World Applied Sciences Journal 30 (11): 1566-1569, 2014
ISSN 1818-4952

DOI: 10.5829/idosi.wasj.2014.30.11.14214

Theoretic Development of Active Security Concept on Elliptical Curve

Nikolay Ivanovich Chervyakov, Mikhail Grigorievich Babenko,
Pavel Alekseevich Lyakhov,
Yekaterina Sergeyevna Kiyashko and Maxim Anatolievich Deryabin

North Caucasian Federal University, prospect Kulakova, 2,
355029, Stavropol, Russian Federation

Abstract: The article develops new theoretical approaches to building of active security concept at elliptical curve points which is based on new perfect secret sharing scheme in points of elliptical curve which allows to represent the set of secret shadows and sign the message using hash-function. Use of algorithm for calculation of bi-linear pairing in elliptical curve points allows to build simplified variant of hash-function. The representation of secret in residue number system allows to reduce the size of secret projection and increase the speed of realization of the stages of sharing and restoration of secret.

Key words: Concept of active security · Threshold secret sharing scheme · Residue number system · Elliptical curve · Neural network of finite ring

INTRODUCTION

At modern stage of development of information society the level of information security sometimes determine security of people's lives and state security. In extreme situations, in short-term wars in order to provide communication Ad-hoc networks are used but transmission of the message through Ad-hoc networks the probability of loss or disclosure of the message is very high [1,2]. The main element of encoding is secret key, which is associated with increased requirements its generation, storage, renewal and elimination. [3]. The most perspective method of keys control is method of active security - regular renewal of the key, one-off passwords and spatial distribution of the secret [4]. Active security system is a tool for resistance to active (mobile) enemy which for some time will have an opportunity to break servers number of which is determined by the structure of access of threshold scheme. It is assumed that secret will be changed when the enemy has managed to compromise $(k-1)$ key of secret sharing system where k is threshold number of users. Building of secret sharing schemes built in elliptical curve points is one of the perspective studies in this sphere.

First threshold verifiable secret sharing scheme was offered by Chor in the work [5]. Works [6-9] describe algorithm for digital signature where elliptical curve is used which allows to provide 6-fold reduction of the size of the field while keeping the same level of security. Accelerated basic operation with elliptical curve points using residue number system (RNS) is described in [10-11]. In [4, 12] it is shown that neural network which represents highly-parallel dynamic structure with typology of directed graph which can get output information by means of reaction of its state to input impacts. The structure of algorithm for processing data represented in the residue number system, as well as the structure of neural network have the features of natural parallelism - this allows to use neural network as tool for description of algorithm. So, the task of development of tested threshold system for secret sharing at elliptical curve points with the use of residue number system in neural-network basis is up-to-date for modern science.

Main Part: Checked threshold secret sharing scheme.

Stage 1: Initialization

Corresponding Author: Chervyakov, North Caucasian Federal University, prospect Kulakova, 2,
355029, Stavropol, Russian Federation.

- Elliptical curve in Weierstrass form $E(F_q)$: $y^2 = x^3 + ax + b$ is generated, where $a,b \in F_q$, и $q > 3$, q is prime number, so $|E(F_q)|=cr$, where $r > 2^{225}$ – prime number. Since $\#EC_q(a,b)$ – number of points of elliptical curve in accordance with Hasse theorem must satisfy the following inequality: $q - 2\sqrt{q} + 1 \le \#EC_q(a,b) \le q + 2\sqrt{q+1}$ [13], then moduli set for RNS $p_1,p_2,...,p_r$ are selected in such a way so that the range of residue number system would be higher then $2(q + 2\sqrt{q} + 1)$.
- Every participator of the scheme U_i (1,...,n) gets public key ($G_1,G_2,P,h, p_1,p_2,...,p_r$), where G_1 – is additive group of points of elliptical curve, G_2 – set of integer positive numbers, P is forming element G_1, h: $G_1 \to G_2$. By chance $s_i \in G_2$ is chosen, $P_i = s_iP$ is calculated and P_i is conveyed to dealer and s_i is secret key. If h is hash-functions, then the secret sharing scheme obtains additional attribute, such as simplified digital signature.
- Dealer checks if $P_i \ne P_j$, for all $i \ne j$, in case if $P_i = P_j$ для $i \ne j$, dealer conveys i and j to the user and they repeat step 2.

