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

AES-like ciphers: are special S-boxes better then random ones? (Virtual isomorphisms again)

In [eprint.iacr.org/2012/663] method of virtual isomorphisms of ciphers was applied for differential/linear cryptanalysis of AES. It was shown that AES seems to be weak against those attacks. That result can be generalized to AES-like ciphers, which diffusion map is a block matrix, and its block size is the same as the S-box size. S-box is possibly weak if it is affine equivalent to a substitution that has the same cycling type as an affine substitution. Class of possibly weak S-boxes is very large; we do not know is there an S-box that is not possibly weak. Strength of AES-like cipher is defined by virtual isomorphism and not by differential/linear properties of the S-box. So we can assume that special S-boxes have little or no advantage comparatively to random nonlinear S-boxes. The conjecture is verified by experiments. If the conjecture is true, then search of the best S-boxes that maximizes the cipher strength against differential and linear attacks joined with virtual isomorphisms has no sense.

1. Introduction

In [10] method of virtual isomorphisms of ciphers was proposed for changing the probabilities of differentials and linear sums and for amplifying cryptanalytic attacks. Ciphers $y = C(x, k)$ and $\mathfrak{y} = \mathfrak{C}(\mathfrak{x}, \mathfrak{k})$ are isomorphic if there exists an computable in both directions bijection $y \leftrightarrow \mathfrak{y}$, $x \leftrightarrow \mathfrak{x}$, $k \leftrightarrow \mathfrak{k}$, $C \leftrightarrow \mathfrak{C}$. Usually cipher C is the real one. But family of its isomorphic images $\mathfrak{C}$ is virtual; it exists in imagine of cryptanalyst.

Next theorem was proved in [10] 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.

Theorem 1 establishes a new approach to cryptanalysis. Usually cryptanalyst searches a new cryptanalytic method that allows decreasing the strength of the cipher (known attacks are ineffective usually for modern ciphers). But now cryptanalyst can apply the known lovely cryptanalytic attack to arbitrary cipher. It is sufficient to find suitable virtual isomorphism such that isomorphic cipher becomes vulnerable to the cryptanalytic attack. Since the number of virtual isomorphisms is extremely large, there is a good chance of success.

In [11] family of virtual isomorphisms of AES was proposed for amplifying differential and linear attacks. AES uses S-box based on finite field inversion T,

which is (with small error) conjugated to the least bit inversion map $\mathfrak{T} = \varphi^{-1}T\varphi$ for auxiliary substitution φ. Let IAES is isomorphic image of AES. In such a way we can obtain next properties of IAES:

1. Isomorphic image $\mathfrak{T}$ of substitution T is affine.
2. Images of diffusion map acting on bytes are affine.
3. The only non-linear map of IAES is IXOR - the image of XOR of 4 bytes of text and the key byte. IXOR is weak map comparatively to initial substitution S.

The most popular cryptanalytic methods are linear [7] and differential [2] that take a large number of known plaintext/ciphertext pairs, and algebraic methods [4, 5, 9], based on solving systems of polynomial equations that take only one or few plaintext/ciphertext pairs. 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 and probability $P(f = 0)$ is 0.5. 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 $P(f = 0) - 0{,}5$ is the bias of substitution. Diffusion maps are usually affine and do not change absolute biases of linear sums.

Linear cryptanalysis looks for linear sums of plaintext, ciphertext and key (and possibly intermediate texts) bits with maximal absolute biases [6]. 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) have 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 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.

Virtual isomorphisms of AES significantly increase probabilities of most likely differentials and biases of linear sums. So the strength of IAES (and hence the strength of AES) to differential and linear attacks seems to be about the square root of corresponding known strength [11].

This is because S-box of AES is weak, and the strength of AES is determined by properties of virtual isomorphism but no by differential and linear properties of the S-box.

This result can be generalized to a family of AES-like ciphers. This family has very large class of possibly weak substitutions (the strength of the cipher with such S-box is determined by proper virtual isomorphism). There is no known algorithm that recognizes possibly weak S-boxes and we do not know does there exist S-box that is not possibly weak. So we can assume that special S-boxes do not increase the strength of such a cipher comparatively to random S-box.

Number of virtual isomorphisms substantially exceeds the number of different keys. This makes the recognition the best of two given S-boxes (or diffusion maps, ciphers) practically impossible.

2. Brief consideration of virtual isomorphisms of AES

This section is based on materials [8, 11].

Standard AES has 10, 12 or 14 rounds, block size is 128 bits, key size is 128, 192 or 256 bits [8]. 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 absolute 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.

