УДК 681.3.06:519.248.681

МЕТОДИ ПОБУДУВАННЯ ДЕТЕРМІНОВАНИХ ГЕНЕРАТОРІВ ВИПАДКОВИХ БІТІВ З ПІДВИЩЕНОЮ ШВИДКОДІЄЮ ТА КРИПТОГРАФІЧНОЮ СТІЙКІСТЮ

Н.В. ШАПОЧКА, Д.С. БАЛАГУРА

Обґрунтовуються методи генерування псевдовипадкових бітів на основі використання властивостей ізоморфізмів простих полів та підполів Галуа, наводиться оцінка стійкості та результати тестування вихідних даних розглянутих генераторів.

Ключові слова: випадкові біти, детермінований генератор випадкових бітів, поле Галуа, підполе Галуа, криптоаналітичні атаки.

ВСТУП

На нинішній час загальним підходом до генерування ключів, ключової інформації та параметрів є стандартизація методів, механізмів та практичних (конкретних) алгоритмів їх генерування. При чому, як можна судити із ряду джерел [1-5], ці методи, механізми та алгоритми стараються захистити від розповсюдження особливо в частині генерування випадкових послідовностей. Таке ж відношення до початку XXI століття було і відносно генерування псевдовипадкових послідовностей (бітів). В останні роки у зв'язку із суттєвим розвитком інфраструктури відкритих ключів виникла потреба в створенні апаратних, апаратно-програмних та програмних засобів генерування ключів. Були розроблені та прийняті спочатку регіональні стандарти [6-8], а потім і міжнародні стандарти [9, 10], в яких були визначені вимоги, методи, механізми та алгоритми реалізації генераторів. При чому, у зв'язку з необхідністю відновлення ключів та ключової інформації в просторі і часі, в них в повному обсязі розглядаються тільки детерміновані генератори випадкових бітів, що визначає їх особливу актуальність.

Основними вимогами, що висуваються до детермінованих генераторів випадкових бітів (ДГВБ), є непередбачуваність, просторова та тимчасова складність, відновлюваність в просторі і часі, необоротність. Період повторення послідовності, що генерується, ДГВБ повинен бути не менше заданого, подібно блочним симетричним шифрам, при чому в якості заданого може використовуватись 2^{128} – нормальний рівень стійкості, 2^{256} – високий, 2^{512} – надвисокий [1]. Вказані властивості можуть бути забезпечені з різними рівнями гарантій.

Існує декілька підходів до визначення рівнів гарантій. Перший підхід пов'язаний з тестуванням псевдовипадкових бітів (тобто випадкових бітів, сформованих детермінованим генератором випадкових бітів) на випадковість, для чого, наприклад, застосовується стандарт FIPS 140-1 або AIS 20.

Кращими, і, як наслідок, визнаними на міжнародному рівні, є три різні методи і ДГВБ, побудовані на їх основі, що викладені в ISO/IEC 18031 [9]. Вони базуються на використанні:

1. Алгоритмів блокового симетричного шифрування.

2. Функцій гешування.

3. Розв'язку теоретико-числових задач, а по суті перетворення в групі точок еліптичних кривих (ЕК).

На наш погляд, залишились актуальними задачі дослідження цих ДГВБ, встановлення класу гарантій і подальший розвиток теорії та практики генерування псевдовипадкових бітів, в тому числі з найвищим рівнем гарантій K4 або P2 згідно AIS 20 (AIS 31). Необхідно відмітити, що в Україні тільки розпочаті роботи в частині створення ДГВБ. В 2009 році гармонізований і введений в дію стандарт ISO/IEC 19790 [10], який є гіршим, ніж ISO/IEC 18031, що було підтверджено за участі авторів при дослідження та гармонізації ISO/IEC 18031.

Метою статті є аналіз якості існуючих, удосконалення та розробка нових методів генерування псевдовипадкових бітів на основі використання перетворень в підполях та полях Галуа із заданим періодом повторення з наступним гешуванням елементів підполів або полів, які у залежності від вимог відповідали б різним рівням класів гарантій та мали більшу, у порівнянні з існуючими, швидкодію.

