УДК 681.324.067

МЕТОД ПОБУДУВАННЯ ВИПАДКОВИХ БІТІВ НА ОСНОВІ СПАРЮВАННЯ ТОЧОК ЕЛІПТИЧНИХ КРИВИХ

І.Д. ГОРБЕНКО, Н.В. ШАПОЧКА, К.А. ПОГРЕБНЯК

Наводиться обґрунтування та викладається сутність і властивості генератора детермінованих випадкових бітів на основі криптографічного перетворення типу спарювання точок еліптичних кривих.

Ключові слова: еліптичні криві, детерміновані випадкові послідовності.

ВСТУП

Нині актуальною є задача криптографічного захисту інформації в різноманітних інформаційних технологіях та інформаційно – телекомунікаційних системах. Суттєво важливими складовими таких систем, від властивостей яких залежить якість надання криптографічних послуг, є засоби генерування ключів та параметрів. Існуючі методи та на їх основі засоби генерування ключів та параметрів можна розділити на два великих класи – випадкових та детермінованих випадкових послідовностей (бітів). Обидва вказані класи генераторів знаходять застосування, але більш широко використовують детерміновані генератори випадкових бітів (ДГВБ) [1], по крайній мірі в частині інтенсивності їх використання.

Також згідно рекомендацій [2] ДГВБ можна розділити на три великих групи:

– ДГВБ на основі перетворень в групі точок еліптичних кривих;

– ДГВБ на основі перетворень з використанням геш – функцій;

– ДГВБ на основі використання блокових шифрів.

Для оцінки властивостей ДГВБ рекомендується використовувати такі показниками, як [3]: період l повторення (довжина) детермінованої випадкової послідовності; основа алфавіту m ДГВБ; ймовірність перекриття в просторі або в часі двох сегментів Y_r та Y_μ; структурна скритність (еквівалентна складність) S_e ДГВБ Y; ентропія $H_k(N_k)$ джерела ключів для випадку, коли генератор детермінованих випадкових послідовностей використовується як джерело ключів; відстань рівнозначності l_0 конкретної послідовності Y_v; безпечний час генератора детермінованих випадкових послідовностей t_b; складність I_y формування послідовності Y; довжина параметрів зворотного зв'язку B_2 та властивості випадковості, рівноймовірності, незалежності та однорідності.

За всіма названими показниками до детермінованого генератора випадкових бітів повинен бути пред'явлений ряд вимог [4]. Так, період повторення повинен бути $l_n \geq l_z$, тобто не менше заданого, основа алфавіту m, ймовірність перекриття $P_n < P_z$ менше допустимої, структурна скритність $S \geq S_g$, ентропія джерела ключів $H \geq H_g$, відстань рівнозначності $l_0 > l_g$, безпечний час $t_b > t_g$, тобто не менш допустимих. Крім того, реалізація Y_i повинна задовольняти вимогам випадковості, рівноймовірності, незалежності та однозначності, а також забезпечувати генерування бітів з необхідною швидкодією.

Проведений аналіз показав, що ДГВБ, які засновані на геш – функціях, мають ряд переваг [4]. Так ДГВБ можуть використовувати будь-яку ISO/IEC криптографічну геш – функцію із ISO/IEC 10118-3 за умови забезпечення достатньої ентропії для початкового значення. Але для таких генераторів необхідно генерувати, в тому числі згідно ключа, символи прообразів з довільним алфавітом послідовності прообразу, завідомо заданим періодом повторення l, допустимою швидкодією (складністю) генерування символів та криптографічною стійкістю проти визначення закону генерування ДГВБ.

Метою цієї статті є обґрунтування можливості, визначення умов побудування, дослідження різних варіантів побудування та розробка рекомендацій відносно застосування ДГВБ, у якого символи прообрази генеруються на основі спарювання точок еліптичних кривих у вигляді елементів підгрупи розширення поля, а безпосередньо символи образи на основі обчислення геш – значень від символів прообразів.

1. МЕТОД ГЕНЕРАЦІЇ ВИПАДКОВИХ БІТІВ НА ОСНОВІ СПАРЮВАННЯ ТОЧОК ЕЛІПТИЧНИХ КРИВИХ

Ідея побудування ДГВБ базується на основній властивості скалярного відображення – його білінійності або властивості спарювання [5]. Вона полягає в тому, що для деяких точок еліптичної кривої B і D над полем F_g, а також цілих a та c є справедливим таке:

$$K = Спарювання(a \bullet B, c \bullet D) = \\ = Спарювання(c \bullet B, a \bullet D). \quad (1)$$

В результаті спарювання точок B та D отримуємо елемент мультиплікативної підгрупи розширення поля F_{q^i}, де i ціле та може приймати значення на відрізку (2, 6).

Ідея побудування ДГВБ полягає в тому, щоб на першому етапі за деяким методом (алгоритмом) спарювання генерувати послідовність елементів мультиплікативної групи розширення поля F_{q^i}, а

на другому від кожного такого елементу обчислювати геш – значення, використовуючи певну геш – функцію.

