УДК 004.056

КРИПТОГЕНЕРАТОР З ВИКОРИСТАННЯМ ПЕРЕТВОРЕННЯ ШУМІВ СЛАБОСТРУМНИХ ЕЛЕКТРОННИХ КІЛ

Корольов В.Ю., *к.т.н.,*
Поліновський В.В.
Центр таймерних обчислювальних систем Інституту кібернетики ім. В.М. Глушкова НАНУ

Предложен новый аппаратно-программный криптогенератор случайных чисел с использованием тепловых шумов для портабельных систем защиты информации.

New hardware-software cryptogenerator of random numbers using Johnson noise for portable information security systems is proposed.

Випадкові числа відіграють важливу роль у захисті інформаційних ресурсів і мереж, що базуються на методах шифрування даних і тому постійно потребують розробки нових та вдосконалення існуючих засобів створення криптографічно стійких послідовностей випадкових чисел [1, 178; 2, 198]. Завдяки генерації випадкових чисел системи комп'ютерної безпеки отримують ключі і вектори ініціалізації алгоритмів шифрування даних, сеансові та транзакційні ключі протоколів взаємної ідентифікації сторін та ін.

Для того щоб відповідати вимозі криптографічної стійкості, отримані послідовності чисел мають задовольняти критерії **випадковості** і **непередбачуваності** [2, 199].

Перевірка послідовності на **випадковість** грунтується на наступних критеріях.

- *Однорідність*. Розподіл чисел у послідовності має бути рівномірним, тобто частота появи у послідовності конкретного значення має бути приблизно однаковою.
- *Незалежність*. Жодне із значень послідовності не повинно математично виводитись з інших значень, навіть за умови, що всі попередні значення відомі.

Існують методи перевірки гіпотез [2, 199], що послідовність чисел відповідає заданому розподілу, але методу, який дозволяє довести незалежність, немає. Тому використовуються тести, які дозволяють показати, що послідовність є залежною. Необхідна кількість тестів для алгоритму генерування випадкових чисел визначається прийнятою умовою, за якою твердження, що послідовність є незалежною, стає правдоподібним.

У задачах типу взаємної ідентифікації сторін для обміну секретними даними або генерування сеансових ключів вимога статистичної випадковості є менш важливою за вимогу **непередбачуваності** елементів послідовності. В *істинно* випадковій послідовності кожне число статистично незалежне від інших чисел послідовності і тому є непередбачуваним. На практиці істинно випадкові числа використовуються рідко, найчастіше використовуються псевдовипадкові числа, тобто отримані за допомогою деякого алгоритму. Тому отримані числа мають бути такими, щоб супротивник не мав практичної можливості розрахувати наступні числа на основі знання попередніх.

Таким чином, *істинно випадкові послідовності* – це послідовності, створені джерелом випадкових чисел і які не можливо повторити достовірно. Тобто якщо два рази запустити генератор істинно випадкових чисел з однакими вхідними даними (при однакових умовах експерименту), то на виході буде отримано дві абсолютно непов'язані між собою випадкові послідовності.

Генератори істинно випадкових чисел не є часто використовуваними пристроями. Потенційно основою для їх побудови можуть бути такі фізичні джерела ентропії, як напівпровідникові діоди в режимі сильного насичення, імпульсні детектори іонізуючого випромінення, газорозрядні лампи, конденсатори з протіканням струму, теплові шуми резистора, тунельний ефект у напівпровідниковому стабілітроні та квантові явища. Проте для вирішення задач захисту інформації на базі флеш-накопичувачів необхідні мініатюрні джерела випадкових чисел, що можуть живитись від USB-шини [3, 242] комп'ютера. Реалізувати такий пристрій можна на базі аналогових кіл за допомогою сучасних операційних підсилювачів. На рис. 1 показано розроблений авторами один із можливих варіантів побудови такого апаратно-програмного генератора криптографічно стійких випадкових чисел.

Розглянемо детально роботу цього пристрою (див. рис. 1).

Як показано на рис. 1, криптогенератор обробляє дані, що зберігаються в трьох сховищах (пулах): шумової послідовності, псевдовипадкових даних з портів вводу-виводу і послідовностей ключа-аутентифікатора [4, 177]. Наповнення пулів 5 і 7 є очевидним із функціональної схеми. Наповнення пулу 6 слід розглянути більш детально.

