

УДК 004.421.5:004.942
DOI: 10.31891/2219-9365-2020-66-2-16

ОРЛЕНКО В. С., ЧЕШУН В. М., АНДРОЩУК О. С.
Хмельницький національний університет
КАТАЄВА А. І.
Донецький національний університет імені Василя Стуса

МОДЕЛЬ ГЕНЕРАТОРА КРИПТОКЛЮЧІВ З ДЖЕРЕЛАМИ ЕНТРОПІЇ ДЛЯ СИСТЕМИ КЛІЄНТ-БАНК

Однією із важливих складових безпеки системи клієнт-банк є механізми захисту, що базуються на використанні криптоключів. Стійкість криптоключів є запорукою надійності системи і, в свою чергу, базується на механізмах генерації псевдовипадкових чисел із застосуванням джерел первинної ентропії, для ефективного використання яких необхідною є наявність адекватних моделей і математичного апарату.

У роботі представлено елементи математичної моделі джерел ентропії і узагальнену графічну модель процесу генерації псевдовипадкових двійкових кодів, які орієнтовані на реалізацію генератора криптоключів для системи клієнт-банк з використанням одного або декількох джерел первинної ентропії. Описано особливості реалізації основних етапів процесу генерації криптоключів підвищеної ентропії та надані рекомендації щодо використання функцій математичної моделі, доведено адекватність запропонованих моделей вирішуваним задачам.

Моделі орієнтовані на реалізацію методу та засобів генерації псевдовипадкових чисел підвищеної ентропії і можуть бути застосовані для зменшення ризиків отримання несанкціонованого доступу до клієнтської інформації в системі клієнт-банк через розкриття криптоключів. В якості джерел ентропії можуть бути використані датчики мобільного телефона або інші пристрої та явища, які характеризуються здатністю формувати пул значень з високим рівнем ентропії.

Ключові слова: система клієнт-банк, криптографічний ключ, генератор псевдовипадкових чисел, ентропія.

ORLENKO V., CHESHUN V., ANDROSHCHUK O.
Khmelnitskyi National University
KATAIEVA A.
Vasyl' Stus Donetsk National University

MODEL OF CRYPTOGRAPHIC KEYS GENERATOR WITH ENTROPY SOURCES FOR THE CLIENT-BANK SYSTEM

One of the important components of the security of the client-bank system is the protection mechanisms based on the use of cryptographic keys. The stability of cryptographic keys is a guarantee of system reliability and, in turn, is based on the mechanisms of generating pseudo-random numbers using primary entropy sources, for the effective use of which it is necessary to have adequate models and mathematical apparatus.

The paper presents elements of the mathematical model of entropy sources and a generalized graphical model of the process of generating pseudo-random binary codes, which are focused on the implementation of the cryptographic keys generator for the client-bank system using one or more primary entropy sources. Peculiarities of realization of the main stages of the process of generating cryptographic keys of high entropy are described and recommendations on the use of functions of the mathematical model are given, the adequacy of the offered models to the solved problems is proved.

The models are focused on the implementation of the method and means of generating pseudo-random numbers of high entropy and can be used to reduce the risk of unauthorized access to customer information in the client-bank system through the disclosure of cryptographic keys. Mobile phone sensors or other devices and phenomena, that are characterized by the ability to form a pool of values with a high level of entropy, can be used as sources of entropy.

Keywords: client-bank system, cryptographic key, pseudo-random number generator, entropy.

Вступ і загальна постановка проблеми. В сучасних умовах абсолютно неможливо уявити діяльність банківської системи України та світу без застосування засобів автоматизації, комп'ютеризації та інформатизації. Основою механізму автоматизованого надання послуг клієнтам банківських установ стала система клієнт-банк – комплекс програмно-апаратних засобів для забезпечення безпечної взаємодії між банком та клієнтом. Враховуючи масштабне вторгнення в сферу банківських послуг інтернет технологій і неможливість існування системи клієнт-банк без їх застосування, останню досить часто ідентифікують як систему електронного банкінгу (e-banking), онлайн-банкінгу (online banking), інтернет-банкінгу або веб-банкінгу [1, 2].

Загалом, систему клієнт-банк можна розглядати як комплекс сервісів і механізмів захисту, які орієнтовані на забезпечення максимальної зручності і безпеки роботи клієнтів з системою.

На прикладі системи «iBank 2 UA» [2, 3] до типових сервісів системи клієнт-банк можна віднести різні види організації доступу до банківських послуг:

- з персонального комп'ютера через пряме з'єднання з банківською мережею (PC banking);
- з телефону в режимі телефонного зв'язку (Phone banking);
- з мобільного телефону клієнта із застосуванням SMS-повідомлень (SMS-банкінг);

– з мобільного телефону із застосуванням спеціалізованих протоколів безпроводної передачі даних WAP GPRS (WAP-банкінг);

– з мобільного телефону із застосуванням спеціального додатку мобільного банкінгу (Mobile-банкінг);

– із застосуванням ресурсів мережі Інтернет (Internet-банкінг, WEB-банкінг, Online-банкінг) тощо.

Для захисту сервісів системи [3–5] використовуються механізми електронного цифрового підпису, хеш функцій, розповсюдження ключів сесії із застосуванням алгоритмів асиметричного шифрування, симетричне шифрування та захищений протокол передачі і автентифікації.