На рис. 1 зображено функціональну схему (алгоритм) ДГВБ на основі спарювання точок еліптичних кривих. Перед початком роботи ДГВБ необхідно встановити в початковий стан, скажемо m. Оскільки ми розглядаємо генератор бітів, то число станів можна приблизно оцінити як . Як правило m повинне бути випадковим, хоча при деяких умовах m може генеруватись і за допомогою іншого ДГВБ. Перед введенням m-бітне початкове число розбивається навпіл і в подальшому використовується в якості x-координат точок на еліптичній кривій, і, таким чином, задаючи випадково x-координати випадково задаються 2 точки еліптичної кривої.

Генерування випадкового елементу мультиплікативної підгрупи розширення поля F_{q^i} здійснюється таким чином. Два випадкових значення t вводяться в елемент $\varphi(x)$, причому t значення може модифікуватись під впливом додаткових даних та/або зворотних даних y. Перетворення $x(t)$ перевіряє x-координату на її приналежність еліптичній кривій, а $\varphi(x)$ знаходить y-координату точки відповідно до значення x шляхом вирішення рівняння еліптичної кривої.

Таким чином, випадково формуються дві точки еліптичної кривої $P(x,y)$ та $Q(x,y)$. Далі ці дві точки спарюються згідно перетворення Вейля [6]. В результаті спарювання формується перший елемент мультиплікативної підгрупи a_1, в подальшому генеруються наступні елементи підгрупи. Зразу відмітимо, що існує можливість рекурентного формування усіх елементів підгрупи порядку q. Для забезпечення необхідної якості випадковості далі застосовується перетворення типу гешування.

Вибір стандарту гешування та параметрів функції гешування складає окремий предмет досліджень. В процесі досліджень було обґрунтовано, що розмір елементів a_1 мультиплікативної підгрупи повинен бути не менше довжини геш-значення l_h. За таких умов, тобто коли $l_h < l_a$, будуть виникати колізії геш–значень елементів мультиплікативної групи, ймовірності виникнення яких залежать від того, наскільки $l_a > l_h$. Результати дослідження виникнення колізій наведені нижче.

Попередній аналіз наведеної схеми, а також проведене програмне моделювання показали, що перетворення спарювання Вейля має значну складність, якщо його застосовувати кожен раз при обчисленні наступного елемента мультиплікативної групи. Пропонується будувати ДГВБ, який базується на властивості білінійного спарювання.

2. ОЦІНКА ЙМОВІРНОСТІ ВИНИКНЕННЯ КОЛІЗІЙ ГЕШ-ЗНАЧЕНЬ

Проведений аналіз ДГВБ показав, що при його застосуванні можуть виникати два різних класи за природою виникнення колізій. До першого відносяться колізії, які виникають при обчисленні геш – значень за умови, що $l_a > l_h$. До другого відносяться колізії, що виникають при випадковому формуванні елементів мультиплікативної підгрупи розширення поля. Розглянемо їх послідовно, орієнтуючись на схему ДГВБ (рис. 1).

Згідно схеми ДГВБ, що наведена на рис. 1, елементи a_i мультиплікативної підгрупи порядку q гешуються з використанням колізійно стійкої геш–функції. За умови, коли $l_a > l_h$, можливі колізії геш–значень, а це означає, що відрізки випадкових бітів довжини l_h будуть співпадати. Тому розглянемо дві основні задачі оцінки колізій.

1. Нехай є деяка функція H обчислення геш-значення від елементів мультиплікативної підгрупи

