Open Problems in the Generation Substitution Field

Oleksandr Kazymyrov

Selmer Center, Department of Informatics,
University of Bergen, Norway
Oleksandr.Kazymyrov@uib.no

IceBreak 2013

Application of S-boxes

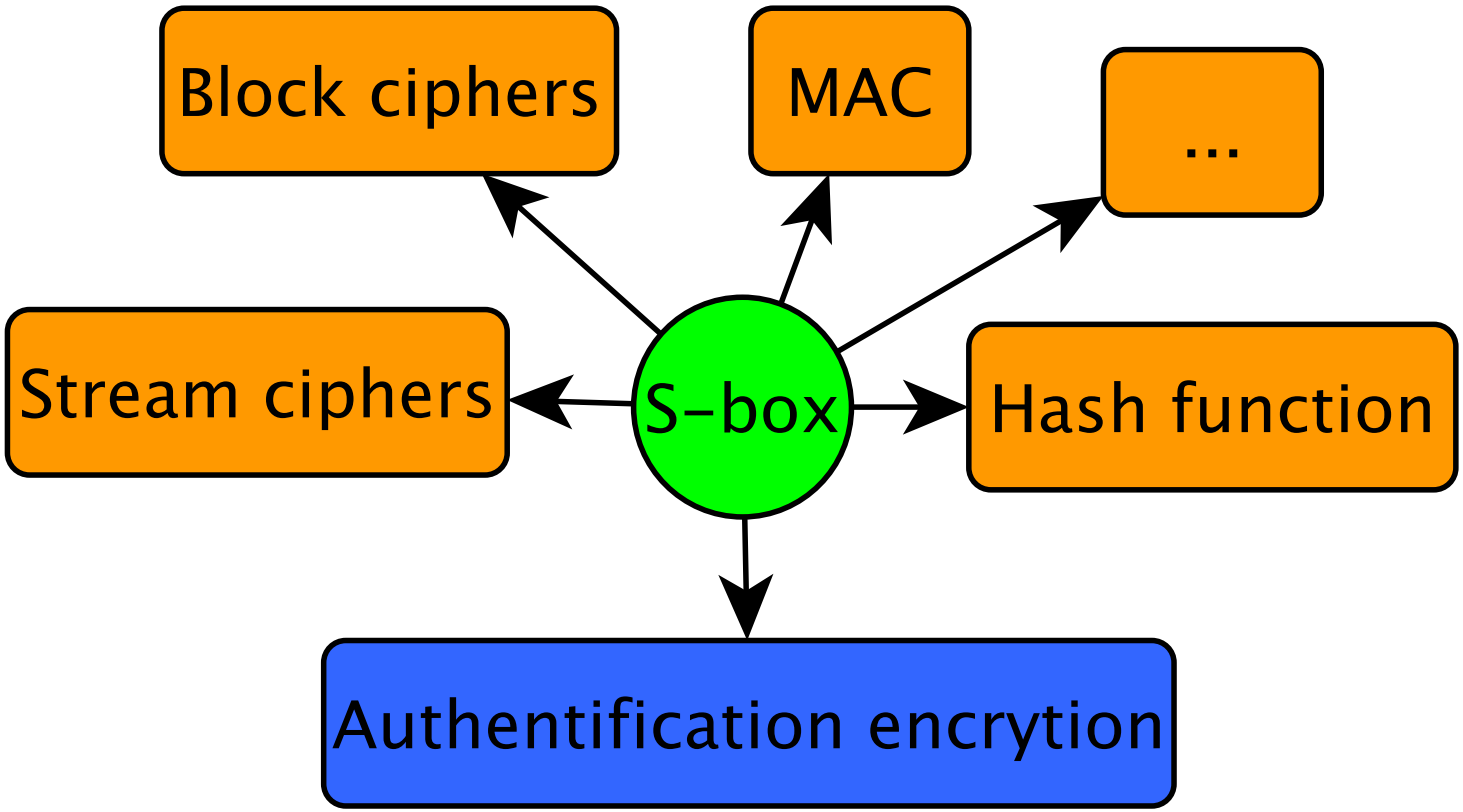

Figure : A Substitution Box

Properties of substitutions

Arbitrary substitution can be represented as the system of equations

$$\begin{cases} g_1(x_1, x_2, \ldots, x_n, y_1, y_2, \ldots, y_m) = 0; \\ g_2(x_1, x_2, \ldots, x_n, y_1, y_2, \ldots, y_m) = 0; \\ \ldots \\ g_r(x_1, x_2, \ldots, x_n, y_1, y_2, \ldots, y_m) = 0. \end{cases} \tag{1}$$

Properties of substitutions

Arbitrary substitution can be represented as the system of equations

$$\begin{cases} g_1(x_1, x_2, \ldots, x_n, y_1, y_2, \ldots, y_m) = 0; \\ g_2(x_1, x_2, \ldots, x_n, y_1, y_2, \ldots, y_m) = 0; \\ \ldots \\ g_r(x_1, x_2, \ldots, x_n, y_1, y_2, \ldots, y_m) = 0. \end{cases} \quad (1)$$

Algebraic immunity

The algebraic immunity $AI(F)$ of any (n, m)-function F is the minimum algebraic degree of all functions in (1).

