BULETINUL ACADEMIEI DE ŞTIINŢE
A REPUBLICII MOLDOVA. MATEMATICA
Number 3(79), 2015, Pages 60–71
ISSN 1024–7696

Generating Cubic Equations as a Method for Public Encryption

N. A. Moldovyan, A. A. Moldovyan, V. A. Shcherbacov

Abstract. The paper introduces a new method for public encryption in which the enciphering process is performed as generating coefficients of some cubic equation over finite ring and the deciphering process is solving the equation. Security of the method is based on difficulty of factoring problem, namely, difficulty of factoring a composite number n that serves as public key. The private key is the pair of primes p and q such that $n = pq$. The deciphering process is performed as solving cubic congruence modulo n. Finding roots of cubic equations in the fields $GF(p)$ and $GF(q)$ is the first step of the decryption. We have described a method for solving cubic equations defined over ground finite fields. The proposed public encryption algorithm has been applied to design bi-deniable encryption protocol.

Mathematics subject classification: 11T71, 11S05, 94A60.
Keywords and phrases: Cryptography, ciphering, public encryption, deniable encryption, public key, cubic equation, Galois field, factoring problem.

Dedicated to the light memory of our colleague and outstanding mathematician Galina Borisovna Belyavskaya

1 Introduction

The public-key encryption algorithm proposed by Rabin [1] uses the public key represented as the pair of integers n and $b < n$, where n is a composite number difficult for factoring; b is an arbitrary integer. To generate an appropriate number n one has to select a pair of strong [2] primes p and q and then compute the value $n = pq$.

Some secret message $M < n$ can be send to the owner of the public key (n, b) in form of the ciphertext C computed as $C = M \cdot (M + b) \pmod{n}$. Decryption of the ciphertext consists in finding roots of the quadratic congruence $x^2 + bx - C \equiv 0 \pmod{n}$. The last can be easily performed using the private key (p, q).

The Rabin cryptosystem is a provably secure public-key cryptosystem, i. e. one can formally prove that decryption of the ciphertext C without knowing the devisors of n is as difficult as factoring the value n. Paper [3] extends the class of provably secure public key cryptosystems based on the difficulty of factoring problem introducing the encryption formula $C = M^k \pmod{n}$, where k $(k \geq 2)$ divides at least one of numbers $p - 1$ and $q - 1$.

Provable security is an important merit of the mentioned public-key cryptosystems. However for all of those cryptosystems the output of the decryption procedure is ambiguous, namely, deciphering process outputs several decrypted texts and only one of them is equal to the encrypted text. The minimum number of the decrypted texts is equal to three and relates to the case $k = 3$ [3].

Recently solving the quadratic congruences like $x^2 - Ax + B \equiv 0 \pmod{n}$ was used in [4] to design the public-key algorithm for encrypting simultaneously two messages into the ciphertext (A, B). That algorithm was put into the base of the sender-deniable encryption protocol. In [4] the authors mentioned potential possibility to construct algorithms for simultaneous encryption of three and four messages into the cryptogram representing the set of coefficients of the cubic and fourth-power congruences, respectively. Naturally, decryption in the last two cases consists in solving congruences like $x^3 - Ax^2 + Bx - D \equiv 0 \pmod{n}$ and $x^4 - Ax^3 + Bx^2 - Dx + E \equiv 0 \pmod{n}$.

The case of using cubic equations represents special interest since it provides potential possibility to design public encryption algorithms that are free from ambiguity of the decryption process, whereas the quadratic and fourth-power equations cannot be used for such purpose.

In this paper we consider the design of the public-encryption algorithms based on using the cubic equation. We consider details of solving cubic equations in the ground field $GF(p)$ in the case when the equations have solutions (this is defined by the design of the encryption algorithm). The described method for solving cubic equations in $GF(p)$ actually determines the decryption algorithm. It is shown that for a particular design the encryption algorithm processes one input message and the decryption procedure outputs one decrypted text, i.e. only the input message.

2 A new method for public encryption

Using the public key n one can encrypt simultaneously three different messages $M < n$, $T < n$, and $U < n$ as generating three coefficients A, B, and D of the cubic equation such that the messages M, T, and U represent three roots of the equation. Since the last values are to be roots, then the encryption is defined by the condition $(x - M)(x - T)(x - U) = x^3 - (M + T + U)x^2 + (MT + MU + TU)x - MTU = 0 \pmod{n}$.

