УДК 004.056.5

д.т.н. Чевардін В.Є. (ВІТІ)
к.т.н. Мазулевський О.Є. (ВІТІ)
Пономарьов О.А. (ВІТІ)

МЕТОД ГЕНЕРАЦІЇ КРИПТОГРАФІЧНИХ ПСЕВДОВИПАДКОВИХ ПОСЛІДОВНОСТЕЙ НА ЕЛІПТИЧНИХ КРИВИХ ПІДВИЩЕНОЇ СТІЙКОСТІ ДО ПЕРЕДБАЧЕННЯ

В роботі проведено аналіз недоліків генераторів псевдовипадкових послідовностей, які побудовані на основі криптографічних примітивів. В якості перспективного напрямку досліджень обраний стандартизований клас генераторів, які використовують в своїх структурах теоретико-складнісні задачі математики і зазначені в стандартах. У визначеному класі генераторів показано як недоліки в структурі стандартизованого генератору можуть привести до появи псевдовипадкових послідовностей з аномально малими періодами. В роботі наведено приклади ранніх зациклень генератору ПВП на еліптичних кривих в канонічній формі. Для оцінки еліптичних кривих великих порядків наведені математичні вирази. Запропоновано метод вдосконалення стандартизованого генератору ПВП на еліптичних кривих в канонічній формі за рахунок ізоморфних перетворень еліптичної кривої. Отримані оцінки числа кроків до зациклення генераторів ПВП та його стійкості до передбачення.

Чевардин В.Е., Мазулевський О.Є., Пономарев А.А. **Метод генерации псевдослучайных последовательностей на эллиптических кривых повышенной стойкости к предсказанию.** *В работе проведен анализ недостатков генераторов псевдослучайных последовательностей, которые построены на основе криптографических примитивов. В качестве перспективного направления исследований выбран стандартизированный класс генераторов, использующих в своих структурах теоретико-сложностные задачи математики. В определенном классе генераторов показано как недостатки в структуре стандартизированного генератора могут привести к появлению псевдослучайных последовательностей с аномально малыми периодами. В работе приведены примеры ранних зацикливаний генератора ПСП на эллиптических кривых в канонической форме. Для оценки эллиптических кривых больших порядков приведены математические выражения. Предложен метод усовершенствования стандартизированного генератора ПВП на эллиптических кривых в канонической форме за счет изоморфных преобразований эллиптической кривой. Полученные оценки числа шагов до зацикливания генераторов ПВП и его стойкости к предсказанию.*

Chevardin V.E. Mazulevskiy O.E., Ponomarev A.A. **Method generating pseudorandom sequences on elliptic curves with raise prediction resistance.** The analyze results of vulnerabilities of pseudorandom sequence generators, which are based on cryptographic primitives were showed in paper. A standardized families of generators witch using the complexity-theoretic mathematic problems in their structures were chosen for researches. In a certain class of generators, it is shown how deficiencies in the structure of a standardized generator can lead to the appearance of pseudo-random sequences with abnormally small periods. The paper presents examples of early loops of the deterministic random bit generator on elliptic curves in canonical form. Mathematical expressions to estimating of elliptic curves large order were given. The improving of standardized deterministic random bit generator on elliptic curves in canonical form method with isomorphic transformations of elliptic curve was proposed. The obtained estimates of step number before looping deterministic random bit generator and its prediction resistance.

