УДК 512.624.95 + 517.772

МЕТОД ГЕНЕРАЦИИ ПСЕВДОСЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ НА ОСНОВЕ ИЗОМОРФНЫХ ТРАНСФОРМАЦИЙ ЭЛЛИПТИЧЕСКОЙ КРИВОЙ

А.В. БЕССАЛОВ, В.Е. ЧЕВАРДИН

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 является получение нижней границы периода случайной последовательности.

Ключевые слова: генератор псевдослучайных последовательностей, эллиптические кривые, изоморфные трансформации, трансформации эллиптической кривой.

ВВЕДЕНИЕ

Одним из важнейших направлений в современной криптографии является разработка и усовершенствование алгоритмов генерации псевдослучайных последовательностей (ПСП). Широкое признание получили алгоритмы генерации ПСП: IEEE 182.3, DRBG block cypher (DRBGBC) – генераторы на основе блочных шифров [9], BBS и другие. Достоинством этих генераторов ПСП является достаточно высокая скорость формирования ПСП. Их криптографическая стойкость считается эквивалентной стойкости примитива, используемого в качестве раундовой функции. Так, к примеру, стойкость генератора IEEE 182.3 эквивалентна стойкости криптографического примитива, лежащего в основе блочно-симметричного шифра DES, стойкость DRBGBC эквивалентна стойкости AES [9], стойкость генератора BBS основана на сложности решения задачи факторизации целого числа, стойкость генератора Dual_EC_DRBG [9] эквивалентна сложности решения задачи дискретного логарифмирования в группе точек кривой.

Учитывая большее доверие к криптопреобразованиям с теоретически доказуемой стойкостью, основное внимание современных исследований устремлено на разработку теоретически стойких криптографических методов на основе преобразований в группе точек эллиптической кривой (ЭК) [1-7]. Ярким примером являются алгоритмы генерации ПСП на ЭК. Однако, существующие алгоритмы построения генераторов ПСП на ЭК [1-7] отличаются высокой вычислительной сложностью, что существенно ограничивает их область применения и конкурентоспособность алгоритму BBS.

В связи с этим, целью данной работы является разработка нового метода генерации ПСП на основе арифметики ЭК, что позволит увеличить число внутренних состояний генератора за счет использования множества изоморфизмов базовой ЭК и, как следствие, сложность восстановления закона формирования ПСП. Это в свою очередь позволит уменьшить характеристику поля Галуа и снизить вычислительные затраты при генерации ПСП без снижения криптографической стойкости генератора ПСП.

1. ОСНОВНЫЕ РЕЗУЛЬТАТЫ РАБОТЫ

Пусть гладкая ЭК над простым полем Галуа характеристики $p \neq 2,3$ [8], $E[F_p]$ задана уравнением в канонической форме:

$$EC: y^2 = x^3 + a_4 x + a_6 \pmod p, \qquad (1)$$

где $a_4, a_6 \in F_p$.

Точки кривой представлены двумя координатами $\{X, Y\} \in F_p$, удовлетворяющими уравнению (1), $P_i = (X_{P_i}, Y_{P_i}) \in E_p$, где E_p – абелева группа точек ЭК. Базовой операцией является скалярное произведение точки[1]. Сложность вскрытия криптосистем, основанных на решении задачи дискретного логарифмирования в группе точек EC[2], определяется ρ-методом Полларда $\approx O(\sqrt{n})$ операций сложения точки кривой.

Для ЭК в форме (1) существует изоморфная трансформация $\varphi: \{u, r, s, t\}$ [8]:

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

где переменные $u, r, s, t \in F_p, u \neq 0$ пробегают все значения: 0..p-1.

Используя для базовой кривой EC фиксированный изоморфизм $\varphi(u,r,s,t)$, получим изоморфную кривую EC'. В таком случае, можем любую точку кривой EC однозначно трансформировать в точку изоморфной кривой EC'. Наличие изоморфной кривой дает возможность получить эквивалентную группу точек кривых, которая не является автоморфизмом базовой группы. Это означает, что последовательности точек изоморфных групп эквиваленты, но отличаются друг от друга. Представим изоморфные трансформации группы точек базовой кривой в виде матрицы (таблица).

[1] Скалярное произведение точки кривой – является сложением точки P с собой k раз, $kP = \underbrace{P + P + .. + P}_{k\ раз} \pmod p$, где $k < \#P$, $\#P$ – порядок точки P.

