Methods and Tools for Analysis of Symmetric Cryptographic Primitives

Oleksandr Kazymyrov

University of Bergen
Norway

1st of December, 2014

The main goal

Improve the resistance of modern iterated cryptographic primitives to advanced attacks through the development of methods and tools of cryptanalysis.

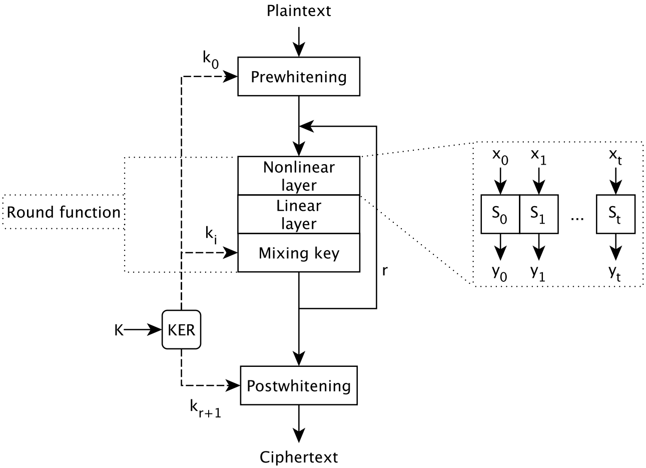
INTRODUCTION

National and international competitions

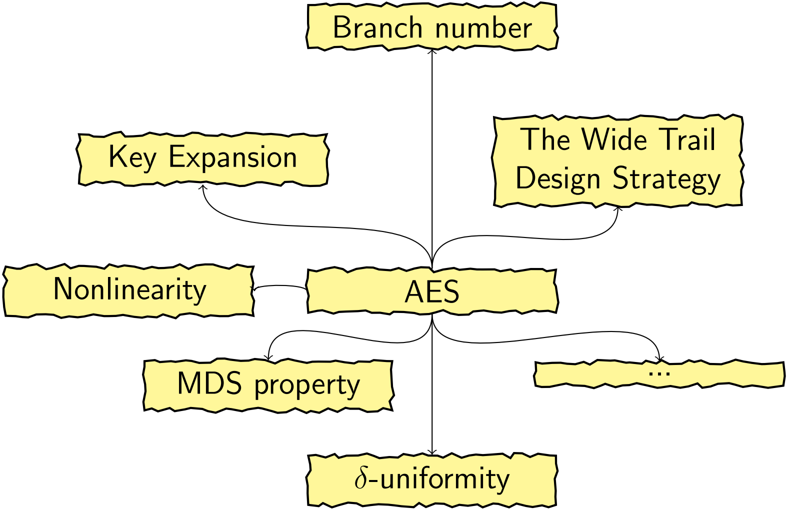
- Advanced Encryption Standard (1997-2001)
- New European Schemes for Signatures, Integrity and Encryption (2000-2003)
- eSTREAM (2004-2008)
- CRYPTREC (2000-2003-...)
- Ukrainian open competition to design a prototype of a block cipher for the new standard (2006-2009)
- SHA-3 (2007-2012)
- Russian closed competition to develop an advanced hash function and block cipher (2010-2012, 2013-...)
- Competition for Authenticated Encryption: Security, Applicability, and Robustness (2014-...)

An iterated block cipher

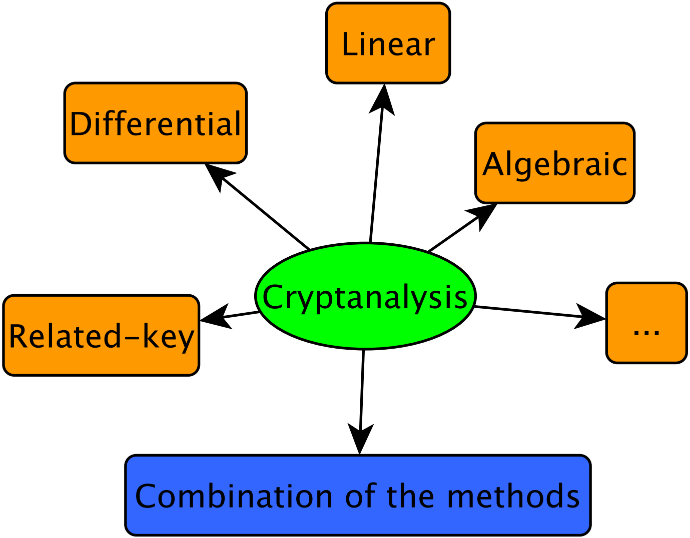
A block cipher encrypts a block of plaintext or message M into a block of ciphertext C using a secret key K.



