СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ

УДК 512.624.95

В.Є. ЧЕВАРДІН, Л.В. КОВАЛЬЧУК

АНАЛІТИЧНІ ОЦІНКИ БЕЗПЕКИ ГЕНЕРАТОРІВ ПСЕВДОВИПАДКОВИХ ПОСЛІДОВНОСТЕЙ НА ЕЛІПТИЧНИХ КРИВИХ

Вступ

Велика увага сьогодні приділяється розробці криптографічних методів, побудованих з використанням перетворень в групі точок еліптичної кривої (ЕК). Яскравим прикладом є алгоритми генерації псевдовипадкових послідовностей (ПВП) на ЕК. В результаті багатьох досліджень в цьому напрямку алгоритм генерації ПВП на еліптичних кривих Dual_EC_DRBG був включений до стандарту NIST SP 800-90A та почав використовуватись в сучасних операційних системах. Однак існуючі алгоритми побудови генераторів ПВП на ЕК [1 – 15] мають високу обчислювальну складність, що обмежує їх використання з одного боку, а з іншого мають певні уразливості, що стосуються зациклень, які приводять до зменшення числа задіяних внутрішніх станів генератора, та, як наслідок, до зниження стійкості до відтворення та передбачення генератора.

Мета статті – отримання оцінок імовірності зациклень та числа кроків до зациклення генераторів ПВП, побудованих з використанням скалярного множення точок еліптичної кривої, та запропонування нового підходу до генерації ПВП для підвищення її стійкості до від-творення.

Основні результати роботи

Для оцінки числа внутрішніх станів, числа кроків до зациклення генератора Dual_EC_DRBG та імовірності зациклення розглянемо сутність криптографічного перетворення, на основі якого побудований генератор.

Структурні особливості широковідомого генератора Dual_EC_DRBG, рекомендованого стандартом [20], детально розглянуті в роботах [6, 13, 15, 18, 19]. Нехай еліптична крива задана рівнянням

$$E: y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,\ a_i \in F_p, \tag{1}$$

де $P, Q \in E_p$.

Тоді блок на виході Dual_EC_DRBG b_i обчислюється за допомогою виразу (2):

$$b_i = extr\left[t_i * Q\right] = extr\left[(\psi(t_{i-1} * P) * Q)\right], \tag{2}$$

де $\psi(P) = X_P \bmod n.$; $t_0 = HDF(seed, nonce, ID)$; n – порядок циклічної підгрупи точок.

Послідовність внутрішніх станів генератора $\{t_1, ..., t_{\upsilon-1}\}$ утворюється за правилом

$$t_i = \psi(P_i) = \psi(\psi(t_{i-1} * P) * P), \tag{3}$$

де $i = \overline{(1, \upsilon)}$, P, Q – базові точки кривої.

Число різних значень (координат точок кривої) на виході другого скалярного множення в виразі (1) дорівнює числу внутрішніх станів генератора. Послідовність виходів другого скалярного множення також залежить від послідовності $\{t_1, ..., t_{\upsilon-1}\}$ та не впливає на порядок слідування внутрішніх станів та їх число. В більшості сучасних робіт стосовно побудови генераторів на еліптичних кривих період такого генератора вважається близьким до кількості n його внутрішніх станів. Однак ця границя не є точною у зв'язку з існуванням для цього типу перетворення зациклень з малим періодом. Розглянемо зациклення генераторів на основі еліптичних кривих детальніше. Для подальшого викладання нам потрібно ввести ряд означень, що стосуються псевдовипадкових генераторів та їх послідовностей.

Нехай

$$\xi_0, \xi_1, ..., \xi_\upsilon \tag{4}$$

– вихідна послідовність деякого псевдовипадкового генератора.

