# СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ

**УДК 512.624.95 + 517.772**

*В.Є. ЧЕВАРДІН, канд. техн. наук*

## АНАЛІЗ СУЧАСНИХ КРИПТОГРАФІЧНИХ ГЕНЕРАТОРІВ ПСЕВДОВИПАДКОВИХ ПОСЛІДОВНОСТЕЙ НА ЕЛІПТИЧНИХ КРИВИХ

### Вступ

Найбільш актуальними задачами сьогодення в галузі криптографічного захисту інформації є розробка нових потокових шифрів та генераторів криптографічно стійких псевдовипадкових послідовностей (ПВП). Це обумовлено різким зростанням за останні десятиріччя обсягів інформації, що циркулює в інформаційно-телекомунікаційних мережах. Внаслідок цього, зросли вимоги до швидкості систем потокового шифрування, швидкості та криптографічної стійкості методів генерації ПВП. Більшість сучасних високошвидкісних генераторів ПВП не відповідають вимогам до криптографічної стійкості, що підтверджено результатами багатьох робіт в цієї галузі [1 – 10].

Відомо, що найбільш надійними генераторами випадкових послідовностей є генератори, побудовані на основі аналізу характеристик та параметрів фізичних явищ та процесів [1 – 5]. Як правило, універсальність та надійність таких генераторів супроводжуються суттєвими ускладненнями практичної реалізації. В зв'язку з цим, на практиці використовують псевдовипадкові послідовності, методи генерації яких запропоновані та розглянуті в багатьох роботах [6 – 10]. Аналіз існуючих робіт дозволив визначити криптографічні генератори ПВП як найбільш надійні та безпечні генератори ПВП, які можна використовувати в схемах генерації гам для потокових шифрів та криптографічних ключів для блокових шифрів.

Широко відомими генераторами є генератори, основані на лінійних конгруентних регістрах зсуву (Stop&Go, Парка – Міллера та інш.), на кодах Ріда – Соломона, на комбінаторних схемах, на модулярних операціях та операціях в простому полі Галуа: Блюма – Мікалі, Шаміра, BBS, RSA. Іншим класом є генератори, основані на блокових шифрах: TDEA, DES, 3DES та інші. Окремим класом генераторів є генератори, основані на геш-функціях: SHA2, SHA256, SHA512 та інш. В сучасних стандартах [25, 16] рекомендовані генератори усіх зазначених класів, кожен з яких має свої переваги та недоліки. Генератор BBS потребує для забезпечення необхідної криптографічної стійкості прості числа довжиною 1024 біта. Це суттєво збільшує обсяги службового трафіку та потребує великих обчислювальних витрат на криптографічні операції, тому використовується в якості еталонного генератору. Генератори на основі блокових шифрів мають більшу швидкість генерації, але жорстко прив'язані до структури блочного шифру та забезпечують криптографічну стійкість лише еквівалентну стійкості блочного шифру, що вимагає постійного аналізу стійкості блокових шифрів, що застосовані.

В зв'язку з цим, протягом останнього десятиріччя почали з'являться генератори нового класу, які використовують перетворення в групі точок еліптичної кривої [10 – 23]. Були отримані різні варіанти побудови генераторів: конгруентних генераторів ПВП [12, 13, 16 – 18], генераторів на основі скалярного множення точок суперсингулярної еліптичної кривої [13, 15], генераторів на основі скалярного множення точок несуперсингулярної еліптичної кривої [19 – 21], генераторів на основі операцій над точками двох ізоморфних еліптичних кривих [10 – 11]. Але практично усі запропоновані схеми генерації ПВП мають суттєві недоліки, що робить актуальними дослідження та аналіз криптографічної стійкості та псевдовипадкових властивостей генераторів на еліптичних кривих.

Метою даної статті є аналіз псевдовипадкових властивостей та криптографічної стійкості найбільш відомих генераторів, побудованих на основі операцій в групі точок еліптичної кривої, визначення обмежень та вимог в схемах генерації, які можуть приховувати загрози криптографічній стійкості та стійкості до відтворення і передбачення ПВП.

**Основні результати роботи**

Незважаючи на переваги лінійного конгруентного генератору ПВП, вони є криптографічно не стійкими [30, 31].

Нехай $G$ – лінійний конгруентний генератор, який задається секретним *seed* та функцією: $x_{i+1} = \alpha x_i + \beta (\mathrm{mod}\, n)$, де $n$ – просте число. Використовують різні *seed*: $\{\alpha, \beta\}$, $\{n, \alpha, \beta\}$, $\{x_0, \alpha, \beta\}$. Найбільш надійним вважається $seed = \{x_0, \alpha, \beta, n\}$. Виходом генератору $G$ є послідовність значень: $x_0, x_1, x_2, x_3, ..., x_{n-1}$.

Для відтворення закону формування внутрішніх станів генератору необхідно обчислити коефіцієнти: $\beta = x_i - \alpha x_{i-1} (\mathrm{mod}\, n)$, $\alpha$ та $n$. Якщо позначити $s_{i+1} = x_{i+1} - x_i (\mathrm{mod}\, n)$, тоді $s_{i+1} = x_{i+1} - x_i (\mathrm{mod}\, n) = (\alpha x_i + \beta) - (\alpha x_{i-1} + \beta) = \alpha (x_i - x_{i-1}) (\mathrm{mod}\, n) = \alpha s_i (\mathrm{mod}\, n)$, звідки $\alpha = s_{i+1} * s_i^{-1} (\mathrm{mod}\, n)$. Існують різні підходи до зламу таких генераторів: визначення коефіцієнтів $\alpha$, $\beta$ методом Марсаглія або Халдіра, використання метода Бояра [32], для Ф-генераторів: $s_i = \sum_{i=1}^{k} \alpha_j \hat{O}_j (s_0, s_1, ... s_{i-1}) (\mathrm{mod}\, n)$. Ці та інші підходи були детально розглянуті в роботах [30 – 32].

Незважаючи на недоліки звичайних лінійних конгруентних генераторів, за останні роки з'явилось багато спроб побудови нових лінійних конгруентних генераторів ПВП. Найбільш відомим підходом стали генератори, які використовують перетворення в групі точок еліптичної кривої. Розглянемо найбільш відомі з них.

*Генератор на еліптичних кривих 1.* В роботах [12, 13] запропоновано метод генерації ПВП на основі використання операції додавання точок еліптичної кривої.