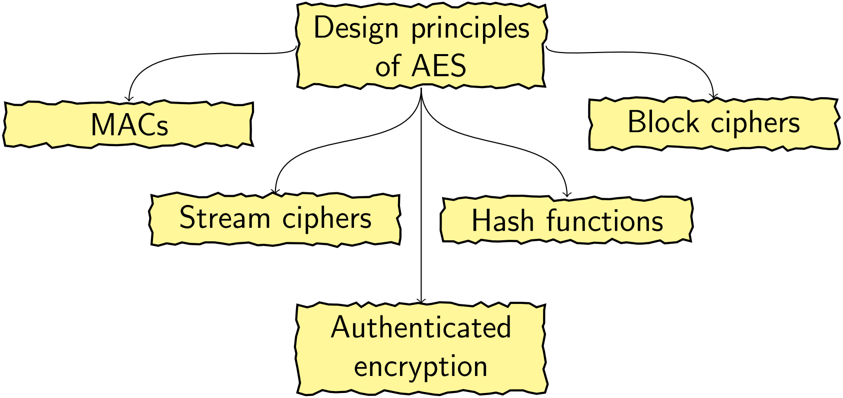
New design principles



Methods of cryptanalysis



Next generation of cryptoprimitives



Substitutions

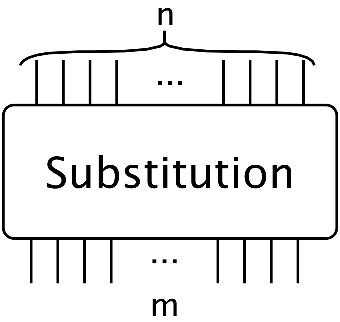


Figure: A substitution box

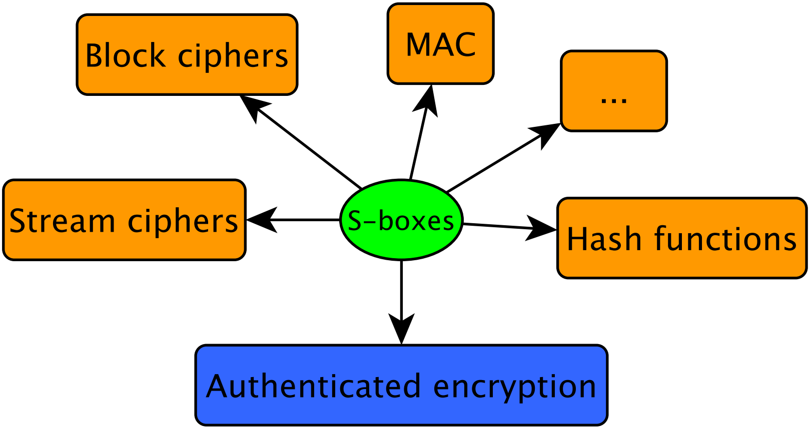
Possible variants

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

Representations

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

Application of substitutions



Properties of substitutions

Definition

Substitution boxes (S-boxes) map an n-bit input message to an m-bit output message.

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

EA-equivalence

- Two functions F and G are called EA-equivalent if

$$F(x) = A_1 \circ G \circ A_2(x) + L_3(x)$$

  for some affine permutations $A_1(x) = L_1(x) + c_1$, $A_2(x) = L_2(x) + c_2$ and a linear function $L_3(x)$.
- Functions F and G are restricted EA-equivalent if some functions of $\{L_1, L_2, L_3, c_1, c_2\}$ are in $\{0, x\}$
  - linear equivalent: $\{L_3, c_1, c_2\} = \{0, 0, 0\}$
  - affine equivalent: $L_3 = 0$

EA-equivalence

For $F, G : \mathbb{F}_2^n \mapsto \mathbb{F}_2^m$ another form of representation of EA-equivalence is a matrix form

$$F(x) = M_1 \cdot G(M_2 \cdot x \oplus V_2) \oplus M_3 \cdot x \oplus V_1$$

where elements of $\{M_1, M_2, M_3, V_1, V_2\}$ have dimensions $\{m \times m, n \times n, m \times n, m, n\}$.
Matrices M_i and vectors V_j are defined over $\mathbb{F}_2$ in the form

$$M = \begin{pmatrix} k_{0,0} & \cdots & k_{0,n-1} \\ k_{1,0} & \cdots & k_{1,n-1} \\ \vdots & \ddots & \vdots \\ k_{m-1,0} & \cdots & k_{m-1,n-1} \end{pmatrix}, \quad V = \begin{pmatrix} v_0 \\ v_1 \\ \dots \\ v_{m-1} \end{pmatrix}.$$

Scientific results

Verification of Restricted EA-equivalence for Vectorial Boolean Functions

Lilya Budaghyan Oleksandr Kazymyrov

Selmer Center, Department of Informatics,
University of Bergen, Norway

WAIFI'12
July 17, 2012

Open problems

1. Verification of EA-equivalence for arbitrary functions.
2. For the given functions F and G find affine permutations A_1, A_2 and a linear function L_3 such that

$$F(x) = A_1 \circ G \circ A_2(x) + L_3(x)$$

The complexity of exhaustive search for $F, G : \mathbb{F}_2^n \mapsto \mathbb{F}_2^n$ equals $\mathcal{O}\left(2^{3n^2+2n}\right)$. For $n = 6$ the complexity is already $\mathcal{O}(2^{120})$.

