UDC 512.624.95 + 517.772

**V.E. CHEVARDIN**

***Military institute of telecommunication and informatization NTUU (KPI) Kiev, Ukraine***

# A PSEUDORANDOM BIT GENERATOR BASED ON ELLIPTIC CURVE TRANSFORMATIONS

*New method of elliptic curve transformations which appear to require probabilistic exponential time of invert have been constructed. New DRGB mechanism on elliptic curve transformations opens additional ways of developing of modern methods to generate cryptographically strong sequences of pseudorandom bits. The method of generate random bit sequences based on isomorphic transformations of elliptic curve points. The existing method permits to increase a number of internal states is given. A complexity of invert generator to enlarges from increase of internal states. One more result of this paper is obtaining lower bound period pseudorandom bit sequences.*

***Keywords**: cryptography, elliptic curves, random bit generators.*

## Introduction

In recent years deterministic random bit generators (DRBG) attracted much attention, especially deterministic random bit generators base on elliptic curve (EC) [1 – 3]. Random bit generators is used in lot of applications for information security, such as digital signature, message authentication codes, key generation systems and others. The greatest actuality acquired cryptoprimitives on elliptic curve [2 – 5]. Elliptic curves offer new permutations that permit to obtain the boundary estimates of the number of DRGB internal states. Another disadvantage of Dual_EC_DRBG is in conditions which make the period random sequence less than order of the cyclic group. There is use of full set of isomorphic transformations curve points for increase cryptographically strength of DRBG.

## 1. Model DUAL_EC_DRBG

Let E 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. Show DRBG mechanism (fig. 1) and model Dual_EC_DRBG (fig. 2) [1].

The instantiation of this DRBG mechanism requires the selection of an appropriate elliptic curve and curve points. The instantiation of this DRBG mechanism requires the selection of an appropriate elliptic curve and curve points.

The maximum security strength that can be supported by the Dual_EC_DRBG is the security strength of the curve used. Backtracking resistance is inherent in the algorithm, even if the internal state is compromised.

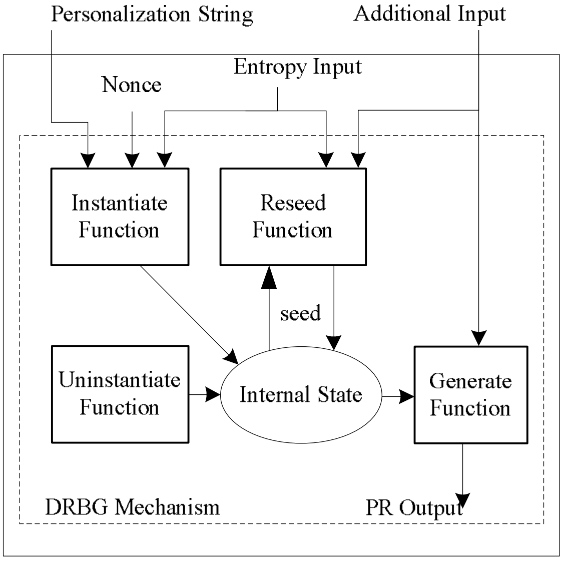

Fig. 1. Model RBG

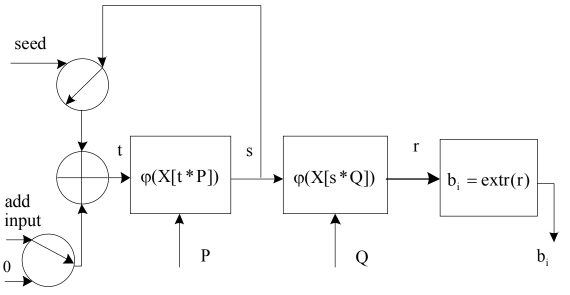

Fig. 2. Model Dual_EC_DRBG

© V.E. Chevardin

Each arrow in the figure 2 represents an Elliptic Curve scalar multiplication operation, followed by the extraction of the X coordinate for the resulting point and for the random output $r_i$, followed by truncation to produce the output. Following a line in the direction of the arrow is the normal operation; inverting the direction implies the ability to solve the ECDLP for that specific curve.

