УДК 681.324.067

Т.О. Гріненко[1], Ю.І. Горбенко[2], Р.І. Мордвінов[1]

[1]*Харківський національний університет радіоелектроніки, Харків*
[2]*ЗАТ «Інститут інформаційних технологій», Харків*

ВЛАСТИВОСТІ ТА ПЕРСПЕКТИВИ ЗАСТОСУВАННЯ ГЕНЕРАТОРІВ ПСЕВДОВИПАДКОВИХ ПОСЛІДОВНОСТЕЙ НА ЕЛІПТИЧНИХ КРИВИХ

Розглядається удосконалений метод генерування псевдовипадкових бітів, що базується на гешуванні точок еліптичних кривих. Наводяться результати аналізу властивостей необоротності та нерозрізнюваності.

Ключові слова: *псевдовипадкова послідовність, псевдовипадкові біти, генератор псевдовипадкових послідовностей, еліптична крива, необоротність, нерозрізнюваність.*

Вступ

Серед стандартів, що визначають методи та засоби генерування псевдовипадкових бітів (ПВБ) значні перспективи має міжнародний стандарт ISO/IEC 18031 «Інформаційні технології – Методи захисту – Генерація випадкових бітів», який містить вимоги щодо генерування псевдовипадкових послідовностей. Разом з тим уже сьогодні стоять завдання дослідження та удосконалення такого виду генераторів ПВБ по критеріям криптографічної стійкості та швидкодії. Так аналіз існуючих публікацій та міжнародних рекомендацій NIST SP 800-90 [1] і міжнародного стандарту ISO/IEC 18031 [2] показали, що вони мають ряд недоліків. Крім того, в AIS 20 [3] коректно і однозначно сформовані вимоги в частині класів стійкості або гарантій К1, К2, К3, К4, що повинні бути виконані.

В [2] стандартизовано метод генерування ПВБ і реалізації відповідного детермінованого генератора випадкових бітів (ДГВБ), що ґрунтуються на застосуванні перетворень в групі точок супернесингулярних ЕК. Першою роботою, яка присвячена розробці ДГВБ на ЕК і була нам доступна, є проект стандарту США ANSI X9.82-3 [4], що опублікований в 2004 р. Перша наша публікація, у якій запропоновано метод побудування ДГВБ на ЕК зроблена у 2001 році [5], практична програмна реалізація генератора та результати досліджень властивостей таких генераторів, була опублікована в 2002 році [6], детально загальні результати доповідалась на 5 міжнародній науково-практичній конференції «Безпека інформації в інформаційно-телекомунікаційних системах», що проводилася в Києві 20-24 травня 2002 р. [7, стор. 47-48]. Порівняльний аналіз методів, що запропоновані в стандартах ANSI X9.82-3 [4, 8], ISO/IEC 18031 [2] та наших пропозицій [5 – 7] дозволяє зробити висновок про їх суттєве співпадання, і як наслідок, наш пріоритет відносно методу генерування ПВБ на еліптичних кривих.

Метою статі є удосконалення методу і алгоритмів побудови ДГВБ на основі використання криптографічних перетворень в групі точок ЕК над простими і розширеннями полів Галуа та застосування стійких до колізій функцій гешування, використання якого дозволить формувати ПВБ з необхідними властивостями нерозрізнюваності та необоротності [3].

1. Загальна характеристика та вимоги до ДГВБ

Одним з основних елементів криптографічних систем, від характеристик якого суттєво залежить її стійкість, є засіб генерації ключів. При цьому, від якості генераторів випадкових та псевдовипадкових чисел, що використовуються, прямо залежить якість одержуваних результатів.

Детермінованим генератором випадкових послідовностей (ДГВП) називають детермінований алгоритм, сукупність алгоритмів чи сукупність алгоритмів та засобів, які для заданої послідовності довжиною k формують при своїй роботі послідовність Y_i символів довжиною $l >> k$, яка володіє більшістю властивостей випадкової послідовності. Дані генератори в деяких джерелах називаються детермінованими генераторами випадкових чисел (ДГВЧ).

