^{t+1} = x_3^t, x_0^{t+1} = F_1^t(x_0^t) \oplus x_1^t$$

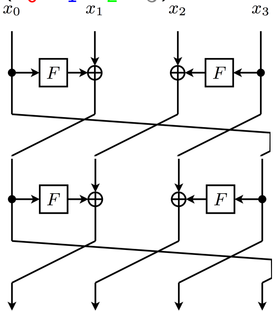
$(x_0^{t+2}, F_2^{t+1}(x_0^t) \oplus x_3^t, x_0^t, F_1^t(x_0^t) \oplus x_1^t))$

Structure

$$(a, b, c, d) \xrightarrow{R^2} (z, F_1(a) \oplus d, a, F_2(a) \oplus b).$$

Initial observation for two rounds

$(x_0^t, x_1^t, x_2^t, x_3^t)$



$(x_0^{t+2}, F_2^{t+1}(x_0^t) \oplus x_3^t, x_0^t, F_1^t(x_0^t) \oplus x_1^t))$

- $F_i^t(x) = f(f(x) + k_{t,i})$ where $k_{t,i} \in \mathcal{C}_{0,1}$
- $(x_0^t, x_1^t, x_2^t, x_3^t) \in \mathbb{F}_{2^8}^{4\times 4\times 4}$

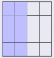
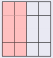
$$\begin{aligned} S_{t+1} &= (x_0^{t+1}, x_1^{t+1}, x_2^{t+1}, x_3^{t+1}) \\ &= (F_1^t(x_0^t) \oplus x_1^t, F_2^t(x_3^t) \oplus x_2^t, x_3^t, x_0^t) \\ S_{t+2} &= (x_0^{t+2}, x_1^{t+2}, x_2^{t+2}, x_3^{t+2}) \\ &= (F_1^{t+1}(x_0^{t+1}) \oplus x_1^{t+1}, F_2^{t+1}(x_3^{t+1}) \oplus x_2^{t+1}, x_3^{t+1}, x_0^{t+1}) \end{aligned}$$

$$x_3^{t+1} = x_0^t, x_2^{t+1} = x_3^t, x_0^{t+1} = F_1^t(x_0^t) \oplus x_1^t$$

Structure

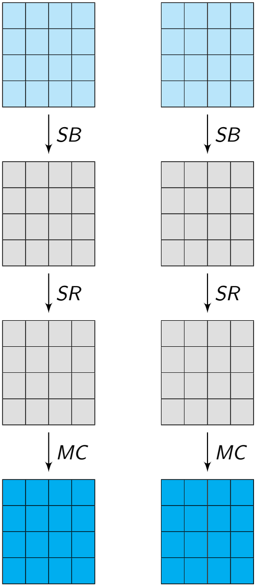
$$(a, b, c, d) \xrightarrow{R^2} (z, F_1(a) \oplus d, a, F_2(a) \oplus b).$$

The parallel F-function

- $f(x)$ one AES round minus key addition
- $f(x) \times f(x)$ (in parallell)
- constants $c_1 =$  and $c_2 =$ 

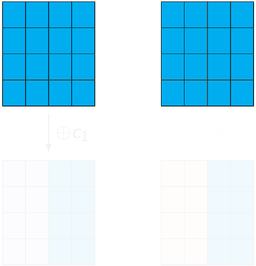
Parallell F-function

$$F_1(a) \times F_2(a) = f(f(a) \oplus c_1) \times f(f(a) \oplus c_2)$$



Trivial Invariant subspace in $f(x) \times f(x)$

$$f(a) \times f(a) = b \times b$$



Constants space

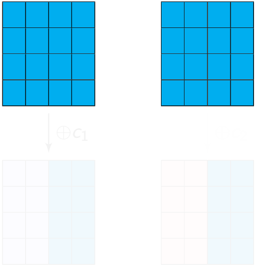
constants $c_1 =$ [grid] and $c_2 =$ [grid]

Adding a constant

We begin with an invariant space $a \times a$

$$f(\ ) \times f(\ ) = \ \times\ $$

then add constants in the middle

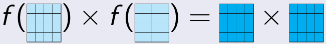


Constants space

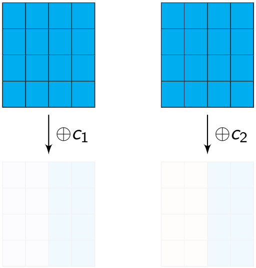
constants $c_1 =$  and $c_2 =$ 

Adding a constant

We begin with an invariant space $a \times a$



...then add constants in the middle...

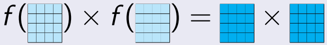


Constants space

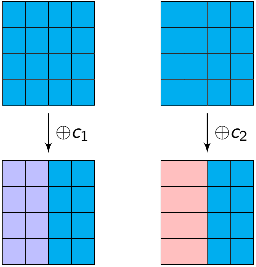
constants $c_1 =$  and $c_2 =$ 

Adding a constant

We begin with an invariant space $a \times a$



...then add constants in the middle...

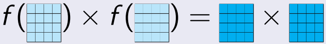


Constants space

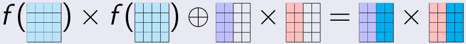
constants $c_1 =$  and $c_2 =$ 

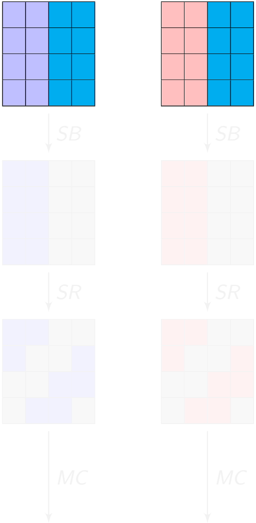
Adding a constant

We begin with an invariant space $a \times a$



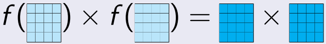
...then add constants in the middle...



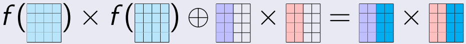


One more round

We begin with an invariant subspace $a \times a$

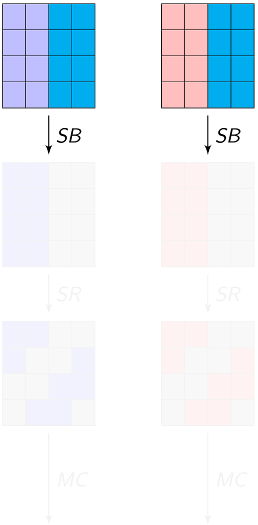


...then add constants in the middle...



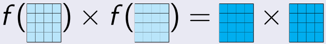
... and apply another AES round...

Subspace trail in paralllel F-function

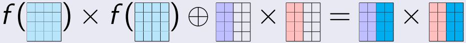


One more round

We begin with an invariant subspace $a \times a$

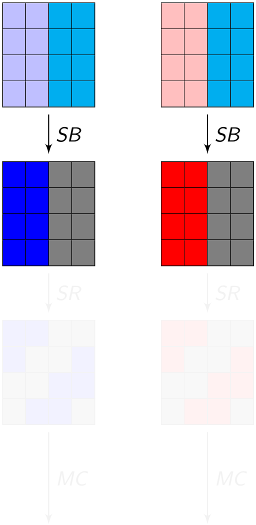


...then add constants in the middle...



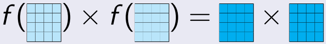
... and apply another AES round...

Subspace trail in paralllel F-function

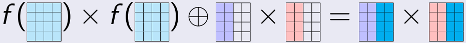


One more round

We begin with an invariant subspace $a \times a$

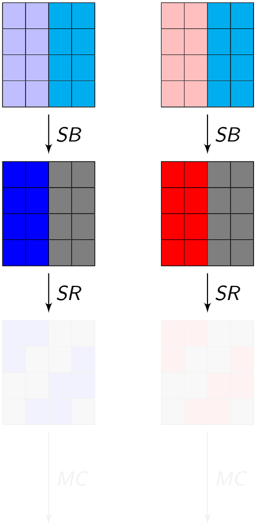


...then add constants in the middle...



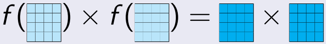
... and apply another AES round...

Subspace trail in paralllel F-function

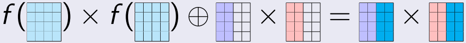


One more round

We begin with an invariant subspace $a \times a$

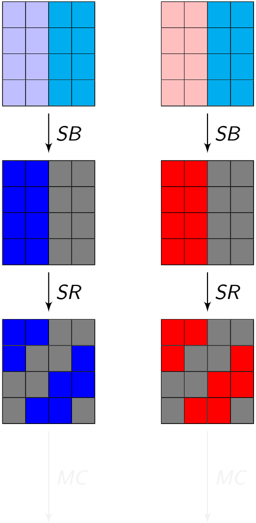


...then add constants in the middle...



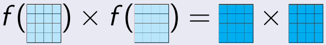
... and apply another AES round...

Subspace trail in paralllel F-function

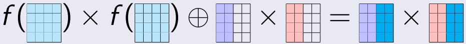


One more round

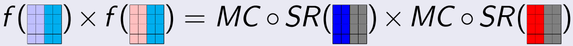
We begin with an invariant subspace $a \times a$



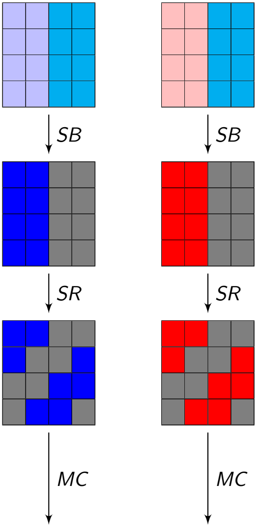
...then add constants in the middle...



... and apply another AES round...

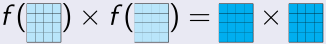


Subspace trail in paralllel F-function

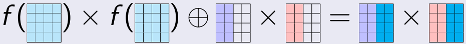


One more round

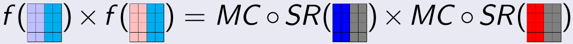
We begin with an invariant subspace $a \times a$



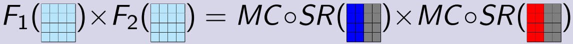
...then add constants in the middle...



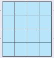
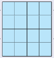
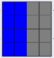
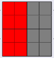
... and apply another AES round...

