Constructing permutations, involutions and orthomorphisms with almost optimal cryptographic parameters

Reynier Antonio de la Cruz Jiménez

Institute of Cryptography, Havana University, Cuba.

Summary

1 Introduction

2 Notations and operations

3 Basic cryptographic properties of S-Boxes

4 General S-Box Design Criteria

5 Construction of nonlinear bijective transformations

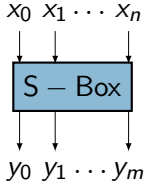
- Permutations
- Involutions
- Orthomorphisms

6 Masking complexity of 8-bit S-Boxes obtained by the scheme of $\hat{\pi}$ and $\hat{\pi}^{(invol)}$

7 Conclusion

Motivation

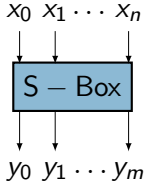
An S-Box is a function mapping a small number of bits n to m bits



Among the whole set of S-Boxes the bijective ones (also-called permutations) are particularly interesting.

Motivation

An S-Box is a function mapping a small number of bits n to m bits



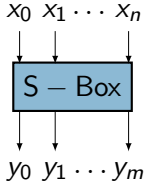
Among the whole set of S-Boxes the bijective ones (also-called permutations) are particularly interesting.

S-Boxes are one of the main crypto primitives for building suitable strong cryptographic products.

Application of S-Boxes

Motivation

An S-Box is a function mapping a small number of bits n to m bits



Among the whole set of S-Boxes the bijective ones (also-called permutations) are particularly interesting.

S-Boxes are one of the main crypto primitives for building suitable strong cryptographic products.

Application of S-Boxes

- Block ciphers;
- Stream ciphers;
- MAC;
- Hash functions;
- Authenticated ciphers.

Motivation

Known methods for constructing S-Boxes

- algebraic constructions;
- pseudo-random generation;
- heuristic techniques;
- constructions from small to large S-Boxes.

Each approach has its advantages and disadvantages respectively.

Motivation

Known methods for constructing S-Boxes

- algebraic constructions;
- pseudo-random generation;
- heuristic techniques;
- constructions from small to large S-Boxes.

Each approach has its advantages and disadvantages respectively.

To construct nonlinear bijective transformations having cryptographic parameters close to optimal is an unsolved problem at present time.

We propose a new construction (using the last approach) for generating such S-Boxes.

Notations and operations

$a \| b$	- concatenation of the vectors a, b of V_l, i.e., a vector from V_{2l} ;
0	- the null vector of V_l;
$\oplus$	- bitwise eXclusive-OR. Addition in $\mathrm{GF}(2^l)$;
$\langle a, b \rangle$	- the scalar product of vectors $a = (a_{l-1}, \ldots, a_0), b = (b_{l-1}, \ldots, b_0)$ of V_l and is equal to $\langle a, b \rangle = a_{l-1}b_{l-1} \oplus \ldots \oplus a_0 b_0$;
$\otimes$	- finite field multiplication;
$\Lambda \circ \Psi$	- a composition of mappings, where Ψ is the first to operate;
Ψ^{-1}	- the inverse transformation to some bijective mapping Ψ
$\chi(\Phi_1, \Phi_2)$	- the Hamming distance between $\Phi_1, \Phi_2 \in S(V_l)$;

Basic cryptographic properties of S-Boxes.

Properties of S-Boxes

Cryptographic properties of S-Boxes deal with the application of attacks on ciphers. For this reason nonlinear bijective transformations must satisfy various criteria for providing high level of protection against different types of attacks.

Properties of S-Boxes

Definition

For $a, b \in V_n$ the Walsh transform $\mathcal{W}_\Phi(a, b)$ of an n-bit S-Box Φ is defined as

$$\mathcal{W}_\Phi(a, b) = \sum_{x \in V_n} (-1)^{\langle b, \Phi(x) \rangle \oplus \langle a, x \rangle}. \tag{1}$$

Definition

The nonlinearity of an n-bit S-Box Φ, denoted by $\mathcal{NL}(\Phi)$, is defined as

$$\mathcal{NL}(\Phi) = 2^{n-1} - \frac{1}{2} \cdot \max_{b \neq 0, a \in \mathrm{GF}(2^n)} |\mathcal{W}_\Phi(a, b)|. \tag{2}$$

From a cryptographic point of view S-Boxes with small values of Walsh coefficients offer better resistance against linear attacks.

Properties of S-Boxes

Definition

The differential uniformity (also called δ-uniformity) of an n-bit S-Box Φ, denoted by δ_Φ, is defined as

$$\delta_\Phi = \max_{a \neq 0, b \in \mathrm{GF}(2^n)} \Delta_\Phi(a, b), \tag{3}$$

where $\Delta_\Phi(a, b) = \#\{x \in \mathrm{GF}(2^n) | \, \Phi(x \oplus a) \oplus \Phi(x) = b\}$.

The resistance offered by an S-Box against differential attacks is related by the highest value of δ, for this reason nonlinear bijective transformations must have a small value of δ-uniformity for a sufficient level of protection against this type of attacks.

Properties of S-Boxes

Definition

The minimum (maximum) algebraic degree of an S-Box Φ, denoted by $\deg(\Phi)$, is the minimum (maximum) among all maximum numbers of variables of the terms in the algebraic normal form of $(\langle a, \Phi(x)\rangle)$ for all possible values x and $a \neq 0$:

$$\deg(\Phi)_{(\min)} = \min_{a \neq 0 \in V_n} \deg\left(\langle a, \Phi(x)\rangle\right), \tag{4}$$

$$\deg(\Phi)_{(\max)} = \max_{a \neq 0 \in V_n} \deg\left(\langle a, \Phi(x)\rangle\right). \tag{5}$$

In general, S-Boxes should have high minimum (maximum) degree because S-Boxes with low degree are susceptible to algebraic attack, higher-order differential, interpolation, cube attacks etc.

Properties of S-Boxes

Definition

The algebraic immunity of U is defined as

$$\mathcal{AI}(U) = \min\left\{ \deg p \;\middle|\; 0 \neq p \in \mathrm{GF}(2)[z_1, \ldots, z_{2n}], p(U) = 0 \right\}. \tag{6}$$

Definition

The graph algebraic immunity of n-bit S-Box Φ, denoted by $\mathcal{AI}_{gr}(\Phi)$, is defined as

$$\mathcal{AI}_{gr}(\Phi) = \min\left\{ \deg p \;\middle|\; 0 \neq p \in \mathrm{GF}(2)[z_1, \ldots, z_{2n}], p(gr(\Phi)) = 0 \right\}, \tag{7}$$

where $gr(\Phi) = \{(x, \Phi(x)) | x \in \mathrm{GF}(2^n)\} \subseteq \mathrm{GF}(2^{2n})$.
Thus we focus on the graph algebraic immunity of S-Box Φ and also on the parameter $r_{\Phi}^{(AI_{gr}(\Phi))}$ referred to as the number of all the independent equations in input and output values of the S-Box Φ, i.e., equations of the form $p(x, \Phi(x)) = 0$, for all $x \in \mathrm{GF}(2^n)$.