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.

Denote T as exponentiation $x \to x^{254}$ in $\mathbb{F}_{256}$. Farther we will decompose AES substitution $S = MT$ 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 $M_{t1} = L_{t1}M$.

Substitution T consists of 127 cycles of length 2 and two cycles of length 1. Hence it is a conjugate with affine substitution $\mathfrak{T}$ defined as the lowest bit inversion, $\mathfrak{T} = \varphi^{-1}T\varphi$ (there exists small error, but it does not change the strength). We can take arbitrary $\varphi(x_0)$ for given x_0 – 256 variants - and compute $\varphi^{-1}(x_0)$. Then take next x_1 and arbitrary $\varphi(x_1)$ – 254 variants - and compute unique $\varphi^{-1}(x_1)$, etc. The number of such φ is near to $\sqrt{256!} = 3 \cdot 10^{253}$, because for any $\varphi(x_i)$ there is unique $\varphi^{-1}(x_i)$.

It is useful to find such φ that has many fixed points. Substitution φ can be easily computed using orbits of elements under action of group $\langle T, \mathfrak{T} \rangle$ so that φ does not change the orbits: $\langle T, \mathfrak{T} \rangle = \langle T, \mathfrak{T}, \varphi \rangle$. We can chose the fixed points of φ as odd or even points of the orbit written as the cycle $(x, T(x), \mathfrak{T}T(x), T\mathfrak{T}T(x), \ldots)$. Maximal number of fixed points of φ is 130. There exist 2^{42} substitutions φ with 130 fixed points.

Choose virtual isomorphism using three additional auxiliary substitutions ψ, χ_1, χ_2 in such a way that images of byte diffusion maps are the identity maps E[1]:

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

Let IAES is the isomorphic image of AES. If φ is known, then wanted substitutions ψ, χ_1, χ_2 exist and are defined uniquely, and φ, ψ, χ_1, χ_2 are affine equivalent each other. Experiments show that if φ, $\mathfrak{M}$, $\mathfrak{M}_t$, $\mathfrak{M}_{t1}$ are changed (but three last substitutions stay affine), then probabilities of most likely differentials and linear sums of IXOR stay approximately the same.

IAES has only one nonlinear operation, namely the image IXOR of XOR for 5 byte summands as the isomorphic image of sum determined by diffusion matrix:

$$\varphi^{-1}(\psi(x_1) + \psi(x_2) + \chi_1(x_3) + \chi_2(x_4) + \varphi(k)).$$

IXOR seems to be weak operation: probabilities of its byte differentials and linear sums are large comparatively to initial substitution S. There exist differentials with non-zero input and zero output of probability 1. The probability of most likely differential of IXOR considered with respect to one summand $\varphi^{-1}(\psi(x) + y)$, $\varphi^{-1}(\chi_1(x) + y)$, $\varphi^{-1}(\chi_2(x) + y)$ is increased by 8.7 times at average (y is changed from 0 to 255) comparatively to differentials of S. The absolute bias of linear sums of IXOR considered with respect to one summand is increased by 3.1 times at average.

The error determined by small difference of cycling types of T and $\mathfrak{T}$ can be deleted if we use quasi-affine substitution $\mathfrak{T}$, its lowest bit is given by equation

$$y_8 = 1 + x_8 + (1 + x_1)\ldots(1 + x_7).$$

This correction does not change probabilities of most likely differentials (linear sums) of the cipher maps and hence it does not significantly change the strength of the cipher.

We can assume that strength of IAES against differential (linear) attacks does not exceed a square root of the known corresponding estimations [11]. Computing the "large" differentials and linear sums of IXOR with four byte input and one byte output will obviously increment the probabilities of most likely differentials and linear sums and hence additionally decrease the strength.

[1] In [11] isomorphic images of byte diffusion map $\mathfrak{M}$, $\mathfrak{M}_t$, $\mathfrak{M}_{t1}$ were the same as in original AES. Changing the byte substitutions $\mathfrak{M}$, $\mathfrak{M}_t$, $\mathfrak{M}_{t1}$ by identity map gives approximately the same maximal probabilities of differentials and linear sums as in [11], but it looks more common for developing algebraic attacks based on virtual isomorphism technique, because it minimizes the lengths of corresponding affine polynomials.

3. Generalization to AES-like ciphers

The strength of IAES (and hence the strength of original AES) is reduced because its S-box S is weak: S is affine equivalent to substitution T that has the same cycling type as the affine substitution $\mathcal{T}$. The strength of AES is determined by the used virtual isomorphism (φ, ψ, χ_1, χ_2), but not by differential and linear properties of the S-box.