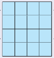
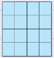
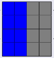
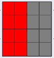


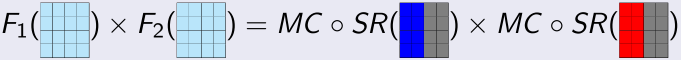
Subspace trail in paralllel F-function

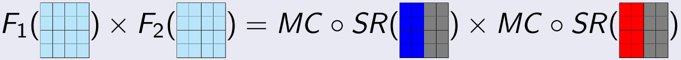


- $(a, b, c, d) \xrightarrow{R^2} (z, F_1(a) \oplus d, a, F_2(a) \oplus b)$
-
- (Imagine $MC \circ SR$ around all values of the state)

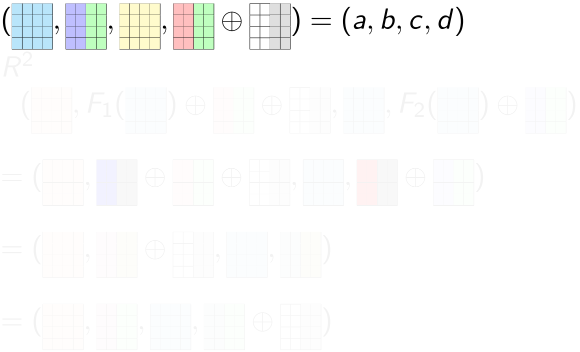
- $(a, b, c, d) \xrightarrow{R^2} (z, F_1(a) \oplus d, a, F_2(a) \oplus b)$
- $F_1($$) \times F_2($$) = MC \circ SR($$) \times MC \circ SR($$)$
- (Imagine $MC \circ SR$ around all values of the state)

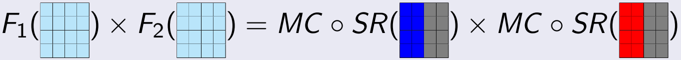
- $(a, b, c, d) \xrightarrow{R^2} (z, F_1(a) \oplus d, a, F_2(a) \oplus b)$
- $F_1($$) \times F_2($$) = MC \circ SR($$) \times MC \circ SR($$)$
- (Imagine $MC \circ SR$ around all values of the state)

- $(a, b, c, d) \xrightarrow{R^2} (z, F_1(a) \oplus d, a, F_2(a) \oplus b)$
- 
- (Imagine $MC \circ SR$ around all values of the state)

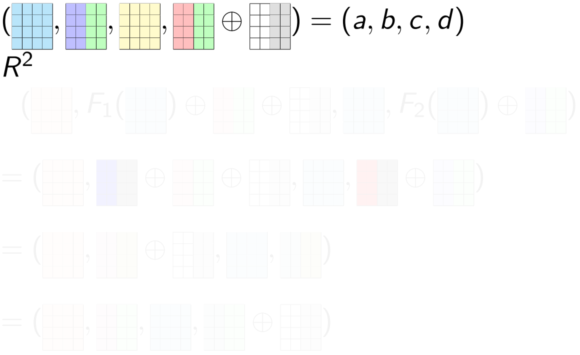
- $(a, b, c, d) \xrightarrow{R^2} (z, F_1(a) \oplus d, a, F_2(a) \oplus b)$
- 

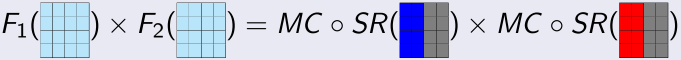
- (Imagine $MC \circ SR$ around all values of the state)



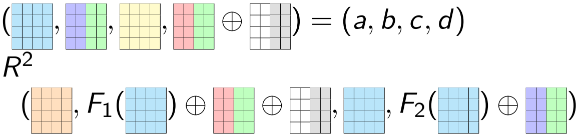
- $(a, b, c, d) \xrightarrow{R^2} (z, F_1(a) \oplus d, a, F_2(a) \oplus b)$
- 

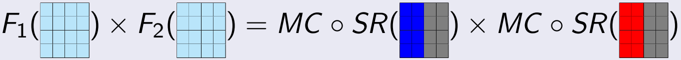
- (Imagine $MC \circ SR$ around all values of the state)



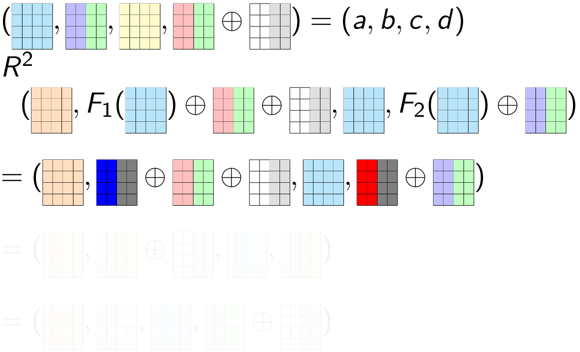
- $(a, b, c, d) \xrightarrow{R^2} (z, F_1(a) \oplus d, a, F_2(a) \oplus b)$
- 

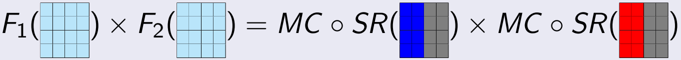
- (Imagine $MC \circ SR$ around all values of the state)



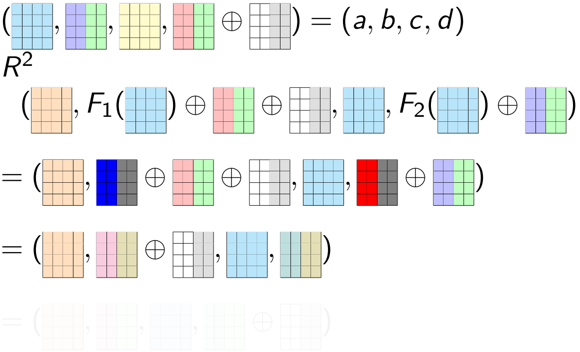
- $(a, b, c, d) \xrightarrow{R^2} (z, F_1(a) \oplus d, a, F_2(a) \oplus b)$
- 

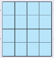
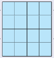
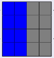
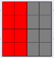
- (Imagine $MC \circ SR$ around all values of the state)

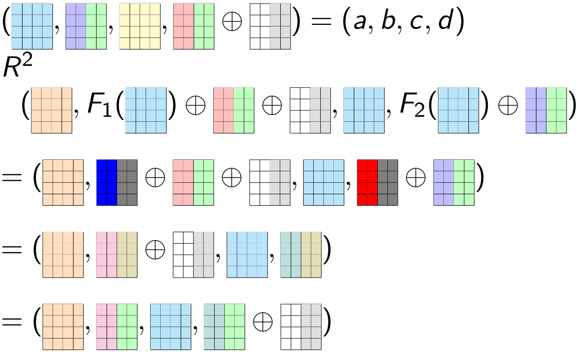


- $(a, b, c, d) \xrightarrow{R^2} (z, F_1(a) \oplus d, a, F_2(a) \oplus b)$
- 

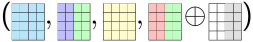
- (Imagine $MC \circ SR$ around all values of the state)



- $(a, b, c, d) \xrightarrow{R^2} (z, F_1(a) \oplus d, a, F_2(a) \oplus b)$
- $F_1($$) \times F_2($$) = MC \circ SR($$) \times MC \circ SR($$)$
- (Imagine $MC \circ SR$ around all values of the state)



Invariant subspaces in Simpira

 $= (a, MC \circ SR(z_1 \oplus x), b, MC \circ SR(z_2 \oplus x \oplus c))$

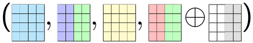
where

- a, b set to all possible values (q^{32})
- z_i set to all possible values in two left columns (q^{16})
- x set to all possible values in two right columns (q^8)
- c random fixed value in two right columns (q^8)

Conclusion for Simpira

- *Invariant subspaces* in round function from *non-invariant subspaces* in AES F-function.
- Covers whole plaintext space with 2^{64} invariant cosets of dimension 56 over $\mathbb{F}_q$ (first time?)
- Trivial distinguisher

Invariant subspaces in Simpira



$$= (a, MC \circ SR(z_1 \oplus x), b, MC \circ SR(z_2 \oplus x \oplus c))$$

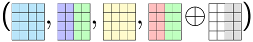
where

- a, b set to all possible values (q^{32})
- z_i set to all possible values in two left columns (q^{16})
- x set to all possible values in two right columns (q^8)
- c random fixed value in two right columns (q^8)

Conclusion for Simpira

- *Invariant subspaces* in round function from *non-invariant subspaces* in AES F-function.
- Covers whole plaintext space with 2^{64} invariant cosets of dimension 56 over $\mathbb{F}_q$ (first time?)
- Trivial distinguisher

Invariant subspaces in Simpira

 $= (a, MC \circ SR(z_1 \oplus x), b, MC \circ SR(z_2 \oplus x \oplus c))$

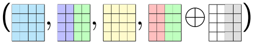
where

- a, b set to all possible values (q^{32})
- z_i set to all possible values in two left columns (q^{16})
- x set to all possible values in two right columns (q^8)
- c random fixed value in two right columns (q^8)

Conclusion for Simpira

- *Invariant subspaces* in round function from *non-invariant subspaces* in AES F-function.
- Covers whole plaintext space with 2^{64} invariant cosets of dimension 56 over $\mathbb{F}_q$ (first time?)
- Trivial distinguisher

Invariant subspaces in Simpira

 $= (a, MC \circ SR(z_1 \oplus x), b, MC \circ SR(z_2 \oplus x \oplus c))$

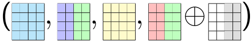
where

- a, b set to all possible values (q^{32})
- z_i set to all possible values in two left columns (q^{16})
- x set to all possible values in two right columns (q^8)
- c random fixed value in two right columns (q^8)

Conclusion for Simpira

- *Invariant subspaces* in round function from *non-invariant subspaces* in AES F-function.
- Covers whole plaintext space with 2^{64} invariant cosets of dimension 56 over $\mathbb{F}_q$ (first time?)
- Trivial distinguisher

Invariant subspaces in Simpira

 $= (a, MC \circ SR(z_1 \oplus x), b, MC \circ SR(z_2 \oplus x \oplus c))$

where

- a, b set to all possible values (q^{32})
- z_i set to all possible values in two left columns (q^{16})
- x set to all possible values in two right columns (q^8)
- c random fixed value in two right columns (q^8)

Conclusion for Simpira

- *Invariant subspaces* in round function from *non-invariant subspaces* in AES F-function.
- Covers whole plaintext space with 2^{64} invariant cosets of dimension 56 over $\mathbb{F}_q$ (first time?)
- Trivial distinguisher

Invariant subspaces in Simpira

(, , ,  $\oplus$ ) $= (a, MC \circ SR(z_1 \oplus x), b, MC \circ SR(z_2 \oplus x \oplus c))$

where

- a, b set to all possible values (q^{32})
- z_i set to all possible values in two left columns (q^{16})
- x set to all possible values in two right columns (q^{8})
- c random fixed value in two right columns (q^{8})

Conclusion for Simpira

- *Invariant subspaces* in round function from *non-invariant subspaces* in AES F-function.
- Covers whole plaintext space with 2^{64} invariant cosets of dimension 56 over $\mathbb{F}_q$ (first time?)
- Trivial distinguisher

Zero-difference cryptanalysis of AES

The zero difference pattern

Definition (Zero difference pattern)

Let $\alpha = (\alpha_0, \alpha_1, \ldots, \alpha_{n-1}) \in \mathbb{F}_q^n$. Define

$$\nu(\alpha) = (z_0, z_1, \ldots, z_{n-1}) \in \mathbb{F}_2^n$$

where

$$z_i = \begin{cases} 1 & \text{if } \alpha_i \text{ is zero,} \\ 0 & \text{otherwise.} \end{cases}$$

Setting

- Let $\alpha = (\alpha_0, \alpha_1, \ldots, \alpha_{n-1}) \in \mathbb{F}_q^n$ denote the state of a block cipher.
- Let $q = 2^k$ and let s be a *kxk* permutation s-box.
- The S-box working on a state is defined by
$$S(\alpha) = (s(\alpha_0), s(\alpha_1), \ldots, s(\alpha_{n-1}))$$
- Let L be a linear layer in the block cipher
- We consider a substitution permutation networn (SPN) of the form $S \circ L \circ S \circ L \circ S$.

Setting

- Let $\alpha = (\alpha_0, \alpha_1, \ldots, \alpha_{n-1}) \in \mathbb{F}_q^n$ denote the state of a block cipher.
- Let $q = 2^k$ and let s be a *kxk* permutation s-box.
- The S-box working on a state is defined by
$$S(\alpha) = (s(\alpha_0), s(\alpha_1), \ldots, s(\alpha_{n-1}))$$
- Let L be a linear layer in the block cipher
- We consider a substitution permutation networn (SPN) of the form $S \circ L \circ S \circ L \circ S$.