Відомо, що для прискорення роботи USB-модуля використовується буферна таблиця [3, 268], яка розміщується в ОЗУ контролера і в яку заносять тільки дані, що не містять стандартні

заголовки пакетів, передбачені USB-протоколом. Тому в пул 6 будуть заноситись псевдовипадкові дані з портів вводу-виводу 9 і 10. Спосіб вибору адреси, зміщення і довжини псевдовипадкової послідовності може визначатись на підставі даних, отриманих від генератора шумової послідовності.

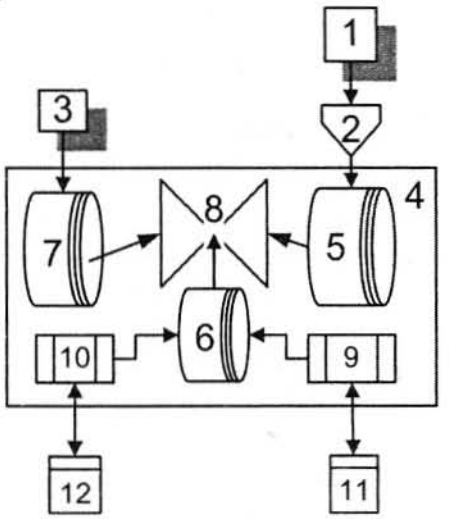

Рис. 1. Функціональна схема роботи апаратно-програмного генератора випадкових чисел:
1 – джерело шуму; 2 – АЦП; 3 – рідер ключа-аутентифікатора; 4 – контролер; 5 – пул шумової послідовності; 6 – пул псевдовипадкових даних з портів вводу-виводу; 7 – пул послідовностей ключа-аутентифікатора; 8 – криптогенератор; 9 – порт вводу-виводу для роботи з флеш-пам'яттю; 10 – порт вводу-виводу для роботи з USB-пристроями; 11 – флеш-пам'ять; 12-USB-порт ПК

Отже, наповнення пулів 5 і 7 є найменш ресурсо затратним, оскільки вони прості накопичувальні сховища, а пул 6 наповнюється за алгоритмом отримання псевдовипадкових даних. Вибірка даних із пулів виконується циклічним рахівником.

У роботі [1, 185] на основі аналізу існуючих алгоритмів генерації шумів обгрунтовано використання алгоритму шифрування AES в режимі CTR з 256 бітними ключами (AES-256) як бази для побудови криптогенераторів, крім того, при передачі даних від портабельного пристрою до комп'ютера доцільно використовувати протокол передачі даних з підвищеним ступенем захисту інформації (ППДПСЗІ).

Розглянемо вимоги до швидкості і обчислювальної стійкості роботи алгоритму. Загальна формула, що визначає кількість блоків, які можна зашифрувати одним ключем до першого повтору блока, наступна [1, 101]:

$$N_B \approx 2^{n/2},$$

де n – розмір блока шифру, який для алгоритму AES дорівнює 128 бітам. Відповідно $N_B = 2^{16}$ байт = 32 МБ. Ймовірність повтору блоку буде дорівнювати 2^{-97}, що вимагатиме від супротивника виконання 2^{113} операцій шифрування на контролері [1, 186].

Швидкість передачі даних за протоколом USB 1.1 становить 12 МБ/с. Для ППДПСЗІ розмір блока становить 20 байт. Виконання 2^{113} кроків займе $2^{113}/(12 \cdot 2^{20}/20) \approx 1{,}38 \cdot 10^{28}$ с $\approx 4{,}4 \cdot 10^{20}$ років для визначення внутрішнього стану генератора випадкових чисел. Зазначимо, що строк експлуатації сучасних обчислювальних пристроїв не перевищує 3–5 років. Отже, використання алгоритму AES-256 CTR для генерування випадкових чисел забезпечує необхідний рівень обчислювальної стійкості.

З точки зору передачі даних справедливою є наступна нерівність:

$$v_{пул} >> v_{ген} >> v_{тр},$$

де $v_{пул}$ – швидкість наповнення пулів;

$v_{ген}$ – швидкість роботи генератора випадкових чисел;

$v_{тр}$ – швидкість транзакцій між хост-комп'ютером і флеш-накопичувачем.