Нехай еліптична крива задана рівнянням

$$E_{a,b,p} : y^2 = x^3 + ax + b (\mathrm{mod}\, p),\ a, b \in F_p, \tag{1}$$

де $p$ – велике просте число.

Ітераційна функція генерації чергового внутрішнього стану генератору

$$P_i = G + P_{i-1} = iG + P_0, \tag{2}$$

де $P_0$ – ініціалізація генератору; $G$ – генератор циклічної групи точок кривої $E_{a,b,p}$.

Черговий стан генератора ПВП обчислюється з використанням виразу (3):

$$s_i = f(P_i) = f(iG + P_0), \tag{3}$$

де $f(P_i)$ – раціональна функція, що відображає точку $(x, y)$ в елемент поля $F_p$.

На основі послідовності точок, отриманих на основі функції (3), отримується послідовність $E_N = \{e_1, \ldots, e_N\}$:

$$e_i = \begin{cases} 1, f(iG) \in \{0, 1, ..., (p-1)/2\}, \\ -1, \hat{a}\ {}^{3}\acute{\imath}\o\ .\ \hat{a}\grave{e}\ddot{\imath}. \end{cases} \tag{4}$$

В роботах [16 – 18] розглянуто декілька способів реалізації функції $f(P_i)$, такі як $f_1(x, y) = x$, $f_2(x, y) = y$, $f_3(x, y) = y/2$, $f_4(x, y) = p(x)$, $f_5(x, y) = p^{-1}(x)$. Розглянемо приклад реалізації цього генератора на малих полях з усіма функціями $f_i(x, y)$.

*Приклад 1.* Нехай задана несингулярна крива: $y^2 = x^3 - 3x + 4 (\mathrm{mod}\, 7)$ та визначена операція скалярного множення точок кривої (табл. 1). Можливі ПВП побудовані на основі базової точки (3,1) наведені в табл. 2.

Таблиця 1

Результати скалярного множення точок кривої $y^2 = x^3 - 3x + 4 (\mathrm{mod}\, 7)$

| *P(X;Y)* | *2P(X;Y)* | *3P(X;Y)* | *4P(X;Y)* | *5P(X;Y)* | *6P(X;Y)* | *7P(X;Y)* | *8P(X;Y)* | *9P(X;Y)* | *10P(X;Y)* |
|---|---|---|---|---|---|---|---|---|---|
| (0,2) | (1,4) | (3,6) | (5,3) | (4,0) | (5,4) | (3,1) | (1,3) | (0,5) | O |
| (0,5) | (1,3) | (3,1) | (5,4) | (4,0) | (5,3) | (3,6) | (1,4) | (0,2) | O |
| (1,3) | (5,4) | (5,3) | (1,4) | O | | | | | |
| (1,4) | (5,3) | (5,4) | (1,3) | O | | | | | |
| (3,1) | (5,3) | (0,2) | (1,3) | (4,0) | (1,4) | (0,5) | (5,4) | (3,6) | O |
| (3,6) | (5,4) | (0,5) | (1,4) | (4,0) | (1,3) | (0,2) | (5,3) | (3,1) | O |
| (4,0) | O | | | | | | | | |
| (5,3) | (1,3) | (1,4) | (5,4) | O | | | | | |
| (5,4) | (1,4) | (1,3) | (5,3) | O | | | | | |

Таблиця 2

Бінарні послідовності, побудовані на основі конгруентного генератора на еліптичних кривих

| *i* | *iG* | $f_1(x, y)$ | $e_i$ | $f_2(x, y)$ | $e_i$ | $f_3(x, y)$ | $e_i$ | $f_4(x, y)$ | $e_i$ | $f_5(x, y)$ | $e_i$ |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | (3,1) | 3 | 1 | 5 | 0 | 1 | 1 | 4 | 0 | 6 | 0 |
| 2 | (5,3) | 5 | 0 | 6 | 0 | 3 | 1 | 5 | 0 | 6 | 0 |
| 3 | (0,2) | 0 | 1 | 0 | 1 | 2 | 1 | 1 | 1 | 0 | 1 |
| 4 | (1,3) | 1 | 1 | 4 | 0 | 3 | 1 | 5 | 0 | 6 | 0 |
| 5 | (4,0) | 4 | 0 | 2 | 1 | 0 | 1 | 0 | 1 | 0 | 1 |
| 6 | (1,4) | 1 | 1 | 4 | 0 | 4 | 0 | 2 | 1 | 1 | 1 |
| 7 | (0,5) | 0 | 1 | 0 | 1 | 5 | 0 | 6 | 0 | 0 | 1 |
| 8 | (5,4) | 5 | 0 | 6 | 0 | 4 | 0 | 2 | 1 | 1 | 1 |
| 9 | (3,6) | 3 | 1 | 5 | 0 | 6 | 0 | 3 | 1 | 1 | 1 |

В роботах [12, 13, 16, 18] були отримані теоретичні значення нормального розсіювання $W(E_T)$ та кореляції, які були взяті за основу для визначення якості псевдовипадкових властивостей генератора. Однак отримані теоретичні показники не дають можливість виявити усі псевдовипадкові властивості ПВП запропонованих генераторів. В ході проведених досліджень запропоновані в цих роботах генератори були реалізовані мовою програмування C++ з використанням найбільш відомої бібліотеки MIRACLE. З використанням розроблених програмних реалізацій генераторів були отримані ПВП та досліджені за методикою тестування псевдовипадкових властивостей NIST STS [27].

Під час проведення дослідження були використані наступні параметри генераторів: функція генерації ПВП задана виразом (3), $f_1(x, y)$ (рис. 1), $f_2(x, y)$ (рис. 2), $f_3(x, y)$ (рис. 3), $f_4(x, y)$ (рис. 4), $f_5(x, y)$ (рис. 5). В якості кривої (1) була обрана крива P-256 (FIPS PUB 186-3) з наступними параметрами:

a = -3,

b = 5ac635d8aa3a93e7b3ebbd55769886bc651d06b0cc53b0f63bce3c3e27d2604b,

p = 115792089210356248762697446949407573530086143415290314195533631308867097853951.