Backtracking resistance is built into the design, as knowledge of $s_1$ does not allow an adversary to determine $s_0$ (and so forth) unless the adversary is able to solve the ECDLP for that specific curve. In addition, knowledge of $r_1$ does not allow an adversary to determine $s_1$ (and so forth) unless the adversary is able to solve the ECDLP for that specific curve.

Show generated random bit sequence method base used isomorphic transformations point that increases number internal state (fig. 3).

## 2. New DRGB mechanism on transformations of elliptic curve

Let two elliptic curves be defined as:

$$E : Y^2 = X^3 + aX + b \bmod p\,, \qquad (2)$$

$$E' : Y^2 = X^3 + a'X + b' \bmod p\,, \qquad (3)$$

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

The elliptic curves E and E' are related isomorphism:

$$\varphi(u, r, s, t) = \begin{cases} X = u^2 X' + r, \\ Y = u^3 Y' + s u^2 X' + t, \end{cases} \qquad (4)$$

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

The new algorithm Dual_EC_DRBG (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 transformation base point $P'_i = \{u_i^2 X_P, u_i^3 Y_P\}$;
   c. Calculating $t_i = t * t_{i-1} \bmod n$, $t_i \in Z_n$;
   d. Calculating $P_i = t_i * P'_i$;
   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 of new DRBG based of isomorphic transformation:

$$r_i = \phi(X[\phi(X[P_i]) * Q])\,,$$

$$r_i = \phi(X[\phi(X[t_i * \varphi_i(P)]) * Q])\,. \qquad (5)$$

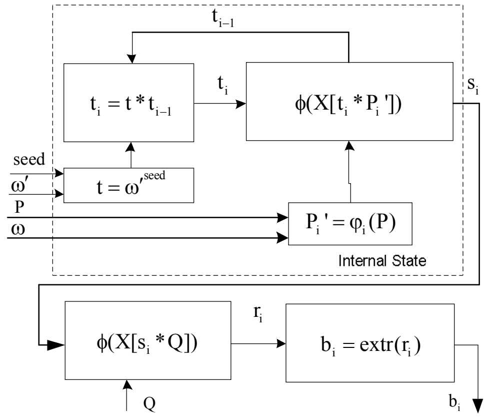

Fig. 3. New model DRGB based on transformations of elliptic curve

## 3. Additional calculation for random bit generation

For obtaining of current point $P_i$ generator $gen\{Z_p\} : \omega$ and generator $gen\{Z_n\} : \omega'$ will be use. A $gen\{Z_p\} : \omega$ will be use for obtaining current value $\varphi_i(P)$ and A $gen\{Z_n\} : \omega'$ will be use for obtaining current value $t_i$.

Parameter u runs all residues in $F_p$.

$$u_i = \omega^{2i} \bmod p\,. \qquad (6)$$

Number of isomorphic points for base point equals $N_{EC} = \frac{1}{2}(p-1)$. So u runs $\{1,..,N_{EC}\}$. Variable $u_i$ is used for calculated value $P'_i = \{u_i^2 X_P, u_i^3 Y_P\}$.

For backtracking resistance value $\omega'$ with secret seed, $(seed, n) = 1$ to used.

$$t = \omega'^{seed} \bmod n = gen\{Z_n\}\,. \qquad (7)$$

For obtaining of current value of scalar $t_i$, generator $gen\{Z_n\} : \omega'$ is used, when n – is an order of cyclic group points (8).

$$t_i = t * t_{i-1} \bmod n\,. \qquad (8)$$

Backtracking resistance of new generator is built into the design, like original Dual_EC_DRBG and number of internal state is increased in to $N_{EC} = 0{,}5 \cdot (p-1)$, which increases complexity of recovery $s_0$ or $s_2$ with $s_1$ (and so forth) unless the adversary is able to solve the ECDLP on isomorphic curve.

