УДК 004.056.55

MODIFICATION OF THE SHAMIR AND BLAKLEY THRESHOLD SECRET SHARING SCHEMES WITH ELLIPTIC CURVES

DOI 10.36994 / 2788-5518-2022-01-03-16

***Oleksii Onatskyi**, Ph.D. State university of intelligent technologies and telecommunications, Odessa, Ukraine. onatsky@meta.ua*

***Oleh Dykyi**, Ph.D. National University «Odessa law academy», Odessa, Ukraine.*

***Oksana Zharova**, Ph.D. Odessa polytechnic state university, Odessa, Ukraine. Ksenia.gds@gmail.com*

***Larysa Yona**, Ph.D. State university of intelligent technologies and telecommunications, Odessa, Ukrain., yonalarisa66@gmail.com*

***Abstract:** Secret sharing is a way to improve the reliability of information storage. The secret sharing scheme is a cryptographic method of sharing a secret among a group of users (parties) each of which obtains a piece of a secret, while the original secret is destroyed, and only a certain coalition of users is able to recover the original secret. The newer cryptanalysis methods and tools, as well as the quickly growing power of the computer systems, demand the further increase of the secret sharing scheme's parameters. This leads to the increased resource demand and complexity of the basic field operations. However, these problems may be solved by implementing the secret sharing schemes based on the technique of elliptic curves. In this paper we suggest the threshold schemes of secret sharing based on elliptic curves. Such schemes excel the ones based on multiplicative groups of integers modulo in cryptographic strength. The use of the technique of elliptic curves in the threshold schemes of secret sharing allows to decrease the size of the scheme's parameters significantly, and at the same time, increase its cryptographic strength (i.e. the computational complexity of the cracking task). The cryptographic systems security relies upon the difficulty of calculating the discrete logarithm over a group of points on elliptic curve. In this paper we briefly review the Mignotte, Asmuth-Bloom, Blakley and Shamir secret sharing schemes. We also suggest the modification of the Shamir and Blakley threshold schemes based on elliptic curves, present the example algorithms and estimate the theoretical information strength of such schemes. The recommended elliptic curves in FIPS 186-4, SEC 2: Recommended Elliptic Curve Domain Parameters and DSTU 4145-2002 may be used in the proposed threshold schemes of secret sharing.*

***Key words:** secret sharing scheme, secret share, secret sharing, secret reconstruction, threshold secret sharing scheme, ideal secret sharing scheme, perfect secret sharing scheme, elliptic curves, elliptic curve discrete logarithm problem.*

МОДИФІКАЦІЯ ПОРОГОВИХ СХЕМ РОЗПОДІЛУ СЕКРЕТУ ШАМІРА ТА БЛЕКЛІ НА ЕЛІПТИЧНИХ КРИВИХ

***Онацький О.В.**, к.т.н.. Державний університет інтелектуальних технологій і зв'язку, Одеса, Україна. onatsky@meta.ua*

***Дикий О.В.**, к.ю.н.Національний університет «Одеська юридична академія», Одеса, Україна. olegdykyj@gmail.com*

***Жарова О.В.**, к.ф.-м.н. Державний університет «Одеська політехніка», Одеса, Україна, Ksenia.gds@gmail.com*

***Йона Л.Г.**, к.т.н. Державний університет інтелектуальних технологій і зв'язку, Одеса, Україна. yonalarisa66@gmail.com*

***Анотація:** Одним із методів підвищення надійності зберігання секретної інформації є використання схем розподілу секрету. Схема розподілу секрету це криптографічний метод розподілу секрету серед груп абонентів (учасників), кожному з яких виділяється частка секрету, а вихідний секрет стирається і тільки певна коаліція абонентів може відновити секрет. В роботі запропоновані порогові схеми розподілу секрету на еліптичних кривих, які перевершують по криптографічній стійкості аналогічним схемам, заснованих на використанні мультиплікативних групах кілець відрахувань. Реалізація порогових схем розподілу секрету на основі математичного апарату еліптичних кривих дозволяє значно зменшити розмір параметрів схем і збільшити криптографічну стійкість (обчислювальну складність завдання злому). Безпека криптосистем на еліптичних кривих заснована на труднощах розв'язання задачі дискретного логарифмування в групі точок еліптичної кривої. В роботі наведено короткий огляд схем розподілу секрету Міньотта, Асмута-Блума, Блеклі, Шаміра і запропонована модифікація порогових схем розподілу секрету Шаміра і Блеклі на еліптичних кривих, надані приклади розрахунків і визначено **теоретико-інформаційну** стійкість запропонованих схем. Для реалізації запропонованих порогових схем розподілу можна використовувати Recommended Elliptic Curves, SEC 2: Recommended Elliptic Curve*

Domain Parameters and ДСТУ 4145-2002.

Ключові слова: *схема розподілу секрету, частка секрету, фаза розподілу секрету, фаза відновлення секрету, порогова схема розподілу секрету, схема розподілу секрету ідеальна, схема розподілу секрету досконална, еліптичні криві, проблема дискретного логарифмування в групі точок еліптичної кривої.*

Introduction

In order to protect the secret information from loss or compromise, it is necessary to further improve the reliability of the information storage. One of the methods to achieve better security of the information storage is the use of secret sharing schemes [1, 2]. The secret sharing schemes are widely used in the information holding, transfer and processing systems, which provide the distributed data storage.

In cryptography the secret sharing scheme is any method of distributing the secret among a group of users (parties) such that each of the users receives only a piece of a secret (the so-called share or shadow), and the original secret is destroyed [1]. The secret can be reconstructed later by a certain number of users. The simplest scheme of secret sharing is to divide the secret into pieces.

