UDC 519.7 DOI 10.17223/20710410/42/4

ELGAMAL CRYPTOSYSTEMS ON BOOLEAN FUNCTIONS[1]

G. P. Agibalov

National Research Tomsk State University, Tomsk, Russia

E-mail: agibalov@mail.tsu.ru

Here is a description of ElGamal public-key encryption and digital signature schemes constructed on the base of bijective systems of Boolean functions. The description is illustrated with a simple example in which the used Boolean functions are written in logical notation. In our encryption and signature schemes on Boolean functions, every one ciphertext or message signature is a pair of values, as in the basic ElGamal cryptosystem on a group. In our case, these values are Boolean vectors. Each vector in the pair depends on the value of a function on a plaintext or on a message, and this function is typically obtained from a given bijective vector Boolean function g by applying some random and secret negation and permutation operations on the sets of variables and coordinate functions of g. For the pair of vectors in the ciphertext or in the message signature, the decryption algorithm produces the plaintext, and the signature verification algorithm accepts the signature, performing some computation on this pair. The signature is accepted for a message if and only if the computation results in this message. All the computations in the processes of encryption, decryption, signing and verification are logical and performed for Boolean values, promising their implementation efficiency to be more high than in the basic ElGamal schemes on groups.

Keywords: *bijective vector Boolean functions, permutation and negation operations, ElGamal encryption, ElGamal signature.*

Introduction

The ElGamal cryptosystems, including the basic encryption and signature schemes as well as their multiple generalizations and variations [1], are typically defined on the base of some groups in which the group operation is easily to apply and the discrete logarithm problem is computationally infeasible. The multiplicative groups $\mathbb{Z}_p^*$, $\mathbb{F}_{2^m}^*$ and additive group of points on elliptic curve over $\mathbb{F}_q$ have received the most attention [1]. It is known that the public-key cryptosystems based on similar groups are particularly susceptible to quantum attacks. The ElGamal cryptosystems are not excluded from this family.

In this paper, we try to propose an alternative mathematical background for constructing ElGamal cryptosystems, namely the algebra of bijective vector Boolean functions with the negation and permutation operations on the sets of their variables and coordinate functions. Section 2 of the paper is a collection of the basic elements of this background that we use in the description of our ElGamal encryption and signature schemes in Sections 3 and 5 respectively and of an illustrative example in Section 4. For any of operations encryption and signature, we consider different variations of the scheme and describe each of them in the form of the corresponding basic ElGamal scheme (encryption or signature). For reader's convenience, Section 1 recalls the basic ElGamal encryption and signature schemes in this form from [1].

[1]The author was supported by the RFBR-grant no. 17-01-00354.

1. Basic ElGamal cryptosystem

1.1. Basic ElGamal encryption scheme

Parameters: p is a large random prime, α is a generator of the multiplicative group $\mathbb{Z}_p^*$, a is a random integer, $1 \leqslant a \leqslant p-2$, m is a plaintext, $m \in \mathbb{Z}_p$.

Public key is (p, α, α^a), *private key* is a.

Encryption: $k \in_R \{1, 2, \ldots, p-2\}$ (here and further, the symbol $\in_R$ means "to be randomly chosen"), $\gamma = \alpha^k \bmod p$, $\delta = m(\alpha^a)^k \bmod p$, (γ, δ) is the *ciphertext*.

Decryption: $\gamma^{-a}\delta (= \alpha^{-ak} m \alpha^{ak}) = m \bmod p$.

1.2. Basic ElGamal signature scheme

Parameters: p is a large random prime, α is a generator of the multiplicative group $\mathbb{Z}_p^*$, a is a random integer, $1 \leqslant a \leqslant p-2$, $\beta = \alpha^a$, m is a message (or its hash value), $m \in \mathbb{Z}_p$.

Public key is (p, α, β), *private key* is a.

Signing: $k \in_R \{1, 2, \ldots, p-2\}$, $(k, p-1) = 1$, $\gamma = \alpha^k \bmod p$, $\delta = k^{-1}(m - a\gamma) \bmod (p-1)$, signature for m is the pair (γ, δ).

Verification: if $\gamma \leqslant 1$ or $\gamma > p-1$, then reject the signature (γ, δ), otherwise accept the signature (γ, δ) if and only if $\beta^\gamma \gamma^\delta = \alpha^m \bmod p$.

2. Algebra of bijective vector Boolean functions

First of all, we note that earlier some elements of this algebra were used in constructing and cryptanalysis of cryptographic systems with functional keys, namely in [2] — for symmetric block ciphers, in [3] — for public-key encryption and signature schemes.