Summary

Restricted EA-equivalence	Complexity	$G(x)$
$F(x) = M_1 \cdot G(M_2 \cdot x)$	$\mathcal{O}(n^2 \cdot 2^n)$	P
$F(x) = M_1 \cdot G(M_2 \cdot x \oplus V_2) \oplus V_1$	$\mathcal{O}(n \cdot 2^{2n})$	P
$F(x) = M_1 \cdot G(x \oplus V_2) \oplus V_1$	$\mathcal{O}(2^{2n+1})$	†
$F(x) = M_1 \cdot G(x \oplus V_2) \oplus V_1$	$\mathcal{O}(n \cdot 2^{3n})$	A
$F(x) = G(M_2 \cdot x \oplus V_2) \oplus V_1$	$\mathcal{O}(n \cdot 2^n)$	P
$F(x) = G(x \oplus V_2) \oplus M_3 \cdot x \oplus V_1$	$\mathcal{O}(n \cdot 2^n)$	A
$F(x) = M_1 \cdot G(x \oplus V_2) \oplus M_3 \cdot x \oplus V_1$	$\mathcal{O}(2^{2n+1})$	‡
$F(x) = M_1 \cdot G(x \oplus V_2) \oplus M_3 \cdot x \oplus V_1$	$\mathcal{O}(n \cdot 2^{3n})$	A

† - G is under condition $\{2^i \mid 0 \leq i \leq m-1\} \subset \mathrm{img}(G')$ where $G'(x) = G(x) + G(0)$.

‡ - G is under condition $\{2^i \mid 0 \leq i \leq m-1\} \subset \mathrm{img}(G')$ where $G'(x) = G(x) \oplus L_G(x) \oplus G(0)$.

Algebraic Attacks Using Binary Decision Diagrams

Oleksandr Kazymyrov† Håvard Raddum‡

† Selmer Center, Department of Informatics,
University of Bergen, Norway

‡ Simula Research Laboratories, Norway

BalkanCryptSec'14
October 16, 2014

Binary decisions diagrams (BDDs)

$$f(x_1, x_2, x_3) = x_1 x_3 + x_1 + x_2 + x_3 + 1$$

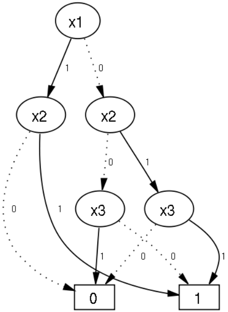
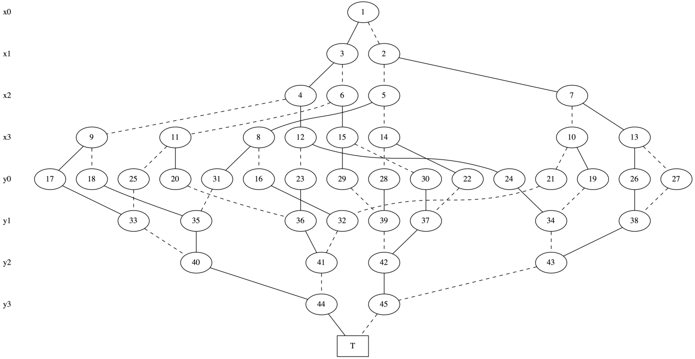


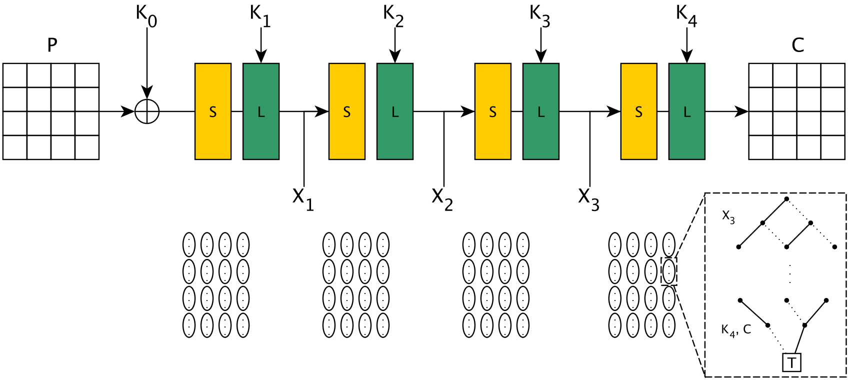
Figure: A binary decision diagram for the f function

S-box representation using BDDs

$$\text{S-box} = \{5, C, 8, F, 9, 7, 2, B, 6, A, 0, D, E, 4, 3, 1\}$$



Description of 4-round AES



Data Encryption Standard (DES)

- 2007: a system of equations for 6-round DES was solved in 68 seconds using MiniSat (Courtois & Bard)
  - But ... necessary to fix 20 bits of the key to correct values
- The BDD method allows to solve 6-round DES in the same time without guessing (8 chosen plaintexts)

# texts / rounds	1	2	3	4	5	6	7	8
4	$2^{22.715}$	$2^{14.506}$	$2^{10.606}$	$2^{10.257}$	$2^{9.805}$	$2^{10.070}$	$2^{10.203}$	$2^{10.381}$
5		$2^{22.110}$	$2^{16.455}$	$2^{13.526}$	$2^{13.995}$	$2^{14.212}$	$2^{14.410}$	$2^{14.704}$
6						$2^{24.929}$	$2^{22.779}$	$2^{20.571}$

Table: Complexities of breaking reduced DES

MiniAES

- There is no previous algebraic attacks for the 10-round version
- The best know "pure" algebraic attack is only for 2 rounds
- The BDD approach allows to break full version of MiniAES using only 1 chosen plaintext