[2] Задача дискретного логарифмирования в группе точек кривой E – по известным параметрам Q, P, p, связанных выражением $P = kQ = \underbrace{Q + Q + .. + Q}_{k\ раз} \pmod p$, необходимо определить неизвестное k.

Таблица

Точки *EC* / Из. транс.	Q_1	Q_2	Q_3	...	Q_n
φ_1	$P^1{}_1$	$P^2{}_1$	$P^3{}_1$	...	$P^n{}_1$
φ_2	$P^1{}_2$	$P^2{}_2$	$P^3{}_2$	...	$P^n{}_2$
...	...	...	...	...	...
φ_{Nec}	$P^1{}_{Nec}$	$P^2{}_{Nec}$	$P^3{}_{Nec}$	...	$P^n{}_{Nec}$

Следовательно, количество различных последовательностей точек будет расти пропорционально числу трансформаций ЭК N_{EC}, что даст положительный эффект при построении генераторов ПСП. В существующих методах [2,3,5-7] для генерации ПСП используются точки из одной группы, соответствующей φ_1 из таблицы, кроме метода [2], в котором предлагается использовать две изоморфные кривые для построения однонаправленной функции. Как показали оценки мощности множества трансформаций ЭК, для канонической формы она растет пропорционально характеристике p поля Галуа, а для трансформации в нормальную форму рост происходит пропорционально p^4. Это свойство ЭК планируется использовать для увеличения числа внутренних состояний генератора ПСП на ЭК, что позволит увеличить нижнюю границу числа выходов генераторов этого класса.

2. СУЩЕСТВУЮЩИЕ МЕТОДЫ ГЕНЕРАЦИИ ПСП НА ОСНОВЕ МЕХАНИЗМА DRBG

В источниках [1-7] представлен ряд подходов к построению генераторов ПСП на основе сложения точек кривой, скалярного произведения, скалярного произведения на двух ЭК [2, 3], спаривания точек кривой [7]. Однако принятым в качестве стандарта является генератор Dual_EC_DRBG [9]. В нем задача восстановления закона формирования ПСП сводится к решению задачи дискретного логарифмирования в группе точек ЭК. Структура генератора DRBG представлена следующей моделью (рис. 1).

Как известно, одним из значимых компонентов такого механизма является источник энтропии, определяемый реализацией DRBG. Функция преобразования метки seed (Reseed) обеспечивает секретность выхода DRBG, если seed или внутреннее состояние стало известным.

Энтропия источника влияет на количество внутренних состояний (рис. 1), следовательно, и на нижнюю границу множества выходных состояний DRBG. Увеличение числа внутренних состояний позволит увеличить сложность восстановления закона формирования ПСП злоумышленником. Рассмотрим функциональную модель генератора Dual_EC_DRBG [9] (рис. 2).

Внутреннее состояние генератора определяется параметрами: (*s*, *seedlen*, *p*, *a*, *b*, *n, P, Q, security_strength, prediction_resistance_flag, reseed_counter*) [9], где *P, Q* – базовые точки кривой порядка *n*, *s* – секретный скаляр.

Функция генерации представлена выражением (3).

$$r_i = \phi(X\left[\phi(X\left[t_{i-1} * P\right]) * Q\right]), \qquad (3)$$

где s – секретное число; $t_0 = seed = hash(s)$; r_i – выход генератора.