Setting

- Let $\alpha = (\alpha_0, \alpha_1, \ldots, \alpha_{n-1}) \in \mathbb{F}_q^n$ denote the state of a block cipher.
- Let $q = 2^k$ and let s be a kxk permutation s-box.
- The S-box working on a state is defined by
$$S(\alpha) = (s(\alpha_0), s(\alpha_1), \ldots, s(\alpha_{n-1}))$$
- Let L be a linear layer in the block cipher
- We consider a substitution permutation networn (SPN) of the form $S \circ L \circ S \circ L \circ S$.

Setting

- Let $\alpha = (\alpha_0, \alpha_1, \ldots, \alpha_{n-1}) \in \mathbb{F}_q^n$ denote the state of a block cipher.
- Let $q = 2^k$ and let s be a kxk permutation s-box.
- The S-box working on a state is defined by
$$S(\alpha) = (s(\alpha_0), s(\alpha_1), \ldots, s(\alpha_{n-1}))$$
- Let L be a linear layer in the block cipher
- We consider a substitution permutation networn (SPN) of the form $S \circ L \circ S \circ L \circ S$.

The S-box

Lemma

For two states α and β in $\mathbb{F}_q^n$, the zero difference pattern is preserved by a permutation S-box

$$\nu(\alpha \oplus \beta) = \nu(S(\alpha) \oplus S(\beta)).$$

Proof.

Follows since $\alpha_i \oplus \beta_i = 0$ iff $s(\alpha_i) \oplus s(\beta_i) = 0$ and thus the S-box preserves the zero difference pattern. □

The S-box

Lemma

For two states α *and* β *in* $\mathbb{F}_q^n$*, the zero difference pattern is preserved by a permutation S-box*

$$\nu(\alpha \oplus \beta) = \nu(S(\alpha) \oplus S(\beta)).$$

Proof.

Follows since $\alpha_i \oplus \beta_i = 0$ iff $s(\alpha_i) \oplus s(\beta_i) = 0$ and thus the S-box preserves the zero difference pattern. □

The exchange operation

Definition

For a vector $c \in \mathbb{F}_2^n$ and a pair of states $\alpha, \beta \in \mathbb{F}_q^n$ define a new state $\rho^c(\alpha, \beta)$ by

$$\rho^c(\alpha, \beta)_i = \begin{cases} \alpha_i & \text{if } c_i = 1, \\ \beta_i & \text{if } c_i = 0. \end{cases}$$

Example

Let $c = (0110)$ and $\alpha = (\alpha_0, \alpha_1, \alpha_2, \alpha_3)$ and $\beta = (\beta_0, \beta_1, \beta_2, \beta_3)$. Then

$$\alpha' = \rho^{(0110)}(\alpha, \beta) = (\beta_0, \alpha_1, \alpha_2, \beta_3)$$

and

$$\beta' = \rho^{(0110)}(\beta, \alpha) = (\alpha_0, \beta_1, \beta_2, \alpha_3)$$

The exchange operation

Definition

For a vector $c \in \mathbb{F}_2^n$ and a pair of states $\alpha, \beta \in \mathbb{F}_q^n$ define a new state $\rho^c(\alpha, \beta)$ by

$$\rho^c(\alpha, \beta)_i = \begin{cases} \alpha_i & \text{if } c_i = 1, \\ \beta_i & \text{if } c_i = 0. \end{cases}$$

Example

Let $c = (0110)$ and $\alpha = (\alpha_0, \alpha_1, \alpha_2, \alpha_3)$ and $\beta = (\beta_0, \beta_1, \beta_2, \beta_3)$. Then

$$\alpha' = \rho^{(0110)}(\alpha, \beta) = (\beta_0, \alpha_1, \alpha_2, \beta_3)$$

and

$$\beta' = \rho^{(0110)}(\beta, \alpha) = (\alpha_0, \beta_1, \beta_2, \alpha_3)$$

Properties of the exchange operation (I)

Lemma

a) $\rho^c(\alpha,\beta)_i \oplus \rho^c(\beta,\alpha)_i = \alpha \oplus \beta$

b) $S(\rho^c(\alpha,\beta)) \oplus S(\rho^c(\beta,\alpha)) = S(\alpha) \oplus S(\beta)$

c) $\rho^c(S(\alpha),S(\beta)) = S(\rho^c(\alpha,\beta))$

Proof.

a)

$$\rho^c(\alpha,\beta) \oplus \rho^c(\beta,\alpha) = \begin{cases} \alpha_i \oplus \beta_i & \text{if } c_i = 1, \\ \beta_i \oplus \alpha_i & \text{if } c_i = 0 \end{cases}$$

b)

$$s(\rho^c(\alpha,\beta)) \oplus s(\rho^c(\beta,\alpha)) = \begin{cases} s(\alpha_i) \oplus s(\beta_i) & \text{if } c_i = 1, \\ s(\beta_i) \oplus s(\alpha_i) & \text{if } c_i = 0 \end{cases}$$

.

c)

$$\rho^c(S(\alpha),S(\beta)) = S(\rho^c(\alpha,\beta)) = \begin{cases} s(\alpha_i) & \text{if } c_i = 1, \\ s(\beta_i) & \text{if } c_i = 0 \end{cases}$$

.

Properties of the exchange operation (I)

Lemma

a) $\rho^c(\alpha, \beta)_i \oplus \rho^c(\beta, \alpha)_i = \alpha \oplus \beta$

b) $S(\rho^c(\alpha, \beta)) \oplus S(\rho^c(\beta, \alpha)) = S(\alpha) \oplus S(\beta)$

c) $\rho^c(S(\alpha), S(\beta)) = S(\rho^c(\alpha, \beta))$

Proof.

a)

$$\rho^c(\alpha, \beta) \oplus \rho^c(\beta, \alpha) = \begin{cases} \alpha_i \oplus \beta_i & \text{if } c_i = 1, \\ \beta_i \oplus \alpha_i & \text{if } c_i = 0 \end{cases}$$

b)

$$s(\rho^c(\alpha, \beta)) \oplus s(\rho^c(\beta, \alpha)) = \begin{cases} s(\alpha_i) \oplus s(\beta_i) & \text{if } c_i = 1, \\ s(\beta_i) \oplus s(\alpha_i) & \text{if } c_i = 0 \end{cases}$$

.

c)

$$\rho^c(S(\alpha), S(\beta)) = S(\rho^c(\alpha, \beta)) = \begin{cases} s(\alpha_i) & \text{if } c_i = 1, \\ s(\beta_i) & \text{if } c_i = 0 \end{cases}$$

.

Properties of the exchange operation (I)

Lemma

a) $\rho^c(\alpha,\beta)_i \oplus \rho^c(\beta,\alpha)_i = \alpha \oplus \beta$

b) $S(\rho^c(\alpha,\beta)) \oplus S(\rho^c(\beta,\alpha)) = S(\alpha) \oplus S(\beta)$

c) $\rho^c(S(\alpha),S(\beta)) = S(\rho^c(\alpha,\beta))$

Proof.

a)

$$\rho^c(\alpha,\beta) \oplus \rho^c(\beta,\alpha) = \begin{cases} \alpha_i \oplus \beta_i & \text{if } c_i = 1, \\ \beta_i \oplus \alpha_i & \text{if } c_i = 0 \end{cases}$$

b)

$$s(\rho^c(\alpha,\beta)) \oplus s(\rho^c(\beta,\alpha)) = \begin{cases} s(\alpha_i) \oplus s(\beta_i) & \text{if } c_i = 1, \\ s(\beta_i) \oplus s(\alpha_i) & \text{if } c_i = 0 \end{cases}$$

.

c)

$$\rho^c(S(\alpha),S(\beta)) = S(\rho^c(\alpha,\beta)) = \begin{cases} s(\alpha_i) & \text{if } c_i = 1, \\ s(\beta_i) & \text{if } c_i = 0 \end{cases}$$

.

Properties of the exchange operation (I)

Lemma

a) $\rho^c(\alpha,\beta)_i \oplus \rho^c(\beta,\alpha)_i = \alpha \oplus \beta$

b) $S(\rho^c(\alpha,\beta)) \oplus S(\rho^c(\beta,\alpha)) = S(\alpha) \oplus S(\beta)$

c) $\rho^c(S(\alpha),S(\beta)) = S(\rho^c(\alpha,\beta))$

Proof.

a)

$$\rho^c(\alpha,\beta) \oplus \rho^c(\beta,\alpha) = \begin{cases} \alpha_i \oplus \beta_i & \text{if } c_i = 1, \\ \beta_i \oplus \alpha_i & \text{if } c_i = 0 \end{cases}$$

b)

$$s(\rho^c(\alpha,\beta)) \oplus s(\rho^c(\beta,\alpha)) = \begin{cases} s(\alpha_i) \oplus s(\beta_i) & \text{if } c_i = 1, \\ s(\beta_i) \oplus s(\alpha_i) & \text{if } c_i = 0 \end{cases}$$

.

c)

$$\rho^c(S(\alpha),S(\beta)) = S(\rho^c(\alpha,\beta)) = \begin{cases} s(\alpha_i) & \text{if } c_i = 1, \\ s(\beta_i) & \text{if } c_i = 0 \end{cases}$$

.

Properties of the exchange operation (I)

Lemma

a) $\rho^c(\alpha,\beta)_i \oplus \rho^c(\beta,\alpha)_i = \alpha \oplus \beta$

b) $S(\rho^c(\alpha,\beta)) \oplus S(\rho^c(\beta,\alpha)) = S(\alpha) \oplus S(\beta)$

c) $\rho^c(S(\alpha),S(\beta)) = S(\rho^c(\alpha,\beta))$

Proof.

a)

$$\rho^c(\alpha,\beta) \oplus \rho^c(\beta,\alpha) = \begin{cases} \alpha_i \oplus \beta_i & \text{if } c_i = 1, \\ \beta_i \oplus \alpha_i & \text{if } c_i = 0 \end{cases}$$

b)

$$s(\rho^c(\alpha,\beta)) \oplus s(\rho^c(\beta,\alpha)) = \begin{cases} s(\alpha_i) \oplus s(\beta_i) & \text{if } c_i = 1, \\ s(\beta_i) \oplus s(\alpha_i) & \text{if } c_i = 0 \end{cases}$$

.

c)

$$\rho^c(S(\alpha),S(\beta)) = S(\rho^c(\alpha,\beta)) = \begin{cases} s(\alpha_i) & \text{if } c_i = 1, \\ s(\beta_i) & \text{if } c_i = 0 \end{cases}$$

.

Properties of the exchange operation (I)

Lemma

a) $\rho^c(\alpha,\beta)_i \oplus \rho^c(\beta,\alpha)_i = \alpha \oplus \beta$

b) $S(\rho^c(\alpha,\beta)) \oplus S(\rho^c(\beta,\alpha)) = S(\alpha) \oplus S(\beta)$

c) $\rho^c(S(\alpha),S(\beta)) = S(\rho^c(\alpha,\beta))$

Proof.

a)

$$\rho^c(\alpha,\beta) \oplus \rho^c(\beta,\alpha) = \begin{cases} \alpha_i \oplus \beta_i & \text{if } c_i = 1, \\ \beta_i \oplus \alpha_i & \text{if } c_i = 0 \end{cases}$$

b)

$$s(\rho^c(\alpha,\beta)) \oplus s(\rho^c(\beta,\alpha)) = \begin{cases} s(\alpha_i) \oplus s(\beta_i) & \text{if } c_i = 1, \\ s(\beta_i) \oplus s(\alpha_i) & \text{if } c_i = 0 \end{cases}$$

.

c)

$$\rho^c(S(\alpha),S(\beta)) = S(\rho^c(\alpha,\beta)) = \begin{cases} s(\alpha_i) & \text{if } c_i = 1, \\ s(\beta_i) & \text{if } c_i = 0 \end{cases}$$

.