In this case the secret can be reconstructed only by joining the pieces from all the users together [3]. Therefore, if at least one of the pieces is lost, it is no longer possible to reconstruct the secret.

The secret sharing scheme involves n users and is managed by a trusted dealer. The major task of a dealer is to divide the secret into n shares and distribute them among the user such that any m (or more) users are able to reconstruct the secret using their shares. Meanwhile, any (m – 1) and less users are unable to do that. Such scheme is called (m, n)-threshold secret sharing scheme, where n is the total number of shares the secret was divided into, and m is the number of shares required to reconstruct the original secret [1, 2].

The secret sharing protocol consists of two major stages:

1. *Secret sharing*. The trusted dealer knowing the secret M generates n shares of a secret $b_1, b_2, \ldots, b_n$ and securely transfers the share b_i to the user A_i ($i = 1, \ldots, n$).

2. *Secret reconstruction*. A certain group of m users join their shares b_i and reconstruct the original secret M.

The best known threshold schemes are the Mignotte, Asmuth-Bloom, Blakley and Shamir secret sharing schemes which utilize the multiplicative groups of a large prime order (Table 1) [1, 2].

The newer cryptanalysis methods and tools, as well as the quickly growing power of the computer systems, demand the further increase of the secret sharing scheme's parameters. This leads to the increased resource demand and complexity of the basic field operations. However, these problems may be solved by implementing the secret sharing schemes based on the technique of elliptic curves (EC). This allows to decrease the size of the scheme's parameters and improve its cryptographic strength [4 … 6].

Development

The aim of the present paper is to implement the threshold schemes of secret sharing based on the elliptic curves.

The cryptographic systems based on elliptic curves (Elliptic Curves Cryptography – ECC) [7 … 10] belong to a class of systems with public key. The security of ECC is generally ensured by the complexity of the discrete logarithm calculation over a group of points on elliptic curve (Elliptic Curve Discrete Logarithm Problem – ECDLP) [4, 5, 7]. The solution of the ECDLP is more complex than that of the discrete logarithm problem (DLP) over the prime field Z_p. This is the main advantage of the use of ECC which provide the same level of strength while using the numbers of the smaller size if compared to the more traditional cryptographic systems relaying upon the complexity of factorization or DLP over the finite field. So, for the same size of numbers, the security level of the cryptographic systems with ECs is much higher. Many studies reported [1, 2, 4, 5, 8, 10] that the cryptographic systems based on EC excel the other systems with public keys in two parameters – the level of strength per bit of a key, and the operation speed when implemented in software or hardware elliptic curve known to all the parties; $\#E_p(a, b)$ is the order of the EC group; M – the secret put into the point P_M on the EC.

In the present paper we suggest the modified Shamir and Blakley threshold schemes of secret sharing based on ECs.

Modification of the Shamir threshold scheme. The parameters of this scheme are: n – the number of secret shares; m – the minimum number of users able to reconstruct the secret; $E_p(a, b)$ is an

The dealer chooses random points on the elliptic curve P_1, P_2, …, P_{m-1} and composes a secret polynomial $F(x) = P_M + P_1x + P_2x^2 + \ldots + P_{m-1}x^{m-1}$.

Secret sharing. The dealer calculates the secret share for each user A_i:

$$\begin{aligned} F(1) &= P_M + P_1 + P_2 + \ldots + P_{m-1}; \\ F(2) &\equiv P_M + 2P_1 + 2^2P_2 + \ldots + 2^{m-1}P_{m-1}; \\ &\ldots \\ F(n) &\equiv P_M + nP_1 + n^2P_2 + \ldots + n^{m-1}P_{m-1}. \end{aligned} \quad (1)$$

The users A_i receive the secret share $F(i)$ together with the number i.

Secret reconstruction. Having the different shares $F(i)$, m users are able to reconstruct the polynomial and the secret P_M. The system of linear equations (1) can be solved with respect to the unknown points P_M, P_1, P_2, …, P_{m-1} using the Lagrange polynomial:

$$F(x) = \sum_{i}^{m} l_i(x)F(i) \pmod p, \quad (2)$$

where $$l_i(x) = \prod_{i \neq j} \frac{x - x_j}{x_i - x_j} \pmod p.$$

Table 1.

Threshold secret sharing schemes

Scheme name	Description
1	2
Mignotte	A secret M is chosen so that $\beta < M < \alpha$, where $\alpha = \prod_{i=1}^{m} p_i$, $\beta = \prod_{i=0}^{n-2} p_{n-i}$, $p_1 < p_2 < \ldots < p_n$ are the coprime numbers. *Secret sharing.* The secret shares are calculated as $b_i \equiv M \bmod p_i$ for each $1 \le i \le n$. The users obtain the numbers $\{p_i, b_i\}$. *Secret reconstruction.* A system of congruences $M \equiv b_{i_m} \bmod p_{i_m}$ is solved.
Modified Mignotte	The prime numbers p_1, p_2, …, p_n are chosen so that $p_1 < p_2 < \ldots < p_n$ and $\sqrt[m]{M} < p_i << \sqrt[m-1]{M}$ for all $1 \le i \le n$. *Secret sharing.* The secret shares are calculated as $b_i \equiv M \bmod p_i$ for each $1 \le i \le n$. The users obtain the numbers $\{p_i, b_i\}$. *Secret reconstruction.* A system of congruences $M \equiv b_{i_m} \bmod p_{i_m}$ is solved.
Karnin-Greene-Hellman	$n + 1$ vectors V_0, V_1, …, V_n and a vector U of dimension m are chosen. The secret $M = U \times V_0$ (the vector V_0 is known to all the users). *Secret sharing.* The secret shares are calculated as $b_i = U \times V_i$ for each $1 \le i \le n$. The users obtain the numbers $\{V_i, b_i\}$. *Secret reconstruction.* A system of equations $U = b_i \times V_i$ is solved with respect to U, and then the secret is calculated as $M = U \times V_0$.