Розрахуємо необхідну швидкість роботи генератора випадкових чисел. Протокол ППДПСЗІ передбачає виконання логічної операції XOR над 20-байтовим пакетом даних і випадковими ключами, створеними криптогенератором. Тому на один пакет даних від ППДПСЗІ криптогенератор AES-256 CTR повинен видати два 16-байтних блоки.

Припустимо, що швидкість транзакцій наближається до швидкості USB-протоколу 1.1, і тоді маємо, що швидкість роботи криптогенератора має бути більшою за 24 МБ/с. Таким чином, отримана швидкість роботи криптогенератора визначає вибір контролера за обчислювальною потужністю.

Розглянемо шуми реальних компонентів електричних кіл, які можуть бути основою для побудови генератора випадкових чисел.

Шуми електронних пристроїв [5, 143] – це небажані випадкові коливання (флуктуації) токів, напруг, напруженостей електромагнітного поля, причиною яких є різні фізичні явища і які мають складну часову та спектральну структуру. У підсилювальних пристроях можуть виникати декілька типів шумів, але є три типи стохастичних процесів, порівняно потужніші за інші: шум Джонсона, шум Шоттки, фліккер-шум. Значення перелічених шумів можуть бути використані як вхідні дані для криптографічного алгоритму генерації випадкових чисел.

В той же час результуючий розподіл густини імовірності шумів у більшості електронних кіл має нормальний (гауссівський), а не рівномірний розподіл, а тому вони не можуть бути безпосередньо використані для побудови криптографічного генератора випадкових чисел.

Для отримання некорельованої послідовності з рівномірним законом розподілу можна

використати методи декореляції і рандомізації [6–8].

Розглянемо функціональні залежності для трьох стохастичних процесів [9, 2].

Шум Джонсона (тепловий шум) зумовлено рухом зарядів під дією енергії оточуючого середовища. Тепловий шум генерується як провідниками, так і напівпровідниками. Ефективне значення напруги шуму Джонсона дорівнює [9, 2]:

$$\overline{E_J^2} = 4kTR\Delta f, \qquad (1)$$

де $\overline{E_J^2}$ – середнє квадратичне значення напруги шуму;

k – постійна Больцмана;

T – температура оточуючого середовища в градусах Кельвіна;

Δf – частотний діапазон (смуга пропускання підсилювача).

Шум Шоттки (дробовий шум) є наслідком нерівномірного руху електронів через перетин провідника або напівпровідника при підключенні його до джерела струму. Ефективне значення напруги шуму Шоттки дорівнює [9, 2]:

$$E_S = kT\sqrt{\frac{2\cdot\Delta f}{q\cdot I}},$$

де I – середнє значення постійного струму кола;

$q = 1{,}6\cdot10^{-19}$ [Кл] – заряд електрона.

Фізичною причиною *фліккер-шуму* (*1/f*-шум) вважають варіації швидкості руху електронів і дірок через перетин напівпровідника, обумовлені дефектами його виробництва. У роботі [9, 7] показано, якщо смуга пропускання пристрою перевищує три декади і більше частоти перегину спектра, де значення білого шуму і фліккер-шуму рівні, значенням фліккер-шуму можна знехтувати (як у випадку, що розглядається нижче).

Існує багато варіантів аналогових схем генератора шуму. На думку авторів, для випадку побудови криптогенераторів на базі USB флешнакопичувачів раціональним є використання резистивного джерела теплового шуму, що підсилюється широкосмуговим операційним підсилювачем (ОП). Така схема має високу стабільність робочої точки, яка в ОП захищена від коливань напруги і, відповідно, може забезпечити регулярний потік випадкових даних із нормальним розподілом на відміну від дешевших транзисторних схем.

Оскільки в стандартних аналого-цифрових перетворювачів (АЦП) вхідна напруга має бути позитивною величиною, то використаємо неінвертовну схему вмикання ОП [10, 18] (рис. 2).

