Alexander Rostovtsev
alexander. rostovtsev@ibks.ftk.spbstu.ru
St. Petersburg State Polytechnic University

Virtual isomorphisms of ciphers: is AES secure against differential / linear attack?

In [eprint.iacr.org/2009/117] method of virtual isomorphisms of ciphers was proposed for cryptanalysis. Cipher is vulnerable to an attack iff isomorphic cipher is vulnerable to this attack. That method is based on conjugation, and it is not practical because all round operations except one become nonlinear. New isomorphism of AES is proposed, its image IAES has only one nonlinear operation IXOR - isomorphic image of XOR of 5 bytes. Maximal probabilities of byte differentials are increased about 10-11 times, maximal biases of linear sums are increased about 3.6 times comparatively to original AES. IAES possesses computable family of differentials of IXOR with two active input bytes, zero output difference and probability 1. Zero output difference decreases the rate of multiplication of active nonlinearities in differential characteristic of IAES.

1. Introduction

In [12] method of virtual isomorphisms of ciphers was proposed for amplifying known cryptanalytic attacks. Ciphers $y = C(x, k)$ and $\mathfrak{y} = \mathfrak{C}(\mathfrak{x}, \mathfrak{k})$ are isomorphic if there exists an invertible computable in both directions map $y \leftrightarrow \mathfrak{y}$, $x \leftrightarrow \mathfrak{x}$, $k \leftrightarrow \mathfrak{k}$, $C \leftrightarrow \mathfrak{C}$. Usually cipher C is the real one. But family of its isomorphic images $\mathfrak{C}$ is virtual; it exists in imagine of cryptanalyst. This explains the term “virtual” in the head of the article. Such technique is not absolutely new. Virtual injective homomorphism AES → BES was proposed in [9].

Isomorphism of ciphers is not equivalence because it does not act transitively: composition of computable maps is not necessary computable (key for one round of encryption is easy to compute, but for 10 rounds it is hard).

Next theorem was proved in [12] for attacks based on known plaintexts and ciphertexts.

Theorem 1. A cipher is vulnerable to a cryptanalytic attack iff isomorphic cipher is vulnerable to the attack.

Hence search of weaknesses of a cipher can be replaced by search of proper isomorphism of the cipher. If φ is arbitrary substitution and F is a function of round encryption, then conjugate function $\mathfrak{F} = \varphi^{-1}F\varphi$ determines simple isomorphism — conjugation.

Two substitutions are conjugate iff they have the same cycling type. Hence the substitution defined by inversion in field $\mathbb{F}_{2^n}$ for sufficiently large n is approximately conjugate with affine substitution that consists of cycles of length 2, such as XOR with a non-zero constant. Considered in [12] simple virtual isomorphism based on conjugated byte substitution is not practical, because its image is affine byte substitution, but other byte operations become non-linear. There are many byte substitutions that map finite field inversion to affine map by conjugation. Used conjugating substitution φ was chosen in such a way that it had many fixed points.

The most popular cryptanalytic methods are linear [8] and differential [3] that take a large number of known pairs plaintext/ciphertext, and algebraic methods [5, 6, 11], based on solving systems of polynomial equations that take one or few pairs plaintext/ciphertext. Combination of these methods is possible also [1].

Let n-bit substitution S maps input vector $\mathbf{x} = (x_1, \ldots, x_n)$ to output vector $\mathbf{y} = (y_1, \ldots, y_n)$. If x_i, y_i are independent variables, then linear function $f = \sum_{i=1}^{n} a_i x_i + \sum_{i=1}^{n} b_i y_i + c$, a_i, b_i, $c \in \mathbb{F}_2$, is balanced one. But if x_i, y_i are algebraically dependent (as inputs/outputs of substitution), then probabilities $P(f = 0)$, $P(f = 1)$ can differ from 0.5. Difference $P(0) - 0{,}5$ is the bias of substitution. Diffusion maps are usually affine and do not change absolute biases of linear sums. Linear operation XOR with the key does not change current linear sum.

Linear cryptanalysis search such linear functions dependent on plaintext, ciphertext, key (and possibly intermediate texts) bits. If there is sufficient number of plaintext/ciphertext pairs, then the wanted key can be computed as the most likely one.

Let $\mathbf{x}$, $\mathbf{x}'$ is a pair of n-bit binary inputs of substitution S, $\mathbf{y} = S(\mathbf{x})$, $\mathbf{y}' = S(\mathbf{x}')$. Denote $\Delta\mathbf{x} = \mathbf{x} + \mathbf{x}'$, $\Delta\mathbf{y} = \mathbf{y} + \mathbf{y}'$, where $\Delta\mathbf{y} = 0$ iff $\Delta\mathbf{x} = 0$. For a substitution S one can compute probability of differential $(\Delta\mathbf{x}, \Delta\mathbf{y})$. We can consider the “move” of input differential through the cipher. The maps used in the cipher can change the current differential and its probability. Probability of current differential equals to product of probabilities of corresponding differentials of maps of the cipher. Affine operations (XOR and diffusion map) has probabilities only 1 or 0, and hence they sometimes do not change probabilities of differentials. Differential cryptanalysis is based on property that distribution of probabilities of differentials of nonlinear substitution is not uniform. Linear cryptanalysis is similar to differential one.

Usually nonlinear substitution of a cipher usually has special properties: its maximal probabilities of differentials and absolute biases of linear sums are as small as possible.

Such substitution is used in standard AES. It is composition of finite field inversion and affine map. Its maximal probability of differential is 4/256 and maximal absolute bias of linear sum is 16/256. Diffusion map of AES (“shift rows” and “mix columns”) is linear and can be written as the block matrix. Apparently complexity of linear and differential attack exceeds the key enumeration.

In this paper we show that conjugating substitution φ that maps finite field inversion (with permuted 0 and 1) to XOR with a constant can have at most 130 fixed points, there exist 2^{42} such substitutions. We propose new virtual isomorphism based on 4 auxiliary affine equivalent byte substitutions that maps AES to IAES (isomorphic AES). IAES has only one non-linear map, it is image of

XOR operation that increments maximal probability of round differential reduced to one byte about 10-11 times and maximal absolute bias about 3,6 times comparatively to original AES. Brief estimation shows that probability of differential is changed from p in AES to $\approx \sqrt{p}$ in IAES, and then we can assume that complexity of differential cryptanalysis of IAES is about a square root of complexity of differential cryptanalysis of AES. Besides of that IAES has computable collisions that give a family of differentials with zero output difference that have probability 1. Zero output difference decreases the rate of multiplication of active nonlinearities in differential characteristic of IAES.

2. Algebraic background

If S, T are elements of symmetric group G, then map σ_S: $T \to STS^{-1}$ is the conjugation. Conjugation is equivalence. If S runs through all group G, we obtain the class of T.

Let G is subgroup of symmetric group of substitutions of n-bit words, G is generated by one, two or more substitutions, and x is input of substitution. Orbit of x is the set of n-bit words that is the union of images of x under action group G. Belonging two words to the same orbit is equivalence. Hence the set of n-bit words if union of orbits defined by G. Two orbits coincide or have no common elements.

If G is generated by one substitution S, then orbits are cycles of S. List of lengths of cycles define cycling type of substitution. Conjugation maps cycle of one substitution to cycle of the same length of other substitution. Hence two substitutions are conjugate iff they have the same cycling type.

Affine substitution is given by equation $\mathbf{y} = L\mathbf{x} + \mathbf{c}$, where L is invertible matrix over $\mathbb{F}_2$, if $\mathbf{c} = 0$ substitution is linear. Affine substitutions form subgroup of symmetric group. Substitutions S, T are affine equivalent if the equality holds $S = ATB$ for some affine substitutions A, B. Affine equivalence of substitutions can be effectively recognized [4].

Let $\mathbf{y} = T(\mathbf{x})$ — arbitrary map of the set of n-bit words to itself. This map can be given also using interpolating polynomials. Such polynomials form the finite ring. Usually ring of NAF polynomials is used:

$$\mathfrak{G}_n[\mathbf{x}] = \mathbb{F}_2[x_1, \ldots, x_n]/(x_1^2 + x_1, \ldots, x_n^2 + x_n).$$

Ring $\mathfrak{G}_n[\mathbf{x}]$ is finite and hence it is Artinian and has dimension 0 [2]. In this ring intersection of ideals coincides with their product. Each prime ideal is the maximal one; it consists of polynomials that take zero in the given point. Any ideal can be uniquely represented as the product of prime ideals. There are 2^n prime ideals. For any $f \in \mathfrak{G}_n[\mathbf{x}]$ equality holds $f(f + 1) = 0$, so non-constant polynomial divides 0.

Prime ideal can be given by one polynomial, such as $1 + x_1 \ldots x_n$. So each ideal can be given by one polynomial. Set of n-bit vectors form affine space $\mathbb{A}^n$.

Automorphisms of ring $\mathsf{G}_n[\mathbf{x}]$ preserves constants 0 and 1 and maps prime ideal to prime ideal (assumption that image of prime ideal is product of two different ideals leads to contradiction, because such map is no invertible). Each permutation of prime ideals (i.e. substitution that acts on the set of n-bit vectors) is automorphism of ring $\mathsf{G}_n[\mathbf{x}]$ and back, any automorphism defines such substitution.

Any substitution is defined by set of polynomials. A map of ring of polynomials to itself is regular if it is given by set of polynomials that define change of variables. If inverse regular map of the ring exists, this map is biregular. Hence all automorphisms of $\mathsf{G}_n[\mathbf{x}]$ are biregular.

Probabilities differentials of n-bit substitution can be written as square matrix of size 2^n [7]. Rows and columns of the matrix correspond to vectors $\Delta\mathbf{x}$, $\Delta\mathbf{y}$ of differential ($\Delta\mathbf{x}$, $\Delta\mathbf{y}$), so any differential corresponds to element of the matrix. Elements of the matrix of differentials are numbers of appearance of given differential if x runs through all set of 2^n vectors.

