Complex cryptographic information secure system based on elliptic curves

Chevardin V.E., Zaika Y.L., Sorokin I.A.

Abstract – **there are results of authentication messages cryptographic schemes and pseudorandom sequences generation based on elliptic curves arithmetic research**.

Keywords – **MAC-codes, generator pseudo-random number, elliptic curve, computation complexity, depend cryptotransformation, elliptic curve.**

I. INTRODUCTION

The development of modern information defense subsystems in telecommunications and many different military purpose automatisation systems are directly connected with the design and improvement of cryptographic mechanisms of information security guarantee. Modern conditions of military operations have higher demands to the pseudorandom sequences generation mechanisms (PSGM) and message authentication schemes for modern radiocommunication systems and data communication systems.

II. CRYPTOGRAPHIC SECURE SYSTEM

Modern message authentication schemes and cryptographic schemes of PSGM generation are researched. Generators are usually used for round keys generation in stream and block ciphering mechanisms. Cryptographic generator's key strength and PSGM generation scheme algorithm's strength are evaluated.

Statistical Test Suite and CRYPT-S, NIST PUB FIPS 140-2 systems are used for determination and appreciation of the characteristics PSGM generators.

But the shown way doesn't allow to mathematically prove the cryptographic strength of the generator and also it's statistical characteristics, because of block- and shift cipher character, which the majority of PSGM generation schemes base on.

As the result of my work, one approach type for GSGM generators formation, based on cryptotransformation using in EC points group is examined. Generator schemes, based on transformation in a points curve group $y^2 = x^3 + Ax + B$ are offered.

As the main cryptoprimitive the curve point scalar multiplication is used.

$$P = k * Q, \quad (1)$$

where k – scalar; Q – base curve point.

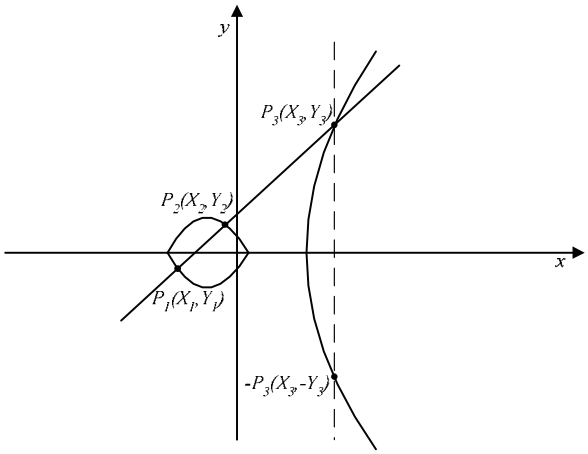

Fig. 1 EC $y^2 = x^3 + Ax + B$

Problem aspects of transformation using in points curve group in PSGM element generation schemes are determined. Cryptotransformation computation complexity of PSGM generation is evaluated. PSGM period borders and cryptotransformation strength of PSGM generation are theoretically based.

Complex information secure system based on transformations in EC points group was developed on the basis of earlier message authentication method and pseudorandom sequences generation scheme.

III. CONCLUSION

So, random point generation time depends on GF(p) elements complexity operations and scalar multiplication. Random base curve point time generation naturally will be bigger then random curve point time generation. It is so because only maximal order points will pick out from the whole number of curve points.

REFERENCES

[1] Kristian Gjosteen, "Comments on Dual-EC-DRBG/NIST SP 800-90 Draft December 2005".

[2] GOST R 34.10-2001 Information technology. Cryptographic data security. Formation and verification processes of [electronic] digital signature.

Chevardin Vladislav, Zaika Yuri, Sorokin Ivan – MITI NTUU "KPI",
str. 44, Poltava, 36009, UKRAINE, chevardin_vlad@mail.ru, zaika_yura@mail.ru, sorokin_i_a@mail.ru.