Virtual isomorphisms are not equivalences because transitivity does not necessary hold. Equivalence partitions the set o cipher into disjoint subsets, but virtual isomorphisms partition the set of ciphers into fuzzy subsets.

Define *AES-like cipher* as a cipher that uses next operations: XOR of text and the round key; fixed nonlinear substitution S; linear diffusion map that is given by block matrix, the size of the block of the matrix is a multiple of the size of input/output of substitution S.

Usually special S-boxes are used in block ciphers (including AES-like ciphers). Such S-boxes satisfy some specific requirements (strict avalanche criterion, probabilities of most likely differentials and maximal absolute biases of linear sums are to be as small as possible, etc.).

Define *possibly weak substitution* (*S-box*) as substitution S that is affine equivalent to some substitution S' such that S' has the same or near the same cycling type as some affine substitution.

Remember that substitutions S_1, S_2 are affine equivalent iff there exist affine substitutions A, B such that $S_1 = AS_2B$ [3]. Affine equivalent substitutions have the same probabilities of most likely differentials and linear sums.AES substitution is affine equivalent to lowest bit inversion and hence it is possibly weak.

Generally affine equivalence between the affine equivalent nonlinear substitutions is defined by few pairs (A, B). The number of such pairs usually is small comparatively to the cardinality of the set of affine substitutions. So we can briefly estimate the number of substitutions that are affine equivalent to given nonlinear substitution, as square of number of affine substitutions.

Number of different possible cycling types of substitution S coincides with the number of partitions of integer 2^n, where n is the size of input/output of S. Wikipedia claims that the number of partitions of an integer is determined asymptotically by the subexponent [12].

If $n = 8$, then the number of partitions is $3.7 \cdot 10^{14}$. Number of affine substitutions is $1.3 \cdot 10^{21}$, its square is $1.7 \cdot 10^{42}$. If $n = 4$, then number of partitions is 257, number of affine substitutions is $3.2 \cdot 10^5$, its square is 10^{11}.

Number of affine equivalent substitutions for given initial substitution is much more then the number of possible cycling types of substitutions. So we can assume that all or almost all substitutions are possibly weak in practice. There is no known algorithm that recognizes whether the tested substitution is possibly weak. Also we do not know anything on existence of a substitution that is not possibly weak.

AES-like ciphers possess a large class of possibly weak S-boxes. The strength of a cipher with such S-box against differential and linear attacks is defined by suitable virtual isomorphism. Notice that differential and linear properties of the S-box are not used directly in corresponding attack. Maximal probabilities of byte differentials and linear sums of IXOR described in previous section and in [11] significantly exceed corresponding probabilities of "random" byte substitution. So if virtual isomorphism is computed carefully, then the strength of AES-like cipher with randomly changed substitution will be approximately the same as the cipher strength when special S-box is used. This shows that the strength of the AES-like cipher depends on the S-box in a weak form.

Hence we can assume that next conjectures have large chances to be true for AES-like ciphers:

Conjecture 1.

1. The strength of a cipher with special S-box is approximately the same as the strength of the cipher with random S-box and the same diffusion map and key schedule.
2. Special S-boxes have little or no advantage comparatively to random S-boxes at average.[2]

Of course, we consider only nonlinear random substitutions.

Virtual isomorphisms depend on the S-box of the cipher indeed. But probabilities of differentials, linear sums of non-linear map of isomorphic cipher seem to be independent of probabilities of differentials and linear sums of the S-box. Moreover, experiments show that the strength of isomorphic cipher (with special or random S-boxes) is less than the strength of original cipher both for special and random S-boxes.

Those conjectures are verified by experiment. Properties of AES with initial S-box and with the random S-box are compared in the appendix. It is shown that the strengths of isomorphic images of those ciphers (and hence the strengths of the ciphers) are approximately the same. Notice that probabilities of most likely differentials of nonlinear map of isomorphic image of AES with random S-box stay more than probabilities of most likely differentials of the S-box. The similar is true for original AES, of course.

Generally the class of virtual isomorphisms of AES-like ciphers can be determined by other equations, different from conjugation. Also virtual isomorphisms can change from one round to another. This will increase the set of weak isomorphic images of the initial cipher and can decrease its strength.

Any block cipher has the key-dependent map. Usually it is the XOR of the text and the round key. But sometimes that operation is different from XOR, for example in GOST and IDEA.

