Deterministic Random Bit Generator on Elliptic Curve Transformations

Vladislav Chevardin

Abstract - **In this paper the method, which uses elliptic curve transformations for random bit generator is given.**

Keywords - **cryptography, discrete logarithms, elliptic curves, random bit generators.**

I. Introduction

In recent years deterministic random bit generators (DRBG) attracted much attention, especially deterministic random bit generators base on elliptic curve (EC) [1,2,3]. Random bit generators is used in lot of applications for information security. The greatest actuality acquired cryptoprimitives on elliptic curve. Elliptic curves offer new permutations that permit to obtain the boundary estimates of the number of DRGB internal states. There is use of full set of isomorphic transformations curve points for increase cryptographically strength of DRBG.

II. New DUAL_EC_DRBG

An elliptic curve mod p is defined by a congruence:

$$E: y^2 = x^3 + ax + b \bmod p\,, \qquad (1)$$

where p is a prime, $p > 3$, and $4a^3 + 27b^2 \neq 0 \bmod p$. (For $p = 2 \vee 3$ the congruence takes a different form.) The elements of the elliptic curve are the solutions (x, y) to the congruence together with an identity element *O*.

The elliptic curves:

$$E: y^2 = x^3 + ax + b \bmod p\,,$$

$$E': y^2 = x^3 + a'x + b' \bmod p\,.$$

The elliptic curve E and E' related isomorphism:

$$\varphi(u,r,s,t) = \begin{cases} X = u^2X' + r, \\ Y = u^3Y' + su^2X' + t, \end{cases} \qquad (2)$$

were $r = 0, s = 0, t = 0, u \neq 0.$

The algorithm DRBG base on elliptic curve transformations (Fig.1).

1. Begin.
2. Generated base parameters: F_p, E_p, point $P = (X_P, Y_P)$ and *Q*, ($n = \# E_p$), $gen\{Z_n\}: \omega'$, $gen\{Z_p\}: \omega$.
3. Generated secret value *seed*, $(seed, n) = 1$.
4. Obtaining session value $t = \omega'^{seed} \bmod n$.
5. Begin cycle:
    a. Calculating $u_i = \omega^{2i} \bmod p$;
    b. Calculating $P'_i = \{u_i^2 X_P, u_i^3 Y_P\}$;
    c. Calculating current $t_i = t * t_{i-1} \bmod n$, $t_i \in Z_n$;
    d. Calculating current $P_i = t_i * P_i'$;
    e. Calculating $s_i = \phi(X[P_i])$;
    f. $r_i = \phi(X[s_i * Q])$;
    g. $b_i = extr(r_i)$.
6. End cycle.
7. End.

The function new DRBG over isomorphic transformation

$$r_i = \phi(X[\phi(X[P_i]) * Q]) = \phi(X[(\phi(X[t_i * \varphi_i(P)]) * Q])\,. \qquad (3)$$

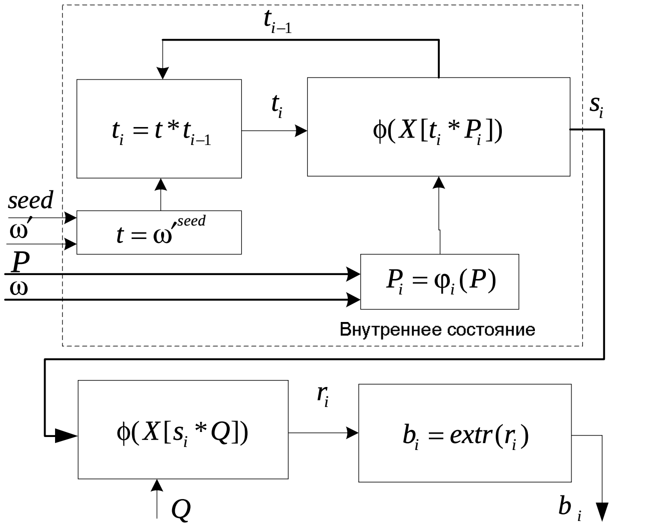

Fig.1 New DRGB base on elliptic curve transformations

III. Conclusion

New method permits to increase the number of internal states of DRGB in $\frac{1}{2}(p-1)$ in comparison to Dual_EC_DRBG and to increase a lower bound of period random bit sequence of generator. New method of elliptic curve transformations which appear to require probabilistic exponential time of invert have been constructed.

References

[1] NIST Special Publication 800-90 Recommendation for Random Number Generation Using Deterministic Random Bit Generators (Revised) / Elaine Barker, John Kelsey // CSDITL NIST. - March 2007.

[2] Burton S. // One-Way Permutations on Elliptic Curves / Burton S. Kaliski, Jr.// Journal of Cryptology (1991) IACR 1991. - P.187-199.

[3] Gjøsteen K. Comments on Dual-EC-DRBG/NIST SP 800-90, Draft December 2005 / Kristian Gjøsteen, March 16, 2006.

Vladislav Chevardin – Ukrainian Technical National University (KPI) , Kovalskiy lane, 22a, 812, Kiev, 03056, UKRAINE,
E-mail: chevardin_vlad@mail.ru