Asmuth-Bloom	A prime number q is chosen so that $q > M$, and n coprime numbers so that: $\forall i, p_i > q$; $\forall i, p_i < p_{i+1}$; $p_1 \cdot p_2 \cdot \ldots \cdot p_m > q \cdot p_{n-m+2} \cdot \ldots \cdot p_n$. The number q is known to all the users. *Secret sharing.* A random number r is chosen, and the value $M' = M + rq$ is calculated. The secret shares are calculated as $b_i \equiv M' \bmod p_i$ for each $1 \le i \le n$. The users obtain the numbers $\{p_i, b_i\}$. *Secret reconstruction.* A system of congruences $M' \equiv b_{i_m} \bmod p_{i_m}$ is solved with respect to M' and the secret is calculated as $M \equiv M' \bmod q$.
Blakley	A prime number p is chosen so that $p > M$, and the whole (random) numbers $x_2, x_3, \ldots, x_m \in Z_p$. The secret point is $M, x_2, x_3, \ldots, x_m$. *Secret sharing.* The secret shares are calculated as $b_i \equiv a_{1i}M + a_{2i}x_2 + \ldots + a_{mi}x_m \pmod p$. The users obtain the numbers $\{a_{1i}, a_{2i}, a_{3i}, \ldots, a_{mi}, b_i\}$. *Secret reconstruction.* A system of congruences $a_{1m}M + a_{2m}x_2 + \ldots + a_{mm}x_m \equiv b_m \pmod p$ is solved.
Shamir	A prime number p is chosen so that $p > M$, as well as the random numbers $a_1, a_2, \ldots, a_{m-1} \in Z_p$ and $F(x) \equiv M + a_1x + a_2x^2 + \ldots + a_{m-1}x^{m-1} \pmod p$ is the secret polynomial. *Secret sharing.* The secret shares are calculated as $F(i) \equiv M + ia_1 + i^2a_2 + \ldots + i^{m-1}a_{m-1} \pmod p$ for each $1 \le i \le n$. The users obtain the numbers $\{F(i), i\}$. *Secret reconstruction.* A system of congruences $M + ia_1 + i^2a_2 + \ldots + i^{m-1}a_{m-1} \equiv F(i) \pmod p$ is solved.

The $F(0)$ coefficient in the polynomial (2) determines the chosen point of the secret $M = P_M$.

Example of the Shamir threshold scheme with EC. Suppose we have to implement a (4, 5)-threshold scheme of secret sharing ($m = 4$, $n = 5$). Let $E_{211}(0, -4)$ be the elliptic curve corresponding to the equation $y^2 = x^3 - 4$; $\#E_{211}(0, -4) = 241$; $p = 211$ and the secret is $M = P_M = (5, 200)$.

The dealer chooses random points on the EC $P_1 = (175, 155)$, $P_2 = (198, 139)$, $P_3 = (150, 126)$ and composes the secret polynomial:

$$F(x) = (5, 200) + (175, 155)x + (198, 139)x^2 + (150, 126)x^3.$$

Secret sharing. For each user A_i the dealer calculates the corresponding secret share:

$F(1) = (5, 200) + (175, 155) + (198,139) + (150, 126) = (13, 100) + (2, 2) = (169, 179)$;
$F(2) = (5, 200) + 2(175, 155) + 2^2(198,139) + 2^3(150, 126) = (74, 201) + (147, 114) = (95, 194)$;
$F(3) = (5, 200) + 3(175, 155) + 3^2(198,139) + 3^3(150, 126) = (17, 30) + (137, 37) = (62, 152)$;
$F(4) = (5, 200) + 4(175, 155) + 4^2(198,139) + 4^3(150, 126) = (195, 139) + (16, 100) = (19, 174)$;

$F(5) = (5, 200) + 5(175, 155) + 5^2(198,139) + 5^3(150, 126) = (2, 2) + (155, 96) = (21, 87)$.

The users receive their secret shares $F(1) = (169, 179)$, $F(2) = (95, 194)$, $F(3) = (62, 152)$, $F(4) = (19, 174)$, $F(5) = (21, 87)$.

Secret reconstruction. Suppose the users A_2, A_3, A_4, A_5 pool their shares (95, 194), (62, 152), (19, 174), (21, 87) and use the Lagrange polynomial to obtain:

$$l_2(x) \equiv \frac{(x-3)(x-4)(x-5)}{(2-3)(2-4)(2-5)} \bmod 241 \equiv -\frac{1}{6}(x-3)(x-4)(x-5) \bmod 241 \equiv$$
$$\equiv 40\left(x^3 - 12x^2 + 47x - 60\right) \bmod 241 \equiv \left(40x^3 + 2x^2 + 193x + 10\right) \bmod 241;$$
$$l_3(x) \equiv \frac{(x-2)(x-4)(x-5)}{(3-2)(3-4)(3-5)} \bmod 241 \equiv \frac{1}{2}(x-2)(x-4)(x-5) \bmod 241 \equiv$$
$$\equiv 121\left(x^3 - 11x^2 + 38x - 40\right) \bmod 241 \equiv \left(121x^3 + 115x^2 + 19x + 221\right) \bmod 241;$$
$$l_4(x) \equiv \frac{(x-2)(x-3)(x-5)}{(4-2)(4-3)(4-5)} \bmod 241 \equiv -\frac{1}{2}(x-2)(x-3)(x-5) \bmod 241 \equiv$$
$$\equiv 120\left(x^3 - 10x^2 + 31x - 30\right) \bmod 241 \equiv \left(120x^3 + 5x^2 + 105x + 15\right) \bmod 241;$$
$$l_5(x) \equiv \frac{(x-2)(x-3)(x-4)}{(5-2)(5-3)(5-4)} \bmod 241 \equiv \frac{1}{6}(x-2)(x-3)(x-4) \bmod 241 \equiv$$
$$\equiv 201\left(x^3 - 9x^2 + 26x - 24\right) \bmod 241 \equiv \left(201x^3 + 119x^2 + 165x + 237\right) \bmod 241.$$