Properties of S-Boxes

Definition

An element $a \in V_n$ is called a fixed point of an n-bit S-Box Φ if $\Phi(a) = a$.

Definition

Two n-bit S-Boxes Φ_1 and Φ_2 are linear (resp. affine) equivalent if there exist linear (resp. affine) mappings A_1, A_2, such that $\Phi_2 = A_2 \circ \Phi_1 \circ A_1$.

It is well-known that the following cryptographic parameters: δ-uniformity, nonlinearity and minimum (maximum) algebraic degree remains invariant under linear (resp. affine) equivalence.

Design Criteria

Our goal, is to find permutations constructed by smaller ones that satisfy the following criteria[1] (which in what follows are called almost optimal):

1. Maximum value of minimum degree;
2. Maximum graph algebraic immunity with the minimum number of equations;
3. Minimum value of δ-uniformity limited by parameter listed above;
4. Maximum value of nonlinearity limited by parameter listed above.

[1] Our design criteria are basically the same as those included in: *A method for generation of high-nonlinear S-boxes based on gradient descent*. Kazymyrov O. V., Kazymyrova V. N., Oliynykov R. V. Mat. Vopr. Kriptogr., 2014, Volume 5, Issue 2, 71-78.

Design Criteria

For example,when $n = 8$ an almost optimal nonlinear bijective transformation $\Phi \in S(V_8)$ should satisfy the following

Set of cryptographic criteria for $8-$bit permutations :

- $\deg(\Phi)_{(\min)} = 7$;
- $\mathcal{AI}_{gr}(\Phi) = 3$ with $r_{\Phi}^{(3)} = 441$;
- $\delta_{\Phi} \leq 8$;
- $\mathcal{NL}(\Phi) \geq 100$.

Let be $n = 2k$ a natural number, where $k \geq 2$. Choosing:

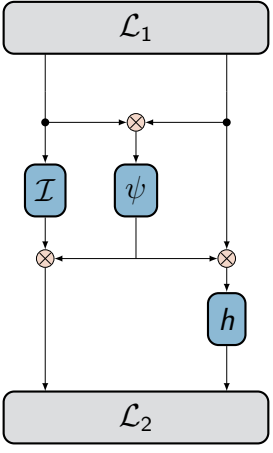
- Finite field inversion function $\mathcal{I} = x^{-1}$ over $\mathrm{GF}(2^k)$;
- Non-bijective k-bit function ψ which has no preimage for 0;
- Arbitrary permutation $h \in S(V_k)$;
- Arbitrary binary matrices $\mathcal{L}_i \in \mathrm{GL}_{2k}(\mathrm{GF}(2)), i = 1, 2$.

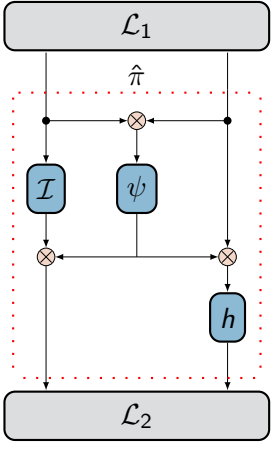
We construct the following $2k$-bit class of permutations π from V_{2k} to V_{2k} as follows

Construction of π

For the input value $(l\|r) \in V_{2k}$ we define the corresponding output value $\pi(l\|r) = (l_1\|r_1)$ as a result of the following computations:

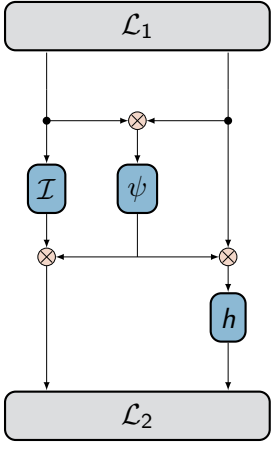
$$(l_1\|r_1) := \mathcal{L}_1(l\|r);$$
$$(l_1\|r_1) := (\mathcal{I}(l_1) \otimes \psi(l_1 \otimes r_1))\|h(r_1 \otimes \psi(l_1 \otimes r_1));$$
$$(l_1\|r_1) := \mathcal{L}_2(l_1\|r_1).$$

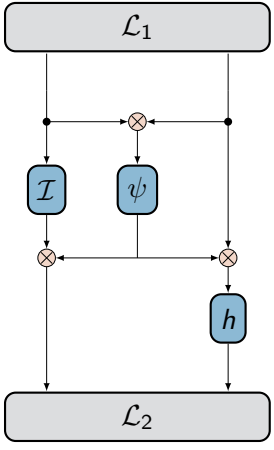




The number of permutations that can be build by using the construction $\hat{\pi}$ is approximately equal to 2^{107}.

Permutations
Some properties of π

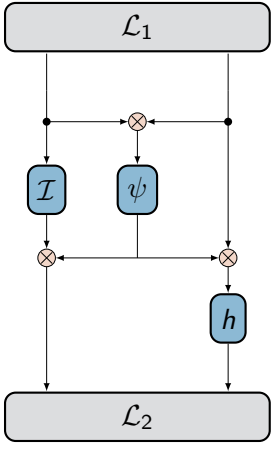




Proposition 1

Let $h = \mathcal{I}$ and ψ — non-bijective k-bit function ψ which has no preimage for 0. Then

$$\mathcal{NL}(\pi) \geq 2^k - \lfloor 2^{\frac{k}{2}+1} \rfloor - 1. \tag{8}$$



Proposition 1

Let $h = \mathcal{I}$ and ψ — non-bijective k-bit function ψ which has no preimage for 0. Then

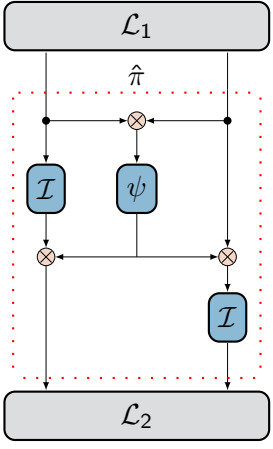
$$\mathcal{NL}(\pi) \geq 2^k - \lfloor 2^{\frac{k}{2}+1} \rfloor - 1. \tag{8}$$