Більшість із зазначених механізмів базується на використанні криптоключів (ключів сесії, ключів підпису тощо), для генерації яких використовуються різні способи і засоби генерації псевдовипадкових чисел як основа забезпечення випадковості, непередбачуваності і криптостійкості значень криптоключів. Це робить систему клієнт-банк як об'єкт захисту в умовах існування ризиків та загроз банківській діяльності в кіберпросторі значною мірою залежною від якості і зручності застосовуваних генераторів криптоключів, що зумовлює актуальність і підвищену зацікавленість у розробці ефективних методів та засобів генерації криптоключів підвищеної ентропії.

Аналіз стану досліджень та публікацій. Генерація криптоключів системи клієнт-банк базується на використанні псевдовипадкових чисел та засобів їх генерації.

Генератори псевдовипадкових чисел (ГПВЧ) набули широкого застосування в різноманітних технічних задачах [6], що зумовило появу великої кількості методів та засобів генерації випадкових і псевдовипадкових чисел. В засобах банківської безпеки, зокрема, випадкові числа широко застосовуються в схемах взаємної аутентифікації. У більшості сценаріїв аутентифікації й розподілу ключа для запобігання атак повторного відтворення (replay-атак) використовуються одноразові коди *ponces* (від англійського «*number that can only be used once*» – число, яке може бути використане один раз). Застосування дійсно випадкових чисел у якості кодів *ponces* не дає супротивникові можливості обчислити або вгадати їх значення.

Генерація якісної випадкової послідовності чисел – найскладніша частина багатьох криптографічних операцій [6].

Спеціалізовані криптографічно сильні ГПВЧ в якості джерел ентропії використовують радіоактивний розпад, фізичні явища оптично-квантової механіки, електричні шуми [7–9]. Хоча подібні ГПВЧ і дають якісні характеристики ентропії послідовності чисел, для масового використання в системах типу клієнт-банк вони не є зручними і доступними.

Базисом ГПВЧ електронних систем, як правило, є програмні або апаратні методи генерації та їх комбінації [6].

Програмні ГПВЧ базуються на певному методі генерації, реалізованому алгоритмічно. До алгоритмічних методів відносять [6,10]:

- метод середини квадрата Джона фон Неймана;
- метод лінійного конгруента Лехмера;
- підвиди алгоритмів Фібоначчі;
- алгоритм Блюма–Блюма–Шуба;
- вихор Мерсенна (генератор Мацумото і Нишимури) тощо.

Апаратні ГПВЧ представлені різноманітними моделями, серед яких можна виділити ряд базових [7, 10, 11]:

- генератори на регістрах зсуву з зворотним зв'язком (FSR);
- генератори на регістрах зсуву з лінійним зворотним зв'язком (LFSR);
- ГПВЧ Геффа;
- ГПВЧ «стій–рушай» («*stop-and-go*») тощо.

Хоча апаратні генератори і не передбачають програмної реалізації алгоритму, в генерованій послідовності чисел наявні залежності, які можуть бути описані алгоритмічно.

Наявність алгоритмічної залежності між числами (певного закону розподілу чисел) в псевдовипадкових послідовностях дозволяє говорити про їх випадковість і непередбачуваність лише в певному обмеженому аспекті, що зумовлює їх вразливість до методів криптоаналізу [7].

Окремий клас ГПВЧ утворюють криптографічні генератори [10, 12]:

- ГПВЧ з циклічним шифруванням;
- ГПВЧ із застосуванням режиму Output Feedback DES;
- ГПВЧ генератор ANSI X9.17 тощо).

Робота криптографічних ГПВЧ базується на методах та алгоритмах сучасної криптографії. Надійність криптографічних ГПВЧ забезпечується не лише набором і послідовністю криптографічних операцій, а і вибором стартових значень (вектор ініціалізації, майстер-ключ), з яких починається виконання цих операцій. Стартові значення для запуску алгоритму генерації криптографічного ГПВЧ формуються із застосуванням явищ або засобів, оцінювані параметри яких можуть розглядатися як випадкові. Зазначені

явища та засоби використовуються для збільшення ентропії генерованих в різних сеансах послідовностей чисел і розглядаються як джерела первинної ентропії ГПВЧ [6, 7, 13].

До джерел первинної ентропії, що використовуються в роботі систем клієнт-банк, відносяться специфічні властивості технічних засобів безпосередньо або у взаємодії з людиною: показники системного годинника, специфічні особливості набору на клавіатурі або роботи з «мишею», параметри локальної або глобальної комп'ютерної мережі, параметри інтегрованих компонентів системи, зміни часу доступу до жорсткого диску тощо [6, 14]. В [6] також зазначається, що такі джерела мають недостатню ентропію і низьку продуктивність, що унеможливає використання їх як ГПВЧ безпосередньо, але дозволяє їх розглядати як слабких криптографічно джерел первинної ентропії.

Стрімке вторгнення на ринок банківських послуг мобільного банкінгу створює не лише нові загрози, але і нові можливості. Зокрема, в [15, 16] описується технологія застосування датчиків мобільних пристроїв в якості ГПВЧ.

Аналіз специфіки роботи датчиків мобільних пристроїв, характерна змінюваність складу датчиків між моделями та різна їх продуктивність – сукупність факторів, які не дозволяють розглядати зазначені датчики як стабільні і високопродуктивні генератори криптоключів системи клієнт банк. В той же час, отримані в ході аналізу результати надають можливість висунення гіпотези про перспективність їх використання в якості ефективних джерел первинної ентропії.

Формулювання цілі статті. Для якісного розв'язування задачі генерації криптоключів системи клієнт-банк із застосуванням датчиків мобільних пристроїв в якості джерел первинної ентропії, в умовах надзвичайно високої складності застосовуваних алгоритмів і методів, великої актуальності набуває вибір математичної моделі для формалізованого представлення даних і ефективної організації їх обробки.