1. МЕТОД ГЕНЕРУВАННЯ ПСЕВДОВИПАДКОВИХ БІТІВ НА ОСНОВІ РЕКУРЕНТНОГО ФОРМУВАННЯ ЗГІДНО КЛЮЧОВИХ ДАНИХ ЕЛЕМЕНТІВ ІЗОМОРФІЗМІВ ПРОСТИХ ПОЛІВ ГАЛУА

Розглянемо спочатку перший метод реалізації ДГВБ – генерування псевдовипадкових бітів на основі рекурентного формування елементів поля Галуа. Генерування псевдовипадкових бітів відбувається у такий спосіб:

1. Ввести або генерувати загальносистемні параметри: модуль p та первісний елемент g побудування елементів поля Галуа, перевірити їх дійсність.

2. Ввести або інсталювати таємний ключ ДГВБ k_j та виробити з нього ключі $k_{\text{п}}$ та $k_{\text{к}}$, де $k_{\text{п}}$ – початковий ключ, а $k_{\text{к}}$ – ключ, що визначає крок зміни показника.

3. Обчислити початкове значення ДГВБ A_1, використовуючи правило

$$A_1 = g^{k_1} (\mathrm{mod}\, p) = g^{k_п + k_к} (\mathrm{mod}\, p). \quad (1)$$

4. Обчислити i-й елемент поля Галуа A_i для ДГВБ, використовуючи правило

$$A_i = g^{k_i} (\mathrm{mod}\, p) = g^{k_п + ik_к} (\mathrm{mod}\, p), \quad (2)$$

де $i \geq 2$ – номер елемента поля Галуа, що генерується, тобто

$$k_i = (k_п + ik_к^{/}) (\mathrm{mod}\, p),\ i = 2,3,...,r,... \quad (3)$$

Оскільки $i = 1$ уже використано в (1), а також (3), $k_k^{/} = 1$ при вказаних значеннях i, або $ik_k^{/}$ повинно бути взаємно простим з $p-1$. За заданих умов A_i буде мати гарантований період $p-1$.

5. Обчислити i-е геш-значення чи значення іншої функції від A_i та прийняти його в якості i-го випадкового слова, тобто

$$X_i = H(A_i) = H(g^{k_п + ik_к} (\mathrm{mod}\, p)). \quad (4)$$

Далі розглянемо другий метод реалізації ДГВБ на основі рекурентного формування елементів підполя Галуа. Сутність методу зводиться до виконання такого.

1. Ввести або генерувати загальносистемні параметри [1] p, q та g побудування елементів підполя Галуа, перевірити їх дійсність.

2. Ввести або інсталювати таємний ключ ДГВБ k_j та виробити з нього ключі $k_п$ та $k_к$, де $k_п$ – початковий ключ, а $k_к$ – ключ, що визначає крок зміни показника.

3. Обчислити початкове значення ДГВБ A_1, використовуючи правило

$$A_1 = g^{(k_1)(\mathrm{mod}\, q)} (\mathrm{mod}\, p) = g^{(k_п + k_к)(\mathrm{mod}\, q)} (\mathrm{mod}\, p). \quad (5)$$

4. Обчислити i-й елемент поля Галуа A_i для ДГВБ, використовуючи правило

$$A_i = g^{(k_i)(\mathrm{mod}\, q)} (\mathrm{mod}\, p) = g^{(k_п + ik_к)(\mathrm{mod}\, q)} (\mathrm{mod}\, p), \quad (6)$$

де i – номер елемента підполя Галуа, що генерується, тобто

$$k_i = (k_п + ik_к^{/}) (\mathrm{mod}\, q),\ i = 2,3,...,r,...$$

5. Обчислити i-е геш-значення чи значення іншої функції від A_i та прийняти його в якості i-го випадкового слова, тобто

$$X_i = H(A_i) = H(g^{(k_?+ik_:)(\mathrm{mod}\, q)} (\mathrm{mod}\, p)). \quad (7)$$

Схеми алгоритмів, що реалізують наведені вище методи генерування ДГВБ, наведені на рис. 1 та 2.

Властивості простих полів Галуа в плані застосування в ДГВБ визначаються нижче наведеними твердженнями.

Твердження 1. В простому полі Галуа $GF(p)$ останні $(p-1)/2$ елементів поля є мультиплікативно зворотними до перших $(p-1)/2$ елементів, починаючи з другого елемента першої половини та останнього елементу другої половини.

Твердження 2. В простому полі Галуа $GF(p)$ перші $(p-1)/2$ елементів поля, починаючи з першого g_0, є адитивно зворотними до $(p-1)/2$ - елементів другої половини, починаючи $g^{(p-1)/2}$.

