International Journal of Education, Social Science & Humanities.
Finland Academic Research Science Publishers
ISSN: 2945-4492 (online) | (SJIF) = 7.502 Impact factor
Volume-11| Issue-6| 2023 Published: |22-06-2023|

PARAMETRIC ELLIPTIC CURVE IN DATA PROTECTION IN NETWORKS PROTOCOL ANALYSIS BASED ON LINES.

https://doi.org/10.5281/zenodo.8077026

Rustamov Alisher Bahodirovich
PhD, Karshi branch of the Tashkent University of Information Technologies named after Muhammad al-Khwarizmi
arustamov_88@mail.ru)

Abstract

The rapid development of information technologies on a global scale creates new problems along with conveniences. Where computer technologies are highly developed, there first of all the sudden failure of application programs, attacks on software and information, and computer crimes. To this day, the means of cryptographic protection of information is one of the urgent issues of ensuring information security.

Keywords

Resources, threats, privacy, integrity, information, vulnerabilities, communication tools, potential, confidentiality

The information transmitted through the information communication systems has become one of the important conditions for the development of the society. It has become a productive resource, a powerful means of communication between people. Therefore, the requirements of the state authorities and management bodies, as well as society in general, for the speed and quality of information transmission are increasing day by day. It is known that the coefficients of the EECH equations used in traditional cryptosystems are open, and closing them does not significantly contribute to increasing cryptoresistance. Because when the number of EECh points announced as open key reaches the number of closed coefficients, it is not difficult to calculate them.

For example, the equation of EECh is in the form $y_0^2 = x_0^3+ax_0+b \pmod p$, where a and b are unknown, based on the given two points of EECh (x_{01}, y_{01}) and (x_{01}, y_{01}), a and b are the following comparisons:

$a \equiv (y_{02}^2 - x_{02}^3 - y_{01}^2 + x_{01}^3)(y_{02}^2 - y_{01}^2)^{-1} \pmod p$,

$b \equiv -ax_{01} + y_{01}^2 - x_{01}^3\, x_{01}^3 \pmod p$ is considered easy.

When using the group of EECh points with parameters $(PE(F_p); +\backslash)$, closing the coefficients of the EECh equations due to the additional secret parameter R

International Journal of Education, Social Science & Humanities.
Finland Academic Research Science Publishers
ISSN: 2945-4492 (online) | (SJIF) = 7.502 Impact factor
Volume-11| Issue-6| 2023 Published: |22-06-2023|

leads to an increase in cryptosystem cryptoresistance. We call such an EECh a parameterized EECh.

The parameter EECh problem is defined as follows.

Definition: If the non-public EECh point group ($PE(F_p)$; +\) with parameter R is the coordinate x2 of $PE(F_p)$ satisfying the equality Q=d*\G =(x_2,y_2) and if the coordinates (x_1, y_1) of the q-order point G=(x_1, y_1) are given, find the parameters R and d; here, for example, the EECh equation is in the form $y^{\backslash 2}=x^{\backslash 3}+ax+B$ (mod p), coefficients a, B are not given.

In the thesis work, the non-public EECh equation $y^{\backslash 2} = x^{\backslash 3}+ax+B$ (mod p), which is isomorphic to $y_{02} = x_{03}+ax_0+b$, which is a special case of the Weierstrass equation, is used as a parametric EECh equation.

The parametric sum of EECh points is defined as "+\".

The sum of points $Q_1(x_1, y_1)$ and $Q_2(x_2, y_2)$ is defined as $Q_3 = Q_1 +\backslash Q_2$ and is carried out based on the following comparisons:

1) $x_1 \neq x_2$ for, $Q_3(x_3, y_3)$:

$x_3 \equiv (L^2-3)R^{-1}-x_1- x_2)$ (mod p),

$y_3 \equiv L(x_1- x_3)+ y_1^-$ (mod p),

in this: $L \equiv(y_2- y_1)\ (x_2- x_1)^{-1}$ (mod p);

2) $x_1=x_2$, $y_1= y_2 \neq 0$ for, $Q_3=(x_3, y_3)$:

$x_3 \equiv (L^2-3)R^{-1}-2x_1$ (mod p),

$y_3 \equiv L(x_1- x_3) + y_1^-$ (mod p),

in this: $L \equiv(3(R\ x_1^{\backslash 2}+1)+a)(2(R\ y_1+1))^{-1}$ (mod p);

3) $x_1=x_2$, $y_2= y_1$ - for, $Q_1=(x_1, x_2)$ i $Q_2=(x_2, y_1^-)$ the parametric sum of points is equal to zero (infinity) O point.