Означення 1. Якщо існує таке $i \geq 0$, що для деякого $k \in \mathbb{N}$ виконується $\xi_i = \xi_{i+k}$, то послідовність

$$\xi_0, \xi_1, ..., \xi_{l-1},$$

де $l = min\{i \geq 0 / \exists k \in \mathbb{N}: \xi_{i+k} = \xi_i\}$
будемо називати передперіодом послідовності (3), якщо $l \geq 1$.

Якщо ж $l = 0$, то будемо вважати, що послідовність (3) є чисто періодичною, або послідовність (2) не має передперіоду. Число l є довжиною передперіоду.

Означення 2. Нехай $\xi_0, \xi_1, ..., \xi_{l-1}$ – передперіод послідовності (3). Тоді величина $T = \min\{k \geq 1 : \xi_{l+k} = \xi_l\}$ називається довжиною періоду послідовності (3).

Означення 3. Нехай задана послідовність (3). 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 (3) для деякого $k \in \mathbb{N}$, має передперіод $t_0, t_1, ..., t_{l-1}$ та довжину періоду $T = \min\{k \geq 1 : t_{l+k} = t_l\}$, де $l = min\{i \geq 0 / \exists k \in \mathbb{N}: t_{i+k} = t_i\}$.

Враховуючи, що кожна точка циклічної групи породжує свою підгрупу точок $\{P, 2P, 3P, ..., (n-1)P\}$, виникнення зациклення є властивістю кожної точки. Кількість кроків до зациклення генератора залежить від того, за скільки кроків відбудеться повторення внутрішнього стану. До зациклення можна прийти, починаючи з будь-якого початкового значення t_0. Операція $\psi(P_i) = X[P_i] (\mathrm{mod}\, n)$, що відбувається на кожній ітерації, потенційно збільшує випадки зациклення генератора.

Імовірність зациклення генератора

Так як властивості точок еліптичної кривої, які впливають на кількість кроків до зациклення, на сьогоднішній день не вивчені, вважають, що розподіл точок в циклічних підгрупах точок кривої мають випадковий характер.

Припущення. Враховуючи випадковий характер розподілу точок в циклічних підгрупах кривої, припустимо, послідовність (4) є випадковою, а її елементи розподілені рівномірно на множині всіх можливих *X*-координат точок циклічної підгрупи.

Враховуючи це припущення та закон формування послідовності (3), множина всіх внутрішніх станів генератора (2) співпадає з множиною всіх *X*-координат точок циклічної підгрупи. Позначимо *NT* – потужність цієї множини, тоді $NT = \frac{n-1}{2}$. Позначимо *L* – номер кроку, на якому відбулось зациклення.

Теорема 1. Нехай $\frac{L^2}{2NT} \to \lambda$, при $L, NT \to \infty$. Тоді для генератора ПВП, який створює послідовність внутрішніх станів (3), імовірність відсутності зациклення до *L*-го кроку ($L<NT$) визначається виразом

$$P(K > L) \to e^{-\frac{L^2}{2NT}} = e^{-\lambda}, L, NT \to \infty. \tag{5}$$

Доведення.

Згідно з припущенням та законом формування внутрішніх станів (3), імовірність події $\{K > L\}$ дорівнює імовірності того, що при рівноімовірному розподілі *L* частинок по *NT* чарунках кожна чарунка містить не більше однієї частинки. У позначеннях теореми 3 [16],

$P(K > L) = P(\nu_2(L, NT) = 0) \to e^{-\lambda}$, при $L, NT \to \infty$, де $\lambda = \lim\limits_{L,\, NT \to \infty} \dfrac{L^2}{2NT}$.

Теорема 1 дозволяє оцінити імовірність зациклення для різних значень числа різних координат точок циклічної групи кривої *NT* та число кроків до зациклення генератора *K* (для достатньо великих значень *NT* та *K*).