Thus, such idea of constructing the public encryption scheme leads to the enciphering procedure that consists in computing the following three coefficients that compose the ciphertext $C = (A, B, D)$:

$$A = (M + T + U) \bmod n,$$
$$B = (MT + MU + TU) \bmod n,$$
$$D = MTU \bmod n.$$

Respectively, deciphering of the cryptogram C is to be performed as solving the cubic equation

$$x^3 - Ax^2 + Bx - D = 0 \pmod{n}. \qquad (1)$$

Solving equation (1) can be performed by the owner of public key n using his private key (p, q) that represents two divisors of the modulus n. For this purpose he is to solve the cubic equation

$$x^3 - Ax^2 + Bx - D = 0 \pmod p \tag{2}$$

and the cubic equation

$$x^3 - Ax^2 + Bx - D = 0 \pmod q. \tag{3}$$

Let x_{1p}, x_{2p}, and x_{3p} be roots of equation (2) and x_{1q}, x_{2q}, and x_{3q} be roots of equation (3). Then nine roots of the equation (1) can be computed solving nine systems of the congruences of the following form

$$\begin{cases} X_{ij} \equiv x_{ip} \pmod p \\ X_{ij} \equiv x_{jq} \pmod q, \end{cases}$$

where $i, j \in \{1, 2, 3\}$. Three of the computed roots are equal to the sensible messages M, T and U that have been encrypted. Other six roots represent some random values and are to be ignored. Thus, solving cubic equations in the ground finite fields is the central part of the considered public-key encryption scheme.

3 Solving cubic equations in the ground finite field

To find roots of the cubic equation (2) over the ground field $GF(p)$ we propose to solve the equation (relative to the unknown $X \in GF(p^2)$)

$$(1,0)X^3 - (A,0)X^2 + (B,0)X - (D,0) = (0,0) \tag{4}$$

over the extension field $GF(p^2)$ that is defined evidently in the vector form [5] with the unity element $(1, 0)$ and zero element $(0, 0)$.

Addition and multiplication of two elements $(a, b), (c, d) \in GF(p^2)$ are defined with the formulas

$$(a,b) + (c,d) = ((a+c) \bmod p, (b+d) \bmod p) \tag{5}$$

and

$$(a,b)(c,d) = ((ac + kbd) \bmod p, (bc + ad) \bmod p), \tag{6}$$

where $k \in GF(p)$ is some specified constant that is equal to a quadratic non-residue, respectively.

Substitution of the unknown x in (2) by the variable $z = x - 3^{-1}A \bmod p$ gives the following equation (like in [6]) that is identical to (2):

$$z^3 + Pz + Q = 0 \bmod p, \tag{7}$$

where $P = B - \frac{A^2}{3} \bmod p$ and $Q = \frac{AB}{3} - \frac{2A^3}{27} - D \bmod p$.

Respectively, with analogous variable substitution $\mathbf{X} = \mathbf{Z} + (3^{-1} \bmod p, 0)(A, 0)$ one can reduce equation (4) to

$$\mathbf{Z}^3 + \mathbf{PZ} + \mathbf{Q} = (0, 0), \tag{8}$$

where

$$\mathbf{P} = (P, 0) = (B, 0) - \tfrac{(A,0)^2}{3} \text{ and}$$

$$\mathbf{Q} = (Q, 0) = \tfrac{(A,0)(B,0)}{3} - \tfrac{2(A,0)^3}{27} - (D, 0).$$

Since for the given coefficients $(A, 0)$, $(B, 0)$, and $(D, 0)$ the equation (4) has at least one solution, for example, $X = (M \bmod p, 0)$, then the equation (8) also has solution and using the method for solving cubic equations which is described in [6] one can derive the following formula for roots of equation (8)

$$\mathbf{Z} = (z, 0) = \alpha + \beta \tag{9}$$

and the following formula for roots of equation (4)

$$\mathbf{X} = (x, 0) = \frac{(A, 0)}{3} + \alpha + \beta, \tag{10}$$

where

$$\alpha = \sqrt[3]{-\frac{\mathbf{Q}}{2} + \sqrt{\frac{\mathbf{Q^2}}{4} + \frac{\mathbf{P^3}}{27}}}; \quad \beta = \sqrt[3]{-\frac{\mathbf{Q}}{2} - \sqrt{\frac{\mathbf{Q^2}}{4} + \frac{\mathbf{P^3}}{27}}}. \tag{11}$$

For the case under consideration ($p > 3$) there exist three different cubic roots α and three different cubic roots β. In formulas (9) and (10) one should select only pairs of the values α and β which satisfy the condition

$$\alpha\beta = -\frac{\mathbf{P}}{3}. \tag{12}$$

4 About number of roots of the cubic equation in $GF(p)$

To consider type and number of roots of the equations (7) and (8) it is useful to formulate the following preliminary statements.

Lemma 1. *Suppose a prime $p > 3$ and $\mathbf{A}$ is a cubic residue in $GF(p^2)$. Then there exist exactly three different cubic roots from $\mathbf{A}$.*

Proof. An arbitrary prime $p > 3$ can be represented as $p = 6t \pm 1$. Respectively $p^2 - 1 = 36t^2 \pm 12t \Rightarrow 3|p^2 - 1$, where $p^2 - 1$ is the order of the multiplicative group of $GF(p^2)$. The last group is a finite cyclic one, therefore it contains exactly two elements ε and ε^2 having order 3 that are non-trivial cubic roots from $(1, 0) \in GF(p^2)$.