The following equality holds for the zero point:

$Q+\backslash O = O +\backslash Q = Q$.

The d-parameter summation of the EECh point to itself is defined as the result of the scalar multiplication of this point by d, and this operation is denoted as " *\ ".

It should be noted that in all cases of the generalized EECh equation of Weierstrass, operations with defined parameters on EECh points (addition +\ and multiplication by a scalar *\) do not cause any difficulties. Based on the addition operation with parameter R≥1, a finite commutative group is formed in the set of all points of EECh.

An improved authentication protocol based on the above steps is described below.

Menezes-Q-Vanstone, i.e. - - protocol is an authentication protocol. protocol provides protection against active attacks using long and short-term keys.

International Journal of Education, Social Science & Humanities.
Finland Academic Research Science Publishers
ISSN: 2945-4492 (online) | (SJIF) = 7.502 Impact factor
Volume-11| Issue-6| 2023 Published: |22-06-2023|

In the Menezes-Q-Vanstone protocol based on parameter EEChs, key distribution between participants A and B is carried out using the following algorithm:

Step 1 - Selection of protocol parameters:

– General large prime number r is generated;

– Parameters a, V and R are selected for EECh, where parameter $R \geq 2^{160}$ is known for legal parties and unknown for illegal parties. Selecting the parameters gives the group of parameterized EECh points $PE(F_n)$.

– In $PE(F_n)$, the generating point G=(x,y) is chosen. When choosing G, it is important that the smallest value of N satisfying the condition N*\G=0 is a very large prime number. Parameters G and $PE(F_N)$ of the cryptosystem are parameters known to all participants.

Step 2 – Key generation.

Actions performed by participant A are as follows:

1. $0 < D_A < N$ generates a random number - a secret key.
2. $0 < K_A < N$ generates a random number - a secret key.
3. $Q_A \equiv D_A * \backslash G$ that is, calculates the long-term public key.
4. $R_A \equiv K_A * \backslash G = (x_A, y_A)$ that is, calculates the short-term public key. Then Q_A va R_A sends to participant V.
5. $Y_A \equiv K_A * \backslash Q_B = (x_1, y_1)$ counts the point.
6. $s_A = (K_A + \backslash D_A * \backslash x_A * \backslash x_1) \bmod N$ calculates an integer.

V The actions performed by the participant are as follows:

1. $0 < D_B < N$ generates a random number - a secret key.
2. $0 < K_B < N$ generates a random number - a short-term, one-time key.
3. $Q_B \equiv D_B * \backslash G$ that is, calculates the long-term public key.
4. $R_B \equiv K_B * \backslash G = (x_B, y_B)$ i.e. short-term R_B public key counts. Then Q_B va R_B sends to participant A.
5. $Y_B \equiv K_B * \backslash Q_A = (x_2, y_2)$ counts the point.
6. $s_B = (K_B + \backslash D_B * \backslash x_B * \backslash x_2) \bmod N$ calculates an integer.

Step 2– Calculating the shared secret key.

A the participant does the following:

1. $Y_B \equiv D_A * \backslash R_B = (x_2, y_2)$ counts the point.
2. $K = s_A (R_B + \backslash x_B * \backslash x_2 * \backslash Q_B)$ counts the point.

International Journal of Education, Social Science & Humanities.
Finland Academic Research Science Publishers
ISSN: 2945-4492 (online) | (SJIF) = 7.502 Impact factor
Volume-11| Issue-6| 2023 Published: |22-06-2023|

V and the participant:

3. $Y_A \equiv D_B * \backslash R_A = (x_1, y_1)$ counts the point.
4. $K = s_B(R_A + \backslash x_A * \backslash x_1 * \backslash Q_A)$ counts the point.