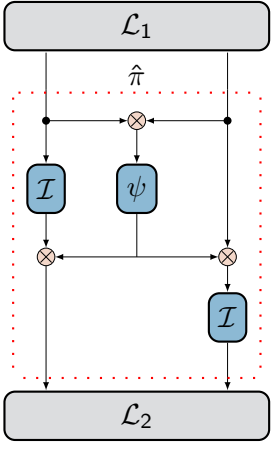
Proposition 2

Let $\psi : V_k \to V_k$ be an arbitrary non-bijective function which has no preimage for 0. Then for the permutation π, when $h = \mathcal{I}$ the following inequalities holds

$$k - 1 \leq \deg(\pi)_{(\max)} \leq 2k - 1. \tag{9}$$

Permutations
Some properties of π





Proposition 3

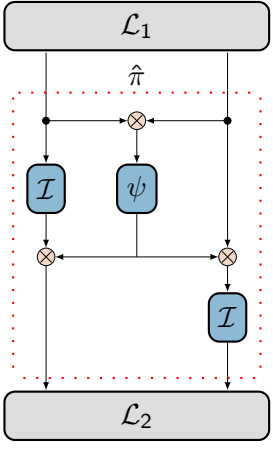
If the lookup-tables of non-bijective k-bit functions

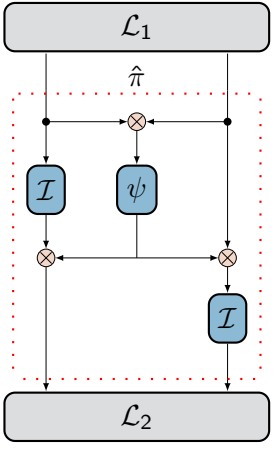
$$\psi = \begin{pmatrix} \dots & i & \dots \\ \dots & \psi(i) & \dots \end{pmatrix}, \hat{\psi} = \begin{pmatrix} \dots & i & \dots \\ \dots & \hat{\psi}(i) & \dots \end{pmatrix}$$

differs from each other exactly in one output value, then for permutations $\hat{\pi}_\psi, \hat{\pi}_{\hat{\psi}}$ the following relation holds:

$$\chi(\hat{\pi}_\psi, \hat{\pi}_{\hat{\psi}}) = \begin{cases} 2 \cdot (2^k - 1), & \text{if} \quad i = 0; \\ 2^k - 1, & \text{if} \quad i \neq 0. \end{cases} \tag{10}$$

Permutations
Some properties of π





Proposition 4

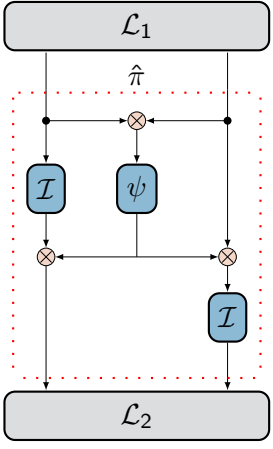
If the lookup-tables of non-bijective k-bit functions

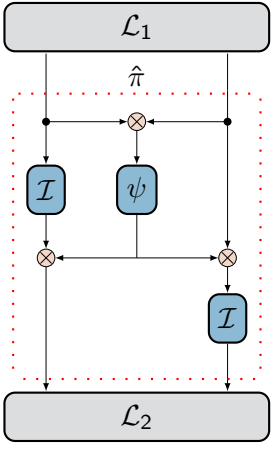
$$\psi = \begin{pmatrix} \dots & i & \dots \\ \dots & \psi(i) & \dots \end{pmatrix}, \hat{\psi} = \begin{pmatrix} \dots & i & \dots \\ \dots & \hat{\psi}(i) & \dots \end{pmatrix}$$

differs from each other exactly in one output value, then for permutations $\hat{\pi}_\psi, \hat{\pi}_{\hat{\psi}}$ the following relation holds:

1. $\mathcal{NL}(\hat{\pi}_\psi) - 2 \cdot \lfloor 2^{\frac{k}{2}+1} \rfloor \leq \mathcal{NL}(\hat{\pi}_{\hat{\psi}}) \leq \mathcal{NL}(\hat{\pi}_\psi) + 2 \cdot \lfloor 2^{\frac{k}{2}+1} \rfloor$, when $i = 0$;
2. $\mathcal{NL}(\hat{\pi}_\psi) - (2^k - 1) \leq \mathcal{NL}(\hat{\pi}_{\hat{\psi}}) \leq \mathcal{NL}(\hat{\pi}_\psi) + (2^k - 1)$, when $i \neq 0$.

Permutations
Some properties of π





Proposition 5

If the lookup-tables of non-bijective k-bit functions

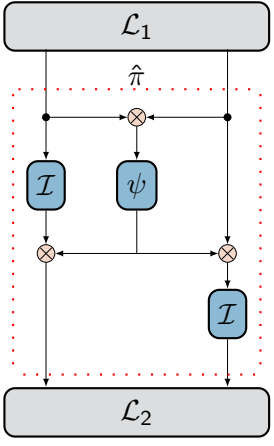
$$\psi = \begin{pmatrix} \dots & i & \dots \\ \dots & \psi(i) & \dots \end{pmatrix}, \hat{\psi} = \begin{pmatrix} \dots & i & \dots \\ \dots & \hat{\psi}(i) & \dots \end{pmatrix}$$

differs from each other exactly in one output value, then for permutations $\hat{\pi}_\psi, \hat{\pi}_{\hat{\psi}}$ the following relation holds:

1. $\delta_{\hat{\pi}_\psi} - 4 \cdot (2^k - 1) \leq \delta_{\hat{\pi}_{\hat{\psi}}} \leq \delta_{\pi_\psi} + 4 \cdot (2^k - 1)$, when $i = 0$;
2. $\delta_{\hat{\pi}_\psi} - 2 \cdot (2^k - 1) \leq \delta_{\hat{\pi}_{\hat{\psi}}} \leq \delta_{\hat{\pi}_\psi} + 2 \cdot (2^k - 1)$, when $i \neq 0$.

Permutations

8-bit permutations having almost optimal cryptographic parameters



By using propositions 4 and 5 we have developed two search algorithms for finding 8-bit S-Boxes with high-values of its basic cryptographic parameters

Algorithm 1: Optimizing differential properties of $\hat{\pi}$

Input: Permutation $\mathcal{I} = x^{-1}$ over $\mathrm{GF}(2^k)$, parameter $\ell \in \mathbb{N}$.