ДГВП використовує алгоритм, що виробляє послідовність бітів з початкового значення, обумовленого початковим числом. ДГВП вважається реалізованим, коли отримано початкове число і визначене початкове значення. У зв'язку з детермінованим характером процесу вважається, що ДГВП виробляє псевдовипадкові, а не випадкові біти. Початкове число, яке використовується для реалізації ДГВП, повинно містити достатню ентропію для гарантії випадковості.

Проведені дослідження підтвердили, що до ДГВБ повинні пред'являтись та виконуватись вимо-

© Т.О. Гріненко, Ю.І. Горбенко, Р.І. Мордвінов

ги до джерела ентропії та додаткових вхідних даних, до внутрішнього стану, до функцій переходу внутрішнього стану та генерації вихідних даних, а також до функції підтримки та до ключів [2].

2. Метод формування ПВБ в групі точок еліптичних кривих

Розглянемо метод генерування ПВБ в групі точок еліптичних кривих. В [5 – 7] був викладений метод формування ПВБ з використанням криптографічних перетворень в групі точок еліптичних кривих. Там же були приведені основні результати досліджень деяких варіантів практичної реалізації генераторів ПВБ в групі точок еліптичних кривих.

Розглянемо постановку задачі [5 – 7].

Нехай дані певні еліптичні криві в афінних координатах E_A

$$y^2 + xy = x^3 + ax + b\left(\mathrm{mod}\, f(x), 2\right) \qquad (1)$$

та в проективних координатах і E_P

$$Y^2 + XYZ = X^3 + aX^2Z^2 + bZ^6\left(\mathrm{mod}\, f(x), 2\right). \qquad (2)$$

Для афінного подання базова точка G з координатами $(x, y) \in E_A$ або $(X, Y, Z) \in E_P$. Розглянемо два методи побудови ПВБ:

$$Q_i = Q_{i-1} + G, \text{ де } Q_i, Q_{i-1} \in E; \qquad (3)$$

$$Q_i = a \times Q_{i-1}, \text{ де } Q_i, Q_{i-1} \in E. \qquad (4)$$

В (3) в якості ключа будемо вважати або значення Q_{i-1} або d_0, прийнявши що

$$Q_0 = d_0 \cdot G, \qquad (5)$$

де d_0 – секретний (особистий) ключ генератора. Таким чином, по суті вирази (3) та (4) задають способи рекурентного генерування ПВБ.

У випадку (3) ми одержуємо послідовність значень Q_i шляхом багаторазового підсумовування точки Q_{i-1} й базової точки G, причому Q_0 задається згідно (5) через секретний ключ генератора.

У випадку (4) отримуємо Q_i шляхом скалярного множення точки Q_{i-1} на число a, причому a залежить від секретного ключа d_0. У цьому випадку виникає питання вибору a, воно може бути секретним ключем генератора, або генеруватись певним чином, наприклад як у нашому випадку $a = \pi(Q_{i-1})$, де π – функція перетворення точки в число [2]. В цьому випадку ми одержуємо

$$Q_i = \pi(Q_{i-1}) \times Q_{i-1}. \qquad (6)$$

Для обох методів побудову ПВБ можна виконати декількома способами на основі вхідних значень Num. Основними з них, на наш погляд, що вимагають досліджень є такі:

$$\mathrm{Num}(Q_i) = X_i \| Y_i \| Z_i, \text{ якщо } Q_i(X_i, Y_i, Z_i) \in E_p; \qquad (7)$$

$$\mathrm{Num}(Q_i) = X_i \| Y_i, \text{ якщо } Q_i(X_i, Y_i, Z_i) \in E_p; \qquad (8)$$

$$\mathrm{Num}(Q_i) = X_i, \text{ якщо } Q_i(X_i, Y_i, Z_i) \in E_p; \qquad (9)$$

$$\mathrm{Num}(Q_i) = x_i \| y_i, \text{ якщо } Q_i(x_i, y_i) \in E_A; \qquad (10)$$

$$\mathrm{Num}(Q_i) = x_i, \text{ якщо } Q_i(x_i, y_i) \in E_A. \qquad (11)$$

У виразах (7) – (11) знак $\|$ – конкатенація значень координат точок ЕК, а $\mathrm{Num}(Q_i)$ – позначення способу формування ПВБ.

