УДК 512.624.95 + 517.772

А.В. БЕССАЛОВ, д-р техн. наук, В.Е.ЧЕВАРДИН, канд. техн. наук

МЕХАНИЗМ ГЕНЕРАЦИИ ПСЕВДОСЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ В СОВРЕМЕННЫХ AD HOC СЕТЯХ

Введение

Одними из показателей, обеспечивающих успех современных военных операций, являются живучесть, надежность и безопасность систем связи и информатизации современных вооруженных сил. По результатам последних исследований, таким требованиям отвечают беспроводные самоорганизующиеся сети [7]. Беспроводные самоорганизующиеся сети (другие названия: беспроводные ad hoc сети, беспроводные динамические сети) – децентрализованные беспроводные сети, не имеющие постоянной структуры [7].

Возросшие требования к безопасности информации в современных информационно-телекоммуникационных системах и невозможность дальнейшего развития военных систем связи без внедрения технологий построения беспроводных самоорганизующихся сетей вызвали противоречие. Для его разрешения применяется ряд подходов [7, 8], основанных на использовании механизмов криптографической защиты информации, в частности механизмов генерации псевдослучайных последовательностей (ПСП). Недостатком существующих подходов является отсутствие таковых к применению криптографических механизмов для генерации теоретически стойких ПСП в ad hoc сетях.

Благодаря большому доверию к криптопреобразованиям с теоретически доказуемой стойкостью основное внимание современных исследований устремлено на разработку криптографических методов на основе преобразований в группе точек эллиптической кривой (ЭК). Ярким примером являются алгоритмы генерации ПСП на ЭК. Однако существующие алгоритмы построения генераторов ПСП на ЭК [1 – 4] отличаются высокой вычислительной сложностью, что существенно ограничивает их применение.

Цель данной работы – разработка нового метода генерации ПСП на основе арифметики ЭК, что позволит увеличить количество 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.

Основные результаты работы

Пусть гладкая ЭК над простым полем Галуа характеристики $p \neq 2,3$ [5], $E[F_p]$ задана уравнением в канонической форме:

$$EC: y^2 = x^3 + a_4 x + a_6 \pmod p, \text{ где } a_4, a_6 \in F_p. \quad (1)$$

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].

Для ЭК в форме (1) существует изоморфная трансформация $\varphi: \{u, r, s, t\}$ [6]:

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

[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.

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 эквивалентны, но отличаются друг от друга. Представим изоморфные трансформации группы точек базовой кривой в виде матрицы:

Точки EC изоморфной трансформации	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, 6] для генерации ПСП используются точки из одной группы, соответствующей φ_1 из таблицы, кроме метода [1, 4], 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.

Существующие методы генерации ПСП на основе механизма DRBG

В источниках [1 – 4, 6] представлен ряд подходов к построению генераторов ПСП на основе сложения точек кривой, скалярного произведения, использования однонаправленных функций на двух ЭК [1, 4]. Однако принятым в качестве стандарта является генератор Dual_EC_DRBG [6]. В нем задача восстановления закона формирования ПСП сводится к решению задачи дискретного логарифмирования в группе точек ЭК. Структура генератора RBG представлена следующей моделью (рис.1).

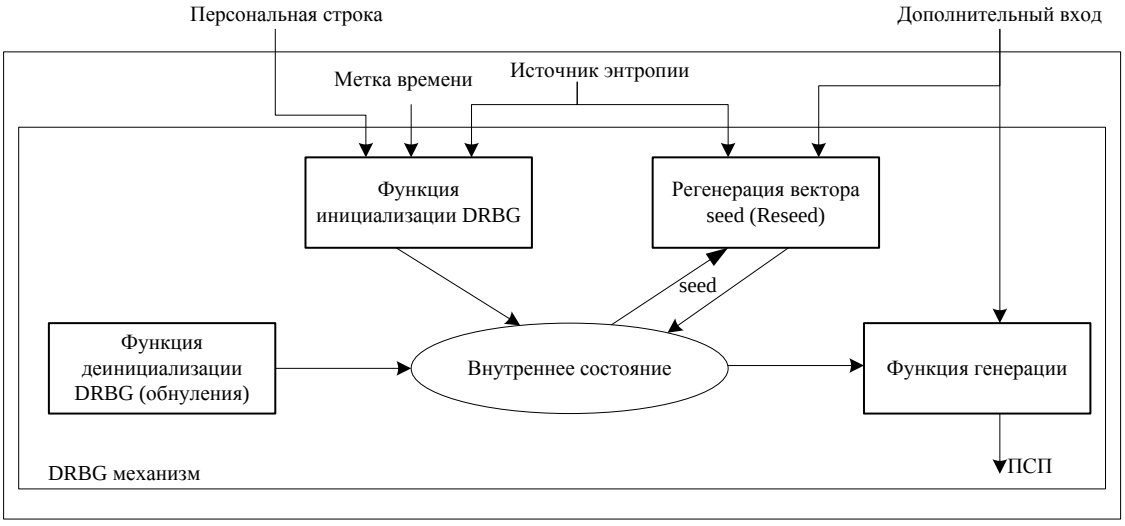

Рис. 1. Функциональная модель RBG – генератора случайных бит

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.2), 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 [6].