Similarly biases of linear sums $\sum_i a_i x_i + \sum_j b_j y_j$ of n-bit substitution can be represented by square matrix of size 2^n which rows and columns correspond to $\sum_i a_i x_i$, $\sum_j b_j y_j$. Element of the matrix is the numbers of case when equality $\sum_i a_i x_i + \sum_j b_j y_j = 0$ holds minus 2^{n-1}, this defines the bias of linear sum.

Any substitution $\mathbf{y} = S(\mathbf{x})$ can be given by set of polynomials of $\mathbf{x}$, $\mathbf{y}$ that take zero if equality $\mathbf{y} = S(\mathbf{x})$ holds. Any set of polynomials defines ideal $\mathfrak{A}$, set of zeroes of the ideal is variety $V(\mathfrak{A})$, and back any set of points of $\mathbb{A}^n$ as variety defines some ideal.

Let $\mathfrak{A} \oplus \mathfrak{B}$ is the sum of ideals. It is ideal generated by polynomials of $\mathfrak{A}$ and $\mathfrak{B}$. Obviously $\mathfrak{A} \oplus \mathfrak{B} \supseteq \mathfrak{A}$, $V(\mathfrak{A} \oplus \mathfrak{B}) \subseteq V(\mathfrak{A})$.

Define probability of differential $\Delta\mathbf{x} = (x_{i_1}, ..., x_{i_k})$ of arbitrary ideal $\mathfrak{A} \subset \mathsf{G}_n[\mathbf{x}]$. Let $\mathfrak{A} = (f(\mathbf{x}))$. Denote $D(f, x_i)$ partial derivative of f by variable x_i. Denote

$$D(f, \{x_i, x_j\}) = D(f, x_i) + D(f, x_j) + D(D(f, x_i), x_j),$$

and farther by induction: $D(f, \{x_{i_1}, ..., x_{i_l}\}) = D(D(f, \{x_{i_1}, ..., x_{i_{l-1}}\}), x_{i_l})$. It is obvious that $D(f, \{x_{i_1}, ..., x_{i_k}\})$ is a polynomial and hence it defines corresponding ideal. Probability of differential $\Delta\mathbf{x} = (x_{i_1}, ..., x_{i_k})$ of ideal $\mathfrak{A} = (f)$ is $\dfrac{\#V((f)) \oplus (D(f, \{x_{i_1}, ..., x_{i_k}\}))}{\#V((f))}$.

This definition generalizes the definition if probability of differential of substitution. In such a way we can define probability of differential for any map of the set of s-bit words to the set of t-bit words.

Similarly we can define nonlinearity of ideal as Hamming distance between polynomial that defines principal ideal and set of affine functions, but this distance is counted only in variety of ideal. This definition generalizes definitions of nonlinearity of Boolean functions and nonlinearity of substitutions.

3. Isomorphisms of AES

Let x, y, k are plaintext, ciphertext and key of cipher C, $\mathfrak{x}$, $\mathfrak{y}$, $\mathfrak{k}$ are plaintext, ciphertext and key of cipher $\mathfrak{C}$. C and $\mathfrak{C}$ are isomorphic ($C \cong \mathfrak{C}$) iff there exists computable in both directions bijection $x \leftrightarrow \mathfrak{x}$, $y \leftrightarrow \mathfrak{y}$, $k \leftrightarrow \mathfrak{k}$ such that equalities $y = C(x, k)$ and $\mathfrak{y} = \mathfrak{C}(\mathfrak{x}, \mathfrak{k})$ hold simultaneously. Cipher C is vulnerable with respect to some attack iff cipher $\mathfrak{C}$ is vulnerable with respect to the same attack.

Technique of virtual isomorphisms can be illustrated as application to AES.

Standard AES has 10, 12 or 14 rounds, block size is 128 bits, key size is 128, 192 or 256 bits [10]. Each round has next operations.

1. Byte substitution S for all 16 bytes of the block. Substitution is defined as composition of exponentiation $y = x^{254}$ in field $\mathbb{F}_{256} = \mathbb{F}_2[t]/(t^8 + t^4 + t^3 + t + 1)$ and affine map over $\mathbb{F}_2$. Exponent y is presented as 8-bit vector $\mathbf{y}$ over $\mathbb{F}_2$, and output of S is $\mathbf{z} = L\mathbf{y} + \mathbf{c}$, where $L = \begin{pmatrix} 1&0&0&0&1&1&1&1\\ 1&1&0&0&0&1&1&1\\ 1&1&1&0&0&0&1&1\\ 1&1&1&1&0&0&0&1\\ 1&1&1&1&1&0&0&0\\ 0&1&1&1&1&1&0&0\\ 0&0&1&1&1&1&1&0\\ 0&0&0&1&1&1&1&1 \end{pmatrix}$, $\mathbf{c} = \begin{pmatrix} 1\\1\\0\\0\\0\\1\\1\\0 \end{pmatrix}$. Any bit of vector $\mathbf{c}$ is the trace of corresponding row of matrix L (considered as element of $\mathbb{F}_{256}$). Denote $M(\mathbf{x}) = L\mathbf{x} + \mathbf{c}$. Substitution M consists of cycles of length 4. Maximal probability of differential of S is 4/256, maximal bias of linear sums is 16/256.

2. Diffusion map (shift rows and mix columns) can be represented by matrix W over $\mathbb{F}_{256}$:

$$W = \begin{pmatrix}
t&0&0&0&0&1+t&0&0&0&0&1&0&0&0&0&1\\
1&0&0&0&0&t&0&0&0&0&1+t&0&0&0&0&1\\
1&0&0&0&0&1&0&0&0&0&t&0&0&0&0&1+t\\
1+t&0&0&0&0&1&0&0&0&0&1&0&0&0&0&t\\
0&0&0&1&t&0&0&0&0&1+t&0&0&0&0&1&0\\
0&0&0&1&1&0&0&0&0&t&0&0&0&0&1+t&0\\
0&0&0&1+t&1&0&0&0&0&1&0&0&0&0&t&0\\
0&0&0&t&1+t&0&0&0&0&1&0&0&0&0&1&0\\
0&0&1&0&0&0&0&1&t&0&0&0&0&1+t&0&0\\
0&0&1+t&0&0&0&0&1&1&0&0&0&0&t&0&0\\
0&0&t&0&0&0&0&1+t&1&0&0&0&0&1&0&0\\
0&0&1&0&0&0&0&t&1+t&0&0&0&0&1&0&0\\
0&1+t&0&0&0&0&1&0&0&0&0&1&t&0&0&0\\
0&t&0&0&0&0&1+t&0&0&0&0&1&1&0&0&0\\
0&1&0&0&0&0&t&0&0&0&0&1+t&1&0&0&0\\
0&1&0&0&0&0&1&0&0&0&0&t&1+t&0&0&0
\end{pmatrix}$$

3. XOR addition of the text and the round key. This operation can be joined with XOR addition of bytes in diffusion map.

So AES can be described in terms of byte exponentiation, byte affine substitution, byte multiplication in field $\mathbb{F}_{256}$ and byte XOR addition.

Matrix W can be considered as block matrix over $\mathbb{F}_2$ with block size 8. Elements 0, 1, t, $1 + t$ of W over $\mathbb{F}_{256}$ correspond to zero block, identity block E, block $L_t = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 \end{pmatrix}$ and block $L_{t1} = L_t + E$. Hence we can consider diffusion map as block matrix with four types of blocks.

Since multiplication in $\mathbb{F}_{256}$ is commutative, there holds equality $L_tL_t = L_{t1}L_t$, but both conditions $M(L_t(x) = L_t(M(x))$, $M(L_{t1}(x) = L_{t1}(M(x))$ are impossible for any x.

Denote U as exponentiation in $\mathbb{F}_{256}$. Farther we will decompose AES substitution $S = UM$ and join affine substitution M to diffusion maps. So blocks of matrix W are changed. Zero block stays the zero block, identity block is changed by affine map M, block L_t is changed by affine map $M_t = L_tM$, block L_{t1} is changed by affine map $M_{t1} = L_{t1}M$. XOR addition of bytes does not change.

Substitution U has 127 cycles of length 2 and two cycles of length 1: $U(0) = 0$, $U(1) = 1$. We will approximately change U by substitution T: $T(1) = 0$, $T(0) = 1$, $T(x) = U(x)$ for $x \neq 0, 1$. Then equality $U(x) = T(x)$ holds with high probability $1 - 2^{-7} = 0{,}92$. Substitution T has only cycles of length 2.

T= {1, 0, 141, 246, 203, 82, 123, 209, 232, 79, 41, 192, 176, 225, 229, 199, 116, 180, 170, 75, 153, 43, 96, 95, 88, 63, 253, 204, 255, 64, 238, 178, 58, 110, 90, 241, 85, 77, 168, 201, 193, 10, 152, 21, 48, 68, 162, 194, 44, 69, 146, 108, 243, 57, 102, 66, 242, 53, 32, 111, 119, 187, 89, 25, 29, 254, 55, 103, 45, 49, 245, 105, 167, 100, 171, 19, 84, 37, 233, 9, 237, 92, 5, 202, 76, 36, 135, 191, 24, 62, 34, 240, 81, 236, 97, 23, 22, 94, 175, 211, 73, 166, 54, 67, 244, 71, 145, 223, 51, 147, 33, 59, 121, 183, 151, 133, 16, 181, 186, 60, 182, 112, 208, 6, 161, 250, 129, 130, 131, 126, 127, 128, 150, 115, 190, 86, 155, 158, 149, 217, 247, 2, 185, 164, 222, 106, 50, 109, 216, 138, 132, 114, 42, 20, 159, 136, 249, 220, 137, 154, 251, 124, 46, 195, 143, 184, 101, 72, 38, 200, 18, 74, 206, 231, 210, 98, 12, 224, 31, 239, 17, 117, 120, 113, 165, 142, 118, 61, 189, 188, 134, 87, 11, 40, 47, 163, 218, 212, 228, 15, 169, 39, 83, 4, 27, 252, 172, 230, 122, 7, 174, 99, 197, 219, 226, 234, 148, 139, 196, 213, 157, 248, 144, 107, 177, 13, 214, 235, 198, 14, 207, 173, 8, 78, 215, 227, 93, 80, 30, 179, 91, 35, 56, 52, 104, 70, 3, 140, 221, 156, 125, 160, 205, 26, 65, 28}.