Точки $G$ та $P_0$ згенеровані у відповідності до стандарту ANSI X9.62 [26]:

- $X(G)$ = 7b29e1ba366a10f482975f7c4fe981a959f001c01d99e22e46f71b6b2b725 168;
- $Y(G)$ = 84d894b0d1a0a54a83b91a652ddda32945e46736d6d6f8cf0ee991514af b5469;
- $X(P_0)$ = c7a5408faa98a47cb5f91208c9040896669650eb1f3ae48cf3a7e7d20ef8a b07;
- $Y(P_0)$ = acfe30c6f87ea601f11ca6e9c647c5a13cf4dbb93c2d1e12bdf832be608c78 26.

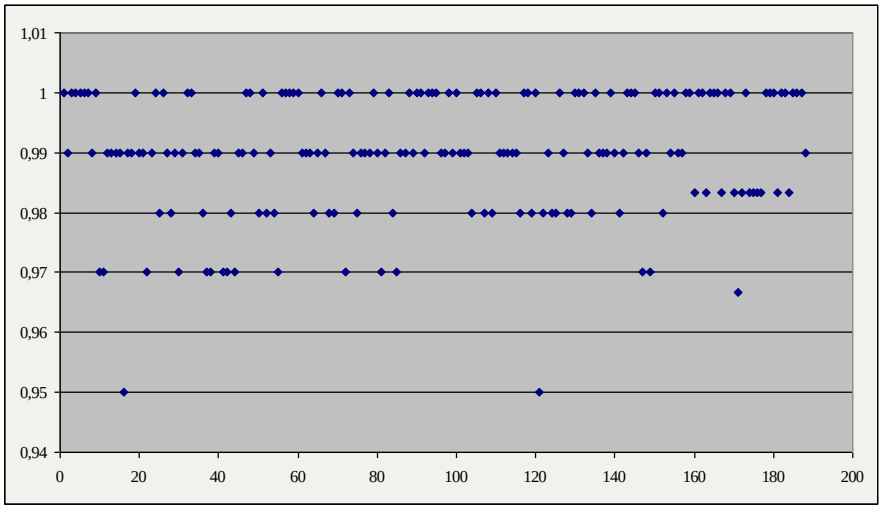


Рис. 1. Результати тестування псевдовипадкових властивостей послідовностей генератора (3), $f(x, y) = x$

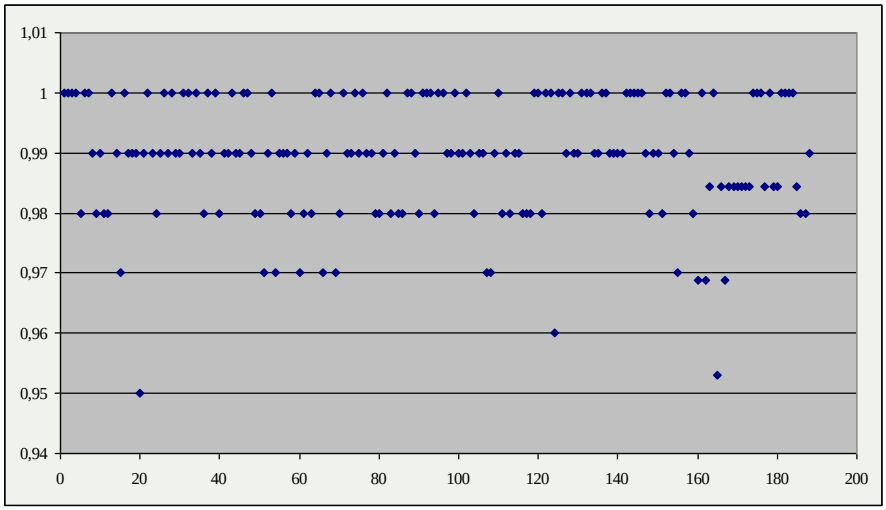


Рис. 2. Результати тестування псевдовипадкових властивостей послідовностей генератора (3), $f(x, y) = y$

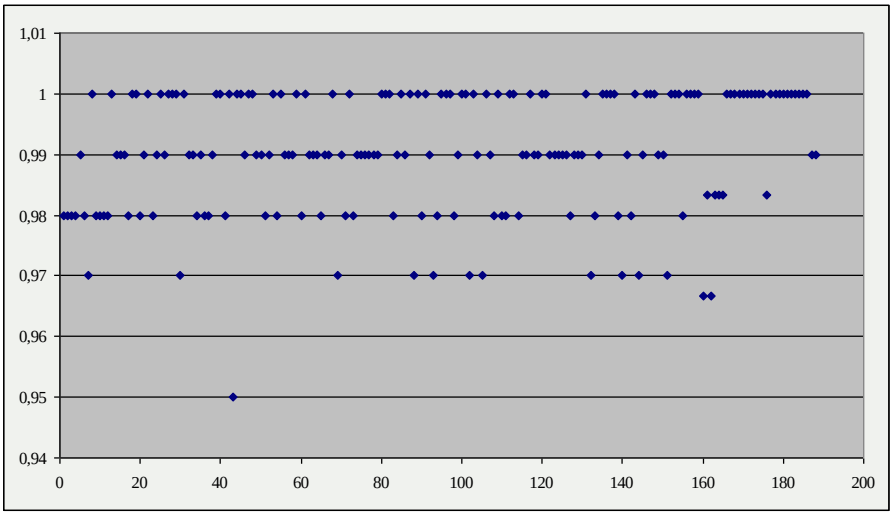


Рис. 3. Результати тестування псевдовипадкових властивостей послідовностей генератора (3), $f(x, y) = x/2$

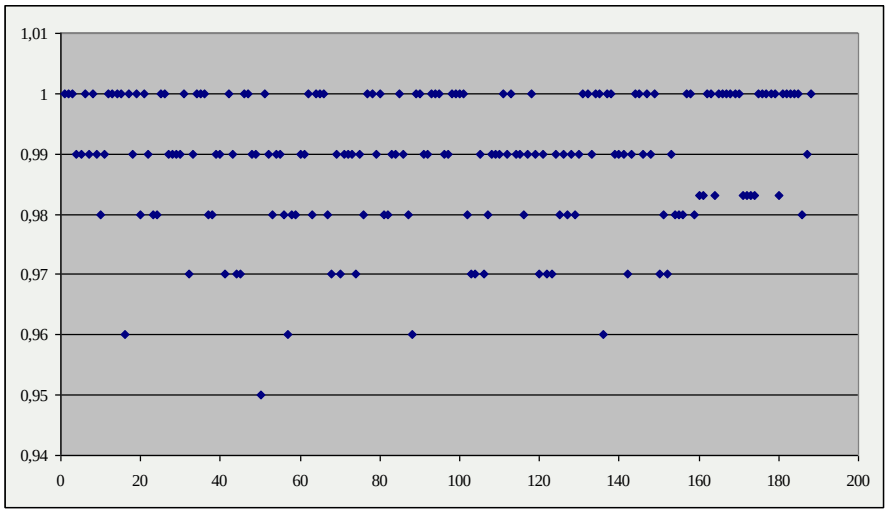


Рис. 4. Результати тестування псевдовипадкових властивостей послідовностей генератора (3), $f(x, y) = y/2$

