Volume-11| Issue-2| 2023 Research Article

MATHEMATICAL FOUNDATIONS OF THE TRANSFER OF THE EL-GAMAL ASYMMETRIC ENCRYPTION ALGORITHM TO ELLIPTIC CURVES

https://doi.org/10.5281/zenodo.7625925

Matyakubov Alisher Samandarovich
National university of Uzbekistan, almasa@list.ru
Berdikhobilova Farangiz
National University of Uzbekistan

Received: 08-02-2023
Accepted: 09-02-2023
Published: 22-02-2023

Abstract:

Keywords:

About: FARS Publishers has been established with the aim of spreading quality scientific information to the research community throughout the universe. Open Access process eliminates the barriers associated with the older publication models, thus matching up with the rapidity of the twenty-first century.

Introduction.

Today, the stability of modern asymmetric algorithms, unlike the stability of symmetric ciphers, is based on certain mathematical problems,. In particular, the problems of decomposition of the given number into prime multipliers (factorization) and discrete logarithmization in the finite field are recognized as the bases of mathematical complexity.

The concept of discrete logarithms was introduced to cryptography in 50s of the 20th century, when rotary machines were replaced by shift registers. Shift registers, in particular, played an important role in determining the position of each element in a given shift sequence.

Today, several modern solving methods of problems of factorization and discrete logarithmization in a finite field, which are considered the fundamental complexity bases of modern asymmetric algorithms, have been developed, and many experts are conducting scientific research in these directions.

In particular, in the science of cryptography, there is a theory called elliptic curves in creating asymmetric algorithms based on new mathematical complexity problems. Below are the main concepts related to elliptic curves [1-6].

We introduce the following concepts.

Definition. If we consider the problem of finding the canonical $n = p_1^{\alpha_1} p_2^{\alpha_2} ....p_s^{\alpha_s}$ decomposition for a given positive integer n, then such a problem is called factorization of the given complex number n, where p_i is an even number of different primes, $\alpha_i \geq 1$.

In practice, especially in the science of cryptology, considers the problem of decomposing the number n = p*q into prime multipliers. Therefore, in the following statements when we will talk about the problem of decomposing (or factorization) into prime multipliers, this situation will be meant.

Definition. Let a, b integers and p prime $1 < a, b < p$. If we consider the problem of finding integer roots in modulo equation $a^x \equiv b(mod\ p)$, then such a problem is called discrete logarithmization problem in the finite field F_p.

Definition. Finding for the given elliptic curve $y^2 = x^3+ax+b(\text{mod } p)$ and its corresponding base point G(x1,y1) , such a number d from equation [d]G(x1,y1) = Q(x2,y2), calls discrete logarithm problem in EC group, where a, b are fixed elements, r is a sufficiently large prime number,

0 < d < n, [n]G(x1,y1) = 0 and n is the order of base point G(x1,y1) , Q(x2,y2) is an open key, and d is a closed key.

Elliptic curves and related concepts

If effective methods for solving factorization and discrete logarithmization problems in a finite field are developed (or proposed) with mathematical complexities of modern asymmetric algorithms, it is not recommended to use such algorithms in practice, and there will be a need to change the algorithm complexity. Then this issue, in turn, raises the following three problems:

1. Changing the requirements for the parameters, i.e. increasing the position of numbers used in the algorithms. However, this situation leads to a significant decrease in the speed of the algorithm.
2. Development of new variants of the asymmetric algorithm through simultaneously use of combinations of factorization and discrete logarithmization of mathematical complexities.
3. Changing the one-sided functions used in algorithms, that is, converting the mathematical complexity to another new complexity. The complexity should be such that with small enough numbers , it would be able to provide a reasonable stability from a practical point of view.

Complexity of analysis

The table below shows the complexity of factorization, discrete logarithmization in a finite field, and discrete logarithmization in an elliptic curve based on the computing capabilities of modern computers when the key lengths are different.

Key length	**Analysis complexity**		
	Factorization	**Discrete logarithmization**	**Discrete logarithmization in EC**

100	$1.3*10^{7}$	$1.3*10^{7}$	$1.1*10^{15}$
200	$7.2*10^{9}$	$7.2*10^{9}$	$1.3*10^{30}$
300	$7.1*10^{11}$	$7.1*10^{11}$	$1.4*10^{45}$
400	$3*10^{13}$	$3*10^{13}$	$1.6*10^{60}$
500	$7.5*10^{14}$	$7.5*10^{14}$	$1.8*10^{75}$
600	$1.3*10^{16}$	$1.3*10^{16}$	$2*10^{90}$
700	$1.7*10^{17}$	$1.7*10^{17}$	$2.3*10^{105}$
800	$1.8*10^{18}$	$1.8*10^{18}$	$2.6*10^{120}$
900	$1.7*10^{19}$	$1.7*10^{19}$	$2.9*10^{135}$
1000	$1.3*10^{20}$	$1.3*10^{20}$	$3.3*10^{150}$

Hence, it is possible to create stabile asymmetric algorithms based on elliptic curves in parameters of small length compared to the complexities of factorization, discrete logarithmization in a finite field. Therefore, below we will get acquainted with the concepts related to elliptic curves [1-7].