It is reasonable to choose conjugate image $\mathfrak{T}$ of T as affine substitution (for example, M^2 or XOR with non-zero constant). Then probabilities of conjugate substitution $\mathfrak{T}$ are only 0 and 1 and biases of linear sums are only 0, ±0.5.

Cryptanalyst may choose arbitrary isomorphism. Complexity of differential/linear attack on isomorphic cipher will be reduced if probabilities of differentials (biases of linear sums) will be sufficiently large.

Define the distance $d(S_1, S_2)$ between two n-bit substitutions as number of inputs for which inequality holds $S_1(x) \neq S_2(x)$. Distance between substitution $S(x)$ and group Aff of affine substitutions is $\min(d(S, A))$, if A runs through all group

Aff. Usually the nearer is S to Aff, the larger are probabilities of differentials and absolute biases of linear sums.

If affine substitution A is the identity, then distance between φ and identity substitution is number of points where inequality holds $\varphi(x) \neq x$. Hence if we want to increase probabilities of differentials, linear sums of substitution φ, it is sufficient to provide large number of fixed points of φ.

Let G is group that acts on the set of n-bit vectors. Denote $\mathrm{Orb}(x, G)$ as the orbit of element $x \in M$ with respect to G. Choose conjugating substitution φ in such a way that it would have many fixed points. For computing φ at first find orbits of set of 8-bit vectors with respect to group $\langle T, \mathfrak{T} \rangle$ generated by substitutions T and $\mathfrak{T}$.

Theorem 2. Let S_1, S_2 are n-bit substitutions that consist of cycles of length 2, and $\langle S_1, S_2 \rangle$ is the group generated by those substitutions. Then $\#\mathrm{Orb}(x, \langle S_1, S_2 \rangle)$ is even.

Proof. Since $S_1^2 = S_2^2 = E$ (identity substitution), group $\langle S_1, S_2 \rangle$ consists of substitutions $\{E, S_1, S_2, S_1S_2, S_2S_1, S_1S_2S_1, S_2S_1S_2, S_1S_2S_1S_2, \ldots\}$. Length of orbit is at least 2. Assume that orbit of some x has length 3. Then $S_1(x)$ is in this orbit and $S_1S_2S_1(x) = x$, so $S_1S_2(x) = S_1(x)$ and $S_2(x) = x$ — contradiction. Similarly one can proof that length of orbit is not 5, 7, etc. ■

Corollary 1. $\mathrm{Orb}(x, \langle T, \mathfrak{T} \rangle)$ have even cardinality for all x.

Easy test shows that among 255 possible $\mathfrak{T}$, given as XOR with constant, only lowest bit inversion gives two orbits of length 2 and 42 orbits of length 6. Other substitutions $\mathfrak{T}$ give more long orbits. This limits the number of conjugating substitutions φ as it is proved in theorem 3.

Let $\varphi^{-1}T\varphi = \mathfrak{T}$. If $\mathrm{Orb}(a, \langle T, \mathfrak{T} \rangle) = \{a, b\}$, then both points of the orbit can be fixed by φ. Indeed, if orbit consists of two elements (a, b), then $T(a) = b$, $T(b) = a$, $\mathfrak{T}(a) = b$, $\mathfrak{T}(b) = a$. Since $\varphi^{-1}T\varphi = \mathfrak{T}$, we can set $\varphi(a) = a$, $\varphi(b) = b$.

Theorem 3. Let n-bit substitutions S_1, S_2 consist of cycles of length 2, and length of orbit of element a defined by group $\langle S_1, S_2 \rangle$ exceeds 2. Then next statements are true.

1. $\mathrm{Orb}(a, \langle S_1, S_2 \rangle) = \mathrm{Orb}(a, \langle S_1, S_1S_2 \rangle) = \mathrm{Orb}(a, \langle S_1, S_2S_1 \rangle) = \mathrm{Orb}(a, \langle S_2, S_1S_2 \rangle) = \mathrm{Orb}(a, \langle S_2, S_2S_1 \rangle)$.
2. Orbit of element a can be written in cyclic form $(a, S_1(a), S_2S_1(a), S_1S_2S_1(a), S_2S_1S_2S_1(a), \ldots)$, where left multiples S_1, S_2 alternate.
3. $\#\mathrm{Orb}(a, \langle S_1, S_2 \rangle) = 2\#\mathrm{Orb}(a, S_1S_2)$.
4. There exists conjugating substitution φ such that $S_1 = \varphi^{-1}S_2\varphi$, and φ fixes all elements in the odd or in the even positions of the orbit $\mathrm{Orb}(a, \langle S_1, S_2 \rangle)$ written in cyclic form (p. 2).

5. There is no conjugating substitution φ that fixes more points of an orbit then a half of length of the orbit.
6. If $S_1 = \varphi^{-1}S_2\varphi$ and φ fixes element on the odd (even) positions of orbit written in the cyclic form, then $\mathrm{Orb}(x, \langle S_1, S_2\rangle) = \mathrm{Orb}(x, \langle S_1, S_2, \varphi\rangle)$ for all x.

Proof. (1). Since $S_1(S_1S_2) = S_2$ group $\langle S_1, S_2\rangle$ can be generated by substitutions S_1, S_1S_2. Since $(S_2S_1)S_1 = S_2$ we obtain $\langle S_1, S_2\rangle = \langle S_1, S_2S_1\rangle$. Similarly $\langle S_1, S_2\rangle = \langle S_2, S_1S_2\rangle = \langle S_2, S_2S_1\rangle$.

(2) and (3). Let length of cycle of element a for substitution S_2S_1 is k. Then $k > 1$, because from equalities $S_2S_1(a) = a$ and $S_1^2(a) = a$ we obtain $S_1(a) = S_2(a)$, and orbit consists of 2 elements — contradiction. Multiplying equality $(S_2S_1)^k(a) = a$ by S_2, obtain $(S_1S_2)^{k1}S_1(a) = S_2(a)$. Hence the cycle contains $S_2(a)$. Similarly $(S_1S_2)^{k1}(a) = S_2S_1(a)$, $(S_1S_2)^{k2}S_1(a) = S_2S_1S_2(a)$. Hence cycle of p. 2 contains a, $S_1(a)$, $S_2(a)$, $S_1S_2(a)$, $S_2S_1(a)$, …, i.e. the whole of element a. Elements of this cycle based on odd positions correspond to cycle of element a for substitution S_2S_1. Since length of the orbit is even, it equals to double length of cycle for substitution S_2S_1.

(4). For computing substitution φ let $\varphi(a) = a$ for some a. Element a is on odd position in cyclically written orbit. Then from equality $S_1(a) = \varphi^{-1}S_2\varphi(a) = \varphi^{-1}(S_2(a))$ obtain $\varphi^{-1}(S_2(a))$. Notice that $S_2(a)$ is situated on even position. Farther define next fixed point $\varphi^{-1}(S_2S_1(a)) = S_2S_1(a)$ (it is on odd position) and obtain $\varphi^{-1}(S_2S_1S_2(a))$ on even position, etc. So we obtain fixed points for all even positions of orbit written as the cycle (p. 2). Similarly we can fix elements on even positions of orbit of element a. It is sufficient to change $a \to S_1(a)$.

(5). Assume that we can fix all elements on odd positions of the orbit and one element on even position. Without loss of generality we can consider that this element is $S_1(a)$. Then substitution φ fixes both a, $S_1(a)$ and we obtain $S_2S_1(a) = a$, that is contradiction (length of orbit exceeds 2 by condition).

(6). Proof follows from the next reasoning: if $y \in \mathrm{Orb}(x, \langle S_1, S_2\rangle)$ and $\varphi(y) = y$, then $\varphi(S_2(y)) = S_1(y)$, and $S_1(y) \in \mathrm{Orb}(x, \langle S_1, S_2\rangle)$, $S_2(y) \in \mathrm{Orb}(x, \langle S_1, S_2\rangle)$. Hence both input and output of φ are in $\mathrm{Orb}(x, \langle S_1, S_2\rangle)$. ■

Experiment shows that if $\mathcal{T}$ is inversion of the lowest bit, then two orbits defined by group $\langle T, \mathcal{T}\rangle$ have length 2: {{0, 1}, {188, 189}}, and other 42 orbits have length 6: {2, 3, 246, 247, 140, 141}, {4, 5, 82, 83, 202, 203}, {6, 7, 209, 208, 122, 123}, …, {214, 215, 234, 235, 227, 226}. If substitution $\mathcal{T}$ defined by for XOR operation with another constant, the number of orbits decreases.

From theorem 3 we have next corollary.

Corollary 2. 1. For substitution T and lowest bit inversion substitution $\mathcal{T}$ there are 2^{42} different conjugating substitutions φ, satisfying equality $\mathcal{T} = \varphi^{-1}T\varphi$ that have 130 fixed points.

2. There are no substitutions $\mathcal{T}$, defined as XOR with other nonzero constants such that holds the equality $\mathcal{T} = \varphi^{-1}T\varphi$, and φ has 130 or more fixed points.

Theorem 4. There is no affine substitution $\mathfrak{T}$ such that $\mathfrak{T}^2 = E$ and $\mathfrak{T}$ has only two fixed points.