Коефіцієнт підсилення схеми з неінвертовним вмиканням ОП розраховують за формулою [10, 19]

$$K_C = \frac{R_4}{R_3} + 1. \qquad (2)$$

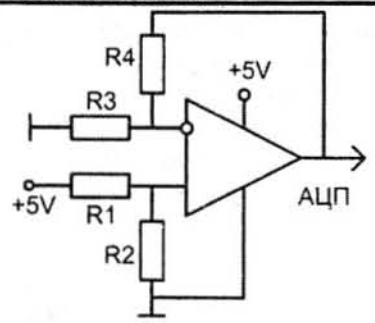

Рис. 2. Принципова електрична схема неінвертовного вмикання ОП

Мінімальне значення суми обмежується вихідним струмом ОП, величини якого має вистачати навантаженню. Звичайно ця сума становить від 50 кОм до 1 МОм.

Наведемо приклад розрахунків основних параметрів підсилювача шумів на базі ОП OPA301 ($K = 10^5$, $\Delta f_{ОП} = 150$ МГц) і АЦП ADS831 ($f_{АЦП} = 80$ млн відліків за секунду, $Umin = 1{,}5$ [В], $Umax = 3{,}5$ [В]) фірми Texas Instruments:

$$E_J = \sqrt{4\cdot1{,}38\cdot10^{-23}\cdot298\cdot10^7\cdot1{,}5\cdot10^8} \approx 0{,}005\ [\text{В}].$$

Напруга живлення від USB-порту становить $E = 5$ [В]. Тоді струм I, що протікає через опори R_1 і R_2:

$$I = \frac{E}{R_1 + R_2} = \frac{5}{10^7 + 1{,}2\cdot10^4} \approx 5{,}0\cdot10^{-7}\ [\text{А}],$$

$$E_S = 1{,}38\cdot10^{-23}\cdot298\cdot\sqrt{\frac{2\cdot1{,}5\cdot10^8}{1{,}6\cdot10^{-19}\cdot5\cdot10^{-7}}} \approx 2{,}5\cdot10^{-4}\ [\text{В}].$$

Відповідно, сумарне значення шуму

$$E_{ШΣ} = E_J + E_S = 5\cdot10^{-3} + 2{,}5\cdot10^{-4} \approx 0{,}005\ [\text{В}].$$

Різниця U_{ADC} між максимальним і мінімальним значеннями вхідної напруги для АЦП ADS831 дорівнює 2 [В]. Тоді необхідний коефіцієнт підсилення кола (рис. 2) дорівнює:

$$K_C = \frac{U_{ADC}}{E_{ШΣ}}.$$

Відповідно, значення другого опору кола зворотного зв'язку ОП (рис. 2) визначимо за формулою (2):

$$R_3 = \frac{R_4}{(K_C - 1)} = \frac{2\cdot10^4}{(400 - 1)} \approx 500\ [\text{Ом}].$$

Розрахуємо значення опорів R_1, R_2, що задають опорну напругу на вході АЦП:

$$U_{АЦП}^{O} = Umin + U_{ADC}/2 = 2{,}5\ [\text{В}].$$

Тоді значення опорної напруги на вході ОП становить:

$$U_o^{BX} = U_{АЦП}^{O} / K_C = 2{,}5/400 = 0{,}00625\ [\text{В}].$$

Для того щоб збільшити рівень шуму Джонсона (1), значення першого опору дільника було вибрано великим – $R_1 = 10$ [МОм].

Значення опору R_2 (рис. 2) визначаємо з рівняння

$$U_O^{BX} = E\frac{R_2}{R_1 + R_2}.$$

Звідки отримуємо $R_2 = 10^7/799 \approx 12$ [КОм].

Представлені розрахунки компонентів широкосмугового підсилювача шумів доводять, що пристрій може бути виконаний у вигляді гібридної інтегральної мікросхеми і конструктивно розміщений у корпусі флеш-накопичувача з USB-інтерфейсом.