Із наведених тверджень 1 та 2 витікає, що з точки зору структурних властивостей перша половина елементів простого поля Галуа однозначно зв'язана з другою половиною, як мультиплікативно, так і адитивно.

Вивчення ансамблевих властивостей простих полів Галуа пов'язано з визначенням числа ізоморфізмів, що існують для заданого простого числа p. При цьому максимальне число ізоморфізмів може бути отриманим у випадку, коли p є «сильним» простим числом, наприклад

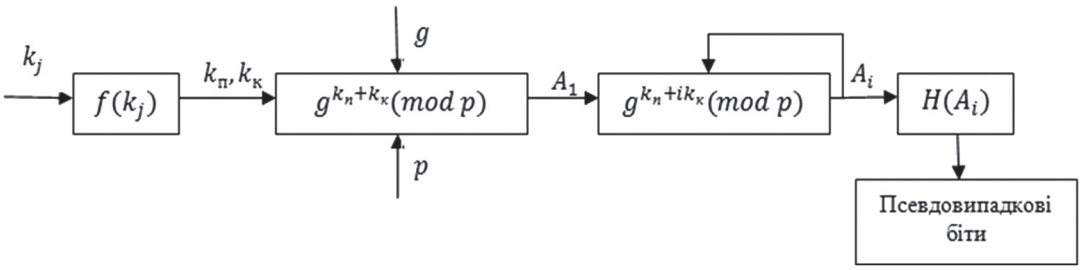

Рис. 1. Схема алгоритму, що реалізує метод генерування детермінованих випадкових послідовностей в простому полі Галуа

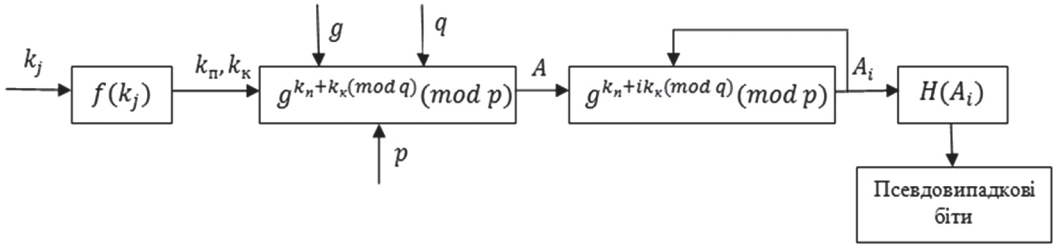

Рис. 2. Схема алгоритму, що реалізує метод генерування детермінованих випадкових послідовностей в підполі простого поля Галуа

$$p = 2 \cdot S + (-)1 , \qquad (8)$$

де S в свою чергу просте число, краще також «сильне». Дійсно для числа $p = 2 \cdot S + 1$ отримаємо, що число ізоморфізмів

$$N_{із} = \phi(\phi(P)) = \phi(\phi(2 \cdot S + 1 \cdot P)) = \\ = \phi(2 \cdot S) = \phi(2)\phi(S) = \phi(S). \qquad (9)$$

Аналізуючи (9), приходимо до висновку, що максимальне значення досягається у випадку, якщо S в свою чергу просте.

Далі розглянемо складність вирішення задачі обернення на випадок простого поля Галуа. Вона зводиться до вирішення порівняння виду (2), тобто

$$A_i = g^{k_i} (\mathrm{mod}\ p) \qquad (10)$$

відносно k_i. Якщо загальні параметри p та g відомі, а також відомий елемент A_i, то визначення A_i зводиться до вирішення дискретного логарифмічного рівняння в полі. Вона носить субекспоненційний характер і в залежності від методу може бути оцінена як [1]

$$I = \exp(\delta \ln(p)^{\gamma} \ln\ln(p)^{(1-\gamma)}) , \qquad (11)$$

де δ та γ – параметри методу розв'язку дискретного логарифмічного рівняння.

Проведемо дослідження властивостей DSA подібного методу, тобто на основі формування елементів підполів Галуа, що визначений формулами (5) – (7).

Необхідно замітити, що властивості полів і підполів Галуа також достатньо вивчені, перше за все при розробці DSA [11] та ГОСТ 34.10–94 [12] електронних цифрових підписів. Дослідження, що наводяться нижче, уточнюють, доповнюють або визначають властивості підполів Галуа.