1 Generate randomly a non-bijective k-bit function ψ and construct $\hat{\pi}_\psi = (\mathcal{I}(l) \otimes \psi(l \otimes r)) \| \mathcal{I}(r \otimes \psi(l \otimes r)) \in S(V_{2k})$.

2 For permutation $\hat{\pi}_\psi \in S(V_{2k})$ calculate the value $\delta_{\hat{\pi}_\psi}$.

3 Initialize the list L:

$$\mathsf{L} = \{(\psi, \hat{\pi}_\psi, \delta_{\hat{\pi}_\psi})\}, \text{where } \#\mathsf{L} = 1.$$

4 Using the list $\mathsf{L} = \{(\psi^{(i)}, \hat{\pi}_{\psi^{(i)}}, \delta_{\hat{\pi}_{\psi^{(i)}}}) | i = 0, \ldots, \#\mathsf{L} - 1\}$ construct the new list

$$\widetilde{\mathsf{L}} = \{(\tilde{\psi}^{(i)}_{j,t}, \hat{\pi}_{\tilde{\psi}^{(i)}_{j,t}}, \delta_{\hat{\pi}_{\tilde{\psi}^{(i)}_{j,t}}})\}, \text{where } \#\widetilde{\mathsf{L}} \leq \#\mathsf{L} \cdot 2^k \cdot (2^k - 2),$$

and for each $i = 0, \ldots, \#\mathsf{L} - 1$, $\delta_{\hat{\pi}_{\tilde{\psi}^{(i)}_{j,t}}} \leq \delta_{\hat{\pi}_{\psi^{(i)}}}$, the non-bijective k-bit functions $\tilde{\psi}^{(i)}_{j,t}, j = 0, \ldots, 2^k - 1, t = 0, \ldots 2^k - 3$, differs from $\psi^{(i)}$ exactly in one output value.

For the list $\widetilde{\mathsf{L}}$ do the following:

(I) Calculate the size $\#\widetilde{\mathsf{L}}$.

(II) Sort the elements of $\widetilde{\mathsf{L}}$ in ascending order.

(III) Numerate the sorted list element by indexes $i = 0, \ldots, \#\widetilde{\mathsf{L}} - 1$.

(IV) Calculate values $m_1 = \min\{\#\mathsf{L} - 1, \#\widetilde{\mathsf{L}} - 1\}, m_2 = \min\{\ell - 1, \#\widetilde{\mathsf{L}} - 1\}$.

5 Compare the first elements of list L and $\widetilde{\mathsf{L}}$:

– If $\sum_{i=0}^{m_1} \delta_{\hat{\pi}_{\tilde{\psi}(i)}} < \sum_{i=0}^{m_1} \delta_{\hat{\pi}_{\psi(i)}}$, then

(I) Clean the list L.

(II) Copy the elements from the list $\widetilde{\mathsf{L}}$ with indexes $i = 0, \ldots, m_2$ to L.

(III) Assign $\#\mathsf{L} = m_2 + 1$.

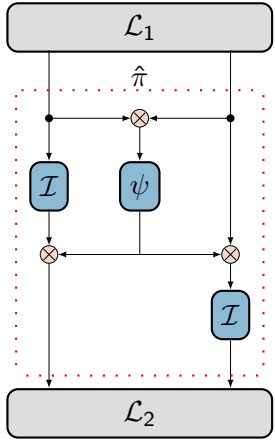
(IV) Go to step 4.

– Otherwise, the algorithm stops.

Output: The list $\widetilde{\mathsf{L}} = \{(\psi^{(i)}, \hat{\pi}_{\psi^{(i)}}, \delta_{\hat{\pi}_{\psi^{(i)}}}) | i = 0, \ldots, \#\widetilde{\mathsf{L}} - 1\}$, $\#\widetilde{\mathsf{L}} \leq \ell$.

Permutations

8-bit permutations having almost optimal cryptographic parameters



By using propositions 4 and 5 we have developed two search algorithms for finding 8-bit S-Boxes with high-values of its basic cryptographic parameters

Algorithm 2: Optimizing (non)linear properties of $\hat{\pi}$

Input: Permutation $\mathcal{I} = x^{-1}$ over $\mathrm{GF}(2^k)$, parameter $\ell \in \mathbb{N}$.

1 Generate randomly a non-bijective k-bit function ψ and construct $\hat{\pi}_\psi = (\mathcal{I}(l) \otimes \psi(l \otimes r) \| \mathcal{I}(r \otimes \psi(l \otimes r)) \in S(V_{2k})$.

2 For permutation $\hat{\pi}_\psi \in S(V_{2k})$ calculate the value $\mathcal{NL}(\hat{\pi}_\psi)$.

3 Initialize the list L:

$$\mathsf{L} = \{(\psi, \hat{\pi}_\psi, \mathcal{NL}(\hat{\pi}_\psi))\}, \text{where } \#\mathsf{L} = 1.$$

4 Using the list $\mathsf{L} = \{(\psi^{(i)}, \hat{\pi}_{\psi^{(i)}}, \mathcal{NL}(\hat{\pi}_{\psi^{(i)}})) | i = 0, \ldots, \#\mathsf{L} - 1\}$ construct the new list

$$\widetilde{\mathsf{L}} = \{(\tilde{\psi}^{(i)}_{s,t}, \hat{\pi}_{\tilde{\psi}^{(i)}_{s,t}}, \mathcal{NL}(\hat{\pi}_{\tilde{\psi}^{(i)}_{s,t}}))\}, \text{where } \#\widetilde{\mathsf{L}} \leq \#\mathsf{L} \cdot 2^k \cdot (2^k - 2),$$

and for each $i = 0, \ldots, \#\mathsf{L} - 1$, $\mathcal{NL}(\hat{\pi}_{\tilde{\psi}^{(i)}_{s,t}}) \geq \mathcal{NL}(\hat{\pi}_{\psi^{(i)}})$, the non-bijective k-bit functions $\tilde{\psi}^{(i)}_{s,t}, j = 0, \ldots, 2^k - 1, t = 0, \ldots 2^k - 3$, differs from $\psi^{(i)}$ exactly in one output value. For the list $\widetilde{\mathsf{L}}$ do the following:

(I) Calculate the size $\#\widetilde{\mathsf{L}}$.
(II) Sort the elements of $\widetilde{\mathsf{L}}$ in ascending order.
(III) Numerate the sorted list element by indexes $i = 0, \ldots, \#\widetilde{\mathsf{L}} - 1$.
(IV) Calculate values $m_1 = \min\{\#\mathsf{L} - 1, \#\widetilde{\mathsf{L}} - 1\}, m_2 = \min\{\ell - 1, \#\widetilde{\mathsf{L}} - 1\}$.