Rounds	4	5	6	7	8	9	10
Complexity	$2^{22.404}$	$2^{23.051}$	$2^{23.440}$	$2^{24.154}$	$2^{24.217}$	$2^{24.862}$	$2^{24.961}$

Table: Complexities of breaking MiniAES

Finding EA-equivalence

#	n	Number of solutions	Seconds used to solve		
			BDD	GB	SAT
1	4	2	$2^{4.05}$	$2^{1.30}$	$2^{13.71}$
2	4	60	$2^{4.86}$	-	$2^{16.77}$
3	4	2	$2^{3.92}$	$2^{1.01}$	$2^{12.08}$
4	5	1	$2^{10.20}$	$2^{11.43}$	$> 2^{18}$ †
5	5	155	$2^{10.48}$	-	$> 2^{18}$ †

† not finished after 78 hours

Summary

- New approaches to the development of algebraic attacks
- The BDD approach allows to reduce complexity of the algebraic attack on DES by 2^{20}
- Firstly presented practical algebraic attack on 10-round MiniAES
- In some cases the BDD method is more universal and shows better results compared to known methods

State Space Cryptanalysis of the MICKEY Cipher

Tor Helleseth[†] Cees J.A. Jansen[‡]
Oleksandr Kazymyrov[†] Alexander Kholosha[†]

[†] Selmer Center, Department of Informatics,
University of Bergen, Norway

[‡] DeltaCrypto BV, The Netherlands

ITA'13
February 11, 2013

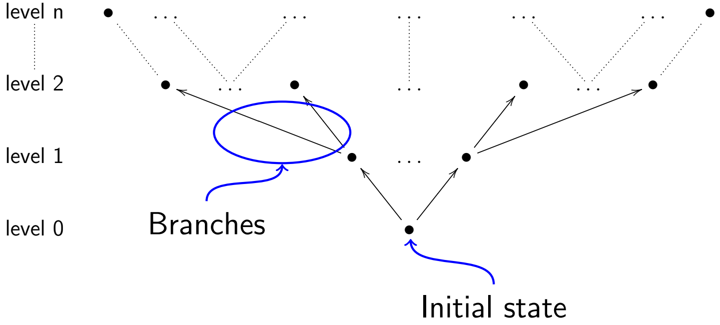
A general attack scenario on stream ciphers

- Recover states of registers (Berlekamp-Massey, algebraic attacks, Rønjom-Helleseth, etc.)
- Find the key based on the known state
  - **allows to estimate the number of possible states**

Note

In some stream ciphers the first step is sufficient to find the key

Tree of backward states



Degree probabilities

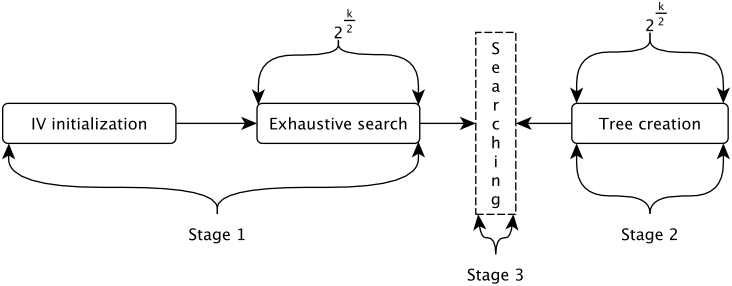
Degree	Key/IV load		Preclock mode		KG	
	80 v2	128 v2	80 v2	128 v2	80 v2	128 v2
0	0.2773	0.2186	0.3052	0.29	0.3041	0.3038
1	0.00001	0.1047	0.4345	0.4534	0.4323	0.4154
2	0.4331	0.3753	0.2523	0.2256	0.2558	0.2698
3	0.00002	0.1029	-	0.0289	-	-
4	0.28	0.1783	0.008	0.0021	0.0079	0.0111
6	0.00007	0.0203	-	-	-	-
8	0.0095	-	-	-	-	-

Determination of key bits based on a backward states tree

Level	Bit probability			
	MICKEY-80 v2		MICKEY-128 v2	
	1	0	1	0
1	0.5	0.5	1	0
2	0.5	0.5	0.5	0.5
3	0.5	0.5	0	1
4	0.5	0.5	0.5	0.5
5	0.4857	0.5143	0.5	0.5

$$\mathcal{O}(2^{126} + 2^{t}) \overset{t \ll 126}{\approx} \mathcal{O}(2^{126}) < \mathcal{O}(2^{128})$$

Meet-in-the-middle attack on MICKEY



$$\mathcal{O}(2^{\frac{k}{2}+2}) = \mathcal{O}_d(2^{\frac{k}{2}}) + \mathcal{O}_i(2^{\frac{k}{2}}) + \mathcal{O}_f(2^{\frac{k}{2}})$$

