A Method For Generation Of High-Nonlinear S-Boxes Based On Gradient Descent

Oleksandr Kazymyrov†, Valentyna Kazymyrova†, Roman Oliynykov‡

† Selmer Center, Department of Informatics,
University of Bergen, Norway
{Oleksandr.Kazymyrov,Valentyna Kazymyrova}@ii.uib.no

‡ Department of Information Technologies Security,
Kharkov National University of Radioelectronics, Ukraine
ROliynikov@gmail.com

CTCrypt 2013

Agenda

What is a substitution?

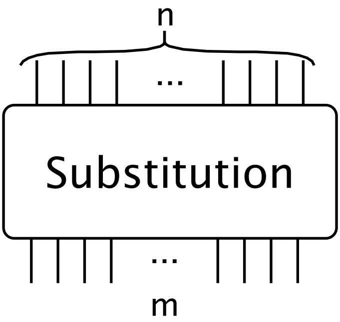

Figure : A Substitution Box

What is a substitution?

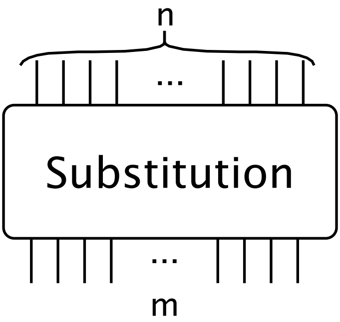

Figure : A Substitution Box

Possible variants

- $n > m$
- $n < m$
- $n = m$

What is a substitution?

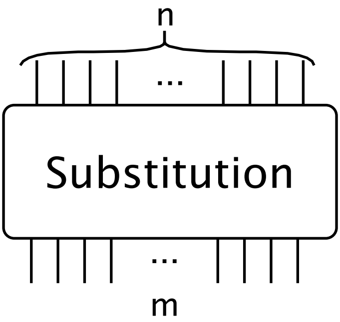

Figure : A Substitution Box

Possible variants

- $n > m$
- $n < m$
- $n = m$
  - $\#img(\text{S-box}) = 2^n$

What is a substitution?

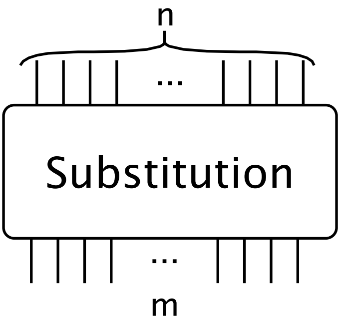

Figure : A Substitution Box

Possible variants

- $n > m$
- $n < m$
- $n = m$
  - $\#img(\text{S-box}) = 2^n$

Representation

- lookup tables
- vectorial Boolean functions
  - Boolean functions
- system of equations

Application of S-boxes

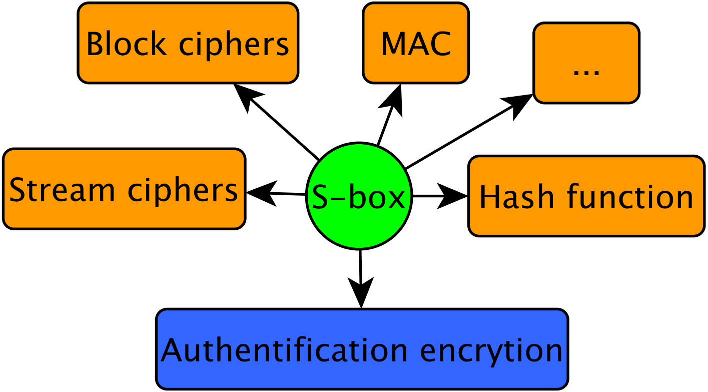

Figure : Usage of S-boxes

Agenda

Properties of substitutions (1/5)

Definition

Let n and m be two positive integers. Any function $F : \mathbb{F}_2^n \mapsto \mathbb{F}_2^m$ is called an (n, m)-function or vectorial Boolean function [1].