The users A_2, A_3, A_4, A_5 reconstruct the secret polynomial and calculate the secret point P_M:

$$F(x) = (95, 194)\,l_2(x) + (62, 152)\,l_3(x) + (19, 174)\,l_4(x) + (21, 87)\,l_5(x) =$$
$$= (95, 194)\left(40x^3 + 2x^2 + 193x + 10\right) + (62, 152)\left(121x^3 + 115x^2 + 19x + 221\right) +$$
$$+ (19, 174)\left(120x^3 + 5x^2 + 105x + 15\right) + (21, 87)\left(201x^3 + 119x^2 + 165x + 237\right) =$$
$$= (183, 153)x^3 + (55, 174)x^2 + (189, 113)x + (94, 154) + (118, 56)x^3 + (21, 124)x^2 +$$
$$+ (87, 50)x + (133, 48) + (52, 17)x^3 + (67, 154)x^2 + (125, 59)x + (55, 174) +$$
$$+ (130, 203)x^3 + (1, 182)x^2 + (192, 10)x + (191, 196) = (150, 126)x^3 + (198, 139)x^2 +$$
$$+ (175, 155)x + (5, 200);$$
$$F(0) = (95, 194)\,l_2(x) + (62, 152)\,l_3(x) + (19, 174)\,l_4(x) + (21, 87)\,l_5(x) = 10(95, 194) +$$
$$+ 221(62, 152) + 15(19, 174) + 237(21, 87) = (94, 154) + (133, 48) + (55, 174) +$$
$$+ (191, 196) = (5, 200).$$

The secret point $M = P_M = F(0) = (5, 200)$ is reconstructed by the users A_2, A_3, A_4, A_5 (Fig. 1).

Let us now consider the case when only three users try to reconstruct the secret – the users A_1, A_2, A_3 or A_3, A_4, A_5. The reconstructed polynomial for the first group (A_1, A_2, A_3) would be $F(x) = (119, 98)x^2 + (125, 59)x + (93, 134)$, and the point $P = (93, 134) \neq P_M$, so the secret is not reconstructed (Fig. 2). The second group (A_3, A_4, A_5) would reconstruct the polynomial $F(x) = (189, 113)x^2 + (19, 37)x + (36, 134)$, and the point $P = (36, 134) \neq P_M$, and again the secret is not reconstructed (Fig. 3). So, by joining the $m - 1$ secret shares, the users reconstruct a random number on EC $P \neq P_M$, which gives no information on the original secret value $M = P_M$.

Modification of the Blakley threshold scheme. The parameters of this scheme are: n – the number of secret shares; m – the minimum number of users allowed to reconstruct the secret; $E_p(a, b)$ is an elliptic curve; $\#E_p(a, b)$ is the order of the curve group; M – the secret put into the point P_M on the EC. The dealer chooses the random points P_2, P_3, …, P_m on the elliptic curve.

Secret sharing. For each user A_i the dealer chooses the random coefficients a_{1i}, a_{2i}, a_{3i}, …, a_{mi} distributed uniformly over Z_p, and calculates the shares:

$$b_i = a_{1i}P_M + a_{2i}P_2 + a_{3i}P_3 + \ldots + a_{mi}P_m. \quad (3)$$

The users A_i receive the numbers $\{a_{1i}, a_{2i}, a_{3i}, \ldots, a_{mi}, b_i\}$.

Secret reconstruction. In order to reconstruct the secret $M = P_M$ having b_i shares, one has to solve the system of equations:

$$\begin{cases} a_{11}P_M + a_{21}P_2 + a_{31}P_3 + \ldots + a_{m1}P_m = b_1; \\ a_{12}P_M + a_{22}P_2 + a_{32}P_3 + \ldots + a_{m2}P_m = b_2; \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ a_{1m}P_M + a_{2m}P_2 + a_{3m}P_3 + \ldots + a_{mm}P_m = b_m, \end{cases} \quad (4)$$

and obtain the secret point P_M.