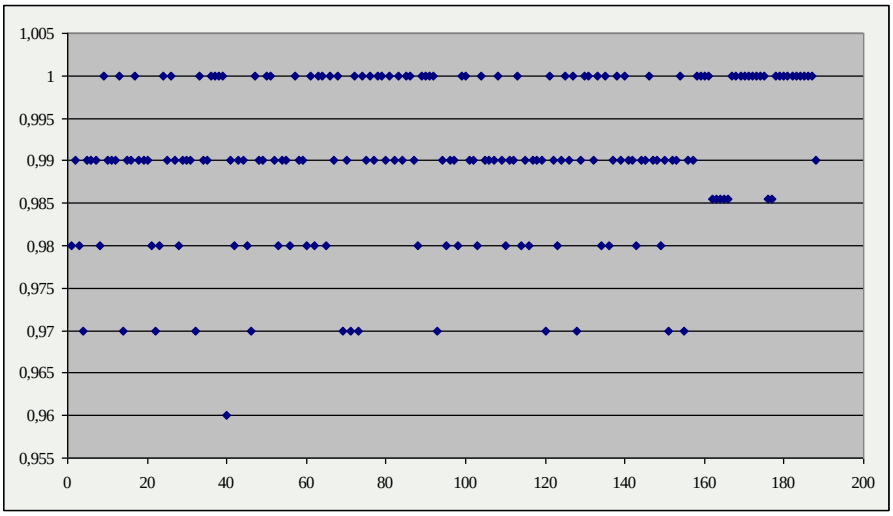


Рис. 5. Результати тестування псевдовипадкових властивостей послідовностей генератора (3), $f(x, y) = 9x+1/x$

Генератор з функцією $f(x, y) = x$ не пройшов тестування за двома тестами NonOverlappingTemplate. Генератор з функцією $f(x, y) = y$ не пройшов тестування за одним тестом NonOverlappingTemplate. Генератор з функцією $f(x, y) = x/2$ не пройшов тестування за одним тестом NonOverlappingTemplate. Генератор з функцією $f(x, y) = y/2$ не пройшов тестування за одним тестом NonOverlappingTemplate. Генератор з функцією $f(x, y) = 9x+1/x$ пройшов тестування за усіма 188 тестами. Як видно з усіх псевдовипадкових портретів, лінійні конгруентні генератори потенційно дозволяють отримати достатньо непогані псевдовипадкові властивості з різними видами функції $f(x, y)$. Але криптографічна стійкість таких генераторів однакова. В роботах [12, 13, 16 – 18] також було показано, що використання більш складних функцій перетворення точки в елемент поля не дає покращення псевдовипадкових властивостей та не впливає на криптографічну стійкість генератора, стійкість до передбачення або відтворення бітів ПВП. Незважаючи на задовільні показники тестування ПВП генератора з $f(x, y) = 9x+1/x$ лінійні конгруентні генератори ПВП не є криптографічно стійкими. В роботі [12] було доведено, що лінійні конгруентні генератори на еліптичних кривих не є криптографічно стійкими. Причина полягає в наступному.

Якщо G – лінійний конгруентний генератор на еліптичних кривих, який задається функцією $P_{i+1} = \alpha P_i + B(\mathrm{mod}\, n)$, де $n = ordP$, $P$ – базова точка еліптичної кривої,

$P_0 = \alpha P + B(\mathrm{mod}\, n)$, $B = \beta * P$, тоді в результаті роботи алгоритму з'являється послідовність точок кривої: $P_0, P_1, ..., P_{n-1}$, які перетворюються за допомогою певної раціональної функції в послідовність бітів. Складність передбачення послідовності точок еквівалентна рішенню задачі дискретного логарифмування:

$$\log_G(\alpha P_0 + B) = \log_G(\alpha P_i + \beta G) = \log_G(\alpha k_i G + \beta G) = \log_G((\alpha k_i + \beta)G) = \alpha k_i + \beta(\mathrm{mod}\, n).$$

Таким чином, незважаючи на можливість побудови статистично безпечних лінійних конгруентних генераторів ПВП на еліптичних кривих, задача зламу такого генератора може бути зведена до рішення задачі дискретного логарифмування в простому полі.

**Генератор на еліптичних кривих 2**

Наступний вид конгруентного генератора на еліптичних кривих – ECPSG I [12]. ECPSG I побудований на основі використання операції додавання точок суперсингулярної еліптичної кривої та обчислення сліду елемента $\alpha = Tr(c_i) = Tr(g(a^i))$, i=0, 1,…, $2^n - 2$.

Нехай еліптична крива $E(F_q)$ визначена над полем $F_{2^m}$, $P \in E(F_q)$, $E(F_q)$ – циклічна група точок кривої, $ord(P) = v+1, ord(P) \mid ord(E_p)$. Функція генерації псевдовипадкових послідовностей задається виразом (2), де на кожній ітерації координати точки перетворюються в елемент скінченого поля $X[P] \to F_2(E(F_q))$, $Y[P] \to F_2(E(F_q))$. Послідовність точок: $\{P, 2P, ..., vP\} = \{P_i\} = \{x_i, y_i\}, 1 \le i \le v$ трансформується в бінарну послідовність. Парність або непарність $v$ залежить від суперсингулярності еліптичної кривої. ПВП створюється шляхом вибору відповідних бітів з двох послідовностей $S_0$ та $S_1$. Сутність алгоритму генерації ПВП згідно ECPSG I заключається в двох етапах:

1) обчислюється $S_0 = \{Tr(X[G]), Tr(X[2G], ..., Tr(X[vG]))$ та

$S_1 = \{Tr(Y[G]), Tr(Y[2G], ..., Tr(Y[vG]))$;

2) обираються $s_{2i} = Tr(Y[iG])$, де $s_{2i-1} = Tr(X[iG])$, $i = 1,..v$.