Описаний криптогенератор є основою для побудови протоколу ПДПСЗІ для USB флеш-накопичувачів. Алгоритм роботи ППДПСЗІ передбачає виконання наступних кроків:

1. Клієнт відправляє серверу свій ідентифікатор – несекретне число (ID), яке відповідає пристрою у базі даних (БД) сервера.
2. Сервер знаходить ID клієнта у БД і зчитує з неї секретний код клієнта. Якщо ідентифікатор відсутній у БД, то обробка запиту припиняється.
3. Сервер генерує сесійний ключ (*KS*). Сесійний ключ – це секретний код, який генерує сервер і використовує протягом усіх транзакцій замість клієнтського секретного коду (*SCk*).
4. Сервер генерує ініціальний транзакційний ключ (KT_0). Транзакційний ключ – це секретний ключ, який генерується сервером для передачі кожного пакета даних (транзакції) (рис. 3). Ініціальний транзакційний ключ розраховується сервером як хеш-функція від секретного коду клієнта:

$$KT_0 = hesh(SCk).$$

Адреса
Ключі обміну даними (Auth)
Хеш-сума даних
Розмір пакета
Поле даних або команд

Рис. 3. Структура пакета обміну даними протоколу ПДПСЗІ

5. Сервер виконує логічну операцію *XOR* над сесійним і тразакційним ключами і відправляє результат у пакеті даних клієнту (поле ключів обміну даними):

$$Auth = XOR(KT_0, KS).$$

6. Ініціальний транзакційний ключ (KT_0) розраховується клієнтом. Клієнт виймає сесійний ключ з пакета, відправленого сервером.

$$KS = XOR(Auth, KT_0).$$

7. Клієнт відправляє серверу пакет з командою "Підтвердження отримання ключа".
8. Сервер генерує новий транзакційний ключ (KT_i), виконує операцію *XOR* з KT_0, а потім розраховує *XOR* із сесійним ключем *KS*.

$$Auth=XOR(KT_i, KS).$$

9. Пакет даних шифрується новим транзакційним ключем і відправляється клієнту.
10. Клієнт виймає новий транзакційний ключ, шифрує ним пакет даних і відправляє його серверу.

Потім виконується повтор кроків 4–10 до закінчення сеансу обміну даними між флеш-накопичувачем і комп'ютером. Очевидно, що отриманий алгоритм дозволяє встановити захищений канал передачі даних між периферійним пристроєм та хост-ПК за допомогою невеликої кількості простих логічних операцій. Отже, протокол є раціональним і може бути реалізованим на недорогих серійних мікроконтролерах.

Для того щоб довести результативність алгоритму, побудуємо формалізовану модель подій і умов, що виникають при його роботі: Результат представимо у вигляді графа мережі Петрі (рис. 4).

Умови

1) Клієнт відправив серверу ID (p_0).
2) ID знайдено у БД (p_1).
3) Сервер відправив *Auth* у пакеті даних (p_2).
4) Клієнт відправляє серверу пакет з командою "Підтвердження отримання ключа" або "Продовження захищеного обміну даними" (p_3).
5) Сервер відправляє KT_i (p_4).
6) Сервер відправляє пакет даних зашифрований KT_i (p_5).
7) Зашифрований KT_i пакет відправлений клієнтом серверу (p_6).
8) Пристрій підключено (p_7).
9) Обмін ключами, даними і командами завершено (p_8).

Події

1) Пуск (t_0).
2) Пошук ID клієнта в БД сервера (t_1).
3) Сервер генерує *KS*. KT_0, розраховує *Auth* (t_2).
4) Клієнт розраховує KT_0, витягає KS (t_3).
5) Сервер генерує KT_i, розраховує *Auth*, шифрує KT_i пакет даних (t_4).
6) Клієнт виймає новий KT_i, шифрує ним пакет даних і відправляє серверу (t_5).
7) Сервер верифікує статус підключення пристрою та продовжує цикл обміну даними (t_6).
8) Початок нового циклу передачі даних клієнтом та видача команди "Продовження захищеного обміну даними"(t_7).
9) Зупинка процесу обміну ключами і даними (t_8).
10) Обробка події спроби підключення до серверу з невірним ID (t_9).

11) Вихід (t_{10}).