Базові елементи моделі джерел ентропії. Для отримання якісного криптографічного генератора псевдовипадкових чисел необхідне виконання ряду умов [6, 12]:

- наявність джерела первинної ентропії;
- визначення способу формування числового представлення вимірюваних параметрів джерела первинної ентропії;
- алгоритм обробки, перетворення і накопичення даних, що містять ентропію;
- спосіб формування послідовності чисел із якісними показниками випадковості на основі даних первинної ентропії.

Для отримання джерела первинної ентропії з достатніми характеристиками невизначеності в формованому цифровому значенні, яке стане основою для генерації псевдовипадкових векторів двійкового коду, першочергово необхідно мати інструментарій кількісної оцінки ентропії джерела.

Мінімальна ентропія $H_{\min}(X)$ характеризує найгірший з можливих варіантів невизначеності щодо об'єкта X : якщо об'єкту X властива мінімальна ентропія h , то імовірність появи певного значення (будь-якого з можливих) не перевищує 2^{-h} .

Припустимо, що q_i – цифрове представлення отриманого від джерела ентропії вектора. Утворимо множину отримуваних від джерела ентропії значень:

Qдж.: $\{q_1, q_2, \dots, q_i, \dots, q_r\}$ – множина вихідних значень з джерела ентропії, представлених в цифровому вигляді.

В багатьох реалізаціях ГПВЧ для збільшення ентропії самого генератора використовується одразу декілька джерел початкової ентропії. Якщо умовно прийняти, що таких джерел для реалізації ГПВЧ застосовано в кількості n , то вони утворюють множину джерел ентропії:

$D: \{d_1, d_2, \dots, d_j, \dots, d_n\}$ – множина використовуваних джерел ентропії (датчиків мобільного пристрою).

За таких умов різноманіття вихідних значень з джерел ентропії можна описати сукупністю множин:

Qдж.1: $\{q_{1.1}, q_{1.2}, \dots, q_{1.i}, \dots, q_{1.p}\}$ – множина представлених в цифровому вигляді векторів вихідних значень з першого джерела ентропії;

Qдж.2: $\{q_{2.1}, q_{2.2}, \dots, q_{2.i}, \dots, q_{2.p}\}$ – множина представлених в цифровому вигляді векторів вихідних значень з другого джерела ентропії;

...

Qдж.j: $\{q_{j.1}, q_{j.2}, \dots, q_{j.i}, \dots, q_{j.p}\}$ – множина представлених в цифровому вигляді векторів вихідних значень з j -го джерела ентропії ($1 < j < n$);

...

Qдж.n: $\{q_{n.1}, q_{n.2}, \dots, q_{n.i}, \dots, q_{n.p}\}$ – множина представлених в цифровому вигляді векторів вихідних значень з n -го джерела ентропії.

Неважко побачити, що при $n=1$ наведена модель зведеться до початкового опису множини вихідних значень з єдиного джерела ентропії. Таким чином, при розгляді задачі створення ГПВЧ доцільно використовувати модель з n джерелами ентропії, окремим варіантом реалізації якої є модель з єдиним джерелом ентропії при $n = 1$.

Для кожного значення $q_{j,i} \in Q_{дж,j}$ можна визначити статистичну імовірність $p(q_i)$ того, що воно буде отримане від джерела в будь-якій операції зчитування вектора даних з джерела ентропії.

Таким чином, ми можемо сформувати множину статистичних даних імовірності отримання різноманітних значень показників датчиків:

$Q_{дж,j}: \{p(q_{j,1}), p(q_{j,2}), \dots, p(q_{j,i}), \dots, p(q_{j,m})\}$ – множина імовірнісних характеристик появи вихідних значень $q_{j,i} \in Q_{дж,j}$ з j -го джерела ентропії ($1 \leq j \leq n$).

За таких умов мінімальна ентропія джерела $Q_{дж,j}$ буде визначатися за формулою:

$$H_{\min}(Q_{дж,j}) = \min(-\log_2 p(q_{j,i})) = -\log_2(\max p(q_{j,i})) \quad (1)$$

У ідеального джерела ентропії імовірності появи всіх значень $q_{j,i} \in Q_{дж,j}$ мають бути однаковими:

$$p(q_{j,i}) = p(q_{j,k}) \quad \forall (q_{j,i} \in Q_{дж,j}, q_{j,k} \in Q_{дж,j}, i \neq k). \quad (2)$$

Умова (2) описує ідеальне джерело ентропії за показниками імовірності отримання різних значень за умови, що вказані значення $q_{j,i} \in Q_{дж,j}$ не є взаємозалежними. На основі (1) і (2) може бути здійснено відбір якісних джерел ентропії і відсів слабких джерел.

Основою джерела ентропії є джерело шуму – певний елемент або явище, що характеризується недетермінованою характеристикою, яка задає ентропію і відповідає за невизначеність значень $q_{j,i} \in Q_{дж,j}$. Якщо джерело шуму i , як наслідок, утворюване ним джерело ентропії неякісні, жоден механізм ГПВЧ не зможе компенсувати брак ентропії.

Класичне джерело ентропії формує випадкові значення у вигляді цифрових векторів, отриманих з недетермінованого процесу. Якщо використовуваний недетермінований процес джерела шуму не формує одразу цифрові вектори, а видає певні аналогові різновиди досліджуваного сигналу, процедура формування зазначених векторів включає операцію оцифровування (дискретизації).

В ідеалі значення, отримувані від джерела шуму, повинні бути представлені двійковими кодами (векторами двійкових кодів) однакової розрядності, яка визначається потребами реалізації методу генерації псевдовипадкових чисел.