Proof. Consider such affine substitution $\mathfrak{T}(\mathbf{x}) = L\mathbf{x} + \mathbf{c}$. Let $L\mathbf{x}_1 + \mathbf{c} = \mathbf{x}_1$, $L\mathbf{x}_2 + \mathbf{c} = \mathbf{x}_2$. Then $L(\mathbf{x}_1 + \mathbf{x}_2) = \mathbf{x}_1 + \mathbf{x}_2$ is unique solution, and we can consider only linear $\mathfrak{T}$. Let $L\mathbf{a} = \mathbf{a}$ is a unique non-zero solution and equality $L^2\mathbf{x} = \mathbf{x}$ holds for all $\mathbf{x}$, i.e. $L^2 = E$. We have $L(\mathbf{x} + \mathbf{a}) = L\mathbf{x} + \mathbf{a}$ for all $\mathbf{x}$. Without loss of generality we can set $\mathbf{a} = (1, 0, \ldots, 0)$. Then first row and first column of L are $\mathbf{a}$. Denote 7*7 block of L with undefined elements as L_7. Then $L_7\mathbf{b} = \mathbf{b}$ is impossible for non-zero $\mathbf{b}$ (alternatively L must have four fixed points). Hence matrix $L_7 + E$ is invertible and $L_7^2 = E$. Then $(L_7 + E)^2 = L_7^2 + E = 0$ must be invertible — contradiction. ■

Corollary 3. There is no affine substitution that is precisely conjugate with respect to inversion in finite field $\mathbb{F}_{256}$.

4. Isomorphic AES for four auxiliary substitutions

Conjugate AES has affine substitution and nonlinear diffusion maps (images of M, M_t, M_{t1}) and nonlinear image of XOR operation. Try to obtain more affine images.

Notice that if $\mathfrak{T} = \varphi^{-1}T\varphi$ and $\mathfrak{T}$ is inversion of lowest bit then isomorphic image of XOR cannot be linear, because equality $\varphi(\psi(x) + \psi(y)) = x + y$ is possible only if ψ is affine and φ is linear. So try to obtain affine images $\mathfrak{M}$, $\mathfrak{M}_t$, $\mathfrak{M}_{t1}$ of affine substitutions M, M_t, M_{t1}.

Equality $\varphi^{-1}(\psi(x) + \psi(y)) = x + y$ can be true for many x, y if substitutions φ, ψ have many fixed points. Compute auxiliary substitutions φ, ψ, χ_1, χ_2 so that next conditions are satisfied:

1. $\mathfrak{T} = \varphi^{-1}T\varphi$,
2. $\mathfrak{M} = M = \psi^{-1}M\varphi$,
3. $\mathfrak{M}_t = M_t = \chi_1^{-1} M_t\varphi^{-1}$,
4. $\mathfrak{M}_{t1} = M_{t1} = \chi_2^{-1}M_{t1}\varphi^{-1}$.

If φ is known, then ψ, χ_1, χ_2 exist and are defined uniquely. Each of them has 130 fixed points, as φ has them. Indeed, if $\varphi(x) = x$, then $\varphi^{-1}(x) = x$, $M(x) = \psi M(x)$, $\psi(M(x)) = M(x)$.is the fixed point. The same is true for other auxiliary substitutions.

Define isomorphic image of AES under those regular automorphisms of ring $\mathfrak{G}_n[\mathbf{x}]$ as IAES.

Theorem 5. If $\mathfrak{M}$, $\mathfrak{M}_t$, $\mathfrak{M}_{t1}$ are arbitrary affine substitutions and $\mathfrak{M} = \psi^{-1}M\varphi$, $\mathfrak{M}_t = \chi_1^{-1}M_t\varphi$, $\mathfrak{M}_{t1} = \chi_2^{-1}M_{t1}\varphi$, then φ, ψ, χ_1, χ_2 are affine equivalent.

Proof follows from definition of affine equivalence and from property that M, M_t, M_{t1} are affine substitutions. ■

Theorem 6. Maps $\mathfrak{T} = \varphi^{-1}T\varphi$, $\mathfrak{M} = \psi^{-1}M\varphi$, $\mathfrak{M}_t = \chi_1^{-1}M_t\varphi$, $\mathfrak{M}_{t1} = \chi_2^{-1}M_{t1}\varphi$ define isomorphism AES → IAES for each round of encryption.

Proof. Consider one round in AES and IAES. Denote x_1, …, x_{16} as bytes of input text of AES, k as round key byte for first byte in AES and $\mathfrak{x}_i \leftarrow \varphi^{-1}(x_i)$, $\mathfrak{k}_i \leftarrow \varphi^{-1}(k_i)$ as corresponding bytes in IAES. First byte of AES is transformed according equation

$$x_1 \leftarrow (k_1 + M_tT(x_1) + M_{t1}T(x_6) + MT(x_{11}) + MT(x_{16})).$$

Corresponding transformation of IAES is

$$\mathfrak{x}_1 \leftarrow \varphi^{-1}(\varphi(\mathfrak{k}_1) + \chi_1(M_t(\mathfrak{T}(\mathfrak{x}_1))) + \chi_2(M_{t1}(\mathfrak{T}(\mathfrak{x}_6))) + \psi(M(\mathfrak{T}(\mathfrak{x}_{11}))) + \psi(M(\mathfrak{T}(\mathfrak{x}_{16})))).$$

Then first summand in the brackets in the right side for IAES transformation is k and coincides with first summand for AES. Second summand is

$$\chi_1(M_t(\mathfrak{T}(\mathfrak{x}_1))) = \chi_1\chi_1^{-1}M_t\varphi\varphi^{-1}T\varphi(\mathfrak{x}_1) = M_tT(x_1),$$

It coincides with the second summand for AES. Similarly other summands for IAES coincide with corresponding summands for AES. The same is true for other bytes and for other rounds. ■

Hence the IAES has only one nonlinear operation, namely the image of XOR for 5 summands (image of substitution T is near to affine). Denote this nonlinear operation as IXOR. This nonlinear operation is defined by ideal of 48 variables (40 input variables and 8 output variables) and hence possesses differentials with corresponding probabilities and linear sums with corresponding biases.

Four auxiliary substitutions are affine equivalent. Since $\mathfrak{M} = \psi^{-1}M\varphi$, $\psi = M\varphi\mathfrak{M}^{-1}$. Similar equations can be obtained for χ_1, χ_2. They can be transformed using right-hand multiplication on an affine substitution, i.e. they can be arbitrary elements of corresponding coset.

5. Results of experiment, security of AES and farther research

Substitutions M, M_t, M_{t1}, φ, ψ, χ_1, χ_2 and tables of maximal probabilities of differentials and biases of linear sums of the IXOR operation are given in the Appendix. Here IXOR as sum of 5 summands is considered as three families of substitutions where one byte is changed and sum of other bytes is fixed. Such differentials and linear sums are “truncated” ones of course.

We have computed probabilities of differentials and linear sums for three families of substitutions:

$$\varphi^{-1}(\psi(x) + y),\ \varphi^{-1}(\chi_1(x) + y),\ \varphi^{-1}(\chi_2(x) + y)$$

for all 256 possible *y*. Since table of differentials for each family is very large, for each *y* only maximal probability of differential and maximal positive/negative biases of linear sums are performed. Any *y* defines some substitution that acts on set of bytes *x*. These three substitutions can be considered as sections of large table of differentials for whole IXOR operation.

Maximal probability of differentials of original AES is 4/256. Three nonlinear substitutions that represent nonlinear IXOR have differentials with probabilities 42/256, 44/256/ 46/256. So probabilities of differentials increase about 10.5 – 11.5 times comparatively to original cipher. Maximal absolute biases of linear sums of IXOR substitutions are 58/256 for all three substitutions, biases are increased about 3.6 times comparatively to original AES.

Estimate complexity of differential attack on 10-round of AES according to [7]. Differential cryptanalysis proposes multiplication of probabilities of differentials in differential characteristic. Beginning from third round all 16 nonlinear IXOR in IAES and all 16 S-boxes in AES become active. Assume that probability of differential of AES in characteristic is *p*, and similar probability in IAES is 8*p* (i.e. instead of *p* we have $\sqrt{p}$). For original AES probability of differential is $2^{-6*16*7} = 2^{-672}$, for IAES probability of differential is $2^{-3*16*7} = 2^{-336}$, so the strength of IAES seems to be a square root of the strength of AES. Notice that in the real cryptanalysis probabilities of differentials can significantly increase using parallel branches in differential characteristic, using boomerang technique, and meet-in-the-middle technique, etc. Notice that there exist collisions of IXOR of probability 1.

In linear cryptanalysis biases of linear sum is proportional to product of biases of bits of the sum. It is common to consider the sum of 4 bytes that are used in IXOR. Mean of this sum contains 16 bits. If all bits of AES linear sum have bias 16/256, then result bias is e^{-34}. If all bits of IAES linear sum have bias 48/256, then result bias is $e^{-16.4}$. This is approximately the square root of bias of AES. Hence we can assume that the strength of AES to linear attack can be significantly reduced too. Hence security of IAES (and hence of AES) to linear and differential attacks is non-evident and takes farther research.

Such complexity estimation is very brief of course. More precise estimation needs modification of linear and differential attacks because probabilities of differentials depend on the key. On the other hand, this dependence can take some information about key byte.

Next theorem shows that there exists a mechanism that gives differentials of probability 1 and retards the multiplication of active inputs of IAXORs in differential characteristic. This is possible because the differentials have zero output difference.

Theorem 7. Let *a*, *b*, *c*, *d* are inputs of IXOR that define output sum

$$z = \varphi^{-1}(\psi(a) + \psi(b) + \chi(c) + \chi(d)).$$

There exists differential of IXOR four bytes with input difference of kind $\{(a, a, c, d,), (a + \Delta, a + \Delta, c, d)\}$ that gives outputs with difference 0.

