© Chevardin V. Pseudorandom bit generator based on Edwards curve isomorphic transformations // Ukrainian Scientific Journal of Information Security, 2015, vol. 21, issue 3, p. 283-286.

ВДОСКОНАЛЕНИЙ ГЕНЕРАТОР ПСЕВДОВИПАДКОВИХ ПОСЛІДОВНОСТЕЙ НА ОСНОВІ ІЗОМОРФНИХ ТРАНСФОРМАЦІЙ КРИВОЇ ЕДВАРДСА

Владислав Чевардін

Військовий інститут телекомунікацій та інформатизації, Україна

ЧЕВАРДІН Владислав Євгенійович, к.т.н.

Рік та місце народження: 1978 рік, м. Краматорськ, Україна.
Освіта: Харківський військовий університет, 2001 рік.
Посада: провідний науковий співробітник Наукового центру зв'язку та інформатизації Військового інституту телекомунікацій та інформатизації з 2013 року.
Наукові інтереси: криптографія, захист комп'ютерних мереж.
Публікації: більше 50 наукових публікацій, серед яких навчальні посібники, наукові статті та патенти на винаходи.
E-mail: chevardin_vlad@mail.ru

Анотація. *У даній статті запропоновано вдосконалений стандартизований генератор ПВП на еліптичних кривих за рахунок використання додаткової функції отримання ізоморфної трансформації базової еліптичної кривої. Ізоморфна трансформація використовується для кожної точки кривої, що отримується після скалярного множення базової точки циклічної підгрупи. За рахунок цього з'являється можливість використовувати всю множину ізоморфних трансформацій еліптичної кривої та збільшити число внутрішніх станів генератора та, як наслідок, збільшити стійкість ПВП до відтворення. Еліптична крива використовується у формі Едвардса, що надає можливість скоротити обчислювальні витрати під час генерації ПВП. Отримані результати оцінки статистичної безпеки вдосконаленого генератору ПВП підтвердили його надійність. Вдосконалений генератор ПВП дозволяє зменшити обчислювальну складність алгоритму та підвищити його пропускну спроможність у порівнянні зі стандартизованим алгоритмом.*

Ключеві слова: *генератор псевдовипадкових послідовностей, еліптична крива, крива Едвардса, ізоморфні трансформації, ізоморфні криві.*

Вступ

Забезпечення стійкого, безпечного та надійного зв'язку в інформаційно-телекомунікаційних системах сучасного суспільства вже неможливо без використання власних генераторів криптографічних ключів, які повинні відповідати підвищеним вимогам до криптографічної стійкості та обчислювальної складності. Для забезпечення безпеки генераторів псевдовипадкових властивостей (ПВП) сьогодні вважають достатнім забезпечення їх криптографічної стійкості еквівалентної стійкості шифру AES (генератори CTR DRBG), стійкості до колізій геш-функцій SHA256/512 (генератори Hash_DRBG) або стійкості еліптичних кривих (генератор Dual_EC_DRBG 256/384/512) [1]. Враховуючи, що побудова криптографічних алгоритмів на основі теоретичних задач є найбільш надійним підходом, який витримує багато спроб криптоаналізу протягом багатьох десятиріч, основна увага більшості сучасних робіт у цьому напрямку відведена генераторам на еліптичних кривих. Відомо, що у генераторів на еліптичних кривих крім переваг є вагомий недолік – це висока обчислювальна складність операцій на еліптичних кривих у порівнянні з алгоритмами на основі блокових шифрів, що обмежує їх широке використання. З метою зменшення обчислювальних витрат генераторів ПВП на еліптичних кривих, в роботі пропонується новий підхід до побудови генераторів ПВП, який застосовує спеціальну форму кривих – криві Едвардса. Так, в проективних координатах групова операція на кривих Едвардса здійснюється виконанням 10M+1S+2D операцій, де M – операція множення в скінченному полі, S – підведення до квадрату, D – множення на коефіцієнт кривої [12].

Аналіз існуючих робіт та постановка задачі дослідження

У роботах [2 – 10] були розроблені різні схеми побудови генераторів на еліптичних кривих, такі як конгруентні генератори, генератори на основі спарювання точок еліптичних кривих, з використанням операцій додавання або множення точок еліптичної кривої. Для більшості з розроблених структур було доведено можливість суттєвого зниження їх криптографічної стійкості. Найбільш привабливою схемою виявилась структура, яка увійшла в стандарт [1], що використовує подвійне

скалярне множення точок еліптичної кривої над простим скінченним полем з фіксованими параметрами (P-256, P-386, P-512). У ході проведених досліджень [13 – 15] були розроблені генератори ПВП на основі ізоморфних трансформацій точок еліптичної кривої над простими полями та їх розширеннями, одна з таких схем наведена на рис. 1., де пунктирними лініями наведені блоки та лінії, які пропонується додати з метою вдосконалення генератора.