2.1. Permutation and negation operations

We begin with the notions of the permutation and negation operations over Boolean vectors. Let n be an integer, $n \geqslant 2$, and $\mathbb{S}_n$ be the set of all permutations of the row $(12\ldots n)$, that is, $\mathbb{S}_n = \{(i_1 i_2 \ldots i_n) : i_j \in \{1, 2, \ldots, n\}, j \neq r \Rightarrow i_j \neq i_r; j, r \in \{1, \ldots, n\}\}$. A permutation $\pi = (i_1 i_2 \ldots i_n) \in \mathbb{S}_n$ is called a *permutation operation* on $\mathbb{F}_2^n$ if the result of its application to any vector $w = w_1 w_2 \ldots w_n$ in $\mathbb{F}_2^n$ is the vector $\pi(w) = w_{i_1} w_{i_2} \ldots w_{i_n}$. A Boolean vector $\sigma = b_1 b_2 \ldots b_n \in \mathbb{F}_2^n$ is called a *negation operation* on $\mathbb{F}_2^n$ if the result of its application to a vector $\alpha = a_1 a_2 \ldots a_n$ in $\mathbb{F}_2^n$ is the vector $\alpha^\sigma = a_1^{b_1} a_2^{b_2} \ldots a_n^{b_n}$, where for a and b in $\mathbb{F}_2$, we have $a^b = a$ if $b = 1$ and $a^b = \neg a$ if $b = 0$. Both of these operations are invertible. The inversions for them are denoted in the usual manner, namely π^{-1} and σ^{-1}. By the definition, if $\pi = (i_1 i_2 \ldots i_n)$, $s(k) = i_k$, and $\pi^{-1} = (j_1 j_2 \ldots j_n)$, then $s^{-1}(i_k) = k$, $s^{-1}(k) = j_k$, and $j_k = s^{-1}(s^{-1}(i_k))$, $k \in \{1, 2, \ldots, n\}$. The permutation and negation operations π and σ are called *identity* and denoted by 1 if $\pi = (12\ldots n)$ and $\sigma = 11\ldots1$ respectively. So $1(w) = w$ and $a^1 = a$.

2.2. Combinatorial and algebraic notations

Let $x = (x_1, x_2, \ldots, x_n)$ be a string of n different Boolean variables, $g : \mathbb{F}_2^n \to \mathbb{F}_2^n$ be a n-dimensional vector Boolean function $g(x)$, and $g_i : \mathbb{F}_2^n \to \mathbb{F}_2$, $i \in \{1, 2, \ldots, n\}$, be the coordinate functions of g. That is, $g(x) = g_1(x) g_2(x) \ldots g_n(x)$. Let π_1, π_2 and σ_1, σ_2 be the symbols of variables with the values, respectively, of permutation operations in $\mathbb{S}_n$ and of negation operations in $\mathbb{F}_2^n$, namely σ_1, π_1 — over the variables in x and σ_2, π_2 — over the coordinates in $g(x)$. Let also $I = \{\sigma_1, \pi_1, \sigma_2, \pi_2\}$, $J \subseteq I$, V_J be the set of all strings of values for the variables in I in which (strings) the value of each variable from $I \setminus J$ is equal to 1, i.e. $V_J = \{(s_1 p_1 s_2 p_2) : s_i = 1$ if $\sigma_i \in I \setminus J$ and $p_i = 1$ if $\pi_i \in I \setminus J$; $s_i \in \mathbb{F}_2^n$ if $\sigma_i \in J$ and $p_i \in \mathbb{S}_n$ if $\pi_i \in J$; $i \in \{1, 2\}\}$,

$$\pi_i^J = \begin{cases} 1, & \text{if} \quad \pi_i \in I \setminus J, \\ \pi_i, & \text{if} \quad \pi_i \in J, \end{cases} \quad \sigma_i^J = \begin{cases} 1, & \text{if} \quad \sigma_i \in I \setminus J, \\ \sigma_i, & \text{if} \quad \sigma_i \in J, \end{cases} \quad i \in \{1, 2\},$$

and $g^J(x)$ be the formula $\pi_2^J(g^{\sigma_2^J}(\pi_1^J(x^{\sigma_1^J})))$. Particularly, for any $a = (s_1 p_1 s_2 p_2) \in V_J$, a formula $g^a(x)$ is defined too as $g^a(x) = p_2(g^{s_2}(p_1(x^{s_1})))$. In fact, $g^J(x)$ is a subformula of $g^I(x) = \pi_2(g^{\sigma_2}(\pi_1(x^{\sigma_1})))$ with the negation and permutation operations from a subset $J \subseteq I$. For example, if $J = \{\sigma_1, \pi_2\}$, then $\pi_1^J = 1$, $\sigma_2^J = 1$, and $g^J(x) = \pi_2(g(x^{\sigma_1}))$.

The formulas $g^J(x)$ for all possible J are given in the Table 1:

Table 1

J	$\varnothing$	$\{\sigma_1\}$	$\{\pi_1\}$	$\{\sigma_2\}$	$\{\pi_2\}$	$\{\sigma_1, \pi_1\}$	$\{\sigma_1, \sigma_2\}$	$\{\sigma_1, \pi_2\}$
$g^J(x)$	$g(x)$	$g(x^{\sigma_1})$	$g(\pi_1(x))$	$g^{\sigma_2}(x)$	$\pi_2(g(x))$	$g(\pi_1(x^{\sigma_1}))$	$g^{\sigma_2}(x^{\sigma_1})$	$\pi_2(g(x^{\sigma_1}))$

$\{\pi_1, \sigma_2\}$	$\{\pi_1, \pi_2\}$	$\{\sigma_2, \pi_2\}$	$\{\sigma_1, \pi_1, \sigma_2\}$	$\{\sigma_1, \pi_1, \pi_2\}$
$g^{\sigma_2}(\pi_1(x))$	$\pi_2(g(\pi_1(x)))$	$\pi_2(g^{\sigma_2}(x))$	$g^{\sigma_2}(\pi_1(x^{\sigma_1}))$	$\pi_2(g(\pi_1(x^{\sigma_1})))$