Враховуючи (3) і (4), а також п'ять способів формування чисел (7) – (11) проведені дослідження таких алгоритмів формування ПВБ:

$$Q_i = Q_{i-1} + G,\ \mathrm{Num}(Q_i) = X_i \| Y_i \| Z_i, \text{ якщо } Q_i(X_i, Y_i, Z_i) \in E_p; \qquad (12)$$

$$Q_i = Q_{i-1} + G,\ \mathrm{Num}(Q_i) = X_i \| Y_i, \text{ якщо } Q_i(X_i, Y_i, Z_i) \in E_p; \qquad (13)$$

$$Q_i = Q_{i-1} + G,\ \mathrm{Num}(Q_i) = X_i, \text{ якщо } Q_i(X_i, Y_i, Z_i) \in E_p; \qquad (14)$$

$$Q_i = Q_{i-1} + G,\ \mathrm{Num}(Q_i) = x_i \| y_i, \text{ якщо } Q_i(x_i, y_i) \in E_A; \qquad (15)$$

$$Q_i = Q_{i-1} + G,\ \mathrm{Num}(Q_i) = x_i, \text{ якщо } Q_i(x_i, y_i) \in E_A; \qquad (16)$$

$$Q_i = \pi(Q_{i-1}) \times Q_{i-1},\ \mathrm{Num}(Q_i) = X_i \| Y_i \| Z_i, \text{ якщо } Q_i(X_i, Y_i, Z_i) \in E_p; \qquad (17)$$

$$Q_i = \pi(Q_{i-1}) \times Q_{i-1},\ \mathrm{Num}(Q_i) = X_i \| Y_i, \text{ якщо } Q_i(X_i, Y_i, Z_i) \in E_p; \qquad (18)$$

$$Q_i = \pi(Q_{i-1}) \times Q_{i-1},\ \mathrm{Num}(Q_i) = X_i, \text{ якщо } Q_i(X_i, Y_i, Z_i) \in E_p; \qquad (19)$$

$$Q_i = \pi(Q_{i-1}) \times Q_{i-1},\ \mathrm{Num}(Q_i) = x_i \| y_i, \text{ якщо }; Q_i(x_i, y_i) \in E_A; \qquad (20)$$

$$Q_i = \pi(Q_{i-1}) \times Q_{i-1},\ \mathrm{Num}(Q_i) = x_i, \text{ якщо } Q_i(x_i, y_i) \in E_A. \qquad (21)$$

Для забезпечення стійкості було запропоновано удосконалити способи генерування ПВБ засобом застосування гешування координат точок еліптичних кривих, тобто значень $\mathrm{Num}(Q_i)$. У загальному випадку отримаємо геш-значення

$$h_i = H\left(\mathrm{Num}(Q_i)\right). \qquad (22)$$

Враховуючи (22) були проведені дослідження таких алгоритмів формування ПВБ:

$$Q_i = Q_{i-1} + G,\ \mathrm{Num}(Q_i) = H\left(X_i \| Y_i \| Z_i\right), \text{ якщо } Q_i(X_i, Y_i, Z_i) \in E_p; \qquad (23)$$

$$Q_i = Q_{i-1} + G,\ \mathrm{Num}(Q_i) = H\left(X_i \| Y_i\right), \text{ якщо } Q_i(X_i, Y_i, Z_i) \in E_p; \qquad (24)$$

$$Q_i = Q_{i-1} + G,\ \mathrm{Num}(Q_i) = H(X_i),$$
якщо $Q_i(X_i, Y_i, Z_i) \in E_p$; (25)

$$Q_i = Q_{i-1} + G,\ \mathrm{Num}(Q_i) = H(x_i \| y_i),$$
якщо $Q_i(x_i, y_i) \in E_A$; (26)