До джерел ентропії висувається ряд вимог [8, 16], які, з урахуванням елементів моделі, можна уточнити:

- вихідні вектори $q_{j,i} \in Q_{дж,j}$ повинні бути незалежними і не підпорядковуватись законам, що можуть бути описані алгоритмічними процедурами будь-якої складності;
- джерело ентропії має бути зручним у використанні за призначенням;
- джерело ентропії повинно бути придатним до випробувань на функціональність;
- процес зняття вихідних значень $q_{j,i} \in Q_{дж,j}$ не повинен впливати на загальну роботу джерела;
- джерело ентропії повинне бути незалежним від зовнішніх факторів і впливів.

Модель процесу генерації псевдовипадкових двійкових векторів підвищеної ентропії.

Робочий процес генерації випадкових значень згідно з наведеними описами і отриманими в ході досліджень результатами можна розділити на послідовні етапи:

- первинне отримання показників датчиків $q_{j,i} \in Q_{дж,j}$;
- виділення з коду векторів $q_{j,i} \in Q_{дж,j}$ розрядів, що несуть максимальну ентропійну складову;
- перетворення векторів $q_{j,i} \in Q_{дж,j}$ в вектор двійкового коду фіксованої розрядності, необхідної для реалізації криптографічного методу генерації псевдовипадкових чисел;
- реалізація криптографічного методу генерації псевдовипадкових чисел.

Для математичного опису процесу генерації псевдовипадкових значень введемо позначення перелічених функцій перетворення ентропійних шумів:

F1 – оператор отримання показників датчиків (операція аналого-цифрового перетворення при використанні аналогових датчиків тощо);

F2 – оператор виділення з вектора (векторів) цифрового коду розрядів, що несуть максимальну складову ентропії;

F3 – функція перетворення складових векторів з виходу функції F2 в єдиний вектор з максимальним збереженням ентропійних властивостей, отримуваних від джерел ентропії;

F4 – оператор перетворення вектора з виходу функції F3 в вектор двійкового коду фіксованої розрядності, необхідної для реалізації криптографічного методу генерації псевдовипадкових чисел;

F5 – функція криптографічного методу генерації псевдовипадкових чисел (криптоключів тощо).

За наведеним переліком і описом операцій розроблено узагальнену графічну модель роботи генератора (рис. 1).

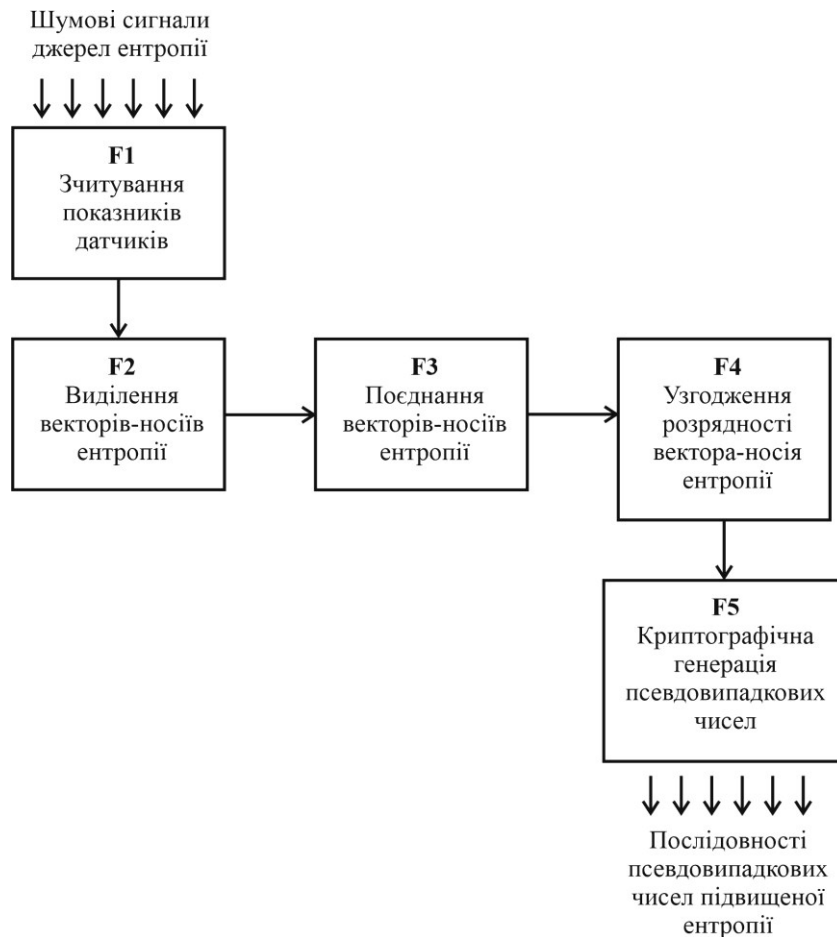


Рис. 1. Узагальнена модель процесу генерації псевдовипадкових чисел підвищеної ентропії

Три рівні наведеної на рис. 1 моделі відповідають розподілу функцій F1–F5 за загальним цільовим призначенням:

- перший рівень представлений функцією F1 і відповідає за сприйняття даних від джерела ентропії і представлення їх у формі, придатній для обробки цифровими програмно-апаратними системами, до числа яких відноситься і система клієнт-банк;

- другий рівень представлений групою функцій F2–F4 і відповідає операціям перетворення початкових цифрових даних, сформованих за недермінованими сигналами від джерела ентропії функцією F1, з метою отримання формату їх представлення, потрібного для реалізації обраного криптографічного алгоритму генерації псевдовипадкових значень;

- третій рівень представлений функцією F5 і відповідає етапу реалізації обраного криптографічного алгоритму генерації псевдовипадкових значень на основі вхідних даних підвищеної ентропії.