If $\mathbf{B}$ is a cubic root from $\mathbf{A}$, then $\varepsilon\mathbf{B}$ and $\varepsilon^2\mathbf{B}$ are also cubic roots from $\mathbf{A}$. Assumption about existence of the fourth cubic root $\mathbf{B}' = \sqrt[3]{\mathbf{A}}$ leads to contradiction about existence of the third element $\varepsilon' = \mathbf{B}/\mathbf{B}' \neq (1, 0)$ having order 3, such that $\varepsilon' \neq \varepsilon$ and $\varepsilon' \neq \varepsilon^2$. □

Lemma 2. *If the value* $-\frac{\mathbf{Q}}{2} \pm \sqrt{\frac{\mathbf{Q^2}}{4} + \frac{\mathbf{P^3}}{27}}$ *is a cubic residue in* $GF(p^2)$*, then the value* $-\frac{\mathbf{Q}}{2} \mp \sqrt{\frac{\mathbf{Q^2}}{4} + \frac{\mathbf{P^3}}{27}}$ *is also a cubic residue.*

Proof. We have

$$\left(-\frac{\mathbf{Q}}{2} \pm \sqrt{\frac{\mathbf{Q^2}}{4} + \frac{\mathbf{P^3}}{27}}\right)^{\frac{p^2-1}{3}} \left(-\frac{\mathbf{Q}}{2} \mp \sqrt{\frac{\mathbf{Q^2}}{4} + \frac{\mathbf{P^3}}{27}}\right)^{\frac{p^2-1}{3}} =$$

$$\left(-\frac{\mathbf{P^3}}{27}\right)^{\frac{p^2-1}{3}} = (-\tfrac{\mathbf{P}}{3})^{p^2-1} = (1,0).$$

For cubic residue $\left(-\frac{\mathbf{Q}}{2} \pm \sqrt{\frac{\mathbf{Q^2}}{4} + \frac{\mathbf{P^3}}{27}}\right)$ we have $\left(-\frac{\mathbf{Q}}{2} \pm \sqrt{\frac{\mathbf{Q^2}}{4} + \frac{\mathbf{P^3}}{27}}\right)^{\frac{p^2-1}{3}} = (1,0)$. Therefore $\left(-\frac{\mathbf{Q}}{2} \mp \sqrt{\frac{\mathbf{Q^2}}{4} + \frac{\mathbf{P^3}}{27}}\right)^{\frac{p^2-1}{3}} = (1,0)$, i. e. the value $\left(-\frac{\mathbf{Q}}{2} \mp \sqrt{\frac{\mathbf{Q^2}}{4} + \frac{\mathbf{P^3}}{27}}\right)$ is a cubic residue in $GF(p^2)$. □

For some vector $\mathbf{V} = (v,u) \in GF(p^2)$ one can define $\overline{\mathbf{V}} = (v,-u) \in GF(p^2)$.

Lemma 3. *Suppose* $\mathbf{V} = (v,u) \in GF(p^2)$ *is a cubic residue and* $\mathbf{R}$ *is one of the cubic roots from* $\mathbf{V}$*. Then* $\overline{\mathbf{R}}$ *is one of cubic roots from* $\overline{\mathbf{V}}$*.*

Proof. Using formula (6) for some element $(a,b) \in GF(p^2)$ it is easy to get $\left(\overline{(a,b)}\right)^3 = \overline{(a,b)^3}$. For $\mathbf{R}$ we have $\overline{\mathbf{R}}^{\mathbf{3}} = \overline{\mathbf{R^3}} = \overline{\mathbf{V}}$. □

For other two cubic roots from $\mathbf{V}$, i.e. for $\varepsilon\mathbf{R}$ and $\varepsilon^2\mathbf{R}$, we have $\left(\overline{\varepsilon\mathbf{R}}\right)^3 = \overline{\mathbf{V}}$ and $\left(\overline{\varepsilon^2\mathbf{R}}\right)^3 = \overline{\mathbf{V}}$, therefore one can write $\sqrt[3]{\overline{\mathbf{V}}} = \overline{\sqrt[3]{\mathbf{V}}}$.