Ключеві слова: *генератор псевдовипадкових послідовностей, криптографічний генератор, еліптична крива, ізоморфні перетворення еліптичної кривої, prediction resistance, elliptic curves, DRBG.*

Постановка проблеми та актуальність дослідження

Сучасні методи асиметричного шифрування та електронного цифрового підпису користуються особливою увагою, так як більшість сучасних інформаційно-телекомунікаційних сервісів вже не використовуються без криптографічних модулів, протоколів цифрового підпису, систем автентифікації та розмежування доступу. Чисельні атаки на програмну реалізацію, закладання прихованих лазівок в алгоритми криптографічного захисту й автентифікації та використання потенційно слабких криптографічних примітивів (методів) призводить до виникнення суттєвих загроз функціонуванню інформаційно-телекомунікаційних систем критичної інфраструктури держави. Це викликає потребу від систем кіберзахисту забезпечення безпеки на рівні математичних методів, алгоритмів та реалізації (програмної, чи програмно-апаратної) [1]. Найбільш небезпечними та складно детектованими загрозами є приховані лазівки в алгоритмах криптографічного захисту інформації. Наприклад, шифр RC4 не забезпечує криптографічної стійкості, але використовується в системах радіозв'язку [2,3], алгоритм шифрування А5 в стандарті стільникового зв'язку не є криптографічно стійкими [4]. Генератори псевдовипадкових послідовностей на основі лінійних регістрів також не

витримують критики та не можуть застосовуватись в криптографічних додатках [6]. В криптографічних системах на еліптичних кривих також є уразливості, в тому числі пов'язані з алгоритмічними лазівками [7-10]. З урахуванням перспективних можливостей квантового криптоаналізу деякі криптографічні системи, особливо це стосується асиметричних криптосистем, швидко втрачають свій рівень стійкості [11]. Це ставить під загрозу сучасні стандартизовані криптографічні алгоритми, з яких особливу увагу викликають генератори криптографічних псевдовипадкових послідовностей [12-15], для яких основними характеристиками згідно [12] є стійкість до відтворення (backtracking resistance), стійкість до передбачення (prediction resistance) та криптографічна стійкість (security strength). Окремим класом з таких генераторів є генератори на основі теоретико-складнісних задач математики, а саме на еліптичних кривих. Один з таких генераторів Dual_EC_DRBG потрапив до деяких стандартів [12,15]. Враховуючі, що стійкість до передбачення генератора залежить від числа внутрішніх станів генератора [12], а саме від числа кроків генератора до першого повторення ПВП, виявлення умов, в яких генератор почне створювати ПВП аномально малої довжини є актуальним науково-технічним завданням.

Аналіз відомих результатів розробки та вдосконалення методів генерації криптографічних псевдовипадкових послідовностей показав, що перші алгоритми генерації ПВП на основі перетворень в групі точок еліптичних кривих почали з'являтись з початком використання еліптичних кривих в криптографії [16]. З появою критики стосовно недосконалості алгоритмів генерації та подальшим їх розвитком з'являлись інші схеми та алгоритми [17], а пізніше і стандартизовані схеми [18]. Початок розвитку квантових комп'ютерів постала загроза для усіх асиметричних криптосистем [11], що викликало нову хвилю досліджень та розробку кандидатів на постквантові алгоритми а разом з цим і статті з критикою щодо їх стійкості [19]. Одним з кандидатів на постквантовий алгоритм стали і алгоритми на основі ізогенії еліптичної кривої [22,23], які є випадком ізоморфізмів еліптичної кривої, які в свою чергу можуть стати додатковим параметром для ускладнення алгоритму генерації ПВП. В зв'язку з цим, метою даної роботи є підвищення стійкості до передбачення генераторів ПВП на еліптичних кривих за рахунок використання ізоморфних трансформацій еліптичної кривої.

Викладення основного матеріалу

Для визначення структури та функцій генераторів ПВП на еліптичних кривих (ЕК) розглянемо деякі аспекти теорії еліптичних кривих.