Наприклад, для генератора на еліптичній кривій, побудованій над полем F_p, де $\log(p) \approx 32$, для різної довжини числа кроків до зациклення імовірність зациклення становить: $P(K > 2^4) \approx 1{,}86e^{-9}$, $P(K > 2^8) \approx 2{,}98e^{-8}$, $P(K > 2^{16}) \approx 7{,}63e^{-6}$, $P(K > 2^{24}) \approx 3{,}93e^{-1}$, $P(K > 2^{32}) \approx 1$. Для генератора на еліптичній кривій, побудованій над полем F_p, де $\log(p) \approx 64$, для різних значень K імовірність зациклення становить: $P(K > 2^8) \approx 1{,}78e^{-15}$, $P(K > 2^{16}) \approx 1{,}16e^{-10}$, $P(K > 2^{24}) \approx 7{,}63e^{-6}$, $P(K > 2^{32}) \approx 3{,}93e^{-1}$, $P(K > 2^{48}) \approx 1$.

Наслідок 1. Імовірність зациклення на *k*-му кроці: $P(l) \approx e^{-\lambda} \cdot \dfrac{k-1}{NT}$, де $\lambda = \dfrac{(k-1)^2}{2NT}$.

Зазначимо, що стійкість генератора буде визначатись не загальною кількістю внутрішніх станів генератора *NT*, а кількістю кроків до зациклення, що може бути суттєво меншим за *NT*. Проте у переважній більшості робіт [3, 6, 13, 10, 19] вважається, що кількість кроків до зациклення дорівнює *NT* або є близькою до *NT*.

Теорема 2. Нехай імовірність появи $\forall t_i$, $i = (0, NT)$ буде $p_1 = p_2 = ... = p_{NT} = \dfrac{1}{NT}$. Задамо деяку $0 < pr < 1$. Тоді для того щоб імовірність зациклення була не меншою за *pr*, необхідно зробити не менше ніж *K* кроків, де

$$K = \sqrt{2aNT} - \frac{a}{3} + \frac{1}{2} + \theta(NT), \tag{6}$$

при $NT \to \infty$,
де $a = -\ln(1 - pr)$,
$\underline{\lim}\theta(NT) = 0$,
$\overline{\lim}\theta(NT) = 1$.

Доведення.

Згідно з припущенням та законом формування внутрішніх станів (3), імовірність потрапляння в чарунку дорівнює $p_1, ..., p_{NT}$, $\sum\limits_{i=1}^{NT} p_i = 1$, тобто координати точок циклічної підгрупи мають рівноімовірний розподіл.

Число кроків до зациклення генератора дорівнюватиме мінімально необхідному числу частинок $K = K(NT, pr, 2)$, таких що $P(K > L) = P(K, NT) \geq pr$. У позначеннях теореми 3 [17] $K = \sqrt{2aNT} - \dfrac{a}{3} + \dfrac{1}{2} + \theta(NT)$.

Наприклад, за умови теореми 1 число кроків до зациклення генератора становить для генератора на еліптичній кривій, побудованій над полем F_p, де $\log(p) = 32$, $NT = 4294967296$.

Таблиця 1

pr	0,0001	0,001	0,01	0,1	0,5	0,9	0,99	0,999

K	927	2932	9292	30084	77163	140639	198894	243595

Наприклад, за умови теореми 1, оцінки числа кроків до зациклення генератора на еліптичній кривій, побудованій над полем F_p, де $\log(p) \approx 64$, $NT = 1{,}84e^{19}$, наведені в табл. 2.

Таблиця 2

pr	0,0001	0,001	0,01	0,1	0,5	0,9	0,99	0,999
K	6E+07	2E+08	6E+08	2E+09	5E+09	9E+09	1E+10	1,6E+10

Розглянемо приклади зациклення генератора, побудованого з використанням операцій на еліптичній кривій. Оцінки кількості кроків до зациклення генератора розраховувались для кожної точки, що обралась як базова, та аналізом кількості кроків до зациклення для всіх можливих скалярних значень t_0.