Розглянемо суттєве для визначення методу твердження, яке визначає існування підгруп порядку q.

Твердження 3. Якщо P, q – прості числа, і q входить в канонічний розклад числа P-1=rq, тоді існує $Z(P, q)$ генераторів (породжуючих елементів), кожен з яких породжує підгрупу порядку q.

Для реалізації методу необхідно вибрати число g – генератор підгрупи, мультиплікативний порядок якого по модулю дорівнює q.

Твердження 4 [13]. Якщо p, q – прості числа, і q входить в канонічний розклад числа p-1, то генератор підгрупи g обчислюється як

$$g = h^{(p-1)/q} (\mathrm{mod}\ p) . \qquad (12)$$

Дійсно, якщо

$$g = h^{(p-1)/q} (\mathrm{mod}\ p) ,$$

то згідно малої теореми Ферма отримуємо, що $g^q = h^{(p-1)} = 1 (\mathrm{mod}\ p)$. Крім того, оскільки $g > 1$ і q – просте число, то g повинне мати порядок підгрупи p з величиною q по модулю p.

У більшості випадків [13] значення h=2 задовольняє вимозі твердження 4.

Таким чином, твердження 4 визначає необхідні та достатні умови обчислення генератора підгрупи g з порядком q по модулю p.

Важливою є також задача вивчення ансамблевих характеристик існування підгруп, тобто по суті визначення розміру множини цілих чисел h, що задовольняють умовам твердження 4. Попередній аналіз дозволив визначити, що ймовірність події, коли g=1 є малою і залежить від p та q, в першу чергу від виду канонічного розкладу p-1. Вирішення цієї задачі аналітично є складним.

2. ОЦІНКА СТІЙКОСТІ ДГВБ

Визнано, що основним методом забезпечення стійкості є використання криптографічних перетворень, тому розглянемо в основному захищеність ключів ДГВБ від їх компрометації. При такій постановці оцінка стійкості зводиться до вирішення задач обернення для випадку простих полів Галуа, а також підполів Галуа. На нинішній час достатньо добре вирішені питання здійснення криптографічних атак на дискретний логарифм виду [1-3] .

При аналізі стійкості будемо вважати, що метою атаки є визначення конкретного значення таємного ключа, що застосовується, наприклад k_i в (2) чи (6). В цьому випадку необхідно вирішити дискретне логарифмічне рівняння виду (2) чи (6), в результаті буде відомий ключ k_i, знання якого дозволяє побудувати певний відрізок елементів підполя чи поля Галуа. При вирішенні задачі криптоаналізу в такій постановці вважається, що криптоаналітику відомі загальні параметри та послідовність елементів A_i.

У випадку (4) та (7) задача, на наш погляд, суттєво ускладнюється, так як значення елементів уже невідомі, а відомі тільки геш-значення від цих елементів. Тому в цьому випадку спочатку необхідно вирішувати задачу визначення прообразу зі складністю 2^{-n-1}, а уже потім вирішувати задачу дискретного логарифмування.

Розглянемо ці дві задачі більш детально. Для розв'язку задач дискретного логарифмування в простому полі Галуа можуть бути застосовані атаки типу «груба сила» та аналітичні атаки. Перші атаки не будемо розглядати, так як при прийнятих значеннях довжин ключів k_i згідно [11] $l_k \geq 256$ бітів, складність атаки буде складати порядку 2^{256} (10^{77}). Ряд аналітичних атак на дискретний логарифм в полі, в кращому випадку, носить субекспоненційний характер виду

$$I = \exp(\delta \ln(p)^{\gamma} \ln\ln(p)^{(1-\gamma)}) , \qquad (13)$$

де δ та γ – параметри методу розв'язку дискретного логарифмічного рівняння. До таких атак відносяться атаки, що ґрунтуються на застосуванні методів Полларда, методу Поліга-Геллмана, загального решета числового поля тощо. В [1] показано, що для випадку застосування методу ρ-Полларда складність атаки I_{ρ} може бути визначена як

$$I_\rho^2 + I_\rho + 2n\ln(1-P_k) = 0, \qquad (14)$$

де $n \geq q$, а P_k – ймовірність, з якою повинна бути здійснена колізія.