As a result of the calculation, both participants generate exactly the same K points.

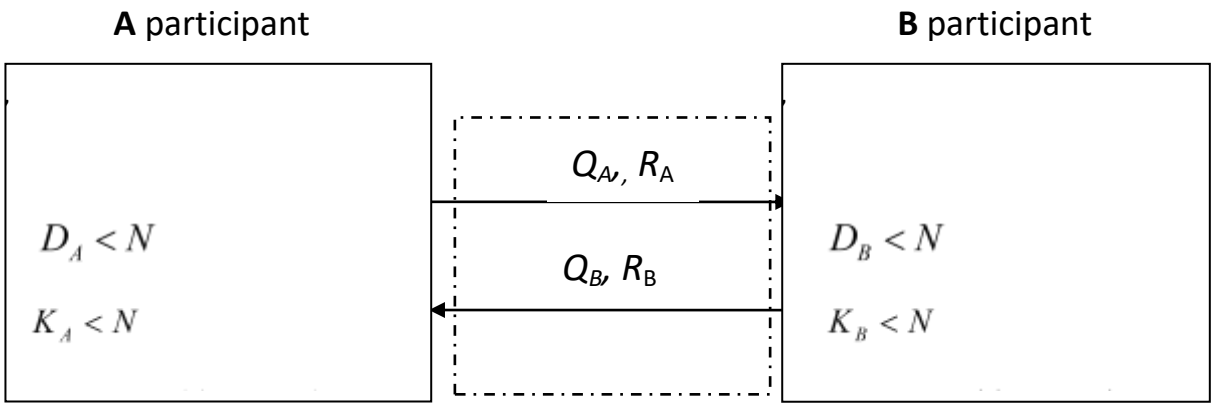

Figure 1. Scheme of the Menezes-Q-Vanstone protocol based on parameterized EEChs

If we check the correctness of the protocol, the shared secret key formula calculated by both participants gives the same value.

A for the participant:

$$K = s_A(R_B + \backslash x_B * \backslash x_2 * \backslash Q_B) = s_A(K_B + \backslash x_B * \backslash x_2 * \backslash D_B) * \backslash G =$$
$$= (K_A + \backslash D_A * \backslash x_A * \backslash x_1) * \backslash (K_B + \backslash x_B * \backslash x_2 * \backslash D_B) * \backslash G .$$

V and for the participant:

$$K = s_B(R_A + \backslash x_A * \backslash x_1 * \backslash Q_A) = s_B(K_A + \backslash x_A * \backslash x_1 * \backslash D_A) * \backslash G =$$
$$= (K_A + \backslash D_A * \backslash x_A * \backslash x_1) * \backslash (K_B + \backslash x_B * \backslash x_2 * \backslash D_B) * \backslash G .$$

Therefore, the shared secret key calculated by these two participants is equal.

LIST OF REFERENCES:

1. Брюс Шнайер «Прикладная криптография. Протокол, алгоритм», Исходные тексты на языке С.И. – М.: ТРИУМФ, 2002.
2. Filatova, S. Chernishova "Authentication in computer systems", 2005.
3. Смарт Н., "Криптография", М. - Техносфера, 2005. 528 с.

4. T. El Gamal, A Public-key Cryptosystem and a Signature Based on Discrete Logarithms. IEEE Trans. Inform. Theory, Vol. IT-31,pp.469-472, July 1985.

5. Miller V. Use of elliptic curves in cryptography // Advances in cryptology — CRYPTO'85 (Santa Barbara, Calif., 1985). 1986. (Lecture Notes in Comput. Sci.; V. 218).

6. P.F.Xasanov, X.P.Xasanov, O.P.Axmedova, A.B.Davlatov «Kriptotahlil va uning maxsus usullari» – Toshkent, 2010 – 175 bet.

7. X.P.Xasanov Takomillashgan diamatrisalar algebralari va parametrli algebra asosida kriptotizimlar yaratish usullari va algoritmlari. Toshkent, FTMTM, 2008.