$$Q_i = Q_{i-1} + G,\ \mathrm{Num}(Q_i) = H(x_i),$$
якщо $Q_i(x_i, y_i) \in E_A$; (27)

$$Q_i = \pi(Q_{i-1}) \times Q_{i-1},\ \mathrm{Num}(Q_i) = H(X_i \| Y_i \| Z_i),$$
якщо $Q_i(X_i, Y_i, Z_i) \in E_p$; (28)

$$Q_i = \pi(Q_{i-1}) \times Q_{i-1},\ \mathrm{Num}(Q_i) = H(X_i \| Y_i),$$
якщо $Q_i(X_i, Y_i, Z_i) \in E_p$; (29)

$$Q_i = \pi(Q_{i-1}) \times Q_{i-1},\ \mathrm{Num}(Q_i) = H(X_i),$$
якщо $Q_i(X_i, Y_i, Z_i) \in E_p$; (30)

$$Q_i = \pi(Q_{i-1}) \times Q_{i-1},\ \mathrm{Num}(Q_i) = H(x_i \| y_i),$$
якщо $Q_i(x_i, y_i) \in E_A$; (31)

$$Q_i = \pi(Q_{i-1}) \times Q_{i-1},\ \mathrm{Num}(Q_i) = H(x_i),$$
якщо $Q_i(x_i, y_i) \in E_A$. (32)

У загальному випадку алгоритм генерування ПВБ в групі точок еліптичної кривої будемо подавати у вигляді

$$Q_i = d_0 \cdot G, \quad (33)$$

де d_0 – секретний (особистий) ключ генератора; G – базова точка, а Q_i – вихідне значення, із якого формується ПВБ. Будемо вважати, що базова точка G та вихідне значення Q_i криптоаналітику відомі. В даному випадку задача криптоаналізу зводиться до знаходження секретного (особистого) ключа d_0.

Структурні схеми алгоритмів, що реалізують наведені вище методи генерування ПВБ, у найбільш узагальненому випадку наведені на рис. 1, 2.

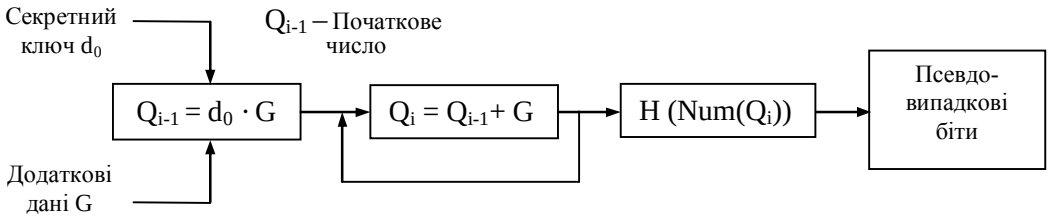

Рис. 1. Алгоритм генерування ПВБ в групі точок еліптичних кривих згідно методу (3)

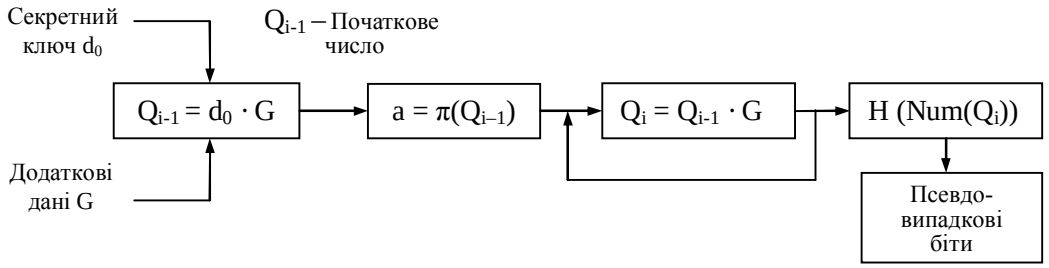

Рис.2. Алгоритм генерування ПВБ в групі точок еліптичних кривих згідно методу (4)

3. Дослідження властивостей необоротності

Нижче наводяться результати дослідження властивостей необоротності, непередбачуваності та нерозрізнюваності для методів, що у загальному випадку наведені на рис. 1, 2 та способів, що задані виразами (7) – (11) та (22).