Число выходов генератора Dual_EC_DRBG равно числу координат точек циклической

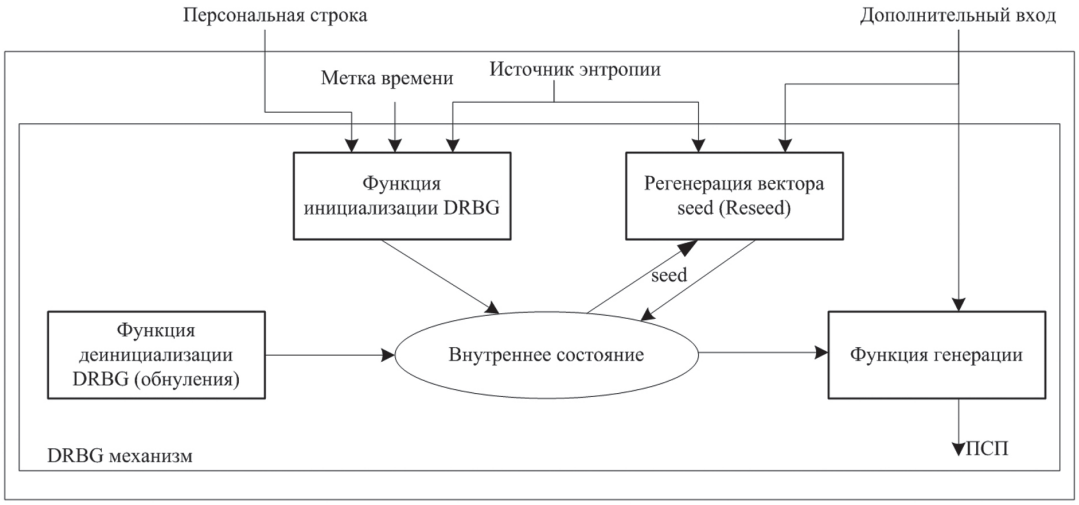

Рис. 1. Функциональная модель DRBG

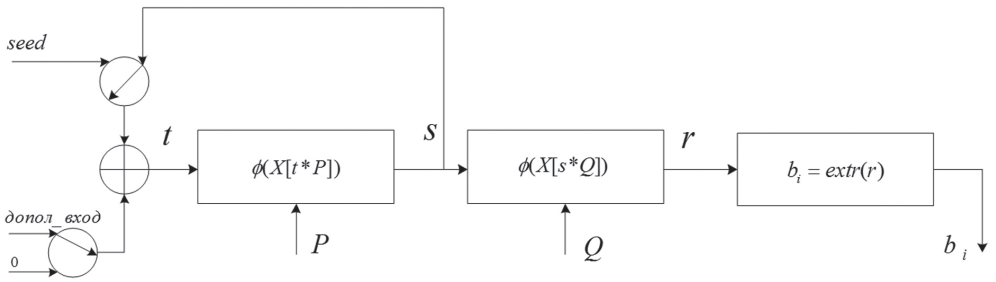

Рис. 2. Модель генератора Dual_EC_DRBG

группы точки Q, т.е. ограничено сверху порядком базовой точки, $n = \#Q$.

Нижняя граница периода Dual_EC_DRBG определяется числом внутренних состояний. Для обеспечения требуемой стойкости эта граница должна быть не ниже n. Учитывая, что внутреннее состояние генератора определяется значением $X[t*P]$, число различных состояний будет не более $n/2$. Верхняя граница будет зависеть от способа генерации скаляра t. Таким образом, возникает ситуация, когда нижняя граница периода ПСП будет равна числу различных $X[t*P]$.

Рассмотрим одну из возможностей, позволяющих увеличить число внутренних состояний генератора Dual_EC_DRBG.

3. МЕТОД ГЕНЕРАЦИИ ПСП НА ОСНОВЕ ИЗОМОРФНЫХ ТРАНСФОРМАЦИЙ ТОЧЕК ЭК

Пусть задана базовая ЭК в канонической форме, EC. Изоморфные трансформации этой кривой заданы выражением (2). Для описания алгоритма генерации генератора (рис. 3) зафиксируем следующие структурные элементы:

1. Базовая эллиптическая кривая EC.
2. Базовые точки кривой – P и Q.
3. Операция получения изоморфной базовой точки $P_i = \varphi_i(P)$.
4. Операция получения текущей точки кривой: $f(P_{i-1}, P_i) = P' = t_i * P_i$.
5. Операция извлечения битов из координаты X текущей точки кривой: $r_i = \phi(X[P_i])$ согласно [9].

Представим функцию генерации текущей точки P':

$$f(P_{i-1}, \varphi_j(P)) = P' = t_i * \varphi_i(P). \quad (4)$$

Используя выражение (4) представим функцию генерации:

$$r_i = \phi(X\left[\phi(X\left[P_i\right])*Q\right]) = \phi(X\left[(\phi(X\left[t_i*\varphi_i(P)\right])*Q\right]), \quad (5)$$

где ϕ – функция преобразования координаты X в целое число.

