A New Encryption Standard of Ukraine: The Kalyna Block Cipher

Roman Oliynykov[1], Ivan Gorbenko[1], Oleksandr Kazymyrov[4], Victor Ruzhentsev[4], Oleksandr Kuznetsov[3], Yurii Gorbenko[1], Oleksandr Dyrda[2], Viktor Dolgov[3], Andrii Pushkaryov[2], Ruslan Mordvinov[4], Dmytro Kaidalov[4]

[1] JSC Institute of Information Technologies,

[2] State Service of Special Communication and Information Protection of Ukraine,

[3] V.N.Karazin Kharkiv National University,

[4] Kharkiv National University of Radio Electronics

Ukraine

roliynykov@gmail.com, gorbenkoi@iit.kharkov.ua, okazymyrov@gmail.com

Abstract

The Kalyna block cipher was selected during Ukrainian National Public Cryptographic Competition (2007-2010) and its slight modification was approved as the new encryption standard of Ukraine in 2015. Main requirements for Kalyna were both high security level and high performance of software implementation on general-purpose 64-bit CPUs. The cipher has SPN-based (Rijndael-like) structure with increased MDS matrix size, a new set of four different S-boxes, pre- and postwhitening using modulo 2^{64} addition and a new construction of the key schedule. Kalyna supports block size and key length of 128, 256 and 512 bits (key length can be either equal or double of the block size). At the time of this paper publishing, no more effective cryptanalytic attacks than exhaustive search are known. In this paper we present the adapted English translated specification of Kalyna as it is given in the national standard of Ukraine.

1 Introducton

Block ciphers are the most widely used symmetric cryptographic primitives. Besides providing confidentiality, they are also used as main components in hashing functions, message authentication codes, pseudorandom number generators, etc.

Until 2015 GOST 28147-89 was the main block cipher used in Ukraine [1]. Even now this cipher still provides acceptable level of practical security. However, its software implementation is significantly slower and less effective on modern

Presented at the Norwegian Information Security Conference 2015 (NISK-2015).

platforms comparing to newer solutions like AES [2]. In addition, more effective theoretical attacks than brute force search were discovered [3].

Based on the experience of international cryptographic competitions, like AES [4] or NESSIE [5], The State Service of Special Communication and Information Protection of Ukraine had been organized National Public Cryptographic Competition [6] to select a block cipher that could become a prototype of the national standard. Main requirements to candidates were a high level of cryptographic security, variable block size and key length (128, 256, 512), and an acceptable performance of encryption in software implementation. There were no restrictions concerning lightweight (hardware) implementations.

The block cipher Kalyna was selected among other candidates [7] and its slight modification (aimed to performance improvement and more compact implementation) was approved as the national standard DSTU 7624:2014 [8].

The new standard describes both the block cipher and ten modes of operation for it. In this paper we describe an adapted version of the specification based on Electronic Code Book (ECB) mode as it is given in the national standard of Ukraine.

2 Symbols and notations

The following notations are used in the standard.

0x	–	prefix of numbers given in the hexadecimal notation;
$GF(2^8)$	–	the finite field with the irreducible polynomial $x^8 + x^4 + x^3 + x^2 + 1$;
$\oplus$	–	logical exclusive OR (XOR) operation for binary vectors;
$\lfloor x \rfloor$	–	integer part of x, i.e. for a rational x the greatest y such that $y \leq x$;
$\lvert X \rvert$	–	the length of the bit sequence X;
$L_{l,r}(X)$	–	the function that returns r least significant bits from the input sequence X of l-bit length;
$R_{l,r}(X)$	–	the function that returns r most significant bits from the input sequence X of l-bit length;
$\gg$	–	the right shift of the fixed length sequence (to the least significant symbols); the most significant symbols are filled with 0's; number of symbols to be shifted is defined by the second argument
$\ll$	–	the left shift of the fixed length sequence (to the most significant symbols); the least significant symbols are filled with 0's; number of symbols to be shifted is defined by the second argument
$\ggg$	–	the cyclic shift (rotation) right of the fixed length sequence (the least significant symbols are moved to the most significant positions);
$\lll$	–	the cyclic shift (rotation) left of the fixed length sequence (the most significant symbols are moved to the least significant positions);
$+$	–	addition defined on the additive group of the least non-negative remainders $\mathbb{Z}_{2^{64}}$ (addition modulo 2^{64});
$\otimes$	–	scalar product of two vectors defined over the finite field;