У випадку застосування правил (22) задача оцінки необоротності генератора у цілому по суті зводиться до послідовного вирішення двох задач – спочатку знаходження по відомому виходу генератора (геш-значення) його прообразу, а потім по відомому прообразу – до вирішення задачі дискретного логарифмування в групі точок еліптичної кривої з визначенням секретного ключа генератора.

Для випадку (7) – (11) необхідно вирішити тільки задачу дискретного логарифмування в групі точок еліптичної кривої з метою визначення секретного ключа генератора.

Для вирішенні задачі знаходження прообразу s по відомому образу r треба виконати

$$I_{пр} = 2^{l_h} - 1 \quad (34)$$

групових операцій, а для створення колізії необхідно виконати

$$I_к = 2^{l_h/2} \quad (35)$$

групових операцій [8].

Дискретне логарифмування в групі точок еліптичних кривих зводиться до знаходження секретного (особистого) ключа d_0 при відомих значеннях точок еліптичних кривих Q_i та G для випадку (33).

Аналіз джерел показав, що вказана задача може бути вирішеною різними методами, але перевагу мають методи Полларда [8].

Так для ρ-Полларда методу параметри I_ρ – складність, порядок точки n та ймовірність здійснення колізії P_k зв'язані між собою таким чином

$$I_\rho^2 - I_\rho + 2n\ln(1-P_k) = 0, \qquad (36)$$

де $n = 2^m$ – порядок базової точки. Формулу (36) можна спростити, враховуючи те, що в реальних ситуаціях $I_\rho^2 >> I_\rho$. За цієї умови (36) має вигляд

$$I_\rho = \sqrt{-2n\ln(1-P_k)} = \sqrt{-2^{m+1}\ln(1-P_k)}. \qquad (37)$$

Аналогічно для λ-Полларда методу [8] за умови, що $I_\lambda^2 >> 1$

$$I_\lambda = \sqrt{-n\ln(1-P_k)}. \qquad (38)$$

В табл. 1 – 3 наведені результати оцінки складності обернення генератора на еліптичних кривих, табл. 1 – для випадку коли використовується тільки скалярне множення, табл. 2 – для випадку застосування тільки гешування, табл. 3 – для випадку застосування як гешування так і скалярного множення, причому складність криптоаналізу визначається як

$$I_з = \left(2^{l_h} - 1\right)\sqrt{-2n\ln(1-P_k)} = \left(2^{l_h} - 1\right)\sqrt{-2^{m+1}\ln(1-P_k)}. \qquad (39)$$

Складність обернення генератора на еліптичних кривих при виконанні тільки скалярного множення, не залежно від ймовірності виникнення колізії, носить експоненційний характер ($P_k = 0,5$, $P_k = 0,99$).

Таблиця 1

Складність обернення генератора для скалярного множення (P_k = 0,99)

Метод \ n	2^{163}	2^{256}	2^{384}	2^{512}
I_ρ	$1,03\cdot10^{25}$	$1,03\cdot10^{39}$	$1,9\cdot10^{58}$	$3,51\cdot10^{77}$
I_λ	$7,33\cdot10^{24}$	$7,3\cdot10^{38}$	$1,34\cdot10^{58}$	$2,48\cdot10^{77}$

Таблиця 2

Складність обернення генератора при гешуванні

Метод \ n	2^{163}	2^{256}	2^{384}	2^{512}
$I_{пр}$	$1,17\cdot10^{49}$	$1,16\cdot10^{77}$	$3,94\cdot10^{115}$	$1,34\cdot10^{154}$
$I_к$	$3,42\cdot10^{24}$	$3,40\cdot10^{38}$	$6,28\cdot10^{57}$	$1,16\cdot10^{77}$