5 Compare the first elements of list L and $\widetilde{\mathsf{L}}$:

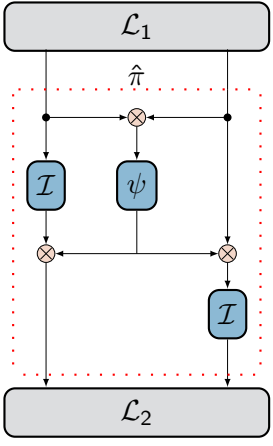
– If $\sum_{i=0}^{m_1} \mathcal{NL}(\hat{\pi}_{\tilde{\psi}^{(i)}}) > \sum_{i=0}^{m_1} \mathcal{NL}(\hat{\pi}_{\psi^{(i)}})$, then
  (I) Clean the list L.
  (II) Copy the elements from the list $\widetilde{\mathsf{L}}$ with indexes $i = 0, \ldots, m_2$ to L.
  (III) Assign $\#\mathsf{L} = m_2 + 1$.
  (IV) Go to step 4.

– Otherwise, the algorithm stops.

Output: The list $\widetilde{\mathsf{L}} = \{(\psi^{(i)}, \hat{\pi}_{\psi^{(i)}}, \mathcal{NL}(\hat{\pi}_{\psi^{(i)}})) | i = 0, \ldots, \#\widetilde{\mathsf{L}} - 1\}, \#\widetilde{\mathsf{L}} \leq \ell$.

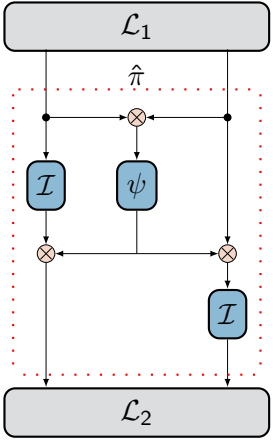
Permutations

8-bit permutations having almost optimal cryptographic parameters



Permutations

8-bit permutations having almost optimal cryptographic parameters



We have found ordinary 8-bit S-Boxes having the following cryptographic parameters

- minimum algebraic degree equal to 7;
- graph algebraic immunity equal to 3 (with 441 equations);
- δ-uniformity equal to 6 or 8;
- nonlinearity in range of 100 up to a value of 104.

Invariant subspaces with respect to the action of $\hat{\pi}$.

The existence of subspaces W of the vector space V_n such that $\hat{\pi}(W \oplus a) = W \oplus b$ for some fixed elements $a, b \in V_n$ are used when mounting structural attacks on block ciphers.[2]

The existence of such structures can:

1. significantly decrease the cryptographic security of block ciphers[3];
2. be used to introduce a backdoor in a block cipher[4].

[2] see, for example: "*A cryptanalysis of PRINT cipher: The invariant subspace attack*" by Leander G., Abdelraheem M., Alkhzaimi H., Zenner E. in CRYPTO'11, Lect. Notes Comput. Sci., 6841 (2011), 206-221.

[3] *A family of trapdoor ciphers* by Rijmen V., Preneel B in FSE'97. Lect. Notes Comp.Sci. - 1997. - V. 1267. - P. 139 - 148.

[4] *Partition-based trapdoor ciphers* by Bannier A., Bodin N and Filiol E, Cryptology ePrint Archive, Report 2016/493, 2016. http://eprint. iacr.org/2016/493.

Permutations

Invariant subspaces with respect to the action of $\hat{\pi}$

The question are:

- How to verify the invariance of a fixed subspace W with respect to the action of some given nonlinear bijective transformation?;
- If there exist such structures (invariant subspaces) in the construction of $\hat{\pi}$ what we can do to fix this weakness?.

- How to verify the invariance of a fixed subspace W with respect to the action of some given nonlinear bijective transformation?.

[5] proposed by Pogorelov B. A. , Pudovkina M. A., in the article: "On the distance from permutations to imprimitive groups for a fixed system of imprimitivity", Discrete Math. Appl., 24:2 (2014), 95-108.

- How to verify the invariance of a fixed subspace W with respect to the action of some given nonlinear bijective transformation?.

By using the so-called W-intersection matrix[5] defined as follows

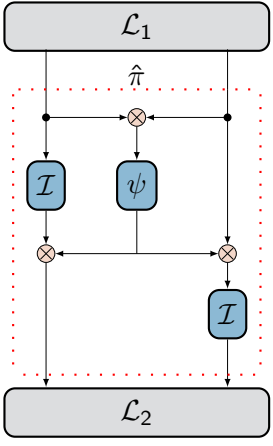
$$\mathcal{M}_{\mathrm{W}}(\Phi) = \left\| c^{\mathrm{W}}_{\alpha,\beta}(\Phi) \right\|_{\alpha,\beta \in \mathcal{R}_{\mathrm{W}}},$$

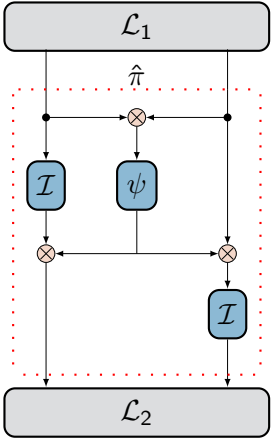
where $\Phi \in S(V_n)$, $c^{\mathrm{W}}_{\alpha,\beta}(\Phi) = \#\left\{ x \in \mathrm{W} \oplus \alpha \,\middle|\, \Phi(x) \in \mathrm{W} \oplus \beta \right\}$, $\mathrm{W} < V_n$, $\dim \mathrm{W} = d \in \{1, 2, \ldots, n-1\}$ and $\mathcal{R}_{\mathrm{W}}$ is the set of coset representatives for the subspace $\mathrm{W} < V_n$.

[5] proposed by Pogorelov B. A. , Pudovkina M. A., in the article: "On the distance from permutations to imprimitive groups for a fixed system of imprimitivity", Discrete Math. Appl., 24:2 (2014), 95-108.