δ-uniform

Arbitrary F is differentially δ-uniform if equation

$$b = F(x) + F(x + a),\ \forall a \in \mathbb{F}_2^n, \forall b \in \mathbb{F}_2^m, a \neq 0$$

has at most δ solutions.

Properties of substitutions (2/5)

Walsh transform

The Walsh transform of an (n, m)-function F at $(u, v) \in \mathbb{F}_2^n \times \mathbb{F}_2^m \backslash \{0\}$

$$\lambda(u, v) = \sum_{x \in \mathbb{F}_2^n} (-1)^{v \cdot F(x) \oplus u \cdot x}, \qquad (1)$$

where "·" denotes inner products in $\mathbb{F}_2^n$ and $\mathbb{F}_2^m$ respectively.

Nonlinearity

$$NL(F) = 2^{n-1} - \frac{1}{2} \max_{v \in \mathbb{F}_2^{m*};\, u \in \mathbb{F}_2^n} |\lambda(u, v)|$$

Properties of substitutions (3/5)

Balancedness

An (n, m)-function F is called balanced if it takes every value of F_2^m the same number of times (2^{n-m}).

Absence of Fixed Points

A substitution must not have fixed point, i.e.

$$F(a) \neq a, \quad \forall a \in \mathbb{F}_2^n .$$

Properties of substitutions (4/5)

The algebraic normal form (ANF) of any (n, m)-function F always exists and is unique:

$$F(x) = \sum_{I \subseteq \{1,\dots,n\}} a_I \left(\prod_{i \in I} x_i \right) = \sum_{I \subseteq \{1,\dots,n\}} a_I x^I, \; a_I \in \mathbb{F}_2^m$$

The algebraic degree of F

$$deg(F) = \max\{|I| \mid a_I \neq 0\}$$

Minimum degree

The minimum algebraic degree of all the component functions of F is called the minimum degree.

Properties of substitutions (5/5)

Arbitrary substitution can be represented as the system of equations

$$\begin{cases} g_1(x_1, x_2, \ldots, x_n, y_1, y_2, \ldots, y_m) = 0; \\ g_2(x_1, x_2, \ldots, x_n, y_1, y_2, \ldots, y_m) = 0; \\ \ldots \\ g_r(x_1, x_2, \ldots, x_n, y_1, y_2, \ldots, y_m) = 0. \end{cases} \quad (2)$$

Properties of substitutions (5/5)

Arbitrary substitution can be represented as the system of equations

$$\begin{cases} g_1(x_1, x_2, \ldots, x_n, y_1, y_2, \ldots, y_m) = 0; \\ g_2(x_1, x_2, \ldots, x_n, y_1, y_2, \ldots, y_m) = 0; \\ \ldots \\ g_r(x_1, x_2, \ldots, x_n, y_1, y_2, \ldots, y_m) = 0. \end{cases} \quad (2)$$

Algebraic immunity

The algebraic immunity $AI(F)$ of any (n, m)-function F is the minimum algebraic degree of all functions in (2).

Agenda

List of properties

Definition

An S-box is a mapping of an n-bit input message to an m-bit output message.

- Minimum degree
- Balancedness
- Nonlinearity
- Correlation immunity
- δ-uniformity
- Cyclic structure
- Algebraic immunity
- Absolute indicator
- Absence of fixed points
- Propagation criterion
- Sum-of-squares indicator
- ...

Necessary properties for stream ciphers (FG)

Definition

An S-box is a mapping of an n-bit input message to an m-bit output message.

- Minimum degree
- Balancedness
- Nonlinearity
- Correlation immunity
- δ-uniformity
- Cyclic structure
- Algebraic immunity
- Absolute indicator
- Absence of fixed points
- Propagation criterion
- Sum-of-squares indicator
- ...

Necessary properties for block ciphers

Definition

An S-box is a mapping of an n-bit input message to an m-bit output message.

- Minimum degree
- Balancedness
- Nonlinearity
- Correlation immunity
- δ-uniformity
- Cyclic structure
- Algebraic immunity
- Absolute indicator
- Absence of fixed points
- Propagation criterion
- Sum-of-squares indicator
- ...