Слід відзначити абсолютну значимість всіх перелічених етапів для отримання якісного результату від робочого процесу ГПВЧ.

Дослідимо особливості реалізації кожного етапу функціональних перетворень за наведеною на рис. 1 блок-схемою з метою вироблення рекомендацій щодо реалізації методу генерації псевдовипадкових чисел підвищеної ентропії для системи клієнт-банк.

На першому етапі шумові сигнали від джерел ентропії, як основні носії зазначеної ентропії, проходять процедуру зчитування показників датчиків, а за потреби – процедуру аналого-цифрового перетворення сигналів з аналогових датчиків (дискретизації) з метою зручності їх подальшої обробки в цифровому вигляді (вхідних векторів-носіїв ентропії). Особливості функції аналого-цифрового перетворення залежать від характеру використовуваного в якості джерела ентропії явища і застосовуваних методів (засобів) перетворення характеристик цього явища в цифрові вектори-описи.

Оскільки на даному етапі джерела ентропії нами ще не ідентифіковано, можна сформулювати лише загальні вимоги щодо реалізації функції аналого-цифрового перетворення F1.

В першу чергу, функція аналого-цифрового перетворення F1 повинна мати достатню чутливість для збереження властивостей ентропії вхідного шумового сигналу у його описах векторами двійкових кодів, тобто, крок дискретизації функції аналого-цифрового перетворення F1 повинен забезпечувати необхідну

точність вимірювання оцінюваного параметра перетворюваного аналогового сигналу в квантовані моменти часу i , як наслідок, точні відображення оцінюваного параметра перетворюваного аналогового сигналу в цифровому представленні.

Операція первинного перетворення аналогового сигналу від джерел ентропії в вектор цифрового коду є традиційною і полягає в дискретизації аналогового значення недетермінованого шумового сигналу з метою отримання його цифрового представлення. Як і для дискретизації будь-якого аналогового сигналу, тут важливим є крок дискретизації і період квантування як передумова одержання якісного відображення властивостей початкового сигналу в його дискретному (цифровому) описі. Саме крок дискретизації визначає точність вимірювання оцінюваного параметра перетворюваного аналогового сигналу в квантовані моменти часу i , як наслідок, точність відображення оцінюваного параметра-носія ентропії перетворюваного аналогового сигналу в цифровому представленні.

Для дискретизації аналогового сигналу від джерела шуму як носія первинної ентропії ГПВЧ важливою є саме шумова зона сигналу з найбільшою ентропією. Це зумовлено тим, що більшість джерел шуму характеризуються неоднорідністю ентропійних характеристик сигналу в різних зонах. Так, наприклад, використовуваний в якості джерела ентропії для ГПВЧ шумовий діод має досить невелику зону вольт-амперної характеристики з непередбачуваною поведінкою сигналу, в той час як на інших ділянках поведінка сигналу в номінальному режимі є абсолютно передбачуваною і непридатною для використання в якості джерела первинної ентропії ГПВЧ.

З іншої сторони, крок дискретизації у відношенні до амплітуди зміни оцінюваного параметра перетворюваного аналогового сигналу безпосередньо визначає вимоги щодо розрядності цифрового вектора опису для однократного виміру. Якщо прийняти амплітуду рівною A , а крок дискретизації рівним Δa , то отримуємо кількість можливих відліків (допустимих оригінальних значень) перетворюваного сигналу:

$$K = \frac{A}{\Delta a}, \quad (3)$$

що визначає вимоги щодо розрядності двійкового коду вектора опису для кожного однократного виміру:

$$R = \log_2 \frac{A}{\Delta a} \quad (4)$$

Враховуючи наявність великої кількості цифрових датчиків, здатних одразу формувати достатньо точні оціночні вектори вимірюваних параметрів, з метою забезпечення максимальної зручності реалізації пропонуваного методу в системі клієнт-банк доцільно використовувати джерело ентропії, оснащене цифровими датчиками з потрібними властивостями для вимірювання використовуваних характеристик шумового сигналу як носія ентропії.

За наявності векторів цифрових описів шумового сигналу саме вони стають носіями складової ентропії цього сигналу.

Як зазначалося в попередньому описі функції F2, на етапі реалізації функції аналого-цифрового перетворення F1 не завжди виходить співставити актуальну для ГПВЧ зону найвищої ентропії сигналу з зоною дискретизації, тому отримувані з F1 вектори-носії ентропії, в більшості випадків, складаються з розрядів, що містять різне навантаження за ентропією. Наприклад, якщо джерело ентропії базується на вимірюванні температури зовнішнього середовища, а для системи клієнт-банк, зокрема, таким середовищем можна вважати приміщення з системами клімат-контролю, то марно очікувати якісної ентропії в цілих розрядах показників датчика температури. Через це при реалізації функції F2 потрібно виділити з векторів цифрового коду саме ті розряди, що несуть максимальну складову ентропії.

Особливості функції F2 визначаються на підставі дослідження властивостей сигналу джерела ентропії за результатами, отримуваними після багатократного застосування функції первинного перетворення F1, із широкомасштабним застосуванням методів статистичного аналізу.

На даному етапі зарано говорити про застосування методів статистичного аналізу через відсутність статистичних даних для їх дослідження.