Identical key-streams for different key/IV pairs

Let z_i^h be i-th bit of a key-stream for h-th pair of $(K_h,\ IV_h)$. Suppose also that

$$K_1 = k_0, k_1, \ldots, k_{n-1}$$

Then it is possible to find such $(K_1,\ IV_1)$ and $(K_2,\ IV_2)$ for which the states of registers will differ by one clock and the key-streams have the property

$$z_i^2 = z_{i+1}^1$$

An example of key/IV with shifted key-streams

$$K_1 = \{d3, ec, f0, 84, 8a, 1d, b1, b7, 4a, dd\}$$

$$IV_1 = \{58, e5, 77, 0a, 9c, a2, 34, c7, cd, 5e\} \ (79 bits)$$

$$K_2 = \{a7, d9, e1, 09, 14, 3b, 63, 6e, 95, ba\}$$

$$IV_2 = \{58, e5, 77, 0a, 9c, a2, 34, c7, cd, 5f\} \ (80 bits)$$

$$Z_1 = \{0, B7, 61, 27, 92, C5, 85, 91, 51, 18, 2A, D6, 7C, 8C, C8, C7, 04\}$$

$$Z_2 = \{\quad B7, 61, 27, 92, C5, 85, 91, 51, 18, 2A, D6, 7C, 8C, C8, C7, 04, 1\}$$

Summary

- Proposed method allows to estimate degrees' probability at the design stage of MICKEY-like ciphers
- Stepping backwards in the state space of MICKEY is possible and feasible in all modes including key/IV load
- A minor change in the feedback function of the R register leads to dramatic changes in cycles
- Thus, it is possible to justify the choice of the encryption algorithm parameters.
- Several practical attack scenarios based on known states were proposed

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

‡ Department of Information Technologies Security,
Kharkov National University of Radioelectronics, Ukraine

CTCrypt'13
June 24, 2013

Optimal substitutions

Definition

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

An optimal permutation for a block cipher has

- the maximum value of minimum degree
- the maximum value of algebraic immunity
  - the minimal value of δ-uniformity
  - the maximal value of nonlinearity
  - without fixed points (cycles of length 1)

Example of criteria

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

- minimum degree 7
- algebraic immunity 3 (441 equations)
- $\delta \leq 8$
- $NL \geq 104$

Proposed method

Definition

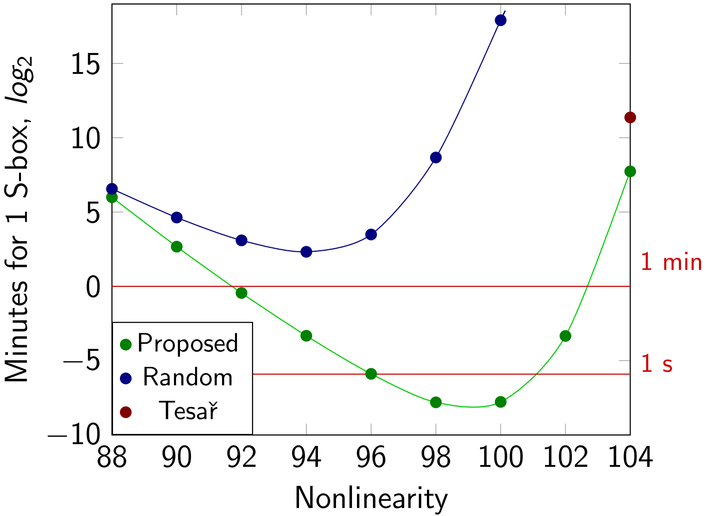
F is a highly nonlinear vectorial Boolean function with low δ-uniformity.

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

Algorithm

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

Performance of practical methods



Comparison with known substitutions

Properties	AES	GOST R 34.11-2012	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)

Summary

- 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 for perspective symmetric cryptoprimitives providing a high level of resistance to differential, linear and algebraic cryptanalysis

Comparison with known substitutions

Properties	AES	GOST R 34.11-2012	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)

A Sage Library for Analysis of Nonlinear Binary Mappings

Anna Maria Eilertsen Oleksandr Kazymyrov
Valentyna Kazymyrova Maksim Storetvedt

Selmer Center, Department of Informatics,
University of Bergen, Norway

CECC'14
May 21, 2014

Design principles

- Orientation on arbitrary n and m
- Code optimization for performance
- Implementation of widely used cryptographic indicators

Generation of substitutions

- Gold
- Kasami
- Welch
- Niho
- Inverse
- Dobbertin
- Dicson
- APN for $n = 6$
- Optimal permutation polynomials for $n = 4$
- Polynomial
- ...

Unification of the functions

generate_sbox calls different methods based on parameters method and T that define generation method and equivalence, respectively.

Additional functionality

- Extra functions
  - Resilience (balancedness and correlation immunity)
  - Maximum value of linear approximation table
  - APN property check (optimized)
- Convert linear functions to matrices and vice versa
- Apply EA- and CCZ-equivalence
- Generation of substitutions
  - Based on user-defined polynomial (trace supported)
  - Random substitution/permutation
  - With predefined properties
- Input/output
  - Set and get S-boxes as lookup tables
  - Get univariate representation/system of equations
  - Convert polynomial to/from internal representation