Таким чином, довжина послідовності визначається як $L(S) = 2v$. Для генераторів ECPSG I рекомендовано обирати суперсингулярні криві, що пов'язано з легкістю визначення періодів ПВП генератору та позбавленням обчислювально складної операції визначення порядку кривої, хоча дозволяється обирати і несуперсингулярні криві. Розглянемо приклад генератора ECPSG I.

*Приклад 2*. Нехай скінчене поле побудовано на основі незведеного поліному $f(x) = x^3 + x + 1$, де α – корінь $f(x)$. Скінчене поле $F_{2^3}$ з використанням незвідного поліному, складається з наступних елементів (поліноміальна та нормальна форма): $\alpha^\infty = 0$, $\alpha^0 = 1$, $\alpha^1 = x$, $\alpha^2 = x^2$, $\alpha^3 = x+1$, $\alpha^4 = x^2 + x$, $\alpha^5 = x^2 + x + 1$, $\alpha^6 = x^2 + 1$. Для зручності запису елементів розширеного поля запишемо їх так: $\alpha^\infty = 0$, $\alpha^0 = 1$, $\alpha^1 = 2$, $\alpha^2 = 4$, $\alpha^3 = 3$, $\alpha^4 = 6$, $\alpha^5 = 7$, $\alpha^6 = 5$. Нехай еліптична крива задана рівнянням $y^2 + y = x^3 + c_4 x + c_6$ з коефіцієнтами: $c_4 = x = 2$, $c_6 = x+1 = 3$ над $F_{2^3}$. Еліптична крива представлена сукупністю пар елементів, що задовольняють рівнянню кривої. Результати скалярного множення точок еліптичної кривої для кожної точки кривої наведені в табл. 3.

Порядок кривої дорівнює $ordE_{2^3} = 9$, тобто крива суперсингулярна. З використанням отриманих результатів скалярного множення точок кривої побудуємо ПВП. З табл. 4 можна бачити, що період ПВП, отриманих за алгоритмом ECPSG I, складає 16 для усіх точок крім двох точок {2,6} та {2,7}, для яких період складає 3, так як порядок цих точок дорівнює 3.

Таблиця 3

Скалярне множення точок кривої $y^2 + y = x^3 + \alpha x + \alpha^3 (\mathrm{mod}\ f(x))$

| № | 1*P | 2*P | 3*P | 4*P | 5*P | 6*P | 7*P | 8*P |
|---|---|---|---|---|---|---|---|---|
| 1 | {1,0} | {5,6} | {2,6} | {7,6} | {7,7} | {2,7} | {5,7} | {1,1} |
| 2 | {1,1} | {5,7} | {2,7} | {7,7} | {7,6} | {2,6} | {5,6} | {1,0} |
| 3 | {2,6} | {2,7} | O | | | | | |
| 4 | {2,7} | {2,6} | O | | | | | |
| 5 | {5,6} | {7,6} | {2,7} | {1,1} | {1,0} | {2,6} | {7,7} | {5,7} |
| 6 | {5,7} | {7,7} | {2,6} | {1,0} | {1,1} | {2,7} | {7,6} | {5,6} |
| 7 | {7,6} | {1,1} | {2,6} | {5,7} | {5,6} | {2,7} | {1,0} | {7,7} |
| 8 | {7,7} | {1,0} | {1,0} | {5,6} | {5,7} | {2,6} | {1,1} | {7,6} |

Оцінка ваги Хемінга ПВП ECPSG I для полів з малим числом елементів показала перебільшення монобітних серій з одиниць, що потенційно викликає загрозу статистичній небезпеці ECPSG I.

Таблиця 4

ПВП отриманих генератором ECPSG I

| № | P | S | L | w(S) |
|---|---|---|---|---|
| 1 | {1,0} | 1010001011011111 | 16 | 10 |
| 2 | {1,1} | 1111011110001010 | 16 | 10 |
| 3 | {2,6} | 0001 | 4 | 1 |
| 4 | {2,7} | 0100 | 4 | 1 |
| 5 | {5,6} | 1010011110001111 | 16 | 10 |
| 6 | {5,7} | 1111001011011010 | 16 | 10 |
| 7 | {7,6} | 1011001110011011 | 16 | 10 |
| 8 | {7,7} | 1110011011001110 | 16 | 10 |

Для тестування реальних ПВП ECPSG 1 були встановлені наступні параметри: крива B-163 зі стандарту FIPS PUB 186-3: $y^2 + y = x^3 + \alpha x + \beta(\mathrm{mod}(x^{163} + x^7 + x^6 + x^3 + 1))$. Коефіцієнти в шістнадцятковій формі: α = 1, β = 20a601907b8c953ca1481eb10512f78744a3205fd, базова точка G з координатами:

$X[G]$ = 3f0eba16286a2d57ea0991168d4994637e8343e36,

$Y[G]$ = 0d51fbc6c71a0094fa2cdd545b11c5c0c797324f1.

Для другого експерименту була обрана крива U-239 зі стандарту ДСТУ 4145-2002: $y^2 + y = x^3 + \alpha x + \beta(\mathrm{mod}(x^{239} + x^{15} + x^2 + x + 1))$, з коефіцієнтами в шістнадцятковій формі: α = 0, β = 1. В якості базової була обрана точка $G$ з координатами:
$X[G]$ = 17039f6aaed44732f28d61eb85196887c8326669bbce15ee01a0b35597fc,
$Y[G]$ = 18e3d24d5736ae66c616392fbe21e0a96b05ff782d78c0f2c0b57977c843.

Використання операції визначення сліду елементів поля Галуа ускладнює процес відтворення послідовності точок кривої на основі послідовності значень $S_0$ та $S_1$. Але це не забезпечує генератору стійкості еквівалентної дискретному логарифмуванню в групі точок еліптичної кривої. Крім цього за результатами статистичних досліджень ECPSG I не пройшов тестування за обома критеріями оцінки статистичної безпеки NIST STS. Проведені дослідження генератору ECPSG I за методикою NIST STS показали неможливість його використання на практиці.