Stage 2. Sharing of secret

Assume that we have $K_1,K_2,...,K_t$ secrets: K_t

- Random number is chosen $s \in Z^*_\alpha$ and sP is published. The matrixes are calculated:

$$H_i = \begin{bmatrix} h(ss_1P) \bmod p_i & h^2(ss_1P) \bmod p_i & \cdots & h^t(ss_1P) \bmod p_i \\ h(ss_2P) \bmod p_i & h^2(ss_2P) \bmod p_i & \cdots & h^t(ss_2P) \bmod p_i \\ \vdots & \vdots & \ddots & \vdots \\ h(ss_nP) \bmod p_i & h^2(ss_nP) \bmod p_i & \cdots & h^t(ss_nP) \bmod p_i \end{bmatrix}$$

where

$$H = \begin{bmatrix} h(ss_1P) & h^2(ss_1P) & \cdots & h^t(ss_1P) \\ h(ss_2P) & h^2(ss_2P) & \cdots & h^t(ss_2P) \\ \vdots & \vdots & \ddots & \vdots \\ h(ss_nP) & h^2(ss_nP) & \cdots & h^t(ss_nP) \end{bmatrix}$$

And its $rang(M) = t$.

- Now we calculate:

$$R^i = H_i \times K \bmod p_i = \begin{bmatrix} R^i_1 \\ R^i_2 \\ \vdots \\ R^i_n \end{bmatrix}$$

- Secret shadows are conveyed $R_i = (R_i^1, R_i^2, ..., R_i^r)$.

Stage 3. Restoration of secret

- Participator gets s_i from t - system users. The matrix is calculated:

$$K^i = \begin{bmatrix} h(ss_1P) \bmod p_i & h^2(ss_1P) \bmod p_i & \cdots & h^t(ss_1P) \bmod p_i \\ h(ss_2P) \bmod p_i & h^2(ss_2P) \bmod p_i & \cdots & h^t(ss_2P) \bmod p_i \\ \vdots & \vdots & \ddots & \vdots \\ h(ss_tP) \bmod p_i & h^2(ss_tP) \bmod p_i & \cdots & h^t(ss_tP) \bmod p_i \end{bmatrix}^{-1} \times \begin{bmatrix} R^i_1 \\ R^i_2 \\ \vdots \\ R^i_t \end{bmatrix}$$

Calculates K with the use of K' the conveyed information.

Stage 4. Renewal of secret

Dealer generates new s'_i and every participator in the scheme calculates s'_iP.

Analysis of Developed Scheme: Criterion of usability for all $i \neq j$ and $k = \overline{1,t}$ is realization of condition $\left(h(ss_iP) - h\left(ss_jP\right)\right) \bmod p_k \neq 0$.

Assume that prime numbers p_i are l-bit words and the elements of the group of points of elliptical curve $\#EC_q(a,b)$ are L-bit. Then the number of modules in the residue number system will be equal to $r = \left\lceil \frac{2L}{l} \right\rceil$. The result of realization of function h are L- bit numbers. So in order to keep H matrix with size $n \times t$ we need $\frac{n \cdot t \cdot (t+1)}{2} L$ bits of memory.

On the other hand, for storage of H matrix the residue number system needs $n.t \,.\, 2 \,.\, L$ bits of memory. So storage of H matrix in residue number system demands size of memory which is $\frac{t+1}{4}$ times less.

Matrix R, the projection of secret demands $(t+1) \,.\, L \,.\, n$ of memory bits and R matrix represented in residue number system demands $2L \,.\, N$ bits of memory or $\frac{t+1}{2}$ times less.

Multiplication of 2 numbers: a with length w bits b with length s bits needs ws bit operations. Then for multiplication of H matrix by K matrix needs $\frac{n \cdot t \cdot (t+1)}{2} L^2$ bit operations. Since operation $H_iK \bmod p_i$ needs $n.t.l^2$ bit operations then calculation of $H \times K$ needs $n.t.l^2$ operations taking into account that $r = \left\lceil \frac{2L}{l} \right\rceil$, we shall get gain equal to $\frac{(t+1)L^2}{2l^2 r} \approx \frac{(t+1)r}{8}$.

For restoration of secret and calculating K we need $\frac{t^2 \cdot (t+1)}{2} L^2$ bit operations and for calculation in the residue number system K^i we need $t^2.l^2.r$ bit operations. For restoration K from K' we need $r.t.l^2$ bit operations. Then for restoration of secret in the RNS we shall need $\frac{t^2 \cdot (t+1)}{2\left(r \cdot t \cdot l^2 + r \cdot t^2 \cdot l^2\right)} L^2 = \frac{t \cdot L^2}{2 \cdot r \cdot l^2} \approx \frac{t \cdot r}{8}$ times less bit operation than in 2-digit system of calculation.

In developed by us new secret sharing scheme the complexity of calculations also depends on the size of field above which elliptical curve is chosen by exponential law. That is why, for efficient realization of the secret sharing scheme it would be appropriate to use neural network of finite ring (NN FR) [14] and ordinary arithmetic elements which fulfill arithmetic operations.

Synthesized in such a way NN can be realized in PLIS Xilinx and provide high efficiency in solution of tasks of increased size which can not be solved by ordinary ECM. Mentioned above method of data sharing is one of the most perspective tools for safety storage of cryptographic keys in distributed computer networks. Besides that this method is a component of new systems of cryptographic protection of data, namely the systems of active security, development of which is considered the most actual branch of modern cryptography. Active security systems protect from long-term attacks of the enemy and provide safe functioning of distributed computer networks.