Permutations

Invariant subspaces with respect to the action of $\hat{\pi}$





Proposition 6

Let $\mathrm{W}_1 = \{(l\|0)|\, l \in V_k\}, \mathrm{W}_2 = \{(0\|r)|\, r \in V_k\}$ be two k-dimensional subspaces of the vector space V_{2k} . Then

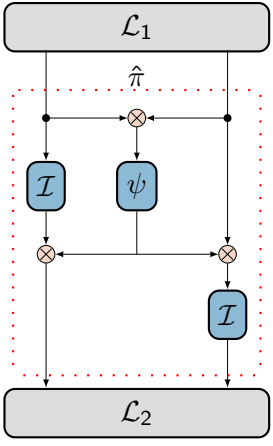
$$c_{0,0}^{\mathrm{W}_1}(\hat{\pi}) = c_{0,0}^{\mathrm{W}_2}(\hat{\pi}) = 2^k. \tag{11}$$

Corollary

The following k-dimensional subspaces $\mathrm{W}_1 \oplus (\alpha_1\|0)$ and $\mathrm{W}_2 \oplus (0\|\alpha_2)$ are invariant with respect to the action of $\hat{\pi}$ for any $\alpha_1, \alpha_2 \in V_k$.

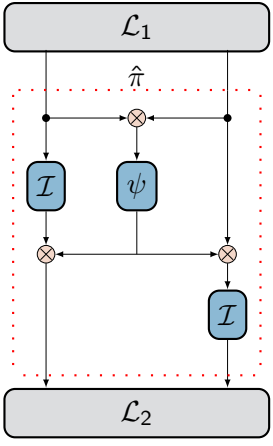
Permutations

Invariant subspaces with respect to the action of $\hat{\pi}$



Permutations

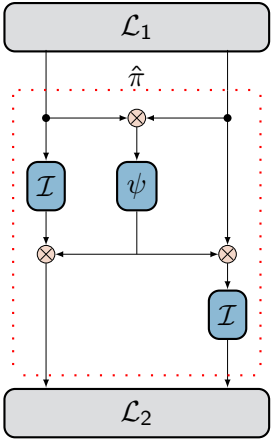
Invariant subspaces with respect to the action of $\hat{\pi}$



- If there exist such structures (invariant subspaces) in the construction of $\hat{\pi}$ what we can do to fix this weakness?.

Permutations

Invariant subspaces with respect to the action of $\hat{\pi}$



- If there exist such structures (invariant subspaces) in the construction of $\hat{\pi}$ what we can do to fix this weakness?.

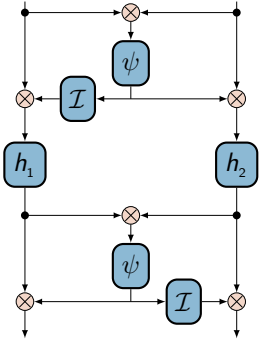
The existence of invariant subspaces can be circumvented by choosing appropriate linear (resp. affine) layers $\mathcal{L}_1$ and $\mathcal{L}_2$ from $\mathrm{GL}_{2k}(\mathrm{GF}(2))$, which also explain why we have inserted these matrices in the original construction of $\pi = \mathcal{L}_1 \circ \hat{\pi} \circ \mathcal{L}_2$.

Involutions.

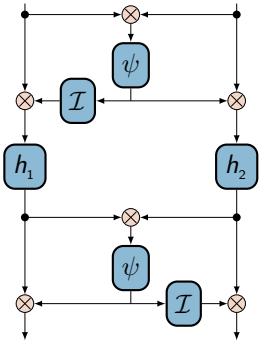
Involutions
Their role in Cryptography

Involutions, i.e, permutations $\Phi \in S(V_n)$ with the property $\Phi(\Phi(x)) = x$ for all $x \in V_n$, have an particular interest in Cryptography because in the case of lightweight block ciphers, these components are used to decrease the cost of the implementation of decryption process.

We have tried to design directly involutions using ours scheme as building block. Choosing two arbitrary k-bit involutions h_1, h_2, the following constructions is able to produce $2k$-bit involutions.



We have tried to design directly involutions using ours scheme as building block. Choosing two arbitrary k-bit involutions h_1, h_2, the following constructions is able to produce $2k$-bit involutions.



Construction of $\hat{\pi}^{(invol)}$

For the input value $(l\|r) \in V_{2k}$ we define the corresponding output value as follows

$$\hat{\pi}^{(invol)}(l\|r) = (\hat{\pi}_3 \circ \hat{\pi}_2 \circ \hat{\pi}_1)(l\|r) = l_1\|r_1 \quad \text{where,}$$

$$\hat{\pi}_1(l\|r) = (l \otimes \mathcal{I}(\psi(l \otimes r)))\,\|\,(r \otimes \psi(l \otimes r));$$

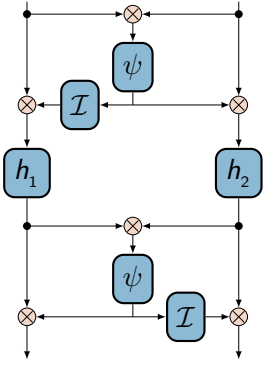
$$\hat{\pi}_2(l\|r) = h_1(l)\,\|\,h_2(r);$$

$$\hat{\pi}_3(l\|r) = \Big(l \otimes \psi(l \otimes r)\Big)\,\|\,\Big(r \otimes \mathcal{I}(\psi(l \otimes r))\Big).$$

The involution property of the whole construction can be derived from the well-known fact, that if M is an involution over V_n, then for any permutation $G \in V_n$, the resulting transformation $F = G^{-1} \circ M \circ G$ is an involution over V_n.

Involutions

8-bit involutions having almost optimal cryptographic parameters



Using the previous construction we have performed a search based on random generation of 4-bit involutions h_1, h_2 and non-bijective 4-bit function ψ for finding almost optimal involutions without fixed points with the following parameters

- minimum algebraic degree equal to 7;
- graph algebraic immunity equal to 3, with 441 equations;
- δ-uniformity equal to 8;
- nonlinearity in range of 100 up to a value of 102.

Orthomorphisms.

Orthomorphisms
Their applications in Cryptography

A permutation $\Phi \in S(V_n)$ is called ortomorphism on $(V_n, \oplus)$, if the mapping $\widehat{\Phi} : V_n \to V_n$, defined as $\widehat{\Phi}(x) = x \oplus \Phi(x)$ is a permutation of $S(V_n)$.

Orthomorphisms
Their applications in Cryptography

A permutation $\Phi \in S(V_n)$ is called ortomorphism on $(V_n, \oplus)$, if the mapping $\widehat{\Phi} : V_n \to V_n$, defined as $\widehat{\Phi}(x) = x \oplus \Phi(x)$ is a permutation of $S(V_n)$.

In Cryptography, applications of orthomorphisms are found in:

1. the construction of authentication codes, mutually orthogonal Latin squares and Quasigroups;
2. the construction of block ciphers, stream ciphers and hash functions.