Let prime number p>3 is given. Then, we call E is an elliptic curve defined on a finite root field F_p, if E consists set of pair number points (x, y), $x, y \in F_p$, satisfying identity

$y^2 \equiv x^3 + ax + b$ (mod p) . (1)

Here $a, b \in F_p$ and the expression $4a^3 + 27b^2$ is defferent from zero by modulo p.

Today, most asymmetric encryption algorithms are based on the problem of discrete logarithmization in a finite field, and the problem of transfering these algorithms to elliptic curves requires special research.

Transferring of El-Gamal asymmetric encryption algorithm to elliptic curves

Below is the problem of transferring the El-Gamal asymmetric encryption algorithm based on discrete logarithm complexity in a finite field to elliptic curves

El-Gamal encryption algorithm	Transferred to EC complexity El-Gamal encryption algorithm
Generation of algorithm parameters	
1. A high-order prime number **p** is determined. **2.** Integers g, x less than the prime	**1.** For a selected $y = x^3 + ax + b(mod\, p)$, the order of $\boldsymbol{p}$ is determined.

number **p** are chosen. **3.** x is a closed switch. **4.** By calculating $y = g^{x}\ (modp)$, open key is found. **5.** A number satisfying the condition $k < \boldsymbol{p}$ and GCD$(k, p-1) = 1$ is selected.	**2.** Belong to EC, $G(x_0, y_0)$ is found. **3.** The closed key is selected with the condition $0 < d < p - 1$. **4.** By calculating $Q = [d]G(x_0, y_0)$, and the public key is found. **5.** An arbitrary $0 < k < p - 1$ number is chosen.
Encryption process	
1. Encrypted information $\boldsymbol{M}$. **2.** $a = g^{k}modp$ expression calculation. **3.** $b = (M \cdot y^{k})modp$ expression calculation. **4.** (a, b) cipher information.	**1.** Encrypted information $\boldsymbol{M}$. **2.** $a = [k]G(x_0, y_0)$ expression calculation. **3.** $b = [k]Q(x_0, y_0) \cdot M$ expression calculation. **4.** (a, b) cipher information.
Decryption process	
1. Calculate the expression $M = (\frac{b}{a^{x}})modp$ and have open text.	1. Calculate the expression $M = (\frac{b}{[x]a})mod\ p$ and have open text.
Correctness of the algorithm	
$M = \frac{b}{a^{x}} \equiv \frac{y^{k}M}{a^{x}} \equiv \frac{g^{xk}M}{g^{x}k} \equiv$ $\equiv M(modp) = M.$	$M = \frac{b}{[x]a}(mod\ p) \equiv \frac{[k]Q \cdot M}{[x]a} \equiv$ $\equiv \frac{[k][x]G \cdot M}{[x][k]G} = M.$

Summary.

When encryption is carried out using the El-Gamal asymmetric encryption algorithm transferred to the elliptic curve, there is no need to express the open information in the form of elliptic curve points.

However, the El-Gamal asymmetric algorithm is the only algorithm in today's cryptography that does not need to be represented as a point on the elliptic curve when encrypting data using an elliptic curve.

Therefore, there is a need to consider approaches related to the creation of new asymmetric algorithms based on elliptic curves.

REFERENCES:

1. Alguliyev R.M., Imamverdiyev Ya.N. Research of international and national digital signature standards on elliptic curves // Questions of information protection. Moscow, 2005.-№2 (69) – Pp. 2-7.

2. Bolotov A.A. and others. Elementary introduction to elliptical cryptography: algebraic and algorithmic basics. Moscow, MEI, 2006.-328 p.

3. Gorbenko I.D., Balagura D.S. Directional encryption schemes in groups of points on an elliptic curve // Bulletin of Kharkiv National University of Radioelectronics 2002, No. 2.

4. Eremeev M.A., Maksimov Yu.N. Construction of cryptosystems based on the properties of elliptic curves // Information technology security. 1995. No. 2. - pp.52-55.

5. Kuryazov D.M. Algorithm for ensuring message confidentiality using elliptic curves // International Journal of Advanced Trends in Computer Science and Engineering (IJATCSE) Volume 9. №1, 2020, India, pp.295-298.

6. Kuryazov D.M. Optimal asymmetric data encryption algorithm // Global Journal of Computer Science and Technology, volume 21 Issue 2, 2021., pp. 29-33.