Гладкою (неособливою) еліптичною кривою порядка n над полем F_p називається множина точок $(X,Y), X,Y \in F_p$, які задовольняють рівнянню $F(X,Y)=0$, де $F(X,Y)$ багаточлен ступені[1] m з коефіцієнтами з F_p. Така крива не повинна мати особливих точок, в яких $\frac{\partial F}{\partial X} \neq 0, \frac{\partial F}{\partial Y} \neq 0$. Множина точок еліптичної кривої разом з точкою на нескінченності з операцією додавання[2] є абелевою групою. Для побудови абелевої групи точок кривої використовують еліптичну криву з ненульовим дискримінантом $\Delta(E) \neq 0$, та j-інваріантом $j \neq \{0, 12^3\}$, для запобігання використанню суперсингулярних кривих [20,21].

Нормальною формою еліптичної кривої на над полем F_p, називається крива виду:

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6. \quad (1)$$

Коли коефіцієнти a_1, a_2, a_3 дорівнюють нулю, крива (1) може бути представлена в канонічній формі (або скороченій формі Веєрштрасса):

---

[1] Ступінь багаточлена є максимальна степінь одночленів, з яких він складається.

[2] $P_{i-1}(x_{i-1}, y_{i-1}) + Q_j\ (x_{Q_j}, y_{Q_j}) = P_i\left(\frac{y_{i-1}-y_{Q_j}}{x_{i-1}-x_{Q_j}} - x_{Q_j} - x_{i-1}, -y_{Q_j} + \frac{y_{i-1}-y_{Q_j}}{x_{i-1}-x_{Q_j}}(x_{Q_j}-x_i)\right)$.

$$y^2 = x^3 + a_4 x + a_6,\ a_4, a_6 \in F_p. \quad (2)$$

Лінійна ізоморфна трансформація координат цієї кривої в канонічній формі задається формулами:

$$y = u^3 \bar{y} + su^2 \bar{x} + t,\ x = u^2 \bar{x} + r,\ u \neq 0,\ r, s, t \in \{0, ..., p-1\}.$$

Лінійна ізоморфна трансформація не змінює значення інваріанту, тобто всі ізоморфні криві мають однаковий інваріант. Коли трансформація має параметри $u = \{1, ..., p-1\}, r = 0, s = 0, t = 0$ ($a_1 = 0, a_2 = 0, a_3 = 0$) крива залишається в канонічній формі.

В такому випадку лінійна ізоморфна трансформація для кривої (2) має вигляд:

$$y = u^3 \bar{y},\ x = u^2 \bar{x},\ u = \{1, ..., p-1\}. \quad (3)$$

З використанням введених визначень та положень теорії еліптичних кривих розглянемо структуру стандартизованого генератору ПВП на еліптичних кривих та введемо поняття послідовності псевдовипадкового генератора та її властивостей.

Нехай

$$\xi_0, \xi_1, ..., \xi_\upsilon \quad (4)$$

– вихідна послідовність деякого псевдовипадкового генератора.

Означення 1. Якщо існує таке $i \geq 0$, що для деякого $k \in N$ виконується $\xi_i = \xi_{i+k}$, то послідовність $\xi_0, \xi_1, ..., \xi_{l-1}$, де $l = \min\{i \geq 0 / \exists k \in N : \xi_{i+k} = \xi_i\}$, будемо називати передперіодом послідовності (4), якщо $l \geq 1$.

Якщо ж $l = 0$, то будемо вважати, що послідовність (4) є чисто періодичною, або послідовність не має передперіоду. Число *l* є довжиною передперіоду.

Означення 2. Нехай $\xi_0, \xi_1, ..., \xi_{l-1}$ – передперіод послідовності (4). Тоді величина $T = \min\{k \geq 1 : \xi_{l+k} = \xi_l\}$ називається довжиною періоду послідовності (4).

Означення 3. Нехай задана послідовність (4). Будемо вважати, що зациклення послідовності відбулося рівно на *K*-му кроці, $K \geq 1$, якщо $K = l + T$, тобто K – це максимальна кількість різних станів, взятих підряд від 0-го стану.