$$h = H(a_i), i = 1,...,q;$$

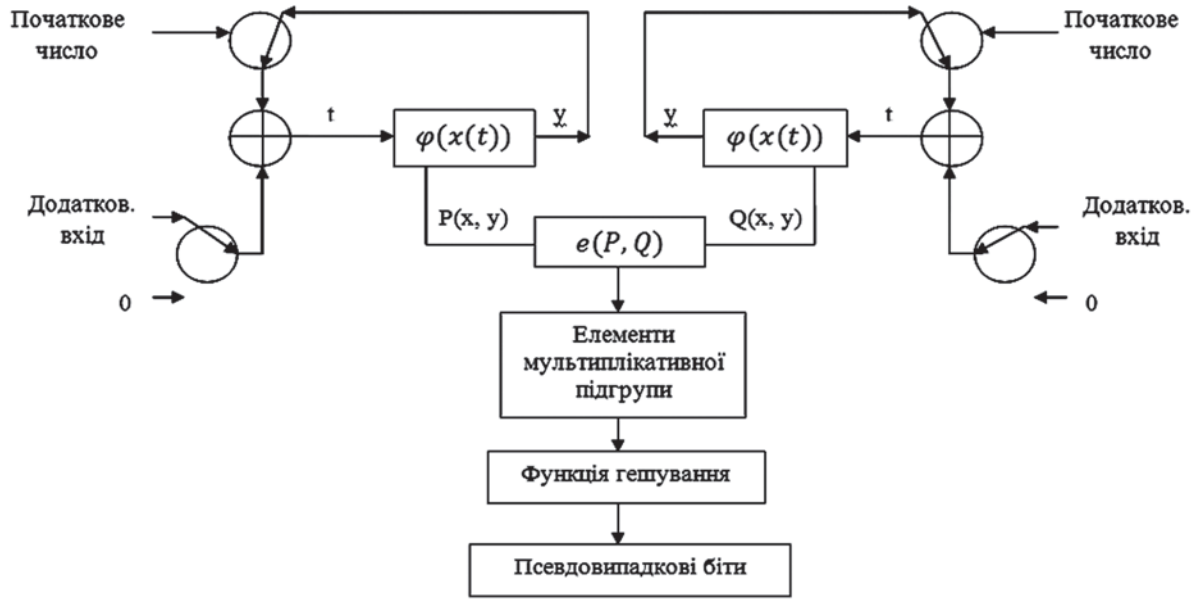


Рис. 1. ДГВБ на основі спарювання точок еліптичних кривих

причому h може приймати $n=2^{l_h}$ значень незалежно від довжини l_a. Необхідно визначити число k випадкових елементів мультиплікативної підгрупи a_i, які необхідно подати на вхід засобу гешування, щоб з імовірністю P_k відбувся хоча б один збіг виду $H(a_i)=H(a_j)$, тобто відбулася колізія.

2. Нехай на виході засобу гешування H з повної множини значень $n=2^{l_h}$ формуються k випадкових геш-значень функції перетворення $H(a_i)$, причому $k\le n$ і ймовірність появи h_i підкоряється рівноймовірному закону розподілу. Необхідно знайти ймовірність $P(n,k)$ того, що ці безлічі містять в собі хоча б по одному елементу x_i і y_j, такі, що $x_i=y_j$.

Важливість вирішення першої задачі пояснюється наступним. По суті k є допустимим значенням числа елементів мультиплікативної групи, при генеруванні яких колізія відбувається з ймовірністю P_k. Друга задача є оберненою першій, в ній необхідно знайти ймовірність колізії при відомих n та k.

Розв'язок виконаємо на основі узагальненого "парадоксу дня народження". В [7] показано, що ймовірність відбуття колізії $P(n,k)$ для загального випадку може бути обчислена.

$$P_k(n,k)=1-\frac{n(n-1)(n-2)...(n-(k-1))}{n\quad n\quad n\qquad\qquad n}=$$
$$=1-1\left(\frac{n-1}{n}\right)\left(\frac{n-2}{n}\right)...\left(\frac{n-(k-1)}{n}\right)= \qquad (2)$$
$$=1-\left(1-\frac{1}{n}\right)\left(1-\frac{2}{n}\right)...\left(1-\frac{k-1}{n}\right).$$

При реальних значеннях n та k зробити обчислення згідно формули практично неможливо. Але якщо врахувати, що в реальних випадках $k<0{,}1n$, то для спрощення (2) можна зробити заміну $(1-x)\le e^{-x}$, в результаті маємо

$$P_k(k,n)=1-e^{-\frac{1}{n}}\cdot e^{-\frac{2}{n}}...e^{-\frac{k-1}{n}}=$$
$$=1-e^{-\frac{1}{n(1+2+3+...+k-1)}}= \qquad . \qquad (3)$$
$$=1-e^{-\frac{k(k-1)}{2n}}=1-e^{-\frac{k(k-1)}{2\cdot 2^{l_h}}}$$

Таким чином, при вказаних обмеженнях одержано аналітичне співвідношення, що зв'язує між собою імовірність колізії $P_k(n,k)=P_k$, число сформованих елементів мультиплікативної підгрупи k довжиною l_h та загальне число елементів мультиплікативної групи $n=2^{l_h}$.

Формула (3) дозволяє:

– зробити оцінку імовірності колізій P_k, розглядаючи її у залежності від k та l_h;

– визначити критичне значення в залежності від допустимого значення імовірності колізії P_k для різних величин k;

– визначити обмеження на число сформованих елементів мультиплікативної підгрупи k, при яких імовірність колізії не перевищує P_k.

При оцінці величин імовірності колізії можна використовувати вираз (3). При цьому для випадку, коли $k^2>>k$, його можна спростити до виду

$$P_k(k,n)\approx 1-e^{-\frac{k^2}{2^{(l_h+1)}}}. \qquad (4)$$

В таблиці 1 наведені значення ймовірностей колізії P_k в залежності від k та l_h.