Таким чином, розглянуті приклади побудови генераторів ПВП не відповідають зростаючим вимогам щодо криптографічної стійкості та стійкості до передбачення та відтворення ПВП. В останні роки особливе місце серед генераторів ПВП на основі еліптичних кривих були визнані генератори, на кожній ітерації в яких використовувалась операція скалярного множення точок еліптичної кривої. Такий підхід дав змогу забезпечити криптографічну стій-

кість, стійкість до передбачення або відтворення ПВП еквівалентну дискретному логарифмуванню в групі точок еліптичної кривої. Результатом став генератор на основі подвійного скалярного множення точок еліптичної кривої, який пізніше був визнаний стандартизованим [25]. Розглянемо його структуру та властивості.

**Генератор на еліптичних кривих 3**

Структурні особливості широковідомого генератора DRBG на основі еліптичних кривих Dual_EC_DRBG, детально були розглянуті в роботі [24]. Функціонування генератора Dual_EC_DRBG описується виразом (5):

$$b_i = extr[t_i * Q] = extr[(X_\psi[t_{i-1} * P] \bmod n) * Q], \quad (5)$$

де $P, Q \in E_p$; $t_i = X_\psi = X[P_i]$, $t_0 = HDF(seed, nonce, ID)$.

Нехай $E_{-3,3}(F_{17}) : y^2 = (x^3 + ax + b) \bmod p$ – крива, визначена над скінченим полем $F_p$. $E_p$ – циклічна підгрупа достатньо великого простого порядку *n*. Послідовність внутрішніх станів генератора: $t_1, ..., t_n$ створюється за правилом: $t_i = X_\psi[t_{i-1} * P] \bmod n$, де $t_1 = X_\psi[t_0 * P]$, $t_0 = seed$. Функція *extr* виділяє певне число біт з *X*-координати точки: output_block_length < log($F_p$) – (13+log(cofactor)). Криптографічна стійкість, стійкість до відтворення та передбачення такого генератора вважається еквівалентною складності задачі дискретного логарифмування в групі точок еліптичної кривої. З використанням методики NIST STS проведемо оцінку статистичної безпеки генератора Dual_EC_DRBG.

Результати тестування наведені наступними графічними портретами (рис. 6 – 8).

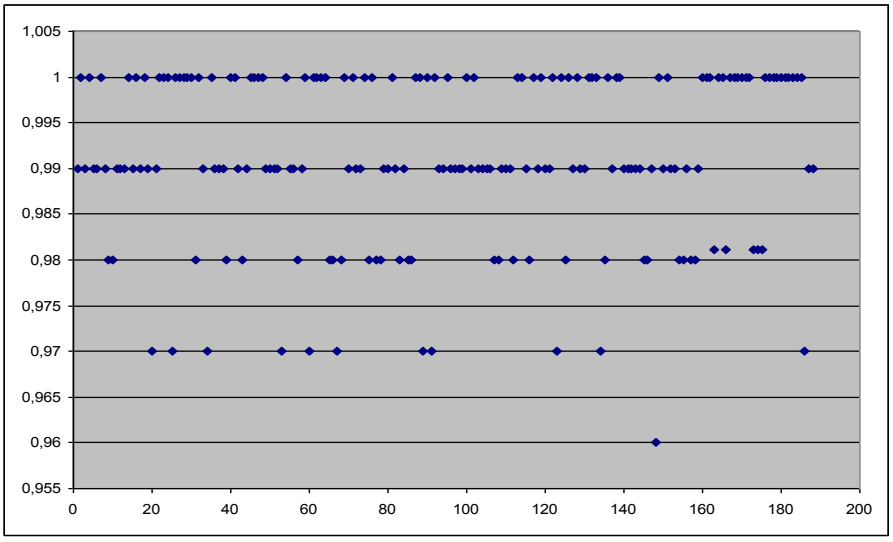


Рис. 6. Результати оцінки статистичної безпеки генератора Dual_EC_DRBG (P-521)

Для створення *seed* в якості значення *entropy* використовувались 80 бітів, які були отримані генератором Dual_EC_DRBG (P-521), для якого *seed* був створений лінійним конгруентним генератором Marsaglia&Zaman random bit generator з бібліотеки MIRACLE. Для проведення експериментів були згенеровані 6 значень *seed*, довжиною 34 байта, кожна з яких була використана для створення *seed* для певного генератору Dual_EC_DRBG згідно вимог [25]. В експериментах були використані стандартизовані криві: P-256 P-384, P-521 з визначеними параметрами.

Отримані псевдовипадкові портрети оцінки властивостей ПВП генераторів Dual_EC_DRBG показали надійність та статистичну безпеку стандартизованих генераторів на основі подвійного скалярного множення точок еліптичної кривої. Але цього недостатньо для доведення криптографічної стійкості запропонованого генератора. В [25] визначена

мінімальна припустима довжина бітового блоку на виході генератора – output_block_length, яка обмежується output_block_length<log($F_p$)-(13+log(cofactor)).

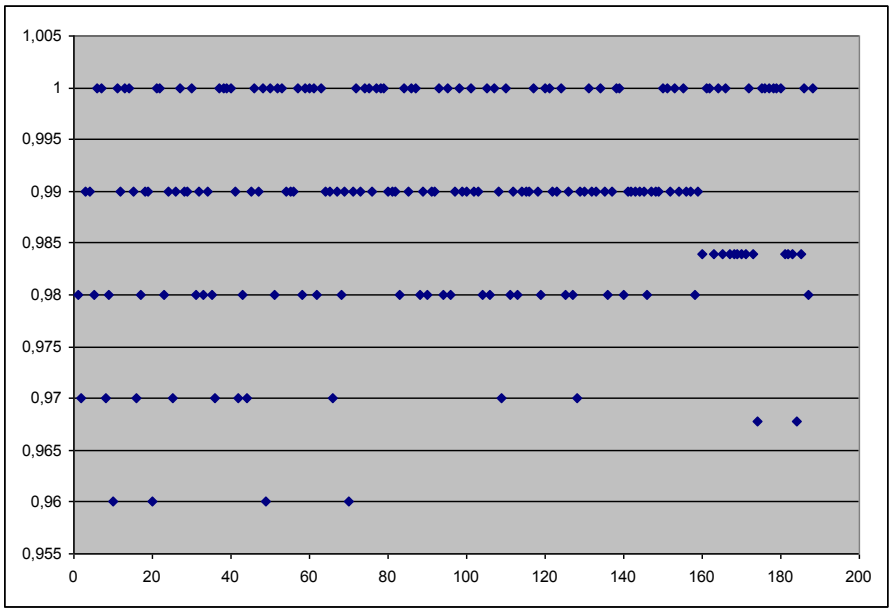


Рис. 7. Результати оцінки статистичної безпеки генератора Dual_EC_DRBG (P-384)