Приклад 1. Нехай ЕК задана рівнянням $E: y^2 = (x^3 - 3x + 3)$ над F_{17}, порядок циклічної групи для обраної кривої дорівнює 23. Черговий стан генератора отримується шляхом обчислення: $t_i = \psi(t_{i-1} * P) = \psi(P_i)$, $P_i = t_{i-1} * P = \psi(P_{i-1}) * P$, де $P \in E_{17}$. Результати скалярного множення для базової точки (4;2) наведені в табл. 3.

Таблиця 3

P	2P	3P	4P	5P	6P	7P	8P	9P	10P	11P	12P
(4;2)	(7;11)	(15;16)	(11;3)	(10;2)	(3;15)	(9;12)	(8;7)	(4;11)	(1;16)	(13;6)	(13;11)
13P	14P	15P	16P	17P	18P	19P	20P	21P	22P	23P	
(1;1)	(14;6)	(8;10)	(9;5)	(3;2)	(10;15)	(11;14)	(15;1)	(7;6)	(4;15)	*O*	

Побудуємо послідовності точок, з яких отримуються значення $t_1, ..., t_n$ для кожної точки кривої до моменту зациклення генератора, але наведемо приклад (табл. 4) тільки для двох точок P = (1;16) та P = (3;15). Визначимо значення передперіоду та періоду відповідних послідовностей. В таблиці наведені значення точок кривої, з яких виділяються значення внутрішнього стану генератора: $t_2, ..., t_9$. Значення *X*-координати точок, тобто $t_i = \psi(P_i)$, в яких
відбуваються зациклення, виділені жирним шрифтом.

Таблиця 4

t_1	t_2	t_3	t_4	t_5	t_6	t_7	t_8	t_9	***l***	***T***
P = (1;16)										
1	(**1**;16)								0	1
3	(9;12)	(7;6)	(4;2)	(**3**;2)					0	4
4	(3;2)	(9;12)	(7;6)	(**4**;2)					0	4
7	(4;2)	(3;2)	(9;12)	(**7**;6)					0	4
8	(13;6)	(**8**;10)							0	2
9	(7;6)	(4;2)	(3;2)	(**9**;12)					0	4
10	(**8**;7)	(13;6)	(**8**;10)						1	2
11	(10;15)	(**13**;11)	(8;10)	(**13**;6)					2	2
13	(8;10)	(**13**;6)							0	2
14	(**7**;11)	(4;2)	(3;2)	(9;12)	(**7**;6)				1	4
15	(**13**;11)	(8;10)	(**13**;6)						1	2
P = (3;15)										
1	(3;15)	(10;15)	(14;6)	(8;10)	(**7**;11)	(11;14)	(15;1)	(**7**;6)	5	3
3	(10;15)	(14;6)	(8;10)	(**7**;11)	(11;14)	(15;1)	(**7**;6)		4	3
4	(**4**;2)								0	1
7	(11;14)	(15;1)	(**7**;6)						0	3
8	(**7**;11)	(11;14)	(15;1)	(**7**;6)					1	3
9	(8;7)	(**7**;11)	(11;14)	(15;1)	(**7**;6)				2	3
10	(14;6)	(8;10)	(**7**;11)	(11;14)	(15;1)	(**7**;6)			3	3

11	(15;1)	(7;6)	(**11**;14)						0	3
13	(14;11)	(8;10)	(**7**;11)	(11;14)	(15;1)	(**7**;6)			3	3
14	(8;10)	(**7**;11)	(11;14)	(15;1)	(**7**;6)				2	3
15	(**7**;6)	(11;14)	(**15**;1)						0	3

Для визначених параметрів генератора ($p=17$, $n=23$) максимальні значення передперіоду та періоду склали $l=7$, $T=6$. Максимальне значення кроку зациклення, тобто числа внутрішніх станів генератора до зациклення склало $k=8$, що менше порядка циклічної групи точок практично в 3 рази.