Таблиця 3

Складність обернення при скалярному множенні та гешуванні (P_k = 0,99)

l_h \ n	2^{163}	2^{256}	2^{384}	2^{512}
160	$1,52\cdot10^{73}$	$1,51\cdot10^{87}$	$2,78\cdot10^{106}$	$5,14\cdot10^{125}$
256	$1,20\cdot10^{102}$	$1,19\cdot10^{116}$	$2,21\cdot10^{135}$	$4,07\cdot10^{154}$
384	$4,09\cdot10^{140}$	$4,07\cdot10^{154}$	$7,51\cdot10^{173}$	$1,38\cdot10^{193}$
512	$1,39\cdot10^{179}$	$1,38\cdot10^{193}$	$2,55\cdot10^{212}$	$4,71\cdot10^{231}$

4. Експериментальні дослідження властивостей нерозрізнюваності та швидкодії

Для тестування генератора ПВЧ на еліптичних кривих на нерозрізнюваність використовувалася методика NIST STS [9]. Було здійснене тестування 20 ПВБ (алгоритми (12) – (21)), а також проведене порівняння властивостей цих ПВБ із властивостями ПВБ генератора псевдовипадкових чисел BBS [6] (тестова вибірка, рекомендована NIST).

Для здійснення тестування були обрані такі параметри: довжина послідовності, що підлягає тестуванню, $n = 10^6$ біт; кількість послідовностей $m = 100$; об'єм вибірки 10^8 біт; рівень значимості $\alpha = 0,01$; число тестів $q = 189$. У табл. 4 наводяться дані по проходженню ПВБ тестів для певних способів [6].

Таблиця 4

Результати тестування ДГВБ на нерозрізнюваність

Генератор	Кількість тестів, у яких тестування пройшли більше 99% послідовностей	Кількість тестів, у яких тестування пройшли більше 96% послідовностей
BBS	**134 (70,8%)**	**189 (100%)**
(12)	119 (63%)	175 (92,6%)
(13)	126 (66,7%)	171 (90,5%)
(15)	128 (67,7%)	181 (95,8%)
(16)	137 (72,5%)	187 (98,9%)
(20)	118 (62,4%)	180 (95,2%)
(21)	123 (65,1%)	187 (98,9%)
(23)	139 (73,5%)	187 (98,9%)
(24)	141 (74,6%)	188 (99,5%)
(25)	**138 (73%)**	**189 (100%)**
(26)	**134 (70,9%)**	**189 (100%)**
(27)	124 (65,6%)	187 (98,9%)
(28)	126 (66,7%)	188 (99,5%)
(29)	146 (77,2%)	188 (99,5%)
(30)	**131 (69,3%)**	**189 (100%)**
(31)	121 (64%)	187 (98,9%)
(32)	127 (67,2%)	188 (99,5%)

Генератори (25), (26), (30) пройшли всі тести. Генератор BBS пройшов всі тести. Якщо застосовувати жорсткий критерій, тобто коли може бути відкинута лише одна послідовність зі ста, то кращий результат показав генератор (25), він має кращі характеристики, чим BBS. Генератор (26) має таку ж статистику, як і BBS.

У табл. 5 наведені результати експериментальної оцінки швидкості формування ПВБ для різних алгоритмів. Результати статистичного тестування запропонованих алгоритмів з використанням методики NIST SP 800-22 показали, що кращими за вимогою нерозрізнюваності є генератори (25), (26) і (30).

Таблиця 5

Результати експериментальної оцінки швидкодії генераторів

Генератор	Кількість отриманих бітів за секунду
(12)	57 600 000
(13)	38 400 000
(23)	12 800 000
(24)	12 800 000
(25)	12 800 000
(26)	63 366
(30)	6 835

Висновки

Складність (швидкість) функціонування ДГВЧ залежить від обраного методу й способу формування ПВБ. Мінімальна складність досягається для методу (3) і способу формування ПВБ (1). У цьому випадку за один крок ГПВБ формується псевдовипадкове число трикратної довжини.

У випадку застосування правила (22) задача оцінки необоротності генератора у цілому по суті зводиться до послідовного вирішення двох задач – знаходження про відомому виходу генератора (гешзначення) його прообразу, а потім по відомому прообразу вирішення задачі дискретного логарифмування в групі точок еліптичної кривої з визначенням секретного ключа генератора.