Критичне значення можна знайти із співвідношень (3) або (4), подавши його у виді

$$1-P_k=e^{-\frac{k(k-1)}{2^{l_i+1}}}=e^{-\frac{k(k-1)}{2n}}. \qquad (5)$$

Прологарифмувавши вираз(5), маємо

$$\ln(1-P_k)=-\frac{\left(k^2+k\right)}{2^{l_i+1}}=-\frac{\left(k^2+k\right)}{2n}. \qquad (6)$$

Далі із (6) спочатку знаходимо як

$$n_{kp}=-\frac{\left(k^2+k\right)}{\left(2\ln(1-P_k)\right)}. \qquad (7)$$

Критичне значення знаходимо із виразу $n_{kp}=2^{l_{kp}}$, отже

$$l_{kp}=\log_2 n_{kp}. \qquad (8)$$

В табл. 2 наведено значення мінімально допустимих довжин (бітів) в залежності від величин k та P_k. Але при виборі значення необхідно враховувати, що геш–значення можуть приймати тільки фіксовані довжини – 160, 256, 384 та 512 бітів.

Таблиця 1

Значення ймовірностей колізії P_k в залежності від k та l_h

l \ k	2	16	32	64	128	256	1024	65536	10^9	10^{12}
8	0,004	0,38	0,867	0,999	~1	~1	–	–	–	–
16	$3.05\cdot10^{-5}$	$1.9\cdot10^{-3}$	$7.7\cdot10^{-3}$	0,031	0,118	0,393	0,999	~1	–	–
32	$4{,}6\cdot10^{-10}$	$2{,}9\cdot10^{-8}$	$1{,}1\cdot10^{-7}$	$4{,}7\cdot10^{-7}$	$1{,}9\cdot10^{-6}$	$7{,}6\cdot10^{-6}$	$1{,}2\cdot10^{-4}$	0.393	~1	–
64	$9{,}7\cdot10^{-20}$	$6{,}2\cdot10^{-18}$	$2{,}5\cdot10^{-17}$	$9{,}9\cdot10^{-17}$	$3{,}9\cdot10^{-16}$	$1{,}7\cdot10^{-15}$	$2.8\cdot10^{-14}$	$1.1\cdot10^{-10}$	0,02	~1
128	~0	~0	~0	~0	~0	~0	~0	$1{,}7\cdot10^{-29}$	$1{,}2\cdot10^{-21}$	$1{,}2\cdot10^{-15}$
256	~0	~0	~0	~0	~0	~0	~0	~0	~0	~0
512	~0	~0	~0	~0	~0	~0	~0	~0	~0	~0

Обмеження на число сформованих елементів мультиплікативної підгрупи k_0, при яких імовірність колізії не перевищує P_k, можна здійснити, використавши (5). В результаті по аналогії з [7] маємо:

$$k^2 + k + 2n\ln(1-P_k) = 0. \quad (9)$$

При значенні $k^2 >> k$ можна використовувати співвідношення

$$k^2 + 2n\ln(1-P_k) = 0.$$

Тоді оцінкою величини k є значення

$$k = \sqrt{-2n\ln(1-P_k)} = \sqrt{-2^{l_h+1}\ln(1-P_k)}. \quad (10)$$

Таким чином, використовуючи наведений математичний апарат, можна зробити оцінки ймовірностей виникнення колізій геш-значень елементів мультиплікативної підгрупи a_i та вибрати довжини геш–значень, тобто вибрати допустимі значення l_h, зважаючи на те, що довжини геш–значень є стандартизованими, як уже вказувалось – 160, 256, 384 та 512 бітів. Також вирішивши параметричне рівняння (9) відносно k_0, знайдемо обмеження на число блоків випадкової послідовності бітів, що можуть бути генеровані на одному і тому ж ключі.

3. ОЦІНКА ЙМОВІРНОСТЕЙ ВИНИКНЕННЯ КОЛІЗІЙ ПРИ ВИПАДКОВОМУ ФОРМУВАННІ ЕЛЕМЕНТІВ МУЛЬТИПЛІКАТИВНОЇ ПІДГРУПИ

Тепер розглянемо другу задачу оцінки ймовірностей виникнення колізій ДГВБ при випадковому формуванні елементів мультиплікативної підгрупи a_i розширення поля порядку q. Будемо розглядати ймовірності виникнення колізій за рахунок того, що при випадковому формуванні елементів мультиплікативної підгрупи a_i можуть відбуватись події, коли відбудеться колізія в виборі одного й того ж елементу мультиплікативної підгрупи a_i. Це справедливо, якщо елементи мультиплікативної підгрупи a_i будемо вибирати випадково й рівноймовірно.

Для цього випадку ймовірність $P(n,k)$ того, що ці безлічі містять в собі хоча б по одному елементу x_i і y_j, такі, що $x_i = y_j$, можна оцінити також використовуючи λ-метод.

В нашому випадку подія $x_i = y_j$ може відбутися з ймовірністю $1/q$, де q – порядок підгрупи.