$\{\sigma_1, \sigma_2, \pi_2\}$	$\{\pi_1, \sigma_2, \pi_2\}$	$\{\sigma_1, \pi_1, \sigma_2, \pi_2\}$
$\pi_2(g^{\sigma_2}(x_1^{\sigma}))$	$\pi_2(g^{\sigma_2}(\pi_1(x)))$	$\pi_2(g^{\sigma_2}(\pi_1(x^{\sigma_1})))$

To make distinction between signs of kinds $g^J(x)$ and $g^{\sigma_2^J}(x)$ as well as between signs of kinds $g^a(x)$ and $g^{s_2}(x)$, we often write $(g(x))^{\sigma_2^J}$ and $(g(x))^{s_2}$ instead of $g^{\sigma_2^J}(x)$ and $g^{s_2}(x)$ respectively. So, $g^J(x) = \pi_2^J(g(\pi_1^J(x^{\sigma_1^J})))^{\sigma_2^J}$ and $g^a(x) = p_2(g(p_1(x^{s_1})))^{s_2}$.

For any vector-columns a, σ in $\mathbb{F}_2^n$ and a permutation $\pi = (i_1 i_2 \dots i_n) \in \mathbb{S}_n$, if $c = \neg\sigma$, $T = (t_{kj})$ is a permutation matrix of order n over $\mathbb{F}_2$ where $t_{kj} = 1 \Leftrightarrow j = i_k$ for all $k, j \in \{1, 2, \dots, n\}$ (we call it *matrix of* π), then $a^\sigma = a \oplus c$ and $\pi(a) = Ta$. This allows us to introduce the more simple notation in which A and D are the matrices of permutations π_1 and π_2 respectively and b and d are the vector-columns $\neg\sigma_1$ and $\neg\sigma_2$ respectively, to use the symbols of variables A, D, b, d instead of symbols of operations $\pi_1, \pi_2, \sigma_1, \sigma_2$ respectively in the sets I, J as well as in the formulas for $f(x), f^{-1}(x)$ and to apply linear algebra methods in solving the equations $y = f(x)$ and $x = f^{-1}(y)$ with regard to unknown key parameters. Further, the fact of such replacement is denoted by the sign $\simeq$. For example, $\{\pi_1, \sigma_1, \sigma_2\} \simeq \{A, b, d\}$, $g^J(x) = \pi_2(g(\pi_1(x^{\sigma_1})))^{\sigma_2} \simeq D(g(A(x \oplus b)) \oplus d)$. The formulas under consideration with symbols of permutation and negation operations $\sigma_1, \pi_1, \sigma_2, \pi_2$ are said to be ones in *combinatorial notation* and the formulas where the operations are represented by symbols b, A, d, D of matrices and vectors are formulas in *algebraic notation.*

All the formulas $g^J(x)$ in algebraic notation are given in the Table 2:

Table 2

J	$\varnothing$	$\{b\}$	$\{A\}$	$\{d\}$	$\{D\}$	$\{b, A\}$	$\{b, d\}$	$\{b, D\}$
$g^J(x)$	$g(x)$	$g(x \oplus b)$	$g(Ax)$	$g(x) \oplus d$	$Dg(x)$	$g(A(x \oplus b))$	$g(x \oplus b) \oplus d$	$Dg(x \oplus b)$

$\{A, d\}$	$\{A, D\}$	$\{d, D\}$	$\{b, A, d\}$	$\{b, A, D\}$
$g(Ax) \oplus d$	$Dg(Ax)$	$D(g(x) \oplus d)$	$g(A(x \oplus b)) \oplus d$	$Dg(A(x \oplus b))$

$\{b, d, D\}$	$\{A, d, D\}$	$\{b, A, d, D\}$
$D(g(x \oplus b) \oplus d)$	$D(g(Ax) \oplus d)$	$D(g(A(x \oplus b)) \oplus d)$

2.3. Permutation-negation compositions

There are two kinds of composition for permutation-negation operations — multiplicative and serial. We begin with the first one.

Multiplicative composition

For any subsets $J, L \subseteq I$, define it as

$$g^{JL}(x) = \pi_2^L(g^J(\pi_1^L(x^{\sigma_1^L})))^{\sigma_2^L}.$$

Particularly, this means that for any $a = (s_1p_1s_2p_2) \in V_J$ and $k = (r_1q_1r_2q_2) \in V_L$, the value $g^{a^k}(x)$ is defined as

$$g^{a^k}(x) = q_2(g^a(q_1(x^{r_1})))^{r_2},$$

where $g^a(x) = p_2(g(p_1(x^{s_1})))^{s_2}$, therefore

$$g^{a^k}(x) = q_2(p_2(g(p_1((q_1(x^{r_1}))^{s_1})))^{s_2})^{r_2}.$$

By the definition, we should write $\left(g^J\right)^L$ and $(g^a)^k$ instead of g^{J^L} and g^{a^k} respectively, but for simplicity we remove the parentheses.

Let $b^J = \neg\sigma_1^J, b^L = \neg\sigma_1^L, d^J = \neg\sigma_2^J, d^L = \neg\sigma_2^L$, and A^J, A^L, D^J, D^L denote the matrices of $\pi_1^J, \pi_1^L, \pi_2^J, \pi_2^L$ respectively. We have $g^{J^{\sigma_2^L}}(x) = g^J(x) \oplus d^L = D^J(g(A^J(x \oplus b^J)) \oplus d^J) \oplus d^L$ and $\pi_1^L(x^{\sigma_1^L}) = A^L(x \oplus b^L)$. Hence, $g^{J^{\sigma_2^L}}(\pi_1^L(x^{\sigma_1^L})) = D^J(g(A^J(A^L(x \oplus b^L) \oplus b^J)) \oplus d^J) \oplus d^L$ and

$$g^{J^L}(x) = D^L(D^J(g(A^J(A^L(x \oplus b^L) \oplus b^J)) \oplus d^J) \oplus d^L).$$

Particularly,

$$g^{a^k}(x) = D'(D(g(A(A'(x \oplus b') \oplus b)) \oplus d) \oplus d'),$$

where $b = \neg s_1, b' = \neg r_1, d = \neg s_2, d' = \neg r_2$, and A, A', D, D' are the matrices of permutations p_1, q_1, p_2, q_2 respectively.