l	–	the block size of Kalyna, $l \in \{128, 256, 512\}$;
k	–	the key length of Kalyna, $k \in \{128, 256, 512\}$ ($k = l$ or $k = 2 \cdot l$);
c	–	the number of columns in the state matrix;
V_j	–	j-dimensional vector space over $GF(2)$, $j \geq 1$;
$T_{l,k}^{(K)}$	–	the basic encryption transformation, a mapping $V_l \mapsto V_l$ parametrized by the encryption key K;
$U_{l,k}^{(K)}$	–	the basic decryption transformation, a mapping $V_l \mapsto V_l$ parametrized by the encryption key K;
$W_1 \vert\vert W_2$	–	concatenation of the two bit sequences in such a way that the left (the least significant) part of the resulting sequence is equal to W_1 and the right (the most significant) one to W_2; the length of the resulting sequence is equal to the sum of the lengths of W_1 and W_2;
$\Xi \circ \Lambda$	–	sequential application of transformations Ξ and Λ (Λ is applied first);
t	–	the number of iterations in the transformations $T_{l,k}^{(K)}$ and $U_{l,k}^{(K)}$;
$\prod_{i=1}^{t} \Lambda^{(i)}$	–	sequential application of the transformations $\Lambda^{(1)}$, $\Lambda^{(2)}$, ..., $\Lambda^{(t)}$ (the transformation $\Lambda^{(1)}$ is applied first);
$\mu_l^{(j)}$	–	representation of non-negative integer j as an l-bit sequence (the little-endian convention is used);
`Kalyna-`l/k	–	application of the transformations $T_{l,k}^{(K)}$ or $U_{l,k}^{(K)}$ with the block size of l bits and the key length of k bits.

3 General parameters

The basic encryption transformation is a mapping: $T_{l,k}^{(K)} : V_l \rightarrow V_l$ that depends on $K \in V_k$, where $l, k \in \{128, 256, 512\}$, such that $k = l$ or $k = 2 \cdot l$. $T_{l,k}^{(K)}$ is implemented as an iterative application of several functions taking a $8 \times c$ matrix over $GF(2^8)$ as an input argument $x \in V_l$. The $8 \times c$ matrix is the cipher internal state.

The basic decryption transformation $U_{l,k}^{(K)}$ parametrized by the encryption key K is the mapping inverse to $T_{l,k}^{(K)}$. All permitted combinations of parameters, that defines `Kalyna-`l/k, are given in Table 1.

4 Input and output data

The basic transformations process an input block of l bits size (either plaintext or ciphertext). The internal state matrix G is represented as $(g_{i,j})$, where $g_{i,j} \in V_8$, $i = \overline{0,7}$ and $j = \overline{0, c-1}$. The internal state matrix is filled by input bytes B_1, B_2, ..., $B_{l/8}$ in the column-by-column order.