Результатом застосування функції F2 є множина векторів з складовою ентропії, отриманих перетвореннями на попередніх етапах сигналів від одного або декількох джерел ентропії. В багатьох випадках отримуваного з функції F2 одиничного вектора недостатньо для реалізації подальших операцій, що зумовлює потребу поєднання декількох таких векторів в одному без втрат або з мінімально допустимими втратами їх ентропійних властивостей. Для виконання відповідного синтезу єдиного вектора з вхідної множини векторів реалізується функція F3.

Стосовно функції F3 слід зазначити, що вона займає проміжне місце між функціями перетворення двійкових кодів F2 і F4 та є залежною від них, тому має бути узгодженою з ними.

Аналіз дозволяє визначити суть функцій F2–F4:

- F2 виділяє складову ентропії з векторів $qj.i \in Q_{dj.j}$;
- F3 поєднує ентропію декількох векторів $qj.i \in Q_{dj.j}$ в одному векторі;
- F4 має передати сумарну ентропію «універсального» вектора на вхід криптографічного алгоритму генерації псевдовипадкових значень в заданій розрядності, тобто, виконати стиснення «універсального» вектора до потрібної розрядності без втрат ентропійних властивостей.

Головне призначення функцій перетворення двійкових кодів F2–F4 – підготувати двійкові дані, що передають характеристики ентропії джерела, до передачі в криптографічний алгоритм генерації псевдовипадкових значень без втрат зазначених властивостей (з мінімізацією втрат).

Стосовно функцій перетворення-поєднання двійкових кодів F3 слід зазначити, що вона може бути реалізована математично або алгоритмічно, але обов'язково з орієнтацією на функцію стиснення F4.

Зазначимо, що в багатьох реалізаціях функцій перетворень F3 і F4 можуть поєднуватися між собою і тому не розглядаються окремо. При цьому слід також зазначити можливість поєднання і інших функцій з наведеного в моделі переліку.

Для оптимального вибору типу перетворення двійкових даних за функцією F3 проведемо аналіз вимог щодо функції стиснення F4.

Призначенням функції F4 є стиснення вектора двійкового коду великої розрядності до фіксованого розміру, необхідного для реалізації обраного криптографічного алгоритму генерації псевдовипадкових значень.

Узагальнюючи опис призначення функції F4 можна дати наступне тлумачення – стиснення вектора двійкового коду довільної розрядності до вектора двійкового коду фіксованої розрядності із збереженням ентропійних властивостей початкового значення.

Аналіз останнього опису вказує на однотипність задач функції F4 з задачами створення хеш-функцій.

Хеш-функції – функції, входним значенням яких є повідомлення довільної довжини, а вихідним значенням – повідомлення фіксованої довжини) [16, 17]. Хеш-функції володіють рядом властивостей, які дозволяють із високою ймовірністю визначати зміни входного повідомлення. Мета хеш-функції – відносно безпечна передача інформації. Прикладом її реалізації є шифрування, при якому повідомлення змінюється таким чином, щоб супротивник не зміг його прочитати, а також доповнення повідомлення контрольним кодом (хеш-кодом), що отримується з повідомлення за певним алгоритмом і призначається для аутентифікації відправника і перевірки цілісності повідомлення.

З подібним призначенням використовують також укорочений цифровий підпис) [17]. Укорочений цифровий підпис може бути отриманий шифруванням певної частини повідомлення обмеженої розмірності (розрядності). Такий фрагмент називається аутентифікатором. Якщо аутентифікатор зашифрований закритим ключем відправника, він є цифровим підписом, за допомогою якого можна перевірити вхідне повідомлення. Недоліком аутентифікаторів, які отримуються шифруванням фрагменту повідомлення, є неможливість перевірки цілісності інших фрагментів передаваного відкритого тексту повідомлення. Більш ефективним визнане застосування аутентифікатора, що є функцією від всього повідомлення, тобто, хеш-функції повідомлення.

Стосовно нашої задачі укорочений цифровий підпис не може розглядатися як ефективний метод стиснення двійкового вектора як носія ентропійних властивостей джерела ентропії, оскільки повторне урізання вектора-носія після функції F2 майже гарантовано призведе до втрат властивостей ентропії цього вектора.

Хеш-функція класифікується як стиснене відображення повідомлення з майже однозначною відповідністю функції до коду повідомлення. Тобто, хеш-функції властиве наслідування властивостей оригінального коду, що є визначальним в нашій задачі.

На користь хеш-функцій як способу реалізації функції стиснення векторів-носіїв характеристик ентропії джерел F4 свідчать і криптографічні методи створення цих функцій, що є притаманним задачам системи клієнт-банк.

До переваг криптографічних хеш-функцій слід віднести і те, що хеш-функція здатна протистояти атакам із використанням криптоаналізу.

Це досягається за рахунок наступних властивостей:

- хеш-функція є односторонньою (незворотною). Тобто, майже для всіх варіантів вихідного коду функції неможливо алгоритмічно або обчислювально відновити початковий варіант коду повідомлення;
- стійкість до колізій першого роду. Для заданого повідомлення обчислювально неможливо підібрати інше повідомлення з аналогічною хеш-функцією;
- стійкість до колізій другого роду. Обчислювально неможливо підібрати пару повідомлень, що мають однакову хеш-функцію.

Наведені аргументи свідчать на користь використання в якості функції стиснення векторів-носіїв ентропійних характеристик джерел ентропії F4 саме криптографічних хеш-функцій.