Properties of the exchange operation (II)

Lemma

Let L be a linear transformation. Then

$$L(\rho^c(\alpha,\beta)) \oplus L(\rho^c(\beta,\alpha)) = L(\alpha) \oplus L(\beta)$$

Proof.

Lemma 2a) gives

$$\rho^c(\alpha,\beta) \oplus \rho^c(\beta,\alpha) = \alpha \oplus \beta$$

and the result follows from the linearity of L. □

Properties of the exchange operation (II)

Lemma

Let L be a linear transformation. Then

$$L(\rho^c(\alpha, \beta)) \oplus L(\rho^c(\beta, \alpha)) = L(\alpha) \oplus L(\beta)$$

Proof.

Lemma 2a) gives

$$\rho^c(\alpha, \beta) \oplus \rho^c(\beta, \alpha) = \alpha \oplus \beta$$

and the result follows from the linearity of L. □

Properties of the zero-difference pattern

Let $\nu(\alpha)$ denote the zero difference pattern of $\alpha = (\alpha_0, \alpha_1, \ldots, \alpha_{n-1})$.

Lemma

a) $\nu(\alpha \oplus \beta) = \nu(S(\alpha) \oplus S(\beta))$

b) $\nu(S(L(\alpha)) \oplus S(L(\beta))) = \nu(S(L(\rho^c(\alpha, \beta))) \oplus S(L(\rho^c(\beta, \alpha))))$

Proof.

a) Since S is a permutation

$$(\alpha_i \oplus \beta_i) = 0 \text{ iff } s(\alpha_i) \oplus s(\beta_i) = 0$$

b) Since Lemma 3 implies

$$L(\rho^c(\alpha, \beta)) \oplus L(\rho^c(\beta, \alpha)) = L(\alpha) \oplus L(\beta)$$

then

$$\begin{aligned}(S(L(\alpha)) \oplus S(L(\beta)))_i = 0 &\text{ iff } (L(\alpha) \oplus L(\beta))_i = 0 \\ &\text{ iff } (L(\rho^c(\alpha, \beta)) \oplus L(\rho^c(\beta, \alpha)))_i = 0 \\ &\text{ iff } (S(L(\rho^c(\alpha, \beta))) \oplus S(L(\rho^c(\beta, \alpha))))_i = 0\end{aligned}$$

Properties of the zero-difference pattern

Let $\nu(\alpha)$ denote the zero difference pattern of $\alpha = (\alpha_0, \alpha_1, \ldots, \alpha_{n-1})$.

Lemma

a) $\nu(\alpha \oplus \beta) = \nu(S(\alpha) \oplus S(\beta))$

b) $\nu(S(L(\alpha)) \oplus S(L(\beta))) = \nu(S(L(\rho^c(\alpha, \beta))) \oplus S(L(\rho^c(\beta, \alpha))))$

Proof.

a) Since S is a permutation

$$(\alpha_i \oplus \beta_i) = 0 \text{ iff } s(\alpha_i) \oplus s(\beta_i) = 0$$

b) Since Lemma 3 implies

$$L(\rho^c(\alpha, \beta)) \oplus L(\rho^c(\beta, \alpha)) = L(\alpha) \oplus L(\beta)$$

then

$$\begin{aligned}(S(L(\alpha)) \oplus S(L(\beta)))_i = 0 &\text{ iff } (L(\alpha) \oplus L(\beta))_i = 0 \\ &\text{ iff } (L(\rho^c(\alpha, \beta)) \oplus L(\rho^c(\beta, \alpha)))_i = 0 \\ &\text{ iff } (S(L(\rho^c(\alpha, \beta))) \oplus S(L(\rho^c(\beta, \alpha))))_i = 0\end{aligned}$$

Properties of the zero-difference pattern

Let $\nu(\alpha)$ denote the zero difference pattern of $\alpha = (\alpha_0, \alpha_1, \ldots, \alpha_{n-1})$.

Lemma

a) $\nu(\alpha \oplus \beta) = \nu(S(\alpha) \oplus S(\beta))$

b) $\nu(S(L(\alpha)) \oplus S(L(\beta))) = \nu(S(L(\rho^c(\alpha, \beta))) \oplus S(L(\rho^c(\beta, \alpha))))$

Proof.

a) Since S is a permutation

$$(\alpha_i \oplus \beta_i) = 0 \text{ iff } s(\alpha_i) \oplus s(\beta_i) = 0$$

b) Since Lemma 3 implies

$$L(\rho^c(\alpha, \beta)) \oplus L(\rho^c(\beta, \alpha)) = L(\alpha) \oplus L(\beta)$$

then

$$\begin{aligned}(S(L(\alpha)) \oplus S(L(\beta)))_i = 0 &\text{ iff } (L(\alpha) \oplus L(\beta))_i = 0\\ &\text{ iff } (L(\rho^c(\alpha, \beta)) \oplus L(\rho^c(\beta, \alpha)))_i = 0\\ &\text{ iff } (S(L(\rho^c(\alpha, \beta))) \oplus S(L(\rho^c(\beta, \alpha))))_i = 0\end{aligned}$$

Properties of the zero-difference pattern

Let $\nu(\alpha)$ denote the zero difference pattern of $\alpha = (\alpha_0, \alpha_1, \ldots, \alpha_{n-1})$.

Lemma

a) $\nu(\alpha \oplus \beta) = \nu(S(\alpha) \oplus S(\beta))$

b) $\nu(S(L(\alpha)) \oplus S(L(\beta))) = \nu(S(L(\rho^c(\alpha, \beta))) \oplus S(L(\rho^c(\beta, \alpha))))$

Proof.

a) Since S is a permutation

$$(\alpha_i \oplus \beta_i) = 0 \text{ iff } s(\alpha_i) \oplus s(\beta_i) = 0$$

b) Since Lemma 3 implies

$$L(\rho^c(\alpha, \beta)) \oplus L(\rho^c(\beta, \alpha)) = L(\alpha) \oplus L(\beta)$$

then

$$\begin{aligned}(S(L(\alpha)) \oplus S(L(\beta)))_i = 0 &\text{ iff } (L(\alpha) \oplus L(\beta))_i = 0 \\ &\text{ iff } (L(\rho^c(\alpha, \beta)) \oplus L(\rho^c(\beta, \alpha)))_i = 0 \\ &\text{ iff } (S(L(\rho^c(\alpha, \beta))) \oplus S(L(\rho^c(\beta, \alpha)))_i = 0\end{aligned}$$

The Zero-differences and the exchange operation

Theorem

Let $\alpha^{'} = \rho^{c}(\alpha, \beta)$ *and* $\beta^{'} = \rho^{c}(\beta, \alpha)$*, then*

$$\nu(S(L(S(\alpha))) \oplus S(L(S(\beta)))) = \nu(S(L(S(\alpha^{'}))) \oplus S(L(S(\beta^{'}))))$$

The Zero-differences and the exchange operation

Theorem

Let $\alpha^{'} = \rho^c(\alpha, \beta)$ *and* $\beta^{'} = \rho^c(\beta, \alpha)$, *then*

$$\nu(S(L(S(\alpha))) \oplus S(L(S(\beta)))) = \nu(S(L(S(\alpha^{'}))) \oplus S(L(S(\beta^{'}))))$$

Proof.

$$\begin{array}{ccccccc}
\alpha & \oplus & \beta & = & \rho^c(\alpha,\beta) & \oplus & \rho^c(\beta,\alpha) \\
\Downarrow & S & \Downarrow & = & \Downarrow & S & \Downarrow \\
S(\alpha) & \oplus & S(\beta) & = & S(\rho^c(\alpha,\beta)) & \oplus & S(\rho^c(\beta,\alpha)) \\
\Downarrow & L & \Downarrow & = & \Downarrow & L & \Downarrow \\
L(S(\alpha)) & \oplus & L(S(\beta)) & = & L(S(\rho^c(\alpha,\beta))) & \oplus & L(S(\rho^c(\beta,\alpha))) \\
\Downarrow & S & \Downarrow & & \Downarrow & S & \Downarrow \\
S(L(S(\alpha)) & \oplus & S(L(S(\beta))) & & S(L(S(\rho^c(\alpha,\beta)))) & \oplus & S(L(S(\rho^c(\beta,\alpha))))
\end{array}$$

$\square$

The Zero-differences and the exchange operation

Theorem

Let $\alpha' = \rho^c(\alpha,\beta)$ *and* $\beta' = \rho^c(\beta,\alpha)$, *then*

$$\nu(S(L(S(\alpha))) \oplus S(L(S(\beta)))) = \nu(S(L(S(\alpha'))) \oplus S(L(S(\beta'))))$$

Proof.

$$\begin{array}{ccccccc}
\alpha & \oplus & \beta & = & \rho^c(\alpha,\beta) & \oplus & \rho^c(\beta,\alpha) \\
\Downarrow & S & \Downarrow & = & \Downarrow & S & \Downarrow \\
S(\alpha) & \oplus & S(\beta) & = & S(\rho^c(\alpha,\beta)) & \oplus & S(\rho^c(\beta,\alpha)) \\
\Downarrow & L & \Downarrow & = & \Downarrow & L & \Downarrow \\
L(S(\alpha)) & \oplus & L(S(\beta)) & = & L(S(\rho^c(\alpha,\beta))) & \oplus & L(S(\rho^c(\beta,\alpha))) \\
\Downarrow & S & \Downarrow & & \Downarrow & S & \Downarrow \\
S(L(S(\alpha))) & \oplus & S(L(S(\beta))) & & S(L(S(\rho^c(\alpha,\beta)))) & \oplus & S(L(S(\rho^c(\beta,\alpha))))
\end{array}$$

□

The Zero-differences and the exchange operation

Theorem

Let $\alpha' = \rho^c(\alpha, \beta)$ *and* $\beta' = \rho^c(\beta, \alpha)$, *then*

$$\nu(S(L(S(\alpha))) \oplus S(L(S(\beta)))) = \nu(S(L(S(\alpha'))) \oplus S(L(S(\beta'))))$$

Proof.

$$\begin{array}{ccccccc}
\alpha & \oplus & \beta & = & \rho^c(\alpha, \beta) & \oplus & \rho^c(\beta, \alpha) \\
\Downarrow & {\color{red}S} & \Downarrow & = & \Downarrow & {\color{red}S} & \Downarrow \\
S(\alpha) & \oplus & S(\beta) & = & S(\rho^c(\alpha, \beta)) & \oplus & S(\rho^c(\beta, \alpha)) \\
\Downarrow & {\color{red}L} & \Downarrow & = & \Downarrow & {\color{red}L} & \Downarrow \\
L(S(\alpha)) & \oplus & L(S(\beta)) & = & L(S(\rho^c(\alpha, \beta))) & \oplus & L(S(\rho^c(\beta, \alpha))) \\
\Downarrow & {\color{red}S} & \Downarrow & & \Downarrow & {\color{red}S} & \Downarrow \\
S(L(S(\alpha))) & \oplus & S(L(S(\beta))) & & S(L(S(\rho^c(\alpha, \beta)))) & \oplus & S(L(S(\rho^c(\beta, \alpha))))
\end{array}$$