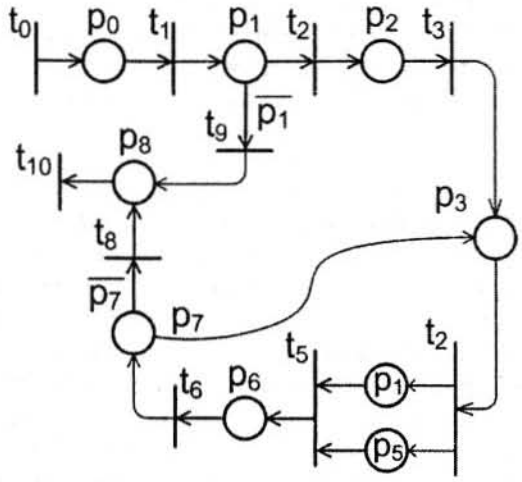

Рис. 4. Граф мережі Петрі для ППДПСЗІ

Таким чином, алгоритм ППДПСЗІ є майже класичним кінцевим автоматом.

Висновки

1) Запропоновано апаратно-програмний криптогенератор випадкових чисел на базі слабострумних електронних кіл.
2) Сформульовано технічні вимоги до швидкості роботи підсистем криптогенератора і обчислювальних алгоритмів, виконання яких необхідно для систем захисту інформації на основі стандартних протоколів передачі даних. Наведено приклад таких розрахунків для USB-протоколу версії 1.1.
3) Побудовано формалізовану модель роботи протоколу передачі даних з підвищеним ступенем захисту інформації між ПК і флеш-накопичувачем. Результат представлено у вигляді графа мережі Петрі.
4) На основі аналізу моделей стохастичних процесів широкополосного підсилювача з резистивним навантаженням показано, що шум Джонсона має найбільшу дисперсію порівняно із шумами Шотткі і фліккер-шумом. Тому залежність для шуму Джонсона було покладено в основу розрахунку електричного кола підсилювача.
5) Розроблено функціональну схему роботи контролера, який забезпечується потоком даних з трьох джерел випадкових і псевдовипадкових даних для формування криптографічностійких випадкових послідовностей.

ЛІТЕРАТУРА

1. Фергюсон Н., Шнайер Б. Практическая криптография: Пер. с англ. – М.: Издательский дом "Вильямс", 2005. – 424 с.: ил.
2. Столлингс В. Криптография и защита сетей: принципы и практика. – 2-е изд.: Пер. с англ. – М.: Издательский дом "Вильямс", 2001. – 672 с.: ил.
3. Гук М.Ю. Шины USB и FireWire. Энциклопедия. – С.Пб.: Питер, 2005. – 540 с.: ил.
4. Корольов В.Ю., Поліновський В.В., Малікова О.В. Побудова системи захисту інформації на базі персоналізованого USB-флеш з використанням ключа-ідентифікатора // Вісник Хмельницького національного університету. – 2008. – № 3. – С. 175–181.
5. Радіотехніка: Енциклопедичний навчальний довідник: Навч. посіб. / За ред. Ю.Л. Мазора, Є.А. Мачуського, В.І. Правди. – К.: Вища школа, 1999. – 838 с.: іл.
6. Пат. 41079 Україна, МПК G 06 F 7/78. Спосіб рандомізації послідовності конгруентних чисел / Т.В. Мітянкіна, В.В. Швидкий, В.В. Щерба, А.І. Щерба, М.О. Мітянкін. – № U2008080187; Заявл. 17.06.2008; Опубл. 12.05.2009, Бюл. 17.
7. Пат. 40649 Україна, МПК G 06 F 7/58. Пристрій декореляції випадкової послідовності / Т.В. Мітянкіна, В.В. Швидкий, М.О. Мітянкін. – № U200811384; Заявл. 22.09.2008; Опубл. 27.04.2009, Бюл. № 8.
8. Митянкина Т.В., Швыдкий В.В., Щерба А.И. Рандомизация последовательности конгруэнтных чисел // Вестник Инженерной академии Украины. – 2008. – №2. – С. 107–111.
9. Texas Instruments Application Report, Noise Analysis in Operational Amplifier Circuits, SLVA043A, 1999.
10. Фолкенберри Л. Применения операционных усилителей и линейных ИС: Пер. с англ. – М.: Мир, 1985. – 572 с.: ил.

Корольов В.Ю., к.т.н., с.н.с., завідувач відділу ПМПТОТ Центру таймерних обчислювальних систем Інституту кібернетики ім. В.М. Глушкова НАНУ.

Поліновський В.В., с.н.с., Центр таймерних обчислювальних систем Інституту кібернетики ім. В.М. Глушкова НАНУ.