Повертаючись до аналізу функції F3, орієнтованої на об'єднання декількох векторів з складовою ентропії в єдиний вектор, слід зазначити, що реалізація функції стиснення векторів-носіїв ентропійних характеристик джерел ентропії F4 як криптографічної хеш-функції усуває потребу операцій стиснення при

виконанні функції F3. Навпаки, для збереження максимуму ентропійних властивостей вхідних у функцію векторів доцільно зберегти їх у початковому стані і передати на вхід хеш-функції F4. Тобто, оптимальним варіантом функції F3 можна визнати символну операцію поєднання двійкових кодів векторів-носіїв ентропії в єдиний вектор без жодних математичних перетворень, що дасть нам результуючий вектор з розрядністю, рівною сумарній розрядності вхідних до функції F3 початкових векторів. Задача ж стиснення вектора двійкового коду великої розрядності з виходу функції F3 до фіксованого розміру, необхідного для реалізації обраного криптографічного алгоритму генерації псевдовипадкових значень, повністю підпадає під функцію F4.

Результатом реалізації функції F4 є вектор з розрядністю, визначеною потребами обраного криптографічного алгоритму генерації псевдовипадкових значень.

Криптографічний алгоритм генерації псевдовипадкових значень реалізує завершальні операції в досліджуваній моделі, позначені як функція криптографічного методу генерації псевдовипадкових чисел F5, що забезпечує очікуваний результат роботи ГПВЧ.

Таким чином, в запропонованій моделі описано і досліджено всі етапи функціонування ГПВЧ підвищеної ентропії для системи клієнт-банк. Результати проведених досліджень свідчать про відповідність властивостей моделі наявним потребам, тобто, про її адекватність модельованим процесам.

Висновки. За результатами дослідження загальних принципів застосування джерел ентропії в роботі генераторів псевдовипадкових чисел запропоновано математичну модель джерела ентропії, адаптовану для вирішення завдань генерації криптоключів системи клієнт-банк, а також створено узагальнену модель процесу генерації псевдовипадкових двійкових векторів підвищеної ентропії. Проведене дослідження властивостей запропонованої моделі дозволило підтвердити її адекватність процесу генерації псевдовипадкових двійкових векторів підвищеної ентропії. В роботі також надані рекомендації щодо застосування запропонованої моделі в практичних реалізаціях генераторів псевдовипадкових двійкових векторів підвищеної ентропії для синтезу криптоключів системи клієнт-банк, що були використані для апробації моделей генераторів у [18]. Отримані результати є основою для реалізації методу та засобів генерації псевдовипадкових чисел в системі клієнт-банк і удосконалення алгоритмів функціонування зазначеної системи.

Література

1. Геселева Н.В. Інформаційна система підтримки електронних платежів через Інтернет / Н.В. Геселева, Г.В. Пронюк, В.В. Добровольський // Економіка і суспільство, 2018. – Випуск №14. – С. 1005–1010.
2. Умови надання банківських послуг з використанням систем дистанційного обслуговування [Електронний ресурс]. – Режим доступу: https://www.bisbank.com.ua/wp-content/uploads/2020/08/dodatok-7-umovy_system_dist_obslugov_z-11.05.2019-do-05.07.2019.pdf
3. Система «iBank 2» для корпоративних клієнтів. [Електронний ресурс]. – Режим доступу: https://ibank.otpbank.ru/Corporate_Internet-Banking_Guide.pdf.
4. Безпека Інтернет-банкінгу в Україні: практичні аспекти [Електронний ресурс]. – Режим доступу: https://bankchart.com.ua/e_banking/statti/bezpeka_internet_bankingu_v_ukrayini_praktichni_aspekti.
5. Гребенюк Н. О. Фінансова безпека банків: система розпізнання загроз та усунення ризиків / Н. О. Гребенюк // Вісник Харківського національного університету імені В. Н. Каразіна. Серія : Економічна. – 2016. – Вип. 91. – С. 53–64.
6. Горицький В.М. Генерація випадкових послідовностей для систем управління ключами / В.М. Горицький, О.В. Снежок, М.С. Височиненко // Сучасний захист інформації, 2012. – №4. – С. 88–95.
7. Грінченко Т. О. Квантові генератори випадкових чисел в криптографії / Т. О. Грінченко, О. П. Нарезний // Системи обробки інформації. – 2015. – Вип. 10. – С. 86–89.
8. Heat transfer and entropy generation in a microchannel with longitudinal vortex generators using nanofluids / Amin Ebrahimiya, Farhad Rikhtegar, Amin Sabaghana, Ehsan Roohia Energy // Energy. – Volume 101, 15 April 2016. – P. 190–201.
9. Круліковський О. В. Особливості вибору хаотичних систем для побудови генераторів псевдовипадкових послідовностей / О. В. Круліковський, С. Д. Галуць, Л. Ф. Політанський // Телекомунікаційні та інформаційні технології. – 2017. – № 2. – С. 31–40.
10. Слеповичев І.І. Генераторы псевдослучайных чисел / И.И. Слеповичев. – Саратов: издательство СГУ, 2017. – 118 с.
11. Реверсивний генератор кодових послідовностей в FPGA / Д. Гаврілов, А. Воловик, О. Звягін, Д. Яровий // Вісник Вінницького політехнічного інституту. – 2019. – № 4. – С. 100–106.
12. Фауре Е. В. Синтез і аналіз псевдовипадкових послідовностей на основі операцій криптографічного перетворення / Е. В. Фауре, С. В. Сисоєнко, Т. В. Миролюк // Системи управління, навігації та зв'язку. – 2015. – Вип. 4. – С. 85–87.
13. Стасєв Ю. В. Метод формування псевдовипадкових послідовностей з поліпшеними автокореляційними властивостями / Ю. В. Стасєв, Д. О. Медведєв, Д. О. Грабенко, Д. В. Жуйков // Збірник наукових праць Харківського університету Повітряних Сил. – 2017. – № 4. – С. 115–118.
14. Sun Y. Random number generation using inertial measurement unit signals for on-body IoT devices / Y. Sun and B. Lo // in Proc. Living Internet Things, Cybersecur. IoT. – 2018. – P. 1–9.
15. Toward sensorbased random number generation for mobile and IoT devices / K. Wallace, K. Moran, E. Novak, G. Zhou, K. Sun // IEEE Internet Things J. – Dec. 2016. – Vol. 3, № 6. – P. 1189–1201.
16. Демський О.О. Метод реалізації генератора випадкових чисел / О.О. Демський, В.О. Бойчук // «Інтелектуальний потенціал – 2018» - збірник наукових праць молодих науковців і студентів з нагоди 30-річчя підготовки ІТ- фахівців в ХНУ. – Хмельницький: ПБНЗ УЕП, 2018. – Ч.3: Кібербезпека та актуальні проблеми комп'ютерних систем і мереж. – С. 40–44.
17. Lane Wagner, How SHA-2 Works Step-By-Step (SHA-256) / Published July 8, 2020. [Електронний ресурс]. – Режим доступу: <https://qvault.io/2020/07/08/how-sha-2-works-step-by-step-sha-256>.
18. Чешун В. М. Оцінка ефективності роботи генератора криптоключів підвищеної ентропії для системи клієнт-банк / В. М. Чешун, В. І. Чорненький, В. В. Яцків // Збірник наукових праць молодих науковців і студентів «Інтелектуальний потенціал – 2020». – Хмельницький: ПБНЗ УЕП, 2020. – Частина 2. – С. 84–93.