Нехай послідовність (4) для деякого $k \in N$, має передперіод $t_0, t_1, ..., t_{l-1}$ та довжину періоду $T = \min\{k \geq 1 : t_{l+k} = t_l\}$, де $l = \min\{i \geq 1 / \exists k \in N : t_{i+k} = t_i\}$.

Нехай стандартизований генератор ПВП є генератором ПВП, на виході якого з'являються X-координата точки кривої $X[t_i * P]$, яка є також наступним входом функції генерації внутрішніх станів (рис. 1). Математична функція генерації внутрішнього стану є скалярним множенням точки кривої $s * Q$, де *s* – скалярне множення точок кривої, *Q* – базова точка еліптичної кривої.

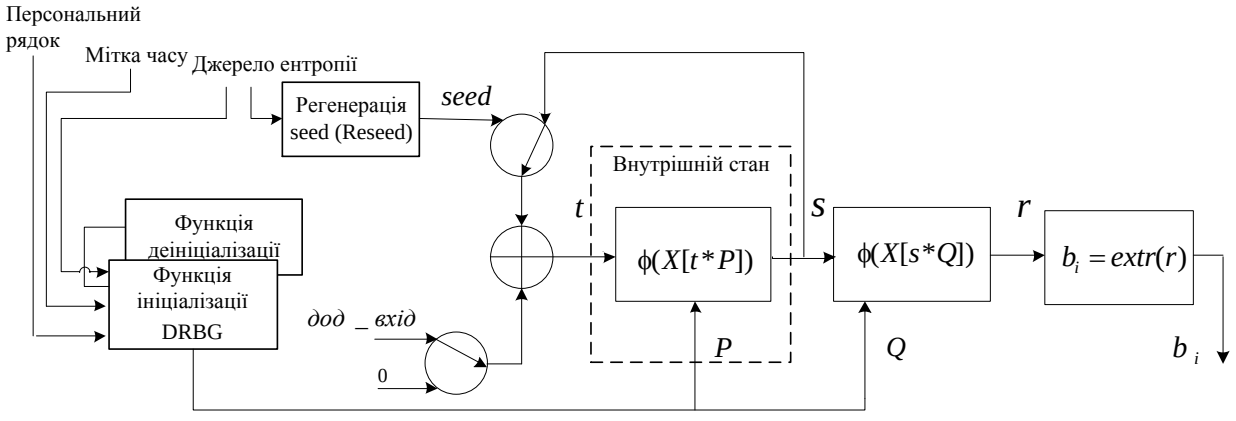

Рис. 1. Функціональна модель генератора Dual_EC_DRBG

Нехай значення *NT* – число кроків до зациклення генератору, яке дорівнює кількості різноманітних значень внутрішнього стану генератору. Враховуючі структуру генератору, значення *NT* визначає потужність простору вхідних значень *s* для другого множення $s*Q$ та визначає стійкість до зламу генератора ПВП.

Враховуючи, що внутрішній стан генератора є значенням $X[t_i * P]$, яке для кривої (1) не перебільшує $n/2$, а період ПВП в цьому випадку буде визначений значенням *NT* тобто числом значень t_i. Значення t_i отримуються з виразу $X[t_i * P]$, тобто їх кількість буде не більше $n/2$.

*Приклад***.** Нехай еліптична крива задана рівнянням $E_{12391}: y^2 = x^3 + 1322x + 3$. Порядок циклічної групи точок кривої дорівнює $n = 12239$, $\log n \approx 14$, $NT = 6119$, $\log n \approx 13$. Для такого генератора розглянемо три випадки: $\log k \approx 2, \log k \approx 3, \log k \approx 6$. Імовірність зациклення, відповідно до кожного з випадків, дорівнює: $P(A_{\log k=2}) = 9,99e^{-1}$, $P(A_{\log k=3}) = 9,94e^{-1}$, $P(A_{\log k=6}) = 6,07e^{-1}$. Значення кількості кроків K до зациклення, розраховані на основі теоретичних оцінок [25], наведені в таблиці 1.