Тому ймовірність того, що $x_i \neq y_j$ обчислюється як:

$$Q(x_i \neq y_j) = 1 - \frac{1}{q}. \quad (11)$$

Якщо Y включає в себе k подій, то ймовірність того, що всі значення $y_1, y_2, .., y_k$ не співпадуть з x_i, може бути обчислена як

$$Q(x_i \neq Y) = \left(1 - \frac{1}{q}\right)^k. \quad (12)$$

Ймовірність того, що хоча б одне значення Y співпаде з x_i, є

$$R(x_i \in Y) = 1 - \left(1 - \frac{1}{q}\right)^k. \quad (13)$$

Нехай всі елементи X різні. Це справедливо, так як $k << q$, наприклад, $k = \sqrt{q}$. Тоді ймовірність того, що

$$R(x_i \notin Y) = \left(1 - \frac{1}{q}\right)^k$$

і

$$R(x \notin Y) = \left(\left(1 - \frac{1}{q}\right)^k\right)^k = \left(1 - \frac{1}{q}\right)^{k^2}. \quad (14)$$

Далі, ймовірність того, що хоча б одна подія із X і Y співпаде, є

$$R(x_i = y_j) = 1 - \left(1 - \frac{1}{q}\right)^{k^2}. \quad (15)$$

Позначимо $x = \frac{1}{q} << 1$ і скористаємося співвідношенням $(1-x) \le e^{-x}$. В результаті отримаємо

$$R(q,k) = 1 - \left(1 - \frac{1}{q}\right)^{k^2} = \left(1 - \left(e^{-1/q}\right)^{k^2}\right) = 1 - e^{-\frac{k^2}{q}}. \quad (16)$$

Таким чином, ймовірність того, що в двох множинах X і Y хоча б по одному елементу співпадуть,

$$P(q,k) = P_з = 1 - e^{-k^2/q}. \quad (17)$$

Перетворюючи (17), отримаємо

$$e^{-k^2/q} = 1 - P_з. \quad (18)$$

Логарифмуючи (18), маємо

$$-\frac{k^2}{q} = \ln(1 - P_з)$$

Таблиця 2

Значення мінімально допустимих довжин (бітів) в залежності від величин k та P_k

P_k \ k	2	8	16	32	64	128	256	1024	32768	65536	10^6	10^9	10^{12}
10^{-3}	11	15	17	19	20	22	24	28	38	40	48	68	88
10^{-6}	21	25	27	28	30	32	34	38	48	50	58	78	98
10^{-9}	31	35	36	38	40	42	44	48	58	60	68	88	108
10^{-12}	41	45	46	48	50	52	54	58	68	70	78	98	118
10^{-16}	54	58	60	62	64	66	68	72	82	84	91	111	131

і далі

$$k^2 = -q\ln\left(\frac{1}{1-P_з}\right)^{-1} = q\ln\left(\frac{1}{1-P_з}\right).$$

Наприкінці отримаємо

$$k = \sqrt{q\ln\left(\frac{1}{1-P_з}\right)}. \qquad (19)$$

Оцінимо значення ймовірностей виникнення колізій ДГВБ при випадковому формуванні елементів мультиплікативної підгрупи a_i. Обчислимо $\lim_{q\to\infty}(1-e^{\frac{-k^2}{q}}) = \lim_{q\to\infty}(1-\frac{1}{e^{\frac{k^2}{q}}})$. Так як $q\to\infty$, то $\frac{k^2}{q}\to 0$, а $e^{\frac{k^2}{q}}\to 1$. Тоді $\lim_{q\to\infty}(1-e^{\frac{-k^2}{q}}) = \lim_{q\to\infty}(1-\frac{1}{e^{\frac{k^2}{q}}})\to 0$.

4. РЕЗУЛЬТАТИ ЕКСПЕРИМЕНТАЛЬНИХ ДОСЛІДЖЕНЬ ДГВБ

Для представленого вище методу генерування випадкових бітів була розроблена універсальна програмна модель ДГВБ, з використанням якої проведено його випробовування та тестування. Випробовувались та тестувались три різні варіанти реалізації генератора:

– ДГВБ реалізований таким чином, коли в якості випадкової послідовності безпосередньо використовується послідовність елементів мультиплікативної підгрупи a_i, тобто без застосування функції гешування;

– ДГВБ, що реалізований згідно рис. 1, а послідовність елементів мультиплікативної підгрупи a_i генерується рекурентно, а початковий стан генератора задається згідно діючого ключа;

– ДГВБ, що реалізований згідно рис. 1, але послідовність елементів мультиплікативної підгрупи a_i вибирається випадково (з використанням ключа), а початковий стан генератора задається згідно діючого ключа;

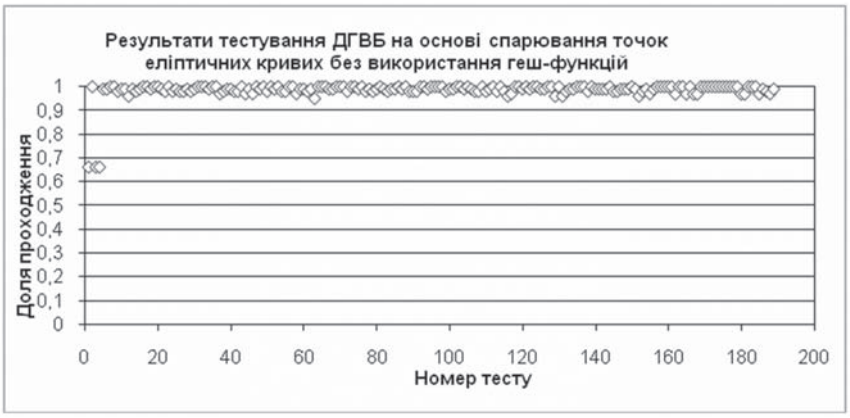
– ДГВБ реалізований таким чином, коли в якості випадкової послідовності безпосередньо використовується послідовність елементів мультиплікативної підгрупи a_i, тобто без застосування функції гешування.