*Приклад 2***.** Нехай еліптична крива задана рівнянням $E_{12391}: y^2 = x^3 + 1322x + 3$. Порядок циклічної групи точок кривої дорівнює $n=12239$, $\log n = 14$, $NT = 6119$. Для такого генератора розглянемо три випадки: $\log k = 2, \log k = 3, \log k = 6$.

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 оцінок [17], наведені в таблиці 5.

Таблиця 5

	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. 1 наведені оцінки *K1, K2, K3, K4, K5, K6, K7, K8* та $K_{експ}$. Значення *NT* перебільшує 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.

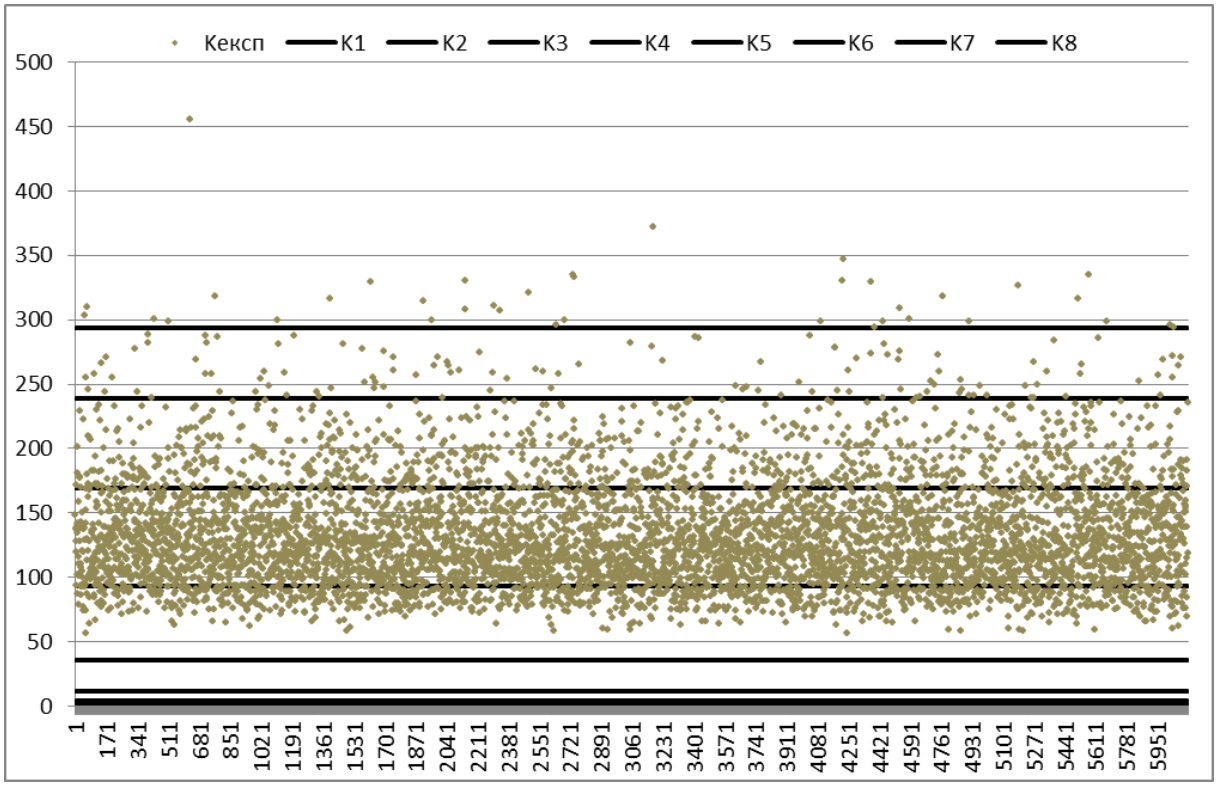

Рис. 1. Оцінки *K1, K4, K5, K6, K7, K8* та $K_{експ}$.