Lemma 4. *Suppose number* 3 *does not divide* $p-1$ *and* ε, $\varepsilon^2 \in GF(p^2)$ *are two non-trivial cubic roots from the unity element* $(1,0)$*. Then* $\overline{\varepsilon} = \varepsilon^2$ *and* $\overline{\varepsilon}^2 = \varepsilon$*.*

Proof. Taking into account Lemma 3 we have $\overline{\varepsilon}^3 = \overline{\varepsilon^3} = \overline{(1,0)} = (1,0)$ hence $\overline{\varepsilon}$ is one of two non-trivial roots from $(1,0)$ that differs from ε. Therefore $\overline{\varepsilon} = \varepsilon^2$ and $\overline{\varepsilon}^2 = \overline{\varepsilon^2} = \varepsilon$. □

Lemma 5. *Suppose* $a \in GF(p)$ *is a quadratic non-residue. Then for* $(a,0) \in GF(p^2)$ *we have* $\sqrt{(a,0)} = \left(0, \pm\sqrt{k^{-1}a}\right)$*, where* k *is the quadratic non-residue used to define the multiplication operation in* $GF(p^2)$ *with formula (6).*

Proof. Using formula (6) we get $\left(0, \pm\sqrt{k^{-1}a}\right)^2 = (a,0)$. □

In general case computation in (11) should be performed in the field $GF(p^2)$, since the value $\frac{\mathbf{Q^2}}{4}+\frac{\mathbf{P^3}}{27}$ can be equal to a quadratic non-residue in the field $GF(p)$.

In the case under consideration $p > 3$, therefore number 3 divides the value p^2-1 and there exist three different cubic roots in $GF(p^2)$ from each of the values $\left(-\frac{\mathbf{Q}}{2}+\sqrt{\frac{\mathbf{Q^2}}{4}+\frac{\mathbf{P^3}}{27}}\right)$ and $\left(-\frac{\mathbf{Q}}{2}-\sqrt{\frac{\mathbf{Q^2}}{4}+\frac{\mathbf{P^3}}{27}}\right)$. Three values α and three values β define all roots of (8). Types of the lasts depend on the value $\Delta = \frac{\mathbf{Q^2}}{4}+\frac{\mathbf{P^3}}{27} \bmod p$.

4.1 Δ is a quadratic non-residue in $GF(p)$

If Δ is equal to a quadratic non-residue in $GF(p)$, then in formulas (9) and (10) elements α and β are two-dimension vectors the second coordinate of which is not equal to zero. Suppose $\alpha = \mathbf{K}$ and $\beta = \overline{\mathbf{K}}$ are cubic roots from $\alpha^3 = -\mathbf{Q}/2 + \left(0, \sqrt{k^{-1}\Delta}\right)$ and $\beta^3 = -\mathbf{Q}/2 - \left(0, \sqrt{k^{-1}\Delta}\right)$, respectively. Then $\alpha' = \varepsilon\mathbf{K}$ and $\alpha'' = \varepsilon^2\mathbf{K}$ ($\beta' = \overline{\alpha'} = \overline{\varepsilon\mathbf{K}} = \varepsilon^2\overline{\mathbf{K}}$ and $\beta'' = \overline{\alpha''} = \overline{\varepsilon^2\mathbf{K}} = \varepsilon\overline{\mathbf{K}}$) are also cubic roots from α^3 (β^3).

There are possible the following two cases.

Case 1. $3 \nmid (p-1)$. In this case $\mathbf{K}\overline{\mathbf{K}} = -\mathbf{P}/3$. Indeed, $\mathbf{K}\overline{\mathbf{K}} \in GF(p)$, $\varepsilon \in GF(p^2)$, and $\mathbf{P} = (P, 0) \in GF(p)$, therefore $\mathbf{K}\overline{\mathbf{K}} \neq -\varepsilon\mathbf{P}/3$. Each of the following three pairs of the values:

1. $\alpha = \mathbf{K}$ and $\beta = \overline{\mathbf{K}}$;
2. $\alpha' = \varepsilon\mathbf{K}$ and $\beta' = \varepsilon^2\overline{\mathbf{K}}$;
3. $\alpha'' = \varepsilon^2\mathbf{K}$ and $\beta'' = \varepsilon\overline{\mathbf{K}}$;

defines one root of each of the equations (7) and (8), since $\alpha\beta = \alpha'\beta' = \alpha''\beta'' = -\mathbf{P}/3$. These three roots of (7), i.e. the values $\alpha+\beta$, $\alpha'+\beta'$ and $\alpha''+\beta''$, are contained in $GF(p)$. Indeed, for example, $\alpha'+\beta' = \varepsilon\mathbf{K} + \varepsilon^2\overline{\mathbf{K}} = \varepsilon\mathbf{K} + \overline{\varepsilon\mathbf{K}}$. Correspondingly, three roots of (8) are also contained in $GF(p)$.

Case 2. $3|(p-1)$. In this case $\varepsilon \in GF(p)$.