Table 1: The number of rounds and the number of rows in the state matrix for different values of block size and key length

#	Block size (l)	Key length (k)	Rounds (t)	Rows of the state matrix (c)
1	128	128	10	2
2		256	14	
3	256	256	14	4
4		512	18	
5	512	512	18	8

5 Encryption

Structure of the basic encryption transformation

The basic encryption transformation $T_{l,k}^{(K)}$ is defined in the following way:

$$T_{l,k}^{(K)} = \eta_l^{(K_t)} \circ \psi_l \circ \tau_l \circ \pi_l' \circ \prod_{\nu=1}^{t-1} (\kappa_l^{(K_\nu)} \circ \psi_l \circ \tau_l \circ \pi_l') \circ \eta_l^{(K_0)},$$

where K – an encryption key of k-bit length,

$\eta_l^{(K_\nu)}$ – the function of addition of the internal state with the round key K_ν modulo 2^{64},

π_l' – the layer of non-linear bijective mapping (S-box layer) that process byte (i.e., elements of V_8) vectors,

τ_l – permutation of elements $g_{i,j} \in GF(2^8)$ of the cipher internal state (right circular shift),

ψ_l – the linear transformation of the internal state elements over the finite field,

$\kappa_l^{(K_\nu)}$ – the function of modulo 2 addition of the round key K_ν and the state matrix.

In the functions π_l', τ_l and ψ_l input argument $x \in V_l$ and output value $\chi(x) \in V_l$, $\chi \in \{\pi_l', \tau_l, \psi_l\}$, are represented as matrices of $8 \times c$ size.

Function of addition modulo 2^{64}

$\eta_l^{(K_\nu)}$ processes columns of the internal state matrix $G = (g_{i,j})$ and columns of the round key matrix $K_\nu = (k_{i,j}^{\nu})$ using modulo 2^{64} addition. The result is also an $8 \times c$ matrix (the internal state after the round key addition). In the addition operation the little-endian convention is used, i.e. less significant bytes have smaller indexes.

Layer of non-linear bijective mapping

The function π_l' implements the S-box layer. Each element $g_{i,j} \in V_8$ of the internal state matrix is substituted by $\pi_{i \bmod 4}(g_{i,j})$, where $\pi_s : V_8 \mapsto V_8$, $s \in \{0, 1, 2, 3\}$, are substitutions (S-boxes) given in Appendix A. For example, let $g_{i,j}$ be 0x23 then $\pi_0(0\text{x}23) = 0\text{x}4F$.

Another set of substitutions different from those presented in Appendix A can be used. In this case, S-boxes must be supplied in the prescribed manner.

Permutation of elements in the internal state

The function τ_l executes cyclic right shift for the rows of the state matrix $G = (g_{i,j})$. The number of shifted elements depends on the row number $i \in \{0, 1, ..., 7\}$, the block size $l \in \{128, 256, 512\}$, and is calculated according to the formula $\delta_i = \lfloor \frac{i \cdot l}{512} \rfloor$. For example, the fifth row of the state matrix of the cipher with the 256-bit block size is circularly shifted right by two positions.

Linear transformation

To perform the function ψ_l each element $g_{i,j} \in V_8$ of the internal state matrix G is represented as an element of the finite field $GF(2^8)$ formed by the irreducible polynomial $\Upsilon(x) = x^8 + x^4 + x^3 + x^2 + 1$, or $0x11D$ in hexadecimal notation.

Each element of the resulting state matrix $W = (w_{i,j})$ is calculated over $GF(2^8)$ according to the formula

$$w_{i,j} = (\upsilon \ggg i) \otimes G_j,$$

where $\upsilon = (0x01, 0x01, 0x05, 0x01, 0x08, 0x06, 0x07, 0x04)$ is the vector that forms the circulant matrix with the MDS property, and G_j is the j^{th} column of the state matrix G.

The vector υ consists of the hexadecimal constants (bytes) that are elements of the finite field $GF(2^8)$. The right circular shift is made with respect to elements of the set υ.

Function of addition modulo 2

The function $\kappa_l^{(K_\nu)}$, which is dependent on the parameter $K_\nu \in V_l$ (the round key of the ν^{th} iteration), takes the cipher internal state $x \in V_l$ as the argument. Both the round key and the internal state are represented as matrices of $8 \times c$ size. In the function $\kappa_l^{(K_\nu)}$ the internal state matrix G and the matrix representation of the round key $K_\nu = (k_{i,j}^\nu)$ are added using the XOR operation. The result is a matrix of $8 \times c$ size.