Perfect nonlinear substitutions

Definition

An S-box is a mapping of an n-bit input message to an m-bit output message.

- Minimum degree
- Balancedness
- Nonlinearity
- Correlation immunity
- δ-uniformity
- Cyclic structure
- Algebraic immunity
- Absolute indicator
- Absence of fixed points
- Propagation criterion
- Sum-of-squares indicator
- ...

Optimal substitutions

Definition

Substitutions satisfying only mandatory criteria essential for a particular cryptographyc algorithm are called optimal.

Optimal substitutions

Definition

Substitutions satisfying only mandatory criteria essential for a particular cryptographyc algorithm are called optimal.

An optimal substitution for a block cipher

- permutation
- maximum value of minimum degree
- without fixed points (cycles of length 1)
- maximum algebraic immunity/minimum number of equations

Optimal substitutions

Definition

Substitutions satisfying only mandatory criteria essential for a particular cryptographyc algorithm are called optimal.

An optimal substitution for a block cipher

- permutation
- maximum value of minimum degree
- without fixed points (cycles of length 1)
- maximum algebraic immunity/minimum number of equations
    - minimum δ-uniformity
    - maximum nonlinearity

Optimal substitutions

Definition

Substitutions satisfying only mandatory criteria essential for a particular cryptographyc algorithm are called optimal.

An optimal permutation for a block cipher

- ~~permutation~~
- maximum value of minimum degree
- ~~without fixed points (cycles of length 1)~~
- maximum algebraic immunity/~~minimum number of equations~~
  - minimum δ-uniformity
  - maximum nonlinearity

Example of criteria

An optimal permutation without fixed points for $n = m = 8$ must have

- minimum degree 7
- algebraic immunity 3 (441 equations)
- $\delta \leq 8$
- $NL \geq 100$

Agenda

Random method

Algorithm

Generate random permutation and check on optimality.

Random method

Algorithm

Generate random permutation and check on optimality.

Practical result

After 12 hours of cluster operation (4096 cores) it was found 27 optimal permutations (with $NL = 100$ and $AI = 3$), four of which were CCZ-nonequivalent.

Random method

Algorithm

Generate random permutation and check on optimality.

Practical result

After 12 hours of cluster operation (4096 cores) it was found 27 optimal permutations (with $NL = 100$ and $AI = 3$), four of which were CCZ-nonequivalent.

Computational restrictions

After 48 hours of cluster operation (22 years on 1 core) no substitutions with $NL = 102$ were found.

Problem

Are such substitutions the best?

Problem

Are such substitutions the best?

Problem

Are such substitutions the best?

- Counterexample was given in STB 34.101.31-2011 [2]. The substitution has $NL = 102$ and $AI = 3$.

Problem

Are such substitutions the best?

- Counterexample was given in STB 34.101.31-2011 [2]. The substitution has $NL = 102$ and $AI = 3$.
- Another example of optimal substitutions generation was given in "A New Method for Generating High Non-linearity S-Boxes" (2010) [3].

Proposed method

Definition

Suppose F is a highly nonlinear vectorial Boolean function with low δ-uniformity.

Algorithm

1. Generate a substitution S based on F.
2. Swap NP values of S randomly and set it to S_t.
3. Test substitution for all criteria depending on their computational complexity. If S_t satisfies all of them except the cyclic properties then go to 4. Otherwise repeat step 2.
4. Return S_t.

Proposed method

Definition

Suppose F is a highly nonlinear vectorial Boolean function with low δ-uniformity.

Algorithm

1. Generate a substitution S based on F.
2. Swap NP values of S randomly and set it to S_t.
3. Test substitution for all criteria depending on their computational complexity. If S_t satisfies all of them except the cyclic properties then go to 4. Otherwise repeat step 2.
4. Return S_t.

Suppose $F = x^{-1}$ for $n = m = 8$ and $NP = 26$.

Performance of the proposed method

Previous method [3]

"With probability 90% the program search one 104 8x8 S-Box up to 44 hours on personal computer (Intel Core 2 Duo E8500/4096 MB /MS Windows 7 Ultimate 64 bit)".