Формулу (14) можна спростити, враховуючи те, що в реальних ситуаціях $I_\rho^2 >> I_\rho$. За цієї умови (14) має вид

$$I_\rho^2 + 2n\ln(1-P_k) = 0 \text{ або}$$

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

У випадку застосування методу загального чи спеціального решета числового поля складність атаки дискретного логарифмування в полі Галуа визначається (13) і згідно даних може бути обчислена як

$$I_{\text{рч}} = \exp(2.06\ln(p)^{1/3}\ln\ln(p)^{(1-1/3)}), \qquad (15)$$

тобто з параметрами складності $(2.06, 1/3)$.

Аналіз отриманих даних показує, що метод генерування псевдовипадкових бітів на основі використання елементів поля Галуа при вказаних довжинах є незахищеним від атаки з використанням решета числового поля. Складність атаки груба сила практично є достатньою. А складність атаки методом ρ-Полларда і відповідно стійкість є достатньою уже при $q = 2^{256}$.

Наведені дані оцінки криптографічної стійкості ДГВБ стосуються тільки оцінки захищеності закону (ключа) формування елементів поля Галуа. Зробимо оцінки стійкості для випадку застосування перетворення типу гешування, тобто згідно (13). В цьому випадку спочатку необхідно знайти прообраз відповідного елемента поля A_i, а потім вирішити дискретне логарифмічне рівняння. Враховуючи сказане вище, в тому числі послідовність подій, маємо таку оцінку складності знаходження ключа відносно ДГВБ:

$$I_{\Gamma_1} = I_{\text{рч}} I_{\text{пр}} = \exp(2.06\ln(p)^{1/3} \times \times\ln\ln(p)^{(1-1/3)})(2^n - 1). \qquad (16)$$

Для випадку застосування ρ-Полларда метода замість (16) отримаємо

$$I_{\Gamma_2} = I_{\text{рч}} I_\rho = \exp(2.06\ln(p)^{1/3} \times \ln\ln(p)^{(1-1/3)})(2^{n/2}). \qquad (17)$$

В табл. 1 наведені значення складності криптоаналізу ДГВБ для першого методу, тобто при використанні елементів простого поля Галуа та наступному їх гешуванні. Аналіз цих даних підтверджує високу захищеність ДГВБ від криптоаналізу як у випадку (16), так і у випадку (17).

Тепер проведемо аналіз стійкості ДГВБ, робота якого ґрунтується на генеруванні елементів підполя Галуа, тобто типу DSA (ДСТУ ГОСТ 34.310–2009). При аналізі та виборі методів обернення, тобто криптоаналізу, будемо розглядати (6) та (7) у порівнянні з (2) та (4). Відмітимо, що (6) відрізняється від (2) тим, що ключ k_i обчислюється по суті по подвійному модулю, спочатку по p, а потім по q.

Як і при аналізі (2), при оцінці (6) будемо розглядати три основні методи – «груба сила», ρ-Полларда та решета числового поля.

На основі аналізу методу «груба сила» відносно (6) можна зробити такі висновки. Оскільки в (6) ключ k_i обчислюється по модулю q, а в (2) по модулю p, а $p>>q$, то атака на (6) методом «груба сила» є значно простішою. В таблиці 2 наведені оцінки складності криптоаналізу методом «груба сила» в підполі при оберненні (6) та (7) при застосуванні двох методів – створення колізій та знаходження другого прообразу. Замітимо, що при оцінках згідно (7) необхідно створювати колізію чи шукати прообраз для кожного елемента підполя.

Аналіз даних таблиці 2 дозволяє зробити висновок, що ДГВБ є захищеним від атак «груба сила».

Далі зробимо оцінку криптографічної стійкості ДГВБ, що ґрунтується на криптографічному перетворенні в підполі Галуа. При оцінці будемо розглядати метод ρ-Полларда та метод решета числового поля.

Аналіз (6), що реалізує першу частину метода, показує, що як і при перетворенні в полі, перетворення в підполі здійснюється за модулем p. Але допустимою областю значень ключа k_i є значення із інтервалу

Таблиця 1

Метод КРА \ p	2^{512}	2^{1024}	2^{2048}	2^{3072}
I_{Γ_1}	$4{,}26*10^{97}$	$7{,}25*10^{104}$	$1{,}09*10^{114}$	$8{,}31*10^{121}$
I_{Γ_2}	$1{,}25*10^{59}$	$2{,}13*10^{66}$	$3{,}21*10^{75}$	$2{,}44*10^{83}$