It is widely known that the designer of the cipher or cryptanalyst gives the most attention to properties of its S-box. S-box is considered as the most important

[2]Hence we can formulate Murphy law for cryptography: any good-looking S-box becomes weak when cipher is studied carefully.

encryption operator and it is selected so that it satisfies some special requirements. The practical utility of special S-boxes is based on belief that such S-boxes indeed increase the strength of a cipher at least against linear and differential attacks.

The matter of this report shows that if conjecture 1 is true, then we cannot recognize which of two S-boxes (excepting few obviously weak cases) appreciably increases the strength against differential and linear attacks joined with virtual isomorphisms technique. Hence we need not compute “the best possible S-box”, almost all S-boxes provide almost the same strength. The proof of those statements follows from next states: the key cardinality is much less then the number of virtual isomorphisms; comparing of two virtual isomorphisms has non-zero complexity; we cannot recognize whether given nonlinear S-box is not possibly weak; almost all nonlinear S-boxes provide the same strength.

The matter of this report shows also that the diffusion map and the key-dependent map of the block cipher have at least the same significance as the S-box.

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. 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.
3. 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.
4. N. Courtois and J. Pieprzyk. Cryptanalysis of block ciphers with overdefined systems of equations // International Association for Cryptologic Research. Cryptology e-print archive, http://eprint.iacr.org/2002/044.
5. J.-C. Faugere. Groebner bases. Applications in cryptology. Invited talk at FSE-07 in Luxemburg. Available at http://fse2007.uni.lu/slides/faugere.
6. H. Heyes and S. Tavares. Substitution-permutation networks resistant to differential and linear cryptanalysis // Journal of cryptology, 1996, v. 9, pp. 1–19.
7. M. Matsui. Linear cryptanalysis method for DES cipher. // Advances in Cryptology — EUROCRYPT ′93, LNCS, v. 765, 1994, pp. 386–397.
8. NIST: Advanced encryption standard (AES), FIPS 197. Technical report, NIST (November, 2001).
9. 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.

10. A. Rostovtsev**.** Changing probabilities of differentials and linear sums via isomorphisms of ciphers // International Association for Cryptologic Research. Cryptology e-print archive, http://eprint.iacr.org/2009/117.
11. A. Rostovtsev**.** Virtual isomorphisms of ciphers: is AES secure against differential / linear attack? // International Association for Cryptologic Research. Cryptology e-print archive, http://eprint.iacr.org/2012/663.
12. Wikipedia, the free encyclopedia. Partition (number theory) // en.wikipedia.org/wiki/Partition_(number theory).

Appendix

Comparison of isomorphic images of the original AES and of the AES with random S-box

Let RAES is the AES with random substitution and IRAES is its isomorphic image. We choose S-box of RAES so that finite field inversion was changed by random substitution that has all cycles of length 2.

Let T, T' are substitutions of AES, RAES that have cycles only of length 2. Let φ', ψ', χ_1', χ_2' are auxiliary byte substitutions that define virtual isomorphism of RAES with the same equations as the isomorphism of AES described in section 2.

T = {0, 1, 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}.

T' = {218, 202, 92, 30, 235, 245, 211, 247, 18, 169, 33, 95, 148, 194, 45, 237, 93, 184, 8, 214, 129, 225, 139, 243, 188, 220, 175, 150, 73, 198, 3, 116, 248, 10, 190, 58, 210, 39, 67, 37, 43, 223, 182, 40, 231, 14, 74, 104, 159, 86, 119, 174, 98, 65, 201, 124, 115, 200, 35, 251, 69, 170, 206, 192, 96, 53, 163, 38, 101, 60, 180, 136, 195, 28, 46, 193, 87, 213, 172, 152, 81, 80, 191, 147, 255, 222, 49, 76, 209, 105, 100, 217, 2, 16, 177, 11, 64, 185, 52, 196, 90, 68, 158, 109, 47, 89, 132, 239, 120, 103, 215, 249, 230, 203, 212, 56, 31, 233, 228, 50, 108, 128, 125, 219, 55, 122, 173, 241, 121, 20, 240, 140, 106, 236, 151, 199, 71, 232, 227, 22, 131, 178, 183, 242, 164, 252, 168, 83, 12, 234, 27, 134, 79, 224, 167, 162, 244, 205, 102, 48, 186, 250, 155, 66, 144, 254, 208, 154, 146, 9, 61, 197, 78, 126, 51, 26, 181, 94, 141, 189, 70, 176, 42, 142, 17, 97, 160, 226, 24, 179, 34, 82, 63, 75, 13, 72, 99, 171, 29, 135, 57, 54, 1, 113, 216, 157, 62, 229, 166, 88, 36, 6, 114, 77, 19, 110, 204, 91, 0, 123, 25, 238, 85, 41, 153, 21, 187, 138, 118, 207, 112, 44, 137, 117, 149, 4, 133, 15, 221, 107, 130, 127, 143, 23, 156, 5, 253, 7, 32, 111, 161, 59, 145, 246, 165, 84}.