Performance

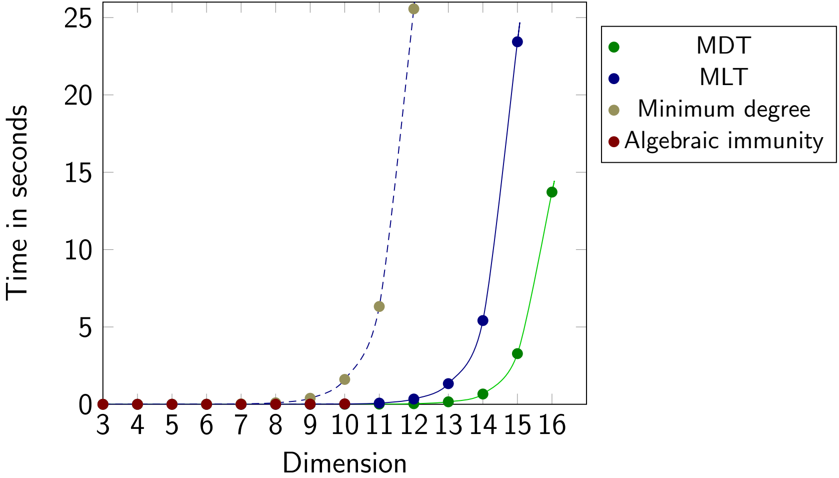


Figure: The relationship between dimension of random substitutions and time of calculation

Summary

- A high performance library to analyze and generate arbitrary binary nonlinear mappings
- Lots of cryptographic indicators and generation functions are included
- Functionality can be expanded quite easily
- Under development
- Source code: `https://github.com/okazymyrov/sbox`

Extended Criterion for Absence of Fixed Points

Oleksandr Kazymyrov Valentyna Kazymyrova

Selmer Center, Department of Informatics,
University of Bergen, Norway

CTCrypt'13
June 25, 2013

Properties of substitutions

Definition

Substitution boxes (S-boxes) map an n-bit input message to an m-bit output message.

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

Definitions and notations

Definition

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

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

Definition

Two ciphers E_i and E_j are isomorphic to each other if there exist invertible maps $\phi : x^i \mapsto x^j$, $\psi : y^i \mapsto y^j$ and $\chi : k^i \mapsto k^j$ such that $y^i = E_i(x^i, k^i)$ and $y^j = E_j(x^j, k^j)$ are equal for all x^i, k^i, x^j and k^j.

Basic functions of AES

The round function consists of four basic transformations

- AddRoundKey (σ_k)
- SubBytes (γ)
- ShiftRows (π)
- MixColumns (θ)

$$E_K(M) = \sigma_{k_{r+1}} \circ \pi \circ \gamma \circ \prod_{i=2}^{r} (\sigma_{k_i} \circ \theta \circ \pi \circ \gamma) \circ \sigma_{k_1}(M).$$

Both MixColumns and ShiftRows are linear transformations with respect to XOR

$$\theta(x + y) = \theta(y) + \theta(y);$$
$$\pi(x + y) = \pi(y) + \pi(y).$$

An isomorphic AES

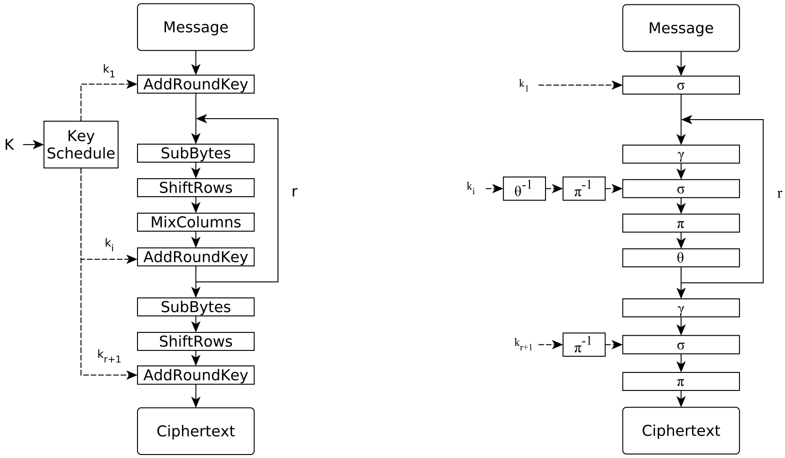


Figure : The encryption algorithm of AES

An isomorphic AES

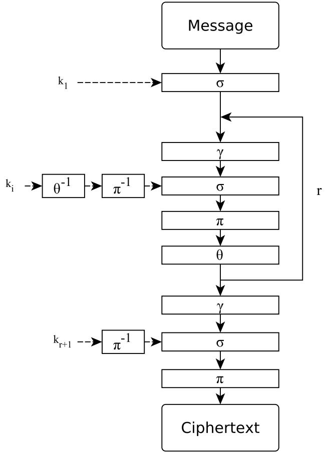
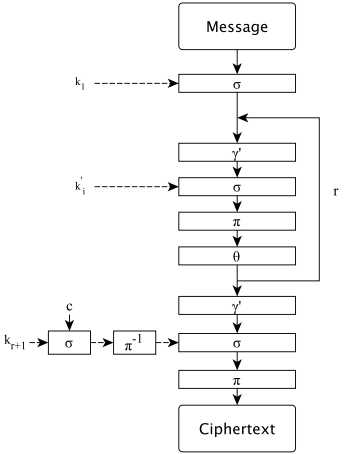


Figure : Isomorphic transformations

Comments on the isomorphic cipher

- The last π function does not increase security.
- Now the S-box has a fixed point ($x = 0$)

$$F(x) = L_1(x^{-1}) = M_1 \cdot x^{-1}$$



Summary

Isomorphic ciphers allow to

- Show redundancy of the last ShiftRow operation of AES
- Prove/disprove necessity of some characteristics of substitutions
- Introduce new criterion for several substitutions
- Show advantages of addition modulo 2^n in comparison with XOR operation