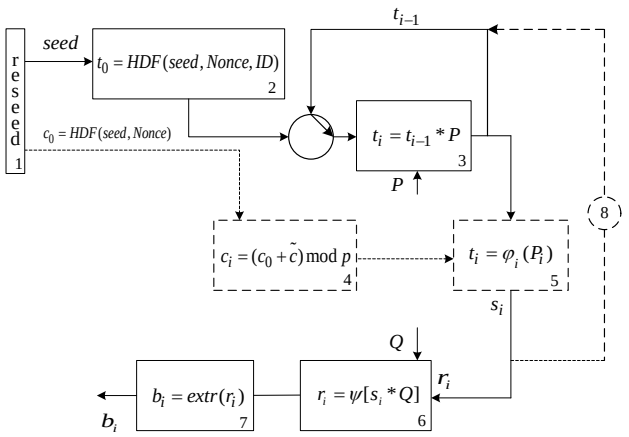

Рис. 1. Функціональна модель вдосконаленого генератора Dual_EC_DRBG

В даній роботі пропонується збільшити число внутрішніх станів генератора та знизити обчислювальну складність генераторів ПВП за рахунок використання часткового випадку еліптичної кривої – форми Едвардса.

Викладення результатів роботи

Криві Едвардса є частковим випадком кривих Веєрштраса та можуть бути приведені до стандартизованої форми. Для будь-якої кривої Едвардса завжди існує нуль абелевої групи – точка O, є точка 2-го порядку та дві точки 4-го порядку. Якщо крива Веєрштраса задовольняє цим умовам, вона може перетворюватись у криву Едвардса.

Загально відомі криві Едвардса [11 – 12] задаються рівнянням (1) з груповою операцією додавання точок кривої

$$E_{E,a,d} : ax^2 + y^2 = c^2(1 + \bar{d}x^2y^2)(\bmod p), \quad (1)$$

де $\bar{d} = c^4 d$, $\bar{d}(1 - \bar{d}c^4) \neq 0, \bar{d} \neq A^2$, $p \equiv 4 \bmod 8$, $p \equiv 3 \bmod 4$.

Множина значень параметра c у виразі (1) створює множину ізоморфних кривих Едвардса. Можна прийняти $a = 1$, $c = 1$, $\bar{d} = d$, тоді здійснюючи заміну: $xc = \bar{x}$, $yc = \bar{y}$, різні криві Едвардса визначаються лише параметром d у рівнянні $E_{E,a,d} : \bar{x}^2 + \bar{y}^2 = 1 + d\bar{x}^2\bar{y}^2 (\bmod p)$, $d(1-d) \neq 0$, $d \neq A^2$. Крім форми (1) також використовують її ізоморфну трансформацію у формі (2), яка використовується в загальновідомій бібліотеці математичних функцій MIRACLE

$$E_{E,a,b} : x^2 + ay^2 = x^2y^2 + b (\bmod p). \quad (2)$$

Для генерації випадкової кривої Едвардса (2) сьогодні вибирають випадкове значення: $b \neq 0$, $a \neq 0$. Після чого, коефіцієнти кривої Едвардса трансформуються в коефіцієнти ізоморфної кривої Веєрштраса. Потім з використанням алгоритму Скуфа визначають порядок кривої. Якщо $\left|E_{E,a,b}\right| \neq 4 * p$, де p – просте число, то генеруються нові параметри кривої. На рис. 1 наведена схема генератора для двох можливих способів. Перший – без впливу результату ізоморфних трансформації на наступний крок генератора. Другий – з урахуванням на кожному кроці результату попередньої трансформації (лінія 8). Використовуючи криву (1) наведемо удосконалений *Dual_EC_ DRBG* для способу 1.