Non-zero most likely differentials of T have probability 4/256. The most likely differentials of substitution T' for non-zero inputs 0, 1, 2, …, 255 have next probabilities (multiplied by 256):

{256, 6, 6, 8, 6, 6, 10, 10, 8, 8, 10, 6, 6, 6, 6, 10, 6, 6, 8, 8, 8, 8, 8, 8, 8, 8, 8, 8, 10, 6, 8, 10, 6, 6, 8, 6, 6, 6, 6, 6, 8, 8, 10, 6, 6, 6, 8, 8, 8, 6, 8, 6, 6, 6, 6, 6, 8, 6, 6, 6, 6, 8, 6, 6, 12, 6, 10, 6, 6, 6, 6, 10, 6, 6, 8, 8, 6, 10, 6, 8, 6, 6, 8, 10, 6, 6, 6, 6, 6, 6, 8, 8, 8, 6, 6, 8, 10, 6, 6, 6, 6, 6, 6, 6, 6, 6, 6, 8, 10, 8, 6, 8, 8, 10, 6, 6, 10, 6, 6, 8, 6, 8, 6, 6, 8, 8, 6, 6, 8, 8, 8, 8, 6, 8, 6, 6, 8, 6, 8, 6, 6, 6, 8, 4, 6, 10, 8, 6, 6, 8, 8, 6, 8, 6, 8, 6, 8, 6, 6, 6, 8, 6, 6, 6, 6, 10, 6, 6, 8, 6, 6, 10, 6, 6, 6, 6, 6, 6, 6, 6, 6, 6, 6, 8, 4, 8, 4, 6, 6, 6, 6, 6, 6, 6, 4, 6, 10, 6, 6, 6, 6, 6, 12, 6, 6, 6, 8, 6, 8, 6, 8, 8, 10, 6, 6, 8, 6, 8, 8, 6, 6, 6, 8, 6, 8, 6, 6, 8, 8, 6, 6, 10, 6, 6, 6, 6, 6, 10, 10, 6, 10, 8, 8, 6, 6, 8, 6, 6, 10, 6, 6, 6, 8, 6, 6}.

Maximal absolute biases of T are 16/256. Maximal positive and negative biases of T' for input linear sums 0, 1, …, 255 are

{128, 22, 22, 22, 24, 20, 22, 22, 24, 32, 20, 20, 22, 22, 24, 24, 22, 22, 24, 24, 24, 22, 20, 22, 20, 22, 24, 24, 22, 22, 22, 22, 28, 20, 22, 22, 18, 24, 20, 20, 24, 18, 24, 26, 18, 28, 22, 24, 22, 22, 26, 22, 24, 24, 22, 22, 22, 24, 22, 22, 20, 34, 24, 24, 24, 24, 22, 20, 22, 20, 22, 26, 28, 20, 22, 28, 24, 26, 22, 22, 22, 22, 22, 20, 24, 24, 22, 20, 38, 26, 22, 22, 20, 24, 30, 22, 20, 22, 22, 24, 22, 16, 22, 24, 24, 20, 18, 28, 24, 28, 22, 24, 18, 28, 20, 22, 24, 20, 22, 22, 26, 22, 22, 28, 24, 22, 24, 20, 24, 26, 20, 26, 20, 22, 20, 24, 26, 22, 22, 24, 24, 22, 26, 18, 22, 24, 20, 22, 22, 28, 24, 20, 22, 20, 22, 22, 22, 22, 18, 20, 18, 20, 24, 28, 24, 20, 20, 24, 22, 22, 20, 28, 24, 26, 22, 34, 22, 28, 22, 24, 22, 20, 22, 22, 26, 28, 24, 20, 20, 24, 22, 28, 24, 20, 26, 18, 20, 18, 22, 20, 22, 26, 24, 22, 24, 22, 28, 22, 18, 22, 24, 20, 24, 30, 22, 24, 24, 18, 22, 24, 22, 22, 22, 20, 28, 24, 20, 18, 22, 22, 22, 24, 20, 22, 24, 18, 24, 22, 24, 26, 24, 20, 24, 22, 22, 18, 24, 22, 24, 24, 20, 22, 24, 24, 38, 18};