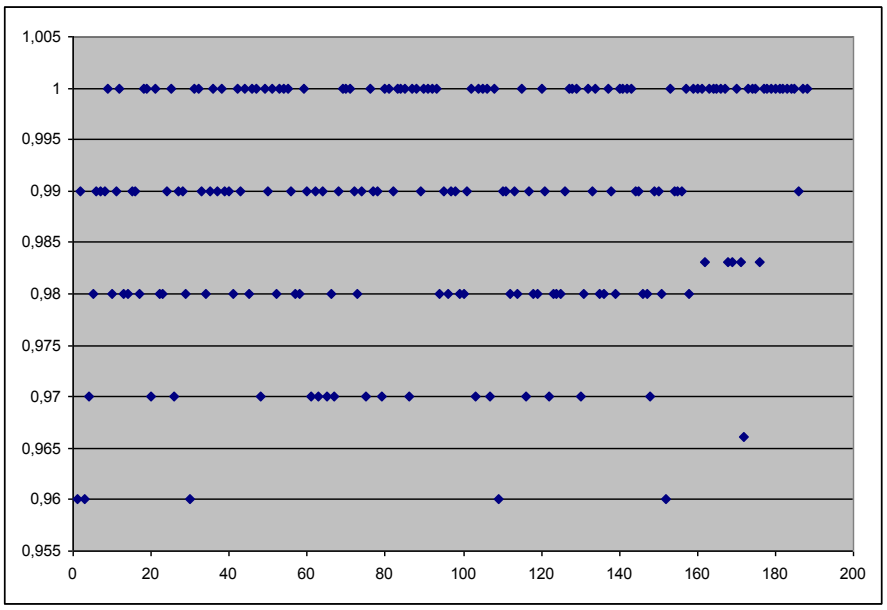


Рис. 8. Результати оцінки статистичної безпеки генератора Dual_EC_DRBG (P-521)

За попередніми результатами аналізу [19] ця границя вважалась достатньою для доведення еквівалентності складності зламу закону генерації ПВП дискретному логарифмуванню на еліптичній кривій. Але в роботах [28 – 29] була висвітлена можливість відтворювати структуру послідовності точок, якщо output_block_length > log($F_p$)/2. Крім цього недоліку, є більш важлива загроза запропонованої в стандарті схеми генерації ПВП – це фіксовані параметри кривої та базові точки кривої, які можуть містити в собі приховану загрозу. Така можливість теоретично існує. Розглянемо її детальніше.

Нехай задана циклічна група точок еліптичної кривої $E_p : y^2 = (x^3 + ax + b) \bmod p$, та генератор цієї групи $P \in E_p$, $n = \#P$. Припустимо, що зловмисник обчислює значення $s*Q = P$, $s < n$ та зберігає у себе $s$. Загальні точки $P$ та $Q$ публікуються для використання під час генерації ПВП. Тоді, якщо зловмисник отримує один з результатів скалярного мно-

ження $R = x*P$, він може відтворити значення внутрішнього стану генератора та обчислювати усі наступні значення внутрішнього стану генератора: $s*R = s*x*P = x*(s*Q) = s*P$, звідки $X[s_i*P] = s_{i+1}$. Це дозволяє стверджувати, що запропонована в стандарті структура генератора не забезпечує стійкість до передбачення, еквівалентну дискретному логарифмуванню.

Для позбавлення цього недоліку необхідно забезпечити виконання наступних вимог:

1) обирати значення output_block_length з урахуванням умови:
   output_block_length < log($F_p$)/2;

2) забезпечити генерацію нових базових точок кривої для кожної реалізації механізму DRBG, а у випадку потреби генерувати криву з новими параметрами (коефіцієнти *a, b, p*);

Альтернативним способом забезпечення є використання додаткових перетворень над групою точок кривої, які ускладнюють процедуру передбачення наступних внутрішніх станів генератора. Прикладом таких операцій можна вважати операції, запропоновані в роботі [24], які дозволяють збільшити період ПВП та як наслідок підвищити стійкість ПВП до передбачення.

**Висновки**

Для проведення досліджень властивостей відомих генераторів ПВП на еліптичних кривих були обрані показники: статистична безпека генераторів, криптографічна стійкість, стійкість до відтворення та передбачення ПВП. Як показали результати досліджень, генератор ПВП, який є статистично безпечним, може мати недоліки в своєї конструкції, які створюють загрози його стійкості. В якості оперативної оцінки стійкості запропонованих генераторів проводиться аналіз його статистичної безпеки, а для повної оцінки стійкості генератора проводяться аналіз криптографічної стійкості, стійкості до передбачення та відтворення ПВП.

Були отримані нові результати оцінки статистичної безпеки лінійних конгруентних генераторів на основі операцій додавання точок еліптичної кривої та їх різновидів, генераторів на основі операції скалярного множення точок кривої, стандартизованих генераторів на основі подвійного скалярного добутку точок еліптичної кривої. Лінійні конгруентні генератори показали недосконаліть своїх конструкцій, а деякі з них також отримали незадовільні оцінки статистичної безпеки. За результатами досліджень були обґрунтовані недоліки існуючих генераторів ПВП, сформовані рекомендації щодо вдосконалення стандартизованого генератора ПВП на еліптичних кривих та подальшого розвитку генераторів цього класу.

Таким чином, проведений аналіз найбільш відомих способів побудови генераторів ПВП на основі еліптичних кривих показав їх недосконаліть, що не дає можливості використовувати такі генератори на практиці. Одним з можливих напрямків подальшого розвитку генераторів на еліптичних кривих було визначено використання додаткових операцій з метою підвищення стійкості генератора до передбачення. Найбільш близькими до таких операцій є ізоморфні трансформації точок еліптичної кривої [24]. Разом з операціями скалярного множення точок кривої це дозволить отримати більш надійні криптографічні генератори ПВП.