Suppose $\mathbf{K}\overline{\mathbf{K}} = -\varepsilon\mathbf{P}/3$. Then each of the following three pairs of the values:

1. $\alpha = \mathbf{K}$ and $\beta = \varepsilon^2\overline{\mathbf{K}}$;
2. $\alpha' = \varepsilon^2\mathbf{K}$ and $\beta' = \overline{\mathbf{K}}$;
3. $\alpha'' = \varepsilon\mathbf{K}$ and $\beta'' = \varepsilon\overline{\mathbf{K}}$;

defines one root of the equations (7) and (8), since $\alpha\beta = \alpha'\beta' = \alpha''\beta'' = -\mathbf{P}/3$. The first and second roots, i.e. the values $\alpha+\beta = \mathbf{K}+\varepsilon^2\overline{\mathbf{K}}$ and $\alpha'+\beta' = \varepsilon^2\mathbf{K}+\overline{\mathbf{K}}$, are contained in $GF(p^2)$. The third root, i.e. the value $\alpha''+\beta'' = \varepsilon\mathbf{K}+\varepsilon\overline{\mathbf{K}} = \varepsilon(\mathbf{K}+\overline{\mathbf{K}})$, is contained in $GF(p)$.

Suppose $\mathbf{K}\overline{\mathbf{K}} = -\mathbf{P}/3$. Then each of the following three pairs of the values:

1. $\alpha = \mathbf{K}$ and $\beta = \overline{\mathbf{K}}$.

2. $\alpha' = \varepsilon\mathbf{K}$ and $\beta' = \varepsilon^2\overline{\mathbf{K}}$;

3. $\alpha'' = \varepsilon^2\mathbf{K}$ and $\beta'' = \varepsilon\overline{\mathbf{K}}$;

defines one root of the equations (7) and (8), since $\alpha\beta = \alpha'\beta' = \alpha''\beta'' = -\mathbf{P}/3$. The first root is equal to $\alpha + \beta = \mathbf{K} + \overline{\mathbf{K}}$, i.e. it is contained in $GF(p)$. The second and third roots, i.e. the values $\alpha' + \beta' = \varepsilon\mathbf{K} + \varepsilon^2\overline{\mathbf{K}} = \varepsilon\left(\mathbf{K} + \varepsilon\overline{\mathbf{K}}\right)$ and $\alpha'' + \beta'' = \varepsilon^2\mathbf{K} + \varepsilon\overline{\mathbf{K}} = \varepsilon\left(\varepsilon\mathbf{K} + \overline{\mathbf{K}}\right)$, correspondingly, are contained in $GF(p^2)$.

Thus, in Case 2 we have one root in $GF(p)$ and two roots in $GF(p^2)$.

It should be noted that in this paper there are considered cubic equations over $GF(p)$ which have solutions, therefore we do not consider the case when the value $-\mathbf{Q}/2 + \left(0, \sqrt{k^{-1}\Delta}\right)$ is a cubic non-residue in $GF(p^2)$.

4.2 Δ is a quadratic residue in $GF(p)$

If Δ is equal to a quadratic residue in $GF(p)$, then in formula (11) the values $\left(-\frac{\mathbf{Q}}{2} + \sqrt{\frac{\mathbf{Q^2}}{4} + \frac{\mathbf{P^3}}{27}}\right)$ and $\left(-\frac{\mathbf{Q}}{2} - \sqrt{\frac{\mathbf{Q^2}}{4} + \frac{\mathbf{P^3}}{27}}\right)$ are elements of $GF(p)$. We consider the following two subcases.

Case 1. $3|(p-1)$. If the number $\left(-\frac{\mathbf{Q}}{2} + \sqrt{\Delta}\right)$ is a cubic residue in $GF(p)$, then we have three cubic roots from this number and three cubic roots from $\left(-\frac{\mathbf{Q}}{2} - \sqrt{\Delta}\right)$ that are elements of $GF(p)$, hence all three roots of equation (7) and all three roots of equation (8) are elements of the field $GF(p)$. If $\left(-\frac{\mathbf{Q}}{2} - \sqrt{\Delta}\right)$ is a cubic non-residue in $GF(p)$, then the vector $(\left(-\frac{\mathbf{Q}}{2} + \sqrt{\Delta}\right), 0)$ is a cubic non-residue in $GF(p^2)$, since

$$\left(\left(-\frac{\mathbf{Q}}{2} + \sqrt{\Delta}\right), 0\right)^{\frac{p^2-1}{3}} = \left(\left(-\frac{\mathbf{Q}}{2} + \sqrt{\Delta}\right)^{\frac{p-1}{3}(p+1)}, 0\right) =$$
$$(\varepsilon^{p+1}, 0) \neq (1, 0),$$

where ε is one of two non-trivial cubic roots from 1 in $GF(p)$, and equations (7) and (8) have no solutions. However the last situation is out of the consideration of the cubic equations having a solution.