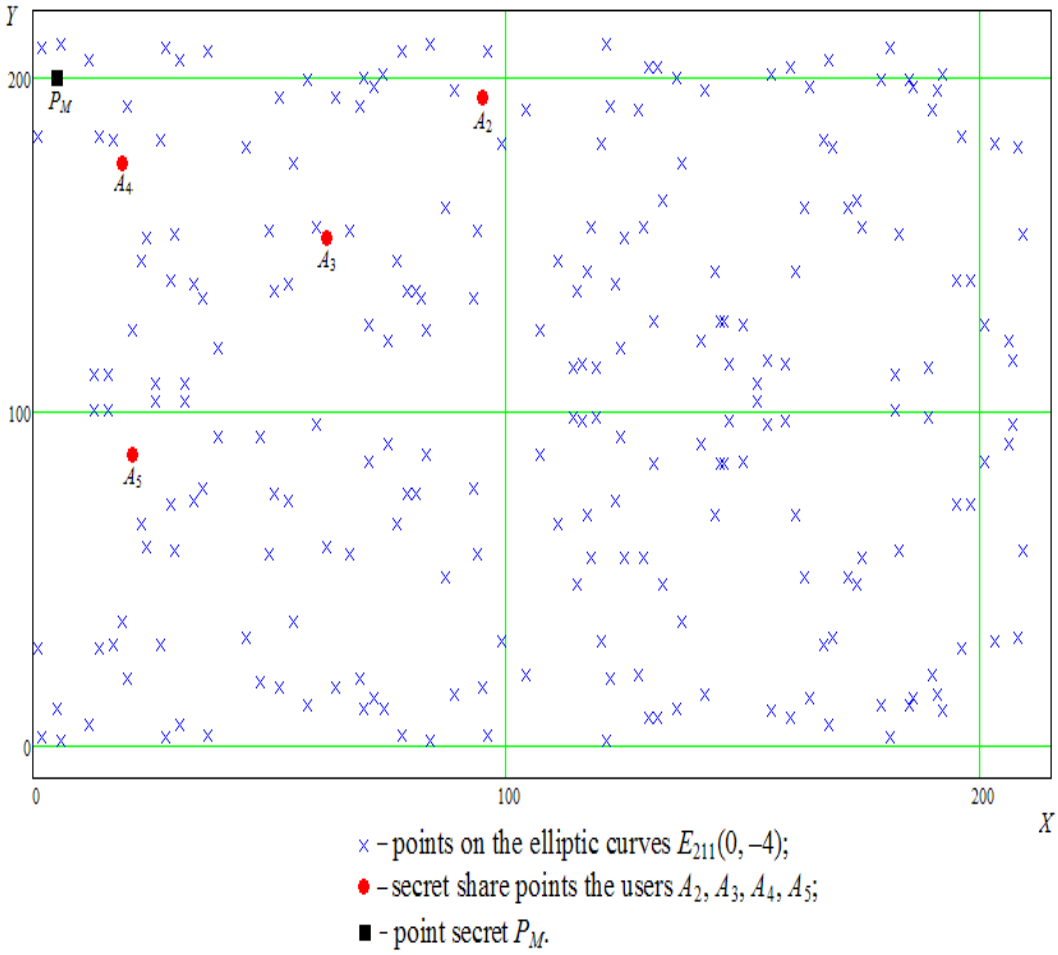

Fig. 1. Secret P_M reconstruction by the users A_2, A_3, A_4 and A_5:

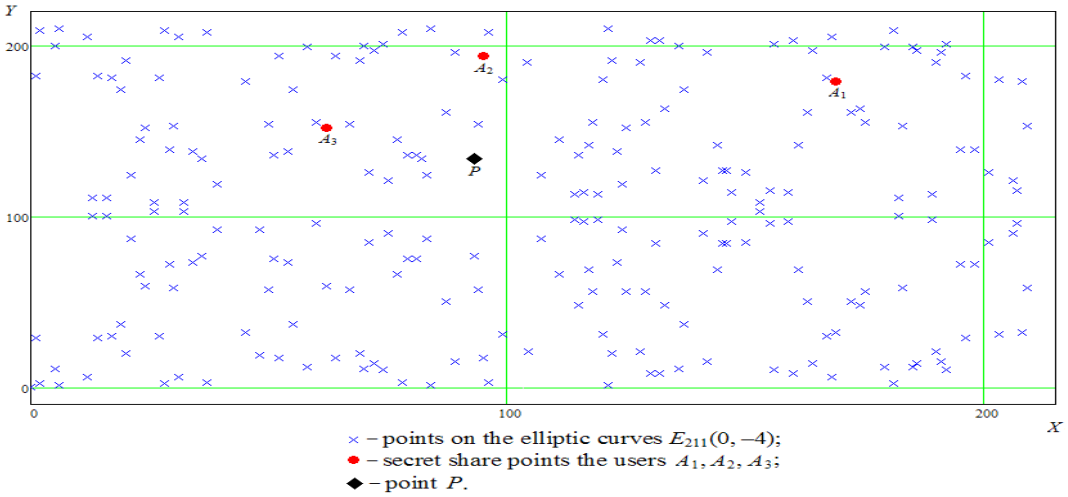

Fig. 2. The secret is not reconstructed by the users A_1, A_2, A_3

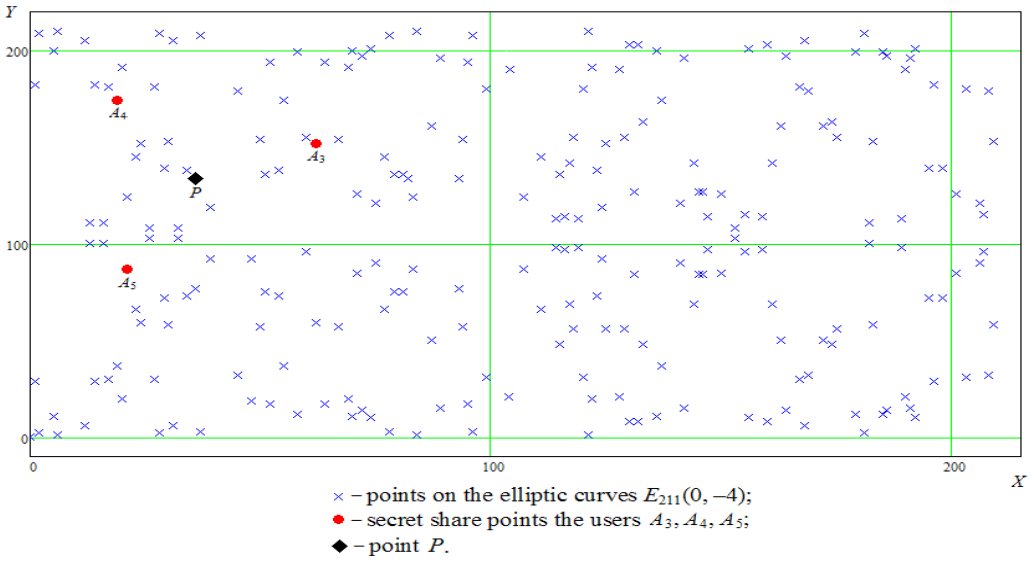

Fig. 3. The secret is not reconstructed by the users A_3, A_4, A_5

Example of the Blakley threshold scheme with EC. Suppose we have to implement the (6, 7)-threshold secret sharing scheme ($m = 6$, $n = 7$) and let the $E_{401}(-5, 90)$ be the elliptic curve corresponding to the equation $y^2 = x^3 - 5x + 90$; $\#E_{401}(-5, 90) = 379$; $p = 401$ and the secret $M = P_M = (326, 344)$.

The dealer chooses the random points on EC: $P_2 = (120, 373)$; $P_3 = (212, 272)$; $P_4 = (185, 95)$; $P_5 = (352, 162)$; $P_6 = (272, 105)$.

Secret sharing. The dealer calculates the secret shares for each user:

– for A_1 choose the coefficients $a_{11} = 25$, $a_{21} = 4$, $a_{31} = 1$, $a_{41} = 87$, $a_{51} = 13$, $a_{61} = 55$ then
$b_1 = 25\ (326, 344) + 4\ (120, 373) + (212, 272) + 87\ (185, 95) + 13\ (352, 162) + 55\ (272, 105) =$
$= (354, 382) + (47, 234) + (212, 272) + (296, 245) + (197, 65) + (233, 196) = (199, 150)$;

– for A_2 choose the coefficients $a_{12} = 17$, $a_{22} = 129$, $a_{32} = 7$, $a_{42} = 49$, $a_{52} = 91$, $a_{62} = 5$ then
$b_2 = 17\ (326, 344) + 129\ (120, 373) + 7\ (212, 272) + 49\ (185, 95) + 91\ (352, 162) + 5\ (272, 105) =$
$= (322, 26) + (326, 57) + (157, 332) + (18, 346) + (151, 158) + (308, 95) = (199, 251)$;

– for A_3 choose the coefficients $a_{13} = 231$, $a_{23} = 63$, $a_{33} = 9$, $a_{43} = 27$, $a_{53} = 3$, $a_{63} = 89$ then
$b_3 = 231\ (326, 344) + 63\ (120, 373) + 9\ (212, 272) + 27\ (185, 95) + 3\ (352, 162) + 89\ (272, 105) =$
$= (110, 35) + (277, 29) + (254, 369) + (322, 26) + (91, 378) + (80, 307) = (157, 332)$;

– for A_4 choose the coefficients $a_{14} = 32$, $a_{24} = 8$, $a_{34} = 301$, $a_{44} = 29$, $a_{54} = 57$, $a_{64} = 3$ then
$b_4 = 32\ (326, 344) + 8\ (120, 373) + 301\ (212, 272) + 29\ (185, 95) + 57\ (352, 162) + 3\ (272, 105) =$
$= (125, 11) + (193, 161) + (360, 335) + (230, 1) + (239, 209) + (194, 48) = (197, 65)$;

– for A_5 choose the coefficients $a_{15} = 19$, $a_{25} = 289$, $a_{35} = 7$, $a_{45} = 43$, $a_{55} = 4$, $a_{65} = 63$ then
$b_5 = 19\ (326, 344) + 289\ (120, 373) + 7\ (212, 272) + 43\ (185, 95) + 4\ (352, 162) + 63\ (272, 105) =$
$= (242, 231) + (107, 151) + (157, 332) + (326, 57) + (127, 357) + (375, 235) = (358, 14)$;

– for A_6 choose the coefficients $a_{16} = 277$, $a_{26} = 9$, $a_{36} = 71$, $a_{46} = 35$, $a_{56} = 42$, $a_{66} = 6$ then

b_6 = 277 (326, 344) + 9 (120, 373) + 71 (212, 272) + 35 (185, 95) + 42 (352, 162) + 6 (272, 105) =
= (127, 357) + (351, 177) + (110, 35) + (63, 20) + (195, 89) + (305, 372) = (62, 77);

– for A_7 choose the coefficients a_{17} = 8, a_{27} = 39, a_{37} = 301, a_{47} = 23, a_{57} = 89, a_{67} = 7 then

b_7 = 8 (326, 344) + 39 (120, 373) + 301 (212, 272) + 23 (185, 95) + 89 (352, 162) + 7 (272, 105) =
= (63, 20) + (379, 299) + (360, 335) + (241, 202) + (61, 227) + (370, 378) = (30, 139).

The users A_i receive the numbers:

A_1 = {25, 4, 1, 87, 13, 55, (199, 150)};
A_2 = {17, 129, 7, 49, 91, 5, (199, 251)};
A_3 = {231, 63, 9, 27, 3, 89, (157, 332)};
A_4 = {32, 8, 301, 29, 57, 3, (197, 65)};
A_5 = {19, 289, 7, 43, 4, 63, (358, 14)};
A_6 = {277, 9, 71, 35, 42, 6, (62, 77)};
A_7 = {8, 39, 301, 23, 89, 7, (30, 139)}.