Таблиця 2

Метод КРА \ q	2^{160}	2^{256}	2^{384}	2^{512}
$I_{\text{ГС}}$	$(2^{160}\text{-}1) \approx 10^{48}$	$(2^{256}\text{-}1) \approx 10^{77}$	$(2^{384}\text{-}1) \approx 10^{116}$	$(2^{512}\text{-}1) \approx 10^{154}$
$I_{\text{ГС}}$ та метод колізій	$\approx 2^{240} \approx 10^{72}$	$\approx 2^{384} \approx 10^{116}$	$\approx 2^{576} \approx 10^{173}$	$\approx 2^{768} \approx 10^{231}$
$I_{\text{ГС}}$ та знаходження прообразу	$\approx 2^{320} \approx 10^{96}$	$\approx 2^{512} \approx 10^{154}$	$\approx 2^{768} \approx 10^{231}$	$\approx 2^{1024} \approx 10^{308}$

$$k_i \in (1, q-1) . \quad (18)$$

Відмінність перетворення в підполі від перетворення в полі полягає в тому, що розміри ключів обмежені величиною інтервалу (18). Задачі дискретного логарифмування для перетворення в полі та перетворення в підполі відповідно (2) та (6) залишаються субекспоненційно складними.

Тому для оцінки складності дискретного логарифмування (обернення) в підполі методом ρ -Полларда можна використовувати формулу [1]

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

де $n \geq q$, а P_k – ймовірність, з якою повинна бути здійснена колізія, а з використанням решета числового поля

$$I_{\text{рч}} = \exp(2.06\ln(p)^{1/3} \ln\ln(p)^{(1-1/3)}) .$$

Далі, з урахуванням гешування та дискретного логарифмування з використанням решета числового поля, оцінку стійкості методу генерування псевдовипадкових чисел на основі перетворень в підполі можна оцінювати з використанням (16) та (17). Тому оцінки, які отримані для дискретного логарифмування в полі Галуа, можуть бути застосованими і для оцінки складності дискретного логарифмування і в підполі Галуа.

Наведені в табл. 1, 2 дані відносно оцінки криптографічної стійкості перетворень в простих полях Галуа та в підполях Галуа, з урахуванням застосування гешування відповідних елементів полів чи підполів, підтверджують, що побудовані з їх використанням ДГВБ забезпечують необхідну криптографічну стійкість проти атак типу «повне розкриття». Збільшення складності може досягатись засобом використання більших значень порядків p простих полів та підполів Галуа. При цьому величина q повинна вибиратись за умови забезпечення стійкості від силових атак.

3. РЕЗУЛЬТАТИ ЕКСПЕРИМЕНТАЛЬНИХ ДОСЛІДЖЕНЬ

Результати оцінки швидкодії генерації псевдовипадкових послідовностей у порівнянні з існуючими методами наведено у табл. 3.

Аналіз даних таблиці 3 показує, що запропоновані генератори мають значні переваги по відношенню до дозволеного для використання додатку А в ДСТУ 4145–2002.

Швидкість генерації псевдовипадкових бітів на основі підполів Галуа забезпечується при умові, що таємний ключ k має довжину в 128 бітів. Якщо довжина k буде збільшуватись, то швидкість ДГВБ на основі полів Галуа буде зменшуватись, і, як наслідок, буде менше швидкості формування псевдовипадкових бітів на основі підполів Галуа.

Для тестування розроблених ДГВБ використовувалася методика NIST STS [14], рекомендована Національним інститутом по стандартизації й технологіям США, розроблена для статистичного тестування алгоритмів-кандидатів на AES.

У табл. 4 наведено дані по проходженню тестів за Правилом 1 [15] розробленими ДГВБ у порівнянні із класичним генератором BBS.

ВИСНОВКИ

Розроблені методи генерування псевдовипадкових бітів, що ґрунтуються на рекурентному формування елементів полів та підполів Галуа та їх перетворенні методом гешування в псевдовипадкові біти, забезпечують необхідну криптографічну стійкість. Також розроблені методи побудови ДГВБ володіють необхідним рівнем гарантій стійкості К3, К4 згідно AIS 20, а також необхідним рівнем необоротності, непередбаченості та нерозрізнюваності, і можуть застосовуватись в якості ключового матеріалу.

Література

[1] *Горбенко Ю.І.* Інфраструктури відкритих ключів. Системи ЕЦП. Теорія та практика / Горбенко Ю.І., Горбенко І.Д.. Харків, ФОРТ. 2010, 593с.