Генератор ПВБ, що ґрунтується на використанні, як скалярного множення на еліптичній кривій, так і гешування, має складність обернення більшу ніж атака груба сила (див. табл. 1 – 4). Це означає що для цього методу атака типу груба сила є найбільш ефективною з точки зору крипто аналітика.

Генератори (25), (26), (30) пройшли всі тести. Генератор BBS також пройшов всі тести, але кращий результат показав генератор (25).

Список літератури

1. NIST SP 800-90. Recommendation for Random Number Generation Using Deterministic Random Bit Generators, June 2006.

2. ISO/IEC 18031 Information technology – Security techniques – Random bit generation. 2005.

3. Application Notes and Interpretation of the Scheme (AIS) 20. Functionality classes and evaluation methodology for Deterministic random number generators, 1999.

4. ANSI X9.82, Part 3 – Draft – July 2004. Random Number Generation, Part 3: Deterministic Random Bit Generators.

5. Гриненко Т.А. Метод формирования и свойства ПВП на эллиптических кривых / Т.А. Гриненко, Ю.И. Горбенко, С.Ю. Орлова // Радиотехника: всеукр. межвед. научно-техн. сб. – 2001. – Вып. 119. – С. 119-123.

6. Гриненко Т.А. Методы формирования псевдослучайных последовательностей в группах точек ЭК. / Т.А. Гриненко, С.И. Збитнев, Д.В. Мялковский. // Радиотехника: всеукр. межвед. науч.-техн. сб. – 2002. – Вып. 126. – С. 115-122.

7. Гриненко Т.А. Методы построения генераторов псевдослучайных чисел в группах точек эллитических кривых и их свойства / Т.А. Гриненко, С.И. Збитнев. // Безпека інформації в інформаційно-телекомунікаційних системах: П'ята Міжнародна науково-практична конференція, 20-24 травня 2002 р. – К., 2002. – С. 47-48.

8. ANSI/X9 X9.82-3:2007. Random Number Generation, Part 3: Deterministic Random Bit Generators. Accredited Standards Committee X9 Incorporated / 11-Sep-2007 / 113 p.

9. Горбенко Ю.І. Інфраструктури відкритих ключів . Системи ЕЦП. Теорія та практика / Ю.І. Горбенко, І.Д. Горбенко. – Х.: Форт, 2010. – 593 с.

10. NIST SP 800-22. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications. April 2000 [Електронний ресурс]. – Режим доступу до ресурсу: http://csrc.nist.gov/publications/nistpubs//SP800-22rev1a.pdf.

Надійшла до редколегії 7.02.2011

Рецензент: канд. техн. наук, доцент О.А. Замула, Харківський національний університет радіоелектроніки, Харків.

СВОЙСТВА И ПЕРСПЕКТИВЫ ПРИМЕНЕНИЯ ГЕНЕРАТОРОВ ПСЕВДОСЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ НА ЭЛЛИПТИЧЕСКИХ КРИВЫХ

Т.А. Гриненко, Ю.И. Горбенко, Р.И. Мордвинов

Рассматривается усовершенствованный метод генерации псевдослучайных бит, основанный на хешировании точек эллиптических кривых. Приводятся результаты анализа свойств необратимости и неразличимости.

Ключевые слова: *псевдослучайная последовательность, псевдослучайные биты, генератор псевдослучайных последовательностей, эллиптическая кривая, необратимость, неразличимость.*

PROPERTIES AND APPLICATION PROSPECTS OF PSEUDO-RANDOM SEQUENCES GENERATORS ON ELLIPTIC CURVES

T.O. Grinenko, Yu.I. Gorbenko, R.I. Mordvinov

It is considered an improved method for pseudorandom bits generation based on the hashing of points on elliptic curves. There are given analysis results of irreversibility and indistinguishability properties.

Keywords: *pseudo-random sequence, pseudo-random bats, generator of pseudo-random sequences, elliptic curve, irreversibility, indistinguishableness.*