Таблиця 1

	1	2	3	4	5	6	7	8
pr	0,0001	0,001	0,01	0,1	0,5	0,9	0,99	0,999
K	2	4	12	36	93	169	239	294

На рис. 2 наведені оцінки *K1, K2, K3, K4, K5, K6, K7, K8* та $K_{експ}$. Значення *NT* перебільшують реальні та теоретичні оцінки числа кроків генератора до зациклення практично в 45 разів. Результати були отримані для кожної точки кривої, яка може використовуватись в якості генератора групи, шляхом перебору всіх можливих $t_0 = seed$ для кожної точки.

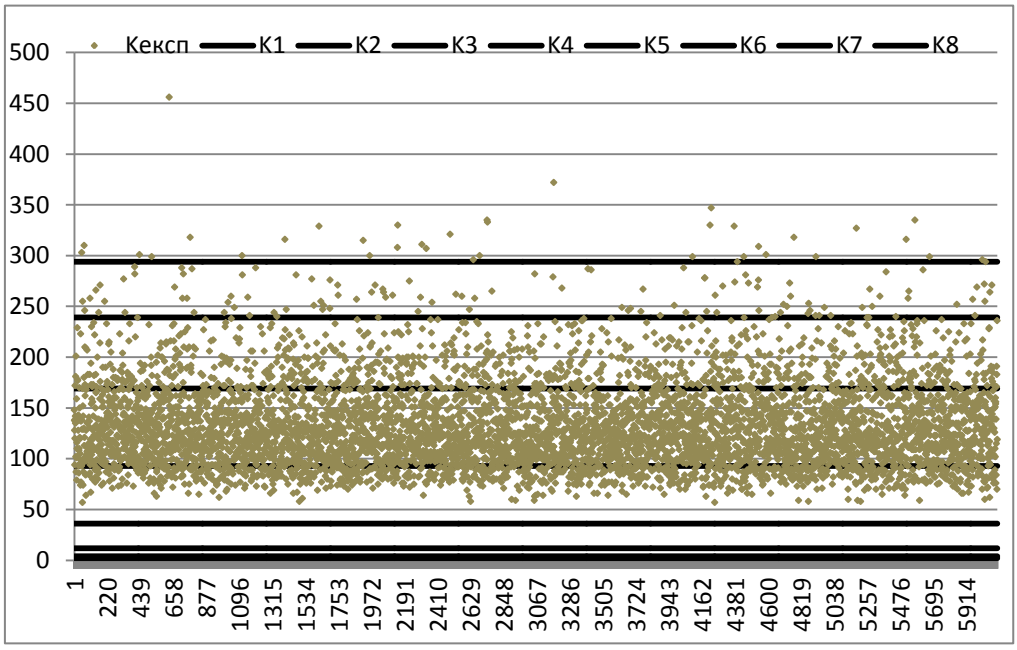

Рис. 2. Оцінки *K1, K4, K5, K6, K7, K8* та $K_{експ}$.

З отриманих результатів можна побачити, що основна частина значень кількості кроків до зациклення генератора знаходиться в межах 93 – 169 кроків, що відповідає границям імовірності зациклення 0,5 – 0,9. Середнє значення числа *K* кроків до зациклення генератора склало 133 кроки, що менше числа *NT* в 46 разів, а довжина значення *K* менша довжини *NT* в 1,78 разів. Це означає, що в середньому після 133 кроків роботи генератора виникне зациклення. Враховуючи середнє значення та середнє відхилення основна частина значень

лежить в границях 100 – 166 кроків, а відношення довжин *NT* та *K* знаходилось в границях (1,7; 1,9). Для генераторів, що використовуються з іншими кривими час проведення експериментів, відношення log(*NT*)/log(*K*) наближалось до 2.