Serial composition

For the subsets $J, L \subseteq I$, it is defined as follows

$$g^L(g^J(x)) = \pi_2^L(g(\pi_1^L((g^J(x))^{\sigma_1^L})))^{\sigma_2^L} = \pi_2^L(g(\pi_1^L((\pi_2^J(g(\pi_1^J(x^{\sigma_1^J})))^{\sigma_2^J})^{\sigma_1^L})))^{\sigma_2^L} =$$
$$= D^L(g(A^L((D^J(g(A^J(x \oplus b^J)) \oplus d^J)) \oplus b^L)) \oplus d^L),$$

and for the permutation-negation operations $a = (s_1p_1s_2p_2) \in V_J$ and $k = (r_1q_1r_2q_2) \in V_L$ — in the following way

$$g^k(g^a(x)) = q_2(g(q_1((g^a(x))^{r_1})))^{r_2} = q_2(g(q_1((p_2(g(p_1(x^{s_1})))^{s_2})^{r_1})))^{r_2} =$$
$$= D'(g(A'((D(g(A(x \oplus b)) \oplus d)) \oplus b')) \oplus d').$$

2.4. Derived functions

The order of operation performing in $g^J(x)$ is determined by the parentheses and the following additional agreement: in a subformula $g^\sigma(u)$, the value of $g(u)$ is calculated before performing the operation σ. So, the operations in $g^J(x)$, including the function g, are performed in the order $\sigma_1^J, \pi_1^J, g, \sigma_2^J, \pi_2^J$. Under particular operations s_1, p_1, s_2, p_2 as possible values for variables $\sigma_1^J, \pi_1^J, \sigma_2^J, \pi_2^J$ respectively, for particular function g and a value α of x, the value of $g^J(\alpha)$ is sequentially computed as follows: $v_1(\alpha) = \alpha^{s_1}$, $v_2(\alpha) = p_1(v_1(\alpha))$, $v_3(\alpha) = g(v_2(\alpha))$, $v_4(\alpha) = v_3^{s_2}(\alpha)$, $g^J(\alpha) = p_2(v_4(\alpha))$. This defines a function $f : \mathbb{F}_2^n \to \mathbb{F}_2^n$ such that $f(x) = p_2(v_4(x))$. By the definition, $f(x)$ is uniquely determined by the function $g(x)$ and negation and permutation transformations of its variables and coordinates. For $a = (s_1, p_1, s_2, p_2)$, we denote it $g^a(x)$ and call it a *derived* function (derived from g by the transformation a). Thus, $g^a(x) = p_2(g^{s_2}(p_1(x^{s_1}))) = p_2(g(p_1(x^{s_1})))^{s_2}$. The second of these expressions for $g^a(x)$ explicitly shows the order of applying operations in the process of computing $g^a(x)$. Schematically, the computation according to it can be expressed with the following chain:

$$x \xrightarrow{s_1} x^{s_1} \xrightarrow{p_1} p_1(x^{s_1}) \xrightarrow{g} g(p_1(x^{s_1})) \xrightarrow{s_2} g^{s_2}(p_1(x^{s_1})) \xrightarrow{p_2} g^a(x).$$

In every case when $g(x)$ is a bijective vector Boolean function on $\mathbb{F}_2^n$, so should be the function $g^a(x)$. Its inverse $g^{a^{-1}}(x)$ satisfies the identity relation $g^{a^{-1}}(g^a(x)) = x$ and can be performed in the following way: if $y = g^a(x)$, then $x = g^{a^{-1}}(y) = [p_1^{-1}(g^{-1}((p_2^{-1}(y))^{s_2}))]^{s_1}$. Schematically, the computation according to this formula can be expressed with the following chain:

$$y \overset{p_2^{-1}}{\to} g^{s_2}(p_1(x^{s_1})) \overset{s_2}{\to} g(p_1(x^{s_1})) \overset{g^{-1}}{\to} p_1(x^{s_1}) \overset{p_1^{-1}}{\to} x^{s_1} \overset{s_1}{\to} x.$$

Computational complexities of function $g(x)$ and its derived functions are of the same order. In particular, if $g(x)$ is of a polynomial complexity, then $g^a(x)$ with known g and a is of a polynomial complexity too what we can not say about $g^{a^{-1}}$.

3. ElGamal encryption on Boolean functions

We need to say that in reality we can construct on Boolean functions very many different variations of ElGamal encryption schemes which can differ each other in public and private keys definitions and in encryption and decryption equations. The following variation seems to have the most simple expression and insufficiently strong private key.