Proof. Notice that $\varphi^{-1}(x) = \varphi^{-1}(y)$ iff $x = y$. Hence we can ignore φ^{-1}. Consider two sets of four bytes (a, b, c, d), (a_1, b_1, c_1, d_1), that define sums

$$z = \psi(a) + \psi(b) + \chi_1(c) + \chi_2(d), z_1 = \psi(a_1) + \psi(b_1) + \chi_1(c_1) + \chi_2(d_1).$$

Then equalities $a = b$, $a_1 = b_1$, $c = c_1$, $d = d_1$ give $z = z_1$ and hence equality of outputs of IXOR. So sets (a, a, c, d) with differences $(\Delta, \Delta, 0, 0)$ give collision (as differential with zero output difference) with probability 1. ■

We use affine $\mathfrak{T}$. But this substitution is not an exact conjugation with finite field inversion. Probability of error is 2^{-7} for each byte. This lack can be eliminated if instead of affine $\mathfrak{T}$ one uses quasi-affine $\mathfrak{T}$, which lowest bit is given by polynomial $y_8 + x_8 + (1 + x_1)\ldots(1 + x_7)$. Then probabilities of differentials of $\mathfrak{T}$ are 1 or (more often) 252/256, but maximal biases of linear sums stay 128/256. Set of orbits with respect to $\langle U, \mathfrak{T}\rangle$ is slightly changed: instead of $\{0, 1\}$ we obtain $\{0\},\{1\}$. Substitutions φ, ψ, χ_1, χ_2 do not change.

Presented material shows that virtual isomorphism is a useful tool for cryptanalysis.

We used isomorphisms that act on cipher maps and have period 1 (initial distortion $\varphi(x)$ is repeated for any round). Similarly one can use isomorphisms that have period of 2 or more rounds. Besides of that we can use quasi-periodic isomorphisms: isomorphisms for next round can differ from the isomorphism of previous round the next round using other φ and other affine $\mathfrak{m}$, $\mathfrak{m}_t$, $\mathfrak{m}_{t1}$.

Proposed virtual isomorphism uses auxiliary substitutions with many fixed points. Possibly this criterion is not optimal for cryptanalysis. Choosing some affine substitution (or possibly non-linear substitution that possesses differentials or linear sums of probability 1) instead of $\mathfrak{T}$ may be more useful. Decomposition of AES substitution $S = MU$, where U is finite field inversion, is not unique. Maybe there exists another decompositions with affine left-hand multiple and suitable cycling type of right-hand multiple that is more useful.

Proposed technique shows that substitution S of some symmetric cipher is possibly weak if it admits decomposition $S = AT$, where A if affine and nonlinear substitution T is conjugate with some affine substitution (precisely or approximately with small error probability). There is no known method to recognize possibly weak substitutions. Also we do not know how many "non-weak" substitutions there are, and does such "non-weak" substitution exist.

References

1. M. Albrecht and C. Cid. Algebraic techniques in differential cryptanalysis. Cryptology e-print archive, report 2008/177, 2008 // Available at http: // e-print.iacr.org/2008/177.

2. M. Atiyah and L. Macdonald. Introduction to commutative algebra, Addison-Wesley, 1969.
3. E. Biham and A. Shamir. Differential cryptanalysis of DES-like cryptosystems // Advances in Cryptology — CRYPTO ′90. LNCS, v. 537, Springer-Verlag, 1991, pp. 2–21.
4. A. Biryukov, C. De Canniere, A. Braeken, and B. Preneel. A toolbox for cryptanalysis: linear and affine equivalence algorithms // Advances in Cryptology — EUROCRYPT 2003. LNCS, v. 2556, Springer–Verlag, 2003, pp. 33–50.
5. N. Courtois and J. Pieprzyk. Cryptanalysis of block ciphers with overdefined systems of equations // LNCS 1666, pp. 19-30.
6. J.-C. Faugere. Groebner bases. Applications in cryptology. Invited talk at FSE-07 in Luxemburg. Available at http://fse2007.uni.lu/slides/faugere.
7. H. Heyes and S. Tavares. Substitution-permutation networks resistant to differential and linear cryptanalysis // Journal of cryptology, 1996, v. 9, pp. 1–19.
8. M. Matsui. Linear cryptanalysis method for DES cipher. // Advances in Cryptology — EUROCRYPT ′93, LNCS, v. 765, 1994, pp. 386–397.
9. S. Murphy and M. Robshaw. Essential algebraic structure within the AES // CRYPTO 2002, LNCS, v. 2442, pp.1-16.
10. NIST: Advanced encryption standard (AES), FIPS 197. Technical report, NIST (November, 2001).
11. H. Raddum and I. Semaev. New technique for solving sparse equation systems. Cryptology e-print archive, report 2006/475, 2006 // Available at http: // e-print.iacr.org/2006/475.
12. A. Rostovtsev**.** Changing probabilities of differentials and linear sums via isomorphism of ciphers// International Association for Cryptologic Research. Cryptology ePrint Archive, http://eprint.iacr.org/2009/117.

Appendix. Auxiliary substitutions, maximal probabilities of differentials and biases of linear sums of IAES

Substitutions T, $\mathfrak{T}$.

T = {1, 0, 141, 246, 203, 82, 123, 209, 232, 79, 41, 192, 176, 225, 229, 199, 116, 180, 170, 75, 153, 43, 96, 95, 88, 63, 253, 204, 255, 64, 238, 178, 58, 110, 90, 241, 85, 77, 168, 201, 193, 10, 152, 21, 48, 68, 162, 194, 44, 69, 146, 108, 243, 57, 102, 66, 242, 53, 32, 111, 119, 187, 89, 25, 29, 254, 55, 103, 45, 49, 245, 105, 167, 100, 171, 19, 84, 37, 233, 9, 237, 92, 5, 202, 76, 36, 135, 191, 24, 62, 34, 240, 81, 236, 97, 23, 22, 94, 175, 211, 73, 166, 54, 67, 244, 71, 145, 223, 51, 147, 33, 59, 121, 183, 151, 133, 16, 181, 186, 60, 182, 112, 208, 6, 161, 250, 129, 130, 131, 126, 127, 128, 150, 115, 190, 86, 155, 158, 149, 217, 247, 2, 185, 164, 222, 106, 50, 109, 216, 138, 132, 114, 42, 20, 159, 136, 249, 220, 137, 154, 251, 124, 46, 195, 143, 184, 101, 72, 38, 200, 18, 74, 206, 231, 210, 98, 12, 224, 31, 239, 17, 117, 120, 113, 165, 142, 118, 61, 189, 188, 134, 87, 11, 40, 47, 163, 218, 212, 228, 15, 169, 39, 83, 4, 27, 252, 172, 230, 122, 7, 174, 99, 197, 219, 226, 234, 148, 139, 196, 213, 157, 248, 144, 107, 177, 13, 214, 235, 198, 14, 207, 173, 8, 78, 215, 227, 93, 80, 30, 179, 91, 35, 56, 52, 104, 70, 3, 140, 221, 156, 125, 160, 205, 26, 65, 28};

$\mathfrak{T}$ = {1, 0, 3, 2, 5, 4, 7, 6, …, 255, 254}.

Orbits of group $\langle T, \mathfrak{T}\rangle$.

Orb = {{0, 1}, {2, 3, 246, 247, 140, 141}, {4, 5, 82, 83, 202, 203}, {6, 7, 209, 208, 122, 123}, {8, 9, 79, 78, 233, 232}, {10, 11, 192, 193, 40, 41}, {12, 13, 225, 224, 177, 176}, {14, 15, 199, 198, 228, 229}, {16, 17, 180, 181, 117, 116}, {18, 19, 75, 74, 171, 170}, {20, 21, 43, 42, 152, 153}, {22, 23, 95, 94, 97, 96}, {24, 25, 63, 62, 89, 8$\mathfrak{T}$8}, {26, 27, 204, 205, 252, 253}, {28, 29, 64, 65, 254, 255}, {30, 31, 178, 179, 239, 238}, {32, 33, 110, 111, 59, 58}, {34, 35, 241, 240, 91, 90}, {36, 37, 77, 76, 84, 85}, {38, 39, 201, 200, 169, 168}, {44, 45, 68, 69, 49, 48}, {46, 47, 194, 195, 163, 162}, {50, 51, 108, 109, 147, 146}, {52, 53, 57, 56, 242, 243}, {54, 55, 66, 67, 103, 102}, {60, 61, 187, 186, 118, 119}, {70, 71, 105, 104, 244, 245}, {72, 73, 100, 101, 166, 167}, {80, 81, 92, 93, 236, 237}, {86, 87, 191, 190, 134, 135}, {98, 99, 211, 210, 174, 175}, {106, 107, 223, 222, 144, 145}, {112, 113, 183, 182, 120, 121}, {114, 115, 133, 132, 150, 151}, {124, 125, 250, 251, 160, 161}, {126, 127, 130, 131, 128, 129}, {136, 137, 158, 159, 154, 155}, {138, 139, 217, 216, 148, 149}, {142, 143, 164, 165, 184, 185}, {156, 157, 220, 221, 248, 249}, {172, 173, 231, 230, 207, 206}, {188, 189}, {196, 197, 212, 213, 219, 218}, {214, 215, 234, 235, 227, 226}}.

Substitutions M, M_t, M_{t1}.