□

The Zero-differences and the exchange operation

Theorem

Let $\alpha' = \rho^c(\alpha, \beta)$ *and* $\beta' = \rho^c(\beta, \alpha)$, *then*

$$\nu(S(L(S(\alpha))) \oplus S(L(S(\beta)))) = \nu(S(L(S(\alpha'))) \oplus S(L(S(\beta'))))$$

Proof.

$$\begin{array}{ccccccc}
\alpha & \oplus & \beta & = & \rho^c(\alpha,\beta) & \oplus & \rho^c(\beta,\alpha) \\
\Downarrow & S & \Downarrow & = & \Downarrow & S & \Downarrow \\
S(\alpha) & \oplus & S(\beta) & = & S(\rho^c(\alpha,\beta)) & \oplus & S(\rho^c(\beta,\alpha)) \\
\Downarrow & L & \Downarrow & = & \Downarrow & L & \Downarrow \\
L(S(\alpha)) & \oplus & L(S(\beta)) & = & L(S(\rho^c(\alpha,\beta))) & \oplus & L(S(\rho^c(\beta,\alpha))) \\
\Downarrow & S & \Downarrow & & \Downarrow & S & \Downarrow \\
S(L(S(\alpha))) & \oplus & S(L(S(\beta))) & & S(L(S(\rho^c(\alpha,\beta)))) & \oplus & S(L(S(\rho^c(\beta,\alpha))))
\end{array}$$

□

The Zero-differences and the exchange operation

Theorem

Let $\alpha' = \rho^c(\alpha, \beta)$ *and* $\beta' = \rho^c(\beta, \alpha)$*, then*

$$\nu(S(L(S(\alpha))) \oplus S(L(S(\beta)))) = \nu(S(L(S(\alpha'))) \oplus S(L(S(\beta'))))$$

Proof.

$$\begin{array}{ccccccc}
\alpha & \oplus & \beta & = & \rho^c(\alpha,\beta) & \oplus & \rho^c(\beta,\alpha) \\
\Downarrow & S & \Downarrow & = & \Downarrow & S & \Downarrow \\
S(\alpha) & \oplus & S(\beta) & = & S(\rho^c(\alpha,\beta)) & \oplus & S(\rho^c(\beta,\alpha)) \\
\Downarrow & L & \Downarrow & = & \Downarrow & L & \Downarrow \\
L(S(\alpha)) & \oplus & L(S(\beta)) & = & L(S(\rho^c(\alpha,\beta))) & \oplus & L(S(\rho^c(\beta,\alpha))) \\
\Downarrow & S & \Downarrow & & \Downarrow & S & \Downarrow \\
S(L(S(\alpha))) & \oplus & S(L(S(\beta))) & & S(L(S(\rho^c(\alpha,\beta)))) & \oplus & S(L(S(\rho^c(\beta,\alpha))))
\end{array}$$

□

Typical use of exchange operation

$$
\begin{array}{ccccccc}
\mu(p^0 & \oplus & p^1) & \overset{(\Leftarrow)}{=} & \mu(p^{0\prime} & \oplus & p^{1\prime}) \\
\Downarrow & S & \Downarrow & = & \Uparrow & S^{-1} & \Uparrow \\
S(p^0) & \oplus & S(p^1) & = & L^{-1}(S^{-1}(c^{0\prime})) & \oplus & L^{-1}(S^{-1}(c^{1\prime})) \\
\Downarrow & L & \Downarrow & = & \Uparrow & L^{-1} & \Uparrow \\
L(S(p^0) & \oplus & L(S(p^1)) & = & S^{-1}(c^{0\prime}) & \oplus & S^{-1}(c^{1\prime}) \\
\Downarrow & S & \Downarrow & & \Uparrow & S^{-1} & \Uparrow \\
c^0 & \oplus & c^1 & \Rightarrow & c^{0\prime} & \oplus & c^{1\prime}
\end{array}
$$

Zero difference preservation

a) Pick two plaintexts p^0 and p^1 with a zero difference $\mu(p^0 \oplus p^1)$.

b) Encrypt p^0 and p^1 to c^0 and c^1.

c) Make two new ciphertexts $c^{0\prime} = \rho^c(c^0, c^1)$ and $c^{1\prime} = \rho^c(c^1, c^2)$.

d) Decrypt $c^{0\prime}$ and $c^{1\prime}$.

e) $\nu(p^0 \oplus p^1) = \nu(p^{0\prime} \oplus p^{1\prime})$

Typical use of exchange operation

$$
\begin{array}{ccccccc}
\mu(p^0 & \oplus & p^1) & \overset{(\Leftarrow)}{=} & \mu(p^{0\prime} & \oplus & p^{1\prime}) \\
\Downarrow & S & \Downarrow & = & \Uparrow & S^{-1} & \Uparrow \\
S(p^0) & \oplus & S(p^1) & = & L^{-1}(S^{-1}(c^{0\prime})) & \oplus & L^{-1}(S^{-1}(c^{1\prime})) \\
\Downarrow & L & \Downarrow & = & \Uparrow & L^{-1} & \Uparrow \\
L(S(p^0)) & \oplus & L(S(p^1)) & = & S^{-1}(c^{0\prime}) & \oplus & S^{-1}(c^{1\prime}) \\
\Downarrow & S & \Downarrow & & \Uparrow & S^{-1} & \Uparrow \\
c^0 & \oplus & c^1 & \Rightarrow & c^{0\prime} & \oplus & c^{1\prime}
\end{array}
$$

Zero difference preservation

a) Pick two plaintexts p^0 and p^1 with a zero difference $\mu(p^0 \oplus p^1)$.

b) Encrypt p^0 and p^1 to c^0 and c^1.

c) Make two new ciphertexts $c^{0\prime} = \rho^c(c^0, c^1)$ and $c^{1\prime} = \rho^c(c^1, c^2)$.

d) Decrypt $c^{0\prime}$ and $c^{1\prime}$.

e) $\nu(p^0 \oplus p^1) = \nu(p^{0\prime} \oplus p^{1\prime})$

Typical use of exchange operation

$$
\begin{array}{ccccccc}
\mu(p^0 & \oplus & p^1) & \overset{(\Leftarrow)}{=} & \mu(p^{0\prime} & \oplus & p^{1\prime}) \\
\Downarrow & S & \Downarrow & = & \Uparrow & S^{-1} & \Uparrow \\
S(p^0) & \oplus & S(p^1) & = & L^{-1}(S^{-1}(c^{0\prime})) & \oplus & L^{-1}(S^{-1}(c^{1\prime})) \\
\Downarrow & L & \Downarrow & = & \Uparrow & L^{-1} & \Uparrow \\
L(S(p^0)) & \oplus & L(S(p^1)) & = & S^{-1}(c^{0\prime}) & \oplus & S^{-1}(c^{1\prime}) \\
\Downarrow & S & \Downarrow & & \Uparrow & S^{-1} & \Uparrow \\
c^0 & \oplus & c^1 & \Rightarrow & c^{0\prime} & \oplus & c^{1\prime}
\end{array}
$$

Zero difference preservation

a) Pick two plaintexts p^0 and p^1 with a zero difference $\mu(p^0 \oplus p^1)$.

b) Encrypt p^0 and p^1 to c^0 and c^1.

c) Make two new ciphertexts $c^{0\prime} = \rho^c(c^0, c^1)$ and $c^{1\prime} = \rho^c(c^1, c^2)$.

d) Decrypt $c^{0\prime}$ and $c^{1\prime}$.

e) $\nu(p^0 \oplus p^1) = \nu(p^{0\prime} \oplus p^{1\prime})$

Typical use of exchange operation

$$
\begin{array}{ccccccc}
\mu(p^0 & \oplus & p^1) & \overset{(\Leftarrow)}{=} & \mu(p^{0\prime} & \oplus & p^{1\prime}) \\
\Downarrow & S & \Downarrow & = & \Uparrow & S^{-1} & \Uparrow \\
S(p^0) & \oplus & S(p^1) & = & L^{-1}(S^{-1}(c^{0\prime})) & \oplus & L^{-1}(S^{-1}(c^{1\prime})) \\
\Downarrow & L & \Downarrow & = & \Uparrow & L^{-1} & \Uparrow \\
L(S(p^0)) & \oplus & L(S(p^1)) & = & S^{-1}(c^{0\prime}) & \oplus & S^{-1}(c^{1\prime}) \\
\Downarrow & S & \Downarrow & & \Uparrow & S^{-1} & \Uparrow \\
c^0 & \oplus & c^1 & \Rightarrow & c^{0\prime} & \oplus & c^{1\prime}
\end{array}
$$

Zero difference preservation

a) Pick two plaintexts p^0 and p^1 with a zero difference $\mu(p^0 \oplus p^1)$.

b) Encrypt p^0 and p^1 to c^0 and c^1.

c) Make two new ciphertexts $c^{0\prime} = \rho^c(c^0, c^1)$ and $c^{1\prime} = \rho^c(c^1, c^2)$.

d) Decrypt $c^{0\prime}$ and $c^{1\prime}$.

e) $\nu(p^0 \oplus p^1) = \nu(p^{0\prime} \oplus p^{1\prime})$

Typical use of exchange operation

$$
\begin{array}{ccccccc}
\mu(p^0 & \oplus & p^1) & \overset{(\Leftarrow)}{=} & \mu(p^{0\prime} & \oplus & p^{1\prime}) \\
\Downarrow & S & \Downarrow & = & \Uparrow & S^{-1} & \Uparrow \\
S(p^0) & \oplus & S(p^1) & = & L^{-1}(S^{-1}(c^{0\prime})) & \oplus & L^{-1}(S^{-1}(c^{1\prime})) \\
\Downarrow & L & \Downarrow & = & \Uparrow & L^{-1} & \Uparrow \\
L(S(p^0) & \oplus & L(S(p^1)) & = & S^{-1}(c^{0\prime}) & \oplus & S^{-1}(c^{1\prime}) \\
\Downarrow & S & \Downarrow & & \Uparrow & S^{-1} & \Uparrow \\
c^0 & \oplus & c^1 & \Rightarrow & c^{0\prime} & \oplus & c^{1\prime}
\end{array}
$$

Zero difference preservation

a) Pick two plaintexts p^0 and p^1 with a zero difference $\mu(p^0 \oplus p^1)$.

b) Encrypt p^0 and p^1 to c^0 and c^1.

c) Make two new ciphertexts $c^{0\prime} = \rho^c(c^0, c^1)$ and $c^{1\prime} = \rho^c(c^1, c^2)$.

d) Decrypt $c^{0\prime}$ and $c^{1\prime}$.

e) $\nu(p^0 \oplus p^1) = \nu(p^{0\prime} \oplus p^{1\prime})$

Typical use of exchange operation

$$
\begin{array}{ccccccccc}
\mu(p^0 & \oplus & p^1) & \overset{(\Leftarrow)}{=} & \mu(p^{0\prime} & \oplus & p^{1\prime}) \\
\Downarrow & S & \Downarrow & = & \Uparrow & S^{-1} & \Uparrow \\
S(p^0) & \oplus & S(p^1) & = & L^{-1}(S^{-1}(c^{0\prime})) & \oplus & L^{-1}(S^{-1}(c^{1\prime})) \\
\Downarrow & L & \Downarrow & = & \Uparrow & L^{-1} & \Uparrow \\
L(S(p^0)) & \oplus & L(S(p^1)) & = & S^{-1}(c^{0\prime}) & \oplus & S^{-1}(c^{1\prime}) \\
\Downarrow & S & \Downarrow & & \Uparrow & S^{-1} & \Uparrow \\
c^0 & \oplus & c^1 & \Rightarrow & c^{0\prime} & \oplus & c^{1\prime}
\end{array}
$$