3.1. Encryption scheme $\mathcal{E}1$

Parameters: n is an integer, $n \geqslant 2$; $g(x) = g_1(x)g_2(x)\dots g_n(x)$ is a bijective vector Boolean function with the coordinate functions $g_1(x), \dots, g_n(x)$ specified in a constructive way and computed with a polynomial (in n) time complexity, $g : \mathbb{F}_2^n \to \mathbb{F}_2^n$; $\varnothing \neq \neq J, L \subseteq I = \{\sigma_1, \pi_1, \sigma_2, \pi_2\}$, where π_1, π_2 and σ_1, σ_2 are the symbols of variables with the values, respectively, of permutation operations in $\mathbb{S}_n$ and of negation operations in $\mathbb{F}_2^n$; $a = (s_1 p_1 s_2 p_2) \in_R V_J$ and $g^a(x) = p_2(g^{s_2}(p_1(x^{s_1})))$.

Public key is $(g(x), g^a(x))$, *private key* is $g^{a^{-1}}(x)$, *secret* parameter is a.

Encryption: m is a *plaintext*, $m \in \mathbb{F}_2^n$; k is a *randomization* parameter, $k = (r_1, q_1, r_2, q_2) \in_R V_L$; $\gamma(m) = g^k(m) = q_2(g^{r_2}(q_1(m^{r_1})))$, $\delta(m) = g^k(m) \oplus g^a(m)$; $(\gamma(m), \delta(m))$ is the *ciphertext*.

Decryption: $m = g^{a^{-1}}(\gamma(m) \oplus \delta(m))$.

Proof that decryption works: $g^{a^{-1}}(\gamma(m) \oplus \delta(m)) = g^{a^{-1}}(g^k(m) \oplus g^k(m) \oplus g^a(m)) = = g^{a^{-1}}(g^a(m)) = m$.

3.2. Encryption scheme $\mathcal{E}2$

Public key is $g^a(x)$, *private key* is $g^{a^{-1}}(x)$, *secret* parameter is a.

Encryption: m is a *plaintext*, $m \in \mathbb{F}_2^n$; k is a *randomization* parameter, $k = (r_1, q_1, r_2, q_2) \in_R V_L$; $\gamma(m) = g^{a^k}(m) = q_2(g^a(q_1(m^{r_1})))^{r_2}$, $\delta(m) = g^{a^k}(m) \oplus g^a(m)$; $(\gamma(m), \delta(m))$ is the *ciphertext*.

Decryption: $m = g^{a^{-1}}(\gamma(m) \oplus \delta(m))$.

Proof that decryption works: $g^{a^{-1}}(\gamma(m) \oplus \delta(m)) = g^{a^{-1}}(g^{a^k}(m) \oplus g^{a^k}(m) \oplus g^a(m)) = = g^{a^{-1}}(g^a(m)) = m$.

3.3. Encryption scheme $\mathcal{E}3$

This variation is proposed by V. A. Roman'kov.

Public key is $g^a(x)$, *private key* is $g^{a^{-1}}(x)$, *secret* parameter is a.

Encryption: m is a *plaintext*, $m \in \mathbb{F}_2^n$; (k, u) are *randomization* parameters, $k = (r_1, q_1, r_2, q_2) \in_R V_L$, $u \in_R \mathbb{F}_2^n$; $\gamma = g^a(g^k(u))$, $\delta = g^k(u) \oplus m$; (γ, δ) is the *ciphertext*.

Decryption: $m = g^{a^{-1}}(\gamma) \oplus \delta$.

Proof that decryption works: $g^{a^{-1}}(\gamma) \oplus \delta = g^{a^{-1}}(g^a(g^k(u))) \oplus g^k(u) \oplus m = g^k(u) \oplus g^k(u) \oplus \oplus m = m$.

3.4. Encryption scheme $\mathcal{E}4$

This variation is proposed by I. A. Pankratova.

Public key is $g^a(x)$, *private key* is $g^{a^{-1}}(x)$, *secret* parameter is a.

Encryption: m is a *plaintext*, $m \in \mathbb{F}_2^n$; u is a *randomization* parameter, $u \in_R \mathbb{F}_2^n$; $\gamma = g^a(u)$, $\delta = u \oplus m$; (γ, δ) is the *ciphertext*.

Decryption: $m = g^{a^{-1}}(\gamma) \oplus \delta$.

Proof that decryption works: $g^{a^{-1}}(\gamma) \oplus \delta = g^{a^{-1}}(g^a(u)) \oplus u \oplus m = u \oplus u \oplus m = m$.

4. Example

Here, we illustrate the ElGamal encryption on Boolean functions effectively represented in an analytical form (not by tables).

Let $n = 4$, $x = x_1x_2x_3x_4$, $g : \mathbb{F}_2^4 \to \mathbb{F}_2^4$, $g(x) = g_1(x)g_2(x)g_3(x)g_4(x)$,

$$g_1(x) = x_1 \oplus x_2 \oplus x_3 \oplus x_4,\ g_2(x) = x_1x_2 \vee \bar{x}_1\bar{x}_2,\ g_3(x) = x_4,\ g_4(x) = x_2\bar{x}_3 \vee x_1x_3,$$

$g^{-1} : \mathbb{F}_2^4 \to \mathbb{F}_2^4$, $g^{-1}(x) = g'_1(x)g'_2(x)g'_3(x)g'_4(x)$. We have

$$\begin{gathered} g'_1(x) = x_2x_4 \vee \bar{x}_1\bar{x}_3x_4 \vee x_1\bar{x}_2\bar{x}_3\bar{x}_4 \vee \bar{x}_1\bar{x}_2x_3\bar{x}_4 \vee x_1x_3x_4, \\ g'_2(x) = x_2x_4 \vee \bar{x}_1x_3x_4 \vee x_1\bar{x}_3x_4 \vee \bar{x}_1\bar{x}_2\bar{x}_3\bar{x}_4 \vee x_1\bar{x}_2x_3\bar{x}_4, \\ g'_3(x) = \bar{x}_1\bar{x}_2\bar{x}_3 \vee \bar{x}_1x_2x_3 \vee x_1x_2\bar{x}_3 \vee x_1\bar{x}_2x_3,\ g'_4(x) = x_3. \end{gathered}$$