6 Decryption

Structure of the basic decryption transformation

The basic encryption transformation $T_{l,k}^{(K)}$ is defined by:

$$U_{l,k}^{(K)} = {}_{-1}\eta_l^{(K_0)} \circ \prod_{\nu=t-1}^{1} ({}_{-1}\pi_l' \circ {}_{-1}\tau_l \circ {}_{-1}\psi_l \circ \kappa_l^{(K_\nu)}) \circ {}_{-1}\pi_l' \circ {}_{-1}\tau_l \circ {}_{-1}\psi_l \circ {}_{-1}\eta_l^{(K_t)}$$

where K – an encryption key of k-bit length,

${}_{-1}\eta_l^{(K_\nu)}$ – the function of subtraction of the round key K_ν from the internal state modulo 2^{64},

${}_{-1}\psi_l$ – the inverse linear transformation of the internal state elements over the finite field,

${}_{-1}\tau_l$ – inverse permutation of elements $g_{i,j} \in GF(2^8)$ of the cipher internal state (left circular shift),

${}_{-1}\pi_l'$ – the layer of inverse non-linear bijective mapping (inverse S-box layer) that processes byte vectors,

$\kappa_l^{(K_\nu)}$ – the function of modulo 2 addition of the round key K_ν and the state matrix (the involutive function).

Like in encryption, in the functions ${}_{-1}\pi'_l$, ${}_{-1}\tau_l$ and ${}_{-1}\psi_l$ input argument $x \in V_l$ and output value $\chi(x) \in V_l$, $\chi \in \{{}_{-1}\pi'_l, {}_{-1}\tau_l, {}_{-1}\psi_l\}$, are taken as matrices of $8 \times c$ size.

Function of subtraction modulo 2^{64}

${}_{-1}\eta_l^{(K_\nu)}$ is the inverse function to $\eta_l^{(K_\nu)}$. The function ${}_{-1}\eta_l^{(K_\nu)}$ processes columns of the internal state matrix $G = (g_{i,j})$ and columns of the round key matrix $K_\nu = (k_{i,j}^\nu)$ using modulo 2^{64} subtraction. The result is an $8 \times c$ matrix (the internal state after round key subtraction).

In the subtraction operation the little-endian convention is used, i.e. less significant bytes have smaller indexes.

Layer of inverse non-linear bijective mapping

The function ${}_{-1}\pi'_l$ implements the inverse S-box layer. Each element $g_{i,j} \in V_8$ of the internal state matrix is substituted by ${}_{-1}\pi_{i \bmod 4}(g_{i,j})$, where ${}_{-1}\pi_s : V_8 \mapsto V_8$, $s \in \{0, 1, 2, 3\}$, are substitutions given in Appendix A. For example, let $g_{i,j}$ be 0x23 then ${}_{-1}\pi_0(\text{0x23}) = \text{0x56}$.

Another set of substitutions different from those presented in Appendix A can be used. In this case, S-boxes must be supplied in the prescribed manner.

Inverse permutation of elements

The function ${}_{-1}\tau_l$ executes cyclic left shift for the rows of the state matrix $G = (g_{i,j})$. The number of shifted elements depends on the row number $i \in \{0, 1, ..., 7\}$, the block size $l \in \{128, 256, 512\}$, and is calculated according to the formula $\delta_i = \lfloor \frac{i \cdot l}{512} \rfloor$. For example, the fifth row of the state matrix of the cipher with the 256-bit block size is circularly shifted left by two positions.

Inverse linear transformation

To perform the function ${}_{-1}\psi_l$ each element $g_{i,j} \in V_8$ of the internal state matrix G is represented as an element of the finite field $GF(2^8)$ formed by the irreducible polynomial $\Upsilon(x) = x^8 + x^4 + x^3 + x^2 + 1$, or $0\text{x}11D$ in hexadecimal notation.