Zero difference preservation

a) Pick two plaintexts p^0 and p^1 with a zero difference $\mu(p^0 \oplus p^1)$.

b) Encrypt p^0 and p^1 to c^0 and c^1.

c) Make two new ciphertexts $c^{0\prime} = \rho^c(c^0, c^1)$ and $c^{1\prime} = \rho^c(c^1, c^2)$.

d) Decrypt $c^{0\prime}$ and $c^{1\prime}$.

e) $\nu(p^0 \oplus p^1) = \nu(p^{0\prime} \oplus p^{1\prime})$

Typical use of exchange operation

$$
\begin{array}{ccccccc}
\mu(p^0 & \oplus & p^1) & \overset{(\Leftarrow)}{=} & \mu(p^{0\prime} & \oplus & p^{1\prime}) \\
\Downarrow & S & \Downarrow & = & \Uparrow & S^{-1} & \Uparrow \\
S(p^0) & \oplus & S(p^1) & = & L^{-1}(S^{-1}(c^{0\prime})) & \oplus & L^{-1}(S^{-1}(c^{1\prime})) \\
\Downarrow & L & \Downarrow & = & \Uparrow & L^{-1} & \Uparrow \\
L(S(p^0)) & \oplus & L(S(p^1)) & = & S^{-1}(c^{0\prime}) & \oplus & S^{-1}(c^{1\prime}) \\
\Downarrow & S & \Downarrow & & \Uparrow & S^{-1} & \Uparrow \\
c^0 & \oplus & c^1 & \Rightarrow & c^{0\prime} & \oplus & c^{1\prime}
\end{array}
$$

Zero difference preservation

a) Pick two plaintexts p^0 and p^1 with a zero difference $\mu(p^0 \oplus p^1)$.

b) Encrypt p^0 and p^1 to c^0 and c^1.

c) Make two new ciphertexts $c^{0\prime} = \rho^c(c^0, c^1)$ and $c^{1\prime} = \rho^c(c^1, c^2)$.

d) Decrypt $c^{0\prime}$ and $c^{1\prime}$.

e) $\nu(p^0 \oplus p^1) = \nu(p^{0\prime} \oplus p^{1\prime})$

Typical use of exchange operation

$$
\begin{array}{ccccccc}
\mu(p^0 & \oplus & p^1) & & & & \\
\Downarrow & S & \Downarrow & & & & \\
S(p^0) & \oplus & S(p^1) & = & L^{-1}(S^{-1}(c^{0\prime})) & \oplus & L^{-1}(S^{-1}(c^{1\prime})) \\
\Downarrow & L & \Downarrow & = & \Uparrow & L^{-1} & \Uparrow \\
L(S(p^0)) & \oplus & L(S(p^1)) & = & S^{-1}(c^{0\prime}) & \oplus & S^{-1}(c^{1\prime}) \\
\Downarrow & S & \Downarrow & & \Uparrow & S^{-1} & \Uparrow \\
c^0 & \oplus & c^1 & \Rightarrow & c^{0\prime} & \oplus & c^{1\prime}
\end{array}
$$

Zero difference preservation

a) Pick two plaintexts p^0 and p^1 with a zero difference $\mu(p^0 \oplus p^1)$.

b) Encrypt p^0 and p^1 to c^0 and c^1.

c) Make two new ciphertexts $c^{0\prime} = \rho^c(c^0, c^1)$ and $c^{1\prime} = \rho^c(c^1, c^2)$.

d) Decrypt $c^{0\prime}$ and $c^{1\prime}$.

Typical use of exchange operation

$$
\begin{array}{ccccccc}
\mu(p^0 & \oplus & p^1) & \overset{(\Leftarrow)}{=} & \mu(p^{0\prime}) & \oplus & p^{1\prime}) \\
\Downarrow & S & \Downarrow & = & \Uparrow & S^{-1} & \Uparrow \\
S(p^0) & \oplus & S(p^1) & = & L^{-1}(S^{-1}(c^{0\prime})) & \oplus & L^{-1}(S^{-1}(c^{1\prime})) \\
\Downarrow & L & \Downarrow & = & \Uparrow & L^{-1} & \Uparrow \\
L(S(p^0) & \oplus & L(S(p^1)) & = & S^{-1}(c^{0\prime}) & \oplus & S^{-1}(c^{1\prime}) \\
\Downarrow & S & \Downarrow & & \Uparrow & S^{-1} & \Uparrow \\
c^0 & \oplus & c^1 & \Rightarrow & c^{0\prime} & \oplus & c^{1\prime}
\end{array}
$$

Zero difference preservation

a) Pick two plaintexts p^0 and p^1 with a zero difference $\mu(p^0 \oplus p^1)$.

b) Encrypt p^0 and p^1 to c^0 and c^1.

c) Make two new ciphertexts $c^{0\prime} = \rho^c(c^0, c^1)$ and $c^{1\prime} = \rho^c(c^1, c^2)$.

d) Decrypt $c^{0\prime}$ and $c^{1\prime}$.

e) $\nu(p^0 \oplus p^1) = \nu(p^{0\prime} \oplus p^{1\prime})$

Three Rounds of AES

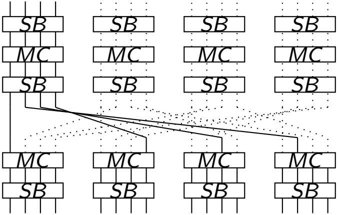


Figure: Three rounds $SB \circ MC \circ SR \circ S = Q \circ S$

$$R^3 = (AK \circ MC \circ SR \circ SB) \circ (AK \circ MC \circ SR \circ SB) \circ (AK \circ MC \circ SR \circ SB).$$

Rewrite in terms of

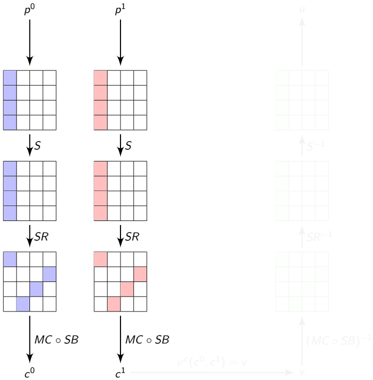
- $S = MC \circ SB \circ MC$
- $L = SR \circ MC \circ SR$

$$R^{*3} = (SB \circ MC \circ SR) \circ (SB \circ MC \circ SB) = Q \circ S$$

Three Round AES Distinguisher

Theorem

Three rounds of AES can be distinguished from a random cipher using one pair of chosen plaintexts and one (adaptively) chosen ciphertext.



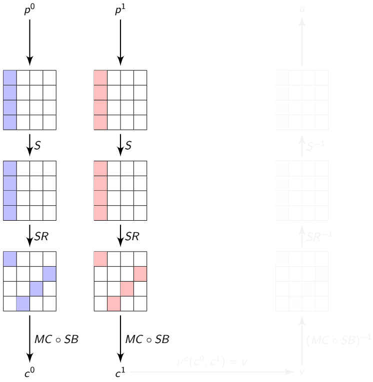
1. Select $p^0 \oplus p^1$ that differ in only one word
2. ask for encryption c^0 and c^1 of p^0 and p^1
3. Let H_i be the image of the ith column of $SR(S(p^0) \oplus S(p^1))$ under $MC \circ SB$
4. select $v = (v_0, v_1, v_2, v_3)$ where $v_i \in \{c_i^0, c_i^1\}$
5. ask for decryption (denote u) of v
6. Then $\nu(p^0 \oplus p^1) = \nu(u \oplus p^i)$ since the ith component of v is in H_i

Probability 2^{-96} for random.

Three Round AES Distinguisher

Theorem

Three rounds of AES can be distinguished from a random cipher using one pair of chosen plaintexts and one (adaptively) chosen ciphertext.



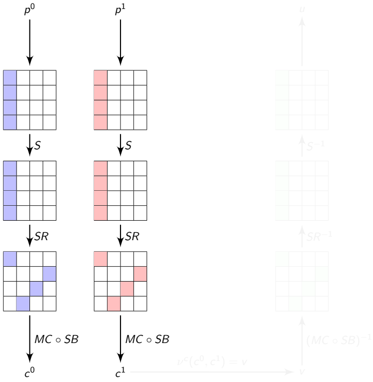
1. Select $p^0 \oplus p^1$ that differ in only one word
2. ask for encryption c^0 and c^1 of p^0 and p^1
3. Let H_i be the image of the ith column of $SR(S(p^0) \oplus S(p^1))$ under $MC \circ SB$
4. select $v = (v_0, v_1, v_2, v_3)$ where $v_i \in \{c_i^0, c_i^1\}$
5. ask for decryption (denote u) of v
6. Then $\nu(p^0 \oplus p^1) = \nu(u \oplus p^i)$ since the ith component of v is in H_i

Probability 2^{-96} for random.

Three Round AES Distinguisher

Theorem

Three rounds of AES can be distinguished from a random cipher using one pair of chosen plaintexts and one (adaptively) chosen ciphertext.



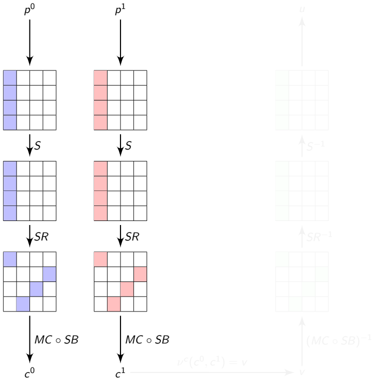
1. Select $p^0 \oplus p^1$ that differ in only one word
2. ask for encryption c^0 and c^1 of p^0 and p^1
3. Let H_i be the image of the ith column of $SR(S(p^0) \oplus S(p^1))$ under $MC \circ SB$
4. select $v = (v_0, v_1, v_2, v_3)$ where $v_i \in \{c_i^0, c_i^1\}$
5. ask for decryption (denote u) of v
6. Then $\nu(p^0 \oplus p^1) = \nu(u \oplus p^i)$ since the ith component of v is in H_i

Probability 2^{-96} for random.

Three Round AES Distinguisher

Theorem

Three rounds of AES can be distinguished from a random cipher using one pair of chosen plaintexts and one (adaptively) chosen ciphertext.



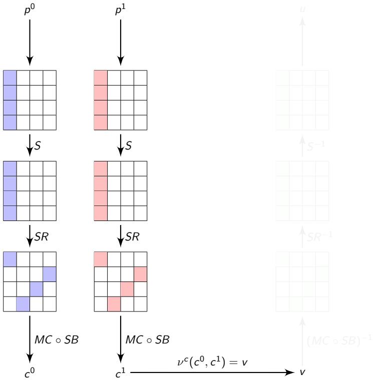
1. Select $p^0 \oplus p^1$ that differ in only one word
2. ask for encryption c^0 and c^1 of p^0 and p^1
3. Let H_i be the image of the ith column of $SR(S(p^0) \oplus S(p^1))$ under $MC \circ SB$
4. select $v = (v_0, v_1, v_2, v_3)$ where $v_i \in \{c_i^0, c_i^1\}$
5. ask for decryption (denote u) of v
6. Then $\nu(p^0 \oplus p^1) = \nu(u \oplus p^i)$ since the ith component of v is in H_i

Probability 2^{-96} for random.