В таблицях 4 та 5 наведені результати тестування ДГВБ тільки на основі спарювання точок еліптичних кривих та класичного генератора BBS[8].

В таблицях 6, 7 та 8 наведені результати тестування ДГВБ згідно рис. 1 та з застосуванням безпосереднього спарювання та гешування з використанням функції гешування SHA-2(з довжиною геш значення 256 бітів).

Таблиця 3

Результати статистичного тестування ДГВБ на основі спарювання точок еліптичних кривих без гешування з використанням NIST SP 800-22



Таблиця 4

ДГВБ на основі спарювання точок еліптичних кривих та генератор BBS

Генератор	Кількість тестів, в яких тестування пройшли більше 99% послідовностей	Кількість тестів, в яких тестування пройшли більше 96% послідовностей
BBS	134 (70,8%)	189 (100%)
ДГВБ на основі спарювання точок еліптичних кривих	133 (70,4%)	185 (97,9%)

Таблиця 5

ДГВБ на основі спарювання точок еліптичних кривих та генератор BBS з урахуванням двох значень P ($P \le 0{,}01$, $P \le 0{,}001$)

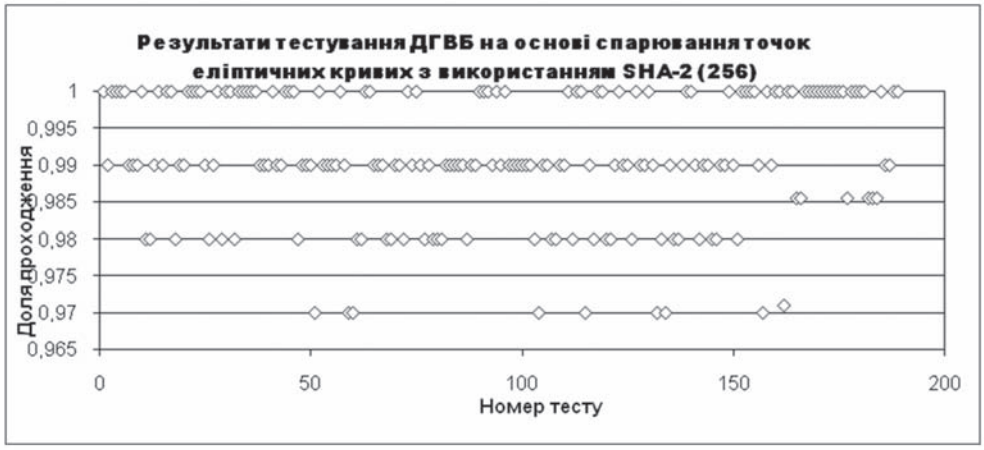
Генератор	Кількість тестів, в яких значення ймовірності $P \le 0{,}01$	Кількість тестів, в яких значення ймовірності $P \le 0{,}001$
BBS	0	0
ДГВБ на основі спарювання точок еліптичних кривих	5	3

В таблицях 9, 10 та 11 наведені результати статистичного тестування ДГВБ на основі спарювання точок еліптичних кривих без гешування з рекурентним генеруванням елементів мультиплікативної підгрупи a_i (модифікований метод).

В таблицях 12, 13 та 14 наведені результати тестування модифікованого ДГВБ згідно рис. 1 з застосуванням безпосереднього спарювання та гешування з використанням функції гешування SHA-2(з довжиною геш значення 384 бітів).

Таблиця 6

ДГВБ на основі спарювання точок еліптичних кривих з використанням SHA-2 (256)



Таблиця 7

ДГВБ на основі спарювання точок еліптичних кривих з застосуванням функції гешування та генератор BBS

Генератор	Кількість тестів, в яких тестування пройшли більше 99% послідовностей	Кількість тестів, в яких тестування пройшли більше 96% послідовностей
BBS	134 (70,8%)	189 (100%)
ДГВБ на основі спарювання точок еліптичних кривих та гешування	142 (75,1%)	189 (100%)