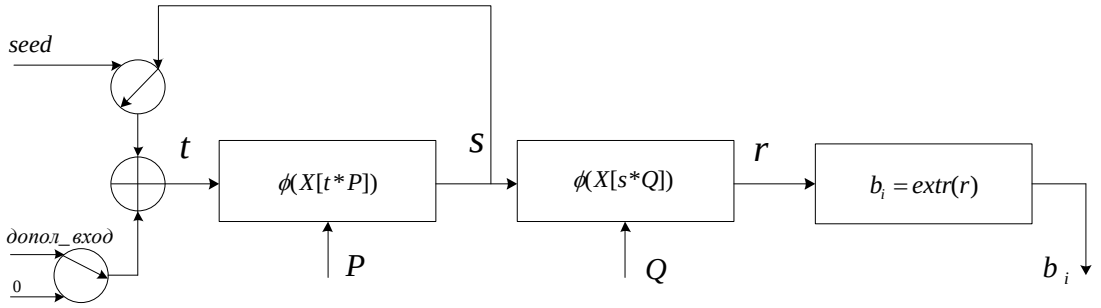

Рис. 2. Модель генератора Dual_EC_DRBG

Внутреннее состояние генератора определяется параметрами: (*s, seedlen, p, a, b, n, P, Q, security_strength, prediction_resistance_flag, reseed_counter*) [6], где *P, Q* – базовые точки кривой порядка *n*, *s* – секретный скаляр.

Функция генерации представлена выражением

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

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

Число выходов генератора Dual_EC_DRBG равно числу координат точек циклической группы точки *Q*, т.е. ограничено сверху порядком базовой точки, $n = \#Q$.

Нижняя граница числа выходов Dual_EC_DRBG определяется количеством внутренних состояний. Для обеспечения требуемой стойкости эта граница должна быть не ниже *n*. Учитывая, что внутренние состояния генератора определяет значение $X[t*P]$, число различных состояний не более $n/2$. Таким образом, возникает ситуация, когда период ПСП будет равен числу различных $X[t*P]$, следовательно и числу различных $\phi(X[t*P])$.

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

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 [6].

Представим функцию генерации текущей точки P':

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

Используя выражение (4) представим функцию генерации:

$$r_i = \phi^t(X[\phi(X[P_i]) * Q]) = \phi^t(X[(\phi(X[t_i * \varphi_i(P)]) * Q]), \tag{5}$$

где ϕ^t – функция сжатия точки кривой (либо извлечения блока бит), t есть метка времени (в данной работе влияние t не учитывается).

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 группу, $P_i = \varphi_i(P)$ (2), результат $b_i = extr(\phi^t(X(s_i * Q)))$ является элементом ПСП (рис.3). При получении значения $P' = t_i * P_i$ функция пробегает все значения из таблицы.

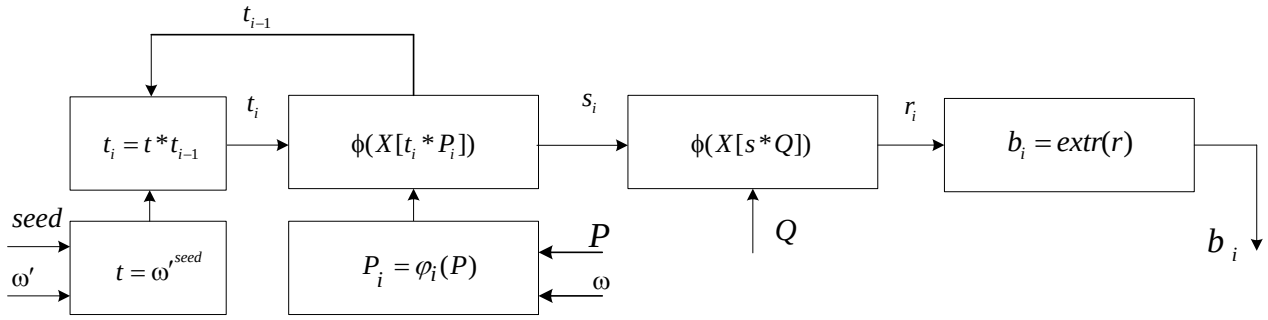

Рис. 3. Модель модифицированного генератора Dual_EC_DRBG

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. Другими словами, можно пробегать все значения φ_i таблицы 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 из выражения

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

Число изоморфных точек базовой точки $N_{EC} = \frac{1}{2}(p-1)$. 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 t – генератор порядка n.

Учитывая выражение (8) выражение для t_i примет вид:

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

Очевидно, что t_i пробегает все значения группы Z_n.

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

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

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 (9) 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 ECTORS 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.

Список литературы: 1. *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. 2. *R. Impagliazzo.* 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. *B. S. Kaliski Jr.* 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. 4. *Gjøsteen K.* Comments on Dual-EC-DRBG/NIST SP 800-90, Draft December 2005 / Kristian Gjøsteen // March 16, 2006. 5. *Husemöller D.* Elliptic Curves, Second Edition // Springer – 2002 / Dale Husemöller; 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). 6. 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. 7. *Yang Y.* A Secure Hop-by-Hop Data Aggregation Protocol for Sensor Networks / Y. Yang, X. Wang, S. Zhu, and G. Cao, // In Proceedings of the 7th ACM international symposium on Mobile ad hoc networking and computing (MobiHoc'06), 2006, pp. 356 – 367. 8. *W. Y. Chang.* Wireless Sensor Networks and Applications. In Network-Centric Service-Oriented Enterprise, pages 157–209. 2008.

НТУУ «КПИ» *Поступила в редколлегию 25.01.2012*