The set of all ortomorphisms of the additive group V_n is denoted by $\mathrm{Orth}(V_n)$. For any permutation $\Phi \in S(V_n)$ we define the following sets as follows

$$\mathcal{D}_\Phi = \left\{ \hat{\Phi}(x) \middle| x \in V_n \right\} = \left\{ \Phi(x) \oplus x \middle| x \in V_n \right\}, \widetilde{\mathcal{D}}_\Phi = V_n \setminus \mathcal{D}_\Phi. \tag{12}$$

Definition

For any $\Phi \in S(V_n)$ the deficit of Φ, denoted by d_Φ, is defined as

$$\mathrm{d}_\Phi = \#\widetilde{\mathcal{D}}_\Phi = 2^n - \#\mathcal{D}_\Phi. \tag{13}$$

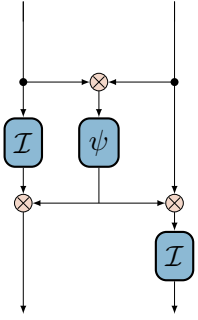
So we have that $\Phi \in \mathrm{Orth}(V_n)$ if and only if $\mathrm{d}_\Phi = 0$, i.e., when $\#\mathcal{D}_\Phi = 2^n$.

Proposition 7

For any $\Phi \in \mathrm{Orth}(V_n)$ the following relations holds $\mathcal{W}_\Phi(a, b) = \mathcal{W}_{\hat{\Phi}}(a \oplus b, b)$ and $\Delta_\Phi(a, b) = \Delta_{\hat{\Phi}}(a, a \oplus b)$.

Orthomorphisms

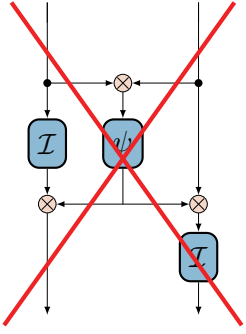
The scheme of $\hat{\pi}$ can not generate orthomorphisms



We can not construct orthomorphisms over V_n using the construction of $\hat{\pi}_\psi$.

Orthomorphisms

The scheme of $\hat{\pi}$ can not generate orthomorphisms



We can not construct orthomorphisms over V_n using the construction of $\hat{\pi}_\psi$.

Proposition 8

Let $\psi : V_k \to V_k$ be an arbitrary non-bijective function which has no preimage for 0. Then, for the permutation $\hat{\pi}_\psi : V_{2k} \to V_{2k}$, defined as

$$\hat{\pi}_\psi(l\|r) = (\mathcal{I}(l) \otimes \psi(l \otimes r))\|\mathcal{I}(r \otimes \psi(l \otimes r)),$$

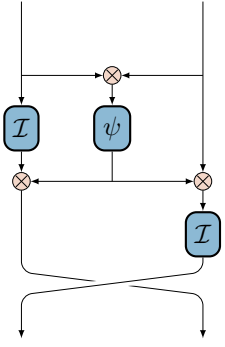
the following inequality holds

$$\#\mathcal{D}_{\hat{\pi}_\psi} < 2^{2k}$$

Orthomorphisms

Modifying the scheme of $\hat{\pi}$ is possible to construct orthomorphisms

In order to construct orthomorphisms over V_{2k} it is therefore advisable to consider the following class of permutations $\dot{\pi}_\psi(l\|r) = \mathcal{I}(r \otimes \psi(l \otimes r))\|(\mathcal{I}(l) \otimes \psi(l \otimes r))$.



Proposition 9

If the lookup-tables of non-bijective k-bit functions

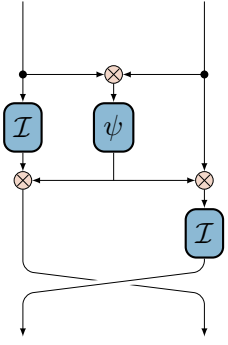
$$\psi = \begin{pmatrix} \dots & i & \dots \\ \dots & \psi(i) & \dots \end{pmatrix}, \hat{\psi} = \begin{pmatrix} \dots & i & \dots \\ \dots & \hat{\psi}(i) & \dots \end{pmatrix}$$

differs from each other exactly in one output value, then for permutations $\dot{\pi}_\psi, \dot{\pi}_{\hat{\psi}}$ the following relations holds:

1. $\mathrm{d}_{\dot{\pi}_\psi} - 2 \cdot (2^k - 1) \leq \mathrm{d}_{\dot{\pi}_{\hat{\psi}}} \leq \mathrm{d}_{\dot{\pi}_\psi} + 2 \cdot (2^k - 1)$, when $i = 0$;
2. $\mathrm{d}_{\dot{\pi}_\psi} - 2^k + 1 \leq \mathrm{d}_{\dot{\pi}_{\hat{\psi}}} \leq \mathrm{d}_{\dot{\pi}_\psi} + 2^k - 1$, when $i \neq 0$.

Orthomorphisms

The scheme of $\dot{\pi}$ can be used to construct orthomorphisms



Proposition 9 can be used for searching highly-nonlinear orthomorphisms.

We have found 8-bit orthomorphisms having the following parameters

- minimum algebraic degree equal to 7;
- graph algebraic immunity equal to 3 (with 441 equations);
- δ-uniformity equal to 8;
- nonlinearity in range of 100 up to a value of 104.

Resilience of $\hat{\pi}$ and $\hat{\pi}^{(invol)}$ against side-channel attacks in terms of its masking complexity.

Masking complexity

Due to the compact representations of $\hat{\pi}$ it is possible combine ours 8-bit S-Boxes with the classical masking countermeasure against side-channel attacks (SCAs) in terms of its masking complexity .

Masking complexity

Definition

The univariate polynomial representation of an n-bit S-Box Φ over $\mathrm{GF}(2^n)$, is defined in a unique fashion as

$$\Phi(X) = \sum_{i=0}^{2^n-1} \nu_i X^i, \nu_i \in \mathrm{GF}(2^n), \tag{14}$$

where coefficients $\nu_i, i = 0, \ldots, 2^n - 1$ can be obtained from Φ by applying Lagrange's Interpolation theorem.

Masking complexity

The polynomial representation of Φ defined by $\Phi(X) = \sum_{i=0}^{2^n-1} \nu_i X^i, \nu_i \in \mathrm{GF}(2^n)$ is based on four kinds of operations[6] over $\mathrm{GF}(2^n)$:

1. additions;
2. multiplications by constants;
3. squares;
4. nonlinear multiplications (i.e. multiplications of two different variables).

Definition

The masking complexity of any n-bit S-Box Φ, denoted by $\mathcal{MC}(\Phi)$, is the minimal number of nonlinear multiplications required to evaluate its polynomial representation over $\mathrm{GF}(2^n)$.