Each element of the resulting state matrix ${}_{-1}W = ({}_{-1}w_{i,j})$ is calculated over $GF(2^8)$ according to the formula

$$w_{i,j} = ({}_{-1}\upsilon \lll i) \otimes G_j,$$

where ${}_{-1}\upsilon = (0\text{x}AD, 0\text{x}95, 0\text{x}76, 0\text{x}A8, 0\text{x}2F, 0\text{x}49, 0\text{x}D7, 0\text{x}CA)$ is the vector that forms the circulant matrix with the MDS property, and G_j is the j^{th} column of the state matrix G.

The vector υ consists of the hexadecimal constants (bytes) that are elements of the finite field $GF(2^8)$. The left circular shift is made with respect to elements of the set υ.

7 Round key generation

Intermediate key K_σ

The length of the intermediate key K_σ is equal to the block size (l bits), and is represented as a matrix of $8 \times c$ size. This key is generated from the encryption key K using the following transformation:

$$\Theta^{(K)} = \psi_l \circ \tau_l \circ \pi'_l \circ \eta_l^{(K_\alpha)} \circ \psi_l \circ \tau_l \circ \pi'_l \circ \kappa_l^{(K_\omega)} \circ \psi_l \circ \tau_l \circ \pi'_l \circ \eta_l^{(K_\alpha)},$$

where $\eta_l^{(\cdot)}$, π'_l, τ_l, ψ_l, $\kappa^{(\cdot)}$ are functions described in Section 5.

When the block size and the key length are equal ($k = l$) then $K_\alpha = K_\omega = K$ (the second argument for the functions $\eta_l^{(\cdot)}$ and $\kappa_l^{(\cdot)}$ is the encryption key).

If the block size and the key length are not equal ($k = 2 \cdot l$), then $K_\alpha || K_\omega = K$, i.e. $K_\alpha = L_{l,l/2}(K)$ and $K_\omega = R_{l,l/2}(K)$.

The l-bit value $\frac{l+k+64}{64}$ (given in the little-endian notation) is taken as an argument for the transformation $\Theta^{(K)}$ to obtain the value of the intermediate key K_σ.

Round keys with even indexes

Each round key K_0, K_1, ..., K_t has the size of the internal cipher state (l bits) and is represented as a matrix of $8 \times c$ size. The generation of round keys depends on the encryption key K, the intermediate key K_σ and the index i.

The round keys K_i with even indexes ($i \in \{0, 2, ..., t\}$) are obtained by the $\Xi^{(K,K_\sigma,i)}$ transformation:

$$\Xi^{(K,K_\sigma,i)} = \eta_l^{(\varphi_i^{(K_\sigma)})} \circ \psi_l \circ \tau_l \circ \pi'_l \circ \kappa_l^{(\varphi_i^{(K_\sigma)})} \circ \psi_l \circ \tau_l \circ \pi'_l \circ \eta_l^{(\varphi_i^{(K_\sigma)})},$$

where $\eta_l^{(\cdot)}$, π'_l, τ_l, ψ_l, $\kappa^{(\cdot)}$ are functions described in Section 5, and $\varphi_i^{(K_\sigma)}$ returns the internal state that consists of the K_σ added modulo 2^{64} with the constant shifted by the round key index. The function $\varphi_i^{(K_\sigma)}$ is defined as $\varphi_i^{(K_\sigma)} = \eta_l^{(K_\sigma)} \left(\vartheta \ll \left(\frac{i}{2}\right)\right)$, where the value $\vartheta = \mu_l^{(0x00010001...0001)}$ has the length of the cipher internal state.

The value $K \ggg 32 \cdot i$ (K is the encryption key) is the input to the transformation $\Xi^{(K,K_\sigma,i)}$ when the key length is equal to the block size ($k = l$).