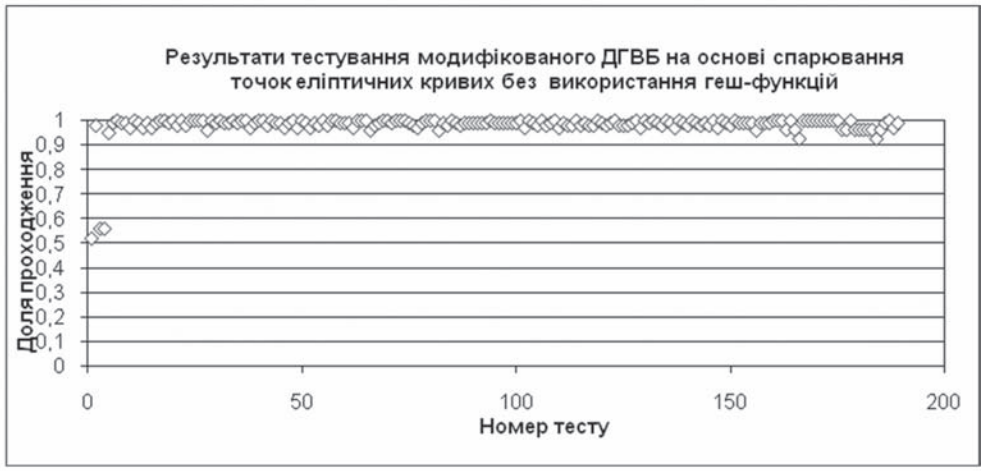
Таблиця 8

ДГВБ на основі спарювання точок еліптичних кривих з застосуванням функції гешування та генератор BBS з урахуванням двох значень P ($P \le 0{,}01$, $P \le 0{,}001$)

Генератор	Кількість тестів, в яких значення ймовірності $P \le 0{,}01$	Кількість тестів, в яких значення ймовірності $P \le 0{,}001$
BBS	0	0
ДГВБ на основі спарювання точок еліптичних кривих та гешування	1	0

Таблиця 9

Модифікований ДГВБ на основі спарювання точок еліптичних кривих без хешування



Таблиця 10

Модифікований ДГВБ на основі спарювання точок еліптичних кривих та генератор BBS

Генератор	Кількість тестів, в яких тестування пройшли більше 99% послідовностей	Кількість тестів, в яких тестування пройшли більше 96% послідовностей
BBS	134 (70,8%)	189 (100%)
Модифікований ДГВБ на основі спарювання точок еліптичних кривих	128 (67,7%)	183 (96,8%)

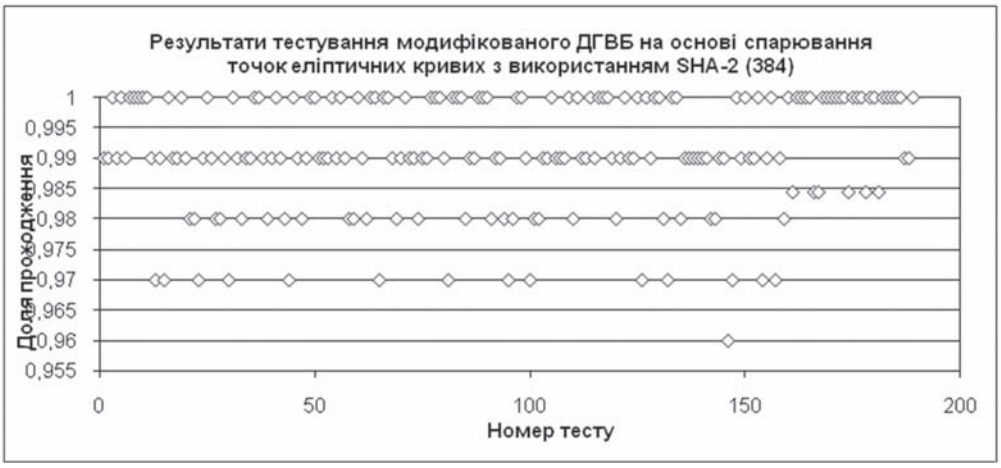
Таблиця 11

Модифікований ДГВБ на основі спарювання точок еліптичних кривих та генератор BBS з урахуванням двох значень P ($P \le 0{,}01$, $P \le 0{,}001$)

Генератор	Кількість тестів, в яких значення ймовірності $P \le 0{,}01$	Кількість тестів, в яких значення ймовірності $P \le 0{,}001$
BBS	0	0
Модифікований ДГВБ на основі спарювання точок еліптичних кривих	7	4

Таблиця 12

Модифікований ДГВБ на основі спарювання точок еліптичних кривих з використанням SHA-2 (384)



Таблиця 13

Модифікований ДГВБ на основі спарювання точок еліптичних кривих з використанням SHA-2 (384) та генератор BBS

Генератор	Кількість тестів, в яких тестування пройшли більше 99% послідовностей	Кількість тестів, в яких тестування пройшли більше 96% послідовностей
BBS	134 (70,8%)	189 (100%)
Модифікований ДГВБ на основі спарювання точок еліптичних кривих *SHA-2 (384)*	142 (75,1%)	189 (100%)

Таблиця 14

Модифікований ДГВБ на основі спарювання точок еліптичних кривих з використанням SHA-2 (384) та генератор BBS з урахуванням P ($P \le 0{,}01$, $P \le 0{,}001$)

Генератор	Кількість тестів, в яких значення ймовірності $P \le 0{,}01$	Кількість тестів, в яких значення ймовірності $P \le 0{,}001$
BBS	0	0
Модифікований ДГВБ на основі спарювання точок еліптичних кривих *SHA-2* (384)	1	0

ВИСНОВКИ

Результати експериментальних досліджень підтвердили, що ДГВБ на основі спарювання точок еліптичних кривих та гешування забезпечують формування випадкових детермінованих бітів з достатніми для більшості додатків якостями.