M = {99, 124, 93, 66, 31, 0, 33, 62, 155, 132, 165, 186, 231, 248, 217, 198, 146, 141, 172, 179, 238, 241, 208, 207, 106, 117, 84, 75, 22, 9, 40, 55, 128, 159, 190, 161, 252, 227, 194, 221, 120, 103, 70, 89, 4, 27, 58, 37, 113, 110, 79, 80, 13, 18, 51, 44, 137, 150, 183, 168, 245, 234, 203, 212, 164, 187, 154, 133, 216, 199, 230, 249, 92, 67, 98, 125, 32, 63, 30, 1, 85, 74, 107, 116, 41, 54, 23, 8, 173, 178, 147, 140, 209, 206, 239, 240, 71, 88, 121, 102, 59, 36, 5, 26, 191, 160, 129, 158, 195, 220, 253, 226, 182, 169, 136, 151, 202, 213, 244, 235, 78, 81, 112, 111, 50, 45, 12, 19, 236, 243, 210, 205, 144, 143, 174, 177, 20, 11, 42, 53, 104, 119, 86, 73, 29, 2, 35, 60, 97, 126, 95, 64, 229, 250, 219, 196, 153, 134, 167, 184, 15, 16, 49, 46, 115, 108, 77, 82, 247, 232, 201, 214, 139, 148, 181, 170, 254, 225, 192, 223, 130, 157, 188, 163, 6, 25, 56, 39, 122, 101, 68, 91, 43, 52, 21, 10, 87, 72, 105, 118, 211, 204, 237, 242, 175, 176, 145, 142, 218, 197, 228, 251, 166, 185, 152, 135, 34, 61, 28, 3, 94, 65, 96, 127, 200, 215, 246, 233, 180, 171, 138, 149, 48, 47, 14, 17, 76, 83, 114, 109, 57, 38, 7, 24, 69, 90, 123, 100, 193, 222, 255, 224, 189, 162, 131, 156};

M_t = {177, 62, 46, 161, 143, 0, 16, 159, 205, 66, 82, 221, 243, 124, 108, 227, 73, 198, 214, 89, 119, 248, 232, 103, 53, 186, 170, 37, 11, 132, 148, 27, 64, 207, 223, 80, 126, 241, 225, 110, 60, 179, 163, 44, 2, 141, 157, 18, 184, 55, 39, 168, 134, 9, 25, 150, 196, 75, 91, 212, 250, 117, 101, 234, 210, 93, 77, 194, 236, 99, 115, 252, 174, 33, 49, 190, 144, 31, 15, 128, 42, 165, 181, 58, 20, 155, 139, 4, 86, 217, 201, 70, 104, 231, 247, 120, 35, 172, 188, 51, 29, 146, 130, 13, 95, 208, 192, 79, 97, 238, 254, 113, 219, 84, 68, 203, 229, 106, 122, 245, 167, 40, 56, 183, 153, 22, 6, 137, 246, 121, 105, 230, 200, 71, 87, 216, 138, 5, 21, 154, 180, 59, 43, 164, 14, 129, 145, 30, 48, 191, 175, 32, 114, 253, 237, 98, 76, 195, 211, 92, 7, 136, 152, 23, 57, 182, 166, 41, 123, 244, 228, 107, 69, 202, 218, 85, 255, 112, 96, 239, 193, 78, 94, 209, 131, 12, 28, 147, 189, 50, 34, 173, 149, 26, 10, 133, 171, 36, 52, 187, 233, 102, 118, 249, 215, 88, 72, 199, 109, 226, 242, 125, 83, 220, 204, 67, 17, 158, 142, 1, 47, 160, 176, 63, 100, 235, 251, 116, 90, 213, 197, 74, 24, 151, 135, 8, 38, 169, 185, 54, 156, 19, 3, 140, 162, 45, 61, 178, 224, 111, 127, 240, 222, 81, 65, 206};

M_{t1} = {210, 66, 115, 227, 144, 0, 49, 161, 86, 198, 247, 103, 20, 132, 181, 37, 219, 75, 122, 234, 153, 9, 56, 168, 95, 207, 254, 110, 29, 141, 188, 44, 192, 80, 97, 241, 130, 18, 35, 179, 68, 212, 229, 117, 6, 150, 167, 55, 201, 89, 104, 248, 139, 27, 42, 186, 77, 221, 236, 124, 15, 159, 174, 62, 118, 230, 215, 71, 52, 164, 149, 5, 242, 98, 83, 195, 176, 32, 17, 129, 127, 239, 222, 78, 61, 173, 156, 12, 251, 107, 90, 202, 185, 41, 24, 136, 100, 244, 197, 85, 38, 182, 135, 23, 224, 112, 65, 209, 162, 50, 3, 147, 109, 253, 204, 92, 47, 191, 142, 30, 233, 121, 72, 216, 171, 59, 10, 154, 26, 138, 187, 43, 88, 200, 249, 105, 158, 14, 63, 175, 220, 76, 125, 237, 19, 131, 178, 34, 81, 193, 240, 96, 151, 7, 54, 166, 213, 69, 116, 228, 8, 152, 169, 57, 74, 218, 235, 123, 140, 28, 45, 189, 206, 94, 111, 255, 1, 145, 160, 48, 67, 211, 226, 114, 133, 21, 36, 180, 199, 87, 102, 246, 190, 46, 31, 143, 252, 108, 93, 205, 58, 170, 155, 11, 120, 232, 217, 73, 183, 39, 22, 134, 245, 101, 84, 196, 51, 163, 146, 2, 113, 225, 208, 64, 172, 60, 13, 157, 238, 126, 79, 223, 40, 184, 137, 25, 106, 250, 203, 91, 165, 53, 4, 148, 231, 119, 70, 214, 33, 177, 128, 16, 99, 243, 194, 82}.

Auxiliary substitutions.

fi = {0, 1, 246, 3, 82, 5, 209, 7, 79, 9, 192, 11, 225, 13, 199, 15, 180, 17, 75, 19, 43, 21, 95, 23, 63, 25, 204, 27, 64, 29, 178, 31, 110, 33, 241, 35, 77, 37, 201, 39, 10, 41, 42, 152, 68, 45, 194, 47, 48, 44, 108, 51, 57, 53, 66, 55, 56, 242, 58, 32, 187, 61, 62, 89, 254, 65, 103, 67, 49, 69, 105, 71, 100, 73, 74, 171, 76, 84, 78, 233, 92, 81, 202, 83, 36, 85, 191, 87, 88, 24, 90, 34, 236, 93, 94, 97, 96, 22, 211, 99, 166, 101, 102, 54, 104, 244, 223, 107, 147, 109, 59, 111, 183, 113, 133, 115, 116, 16, 60, 119, 112, 121, 6, 123, 250, 125, 130, 127, 126, 129, 128, 131, 132, 150, 86, 135, 158, 137, 217, 139, 2, 141, 164, 143, 106, 145, 146, 50, 138, 149, 114, 151, 20, 153, 136, 155, 220, 157, 154, 159, 124, 161, 162, 46, 184, 165, 72, 167, 168, 38, 170, 18, 231, 173, 98, 175, 176, 12, 239, 179, 117, 181, 182, 120, 142, 185, 186, 118, 188, 189, 190, 134, 40, 193, 163, 195, 212, 197, 198, 228, 200, 169, 4, 203, 252, 205, 206, 172, 208, 122, 210, 174, 219, 213, 234, 215, 216, 148, 218, 196, 248, 221, 222, 144, 224, 177, 226, 214, 14, 229, 230, 207, 232, 8, 227, 235, 80, 237, 238, 30, 240, 91, 52, 243, 70, 245, 140, 247, 156, 249, 160, 251, 26, 253, 28, 255};

psi ={0, 47, 2, 87, 216, 5, 86, 13, 8, 9, 10, 11, 210, 150, 233, 50, 16, 17, 18, 19, 167, 46, 164, 91, 24, 25, 51, 27, 28, 129, 30, 107, 32, 197, 34, 35, 36, 37, 140, 244, 192, 252, 61, 120, 44, 45, 58, 155, 48, 49, 255, 154, 52, 53, 54, 55, 56, 57, 21, 77, 79, 97, 62, 41, 64, 65, 66, 67, 68, 230, 70, 71, 72, 73, 74, 75, 85, 92, 182, 195, 80, 81, 82, 83, 175, 209, 115, 166, 208, 229, 90, 174, 59, 123, 193, 136, 96, 42, 98, 99, 100, 101, 102, 103, 93, 105, 212, 237, 108, 40, 4, 111, 33, 113, 114, 6, 116, 117, 180, 119, 165, 251, 122, 104, 124, 214, 126, 29, 253, 127, 213, 22, 132, 133, 134, 135, 143, 137, 138, 149, 190, 141, 139, 95, 144, 145, 130, 147, 148, 142, 7, 151, 14, 94, 26, 1, 156, 157, 158, 159, 69, 161, 162, 78, 131, 43, 3, 219, 128, 169, 170, 171, 125, 173, 23, 189, 176, 177, 106, 179, 217, 121, 163, 183, 184, 185, 186, 187, 188, 84, 38, 191, 109, 153, 204, 60, 196, 112, 198, 199, 200, 201, 202, 203, 232, 205, 206, 207, 240, 76, 236, 211, 178, 146, 172, 225, 110, 118, 218, 20, 220, 221, 222, 223, 224, 231, 226, 227, 228, 238, 160, 215, 194, 152, 234, 235, 12, 31, 89, 239, 88, 241, 242, 243, 245, 39, 246, 247, 248, 249, 250, 181, 63, 168, 254, 15};

hi1 = {0, 171, 236, 134, 4, 5, 105, 153, 8, 9, 23, 210, 12, 25, 192, 15, 226, 17, 18, 70, 126, 158, 22, 157, 24, 77, 26, 27, 28, 166, 39, 20, 32, 33, 34, 35, 36, 37, 42, 97, 40, 41, 104, 57, 114, 45, 61, 224, 21, 49, 50, 51, 52, 234, 148, 2, 16, 131, 58, 59, 82, 180, 62, 14, 254, 11, 66, 67, 71, 74, 223, 175, 72, 193, 199, 3, 47, 13, 78, 79, 80, 81, 149, 1, 84, 85, 86, 139, 88, 89, 108, 91, 92, 93, 94, 95, 54, 30, 98, 99, 100, 101, 244, 103, 38, 246, 73, 214, 187, 109, 110, 111, 243, 113, 119, 208, 204, 117, 143, 44, 172, 121, 250, 123, 124, 218, 31, 7, 151, 129, 130, 43, 132, 133, 75, 116, 136, 137, 211, 173, 140, 141, 142, 181, 144, 145, 146, 122, 96, 60, 150, 205, 152, 127, 154, 155, 156, 10, 48, 159, 160, 161, 115, 163, 164, 165, 174, 219, 168, 169, 215, 83, 232, 87, 29, 68, 176, 177, 178, 179, 46, 118, 182, 183, 184, 185, 186, 90, 125, 189, 107, 191, 63, 106, 194, 195, 196, 197, 198, 69, 200, 201, 202, 203, 135, 128, 206, 207, 162, 167, 65, 237, 64, 213, 190, 222, 216, 53, 188, 209, 220, 221, 170, 19, 76, 102, 56, 227, 228, 229, 230, 231, 120, 233, 217, 112, 55, 138, 238, 239, 240, 241, 242, 235, 225, 245, 6, 247, 248, 249, 147, 251, 252, 253, 212, 255};