Secret reconstruction. Suppose the users A_1, A_2, A_4, A_5, A_6, A_7 pool their shares and compose the system of linear equations:

$$\begin{cases} 25P_M + 4P_2 + P_3 + 87P_4 + 13P_5 + 55P_6 = (199, 150); \\ 17P_M + 129P_2 + 7P_3 + 49P_4 + 91P_5 + 5P_6 = (199, 251); \\ 32P_M + 8P_2 + 301P_3 + 29P_4 + 57P_5 + 3P_6 = (197, 65); \\ 19P_M + 289P_2 + 7P_3 + 43P_4 + 4P_5 + 63P_6 = (358, 14); \\ 277P_M + 9P_2 + 71P_3 + 35P_4 + 42P_5 + 6P_6 = (62, 77); \\ 8P_M + 39P_2 + 301P_3 + 23P_4 + 89P_5 + 7P_6 = (30, 139). \end{cases} \quad (5)$$

This system of linear equations may be solved using the Gauss method, through the Cramer's rule, the matrix method or the method of substitution. Let us solve the system (5) using the substitution.

$$\begin{cases} 25P_M = (199, 150) - 4P_2 - P_3 - 87P_4 - 13P_5 - 55P_6; \\ 5P_2 = (107, 250) + 24P_3 - 5P_4 - 67P_5 + 184P_6; \\ 117P_3 = 127P_4 - 71P_5 - 301P_6 - (328, 85); \\ 110P_4 = (221, 44) + 94P_5 + 306P_6; \\ 112P_5 = (235, 237) - 308P_6; \\ 123P_6 = (30, 139) - (120, 28) = (354, 382). \end{cases}$$

$$\begin{cases} P_M = (387, 116) - 364P_2 - 91P_3 - 337P_4 - 46P_5 - 78P_6; \\ P_2 = (254, 369) + 308P_3 - P_4 - 165P_5 + 340P_6; \\ P_3 = 27P_4 - 33P_5 - 252P_6 - (47, 167); \\ P_4 = (342, 39) + 118P_5 + 368P_6; \\ P_5 = (375, 235) - 287P_6; \\ P_6 = (272, 105). \end{cases}$$

$$
\begin{cases}
P_M = (387,116) - 364P_2 - 91P_3 - 337P_4 - 46P_5 - 78P_6 = \\
\quad = (387,116) - 364(120,373) - 91(212,272) - 337(185,95) - 46(352,162) - 78(272,105) = \\
\quad = (387,116) - (238,58) - (237,114) - (197,336) - (243,53) - (109,252) = (326,344); \\
P_2 = (254,369) + 308P_3 - P_4 - 165P_5 + 340P_6 = \\
\quad = (254,369) + 308(212,272) - (185,95) - 165(352,162) + 340(272,105) = \\
\quad = (254,369) + (110,366) - (185,95) - (118,395) + (249,296) = (120,373); \\
P_3 = 27P_4 - 33P_5 - 252P_6 - (47,167) = 27(185,95) - 33(352,162) - 252(272,105) - (47,167) = \\
\quad = (322,26) - (361,394) - (149,152) - (47,167) = (212,272); \\
P_4 = (342,39) + 118P_5 + 368P_6 = (342,39) + 118(352,162) + 368(272,105) = \\
\quad = (342,39) + (2,331) + (338,132) = (185,95); \\
P_5 = (375,235) - 287(272,105) = (352,162); \\
P_6 = (272,105).
\end{cases}
$$

The secret $M = P_M = (326, 344)$ is reconstructed by six users A_1, A_2, A_4, A_5, A_6, A_7 (Fig. 4).

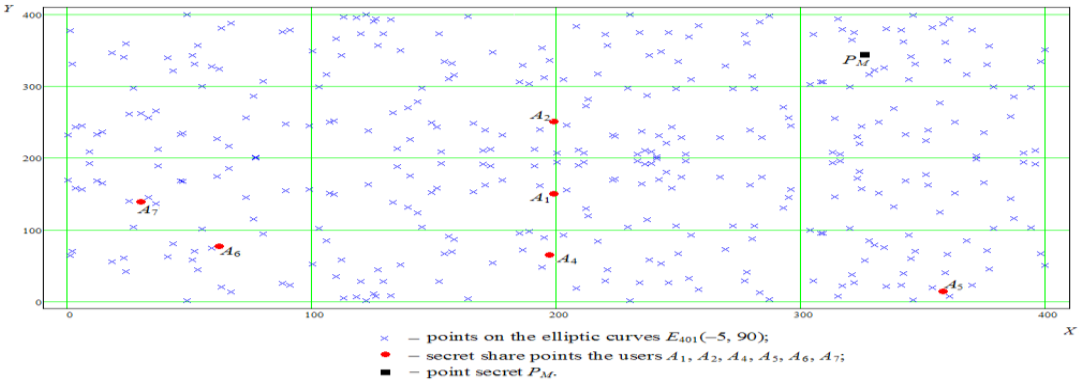

Fig. 4. Secret P_M reconstruction by the users A_1, A_2, A_4, A_5, A_6 and A_7

Let us now consider the case when $m - 1$ users try to reconstruct the secret. The users have to solve the underdetermined system of linear equations, since the number of equations is less than the number of unknowns. Such system has either infinite number of solutions or none at all.

Conclusions

The secret sharing schemes possess the quality of information-theoretic strength. The secret sharing scheme is called ideal if each of the shares consists of the same number of bits as the whole secret [2, 3]. The secret sharing scheme is called perfect if the secret shares of any non-qualified coalition of $m - 1$ users provide no information on the value of the secret [2, 3].