{0, -20, -22, -24, -20, -18, -26, -26, -22, -22, -28, -22, -16, -22, -22, -22, -26, -20, -22, -22, -24, -28, -20, -20, -22, -32, -22, -22, -22, -18, -20, -20, -24, -24, -28, -18, -22, -24, -28, -24, -22, -20, -22, -22, -20, -24, -22, -28, -24, -24, -26, -20, -26, -22, -18, -32, -22, -20, -26, -22, -22, -20, -22, -20, -22, -18, -24, -18, -24, -26, -26, -26, -20, -22, -30, -22, -22, -20, -22, -24, -26, -22, -26, -22, -20, -22, -24, -26, -20, -22, -20, -20, -22, -24, -20, -28, -20, -24, -26, -22, -26, -24, -24, -24, -20, -20, -22, -28, -22, -20, -24, -20, -26, -22, -20, -22, -18, -20, -22, -24, -20, -28, -24, -26, -20, -22, -26, -20, -22, -20, -24, -24, -24, -22, -22, -18, -22, -22, -30, -24, -22, -22, -26, -28, -20, -26, -22, -24, -20, -24, -22, -28, -22, -36, -22, -24, -22, -20, -20, -22, -22, -18, -28, -18, -24, -22, -22, -24, -16, -20, -22, -22, -20, -20, -28, -20, -22, -32, -26, -28, -20, -18, -22, -22, -20, -18, -28, -22, -24, -20, -20, -18, -18, -18, -22, -22, -20, -22, -26, -18, -24, -20, -18, -28, -22, -24, -18, -22, -22, -24, -26, -26, -20, -26, -24, -20, -22, -22, -28, -26, -24, -20, -28, -28, -18, -18, -28, -22, -22, -20, -20, -26, -22, -24, -26, -20, -24, -22, -20, -20, -20, -20, -22, -24, -26, -22, -20, -28, -32, -20, -24, -18, -22, -20, -28, -22}.

$\mathfrak{T} = \mathfrak{T}'$ are the lowest bit inversion substitutions. Orbits of group $\langle T, \mathfrak{T} \rangle$ have length 2 (2 orbits) or 6 (42 orbits). Orbits of group $\langle T', \mathfrak{T}' \rangle$ have length 2 (1 orbit), 78 (1 orbit), 176 (1 orbit). Auxiliary substitution φ has 130 fixed points. Auxiliary substitution φ′ of RAES has 129 fixed points. Next auxiliary substitutions were used.

φ = {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}.

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

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

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

χ_1 = {177, 62, 61, 161, 181, 0, 226, 159, 128, 66, 149, 221, 235, 124, 187, 227, 193, 198, 190, 89, 44, 248, 120, 103, 234, 186, 215, 37, 210, 132, 96, 27, 254, 207, 19, 80, 31, 241, 102, 110, 82, 179, 163, 114, 236, 141, 10, 18, 184, 2, 97, 168, 75, 9, 77, 150, 196, 3, 91, 64, 147, 117, 101, 217, 65, 93, 13, 194, 55, 99, 208, 252, 29, 33, 49, 107, 144, 20, 15, 151, 104, 165, 118, 58, 126, 155, 173, 4, 86, 53, 201, 223, 38, 231, 247, 172, 35, 232, 125, 51, 166, 146, 130, 25, 95, 162, 63, 79, 30, 238, 212, 113, 209, 84, 71, 203, 229, 73, 250, 245, 219, 40, 16, 183, 127, 22, 105, 137, 6, 121, 246, 230, 200, 175, 139, 216, 211, 5, 158, 154, 46, 59, 57, 164, 192, 129, 145, 39, 21, 191, 68, 32, 119, 253, 138, 98, 47, 195, 237, 92, 153, 136, 152, 157, 131, 182, 174, 41, 123, 225, 228, 214, 74, 202, 188, 85, 255, 243, 54, 239, 106, 78, 94, 167, 43, 12, 28, 122, 189, 50, 34, 87, 60, 26, 23, 133, 83, 36, 52, 90, 233, 244, 143, 249, 222, 88, 72, 69, 109, 56, 242, 218, 1, 220, 135, 67, 17, 48, 142, 171, 224, 160, 176, 14, 100, 112, 251, 204, 108, 213, 197, 199, 24, 205, 116, 8, 42, 169, 185, 148, 156, 70, 134, 140, 115, 45, 180, 178, 76, 111, 7, 240, 170, 81, 11, 206}.