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 кроків до зациклення генератора склало 133 кроки, що менше числа *NT* в 46 разів, а довжина значення *K* менша довжини *NT* в 1,6 разів. Це означає, що в середньому після 133 кроків роботи генератора виникне зациклення. Для генераторів, що використовуються з іншими параметрами відношення NT / K знаходилась в границях $(1,6;1,7)$.

Вдосконалений генератор Dual_EC_DRBG

Нехай задана базова еліптична крива $E_{a,b,p} : y^2 = x^3 + ax^2 + b,\ p \neq 2,3, a,b \in F_p$ та її точки: $P(X_P, Y_P)$, $Q(X_Q, Y_Q) \in E_p$, $|E_p| = n$, $j \notin \{0, 12^3\}$. Для базової кривої, як було доведено раніше, існує можливість ізоморфної трансформації канонічної форми кривої в канонічну. Враховуючи, що для ізоморфної трансформації канонічної форми кривої (1) в іншу канонічну відповідні коефіцієнти трансформації кривої дорівнюють $s = r = t = 0$, що дозволяє задавати будь-яку трансформацію базової кривої в канонічній формі лише за допомогою параметра трансформації *u*. Коефіцієнти ізоморфної кривої розраховуються як $\bar{a}_4 = u^4 a_4, \bar{a}_6 = u^6 a_6$ [21, 22]. В такому випадку, лінійне ізоморфне перетворення координат цієї кривої задається виразами: $\bar{x} = xu^2$, $\bar{y} = yu^3$, $u \neq 0$. Крім цього, для вдосконалення генератора Dual_EC_DRBG необхідно обчислювати лише значення *X*-координати, тобто достатньо виконувати лише одну операцію піднесення до степеня 2 в простому полі: $\bar{x} = xu^2$. Побудуємо процедуру генерації чергового внутрішнього стану вдосконаленого Dual_EC_DRBG.

Функція f_k генерації внутрішніх станів генератора задана двома функціями: скалярним множенням $t * P$, де $t_0 = seed$ та ізоморфною трансформацією точки $P_i = t_i * P$, де параметр трансформації задається виразом $u_i = (u_{i-1} + 1) \bmod p$, $u_0 = HDF(seed)$. Значення u_i можна змінювати випадково, але треба впевнитись, що u_i пробіжить всі можливі значення.

Значення *X*-координати точки кривої, що отримана за рахунок ізоморфної трансформації з канонічної в канонічну форму, здійснюється за виразом $X[\varphi(P_i)] = u_i^2 X[P] \bmod p$.

З урахуванням встановлених параметрів, алгоритм генерації ПВП має наступні кроки.

Початок.

Введення параметрів: рівень безпеки генератора – *security_strenth*, довжина ПВП – L_{PRS}, характеристика поля *p*, коефіцієнти кривої *a* та *b* з урахуванням вимог до криптографічно стійких кривих, вхідна ентропія *entropy* довжина $l_{entropy}$, довжина вихідного блоку l_b, початкове секретне значення параметра ізоморфної трансформації $u_0 = HDF(seed)$. Задаються границі лічильника $0 < i < L_{PRS} / l_b$.

Крок 1. Генерується секретний *seed*.

Крок 2. Встановлюються початкові значення t_0, u_0.

Крок 3. Початок циклу $for(i = 0, i < L_{PRS} / l_b, i++)$.

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

Крок 3.2. Обчислюється $u_i = (u_{i-1} + 1) \bmod p$.

Крок 3.3. Обчислюється *X*-координата точки 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 генератора Dual_EC_DRBG можна представити наступною функцію генерації чергового значення b_i:

$$b_i = extr(r_i) = extr(\psi(\varphi(P_i)) * Q) = extr(\psi(\varphi(\psi(P_{i-1}) * P) * Q)), \qquad (7)$$

де P, Q – базові точки кривої, порядку n; $\varphi(P_i) = u_i{}^2 X[P_i] \bmod p$; $\psi(P) = X_P \bmod n$.