Генератор Dual_EC_ DRBG на основі ізоморфних трансформацій кривих Едвардса

Для генерації кривої з числа елементів скінченного поля обирається число $d \in F^*_p$, таке що $d(1-d) \neq 0$, $d \notin Q_p$. Генеруються дві базові точки P та Q простого порядку $n = (p+1)/4$. Ізоморфна трансформація базової кривої Едврадса реалізується шляхом лінійного зсуву координат точок базової кривої: $x = cX$, $y = cY$, що дає ізоморфну криву для кривої (1). Використовуючи параметр c для кривої (1), як параметр ізоморфної трансформації, можна здійснити трансформацію будь-якої точки базової кривої в точку ізоморфної кривої. З використанням загальносистемних параметрів генератора ПВП генерується за таким алгоритмом:

Початок

Введення параметрів: рівень безпеки генератора – *security_strenth*, довжина ПВП – *fin*, характеристика поля *p*, коефіцієнти кривої (1) з урахуванням вимог до криптографічно стійких кривих, значення вхідної ентропії *entropy* довжиною $l_{entropy}$, довжина вихідного блока l_b,. Задаються границі лічильника $0 < i < i_{fin}$, $\tilde{c} = const$. Генерація змінної $\tilde{c}$ може відбуватись також на кожному кроці, але тоді треба впевнитись, що випадкова функція не зменшує період послідовності різних значень $\tilde{c}$.

Крок 1. Генерується секретний *seed*.

Крок 2. Генеруються початкові значення t_0, c_0.

Крок 3. Початок $for(i = 0, i < i_{fin}, i++)$.

Крок 3.1. Обчислюється $t_i = \psi(t_{i-1} * P)$.

Крок 3.2. Обчислюється $c_i = (c_{i-1} + \tilde{c}) \bmod p$.

Крок 3.3. Обчислюється точка ізоморфної кривої: $\varphi(P_i)$.

Крок 3.4. Обчислюється $s_i = \psi(\varphi(P_i))$.

Крок 3.5. Обчислюється $Q_i = s_i * Q$.

Крок 3.6. Обчислюється $r_i = \psi(Q_i)$.

Крок 3.7. Обчислюється $b_i = extr(r_i)$.

Крок 3.8. Вивід b_i.

Крок 3.9. Кінець циклу $for()$.

Крок 4. Видалення з оперативної пам'яті змінних.

Кінець

Математичний опис вдосконаленого Dual_EC_DRBG можна представити виразом (3)

$$b_i = extr\{\varphi(\psi(P_i))*Q\} = extr\{\varphi(\psi(t_{i-1}*P))*Q]]\}, \quad (3)$$

де $P, Q \in E_{E,a,d}$,

$t_i = \psi(P_i) = X[P_i] \bmod n$, $i = \{1, n\}$,

$t_0 = HDF(seed, nonce, ID)$;

$\varphi(P_i) = c_i X[P_i] \bmod p$.

У табл.1 містяться рекомендовані значення параметрів кривих Едвардса.

Таблиця 1

Рекомендовані значення параметрів кривих Едвардса

Крива Едвардса	Просте число p	Коефіцієнти кривої		Порядок базової точки n	h
		a	d		
$E_{E,23,-6}$	$2^{160} - 47$	23	-6	$(2^{160} - 46)/4$	4
$E_{E,102,47}$	$2^{192} - 2^{64} - 1$	102	47	$(2^{192} - 2^{64})/4$	4
$E_{E,121666,121665}$	$2^{255} - 19$	121666	121665	$(2^{255} - 18)/4$	4

Кількість внутрішніх станів генератора (3) визначається числом непарних точок кривої Едвардса, тобто потенційно складе $(p+1)/8$. Але з урахуванням можливих зациклень Dual_EC_DRBG в загальному випадку період ПВП не перебільшить границю $(p+1)/8$, а може бути на багато менше, що буде досліджено в іншому разі.

Для проведення експериментальних досліджень була обрана крива Едвардса Edw-160 (Twisted Inverted Edwards curve): $x^2 + ay^2 = x^2y^2 + b(\bmod p)$, де a = 1, b = 262, p = 1461501637330902918203684832716283019655932542919 з кофактором 4. Порядок циклічної групи n = 3fffffffffffffffffffbd446095ae59e082fae7. Обрана крива Edw-160 є ізоморфною кривій Веєрштраса: $E: y^2 = x^3 + ax + b(\bmod p)$ з коефіцієнтами: a = 59898656799953713773451537841968328905442255637 6, b = 3244889084624952062455583825456419162611363088 2.