Результати оцінки середнього значення довжини послідовності для генератора на еліптичних кривих показали, що довжина числа кроків до першого зациклення генератора менше довжини порядка циклічної групи точок кривої приблизно в 1,7 – 2 разів. Для реальних генераторів це означає зменшення рівня стійкості з 2^{256} до 2^{150}. Очевидно, що збільшення числа внутрішніх станів без витрат часу є одним з можливих шляхів вдосконалення генераторів цього класу.

ВДОСКОНАЛЕНИЙ МЕТОД ГЕНЕРАЦІЇ ПВП НА ОСНОВІ ЕК

Нехай базова еліптична крива задана у канонічній формі E_p (2), ізоморфні трансформації кривої задані виразом (3). Для опису алгоритму генерації зафіксуємо наступні операції: отримання ізоморфної базової точки $P_i = \varphi_i(P)$, отримання раундової точки кривої, $f(P_{i-1}, P_i) = P' = t_i * P_i$, перетворення координати X в бітову послідовність, $r_i = \phi(X[P_i])$, компресія бітової послідовності в блок біт $b_i = extr(r_i)$ (один біт) згідно [12].

Структура вдосконаленого генератора наведена на рис. 3.

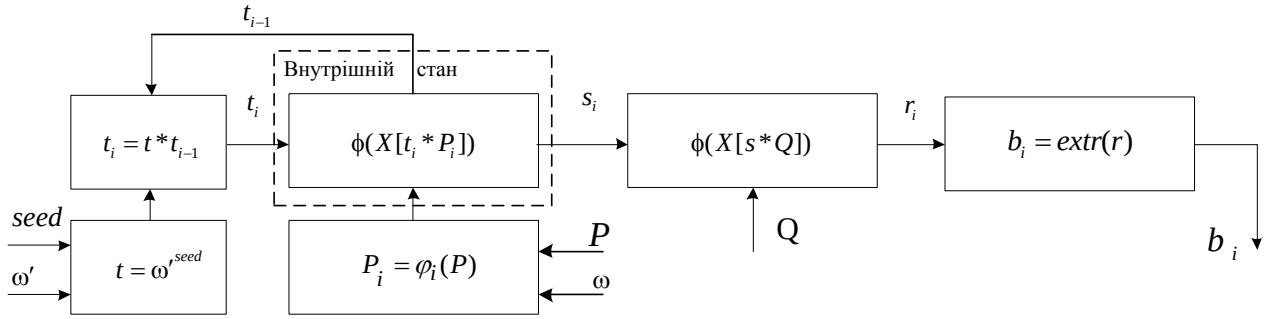

Рис. 3. Модель модифікованого генератора Dual_EC_DRBG

Алгоритм генерації має наступні кроки.

Початок алгоритму. Встановлення початкового стану генератора: *p*, *A*, *B*, *P*, *Q*, $l_{ПВП}$.

Крок 1. Обчислення скалярне число *t*:

$$t = \omega'^{seed} \bmod n, \tag{5}$$

де *n* – порядок циклічної групи точок *P* й *Q* (просте число);

ω' – генератор групи Z_n;

seed – секретне число, $(seed, n) = 1$.

Крок 2. Обчислення значення раундового скаляра t_i наступним чином:

$$t_i = t * t_{i-1} \bmod n. \tag{6}$$

Крок 3. Обчислення значення u_i:

$$u_i = \omega^{2i} \bmod p, \tag{7}$$

де ω – генератор групи Z_p, *p* – характеристика поля Галуа.

Крок 4. Розрахунок значень координат ізоморфної точки P_i: $x_{P_i} = u_i^2 \bar{x} \bmod p$, $y_{P_i} = u_i^3 \bar{y} \bmod p$.

Крок 5. Розрахунок значення внутрішнього стану генератора:

$$r_i = X[t_i \underset{scal\,mull}{*} P_i] = X[t_i \underset{scal\,mull}{*} \varphi_i(P)]. \tag{8}$$

Крок 6. Отримання бітового блока (біт) з послідовності r_i:

$$b_i = extr(r_i). \tag{9}$$

Кінець алгоритму.