The modified Blakley secret sharing scheme with EC is not ideal, since the size of each share is m times larger than the secret itself. However, this scheme is perfect, since the system of $m - 1$ linear equations with m unknowns has infinite number of solutions. Therefore, the reconstructed secret $M = P_M$ can be any point on EC.

The modified Shamir secret sharing scheme with EC is both perfect and ideal. It is ideal because each user receives the secret share $F(i)$ of the same size as the secret $M = P_M$. It is perfect because by joining less than m secret shares, the users obtain a random point on EC $P \neq P_M$, which provides no information on the real secret $M = P_M$.

The suggested secret sharing schemes based on the group addition law for the elements of the additive Abelian group on EC, excel the similar schemes based on the modulo multiplicative groups in cryptographic strength. Additionally, the complexity of the transformation in the Abelian group on EC can be estimated as $O\left(\log^2 p\right)$, and in the multiplicative group on a field – as $O\left(\log^3 p\right)$, so the advantage of the use of ECs is obvious. The elliptic curves recommended by FIPS 186-4 (Appendix D: NIST Recommended Elliptic Curves) [11], SEC 2: Recommended Elliptic Curve Domain Parameters [12] and DSTU 4145-2002 [13] can be used to implement such secret sharing schemes.

The developed threshold secret sharing schemes with EC can be used in various tasks of the data storage, processing and transfer, the key management, the secure electronic voting and other areas where the protection against the unauthorized access is critical.

Література

1. Schneier B. Applied Cryptography: Protocols, Algorithms and Source Code in C : 20th Anniversary Edition : Wiley, 2015. 784 p.
2. Menezes A., Oorschot P., Vanstone S. Handbook of Applied Cryptography : CRC Press, 1996. 816 p.
3. Погорелов Б. А., Сачков В. Н. Словарь криптографических терминов : М.: МЦНМО, 2006. 91 с.
4. Василенко О. Н. Теоретико-числовые алгоритмы в криптографии : М.: МЦНМО, 2003. 328 с.
5. Stavroulakis P., Stamp M. Handbook of Information and Communication Security : Berlin : Springer-Verlag, 2010. 863 p.
6. Горбенко І. Д., Горбенко Ю. І. Прикладна криптологія. Теорія. Практика : монографія, Харків : Видавництво «Форт», 2012. 880 с.
7. Болотов А. А., Гашков С. Б., Фролов А. Б. Элементарное введение в эллиптическую криптографию: Протоколы криптографии на эллиптических кривых : М.: КомКнига, 2006. 280 с.
8. Hankerson D., Menezes A., Vanstone S. Guide to Elliptic Curve Cryptography : Springer-Verlag, 2004. 358 p.
9. Горбенко Ю. І., Горбенко І. Д. Інфраструктури відкритих ключів. Електронний цифровий підпис. Теорія та практика : монографія, Харків : Видавництво «Форт», 2010. 608 с.
10. An Elliptic Curve Cryptography (ECC).Primer why ECC is the next generation of public key cryptography. The Certicom ‘Catch the Curve’ : White Paper Series, 2004. 24 p.
11. FIPS 186-4. URL: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf
12. SEC 2: Recommended Elliptic Curve Domain Parameters. URL: https://www.secg.org/SEC2-Ver-1.0.pdf
13. ДСТУ 4145-2002. URL: http://itender-online.ru/help/dstu-4145-2002.pdf

References

1. Schneier B. Applied Cryptography: Protocols, Algorithms and Source Code in C : 20th Anniversary Edition : Wiley, 2015. 784 p.
2. Menezes A., Oorschot P., Vanstone S. Handbook of Applied Cryptography : CRC Press, 1996. 816 p.
3. Pogorelov B. A., Sachkov V. N. Slovar kriptograficheskih terminov : M.: MTsNMO, 2006. 91 s.
4. Vasilenko O. N. Teoretiko-chislovyie algoritmyi v kriptografii : M.: MTsNMO, 2003. 328 s.
5. Stavroulakis P., Stamp M. Handbook of Information and Communication Security : Berlin : Springer-Verlag, 2010. 863 p.
6. Ghorbenko I. D., Ghorbenko Ju. I. Prykladna kryptologhija. Teorija. Praktyka : monoghrafija, Kharkiv : Vydavnyctvo «Fort», 2012. 880 s.
7. Bolotov A. A., Gashkov S. B., Frolov A. B. Elementarnoe vvedenie v ellipticheskuyu kriptografiyu: Protokolyi kriptografii na ellipticheskih krivyih : M.: KomKniga, 2006. 280 s.
8. Hankerson D., Menezes A., Vanstone S. Guide to Elliptic Curve Cryptography : Springer-Verlag, 2004. 358 p.
9. Ghorbenko Ju. I., Ghorbenko I. D. Infrastruktury vidkrytykh kljuchiv. Elektronnyj cyfrovyj pidpys. Teorija ta praktyka : monoghrafija, Kharkiv : Vydavnyctvo «Fort», 2010. 608 s.
10. An Elliptic Curve Cryptography (ECC).Primer why ECC is the next generation of public key cryptography. The Certicom ‘Catch the Curve’ : White Paper Series, 2004. 24 p.
11. FIPS 186-4. URL: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf
12. SEC 2: Recommended Elliptic Curve Domain Parameters. URL: https://www.secg.org/SEC2-Ver-1.0.pdf
13. ДСТУ 4145-2002. URL: http://itender-online.ru/help/dstu-4145-2002.pdf