Изначально устанавливается состояние генератора: вводится характеристика p поля Галуа, коэффициенты базовой кривой EC, базовые точки P и Q, требуемая длина ПСП $l_{\text{ПСП}}$ ($l_{\text{ПСП}}$ задает количество итераций). С помощью однократного преобразования базовой точки кривой EC (скалярного умножения) получаем на каждой итерации новую точку $P' = t_i * \varphi_i(P)$. Последовательность таких точек кривой будет обладать периодом, равным порядку циклической группы точек n. Кроме операции над базовой точкой в своей группе будем каждую итерацию трансформировать точку базовой кривой в изоморфную, $P_i = \varphi_i(P)$ (2). Результат после второго скалярного произведения $b_i = extr(\phi(X(s_i * Q)))$ будет элементом ПСП (рис. 3). Результат произведения $P' = t_i * P_i$ пробегает все точки таблицы.

С целью повышения сложности восстановления внутренних состояний DRBG изоморфизм можно выбирать специальной функцией, задающей параметры изоморфизма $\varphi_i = \{u_i, r_i, s_i, t_i\}$ определенным образом (по случайному закону или в определенном порядке). Далее рассмотрим один из вариантов функции, генерирующей значения u_i изоморфизма $\varphi_i = \{u_i, r_i, s_i, t_i\}$.

Для получения текущей базовой точки P_i, зафиксируем генератор ω группы Z_p, где p – характеристика поля Галуа. Затем, учитывая, что u пробегает все значения вычетов в поле p, текущее значение u_i получим:

$$u_i = \omega^{2i} \bmod p = u_{i-1} * \omega^2 \bmod p. \quad (6)$$

Число изоморфных точек базовой точки равно $N_{EC} = \frac{1}{2}(p-1)$. Параметр u пробегает все значения $\{1,..,N_{EC}\}$.

Для получения текущего значения скаляра t, будем использовать генератор ω' группы Z_n, где n – порядок циклической группы точек кривой (простое число), которой принадлежат точки P и Q.

Текущее значение скаляра t_i получим следующим образом:

$$t_i = t_{i-1} * t \bmod n, \quad (7)$$

где t – генератор мультипликативной группы Z_n.

Для обеспечения криптографической стойкости генератора (рис. 3) значение ω' будем использовать в преобразованном виде. Для этого выбирается секретное число $seed$, так что $(seed, n) = 1$. Число t определяется выражением (8).

$$t = \omega'^{seed} \bmod n, \quad (8)$$

где ω' – генератор Z_n.

Учитывая выражение (8) выражение для t_i примет вид:

$$t_i = t_{i-1} * t \bmod n = t_{i-1} * \omega'^{seed} \bmod n \quad (9)$$

Очевидно, что t_i пробегает все значения группы Z_n.

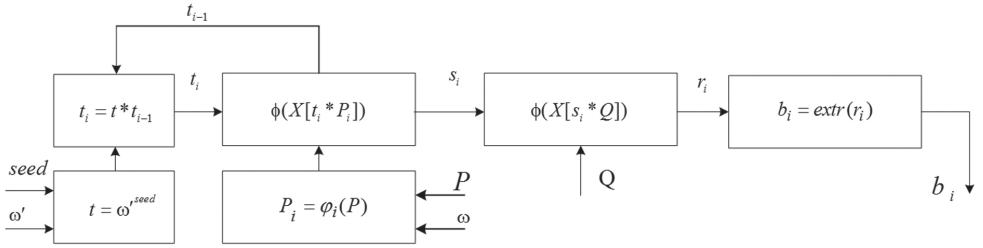

Рис. 3. Модель модифицированного генератора Dual_EC_DRBG

Учитывая граничные значения числа изоморфизмов ЭК в канонической форме, $N_{EC} = \frac{1}{2}(p-1)$, число внутренних состояний модифицированного генератора Dual_EC_DRBG определяется значением (10).

$$N = \frac{1}{2}(p-1) * n, \qquad (10)$$

где n – порядок циклической группы точек кривой; p – характеристика поля Галуа.

ВЫВОДЫ

Таким образом, разработан новый метод генерации ПСП на основе применения изоморфных трансформаций точек ЭК. Получено аналитическое выражение (10) для оценки числа внутренних состояний генератора Dual_EC_DRBG с использованием предложенного метода. Полученный метод позволяет в $\frac{1}{2}(p-1)$ раз увеличить число внутренних состояний генератора Dual_EC_DRBG, что увеличивает сложность вскрытия закона формирования ПСП злоумышленником. Применение разработанного метода также позволяет избежать существующих недостатков Dual_EC_DRBG.