Case 2. $3 \nmid (p-1)$. In $GF(p)$ there exists one cubic root from $\left(-\frac{\mathbf{Q}}{2} + \sqrt{\Delta}\right)$ and one cubic root from $\left(-\frac{\mathbf{Q}}{2} - \sqrt{\Delta}\right)$. Let $K = \sqrt[3]{-\frac{Q}{2} + \sqrt{\frac{Q^2}{4} + \frac{P^3}{27}}}$ and $\tilde{K} = \sqrt[3]{-\frac{Q}{2} - \sqrt{\frac{Q^2}{4} + \frac{P^3}{27}}}$. In $GF(p^2)$ there exists two additional cubic roots from each of the values $\left(-\frac{\mathbf{Q}}{2} + \sqrt{\frac{\mathbf{Q^2}}{4} + \frac{\mathbf{P^3}}{27}}\right)$ (the roots $K\varepsilon$ and $K\varepsilon^2$, where $\varepsilon, \varepsilon^2 \in GF(p^2)$ are non-trivial cubic roots from the unity element $(1,0)$) and $\left(-\frac{\mathbf{Q}}{2} - \sqrt{\frac{\mathbf{Q^2}}{4} + \frac{\mathbf{P^3}}{27}}\right)$ (the roots $\tilde{K}\varepsilon$ and $\tilde{K}\varepsilon^2$). We have $K\tilde{K} = -P/3 \bmod p = \mathbf{P}/3$ and one root of (7) is equal to $K + \tilde{K} \bmod p \in GF(p)$.

We have also $K\varepsilon\tilde{K}\varepsilon^2 = -\mathbf{P}/3$ and $K\varepsilon^2\tilde{K}\varepsilon = -\mathbf{P}/3$ that gives two roots of (7) $K\varepsilon + \tilde{K}\varepsilon^2$ and $K\varepsilon^2 + \tilde{K}\varepsilon$ that are elements of $GF(p^2)$ with the second coordinate different from zero.

4.3 $\mathbf{\Delta = 0}$

We consider the following two cases.

Case 1. $3|(p-1)$. If $-Q/2$ is a cubic residue in $GF(p)$, then in $GF(p)$ there exists three cubic roots from $-Q/2$. Suppose these three roots are the values K, $K' = eK$, and $K'' = e^2K$, where $e, e^2 \in GF(p)$ and are non-trivial cubic roots from 1. Then, taking into account that $K^2 = -P/3$, we have the following three roots of (7): $2K$, $K' + K''$, and $K'' + K'$ that are elements of $GF(p)$, the last two roots being equal.

If $-Q/2$ is a cubic non-residue in $GF(p)$, then the vector $(-Q/2, 0)$ is a cubic non-residue in $GF(p^2)$, since

$$(-Q/2, 0)^{\frac{p^2-1}{3}} = \left((-Q/2)^{\frac{p-1}{3}(p+1)}, 0\right) = \left(e^{p+1}, 0\right) \neq (1, 0),$$

where $e \in GF(p)$ is a cubic root from 1, and there are no solutions for (7) and (8), therefore the last situation is out of the consideration of the cubic equations over $GF(p)$ which have solutions.

Case 2. $3 \nmid (p-1)$. In $GF(p)$ there exists one cubic root from $-Q/2$. Let $K = \sqrt[3]{-Q/2} \bmod p$. In $GF(p^2)$ there exists two additional cubic roots from $-Q/2$, namely, the roots $K' = K\varepsilon$ and $K'' = K\varepsilon^2$, where $\varepsilon, \varepsilon^2 \in GF(p^2)$ are non-trivial cubic roots from the unity element $(1, 0)$. Taking into account that $K^2 = -P/3$, we have the following three roots of equation (7): $2K \in GF(p)$, $(K' + K'')$, $(K'' + K') \in GF(p^2)$, the last two being equal.

Table 1. Number and type of roots of cubic equation (7) with condition that this equation has a solution.

Δ is a quadratic non-residue in $GF(p)$		Δ is a quadratic residue in GF(p)		$\Delta = 0$ $Q^2/4 = -P^3/27 \bmod p$	
$3 \nmid (p-1)$	$3\|(p-1)$	$3\|(p-1)$	$3 \nmid (p-1)$	$3\|(p-1)$	$3 \nmid (p-1)$
Three different roots contained in $GF(p)$	One root in $GF(p)$ and two different roots in $GF(p^2)$	Three different roots contained in $GF(p)$	One root in $GF(p)$ and two different roots in $GF(p^2)$	Three roots contained in $GF(p)$ two of them being equal	One root in $GF(p)$ and two equal roots in $GF(p^2)$

5 Public encryption cryptoscheme free from the decryption ambiguity

To avoid the decryption ambiguity one can put the cubic equation that relates to the Case 2 from Subsections 4.1 and 4.2 into the base of public encryption algorithm. To encrypt the message M one is to generate random numbers T and U such that the value $T^2/4-U$ is quadratic non-residue modulo p and modulo q and then compute the cryptogram in form of the coefficients of the following cubic equation

$$(x-M)(x^2+Tx+U)=x^3-(M+T)x^2+(U-TM)x-MU=0 \bmod n.$$

Thus, the enciphering procedure that consists in computing the following three coefficients that compose the ciphertext $C=(A,B,D)$:

$$\begin{aligned} A &= M+T \bmod n, \\ B &= U-TM \bmod n, \\ D &= MU \bmod n. \end{aligned} \tag{13}$$

The first step of the public encryption, i.e. finding a value that is equal to a non-residue mod$n$, cannot be surely performed without knowing prime divisors of n. Therefore a non-residue N is to be generated by owner of the public key, i.e. he generates his public key as the pair of numbers n and N. Using such public key the encryption of the message M is to be performed as follows:

1. Generate a random number T and compute the value $U=T^2/4-N \bmod n$.
2. Compute the cryptogram $C=(A,B,D)$ using formulas (13).