Let also $J = L = I$, $V_J = V_L = \{(s_1, p_1, s_2, p_2) : p_1, p_2 \in \mathbb{S}_4;\ s_1, s_2 \in \mathbb{F}_2^4\}$;

$$\begin{gathered} a = (s_1, p_1, s_2, p_2) \in V_J,\ p_1 = 2341,\ p_2 = 4123,\ s_1 = 1001, s_2 = 0111; \\ k = (r_1, q_1, r_2, q_2) \in V_L,\ q_1 = 4321,\ q_2 = 3412,\ r_1 = 0001, r_2 = 1000. \end{gathered}$$

We have that

$$\begin{gathered} x^{s_1} = x_1\bar{x}_2\bar{x}_3x_4,\ p_1(x^{s_1}) = \bar{x}_2\bar{x}_3x_4x_1, \\ g^{s_2}(x) = \bar{g}_1(x)g_2(x)g_3(x)g_4(x),\ p_2(g^{s_2}(x)) = g_4(x)\bar{g}_1(x)g_2(x)g_3(x); \\ g^a(x) = p_2(g^{s_2}(p_1(x^{s_1}))) = (g_4(\bar{x}_2\bar{x}_3x_4x_1), \bar{g}_1(\bar{x}_2\bar{x}_3x_4x_1), g_2(\bar{x}_2\bar{x}_3x_4x_1), g_3(\bar{x}_2\bar{x}_3x_4x_1)) = \\ = ((\bar{x}_3\bar{x}_4 \vee \bar{x}_2x_4), \neg(\bar{x}_2 \oplus \bar{x}_3 \oplus x_4 \oplus x_1), (\bar{x}_2\bar{x}_3 \vee x_2x_3), (x_1)); \\ y = y_1y_2y_3y_4,\ p_2^{-1}(y) = y_2y_3y_4y_1,\ (p_2^{-1}(y))^{s_2} = \bar{y}_2y_3y_4y_1, \\ p_1^{-1}(x) = x_4x_1x_2x_3,\ (p_1^{-1}(x))^{s_1} = x_4\bar{x}_1\bar{x}_2x_3; \\ g^{a^{-1}}(y) = [p_1^{-1}(g^{-1}((p_2^{-1}(y))^{s_2}))]^{s_1} = [p_1^{-1}(g^{-1}(\bar{y}_2y_3y_4y_1))]^{s_1} = [p_1^{-1}(g'_1(\bar{y}_2y_3y_4y_1), g'_2(\bar{y}_2y_3y_4y_1), \\ g'_3(\bar{y}_2y_3y_4y_1), g'_4(\bar{y}_2y_3y_4y_1)]^{s_1} = [g'_4(\bar{y}_2y_3y_4y_1), \bar{g'}_1(\bar{y}_2y_3y_4y_1), \bar{g'}_2(\bar{y}_2y_3y_4y_1), \\ g'_3(\bar{y}_2y_3y_4y_1)] = [y_4, \neg(y_1y_3 \vee y_1y_2\bar{y}_4 \vee \bar{y}_1\bar{y}_2\bar{y}_3\bar{y}_4 \vee \bar{y}_1y_2\bar{y}_3y_4 \vee y_1\bar{y}_2y_4), \\ \neg(y_1y_3 \vee y_1y_2y_4 \vee y_1\bar{y}_2\bar{y}_4 \vee \bar{y}_1y_2\bar{y}_3\bar{y}_4 \vee \bar{y}_1\bar{y}_2\bar{y}_3y_4), y_2\bar{y}_3\bar{y}_4 \vee y_2y_3y_4 \vee \bar{y}_2y_3\bar{y}_4 \vee \bar{y}_2\bar{y}_3y_4]; \\ x^{r_1} = \bar{x}_1\bar{x}_2\bar{x}_3x_4,\ q_1(x^{r_1}) = x_4\bar{x}_3\bar{x}_2\bar{x}_1,\ g^{r_2}(x) = g_1(x)\bar{g}_2(x)\bar{g}_3(x)\bar{g}_4(x), \\ q_2(g^{r_2}(x)) = \bar{g}_3(x)\bar{g}_4(x)g_1(x)\bar{g}_2(x); \\ g^k(x) = y = y_1y_2y_3y_4 = q_2(g^{r_2}(q_1(x^{r_1}))) = \\ = (\bar{g}_3(x_4\bar{x}_3\bar{x}_2\bar{x}_1), \bar{g}_4(x_4\bar{x}_3\bar{x}_2\bar{x}_1), g_1(x_4\bar{x}_3\bar{x}_2\bar{x}_1), \bar{g}_2(x_4\bar{x}_3\bar{x}_2\bar{x}_1)) = \\ = (x_1, \neg(x_2\bar{x}_3 \vee \bar{x}_2x_4), x_4 \oplus \bar{x}_3 \oplus \bar{x}_2 \oplus \bar{x}_1, \neg(\bar{x}_3x_4 \vee x_3\bar{x}_4)); \\ q_2^{-1}(y) = y_3y_4y_1y_2,\ (q_2^{-1}(y))^{r_2} = y_3\bar{y}_4\bar{y}_1\bar{y}_2,\ q_1^{-1}(x) = x_4x_3x_2x_1,\ (q_1^{-1}(x))^{r_1} = \bar{x}_4\bar{x}_3\bar{x}_2x_1; \end{gathered}$$