Number of isomorphic transformation curve in canonical form equals $N_{EC} = 0,5 \cdot (p-1)$. So number of internal states of new method equals:

$$N = 0,5 \cdot (p-1) \cdot n, \qquad (9)$$

$n$ – order of cyclic group of point; $p$ – characteristic of field.

## Conclusion

New method permits to increase the number of internal states of DRGB in $0,5 \cdot (p-1)$ 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. New DRGB mechanism on elliptic curve transformations opens additional ways of developing of modern methods to generate cryptographically strong sequences of pseudorandom bits. This method may will be modify for increase cryptographically strength. Parameter $gen\{Z_p\} : \omega$ must be obtain with secret seed for increase cryptographically strength. These algorithms will be showed in the future.

## References

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

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

*3. Gjøstee, K. Comments on Dual-EC-DRBG [Text] / K. Gjøstee. – NIST SP 800-90, Draft December 2005. – 2006.*

*4. Impagliazzo, R. Pseudo-random generation from one-way functions [Text] / R. Impagliazzo, L. Levin, M. Luby // Proceedings of the 21st Annual ACM Symposium on Theory of Computing, ACM, New York. – 1989. – P. 12 – 24.*

*5. Kaliski jr., B.S. A pseudo-random bit generator based on elliptic logarithms, Advances in Cryptology: Proceedings of Crypto '86 [Text] / B.S. Kaliski jr. // Lecture Notes in Computer Science. – New York: Springer-Verlag, 1987. – V. 263. – P. 84 – 103.*

*Поступила в редакцию 21.01.2012*

**Рецензент**: д-р техн. наук Л.В. Ковальчук, Інститут спеціального зв'язку та захисту інформації, Київ, Україна.

### ГЕНЕРАТОР ПСЕВДОВИПАДКОВИХ БІТ НА ОСНОВІ ТРАНСФОРМАЦІЙ ЕЛІПТИЧНОЇ КРИВОЇ

***В.Є. Чевардін***

Запропонований новий метод еліптичних перетворень кривої, що вимагає імовірнісного експоненціального часу інвертування. Новий механізм DRGB на еліптичних перетвореннях кривої відкриває додаткові шляхи розвитку сучасних методів, щоб отримувати криптографічний сильні псевдовипадкові бітові послідовності. Метод генерації випадкових бітових послідовностей оснований на ізоморфних трансформаціях точок еліптичної кривої. Запропонований метод відрізняється від існуючих підвищенням числа внутрішніх станів. Це дозволило підвищити складність відтворення закону формування випадкової послідовності. Одним з результатів також є отримання нижньої границі періоду псевдовипадкових послідовностей.

**Ключові слова**: криптографія, еліптичні криві, генератори випадкових послідовностей.

### ГЕНЕРАТОР ПСЕВДОСЛУЧАЙНЫХ БИТ НА ОСНОВЕ ТРАНСФОРМАЦИЙ ЭЛЛИПТИЧЕСКОЙ КРИВОЙ

***В.Е. Чевардин***

Предложен новый метод эллиптических преобразований кривой, требующий вероятностного экспоненциального времени инвертирования. Новый механизм DRGB на эллиптических преобразованиях кривой открывает дополнительные пути развития современных методов, чтобы получать криптографически сильные псевдослучайные битовые последовательности. Метод генерации случайных битовых последовательностей основанный на изоморфных трансформациях точек эллиптической кривой. Предложенный метод отличается от существующих увеличением числа внутренних состояний. Это позволило повысить сложность восстановления закона формирования случайных последовательностей. Одним из результатов также является получение нижней границы периода псевдослучайных последовательностей.

**Ключевые слова**: криптография, эллиптические кривые, генераторы случайных последовательностей.

**Чевардин Владислав Евгеньевич** – канд. техн. наук, докторант Военного института телекоммуникаций и информатизации НТУУ (КПИ), Киев, Украина, e-mail: chevardin_vlad@mail.ru.