З використанням запропонованого алгоритму була розроблена програмна реалізація генератора ПВП на основі мови програмування С++ та отримані ПВП з параметрами рекомендованим в стандартах [12,15].

Математичний вираз функції генерації псевдовипадкових бітів з використанням вдосконаленого генератора ПВП можна отримати підстановкою виразів (5 – 7) в вираз (8):

$$r_i = \phi(X\left[\phi\left(X\left[\omega'^{seed} * t_{i-1} (\mathrm{mod}\, n) \underset{scal\, mull}{*} (\omega^{4i} * X_P (\mathrm{mod}\, p), \omega^{6i} * Y_P (\mathrm{mod}\, p))\right]\right) \underset{scal\, mull}{*} Q\right]). \quad (10)$$

Для оцінки стійкості до передбачення вдосконаленого генератора скористаємось введеними значеннями *NT* та іншими параметрами генератору ПВП.

Скаляр t_i пробігає усі елементи Z_n, внаслідок чого $P_i = t_i * P$, $P_i \in E^i{}_p$ (E_p^i – ізоморфна група точок, за умовою $\#E$ – просте). Параметр u_i пробігає усі значення від'ємників у полі, число яких NT. У такому випадку, період послідовності значень $X[P_i] = X[t_i * \varphi_i(P)]$, які потрапляють у якості скалярів на вхід $s*Q = X[P_i]*Q$, буде дорівнювати *NT*. Період ПВП у такому випадку буде дорівнювати *NT*.

Враховуючи граничні значення числа ізоморфізмів ЕК у канонічній формі, а саме верхня границя яких дорівнюватиме $NT = 1/2(p-1)$, верхня границя числа внутрішніх станів вдосконаленого генератора Dual_EC_DRBG буде визначена виразом:

$$NT = 1/2(p-1)*n,$$

де *n* – порядок циклічної групи точок кривої, *p* – характеристика поля Галуа.

Наприклад, для забезпечення стійкості до передбачення генератора ПСП еквівалентної значенню 2^{512} необхідно використовувати циклічну групу точок, порядок якої є 257-бітним числом. Або якщо зафіксувати стійкість до передбачення генератору то можливо використовувати довжину характеристики поля 128 бітів та довжину параметру ізоморфної трансформації 129, що дозволить отримати рівень стійкості стандартизованого генератору ПВП 2^{257}.

Висновки

Таким чином, в ході досліджень було запропоновано нове рішення наукового завдання щодо вдосконалення методу генерації ПВП на еліптичних кривих за рахунок збільшення періоду ПВП (числа кроків до зациклення) з використанням ізоморфних перетворень еліптичних кривих. Отриманий метод дозволив у $1/2(p-1)$ разів збільшити число внутрішніх станів генератора, а також збільшити період криптографічної ПВП, що дозволило підвищити стійкість генератора ПВП до передбачення пропорційно характеристики поля *p*. При фіксованому значенні числа внутрішніх станів вдосконалений генератор ПВП дозволяє скоротити бітову довжину характеристики *p* поля та підвищити його швидкодію.

В подальшому, підхід до використання ізоморфних перетворень може бути застосований для побудови алгоритмів генерації криптографічних ключів для різних додатків криптографічного захисту, які використовуються в інформаційно-телекомунікаційних системах критичної інфраструктури.

ЛІТЕРАТУРА

1. Thurimella R. Cryptography for Cyber Security and Defense: Information Encryption and Cyphering / R. Thurimella and L. C. Baird III // IGI Global, 2009, chapter title: „Network Security".

2. Knudsen L., Meier W., Preneel B., Rijmen V., Verdoolaege S. Analysis methods for (alleged) RC4 / ASIACRYPT: International Conference on the Theory and Application of Cryptology. LNCS, Springer-Verlag. – 1998. P. 327 – 341.