χ_1' = {177, 142, 46, 104, 143, 8, 178, 159, 205, 214, 120, 221, 10, 124, 108, 141, 131, 198, 204, 89, 235, 248, 232, 154, 47, 186, 170, 85, 52, 132, 148, 161, 82, 207, 223, 34, 126, 242, 241, 110, 60, 44, 163, 94, 2, 74, 95, 18, 184, 92, 39, 245, 134, 188, 25, 102, 196, 203, 91, 80, 250, 99, 149, 234, 9, 93, 225, 194, 236, 146, 138, 252, 11, 33, 49, 157, 144, 4, 15, 69, 42, 165, 30, 58, 176, 155, 139, 55, 86, 226, 158, 70, 73, 231, 247, 112, 35, 210, 171, 51, 29, 201, 238, 13, 217, 208, 192, 200, 97, 167, 111, 113, 249, 84, 68, 83, 229, 27, 122, 90, 246, 40, 56, 22, 153, 150, 19, 137, 119, 121, 180, 230, 38, 71, 87, 32, 24, 5, 21, 116, 96, 59, 3, 164, 14, 57, 145, 123, 48, 243, 175, 37, 114, 128, 152, 98, 76, 162, 211, 130, 127, 136, 77, 23, 65, 182, 237, 41, 66, 244, 228, 117, 6, 202, 218, 168, 255, 78, 50, 239, 193, 115, 43, 209, 172, 12, 28, 7, 189, 53, 181, 173, 190, 26, 174, 133, 107, 36, 216, 187, 233, 75, 118, 62, 195, 88, 72, 101, 109, 166, 16, 125, 31, 220, 254, 67, 17, 215, 183, 1, 185, 160, 179, 63, 100, 253, 251, 147, 199, 213, 197, 219, 106, 151, 135, 191, 227, 169, 79, 54, 156, 105, 103, 140, 0, 45, 61, 81, 224, 64, 212, 240, 222, 129, 20, 206}.

χ_2 = {210, 66, 70, 227, 222, 0, 39, 161, 129, 198, 190, 103, 60, 132, 205, 37, 67, 75, 195, 234, 117, 9, 136, 168, 62, 207, 120, 110, 118, 141, 160, 44, 3, 80, 53, 241, 32, 18, 170, 179, 247, 212, 229, 151, 52, 150, 31, 55, 201, 6, 162, 248, 221, 27, 215, 186, 77, 4, 236, 192, 180, 159, 174, 107, 194, 230, 23, 71, 89, 164, 112, 5, 38, 98, 83, 189, 176, 61, 17, 184, 185, 239, 155, 78, 130, 173, 246, 12, 251, 95, 90, 97, 106, 41, 24, 244, 100, 56, 134, 85, 235, 182, 135, 42, 224, 231, 64, 209, 34, 50, 124, 147, 114, 253, 200, 92, 47, 219, 15, 30, 109, 121, 49, 216, 128, 59, 187, 154, 10, 138, 26, 43, 88, 240, 156, 105, 116, 14, 163, 175, 115, 76, 74, 237, 65, 131, 178, 104, 63, 193, 204, 96, 153, 7, 158, 166, 113, 69, 54, 228, 171, 152, 169, 167, 133, 218, 242, 123, 140, 35, 45, 122, 223, 94, 197, 255, 1, 20, 91, 48, 191, 211, 226, 233, 125, 21, 36, 142, 199, 87, 102, 249, 68, 46, 57, 143, 245, 108, 93, 238, 58, 28, 144, 11, 99, 232, 217, 206, 183, 72, 22, 111, 2, 101, 137, 196, 51, 81, 146, 252, 33, 225, 208, 19, 172, 145, 13, 84, 181, 126, 79, 73, 40, 86, 157, 25, 127, 250, 203, 188, 165, 202, 139, 148, 149, 119, 220, 214, 213, 177, 8, 16, 254, 243, 29, 82}.