$$g^{k^{-1}}(y) = [q_1^{-1}(g^{-1}((q_2^{-1}(y))^{r_2}))]^{r_1} = [q_1^{-1}(g^{-1}(y_3\bar{y}_4\bar{y}_1\bar{y}_2))]^{r_1} =$$
$$= [q_1^{-1}(g'_1(y_3\bar{y}_4\bar{y}_1\bar{y}_2), g'_2(y_3\bar{y}_4\bar{y}_1\bar{y}_2), g'_3(y_3\bar{y}_4\bar{y}_1\bar{y}_2), g'_4(y_3\bar{y}_4\bar{y}_1\bar{y}_2)]^{r_1} =$$
$$= [\bar{g'}_4(y_3\bar{y}_4\bar{y}_1\bar{y}_2), \bar{g'}_3(y_3\bar{y}_4\bar{y}_1\bar{y}_2), \bar{g'}_2(y_3\bar{y}_4\bar{y}_1\bar{y}_2), g'_1(y_3\bar{y}_4\bar{y}_1\bar{y}_2)] =$$
$$= [y_1, \neg(y_1\bar{y}_3y_4 \vee \bar{y}_1\bar{y}_3\bar{y}_4 \vee y_1y_3\bar{y}_4 \vee \bar{y}_1y_3y_4), \neg(\bar{y}_2\bar{y}_4 \vee \bar{y}_1\bar{y}_2\bar{y}_3 \vee y_1\bar{y}_2y_3 \vee y_1y_2\bar{y}_3y_4 \vee \bar{y}_1y_2y_3y_4),$$
$$\bar{y}_2\bar{y}_4 \vee y_1\bar{y}_2\bar{y}_3 \vee y_1y_2y_3y_4 \vee \bar{y}_1y_2\bar{y}_3y_4 \vee \bar{y}_1\bar{y}_2y_3];$$
$$g^{a^k}(x) = q_2(g^a(q_1(x^{r_1})))^{r_2} = q_2(g^a(x_4\bar{x}_3\bar{x}_2\bar{x}_1))^{r_2} =$$
$$= q_2((x_1x_2 \vee \bar{x}_1x_3), \neg(x_4 \oplus \bar{x}_3 \oplus \bar{x}_2 \oplus \bar{x}_1), (x_2x_3 \oplus \bar{x}_2\bar{x}_3), x_4)^{r_2} =$$
$$= q_2((x_1x_2 \vee \bar{x}_1x_3), \neg(x_1 \oplus x_2 \oplus x_3 \oplus x_4), \neg(x_2x_3 \oplus \bar{x}_2\bar{x}_3), \bar{x}_4) =$$
$$= (\bar{x}_2x_3 \vee x_2\bar{x}_3, \bar{x}_4, x_1x_2 \vee \bar{x}_1x_3, \neg(x_1 \oplus x_2 \oplus x_3 \oplus x_4)).$$

Suppose, we want to encrypt the plaintext $m = x_1x_2x_3x_4 = 1010$, applying the scheme $\mathcal{E}1$. We compute $\gamma(m) = \gamma(1010) = g^k(1010) = 1110$, $g^a(m) = g^a(1010) = 0101$, $\delta(m) = \delta(1010) = g^k(1010) \oplus g^a(1010) = 1110 \oplus 0101 = 1011$ and obtain the ciphertext $(\gamma(m), \delta(m)) = (1110, 1011)$. To decrypt this ciphertext, we compute $g^{a^{-1}}(\gamma(m) \oplus \delta(m)) = g^{a^{-1}}(1110 \oplus 1011) = g^{a^{-1}}(0101) = 1010 = m$.

Suppose, we also want to encrypt the same plaintext $m = 1010$, applying the scheme $\mathcal{E}2$. In this case, we compute $\gamma(m) = g^{a^k}(1010) = 1101$, $g^a(m) = 0101$, $\delta(m) = g^{a^k}(1010) \oplus g^a(1010) = 1101 \oplus 0101 = 1000$ and obtain the ciphertext $(\gamma(m), \delta(m)) = (1101, 1000)$. To decrypt this ciphertext, we compute $g^{a^{-1}}(\gamma(m) \oplus \delta(m)) = g^{a^{-1}}(1101 \oplus 1000) = g^{a^{-1}}(0101) = 1010 = m$.

Now, by applying to $m = 1010$ the encryption scheme $\mathcal{E}3$ under $u = 1100$, we obtain $g^k(u) = 1011$, $\gamma = g^a(g^k(u)) = 1001$, $\delta = g^k(u) \oplus m = 0001$, $g^{a^{-1}}(\gamma) \oplus \delta = 1011 \oplus 0001 = 1010 = m$.

At last, by applying to $m = 1010$ the encryption scheme $\mathcal{E}4$ under $u = 1100$, we obtain $\gamma = g^a(u) = 1101$, $\delta = u \oplus m = 0110$, $g^{a^{-1}}(\gamma) \oplus \delta = 1100 \oplus 0110 = 1010 = m$.