hi2 = {0, 1, 252, 124, 139, 5, 52, 7, 171, 9, 187, 11, 12, 13, 14, 180, 16, 17, 18, 65, 60, 21, 22, 42, 24, 25, 10, 27, 35, 118, 30, 57, 61, 213, 104, 170, 36, 37, 235, 72, 40, 41, 215, 43, 44, 45, 46, 47, 48, 39, 50, 51, 89, 202, 158, 55, 136, 167, 58, 59, 145, 130, 107, 163, 19, 64, 66, 191, 247, 69, 220, 71, 49, 206, 133, 75, 76, 77, 78, 79, 80, 63, 82, 83, 137, 85, 129, 87, 88, 6, 90, 188, 92, 93, 94, 62, 96, 53, 98, 254, 100, 101, 102, 103, 162, 105, 127, 95, 108, 114, 110, 197, 231, 33, 233, 70, 54, 151, 194, 119, 99, 121, 195, 123, 192, 74, 126, 185, 8, 184, 32, 131, 132, 125, 111, 135, 244, 157, 138, 221, 140, 141, 15, 143, 222, 20, 146, 147, 148, 112, 150, 153, 152, 117, 154, 144, 246, 84, 116, 159, 91, 161, 34, 81, 164, 165, 166, 31, 168, 169, 28, 128, 172, 173, 174, 175, 176, 177, 178, 179, 142, 205, 182, 183, 86, 106, 186, 26, 160, 122, 68, 219, 3, 193, 29, 189, 196, 134, 198, 199, 240, 201, 97, 203, 200, 238, 223, 207, 208, 209, 210, 211, 212, 113, 214, 23, 216, 217, 218, 67, 115, 4, 155, 73, 224, 225, 226, 227, 228, 229, 230, 149, 232, 109, 234, 242, 236, 237, 181, 239, 204, 241, 38, 243, 56, 2, 249, 190, 248, 156, 250, 251, 245, 253, 120, 255}.

Lists of maximal probabilities if differentials of substitutions that represent IXOR: $\varphi^{-1}(\psi(x) + y)$, $\varphi^{-1}(\chi_1(x) + y)$, $\varphi^{-1}(\chi_2(x) + y)$ for $y = 0, \ldots, 255$ (elements of the list are to be divided by 256).

{30, 32, 32, 38, 32, 38, 34, 34, 30, 38, 36, 32, 28, 36, 28, 32, 32, 40, 32, 34, 34, 32, 26, 40, 36, 32, 30, 36, 34, 32, 30, 40, 34, 38, 36, 32, 32, 38, 40, 32, 28, 38, 32, 34, 36, 38, 34, 34, 36, 36, 34, 32, 36, 32, 32, 42, 32, 34, 32, 34, 34, 38, 34, 36, 32, 36, 32, 36, 42, 34, 38, 38, 30, 38, 36, 36, 32, 40, 28, 38, 34, 40, 38, 34, 34, 36, 32, 32, 28, 42, 32, 32, 32, 36, 32, 34, 32, 34, 30, 40, 38, 36, 32, 42, 32, 38, 30, 30, 34, 32, 28, 42, 28, 36, 36, 38, 36, 36, 36, 34, 28, 38, 32, 38, 32, 38, 34, 32, 30, 36, 34, 32, 36, 34, 28, 36, 38, 34, 34, 34, 34, 40, 36, 34, 32, 34, 38, 34, 34, 30, 30, 36, 32, 38, 38, 28, 40, 32, 38, 42, 34, 38, 36, 38, 34, 34, 32, 36, 32, 36, 36, 32, 36, 36, 38, 38, 36, 36, 34, 34, 38, 32, 38, 42, 34, 36, 38, 30, 34, 32, 32, 34, 32, 36, 30, 34, 38, 30, 36, 40, 32, 38, 34, 38, 30, 36, 34, 34, 34, 32, 32, 36, 34, 38, 36, 34, 34, 32, 34, 32, 36, 38, 34, 34, 36, 34, 30, 36, 32, 30, 30, 36, 36, 36, 30, 40, 36, 32, 36, 36, 34, 32, 34, 34, 34, 36, 32, 38, 34, 38, 38, 36, 34, 34, 34, 34};

{34, 34, 38, 34, 34, 36, 38, 34, 40, 34, 32, 36, 30, 34, 32, 40, 34, 34, 28, 34, 34, 36, 36, 38, 32, 40, 36, 36, 36, 40, 32, 34, 36, 36, 38, 32, 34, 34, 42, 32, 40, 32, 30, 42, 34, 30, 34, 38, 36, 34, 32, 32, 36, 36, 34, 34, 36, 40, 32, 38, 32, 38, 32, 30, 32, 38, 36, 34, 38, 38, 32, 34, 36, 40, 32, 34, 38, 32, 32, 34, 36, 34, 34, 34, 38, 30, 34, 34, 30, 34, 36, 32, 34, 34, 36, 36, 34, 32, 36, 30, 38, 36, 36, 34, 38, 32, 34, 30, 36, 32, 34, 38, 38, 34, 44, 36, 36, 26, 38, 34, 34, 32, 38, 30, 38, 32, 36, 34, 32, 34, 38, 34, 32, 36, 36, 38, 36, 32, 30, 36, 32, 32, 32, 40, 34, 34, 30, 36, 36, 36, 32, 34, 36, 42, 34, 36, 34, 42, 34, 34, 30, 34, 38, 34, 34, 34, 42, 30, 36, 34, 30, 40, 38, 30, 34, 36, 36, 34, 32, 34, 34, 36, 32, 34, 38, 38, 36, 36, 36, 38, 32, 32, 34, 38, 36, 32, 38, 38, 34, 30, 36, 38, 34, 36, 38, 32, 36, 34, 32, 34, 34, 34, 42, 28, 34, 32, 34, 34, 38, 32, 36, 34, 36, 36, 34, 34, 36, 32, 40, 36, 38, 30, 38, 34, 32, 32, 36, 32, 32, 34, 40, 36, 44, 32, 38, 32, 36, 32, 34, 30, 38, 30, 36, 32, 36, 34};

{30, 28, 30, 34, 40, 28, 36, 32, 38, 34, 46, 28, 32, 34, 32, 40, 30, 46, 34, 36, 36, 38, 38, 36, 34, 36, 30, 44, 32, 36, 30, 40, 30, 40, 32, 34, 36, 38, 34, 36, 38, 30, 36, 30, 34, 38, 34, 38, 32, 36, 34, 36, 36, 28, 34, 30, 38, 32, 36, 34, 32, 36, 32, 32, 32, 34, 32, 38, 36, 36, 34, 34, 36, 38, 30, 32, 32, 36, 30, 36, 34, 36, 36, 34, 40, 32, 34, 36, 40, 34, 44, 34, 38, 36, 40, 36, 32, 38, 34, 34, 36, 34, 36, 32, 42, 36, 34, 32, 32, 38, 30, 38, 28, 34, 34, 36, 34, 36, 34, 34, 34, 36, 36, 34, 28, 38, 30, 36, 36, 28, 38, 34, 40, 34, 30, 36, 30, 34, 38, 32, 40, 32, 36, 32, 36, 38, 36, 38, 26, 44, 32, 36, 30, 36, 32, 38, 34, 38, 34, 42, 36, 36, 34, 34, 32, 34, 28, 36, 36, 38, 34, 40, 38, 38, 36, 36, 40, 32, 34, 30, 34, 36, 32, 36, 38, 36, 34, 30, 36, 28, 36, 32, 30, 38, 36, 34, 32, 36, 30, 36, 32, 34, 30, 38, 34, 36, 34, 34, 36, 36, 34, 38, 30, 34, 34, 32, 36, 38, 40, 34, 42, 30, 44, 32, 36, 30, 34, 30, 32, 38, 32, 34, 34, 36, 32, 38, 32, 38, 36, 38, 40, 34, 36, 36, 34, 38, 30, 36, 32, 36, 30, 36, 36, 32, 36, 32}.

List of minimal and maximal biases of substitutions $\varphi^{-1}(\psi(x) + y)$ for $y = 0, \ldots, 255$ (elements of the list are to be divided by 256).

{54, 48, 48, 50, 50, 50, 56, 48, 46, 52, 50, 46, 48, 46, 50, 48, 54, 54, 48, 56, 52, 44, 46, 50, 46, 48, 48, 50, 46, 48, 44, 50, 48, 52, 46, 52, 46, 52, 50, 44, 48, 50, 52, 44, 48, 50, 44, 50, 48, 46, 46, 48, 50, 50, 46, 50, 50, 50, 48, 52, 46, 50, 50, 52, 46, 50, 52, 52, 52, 48, 46, 48, 48, 50, 56, 50, 50, 48, 44, 56, 46, 54, 56, 50, 50, 52, 46, 52, 44, 54, 46, 54, 44, 48, 46, 52, 48, 52, 44, 48, 48, 52, 52, 48, 46, 50, 52, 48, 50, 48, 44, 50, 46, 52, 46, 48, 48, 52, 52, 50, 48, 52, 50, 46, 46, 48, 50, 52, 48, 50, 52, 44, 46, 50, 50, 54, 50, 50, 48, 44, 50, 48, 50, 44, 48, 50, 52, 52, 48, 46, 48, 48, 48, 54, 54, 44, 52, 48, 50, 50, 52, 50, 48, 46, 52, 44, 48, 54, 48, 50, 50, 48, 52, 48, 48, 50, 50, 50, 46, 46, 48, 48, 50, 54, 46, 58, 50, 44, 52, 50, 48, 44, 50, 52, 58, 48, 48, 46, 46, 46, 44, 50, 50, 58, 52, 50, 48, 46, 54, 44, 48, 48, 44, 50, 46, 48, 42, 46, 52, 52, 48, 52, 46, 48, 50, 44, 46, 50, 48, 44, 50, 50, 46, 50, 46, 52, 54, 50, 46, 50, 54, 52, 46, 48, 48, 50, 48, 54, 52, 50, 50, 46, 44, 50, 50, 46};