3. Mantin I., Shamir A. A practical attack on broadcast RC4 / In FSE: Fast Software Encryption. – 2001.

4. Biham E., Dunkelman O. Cryptanalysis of the A5/1 GSM Stream Cipher / Progress in Cryptology, Proc. Of Indocrypt' 00.: Lecture Notes in Computer Science. – Springer-Verlag, 2000. – Vol. 1977. – P. 43 – 51.

5. Coppersmith D. Cryptanalysis of stream ciphers with linear masking // Proc. Crypto2002. Cryptology ePrint Arhive, Report 2002/020, 2002.

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

7. Güuneysu T., Paar C., Pelzl J. On the Security of Elliptic Curve Cryptosystems against Attacks with Special-Purpose Hardware / Horst G¨ortz Institute for IT Security, Ruhr University Bochum, Germany. – 2006. P. 1 – 20. Web: http://www.copacobana.org/paper/mppr_SHARCS2006.pdf

8. Marc J., Koc C., Naccache D., Paar C. Hessian elliptic curves and side-channel attacks / Cryptographic hardware and embedded systems – CHES 2001. LNCS 2162, Springer. – 2001. – P. 402 – 410.

9. Brier E., Joye M., Naccache D, Paillier P. ed. Weierstrass elliptic curves and side-channel attacks/ Public key cryptography. LNCS 2274, Springer. – 2002. – P. 335 – 345.

10. Billet O., Joye M., Fossorier M., Hoeholdt T., Poli A. ed. The Jacobi model of an elliptic curve and side-channel analysis/ Applied algebra, algebraic algorithms and error-correcting codes. LNCS 2643, Springer. -2003. – P. 34 – 42. URL: eprint.iacr.org/2002/125.

11. Shor P. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer, in Proc./ Shor P.W. // IEEE Computer Society Press 1994. – P. 31.

12. NIST Special Publication 800-90A. Recommendation for Random Number Generation Using Deterministic Random Bit Generators / Elaine Barker, John Kelsey // Computer Security Division Information Technology Laboratory National Institute of Standards and Technology. – January 2012.

13. ISO/IEC 18031 Information technology. – Security techniques – Random bit generation.

14. ANSI X.9.82, Part 3 – Draft – July 2004. Random Number Generator, Part 3: Deterministic Random Bit Generators.

15. Application Notes and Interpretation of the Scheme (AIS) 31. Functionality classes and evaluation methodology for physical random number generators. Certification body of the BSI in context of certification scheme. BSI, 2001, 38 p.

16. 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.

17. 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.

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

19. N. Howgrave-Graham. A hybrid lattice reduction and meet-in-the-maiddle-attack against NTRU. Crypto 2007.

20. Husemöller D., Theisen S., Forster O., Lawrence R. Elliptic Curves, Second Edition / Springer – 2002. – P. 487.

21. Бессалов А. Криптосистемы на эллиптических кривых: Учеб. Пособие. – К.: ІВЦ «Видавництво «Політехніка»», 2004. – С. 224.

22. Rostovtsev A., Stolbunov A. Public-key cryptosystem based on isogenies. – Cryptology ePrint Archive, Report 2006/145.

23. Bostan A., Morain F., Salvy B. Fast algorithms for computing isogenies between elliptic curves. – INRIA-00091441, version 1–6 Sep. 2006.

24. Василенко О. Н. Об алгоритмах построения изогений эллиптических кривых над конечными полями и их приложениях, Матем. вопр. криптогр., 2010, том 1, выпуск 1, 7–22.

25. Чевардін В.Є., Ковальчук Л. В. Аналітичні оцінки зациклень генераторів псевдовипадкових послідовностей на еліптичних кривих // Науково-технічний журнал „Радиотехника". ХНУРЕ. Харків. 2015. №183. С. 150 – 160.