Conclusion

At least the absence of fixed points criterion has to be reviewed with other components of ciphers

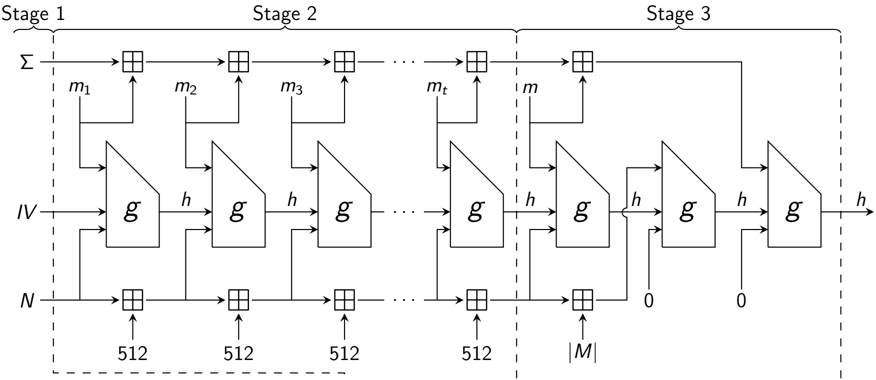
Algebraic Aspects of the Russian Hash Standard GOST R 34.11-2012

Oleksandr Kazymyrov Valentyna Kazymyrova

Selmer Center, Department of Informatics,
University of Bergen, Norway

CTCrypt'13
June 25, 2013

The hash function Stribog



$\Sigma = N = 0^{512}$

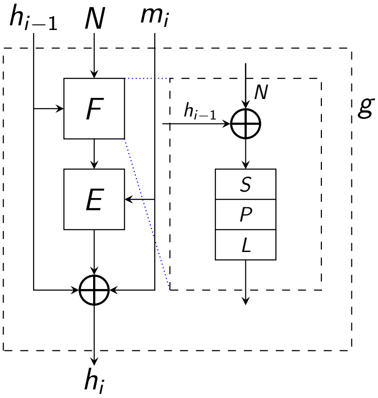
$$IV = \begin{cases} 0, & \text{Stribog-512} \\ (00000001)^{64}, & \text{Stribog-256} \end{cases}$$

$$t = \left\lfloor \frac{|M|}{512} \right\rfloor$$

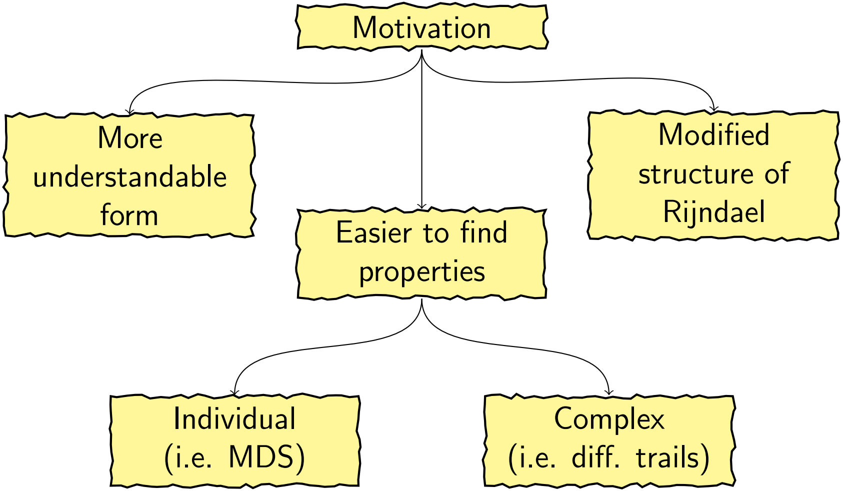
$m = 0^{512-|M|}||1||M$

$$H = \begin{cases} h, & \text{Stribog-512} \\ MSB_{256}(h), & \text{Stribog-256} \end{cases}$$

Construction of the compression function g



Motivation


Motivation
More understandable form
Easier to find properties
Modified structure of Rijndael
Individual (i.e. MDS)
Complex (i.e. diff. trails)

State representation

An alternative representation

- Reverse input bits
- AES-like transformations (states as in Grøstl)
- Reverse output bits

$$
\begin{array}{ccc}
B_0, B_1, \ldots, B_{63} & & B'_0, B'_1, \ldots, B'_{63} \\
\updownarrow & & \updownarrow \\
b_0, b_1, \ldots, b_{511} & \xleftrightarrow{\text{bit reversing}} & b_{511}, b_{510}, \ldots, b_0
\end{array}
$$

The Transposition and SubBytes operations

- Transposition is an invariant operation.
- The new S-box has the form $F(x) = D \circ G \circ D(x)$ for linearized polynomial $D : \mathbb{F}_{2^n} \mapsto \mathbb{F}_{2^n}$.