[6] *Higher-order masking schemes for s-boxes* by Carlet C., Goubin L., Prouff E., Quisquater M., and Rivain M. FSE,volume 7549 of LNCS, pages 366-384. Springer, 2012.

Masking complexity

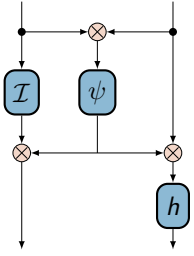
Denoting by $\mathcal{M}_k^n$ as the class of exponents α such that X^α has a masking complexity equal to k we summarizes in next Table the results for the cyclotomic classes $C_\alpha = \{\alpha \cdot 2^j \mod (15) \,|\, j = 0, 1, 2, 3.\}$ in $\mathcal{M}_k^4$.

k	Cyclotomic classes in $\mathcal{M}_k^4$
0	$C_0 = \{0\}, C_1 = \{1, 2, 4, 8\}$
1	$C_3 = \{3, 6, 12, 9\}, C_5 = \{5, 10\}$
2	$C_7 = \{7, 11, 13, 14\}$

Masking complexity

The number of field multiplications for any 4-bit permutation and any 4-bit non-bijective function is lower bounded by 0 and upper bounded by 3,4 respectively.[7]

k	Cyclotomic classes in $\mathcal{M}_k^4$
2	$C_7 = \{7, 11, 13, 14\}$



Masking complexity of $\hat{\pi}$

So, for 8-bit S-Boxes produced by the scheme of $\hat{\pi}$ we obtain the following bounds:

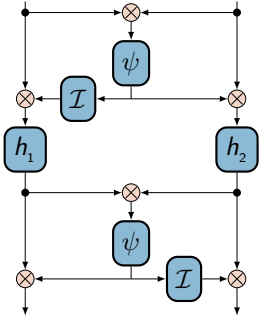
$$5 \leq \#\text{ nonl. mult. of } \hat{\pi} \leq 12. \qquad (15)$$

[7] *Higher-order masking schemes for s-boxes* by Carlet C., Goubin L., Prouff E., Quisquater M., and Rivain M. FSE,volume 7549 of LNCS, pages 366-384. Springer, 2012.

Masking complexity

The number of field multiplications for any 4-bit permutation and any 4-bit non-bijective function is lower bounded by 0 and upper bounded by 3,4 respectively.[8]

k	Cyclotomic classes in $\mathcal{M}_k^4$
2	$C_7 = \{7, 11, 13, 14\}$



Masking complexity of $\hat{\pi}^{(invol)}$

So, for 8-bit involutions produced by the scheme of $\hat{\pi}^{(invol)}$ we obtain the following bounds:

$$10 \leq \#\text{ nonl. mult. of } \hat{\pi}^{(invol)} \leq 24. \qquad (16)$$

[8] *Higher-order masking schemes for s-boxes* by Carlet C., Goubin L., Prouff E., Quisquater M., and Rivain M. FSE,volume 7549 of LNCS, pages 366-384. Springer, 2012.

Masking complexity

Comparison of 8-bit S-Boxes w.r.t. # nonl. multiplications

S-Box class	# nonl. multiplications
AES's S-Box	4 ($GF(2^8)$)
AES's S-Box	5 ($GF(2^4)$)
Clefia S-Box	10 ($GF(2^8)$)
Iceberg S-Box	18 ($GF(2^4)$)
Khazad S-Box	18 ($GF(2^4)$)
Picaro S-Box	4 ($GF(2^4)$)
Zorro S-Box	4 ($GF(2^4)$)
S-Boxes based on $\hat{\pi}$ scheme [this work]	$5 \leq$ # nonl. multiplications ≤ 12 ($GF(2^4)$)
S-Boxes based on $\hat{\pi}^{(invol)}$ scheme [this work]	$10 \leq$ # nonl. multiplications ≤ 24 ($GF(2^4)$)

S-Boxes based on $\hat{\pi}$ scheme exhibits better values of fields multiplications than S-Boxes of Clefia, Iceberg and Khazad respectively, having at the same time stronger cryptographic properties but at the cost of a worse number of nonlinear multiplications compared with the AES, Picaro and Zorro S-Boxes.

Masking complexity

Comparison of 8-bit S-Boxes w.r.t. # nonl. multiplications

S-Box class	# nonl. multiplications
AES's S-Box	4 ($GF(2^8)$)
AES's S-Box	5 ($GF(2^4)$)
Clefia S-Box	10 ($GF(2^8)$)
Iceberg S-Box	18 ($GF(2^4)$)
Khazad S-Box	18 ($GF(2^4)$)
Picaro S-Box	4 ($GF(2^4)$)
Zorro S-Box	4 ($GF(2^4)$)
S-Boxes based on $\hat{\pi}$ scheme [this work]	$5 \leq$ # nonl. multiplications ≤ 12 ($GF(2^4)$)
S-Boxes based on $\hat{\pi}^{(invol)}$ scheme [this work]	$10 \leq$ # nonl. multiplications ≤ 24 ($GF(2^4)$)

As we an see S-Boxes based on $\hat{\pi}^{(invol)}$ scheme have more finite field multiplications which have an impact on the masking complexity of these kind of permutations despite the fact that these involutions have good values of its basic cryptographic parameters.

Conclusion.

Conclusion

- We have presented some new schemes based on the well-known Lai-Massey structure for constructing S-Boxes of dimension $n = 2k, k \geq 2$;
- The main cores of our constructions are: the inversion in GF(2^k), an arbitrary k-bit non-bijective function (which has no preimage for 0) and k-bit permutations.
  - Combining these components with the finite field multiplication, we provide ordinary permutations, involutions and orthomorphisms with high values of its basic cryptographic parameters.

Conclusion

- Despite the fact that the scheme of $\hat{\pi}$ leads to the predominant appearance of S-Boxes with high cryptographic parameters it has a weakness: the existence of some structures which are invariant with respect to the action of this nonlinear bijective transformation.
  - It is necessary to compose $\hat{\pi}$ with appropriate linear (resp. affine) layers $\mathcal{L}_1$ and $\mathcal{L}_2$ from $\mathrm{GL}_{2k}(\mathrm{GF}(2))$ to circumvent the existence of such subspaces.

Conclusion

- We have study the resilience of the proposed constructions against side-channel attacks in terms of its masking complexity;
- The main advantage of our 8-bit permutations is that they can be constructed using smaller 4-bit components which could be useful for the implementation of the S-Box in hardware or using a bit-sliced approach.

THE END

THANKS FOR YOUR ATTENTION

Questions?