{-30, -48, -46, -58, -46, -56, -48, -54, -48, -46, -54, -44, -46, -48, -52, -48, -46, -50, -48, -50, -52, -44, -48, -50, -52, -44, -46, -50, -48, -50, -46, -50, -48, -52, -52, -46, -48, -46, -46, -48, -46, -52, -44, -48, -50, -50, -50, -50, -52, -48, -46, -56, -54, -46, -54, -50, -52, -44, -48, -50, -46, -46, -54, -46, -44, -52, -46, -50, -54, -48, -48, -52, -48, -54, -54, -46, -50, -46, -44, -52, -44, -46, -48, -48, -44, -50, -50, -48, -54, -50, -50, -48, -46, -52, -48, -50, -46, -52, -48, -56, -48, -52, -44, -50, -44, -54, -48, -52, -48, -48, -44, -50, -46, -52, -50, -48, -50, -46, -48, -50, -46, -52, -46, -48, -46, -54, -48, -50, -46, -48, -54, -46, -46, -48, -46, -50, -54, -52, -52, -48, -48, -54, -48, -46, -48, -50, -46, -48, -48, -46, -50, -50, -48, -48, -52, -48, -52, -48, -52, -46, -54, -48, -50, -44, -54, -48, -46, -50, -48, -48, -50, -48, -52, -50, -50, -56, -46, -46, -48, -50, -48, -42, -48, -50, -48, -48, -50, -46, -50, -48, -46, -52, -48, -48, -50, -54, -50, -52, -50, -50, -48, -48, -50, -54, -44, -48, -52, -46, -48, -48, -46, -50, -46, -48, -52, -50, -48, -50, -50, -48, -50, -54, -46, -50, -52, -50, -42, -54, -46, -44, -52, -52, -50, -48, -44, -56, -52, -50, -52, -50, -46, -48, -50, -48, -44, -56, -48, -50, -48, -52, -46, -50, -46, -50, -46, -48}.

List of minimal and maximal biases of substitutions $\varphi^{-1}(\chi_1(x) + y)$ for $y = 0, \ldots, 255$ (elements of the list are to be divided by 256).

{54, 46, 50, 52, 46, 54, 44, 48, 48, 46, 48, 50, 44, 48, 48, 48, 50, 50, 46, 50, 52, 54, 48, 48, 46, 52, 48, 52, 48, 50, 50, 52, 52, 46, 52, 46, 44, 50, 50, 48, 52, 40, 46, 46, 48, 52, 44, 46, 52, 46, 50, 50, 46, 46, 46, 50, 46, 52, 48, 50, 46, 52, 48, 46, 48, 50, 48, 46, 44, 48, 48, 48, 48, 46, 46, 50, 52, 48, 52, 50, 48, 46, 44, 48, 52, 50, 46, 48, 50, 48, 50, 48, 50, 54, 50, 50, 50, 58, 46, 44, 48, 50, 48, 48, 48, 46, 46, 52, 48, 46, 46, 52, 50, 52, 46, 50, 50, 46, 54, 48, 48, 52, 50, 46, 50, 50, 46, 50, 48, 50, 52, 50, 48, 48, 48, 48, 48, 50, 46, 48, 56, 50, 48, 50, 48, 46, 50, 52, 52, 48, 46, 50, 46, 50, 50, 52, 48, 52, 50, 46, 48, 50, 48, 46, 46, 48, 56, 46, 54, 46, 46, 52, 52, 46, 44, 48, 50, 48, 44, 50, 46, 52, 48, 48, 52, 48, 58, 46, 48, 50, 48, 48, 48, 48, 52, 50, 48, 48, 52, 46, 46, 52, 50, 48, 54, 48, 42, 54, 46, 48, 52, 56, 48, 44, 48, 48, 48, 50, 52, 46, 52, 48, 52, 52, 46, 46, 50, 46, 50, 50, 52, 46, 52, 44, 48, 52, 46, 46, 50, 50, 50, 44, 48, 48, 50, 54, 44, 46, 48, 46, 48, 48, 50, 46, 54, 52};

{-30, -54, -46, -52, -46, -50, -46, -56, -52, -52, -44, -48, -46, -56, -46, -46, -48, -50, -44, -50, -46, -54, -46, -48, -46, -52, -48, -48, -44, -48, -48, -54, -50, -50, -52, -46, -46, -58, -50, -46, -48, -48, -50, -50, -48, -48, -46, -50, -48, -52, -48, -52, -48, -54, -42, -54, -48, -46, -50, -52, -48, -54, -52, -48, -52, -52, -48, -46, -50, -54, -46, -44, -48, -48, -48, -50, -50, -46, -46, -50, -46, -44, -46, -48, -48, -48, -50, -50, -46, -50, -50, -44, -44, -50, -44, -48, -46, -46, -52, -48, -46, -50, -46, -48, -48, -44, -52, -48, -48, -46, -46, -52, -46, -50, -56, -48, -52, -46, -50, -46, -52, -48, -52, -50, -48, -50, -54, -48, -46, -46, -48, -50, -48, -56, -46, -48, -50, -50, -44, -46, -52, -44, -48, -50, -50, -54, -50, -48, -50, -48, -44, -54, -48, -52, -44, -48, -50, -54, -48, -50, -46, -48, -46, -46, -48, -50, -52, -46, -56, -48, -48, -50, -54, -50, -52, -

48, -48, -50, -46, -50, -52, -52, -48, -46, -48, -48, -50, -46, -50, -46, -52, -46, -50, -50, -52, -44, -50, -50, -50, -50, -48, -56, -46, -48, -46, -46, -46, -48, -46, -46, -50, -46, -48, -46, -50, -50, -48, -56, -46, -44, -48, -50, -50, -48, -48, -46, -52, -50, -54, -50, -52, -50, -48, -44, -48, -50, -56, -48, -48, -50, -52, -48, -52, -48, -50, -44, -52, -48, -52, -50, -52, -42, -54, -44, -50, -48}.

List of minimal and maximal biases of substitutions $\varphi^{-1}(\chi_2(x) + y)$ for $y = 0, \ldots, 255$ (elements of the list are to be divided by 256).

{50, 46, 48, 46, 52, 46, 48, 46, 48, 44, 50, 44, 54, 50, 52, 50, 48, 50, 46, 50, 52, 48, 50, 48, 50, 48, 48, 62, 48, 56, 44, 56, 42, 46, 50, 54, 44, 50, 46, 46, 52, 46, 50, 48, 48, 48, 46, 50, 44, 50, 52, 48, 50, 50, 50, 50, 50, 46, 50, 46, 48, 52, 48, 46, 48, 50, 46, 50, 46, 48, 50, 48, 52, 52, 48, 52, 46, 48, 48, 50, 54, 50, 50, 46, 50, 50, 50, 50, 48, 48, 58, 48, 52, 48, 52, 44, 44, 50, 54, 54, 50, 54, 52, 48, 48, 52, 48, 46, 44, 50, 46, 48, 50, 48, 50, 54, 50, 48, 50, 46, 50, 50, 50, 44, 48, 50, 48, 48, 52, 44, 50, 46, 46, 48, 44, 50, 50, 50, 50, 46, 50, 42, 52, 48, 50, 48, 46, 52, 40, 50, 52, 54, 46, 52, 46, 50, 50, 48, 46, 48, 48, 48, 50, 50, 50, 52, 48, 50, 48, 50, 50, 48, 50, 54, 44, 50, 50, 44, 54, 48, 48, 48, 44, 52, 46, 50, 48, 46, 48, 44, 48, 46, 44, 44, 50, 48, 48, 50, 48, 52, 48, 54, 46, 52, 46, 50, 50, 52, 50, 48, 46, 46, 52, 50, 50, 48, 48, 48, 50, 54, 48, 52, 46, 46, 52, 44, 48, 48, 54, 50, 48, 46, 48, 44, 50, 46, 50, 50, 50, 46, 52, 46, 46, 52, 46, 48, 50, 48, 46, 50, 44, 54, 54, 46, 50, 46};

{-32, -44, -48, -48, -54, -44, -52, -52, -48, -46, -56, -46, -48, -48, -48, -48, -46, -48, -50, -48, -46, -52, -52, -46, -54, -48, -42, -56, -46, -54, -44, -50, -44, -56, -44, -52, -50, -48, -48, -48, -50, -46, -46, -50, -48, -48, -48, -52, -46, -48, -50, -46, -58, -46, -50, -50, -50, -50, -52, -46, -50, -48, -48, -48, -48, -50, -44, -52, -48, -46, -48, -50, -48, -46, -48, -50, -48, -52, -54, -56, -50, -54, -50, -46, -52, -44, -52, -50, -48, -46, -48, -52, -48, -46, -48, -46, -42, -50, -48, -46, -50, -44, -48, -50, -54, -48, -52, -44, -48, -52, -50, -48, -48, -50, -48, -50, -54, -46, -54, -48, -48, -44, -54, -44, -52, -46, -46, -50, -50, -48, -48, -48, -50, -46, -44, -54, -48, -50, -50, -46, -52, -48, -50, -50, -52, -52, -50, -52, -44, -50, -46, -48, -56, -48, -46, -52, -48, -46, -48, -48, -48, -48, -48, -46, -46, -50, -52, -52, -46, -50, -50, -50, -48, -46, -48, -50, -50, -46, -48, -48, -48, -50, -46, -50, -46, -48, -46, -52, -48, -48, -50, -52, -58, -54, -50, -48, -54, -50, -48, -50, -46, -50, -46, -56, -48, -52, -46, -44, -50, -48, -50, -48, -46, -52, -52, -48, -52, -48, -50, -46, -50, -54, -58, -52, -52, -48, -48, -48, -46, -52, -46, -48, -50, -50, -46, -50, -46, -46, -48, -50, -48, -48, -48, -48, -48, -52, -44, -52, -46, -48, -46, -48, -54, -48, -46, -44}.