Приклад 3. Зафіксована крива $y^2 = x^3 + 4x + 3 \bmod 1231$, $NT = 1187$. Результати експериментальних та теоретичних оцінок числа кроків до зациклення для класичного та вдосконаленого Dual_EC_DRBG: $K_{експ}$, $K(pr = 0,1) = 36$, $K(pr = 0,5) = 53$, $K(pr = 0,9) = 77$, $K(pr = 0,99) = 98$ наведені на рис. 2.

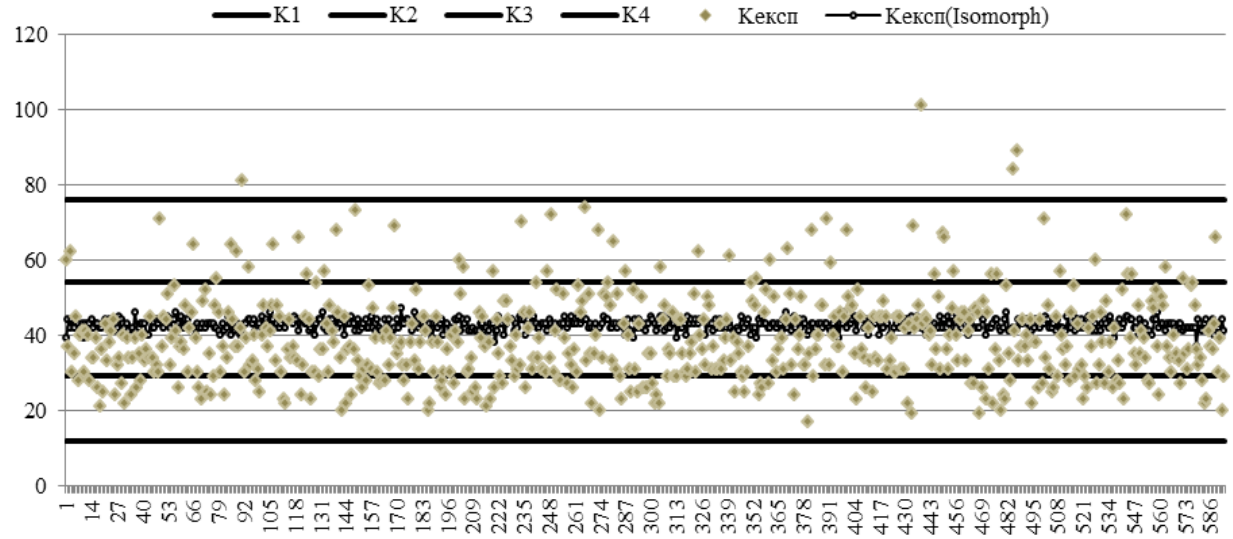

Рис. 2. Оцінки $K1(pr = 0,1) = 12$, $K2(pr = 0,5) = 29$, $K3(pr = 0,9) = 54$, $K4(pr = 0,99) = 76$, $K_{експ}$, $K_{експ}(Isomorph)$

Висновки

Вперше отримані оцінки імовірності зациклення генератора Dual_EC_DRBG та інших генераторів, які використовують в якості функції генерації внутрішнього стану скалярне множення точок кривої. Сформульовані теоретичні положення дозволили оцінити імовірність зациклення генераторів ПВП на еліптичних кривих (5) та число кроків до зациклення генератора (6), які надають можливість отримати більш точні оцінки стійкості ПВП до відтворення ніж існуючі в стандарті [20]. Так формула (6) дозволяє визначити, що реальна довжина числа кроків до зациклення генераторів на еліптичних кривих менше за довжину значення NT в два рази.

В статті наведено вдосконалений генератор ПВП на еліптичних кривих (7), за рахунок використання всієї множини ізоморфних трансформацій еліптичної кривої, який відрізняється від стандартизованого підвищенням мінімальної кількості кроків до зациклення, та, як наслідок, підвищенням стійкості до відтворення ПВП.