**Список літератури:** 1.*Davis D.* Cryptographic Randomness from Air Turbulence in Disk Drives / D. Davis, R. Ihaka, Ph. Fenstermacher // In Proceedings of the 14th Annual International Cryptology Conference on Advances in Cryptology. Springer-Verlag. – 1994. – P. 114 – 120 . 2. *Walker J.* HotBits: Genuine Random Numbers, Generated by Radioactive Decay / J. Walker // 1996. Online: http://www.fourmilab.ch/hotbits/. 3. *Haahr M.* True Random Number Service / M. Haahr // random.org. – 1998. URL: http://random.org/. 4. *Jakobsson M.* A Practical Secure Physical Random Bit Generator / M. Jakobsson, Elizabeth Shriver, Bruce K. Hillyer, A. Juels // Proceedings of the 5th ACM Conference on Computer and Communications Security. ACM Press. – 1998. – P. 103-111. 5. *Geisler M.* About Random Bits / M. Geisler, M.Kroigard, A. Danielsen // Computer Science – 2004. – P. 17. URL: http://daimi.au.dk/~mg/mamian/random-bits.pdf. 6. *Shamir A.* On the generation of cryptographically strong pseudo-random sequences / A. Shamir // 8th International Colloquium on Automata, Languages, and

Programming, Lecture Notes in Computer Science Springer-Verkag, New york, 1981. 7. *Blum M*. How to generate cryptographically strong sequences of pseudo random bits / M. Blum, S. Micali // IEEE 23rd Symposium on the Foundations of Computer Science (1982), P. 112 – 117. 8. *Blum L.* A Simple Unpredictable Pseudo-Random Number Generator / L. Blum, M. Blum,M. Shub // SIAM Journal on Computing, 15(2). – 1986. – P. 364–383. 9. *Impagliazzo R.* One-way functions are essential for complexity based cryptography / R. Impagliazzo, M. Luby // Proc. 30th Annu. Symp. On Found. of Comput. Sci. 1989. P. 230 – 235. 10. *Impagliazzo R.* Pseudo-random generation from one-way functions / R. Impagliazzo , L. Levin, M. Luby // Proc. 21st Annu. ACM Symp. on Theory of Computing. 1989. P. 12 – 24. 11. *Burton S.* One-Way Permutations on Elliptic Curves / S. Burton, Jr. Kaliski // Journal of Cryptology (1991) International Association for Cryptologic Research. 1991. – P.187 – 199. 12. *Hallgren S.* Linear congruential generators over elliptic curves, Tech. Report CS-94-143, Carnegie Mellon Univ., 1994. 13. *Gong G*. Elliptic curve pseudorandom sequence generators / G. Gong, T. A. Berson, D. R. Stinson // Selected Areas in Cryptography (Kingston, ON, 1999), Springer, 2000, 34 – 48. 14. *Shparlinski I.* On the Naor-Reingold pseudo-random function from elliptic curves / *Shparlinski I. E.* // Applicable Algebra in Engineering, Communication and Computing 11 (2000), pp. 27 – 34. 15. *Beelen P.* Pseudorandom sequences from elliptic curves / Beelen P., Doumen J. // Finite Fields with Applications to Coding Theory, Cryptography and Related Areas, Springer-Verlag, Berlin, 2002, 37 – 52. 16. *Gong G.* Linear recursive sequences over elliptic curves / *Gong G.*, C. C. Y. Lam // Sequences and their Applications (Bergen, 2001), Springer, 2002. 182–196. 17. *El Mahassni E.* On the uniformity of distribution of congruential generators over elliptic curves / *E. El Mahassni, I. E. Shparlinski //* In Proc. Intern. Conf. on Sequences and Their Applications, Bergen 2001, Springer-Verlag, London, (2002) pp. 257–264. 18. *Hess F.* On the linear complexity and multidimensional distribution of congruential generators over elliptic curves / F. Hess, I. E. Shparlinski // Des. Codes Cryptogr. 35 (2005), 1, 111–117. 19. *Gjøsteen K*. Comments on Dual-EC-DRBG/NIST SP 800-90, Draft December 2005 / K. Gjøsteen // March 16. – 2006. 20. *Lange T.* Distribution of some sequences of points on elliptic curves / T. Lange, I. E. Shparlinski // J. Math. Cryptol. 1 (2007), 1–11. 21. *Liu H.* Large families of elliptic curve pseudorandom binary sequences / H. Liu, T. Zhan, X. Wang, // Acta Arith. 140 (2009), 135–144. 22. *Shparlinski I. E.* Pseudorandom number generators from elliptic curves. Recent trends in cryptography, 121–141, Contemp. Math., 477, Amer. Math. Soc., Providence, RI, 2009. 23. *Горбенко І.* Метод побудування випадкових бітів на основі спарювання точок еліптичних кривих / Горбенко І. Д., Шапочка Н. В., Погребняк К. А. // Прикладная радиоэлектроника. – 2010. – № 3. – 2010. -С. 386 – 394. 24. *Бессалов А*. Метод генерации псевдослучайных последовательностей на основе изоморфных трансформаций эллиптической кривой / Бессалов А. В., Чевардин В. Е. // Прикладная радиоэлектроника. – 2012. – Т. 11. № 2. – С. 234 – 237. 25. *NIST* Special Publication 800-90A. Recommendation for Random Number Generation Using Deterministic Random Bit Generators. Computer Security Division Information Technology Laboratory National Institute of Standards and Technology. – January 2012. 26. ANSI X 9.17 (Revised), \American National Standard for Financial Institution Key Management (Wholesale)," American Bankers Association, 1985. 27. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications / National Institute of Standards and Technology. – 2010. http://csrc.nist.gov/groups/ST/toolkit/rng/documents/SP800-22rev1a.pdf. 28. *Schoenmakers B.* Cryptanalysis of the Dual Elliptic Curve Pseudorandom sequences from elliptic curves / Schoenmakers B., Sidorenko A. // 2006. URL: cr.yp.to/newelliptic/edwards2-20080611.pdf. 29. *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. 30. *Plumstead* (Boyarj, J.B., Inferring a Sequence Generated by a Linear Congruence, Proc. of the 23rd IEEE Symp. on Foundations ofComputer Science, 1982, pp. 153-159. 31. *Yao, A.* Theory and applications of trapdoor function. In Proc. 23rd IEEE Symposium on Foudations of Computer Science, pp. 80-91. 32. *Hugo Krawczyk*. How to predict congruential generators / TECHNION – Israel Institute of Technology Computer Science Department. December 1988. P. 1 – 15.

| НТУУ КПІ | *Надійшла до редколегії 14.03.2014* |
|---|---|