Properties of substitutions

Arbitrary substitution can be represented as the system of equations

$$\begin{cases} g_1(x_1, x_2, \ldots, x_n, y_1, y_2, \ldots, y_m) = 0; \\ g_2(x_1, x_2, \ldots, x_n, y_1, y_2, \ldots, y_m) = 0; \\ \ldots \\ g_r(x_1, x_2, \ldots, x_n, y_1, y_2, \ldots, y_m) = 0. \end{cases} \quad (1)$$

Algebraic immunity

The algebraic immunity $AI(F)$ of any (n, m)-function F is the minimum algebraic degree of all functions in (1).

Minimum degree

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

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 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 for $n = m = 8$

An optimal permutation without fixed points must have

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

Random method

Algorithm

Generate random permutation and check for optimality.

Random method

Algorithm

Generate random permutation and check for optimality.

Practical result

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

Random method

Algorithm

Generate random permutation and check for optimality.

Practical result

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

Restrictions

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

Problem 1

Are such susbtitutions the best?

Problem 1

Are such susbtitutions the best?

No. Counterexample was given in STB 34.101.31-2011. The optimal substitution has $NL = 102$.

Problem 1

Are such susbtitutions the best?

No. Counterexample was given in STB 34.101.31-2011. The optimal substitution has $NL = 102$.

How to generate such substitutions?

Problem 1

Are such susbtitutions the best?

No. Counterexample was given in STB 34.101.31-2011. The optimal substitution has $NL = 102$.

How to generate such substitutions?

Answer: "A Method For Generation Of High-Nonlinear S-Boxes Based On Gradient Descent".

Problem 1

Are such susbtitutions the best?

No. Counterexample was given in STB 34.101.31-2011. The optimal substitution has $NL = 102$.

How to generate such substitutions?

Answer: "A Method For Generation Of High-Nonlinear S-Boxes Based On Gradient Descent" (2013) and "A New Method for Generating High Non-linearity S-Boxes" (2010).

Problem 1

Are such susbtitutions the best?

No. Counterexample was given in STB 34.101.31-2011. The optimal substitution has $NL = 102$.

How to generate such substitutions?

Answer: "A Method For Generation Of High-Nonlinear S-Boxes Based On Gradient Descent" (2013) and "A New Method for Generating High Non-linearity S-Boxes" (2010).

Improvements

Problem 1

Are such susbtitutions the best?

No. Counterexample was given in STB 34.101.31-2011. The optimal substitution has $NL = 102$.

How to generate such substitutions?

Answer: "A Method For Generation Of High-Nonlinear S-Boxes Based On Gradient Descent" (2013) and "A New Method for Generating High Non-linearity S-Boxes" (2010).

Improvements

1. How to predict the number of swapping points?

Problem 1

Are such susbtitutions the best?

No. Counterexample was given in STB 34.101.31-2011. The optimal substitution has $NL = 102$.

How to generate such substitutions?

Answer: "A Method For Generation Of High-Nonlinear S-Boxes Based On Gradient Descent" (2013) and "A New Method for Generating High Non-linearity S-Boxes" (2010).

Improvements

1. How to predict the number of swapping points?
2. Predict properties of the substitution after NP exchanges.

Problem 1

Are such susbtitutions the best?

No. Counterexample was given in STB 34.101.31-2011. The optimal substitution has $NL = 102$.

How to generate such substitutions?

Answer: "A Method For Generation Of High-Nonlinear S-Boxes Based On Gradient Descent" (2013) and "A New Method for Generating High Non-linearity S-Boxes" (2010).

Improvements

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

Comparison with known substitutions

Properties	AES	GOST	STB	Kalyna	New
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 : Comparison of Substitutions

Problems

Problem 2

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

Problems

Problem 2

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

- Prove that for $n = 8$ $NL(F) = 104$ is the maximum value with optimal properties.

Problems

Problem 2

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

- Prove that for $n = 8$ $NL(F) = 104$ is the maximum value with optimal properties.

Problem 3

Find a class of $F : \mathbb{F}_2^n \mapsto \mathbb{F}_2^{2n}$ with $\#img(F) = 2^n$, $\delta = 2$ and maximum nonlinearity.

Problems

Problem 2

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

- Prove that for $n = 8$ $NL(F) = 104$ is the maximum value with optimal properties.

Problem 3

Find a class of $F : \mathbb{F}_2^n \mapsto \mathbb{F}_2^{2n}$ with $\#img(F) = 2^n$, $\delta = 2$ and maximum nonlinearity.

- Give an example for $n = 8$ or $n = 10$.

Problems

Problem 2

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

- Prove that for $n = 8$ $NL(F) = 104$ is the maximum value with optimal properties.

Problem 3

Find a class of $F : \mathbb{F}_2^n \mapsto \mathbb{F}_2^{2n}$ with $\#img(F) = 2^n$, $\delta = 2$ and maximum nonlinearity.

- Give an example for $n = 8$ or $n = 10$.

Conjecture

APN pemutations over $\mathbb{F}_{2^n}$ $(n = 2k)$ exist iff they exist in a subfield.

GOST R 34.11-2012

Information

From the 1st of January 2013 the are two new standards GOST R 34.10-2012 and GOST R 34.11-2012.

- Description
- RFC Draft
- "Algebraic Aspects of the Russian Hash Standard GOST R 34.11-2012" (CTCrypt 2013)
- Implementation