The use of NN FR can provide significant advantage in the speed of encoding /decoding of message which makes this threshold secret sharing system efficient for use. However, for transmission of messages through unprotected channels it is necessary to check if this system is perfect. Therefore, for checking we must formulate and prove 2 theorems.

Theorem 1: Any t or more secret shadows allows to restore secret.

Proof: Since group of points on elliptical curve is cyclic and bi-linear pairing of points of elliptical curve should make the direct sum 2 additive groups correspond to 1 multiplicative group, in this case H matrix must correspond to matrix:

$$G = \begin{bmatrix} 1 & g & \cdots & g^t \\ 1 & g^2 & \cdots & g^{2t} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & g^n & \cdots & g^{nt} \end{bmatrix}$$

Let us consider first t lines of G matrix and name this matrix:

$$G' = \begin{bmatrix} 1 & g & \cdots & g^t \\ 1 & g^2 & \cdots & g^{2t} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & g^t & \cdots & g^{t^2} \end{bmatrix}$$

It is Vondermonde matrix whose determinant is different from zero, therefore G matrix lines are linearly independent. Therefore if we know t and more secret

shadows we shall be able to restore the secret if we solve simultaneous equations with *t* and more lines and the same number of columns (unknown values).

The Theorem Is Proved

Theorem 2: Any (t-1) or less secret shadows do not allow to restore secret and get some additional information about it.

Proof: Matrix H is equivalent to G matrix and G matrix is Vondermonde matrix where lines are linearly independent.

Since the number variables of *t* and the number of known parts (*t-1*) or less we get simultaneous linear equations whose solution is solution space with size capacity of 1 or more, therefore the system of equations has set of solutions, so the probability of selection of true secret is 0. All said above allows to conclude that if (*t-1*) or less secret shadows are known the enemy still is not able to get any additional information about secret.

The Theorem Is Proved: Proving of theorems 1 and 2 testify that built neural-network secret sharing scheme is perfect secret sharing scheme.

Inference: Developed by us secret sharing scheme at points of elliptical curve has the following parameters:

- Theorems 1 and 2 demonstrate that it is perfect.
- Secret sharing scheme allows to convey within 1 communication contact a lot of secrets - complete data package describing object in full which increase traffic capacity of communication channel.
- Because of use of hash-function based on bi-linear pairing we get secret sharing scheme with short digital signature.
- Due to use of residue number system the advantage is equal to 4,37 times at average for secret sharing scheme for 10 participators with allowed coalition of 5 participators.

ACKNOWLEDGEMENTS

This work was written in the framework of basic part of State task #8581.

REFERENCES

1. He, J. and E. Dawson, 1994. Multistage secret sharing based on one-way function. Electronics Letters, 19(30): 1591-1592.
2. He, J. and E. Dawson, 1995. Multisecret-sharing scheme based on one-way function. Electronics Letters, 2(31): 93-95.
3. Petrov, A.A., 2000. Computer security. Cryptographic methods of protection. Moscow: DMK.
4. Chervyakov, N., A. Evdokimov and A. Galushkin, 2012. Use of artificial neural networks and the residue number system in cryptography. Moscow: PHYSMATLIT.
5. Chor, B. and S. Goldwasser, 1985. Verifiable secret sharing and achieving simultaneity in the presence of faults. In Proceedings of 26th IEEE Symposium. FOCS, IEEE, pp: 251-260.
6. Chen, W., X. Long, Y.B. Bai and X.P. Gao, 2007. A new dynamic threshold secret sharing scheme from bilinear maps. In International conference on parallel processing workshops, IEEE, pp: 19-22.
7. Wang, S.S., 2011. Verifiable Threshold Scheme in Multi-Secret Sharing Distributions upon Extensions of ECC. Wireless personal communications, 56(1): 173-182.
8. Koblitz, N., 1993. Introduction to elliptic curves and modular forms. New York: Springer, pp: 248.
9. Washington, L.C., 2009. Elliptic curves: Number theory and cryptography. Boca Raton: CRC Press, pp: 524.
10. Omondi, A. and B. Premkumar, 2007. Residue Number Systems: Theory and Implementation. World Scientific Pub Co Inc, pp: 296.
11. Chervyakov, N., V. Averbukh and M. Babenko, 2012. Approximated method to carry out non-modular operations in residue number system. Fundamental Research, 6(1): 189-193.
12. Chervyakov, N. and M. Babenko, 2010. Algebraic approaches to development of algorithms for encoding of alphabet letters by elliptical curve points. Neural computers: development and use, 9: 19-25.
13. Koblitz, N., 1994. A Course in Number Theory and Cryptography. New York: Springer-Verlag, pp: 235.
14. Galushkin, A., 2000. Neural computers. Moscow: IPRZh Radiotechnika.