В якості базових точок кривої були випадкових. Точки P и Q порядку n:

$X[P]$ = c56ce8c38cb8b871e85ac328e025800087a336a4,

$Y[P]$ = 128e02611212dfde63a2f4abc7770fbc45a8c089,

$X[Q]$ = 60b53045ebbddee1f9f5e77b90462035805b446d,

$Y[Q]$ = 2b4fdcd5496b1cca1c176a3c09f600ec705bffdf.

Dual_EC_DRBG(Edw-160) був реалізований на мові C/C++ з бібліотекою багатознакової цілочисельної та раціональної арифметики MIRACL. Результати оцінки псевдовипадкових властивостей генератора Dual_EC_DRBG наведені на рис. 2.

Результати оцінки статистичної безпеки генератора Dual_EC_DRBG (Edw-160) підтверджують статистичну безпеку генераторів на кривих Едвардса.

Часові та швидкісні показники Dual EC DRBG (Edw-160), отримані з використанням робочої станції „PC-E7500" (Intel™ Core™ 2 Duo Wolfdale™ Yorkfield™ CPU-E7500 (частота (*CPU_clock*): 2933000000 Hz; набір інструкцій: x86, x86-64, MMX, SSE, SSE2, SSE3, SSSE3; оперативна пам'ять: DDR2-800 2047 Мб)) з 32-бітним компілятором.

Для оцінки обчислювальної складності алгоритму генерації ПВП використовувалась пропускна спроможність алгоритму (*Rate*) та обчислювальна складність алгоритму $Perform = (util * CPU\_clock)/Rate$, де *Util* – утилізація ядра процесора, *Rate* – пропускна спроможність алгоритму, K_{trun} – коефіцієнт передачі [0,05; 0,9] в залежності від довжини значення b_i.

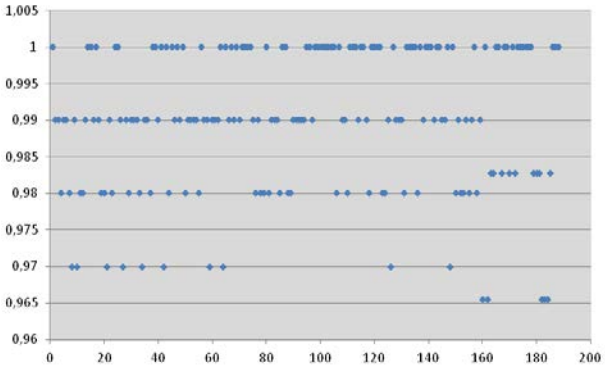

Рис. 2. Результати оцінки статистичної безпеки Dual_EC_DRBG (Edw-160)

Обчислювальна складність алгоритму, яка вимірюється в cpb (cycles per byte), дає оцінку числа тактів процесора, необхідних для обробки 1 байта вхідної інформації. Так, для Dual EC DRBG(Edw-160) при $Util = 52\%$ $Rate = 32315$ байт/сек, $Perform = 47196,5$ cpb, а для Dual EC DRBG(E-160) – $Rate = 24524$ байт/сек, $Perform = 62190,5$ cpb.

Висновки

Вдосконалення Dual_EC_DRBG на основі кривих Едвардса дозволило знизити обчислювальні витрати під час генерації та розповсюдження криптографічних ключів. Виграш у пропускній спроможності Dual_EC_DRBG, побудованого на основі кривих Едвардса склав 1,317 у порівнянні з класичним Dual_EC_DRBG, побудованим на основі тієї ж самої кривої в формі Веєрштраса. Для інших кривих, зазначених в стандарті [1], виграш склав 1,4-1,5 разів. Об'єм обчислень у генераторі на еліптичній кривій над полем з характеристикою p, де $\log p \approx 160$, зменшився на 25 %. Крім зазначеного виграшу під час генерації ПВП, криві Едвардса дозволять також зменшити час передобчислень для генерації параметрів кривої та її точок. Використання ізоморфних трансформацій кривих Едвардса на кожному кроці дозволить також позбавитись випадків використання ПВП з малим періодом зациклень та, як наслідок, збільшити стійкість ПВП до відтворення.

Література

[1] 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.

[2] 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.

[3] Krawczyk H. How to predict congruential generators / H. Krawczyk // TECHNION – Israel Institute of Technology Computer Science Department. December 1988. – P. 1-15.

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

[5] 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.

[6] Hallgren S. Linear congruential generators over elliptic curve. // Cornegie Mellon Univ., 1994, CS-94-M3. – P. 1-10.