Список літератури: 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. *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. *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. *Hallgren, S.* Linear congruential generators over elliptic curve. // Cornegie Mellon Univ., 1994, CS-94-M3. – P. 1 – 10. 5. *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. 6. *Shparlinski, I.* On the Naor-Reingold pseudo-random function from elliptic curves / I. E. Shparlinski // Applicable Algebra in Engineering, Communication and Computing 11. – 2000. – P. 27 – 34. 7. *Beelen, P.* Pseudorandom sequences from elliptic curves / P. Beelen, J. Doumen // Finite Fields with Applications to Coding Theory, Cryptography and Related Areas, Springer-Verlag, Berlin. – 2002. – P. 37 – 52. 8. *Гриненко, Т.* Методы формирования псевдослучайных последовательностей в группах точек эллиптических кривых / Т. А. Гриненко, С. И. Збитнев, Д. В. Мялковский // Радиотехника. – 2002. – Вып. 119. – С. 119 – 123. 9. *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. 10. *Hess, F.* On the linear complexity and multidimensional distribution of congruential generators over elliptic curves / F. Hess, I. E. Shparlinski // Des. Codes Cryptogr. – 2005. – 35,1. – P. 111 – 117. 11. *Lange, T.* Distribution of some sequences of points on elliptic curves / T. Lange, I. E. Shparlinski // J. Math. Cryptol. – 20076. – 1. – P. – 1 – 11. 12. *Liu, H.* Large families of elliptic curve pseudorandom binary sequences / H. Liu, T. Zhan, X. Wang, // Acta Arith. – 2009. – 140. – P. 135 – 144. 13. *Shparlinski, I. E.* Pseudorandom number generators from elliptic curves. Recent trends in cryptography, 121 – 141, Contemp. Math., 477, Amer. Math. Soc., Providence, RI, 2009. 14. *Горбенко, І.* Метод побудування випадкових бітів на основі спарювання точок еліптичних кривих / І. Д. Горбенко, Н. В. Шапочка, К. А. Погребняк // Прикладная радиоэлектроника. – 2010. – №3. – С. 386 – 394. 15. *Schoenmakers, B.* Cryptanalysis of the Dual Elliptic Curve Pseudorandom sequences from elliptic curves / Schoenmakers B., Sidorenko A. 2006. 16. *Колчин, В.Ф.* Случайные размещения / В.Ф. Колчин, Б.А. Севастьянов, В.П. Чистяков. – М. : Наука, 1976. – 224 с. 17. *Ендовицкий, П. А.* Решение обобщенной обратной задачи о днях рождениях / П. А. Ендовицкий // Доповіді Національної академії наук України. – 2012. – N7. – С. 20 – 27. 18. *Зайцева, Н.* Атака розпізнавання на генератори псевдовипадкових послідовностей на основі еліптичних кривих / Н. Ю. Зайцева, Л. О. Завадська // Теоретичні і прикладні проблеми фізики, математики та інформатики. Збірка тез доповідей. ВПІ ВПК «Політехніка». – Київ, 2012. – С. 238 – 239. 19. *Gjøsteen, K.* Comments on Dual-EC-DRBG/NIST SP 800-90, Draft December 2005 / Kristian Gjøsteen // March 16, 2006. 20. *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. 21. *Бессалов, А.* Число ізоморфізмів еліптичної кривої при трансформаціях канонічної форми рівняння / А. В. Бессалов, В. Є. Чевардін // Системні дослідження та інформаційні технологій. – ІПСА «КПІ» МОН та НАНУ. – Вип. № 4. – Київ, 2012. – С. 119 – 123. 22. *Чевардін, В.* Изоморфные трансформации эллиптической кривой над конечным полем / В. Є. Чевардін // Кибернетика и системный анализ. – 2013. – Т. 49, № 3. – С. 168 – 171.

ВІТІ *Надійшла до редколегії 02.12.2015*