If the block size and the key length are not equal ($k = 2 \cdot l$), then the following values are used as the input to the transformation $\Xi^{(K,K_\sigma,i)}$:

- $L_{k,l}(K \ggg 16 \cdot i)$ to generate the round keys with even indexes divisible by 4 ($i = \{0, 4, 8, ...\}$);
- $R_{k,l}(K \ggg 64 \cdot \lfloor \frac{i}{4} \rfloor)$ to generate the round keys with even indexes not divisible by 4 ($i = \{2, 6, 10, ...\}$).

Round keys with odd indexes

Each round key with odd index is generated from the previous round key with even index according to the formula:

$$K_i = (K_{i-1} \lll (\frac{l}{4} + 24)),$$

where l is the size of the cipher internal state (in bits) and $i \in \{1, 3, ..., t-1\}$.

8 Conclusions

Kalyna ia a block cipher with SPN-based (Rijndael-like) structure. It has increased MDS matrix size, a new set of four different S-boxes, pre- and postwhitening using modulo 2^{64} addition and the key schedule based on the round function transformations only. Kalyna supports block size and key length of 128, 256 and 512 bits (key length can be either equal or double of the block size). Kalyna is adopted as the new Ukrainian encryption standard DSTU 7624:2014 that also includes ten modes of operation and test vectors. The description of the block cipher given in this paper is an adapted English version of the Kalyna specification from the original standard.

References

[1] Government Committee of the USSR for Standards. *GOST 28147-89. State Standard of the USSR. Information Processing Systems. Cryptographic protection. Algorithm of cryptographic transformation.* Government Committee of the USSR for Standards, 1990 (in Russian).

[2] National Institute of Standards and Technology (NIST). *Advanced Encryption Standard (AES).* Federal Information Processing Standards (FIPS) Publication 197, Nov. 2001.

[3] Courtois, Nicolas T. *Security evaluation of GOST 28147-89 in view of international standardisation.* Cryptologia 36.1 (2012): 2-13.

[4] National Institute of Standards and Technology (NIST). *Announcing Development Of A Federal Information Processing Standard For Advanced Encryption Standard.* `http://csrc.nist.gov/archive/aes/pre-round1/aes_9701.txt`. Jan. 1997.

[5] NESSIE *New European Schemes for Signatures, Integrity, and Encryption.* `https://www.cosic.esat.kuleuven.be/nessie`, 2004.

[6] State Service of Special Communication and Information Protection of Ukraine. *Statement on Public Competition of Cryptographic Algorithms.* `http://www.dstszi.gov.ua/dstszi/control/ua/publish/printable_article?art_id=48387`, 2006 (in Ukrainian).

[7] Oliynykov Roman, Gorbenko Ivan, Dolgov Victor, Ruzhentsev Victor. *Results of Ukrainian National Public Cryptographic Competition.* Tatra Mountains Mathematical Publications, 47(1), 99-113. 2009.

[8] Roman Oliynykov, Ivan Gorbenko, Oleksandr Kazymyrov, Victor Ruzhentsev, Oleksandr Kuznetsov, Yurii Gorbenko, Oleksandr Dyrda, Viktor Dolgov, Andrii Pushkaryov, Ruslan Mordvinov, Dmytro Kaidalov. *DSTU 7624:2014. National Standard of Ukraine. Information technologies. Cryptographic Data Security. Symmetric block transformation algorithm.* Ministry of Economical Development and Trade of Ukraine, 2015 (in Ukrainian).

A S-boxes for the Kalyna block cipher (hexadecimal notation)

Substitution π_0

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

Substitution π_1

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

Substitution π_2

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

Substitution π_3

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

Substitution $_{-1}\pi_0$

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

Substitution $_{-1}\pi_1$

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

Substitution $_{-1}\pi_2$

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

Substitution $_{-1}\pi_3$

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