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	3F	FB	D7	E0	9F	E5	A8	04	97	07	AD	87	A0	B5	4C	9A
1	DF	EB	4F	0C	81	58	CF	D3	E8	3B	FD	B1	60	31	B6	8B
2	F3	7C	57	61	47	78	08	B4	C9	5E	10	32	C7	E4	FF	67
3	C4	3E	BF	11	D1	26	B9	7D	28	72	39	53	FE	96	C3	9C
4	BB	24	34	CD	A6	06	69	E6	0F	37	70	C1	40	62	98	2E
5	5F	6B	16	D6	3C	1C	1E	A4	8F	14	C8	55	B7	A5	63	F5
6	8C	C2	12	B8	F7	46	59	90	99	0D	6E	1F	F1	AA	51	2D
7	20	9D	73	E7	71	64	4D	36	FA	50	BA	A1	CB	A9	B0	C6
8	77	AF	2C	1A	18	E9	85	8E	EE	F0	0E	D8	21	A2	AE	65
9	23	9E	54	EC	38	1D	89	D9	6C	17	4E	CA	D0	C5	2A	66
A	76	15	13	35	3A	00	DE	D4	74	29	30	FC	56	7A	AC	2F
B	A3	44	5C	9B	80	F9	79	A7	B3	CC	ED	1B	2B	AB	BD	D2
C	88	95	8A	02	5A	CE	94	25	DB	7B	6A	92	75	49	BC	4B
D	5B	6F	45	27	42	41	F6	0B	DD	0A	E2	09	19	BE	01	43
E	68	93	D5	EF	84	22	E3	DA	5D	3D	48	7F	05	F4	7E	03
F	B2	C0	33	91	F2	82	8D	4A	83	52	E1	86	F8	DC	EA	6D

Table: The table representation of F

Representation of MixColumns

Let $L : \mathbb{F}_{2^n} \mapsto \mathbb{F}_{2^n}$ be a linear function of the form

$$L(x) = \sum_{i=0}^{n-1} \delta_i x^{2^i}, \quad \delta_i \in \mathbb{F}_{2^n}.$$

Proposition (Paper VII)

Any linear function $L : \mathbb{F}_{2^n} \mapsto \mathbb{F}_{2^m}$ can be converted to a matrix with the complexity $\mathcal{O}(n)$.

$$L(x) = \delta x, \quad \delta_i = 0, \text{ for } 1 \leq i \leq n-1.$$

Representation of MixColumns

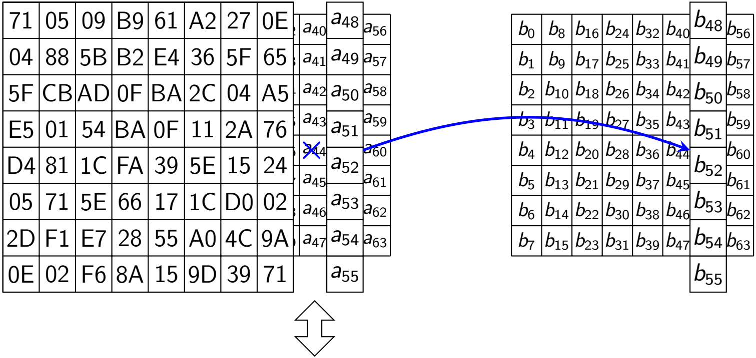
The main steps of the proposed algorithm to obtain an MDS matrix over $\mathbb{F}_{2^8}$ from a 64×64 bit matrix are

- for every irreducible polynomial (30)
  - convert each of 8×8 submatrices to an element of the field
  - check the MDS property of the resulting matrix

An additional transformation

It is necessary to transpose the matrix of Stribog before applying the algorithm.

MixColumns



71	05	09	B9	61	A2	27	0E
04	88	5B	B2	E4	36	5F	65
5F	CB	AD	0F	BA	2C	04	A5
E5	01	54	BA	0F	11	2A	76
D4	81	1C	FA	39	5E	15	24
05	71	5E	66	17	1C	D0	02
2D	F1	E7	28	55	A0	4C	9A
0E	02	F6	8A	15	9D	39	71

Multiplying a vector by the constant 8×8 matrix G over $\mathbb{F}_{2^8}$ with the primitive polynomial $f(x) = x^8 + x^6 + x^5 + x^4 + 1$

$$B = G \cdot A$$

Summary

- GOST R 34.11-2012 is based on GOST 34.11-94 as well as on Whirlpool/Grøstl/AES
- The proposed method for reconstructing of initial representation has many application fields
- Nonlinear dependence of the performance and the message length

  - More details on `https://github.com/okazymyrov`

Conclusions

- Cryptanalytic methods applied to MICKEY, DES and MiniAES can be used to improve cryptographic properties of prospective ciphers
- In the post-AES era many cryptoprimitives providing a high security level use random substitutions
- The new heuristic method to generate S-boxes was proposed
    - Surpass analogues used in Russian and Belorussian standards

Conclusions

- Several methods to check REA-equivalences of two binary nonlinear mappings have been proposed
- Isomorphic representations open new directions in cryptanalysis
  - Nonlinear mappings
  - Overall design principles
- The main practical result is the designed software for effective generation and calculation of indicators of arbitrary nonlinear binary mappings.

Methods and Tools for Analysis of Symmetric Cryptographic Primitives

Oleksandr Kazymyrov

University of Bergen
Norway

1st of December, 2014