Decryption of the cryptogram C consists in finding the roots of the equation (1) which are contained in Z_n. Each of the equations (2) and (3) has a unique solution in $GF(p)$ and $GF(q)$, respectively. Therefore there exists only one root of equation (1) that can be computed solving the following system of two congruences

$$\begin{cases} M \equiv M_p \bmod p \\ M \equiv M_q \bmod q, \end{cases} \tag{14}$$

where $M_p \in GF(p)$ and $M_q \in GF(q)$ are roots of equations (2) and (3), respectively. In correspondence with the Chinese remainder theorem the solution of the system (14) is

$$M=\left[M_pq\left(q^{-1} \bmod p\right)+M_qp\left(p^{-1} \bmod q\right)\right] \bmod pq.$$

One of steps of the decryption procedure is finding cubic roots in the field of the two-dimension vectors defined over the ground finite field. Next section considers this case.

6 Finding cubic roots in $GF(p^2)$

Since $3|p^2-1$, there exist three cubic roots from a cubic residue $\mathbf{Y}$ in $GF(p^2)$. In the case $p^2=7 \bmod 9$ it is rather simple to compute one cubic root $\mathbf{J}=\mathbf{Y}^{1/3}$

using the following formula

$$\mathbf{J} = \mathbf{Y}^{\frac{p^2+2}{3}}.$$

Proof that this formula works is as follows

$$\mathbf{J}^3 = (\mathbf{Y})^{\frac{p^2+2}{3}} = \mathbf{Y}\,(\mathbf{Y})^{\frac{p^2-1}{3}} = \mathbf{Y}.$$

Thus, to find a cubic root (if it exists) in the case $3|(p^2-1)$ it is sufficient to perform one exponentiation operation. Two other roots can be computed multiplying the last by the non-trivial roots from the unity element $(1,0)$. For some arbitrary prime p finding cubic roots in $GF(p^2)$ can be performed with method like that described in [7] for finding cubic roots in $GF(p)$, where $3|(p-1)$.

7 Bi-deniable hybrid-encryption protocol secure against active coercer

The public encryption algorithm proposed in Section 5 can be used for designing bi-deniable encryption protocol as follows. The idea is to include in the protocol the entity authentication stage that provides protection against active attackers, including the case of active coercer, and possibility to implement the hidden exchange of single-use public keys [9, 10]. The single-use public keys are used to agree the single-use shared key with which the secret message is derived from the ciphertext directed from sender to receiver. While using the private keys of the sender and receiver and all values sent via communication channel, after the secret communication terminates the coercive attacker is able only to disclose a fake message from the ciphertext.

Suppose $y_A = g^{x_A} \bmod p'$ and $y_B = g^{x_B} \bmod p'$, where p' is a sufficiently large prime and g is a primitive element modulo p', are public keys of the sender and receiver, correspondingly, that are to be used in frame of the ElGamal's signature scheme [11]. The values x_A and x_B are their private keys. Additionally the receiver has other public key (n, N) that is to be used in frame of the public encryption scheme described in Section 5.

The following protocol, where Alice is the sender of secret message $S < n$ and Bob is receiver, presents the bi-deniable hybrid encryption scheme.

1. Alice generates a uniformly random value $k_A < p' - 1$ and computes the value $R_A = g^{k_A} \bmod p'$ and her signature $Sign_A(R_A)$ to R_A. Then she sends the values $Sign_A(R_A)$ and R_A to Bob.

2. Bob verifies the signature $Sign_A(R_A)$. If the signature is invalid he terminates the communication session. Otherwise he generates a uniformly random value $k_B < p' - 1$ and computes the value $R_B = g^{k_B} \bmod p'$, his signatures $Sign_B(R_B)$ to R_B and his signature $Sign_B(R_A)$ to R_A. Then he sends the values R_B, $Sign_B(R_B)$, and $Sign_B(R_A)$ to Alice.

3. Alice verifies the signatures $Sign_B(R_B)$ and $Sign_B(R_A)$. If at least one of the signatures is invalid she terminates the communication session. Otherwise she

generates a fake message $M < n$ and encrypts simultaneously two messages S and M as follows:

3.1. Compute the common key related to the public keys y_A and y_B : $Z_{AB} = y_B^{x_A} \bmod p'$.

3.2. Compute the common single-use key related to the single-use public keys R_A and R_B : $W_{AB} = R_B^{k_A} \bmod p'$.