Three Round AES Distinguisher

Theorem

Three rounds of AES can be distinguished from a random cipher using one pair of chosen plaintexts and one (adaptively) chosen ciphertext.



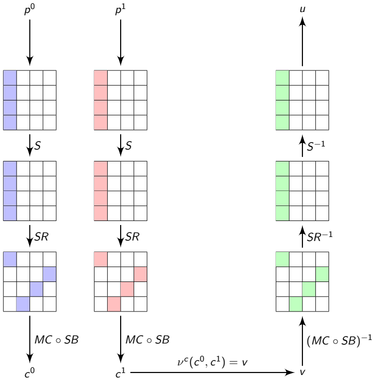
1. Select $p^0 \oplus p^1$ that differ in only one word
2. ask for encryption c^0 and c^1 of p^0 and p^1
3. Let H_i be the image of the ith column of $SR(S(p^0) \oplus S(p^1))$ under $MC \circ SB$
4. select $v = (v_0, v_1, v_2, v_3)$ where $v_i \in \{c_i^0, c_i^1\}$
5. ask for decryption (denote u) of v
6. Then $\nu(p^0 \oplus p^1) = \nu(u \oplus p^i)$ since the ith component of v is in H_i

Probability 2^{-96} for random.

Three Round AES Distinguisher

Theorem

Three rounds of AES can be distinguished from a random cipher using one pair of chosen plaintexts and one (adaptively) chosen ciphertext.



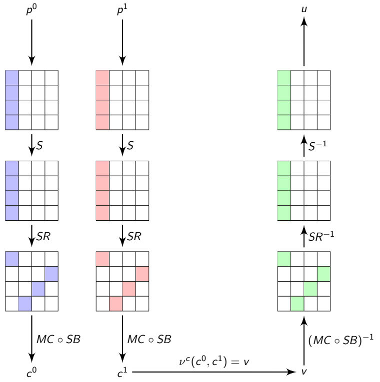
1. Select $p^0 \oplus p^1$ that differ in only one word
2. ask for encryption c^0 and c^1 of p^0 and p^1
3. Let H_i be the image of the ith column of $SR(S(p^0) \oplus S(p^1))$ under $MC \circ SB$
4. select $v = (v_0, v_1, v_2, v_3)$ where $v_i \in \{c_i^0, c_i^1\}$
5. ask for decryption (denote u) of v
6. Then $\nu(p^0 \oplus p^1) = \nu(u \oplus p^i)$ since the ith component of v is in H_i

Probability 2^{-96} for random.

Three Round AES Distinguisher

Theorem

Three rounds of AES can be distinguished from a random cipher using one pair of chosen plaintexts and one (adaptively) chosen ciphertext.



1. Select $p^0 \oplus p^1$ that differ in only one word
2. ask for encryption c^0 and c^1 of p^0 and p^1
3. Let H_i be the image of the ith column of $SR(S(p^0) \oplus S(p^1))$ under $MC \circ SB$
4. select $v = (v_0, v_1, v_2, v_3)$ where $v_i \in \{c_i^0, c_i^1\}$
5. ask for decryption (denote u) of v
6. Then $\nu(p^0 \oplus p^1) = \nu(u \oplus p^j)$ since the ith component of v is in H_i

Probability 2^{-96} for random.

Four Rounds of AES

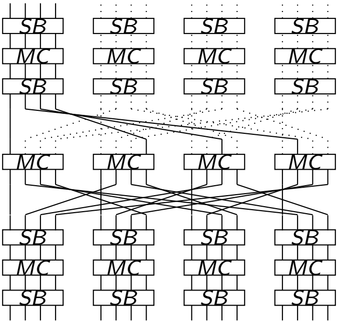
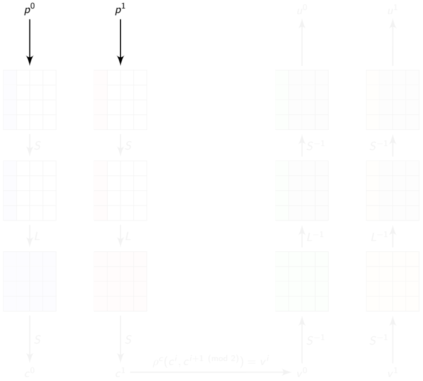


Figure: $S \circ L \circ S$ in AES

Four Round AES Distinguisher

Theorem

Four rounds of AES can be distinguished from a random cipher using one pair of chosen plaintexts and one (adaptively) chosen ciphertext pair.



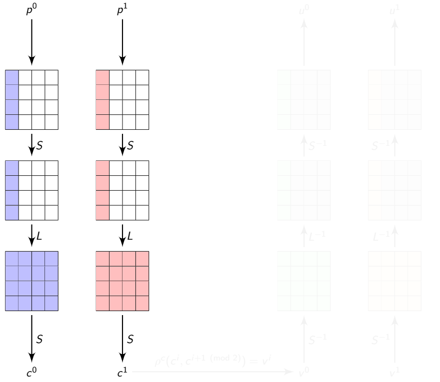
1. Select $p^0 \oplus p^1$ that differ in only one word
2. ask for encryption c^0 and c^1 of p^0 and p^1
3. construct $v^0 = \rho^c(c^0, c^1), v^1 = \rho^c(c^1, c^0)$
4. get plaintexts u^0, u^1.
5. if AES, then same zero difference pattern (prob for random $= 2^{96}$)

Extends to 5-round distinguisher and key-recovery.

Four Round AES Distinguisher

Theorem

Four rounds of AES can be distinguished from a random cipher using one pair of chosen plaintexts and one (adaptively) chosen ciphertext pair.



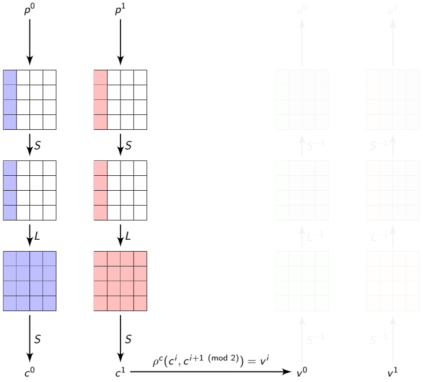
1. Select $p^0 \oplus p^1$ that differ in only one word
2. ask for encryption c^0 and c^1 of p^0 and p^1
3. construct $v^0 = \rho^c(c^0, c^1), v^1 = \rho^c(c^1, c^0)$
4. get plaintexts u^0, u^1.
5. if AES, then same zero difference pattern (prob for random $= 2^{96}$)

Extends to 5-round distinguisher and key-recovery.

Four Round AES Distinguisher

Theorem

Four rounds of AES can be distinguished from a random cipher using one pair of chosen plaintexts and one (adaptively) chosen ciphertext pair.



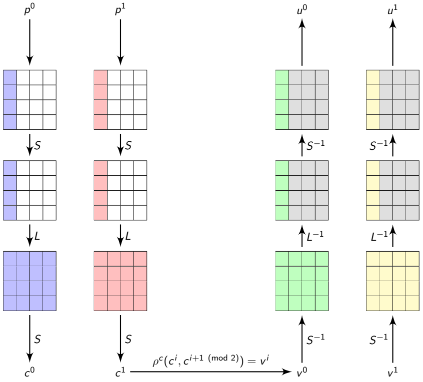
1. Select $p^0 \oplus p^1$ that differ in only one word
2. ask for encryption c^0 and c^1 of p^0 and p^1
3. construct $v^0 = \rho^c(c^0, c^1), v^1 = \rho^c(c^1, c^0)$
4. get plaintexts u^0, u^1.
5. if AES, then same zero difference pattern (prob for random $= 2^{96}$)

Extends to 5-round distinguisher and key-recovery.

Four Round AES Distinguisher

Theorem

Four rounds of AES can be distinguished from a random cipher using one pair of chosen plaintexts and one (adaptively) chosen ciphertext pair.



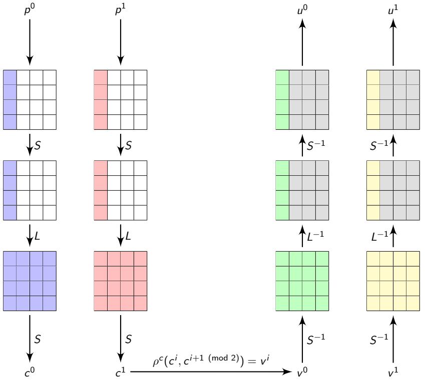
1. Select $p^0 \oplus p^1$ that differ in only one word
2. ask for encryption c^0 and c^1 of p^0 and p^1
3. construct $v^0 = \rho^c(c^0, c^1), v^1 = \rho^c(c^1, c^0)$
4. get plaintexts u^0, u^1.
5. if AES, then same zero difference pattern (prob for random $= 2^{96}$)

Extends to 5-round distinguisher and key-recovery.

Four Round AES Distinguisher

Theorem

Four rounds of AES can be distinguished from a random cipher using one pair of chosen plaintexts and one (adaptively) chosen ciphertext pair.



1. Select $p^0 \oplus p^1$ that differ in only one word
2. ask for encryption c^0 and c^1 of p^0 and p^1
3. construct $v^0 = \rho^c(c^0, c^1), v^1 = \rho^c(c^1, c^0)$
4. get plaintexts u^0, u^1.
5. if AES, then same zero difference pattern (prob for random $= 2^{96}$)

Extends to 5-round distinguisher and key-recovery.

6 Round AES as $S \circ L \circ S \circ L \circ S$

- 6 rounds AES is $S \circ L \circ S \circ LS$
- preserve zero differences in middle
- combine with impossible differential property
- first distinguisher for 6 rounds (high complexity)

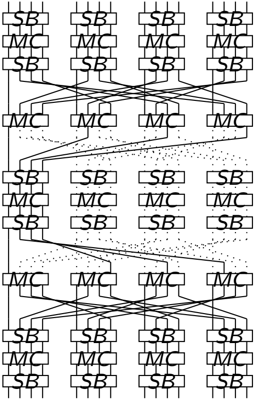


Figure: Six Rounds AES

Conclusion

- new records 3-6 round distinguishers AES
- new record 5 round key recovery
- can be applied directly to similar designs as well
- can be improved (more rounds) for lightweight designs

Conclusion

Thank you!