Кращі статистичні характеристики по NIST-SP 800-22 забезпечує модифікований ДГВБ, коли спарювання виконується тільки при обчисленні генератора підгрупи та гешування з використанням функції гешування SHA-2(з довжиною геш значення 384 бітів) по NIST-SP 800 -22.

Як слідує із таблиць 6-8 та 12-14 ДГВБ зі спарюванням точок еліптичних кривих та подальшим гешуванням елементів мультиплікативної підгрупи a_i по статистичним характеристикам перевершують класичний ДГВБ BBS.

Разом з тим для практичної реалізації ДГВБ необхідно ще вирішувати ряд теоретичних та практичних питань. До них необхідно віднести питання генерування загальних параметрів, вибору функцій гешування та їх параметрів, оптимізації обчислень та доведення криптографічних властивостей такого ДГВБ.

Література.

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

[2] ISO/IEC 18031:2005(E), Information technology – Security techniques – Random bit generation.

[3] *Горбенко І.Д.* Навчальний посібник "Захист інформації в інформаційно-телекомунікаційних системах" / І.Д. Горбенко, Т.О. Гріненко. – Х.: ХНУРЕ, 2003. - 368 с.

[4] *Горбенко І.Д.* Обгрунтування вимог до генераторів випадкових бітів згідно ISO/IEC 18031 / І.Д. Горбенко, Н.В. Шапочка, О.О. Козулін. – К.: Радіоелектронні і комп'ютерні системи, 2009.

[5] *Koblitz N.* Pairing-based cryptography at high security levels, Proceedings of the Tenth IMA International Conference on Cryptography and Coding. / Koblitz N., Menezes A. J. // Springer-Verlag, LNCS 3796. – 2005. –Pp. 13-36.

[6] *Maas M.* Pairing-Based Cryptography / M. Maas. – TECHNISCHE UNIVERSITEIT EINDHOVEN, 2004. – 91p.

[7] *Потій О.В.* Метод оцінки ймовірностей колізій у безумовно стійких та обчислювально стійких криптосистемах / О.В. Потій, Ю.І. Горбенко, Є.В. Попович. // Прикладна радіоелектроніка, 2003.

[8] *Потий О.В.* Статистическое тестирование генераторов случайных и псевдослучайных чисел с использованием набора статистических тестов NIST STS / А.В. Потий, С.Ю. Орлова, Т.А. Гриненко // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. 2001. Вип. 2. С. 206-214.

Надійшла до редколегії 10.06.2010.

Горбенко Іван Дмитрович, доктор техн. наук, професор, завідувач кафедри безпеки інформаційних технологій Харківського національного університету радіоелектроніки, головний конструктор ЗАТ «Інститут інформаційних технологій». Область наукових інтересів: криптографічні системи та протоколи; проектування та розробка систем, комплексів та засобів криптографічного захисту інформації.

Шапочка Наталя Вікторівна, аспірантка кафедри безпеки інформаційних технологій Харківського національного університету радіоелектроніки. Область наукових інтересів: розробка та застосування методів генерації випадкових послідовностей.

Погребняк Костянтин Анатолійович, канд. техн. наук, асистент кафедри безпеки інформаційних технологій Харківського національного університету радіоелектроніки. Область наукових інтересів: застосування алгебраїчної геометрії у системах криптографічного захисту інформації; асиметрична криптографія.

УДК 681.324.067

Метод построения детерминированных случайных последовательностей на основе спаривания точек эллиптических кривых / И.Д Горбенко, Н.В. Шапочка, К.А. Погребняк // Прикладная радиоэлектроника: науч.-техн. журнал. – 2010. Том 9. № 3. – С. 386-393.

Приводится обоснование и описывается сущность и свойства генератора детерминированных случайных последовательностей на основе криптографического преобразования, такого как спаривание точек эллиптических кривых.

Ключевые слова: элиптические кривые, детерминированные случайные последовательности.

Табл. 14. Ил. 01. Библиогр.: 08 назв.

UDK 681.324.067

A method of constructing deterministic random sequences on the base of pairing points of elliptic curves / I.D. Gorbenko, N.V. Shapochka, K.A. Pogrebnyak // Applied Radio Electronics: Sci. Mag. – 2010. Vol. 9. № 3. – P. 386-393.

The paper provides substantiation and describes the nature and properties of a generator of deterministic random sequences on the base of cryptographic transformation such as pairing points of elliptic curves.

Key words: elliptic curves, deterministic random sequences.

Tab. 14. Fig. 01. Ref.: 08 items.