χ_2' = {210, 146, 115, 185, 144, 25, 214, 161, 86, 122, 136, 103, 31, 132, 181, 150, 133, 75, 84, 234, 60, 9, 56, 175, 113, 207, 254, 255, 93, 141, 188, 227, 247, 80, 97, 102, 130, 22, 18, 179, 68, 117, 229, 226, 6, 223, 224, 55, 201, 228, 104, 30, 139, 197, 42, 170, 77, 92, 236, 241, 15, 164, 190, 62, 27, 230, 35, 71, 52, 182, 158, 5, 29, 98, 83, 167, 176, 12, 17, 206, 127, 239, 34, 78, 208, 173, 156, 89, 251, 39, 163, 202, 219, 41, 24, 145, 100, 118, 252, 85, 38, 90, 50, 23, 107, 112, 65, 88, 162, 233, 177, 147, 11, 253, 204, 245, 47, 44, 142, 238, 26, 121, 72, 59, 171, 186, 53, 154, 153, 138, 220, 43, 106, 200, 249, 96, 40, 14, 63, 157, 160, 76, 4, 237, 19, 74, 178, 140, 81, 20, 240, 110, 151, 129, 169, 166, 213, 231, 116, 135, 128, 152, 215, 57, 194, 218, 54, 123, 198, 28, 45, 159, 10, 94, 111, 248, 1, 211, 87, 48, 67, 149, 125, 114, 244, 21, 36, 8, 199, 95, 222, 246, 195, 46, 242, 143, 189, 108, 105, 205, 58, 221, 155, 66, 69, 232, 217, 174, 183, 235, 49, 134, 32, 101, 3, 196, 51, 120, 216, 2, 203, 225, 212, 64, 172, 7, 13, 180, 73, 126, 79, 109, 191, 184, 137, 193, 37, 250, 209, 91, 165, 187, 168, 148, 0, 119, 70, 243, 33, 192, 124, 16, 99, 131, 61, 82}.

Probabilities of most likely differentials of non-linear map of IAES of kind $\varphi^{-1}(\psi(x) + y)$ for $y = 0, 1, \ldots, 255$ are (after multiplying 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}.

Probabilities of most likely differentials of non-linear map of IRAES of kind $\varphi'^{-1}(\psi'(x) + y)$ for $y = 0, 1, \ldots, 255$ are (after multiplying by 256):

{38, 28, 30, 32, 42, 30, 28, 36, 22, 36, 40, 28, 30, 34, 30, 28, 30, 30, 30, 32, 36, 30, 30, 40, 30, 38, 38, 28, 34, 28, 38, 28, 32, 36, 32, 32, 30, 38, 32, 30, 40, 24, 24, 38, 34, 30, 32, 34, 32, 34, 38, 32, 26, 40, 42, 28, 34, 30, 24, 42, 30, 30, 30, 30, 32, 36, 36, 30, 34, 28, 34, 34, 36, 32, 30, 34, 40, 26, 28, 36, 30, 36, 36, 28, 34, 38, 30, 34, 30, 38, 34, 30, 36, 28, 28, 44, 34, 32, 30, 40, 30, 34, 34, 36, 28, 34, 32, 30, 30, 36, 34, 28, 36, 36, 26, 34, 38, 34, 30, 34, 32, 34,

36, 34, 28, 36, 36, 26, 30, 34, 38, 28, 34, 36, 28, 36, 32, 32, 32, 28, 36, 28, 26, 36, 28, 40, 36, 30, 30, 34, 30, 32, 30, 38, 34, 30, 40, 26, 26, 38, 40, 24, 28, 40, 32, 30, 32, 34, 30, 34, 32, 34, 28, 36, 38, 26, 34, 28, 30, 34, 32, 34, 30, 34, 30, 30, 32, 34, 28, 38, 40, 28, 32, 32, 30, 32, 36, 30, 28, 40, 28, 40, 36, 26, 36, 28, 32, 34, 34, 32, 40, 34, 42, 28, 36, 36, 24, 36, 36, 30, 32, 32, 30, 34, 38, 28, 32, 32, 28, 36, 40, 28, 34, 28, 24, 42, 30, 38, 32, 32, 32, 30, 26, 36, 24, 40, 38, 28, 38, 26, 26, 36, 32, 30, 40, 30}.

At average maximal probabilities of most likely differentials for random y are approximately equal both for AES and RAES (0.134 for IAES and 0.127 for IRAES). Similar is true for other byte differences $\varphi^{-1}(\chi_1(x) + y)$, $\varphi^{-1}(\chi_2(x) + y)$ for AES and RAES.

Similarly maximal absolute biases of nonlinear byte maps of IAES and of IRAES are approximately the same at average for random y (0.194 for IRAES and 0.191 for IAES).

If we change the random substitution T' of RAES, then probabilities of differentials and linear sums of T' obviously change too, but maximal probabilities of differentials and linear sums of IXOR for IRAES are almost the same as for IAES. Hence the strengths of AES and RAES against differential (linear) attack using virtual isomorphism technique are near the same, and special S-box of AES is not better than random S-box of RAES with respect to differential (linear) attack.