Exchange operation and $S \circ L \circ S \circ L \circ S$ ciphers

Theorem

Let

- $p^{0\prime} = \rho^c(p^0, p^1)$ $p^{1\prime} = \rho^c(p^1, p^0)$
- $c^{0*} = \rho^c(c^0, c^1)$ $c^{1*} = \rho^c(c^1, c^0)$
- $G_2 = S \circ L \circ S$

$$\nu(G_2(p^{0\prime}) \oplus G_2(p^{1\prime})) = \nu(G_2^{-1}(c^{*0}) \oplus G_2^{-1}(c^{*1})).$$

Exchange operation and $S \circ L \circ S \circ L \circ S$ ciphers

Theorem

Let

- $p^{0\prime} = \rho^c(p^0, p^1)$ $p^{1\prime} = \rho^c(p^1, p^0)$
- $c^{0*} = \rho^c(c^0, c^1)$ $c^{1*} = \rho^c(c^1, c^0)$
- $G_2 = S \circ L \circ S$

$$\nu(G_2(p^{0\prime}) \oplus G_2(p^{1\prime})) = \nu(G_2^{-1}(c^{*0}) \oplus G_2^{-1}(c^{*1})).$$

$$\begin{array}{ccccccccccc}
p^0 & \oplus & p^1 & = & p^{0\prime} & \oplus & p^{1\prime} & & p^{0*} & \oplus & p^{1*} \\
\Downarrow & S & \Downarrow & = & \Downarrow & S & \Downarrow & & \Uparrow & S^{-1} & \Uparrow \\
S(p^0) & \oplus & S(p^1) & = & S(p^{0\prime}) & \oplus & S(p^{1\prime}) & & & & \\
\Downarrow & L & \Downarrow & = & \Downarrow & L & \Downarrow & & \Uparrow & L^{-1} & \Uparrow \\
L(S(p^0)) & \oplus & L(S(p^1)) & = & L(S(p^{0\prime})) & \oplus & L(S(p^{1\prime})) & & G_2^{-1}(c^{0*}) & \oplus & G_2^{-1}(c^{1*}) \\
\Downarrow & S & \Downarrow & = & \Downarrow & S & \Downarrow & & \Uparrow & S^{-1} & \Uparrow \\
\Downarrow & L & \Downarrow & = & G_2(p^{0\prime}) & \oplus & G_2(p^{1\prime}) & & \Uparrow & L^{-1} & \Uparrow \\
\Downarrow & S & \Downarrow & & & & & & \Uparrow & S^{-1} & \Uparrow \\
c^0 & \oplus & c^1 & & & \Rightarrow & & & c^{0*} & \oplus & c^{1*}
\end{array}$$

Exchange operation and $S \circ L \circ S \circ L \circ S$ ciphers

Theorem

Let

- $p^{0\prime} = \rho^c(p^0, p^1)$ $p^{1\prime} = \rho^c(p^1, p^0)$
- $c^{0*} = \rho^c(c^0, c^1)$ $c^{1*} = \rho^c(c^1, c^0)$
- $G_2 = S \circ L \circ S$

$$\nu(G_2(p^{0\prime}) \oplus G_2(p^{1\prime})) = \nu(G_2^{-1}(c^{*0}) \oplus G_2^{-1}(c^{*1})).$$

p^0	$\oplus$	p^1	$=$	$p^{0\prime}$	$\oplus$	$p^{1\prime}$	p^{0*}	$\oplus$	p^{1*}
$\Downarrow$	S	$\Downarrow$	$=$	$\Downarrow$	S	$\Downarrow$	$\Uparrow$	S^{-1}	$\Uparrow$
$S(p^0)$	$\oplus$	$S(p^1)$	$=$	$S(p^{0\prime})$	$\oplus$	$S(p^{1\prime})$			
$\Downarrow$	L	$\Downarrow$	$=$	$\Downarrow$	L	$\Downarrow$	$\Uparrow$	L^{-1}	$\Uparrow$
$L(S(p^0))$	$\oplus$	$L(S(p^1))$	$=$	$L(S(p^{0\prime}))$	$\oplus$	$L(S(p^{1\prime}))$	$G_2^{-1}(c^{0*})$	$\oplus$	$G_2^{-1}(c^{1*})$
$\Downarrow$	S	$\Downarrow$	$=$	$\Downarrow$	S	$\Downarrow$	$\Uparrow$	S^{-1}	$\Uparrow$
$\Downarrow$	L	$\Downarrow$	$=$	$G_2(p^{0\prime})$	$\oplus$	$G_2(p^{1\prime})$	$\Uparrow$	L^{-1}	$\Uparrow$
$\Downarrow$	S	$\Downarrow$					$\Uparrow$	S^{-1}	$\Uparrow$
c^0	$\oplus$	c^1			$\Rightarrow$		c^{0*}	$\oplus$	c^{1*}

Exchange operation and $S \circ L \circ S \circ L \circ S$ ciphers

Theorem

Let

- $p^{0\prime} = \rho^c(p^0, p^1)$ $p^{1\prime} = \rho^c(p^1, p^0)$
- $c^{0*} = \rho^c(c^0, c^1)$ $c^{1*} = \rho^c(c^1, c^0)$
- $G_2 = S \circ L \circ S$

$$\nu(G_2(p^{0\prime}) \oplus G_2(p^{1\prime})) = \nu(G_2^{-1}(c^{*0}) \oplus G_2^{-1}(c^{*1})).$$

$$\begin{array}{ccccccccccc}
p^0 & \oplus & p^1 & = & p^{0\prime} & \oplus & p^{1\prime} & & p^{0*} & \oplus & p^{1*} \\
\Downarrow & S & \Downarrow & = & \Downarrow & S & \Downarrow & & \Uparrow & S^{-1} & \Uparrow \\
S(p^0) & \oplus & S(p^1) & = & S(p^{0\prime}) & \oplus & S(p^{1\prime}) & & & & \\
\Downarrow & L & \Downarrow & = & \Downarrow & L & \Downarrow & & \Uparrow & L^{-1} & \Uparrow \\
L(S(p^0)) & \oplus & L(S(p^1)) & = & L(S(p^{0\prime})) & \oplus & L(S(p^{1\prime})) & & G_2^{-1}(c^{0*}) & \oplus & G_2^{-1}(c^{1*}) \\
\Downarrow & S & \Downarrow & = & \Downarrow & S & \Downarrow & & \Uparrow & S^{-1} & \Uparrow \\
\Downarrow & L & \Downarrow & = & G_2(p^{0\prime}) & \oplus & G_2(p^{1\prime}) & & \Uparrow & L^{-1} & \Uparrow \\
\Downarrow & S & \Downarrow & & & & & & \Uparrow & S^{-1} & \Uparrow \\
c^0 & \oplus & c^1 & & & \Rightarrow & & & c^{0*} & \oplus & c^{1*}
\end{array}$$

Exchange operation and $S \circ L \circ S \circ L \circ S$ ciphers

Theorem

Let

- $p^{0\prime} = \rho^c(p^0, p^1)$ $p^{1\prime} = \rho^c(p^1, p^0)$
- $c^{0*} = \rho^c(c^0, c^1)$ $c^{1*} = \rho^c(c^1, c^0)$
- $G_2 = S \circ L \circ S$

$$\nu(G_2(p^{0\prime}) \oplus G_2(p^{1\prime})) = \nu(G_2^{-1}(c^{*0}) \oplus G_2^{-1}(c^{*1})).$$

$$\begin{array}{ccccccccccc}
p^0 & \oplus & p^1 & = & p^{0\prime} & \oplus & p^{1\prime} & & & & \\
\Downarrow & S & \Downarrow & = & \Downarrow & S & \Downarrow & & & & \\
S(p^0) & \oplus & S(p^1) & = & S(p^{0\prime}) & \oplus & S(p^{1\prime}) & & & & \\
\Downarrow & L & \Downarrow & = & \Downarrow & L & \Downarrow & & & & \\
L(S(p^0)) & \oplus & L(S(p^1)) & = & L(S(p^{0\prime})) & \oplus & L(S(p^{1\prime})) & & & & \\
\Downarrow & S & \Downarrow & = & \Downarrow & S & \Downarrow & & & & \\
\Downarrow & L & \Downarrow & = & G_2(p^{0\prime}) & \oplus & G_2(p^{1\prime}) & & & & \\
\Downarrow & S & \Downarrow & & & & & & & & \\
c^0 & \oplus & c^1 & & & \Rightarrow & & & c^{0*} & \oplus & c^{1*}
\end{array}$$

Exchange operation and $S \circ L \circ S \circ L \circ S$ ciphers

Theorem

Let

- $p^{0\prime} = \rho^c(p^0, p^1)$ $p^{1\prime} = \rho^c(p^1, p^0)$
- $c^{0*} = \rho^c(c^0, c^1)$ $c^{1*} = \rho^c(c^1, c^0)$
- $G_2 = S \circ L \circ S$

$$\nu(G_2(p^{0\prime}) \oplus G_2(p^{1\prime})) = \nu(G_2^{-1}(c^{*0}) \oplus G_2^{-1}(c^{*1})).$$

$$\begin{array}{cccccccccc}
p^0 & \oplus & p^1 & = & p^{0\prime} & \oplus & p^{1\prime} & p^{0*} & \oplus & p^{1*} \\
\Downarrow & S & \Downarrow & = & \Downarrow & S & \Downarrow & \Uparrow & S^{-1} & \Uparrow \\
S(p^0) & \oplus & S(p^1) & = & S(p^{0\prime}) & \oplus & S(p^{1\prime}) & & & \\
\Downarrow & L & \Downarrow & = & \Downarrow & L & \Downarrow & \Uparrow & L^{-1} & \Uparrow \\
L(S(p^0)) & \oplus & L(S(p^1)) & = & L(S(p^{0\prime})) & \oplus & L(S(p^{1\prime})) & G_2^{-1}(c^{0*}) & \oplus & G_2^{-1}(c^{1*}) \\
\Downarrow & S & \Downarrow & = & \Downarrow & S & \Downarrow & \Uparrow & S^{-1} & \Uparrow \\
\Downarrow & L & \Downarrow & = & G_2(p^{0\prime}) & \oplus & G_2(p^{1\prime}) & \Uparrow & L^{-1} & \Uparrow \\
\Downarrow & S & \Downarrow & & & & & \Uparrow & S^{-1} & \Uparrow \\
c^0 & \oplus & c^1 & & & \Rightarrow & & c^{0*} & \oplus & c^{1*}
\end{array}$$

Exchange operation and $S \circ L \circ S \circ L \circ S$ ciphers

Theorem

Let

- $p^{0\prime} = \rho^c(p^0, p^1)\ p^{1\prime} = \rho^c(p^1, p^0)$
- $c^{0*} = \rho^c(c^0, c^1)\ c^{1*} = \rho^c(c^1, c^0)$
- $G_2 = S \circ L \circ S$

$$\nu(G_2(p^{0\prime}) \oplus G_2(p^{1\prime})) = \nu(G_2^{-1}(c^{*0}) \oplus G_2^{-1}(c^{*1})).$$

$$\begin{array}{ccccccccccc}
p^0 & \oplus & p^1 & = & p^{0\prime} & \oplus & p^{1\prime} & & p^{0*} & \oplus & p^{1*} \\
\Downarrow & S & \Downarrow & = & \Downarrow & S & \Downarrow & & \Uparrow & S^{-1} & \Uparrow \\
S(p^0) & \oplus & S(p^1) & = & S(p^{0\prime}) & \oplus & S(p^{1\prime}) & & & & \\
\Downarrow & L & \Downarrow & = & \Downarrow & L & \Downarrow & & \Uparrow & L^{-1} & \Uparrow \\
L(S(p^0)) & \oplus & L(S(p^1)) & = & L(S(p^{0\prime})) & \oplus & L(S(p^{1\prime})) & & G_2^{-1}(c^{0*}) & \oplus & G_2^{-1}(c^{1*}) \\
\Downarrow & S & \Downarrow & = & \Downarrow & S & \Downarrow & & \Uparrow & S^{-1} & \Uparrow \\
\Downarrow & L & \Downarrow & = & G_2(p^{0\prime}) & \oplus & G_2(p^{1\prime}) & & \Uparrow & L^{-1} & \Uparrow \\
\Downarrow & S & \Downarrow & & & & & & \Uparrow & S^{-1} & \Uparrow \\
c^0 & \oplus & c^1 & & & \Rightarrow & & & c^{0*} & \oplus & c^{1*}
\end{array}$$