5. ElGamal signature scheme on Boolean functions

The ElGamal signature schemes are all randomized ones, as are all ElGamal encryption schemes. This means that there are many valid signatures for any given message, as are many ciphertexts for any given plaintext. It is known (see, for instance, [4]) there is a method by which an adversary can sign a random message m without knowing the private key by choosing (γ, δ) and m simultaneously. Any adversary knowing a valid signature (γ, δ) for a message m can also sign various other messages [4]. Both of these methods for producing the valid forged signatures do not "enable an opponent to forge a signature on a message of his own choosing". The ElGamal signature schemes on Boolean functions described in this paper below enable an adversary, knowing a valid signature (γ, δ) for a message m, to produce valid forged signatures (γ', δ') for the same message m and do not seem to represent a threat to the security of our ELGamal signature schemes, as do not these methods to the security of the ElGamal signature schemes on groups.

Each of encryption schemes $\mathcal{E}1$–$\mathcal{E}4$ becomes a signature scheme with appendix after appointing keys and equations to play the proper roles in it. So we obtain the following ElGamal signature schemes on Boolean functions. In the description of them, the terms that are not explained once more have the former meanings.

5.1. Signature scheme $\mathcal{S}1$

Private key (for signing) is $\{g(x), a\}$, *public key* (for verifying) is $g^{a^{-1}}(x)$.

Signing: m is a message, $m \in \mathbb{F}_2^n$; $\gamma(m) = g^k(m)$, $\delta(m) = g^k(m) \oplus g^a(m)$, $k \in_R V_L$; $(\gamma(m), \delta(m))$ is the signature.

Verification: accept the signature iff $g^{a^{-1}}(\gamma(m) \oplus \delta(m)) = m$.

5.2. Signature scheme $\mathcal{S}2$

Private key (for signing) is $g^a(x)$, *public key* (for verifying) is $g^{a^{-1}}(x)$, *secret* parameter is a.

Signing: m is a message, $m \in \mathbb{F}_2^n$; $\gamma(m) = g^{a^k}(m)$, $\delta(m) = g^{a^k}(m) \oplus g^a(m)$, $k \in_R V_L$; $(\gamma(m), \delta(m))$ is the signature.

Verification: accept the signature iff $g^{a^{-1}}(\gamma(m) \oplus \delta(m)) = m$.

5.3. Signature scheme $\mathcal{S}3$

Private key (for signing) is $\{g(x), a\}$, *public key* (for verifying) is $g^{a^{-1}}(x)$.

Signing: m is a message, $m \in \mathbb{F}_2^n$; $k \in_R V_L$, $u \in_R \mathbb{F}_2^n$; $\gamma = g^a(g^k(u))$, $\delta = g^k(u) \oplus g^a(m)$; (γ, δ) is the signature.

Verification: accept the signature iff $g^{a^{-1}}(g^{a^{-1}}(\gamma) \oplus \delta) = m$.

5.4. Signature scheme $\mathcal{S}4$

Private key (for signing) is $g^a(x)$, *public key* (for verifying) is $g^{a^{-1}}(x)$, *secret* parameter is a.

Signing: m is a message, $m \in \mathbb{F}_2^n$; $u \in_R \mathbb{F}_2^n$; $\gamma = g^a(u)$, $\delta = u \oplus g^a(m)$; (γ, δ) is the signature.

Verification: accept the signature iff $g^{a^{-1}}(g^{a^{-1}}(\gamma) \oplus \delta) = m$.

5.5. Signature scheme $\mathcal{S}5$

Private key (for signing) is $g^a(x)$, *public key* (for verifying) is $g^{a^{-1}}(x)$, *secret* parameter is a.

Signing: m is a message, $m \in \mathbb{F}_2^n$; $u \in_R \mathbb{F}_2^n$; $\gamma = u$, $\delta = u \oplus g^a(m)$; (γ, δ) is the signature.

Verification: accept the signature iff $g^{a^{-1}}(\gamma \oplus \delta) = m$.

Conclusion

We should say that the paper doesn't provide a solution of a research problem. We have only described a new approach to constructing ElGamal encryption and signature schemes by using the algebra of bijective vector Boolean functions with the negation and permutation operations on the sets of variables and coordinate functions in them. We are not really sure whether the given schemes are secure or not. Naturally this approach has begot quite a large number of new problems for a subsequent research. These problems are directly related to the cryptanalysis of new ElGamal cryptographic schemes described (or not yet) in the paper, to constructing ElGamal signature schemes on Boolean functions with message recovery, and to the development of the used algebra. Computational methods and estimates of their complexity are the most important subject in researching the last.

Acknowledgements

I would like to thank my colleagues Irina A. Pankratova for reading and editing the manuscript and for suggesting me the encryption scheme $\mathcal{E}4$, and Vitaliy A. Romankov for suggesting me the encryption scheme $\mathcal{E}3$.

REFERENCES

1. *Menezes A., van Oorshot P., and Vanstone S.* Handbook of Applied Cryptography. CRC Press Inc., 1997. 661 p.
2. *Agibalov G. P.* Substitution block ciphers with functional keys. Prikladnaya Diskretnaya Matematika, 2017, no. 38, pp. 57–65.
3. *Agibalov G. P. and Pankratova I. A.* Asymmetric cryptosystems on Boolean functions. Prikladnaya Diskretnaya Matematika, 2018, no. 40, pp. 23–33.
4. *Stinson D. R.* Cryptography: Theory and Practice. CRC Press Inc., 1995. 434 p.