[7] Gong G. Elliptic curve pseudorandom sequence generators / G. Gong, T. A. Berson, D. R. Stinson // Selected Areas in Cryptography (Kingston, ON, 1999), Springer, 2000, p. 34-48.

[8] Lange T. Certain exponential sums and random walks on elliptic curves / T. Lange, I. E. Shparlinski // Canadian Jornal of Mathematics 57. – 2005. – P. 338-350.

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

[10] Горбенко І.Д. Метод побудування випадкових бітів на основі спарювання точок еліптичних кривих / Горбенко І.Д., Шапочка Н.В., Погребняк К.А. // Прикладная радиоэлектроника. – 2010. – № 3. – С. 386-394.

[11] Edwards H. A normal form for elliptic curves / H.M. Edwards // Bulletin of the American Mathematical Society 44 (July 2007). – P. 393 – 422. URL: http://www.ams.org/bull/2007-44-03/S0273-0979-07-01153-6/home.html

[12] Lange T. Binary Edwards curves / Lange T., R.R. Farashahi // Cryptographic Hardware and Embedded Systems – CHES 2008, 10th International Workshop, Washington, D.C., USA / Proceedings. Elisabeth Oswald and Pankaj Rohatgi ed. LNCS 5154, Springer. – 2008. – P.244-265. [Електр. ресурс]. – Режим доступу до ресурсу: cr.yp.to/newelliptic/edwards2-20080611.pdf

[13] Chevardin V. A pseudorandom bit generator based on elliptic curve transformations / Chevardin V. E. // Радіоелектронні і комп'ютерні системи. – № 5 (57). – Х.: «ХАІ», 2012. – С. 48-50.

[14] Бессалов А. Метод генерации псевдо-случайных последовательностей на основе изоморфных трансформаций эллиптической кривой / А.В. Бессалов, В.Е. Чевардин // Прикладная радиоэлектроника. – Т. 1, № 2. – 2012. – С. 234-237.

[15] Чевардін В. Изоморфные трансформации эллиптической кривой над конечным полем / В.Є. Чевардін // Кибернетика и системный анализ. – Т. 49, № 3. – 2013. – С. 168-171.

УДК 512.624.95 (045)

Чевардин В.Е. Генератор псевдослучайных последовательностей на основе изоморфных трансформаций кривой Эдвардса

Аннотация. *В данной статье предлагается усовершенствованный стандартизированный генератор ПСП на эллиптических кривых за счет использования дополнительной функции получения изоморфной трансформации базовой эллиптической кривой. Изоморфная трансформация используется для каждой точки кривой, получаемой после скалярного умножения базовой точки циклической подгруппы. За счет этого появляется возможность использовать все множество изоморфных трансформаций эллиптической кривой и увеличить число внутренних состояний генератора и, как следствие, увеличить стойкость ПСП к воспроизведению. Эллиптическая кривая используется в форме Эдвардса, что позволяет сократить вычислительные затраты при генерации ПСП. Полученные результаты оценки статистической безопасности усовершенствованного генератора ПСП подтвердили его надежность. Усовершенствованный генератор ПСП позволяет уменьшить вычислительную сложность алгоритма и повысить его пропускную способность по сравнению со стандартизированным алгоритмом.*

Ключевые слова: *генератор псевдослучайных последовательностей, эллиптическая кривая, кривая Эдвардса, изоморфные трансформации, изоморфные кривые.*

Chevardin V. Pseudorandom bit generator based on Edwards curve isomorphic transformations

Abstract. *This article provides an improved standardized pseudorandom bit generator on elliptic curves through the use of additional functions to get an isomorphic transformation of the base elliptic curve. Isomorphic transformation is used for each point witch obtained after the scalar multiplication of the base point in the cyclic subgroup. In this way it is possible to use the whole set of elliptic curve isomorphic transformations and increase the number of generator internal states and, as a consequence, increase the resistance to recovery of pseudorandom sequence. The elliptic curve is used in the Edwards form, which reduces the computational cost in the generation of the pseudorandom sequence. The results of the analyses of the statistical security are confirmed its security. An improved pseudorandom bit generator can reduce the computational complexity of the algorithm and increase its capacity compared with a standardized algorithm.*

Key words: *pseudorandom bit generator, elliptic curve, Edwards curve, isomorphic transformations, isomorphic curves.*

Отримано 6 *жовтня 2015 року*, затверджено редколегією *30 жовтня 2015 року*