Для обеспечения более высокой криптографической стойкости полученного метода генерации ПСП значение u_i можно получать аналогичным образом, на основе секретного числа *seed*.

При фиксированном значении числа внутренних состояний генератора Dual_EC_DRBG разработанный метод позволит сократить битовую длину характеристики p поля при фиксированной стойкости генератора. Следует также отметить применимость полученного метода ко всем генераторам ПСП на ЭК.

Литература

[1] Kaliski Jr. B. S. A pseudo-random bit generator based on elliptic logarithms / B. S. Kaliski Jr. // Advances in Cryptology: Proceedings of Crypto '86 (Lecture Notes in Computer Science, vol. 263), Springer-Verlag, New York, 1987, pp. 84-103.

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

[3] *Burton S.* One-Way Permutations on Elliptic Curves / Burton S. Kaliski, Jr. // Journal of Cryptology (1991) International Association for Cryptologic Research. 1991. - P.187-199.

[4] *Гриненко Т.А.* Методы формирования псевдослучайных последовательностей в группах точек эллиптических кривых / Т.А. Гриненко, С.И. Збитнев, Д.В. Мялковский // Радиотехника: Всеукр. межвед. науч.-техн. сб. 2002. Вып.119.С.119-123.

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

[6] *Гріненко Т.О.* Дослідження властивостей генераторів псевдовипадкових бітів на еліптичній кривій на відповідність міжнародному стандарту ISO/IEC 18031 / Гріненко Т.О., Погребняк К.А. // Журнал "Прикладная радиоэлектроника" 2009 №3. Харьков - 2009, сс. 372 – 377.

[7] *Горбенко І.Д.* Метод побудування випадкових бітів на основі спарювання точок еліптичних кривих / Горбенко І.Д., Шапочка Н.В., Погребняк К.А. // Журнал "Прикладная радиоэлектроника" 2010 №3. Харьков - 2010, сс. 386 - 394.

[8] *Husemцller D.* Elliptic Curves, Second Edition // Springer – 2002 / Dale Husemцller; with appendices by Stefan Theisen, Otto Forster, and Ruth Lawrence. - p. cm. — (Graduate texts in mathematics; 111) Includes bibliographical references and index. ISBN 0-387-95490-2 (alk. paper).

[9] NIST Special Publication 800-90 Recommendation for Random Number Generation Using Deterministic Random Bit Generators (Revised) / Elaine Barker, John Kelsey // Computer Security Division Information Technology Laboratory National Institute of Standards and Technology. - March 2007.

Поступила в редколлегию 22.03.2012

Бессалов Анатолий Владимирович, фото и сведения об авторе см. на с. 226.

Чевардин Владислав Евгеньевич, кандидат технических наук, докторант ВИТИ НТУУ «КПИ». Область научных интересов: криптографическая защита информации.

УДК 512.624.95 + 517.772

Метод генерації псевдовипадкових послідовностей на основі ізоморфних трансформацій еліптичної кривої / А.В. Бессалов, В.Є. Чевардін // Прикладна радіоелектроніка: наук.-техн. журнал. – 2012. – Том 11. № 2. – С. 234–237.

Запропоновано метод генерації випадкових бітових послідовностей оснований на ізоморфних трансформаціях точок еліптичної кривої. 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 випадкової послідовності.

Ключові слова: генератор псевдовипадкових послідовностей, еліптична крива, ізоморфні трансформації, трансформації еліптичної кривої.

Табл. 01. Іл. 03. Бібліогр.: 9 найм.

UDC 512.624.95 + 517.772

A method of generating pseudorandom sequences based on elliptic curve isomorphic transformations / A.V. Bessalov, V.E. Chevardin // Applied Radio Electronics: Sci. Journ. – 2012. Vol. 11. № 2. – P. 234–237.

A method of generating random bit sequences based on isomorphic transformations of elliptic curve points is proposed. The method is different from the existing ones by an increased number of internal states. It has allowed to increase the complexity of restoring the law of forming random sequences. One of the results is also obtaining the lower boundary of a random sequence period.

Keywords: pseudorandom sequence generator, elliptic curves, isomorphic transformations, elliptic curve transformations.

Tab. 01. Fig. 03. Ref.: 9 items.