Performance of the proposed method

Previous method [3]

"With probability 90% the program search one 104 8x8 S-Box up to 44 hours on personal computer (Intel Core 2 Duo E8500/4096 MB /MS Windows 7 Ultimate 64 bit)".

Computational result of proposed method

During 1 hour of cluster operation 1152 optimal permutations (except cyclic properties) with $NL = 104$ and $AI = 3$ were generated.

Performance of the proposed method

Previous method [3]

"With probability 90% the program search one 104 8x8 S-Box up to 44 hours on personal computer (Intel Core 2 Duo E8500/4096 MB /MS Windows 7 Ultimate 64 bit)".

Computational result of proposed method

During 1 hour of cluster operation 1152 optimal permutations (except cyclic properties) with $NL = 104$ and $AI = 3$ were generated.

Performance comparison

If the swapping function exchanges values randomly then time needed to generate 1 optimal substitution on a PC with one core on average equals 3.5 hours.

Comparison with known substitutions

Properties	AES	GOST R 34.11-2012 [4]	STB 34.101.31-2011	Kalyna S0	Proposed S-box
δ-uniformity	4	8	8	8	8
Nonlinearity	112	100	102	96	104
Absolute Indicator	32	96	80	88	80
SSI	133120	258688	232960	244480	194944
Minimum Degree	7	7	6	7	7
Algebraic Immunity	2(39)	3(441)	3(441)	3(441)	3(441)

Table : Substitutions comparison

Changed criteria for $n = m = 8$

An optimal permutation without fixed points must have

- minimum degree 7
- algebraic immunity 3
- $\delta \leq 8$
- $NL \geq 104$

Outline

1. Introduction
2. Preliminaries
3. Optimal substitutions
4. A new method to generate optimal substitutions
5. Conclusions & Open problems

Conclusions

- The analysis shows that both theoretical and random methods fail in case of optimal substitutions.

Conclusions

- The analysis shows that both theoretical and random methods fail in case of optimal substitutions.
- The proposed method has the highest performance among the known methods available in public literature.

Conclusions

- The analysis shows that both theoretical and random methods fail in case of optimal substitutions.
- The proposed method has the highest performance among the known methods available in public literature.
- Application of the proposed method allows to generate optimal permutations, the use of which in perspective symmetric cryptoprimitives provides a high level of resistance with respect to differential, linear and algebraic cryptanalysis.

Open problems

Open problem 1

- How to predict the number of swapping points?
  - Predict properties of the substitution after NP exchanges.
- Faster algorithm.

Open problems

Open problem 1

- How to predict the number of swapping points?
  - Predict properties of the substitution after NP exchanges.
- Faster algorithm.

Open problems

Open problem 1

- How to predict the number of swapping points?
  - Predict properties of the substitution after NP exchanges.
- Faster algorithm.

Open problems

Open problem 1

- How to predict the number of swapping points?
  - Predict properties of the substitution after NP exchanges.
- Faster algorithm.

Open problems

Open problem 1

- How to predict the number of swapping points?
  - Predict properties of the substitution after NP exchanges.
- Faster algorithm.

Open problem 2

Find the upper bound of nonlinearity for optimal $F : \mathbb{F}_2^n \mapsto \mathbb{F}_2^n$

- Prove/disprove that $NL(F) = 104$ is the maximum value for 8×8 substitutions with optimal properties.
- Find the upper bound of $NL(F)$ with maximum value of $AI(F)$.

References

- Crama Y., Hammer P.L. Boolean Models and Methods in Mathematics Computer Science, and Engineering. Encyclopedia of Mathematics and its Applications // Cambridge University Press. — 2010.
- Information Technology. Information Security. Cryptographic algorithms of encryption and data integrity. // STB 34.101.31-2011.
- Tesař P. A New Method for Generating High Non-linearity S-Boxes // Radioengineering. — 2010. V. 19, NO. 1. — P. 23-26.
- Information technology. Cryptographic Data Security. Hash-functions. // GOST R 34.10-2012.