[2] *Введение в криптологию* / Под ред. В.В. Ященко. Серия: Новые математические дисциплины. М.: МЦНМО – ЧеРо, 1998. – 271 с.

[3] *Б. Шнаер.* Прикладная криптографія / Б. Шнаер // 2-е издание.

[4] *Ю.С. Харин.* Математические и компьютерные основы криптологии: Учеб. пособие / Ю.С. Харин,

Таблиця 3

Функція гешув. / Вид ДГВБ	Без гешування	SHA-1	SHA-256	SHA-384	SHA-512
ДГВБ на основі полів Галуа	34,8	10,1	16,3	24,4	30,5
ДГВБ на основі підполів Галуа	27,1	8	12,2	17,4	27,1
ДГВБ згідно ДСТУ 4145–2002 для X9.17	4,3	-	-	-	-
ДГВБ на еліптичних кривих згідно ISO/IEC 18031	2,0	-	-	-	-

Таблиця 4

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 полів Галуа	135 (71,4%)	189 (100%)
ДГВБ на основі підполів Галуа	134 (70,8%)	189 (100%)

В.И. Берник, Г.В. Матвеев, С.В. Агиевич // Мн.: Новое знание. – 2003. – 382с.

[5] *Фомичев В.М.* Дискретная математика и криптология. Курс лекций / Под общ. ред. д-ра физ.-мат. н. Н.Д. Подуфалова // – М.: ДИАЛОГ-МИФИ. – 2003 – 400 с.

[6] Federal Information Processing Standards Publication (FIPS PUB) 140-1. Security requirements for cryptographic modules. NIST, 1994.

[7] Application Notes and Interpretation of the Scheme (AIS) 20. Functionality classes and evaluation methodology for physical random number generators. Certification body of the BSI in context of certification scheme. BSI, 1999.

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

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

[10] *ISO/IEC* 19790:2006 Information technology – Security techniques – Security requirements for cryptographic modules.

[11] *FIPS PUB* 186-3. Digital Signature Standard (DSS).

[12] *ГОСТ Р* 34.10-94. Информационная технология. Криптографическая защита информации. Процедуры выработки и проверки электронной цифровой подписи на базе асимметричного криптографического алгоритма.

[13] *FIPS PUB* 186-1. Digital Signature Standard (DSS).

[14] *NIST IR* 6390. A Statistical Test Suite for the Validation of Random Number Generators and Pseudo Random Number Generators for Cryptographic Applications, 2000.

[15] *NIST SP* 800-22. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications. August 2008.

Надійшла до редколегії 23.05.2011

Шапочка Наталя Вікторівна, асистент кафедри безпеки інформаційних технологій ХНУРЕ. Область наукових інтересів: розробка та застосування методів генерації випадкових послідовностей.

Балагура Дмитро Сергійович, доцент кафедри безпеки інформаційних технологій ХНУРЕ. Область наукових інтересів: інформаційні технології, захист інформації, криптографічні протоколи вироблення та узгодження ключів.

УДК 681.3.06:519.248.681

Методы построения детерминированных генераторов случайных битов с повышенным быстродействием и криптографической стойкостью / Н.В. Шапочка, Д.С. Балагура // Прикладная радиоэлектроника: науч.-техн. журнал. – 2011. Том 10. № 2. – С. 153–158.

Обосновываются методы генерирования псевдослучайных битов на основе использования свойств изоморфизмов простых полей и подполей Галуа, приводится оценка стойкости и результаты тестирования выходных данных рассмотренных генераторов.

Ключевые слова: случайные биты, детерминированный генератор случайных бит, поле Галуа, подполе Галуа, криптоаналитические атаки.

Табл. 4. Ил. 02. Библиогр.: 15 назв.

UDK 681.3.06:519.248.681

Methods for constructing deterministic generators of random bits with high speed and cryptographic security / N.V. Shapochka, D.S. Balagura // Applied Radio Electronics: Sci. Journ. – 2011. Vol. 10. № 2. – P. 153–158.

The paper justifies methods to generate pseudorandom bits using the isomorphism properties of simple fields and Galois subfields, provides an assessment of security and the output data test results of the considered generators.

Keywords: random bits, deterministic generator of random bits, Galois field, Galois subfield, cryptoanalytical attacks.

Tab. 4. Fig. 02. Ref.: 15 items.