3.3. Compute the values $T = W_{AB}S \bmod n$ and $U = T^2/4 - N \bmod n$. Then, using the public-encryption algorithm described in Section 5, compute the cryptogram $C = (A, B, D)$ and send C to Bob.

Bob discloses the secret message using the following algorithm.

Decryption algorithm.

1. Using his private key (p, q) Bob finds the root M of equation (1) with coefficients A, B, and D taken from the cryptogram C.

2. Then Bob computes the secret message S as follows:

2.1. Compute the common single-use key related to the single-use public keys R_A and R_B : $W_{AB} = R_A^{k_B} \bmod p'$.

2.2. Compute the value $T = (A - M) \bmod n$.

2.3. Compute the secret message $S = T{W_{AB}}^{-1} \bmod n$.

Dishonest decryption algorithm:

Using Bob's private key (p, q) the coercer computes the root M from the equation (1) with coefficients taken from the cryptogram.

The coercer is able to compute the value $T = A - M \bmod n$, however he is not able to distinguish the values R_A, R_B, and T from uniformly random values and to disclose the secret message S (until he solves the discrete logarithm problem modulo p'), even if he is provided with private keys x_A and x_B.

8 Conclusion

We considered a method for computing the roots of cubic equation over the ground finite field $GF(p)$ in the case when the equation definitely has solutions. This case takes place in the public encryption scheme characterized in simultaneous encryption of three messages [8]. This scheme includes the decryption procedure that is ambiguous. Using the obtained results related to analysis of number and type of the roots of the cubic equations we have proposed a new method for public encryption based on solving the cubic equations, which is free from ambiguity of the decryption procedure. The proposed method has been used to design a new bi-deniable encryption protocol that is sufficiently practical.

Acknowledgements. The first author was supported by Russian Foundation for Basic Research, project # 14-07-00061-a, and the second author was supported by Government of Russian Federation, Grant 074-U01.

References

[1] Rabin M. O. *Digitalized signatures and public key functions as intractable as factorization.* Technical report MIT/LCS/TR-212, MIT Laboratory for Computer Science, 1979.

[2] Gordon J. *Strong primes are easy to find.* Advances in cryptology – EUROCRYPT'84, Springer-Verlag LNCS, 1985, **209**, p. 216–223.

[3] Moldovyan N. A., Moldovyan A. A. *Class of Provably Secure Information Authentication Systems.* Springer Verlag CCIS, 2007, **1**, p. 147-152.

[4] Moldovyan N. A., Moldovyan A. A., Shcherbacov V. A. *Provably Sender-Deniable Encryption Scheme.* Proceedings of The Third Conference of Mathematical Society of the Republic of Moldova (IMCS-50). Chisinau, 19-23 August, Institute of Mathematics and Computer Science, Academy of Sciences of Moldova, 2014, p. 134-141.

[5] Moldovyan N. A., Moldovyanu P. A. *Vector form of the finite fields $GF(p^m)$.* Bul. Acad. Ştiinţe Repub. Mold., Mat., 2009, No. 3, p. 57-63.

[6] Alexeev V. B. *Abel theorem in problems and solutions.* MTSNMO, Moscow, 2001 (in Russian).

[7] Nishihara N., Harasawa R., Sueyoshi Y., Kudo A. *Root computation in finite fields.* IEICE Trans. Fundamentals, 2013, **E96-A**, No. 6, p. 1081-1087.

[8] Moldovyan N. A., Moldovyan A. A., Shcherbacov V. A. *Provably sender-deniable encryption scheme.* Computer Science Journal of Moldova, 2015, **23,** No. 1(67), p. 62-71.

[9] Moldovyan A. A., Moldovyan N. A., Shcherbacov V. A. *Bi-Deniable Public-Key Encryption Protocol Secure Against Active Coercive Adversary.* Bul. Acad. Ştiinţe Repub. Mold., Mat., 2014, No. 3(76), p. 23-29.

[10] Moldovyan A. A., Moldovyan N. A. *Practical Method for Bi-Deniable Public-Key Encryption.* Quasigroups and related systems, 2014, **22**, p. 277-282.

[11] ElGamal T. *A public key cryptosystem and a signature scheme based on discrete logarithms.* IEEE Transactions on Information Theory, 1985, **IT-31**, No. 4. p. 469-472.

Received October 02, 2015

N.A. Moldovyan
St. Petersburg Institute for Informatics
and Automation of Russian Academy of Sciences
14 Liniya, 39, St. Petersburg 199178
Russia
E-mail: *nmold@mail.ru*

A.A. Moldovyan
ITMO University
Kronverksky pr., 10, St.Petersburg, 197101
Russia
E-mail: *maa1305@yandex.ru*

V.A. Shcherbacov
Institute of Mathematics and Computer Science
Academy of Sciences of Moldova
Academiei str. 5, MD−2028 Chişinău
Moldova
E-mail: *scerb@math.md*