References

1. Gheseleva N.V. Informacijna systema pidtrymky elektronnykh platezhiv cherez Internet / N.V. Gheseleva, Gh.V. Pronjuk, V.V. Dobrovol'skyj // *Ekonomika i suspil'stvo*, 2018. – Vypusk #14. – S. 1005–1010.
2. Umovy nadannja bankiv'skykh poslugh z vykorystannjam system dystancijnogho obslughovuvannja [Elektronnyj resurs]. – URL: https://www.bisbank.com.ua/wp-content/uploads/2020/08/dodatok-7-umovy_system_dist_obsługov_z-11.05.2019-do-05.07.2019.pdf
3. Systema «iBank 2» dlja korporatyvnykh kljentiv. [Elektronnyj resurs]. – URL: https://ibank.otpbank.ru/Corporate_Internet-Banking_Guide.pdf.
4. Bezpeka Internet-bankinghu v Ukrajinі: praktychni aspekty [Elektronnyj resurs]. – URL: https://bankchart.com.ua/e_banking/statti/bezpeka_internet_bankinghu_v_ukrayini_praktychni_aspekty.
5. Ghrebenjuk N. O. Finansova bezpeka bankiv: systema rozpoznavannja zagroz ta usunenennja ryzykiv / N. O. Ghrebenjuk // *Visnyk Kharkiv's'kogho nacional'nogho universytetu imeni V. N. Karazina. Serija : Ekonomichna*. – 2016. – Vyp. 91. – S. 53–64.
6. Ghoryc'kyj V.M. Gheneracija vypadkovykh poslidovnostej dlja system upravlinnja kljuchamy / V.M. Ghoryc'kyj, O.V. Snjezhok, M.S. Vysochinenko // *Suchasnyj zakhyst informacii*, 2012. – #4. – S. 88–95.
7. Ghrinenko T. O. Kvantovi gheneratory vypadkovykh chysel v kryptoghrafiji / T. O. Ghrinenko, O. P. Narjezhnij // *Systemy obrobky informacii*. – 2015. – Vyp. 10. – S. 86–89.
8. Heat transfer and entropy generation in a microchannel with longitudinal vortex generators using nanofluids / Amin Ebrahimia, Farhad Rikhtegar, Amin Sabaghana, Ehsan Roohia Energy // *Energy*. – Volume 101, 15 April 2016. – P. 190–201.
9. Krulikov'skyj O. V. Osoblyvosti vyboru khaotychnykh system dlja pobudovy gheneratoriv psevdovypadkovykh poslidovnostej / O. V. Krulikov'skyj, S. D. Ghaljuk, L. F. Politan'skyj // *Telekomunikacijni ta informacijni tekhnologiji*. – 2017. – # 2. – S. 31–40.
10. Slepovichev I.I. Generatory psevdosluchaynykh chysel / I.I. Slepovichev. – Saratov: izdatel'stvo SGU, 2017. – 118 s.
11. Reversyvnij ghenerator kodovykh poslidovnostej na FPGA / D. Ghavrilo, A. Volovyk, O. Zvjaghin, D. Jarovyj // *Visnyk Vinnyckogho politekhnichnogho instytutu*. – 2019. – # 4. – S. 100–106.
12. Faure E. V. Syntez i analiz psevdovypadkovykh poslidovnostej na osnovi operacij kryptoghrafichnogho peretvorennja / E. V. Faure, S. V. Sysojenko, T. V. Myronjuk // *Systemy upravlinnja, navighacii ta zv'jazku*. – 2015. – Vyp. 4. – S. 85–87.
13. Stasjev Ju. V. Metod formuvannja psevdovypadkovykh poslidovnostej z polipshenyj avtokoreljacijnyj vlastyvostjamy / Ju. V. Stasjev, D. O. Medvedjev, D. O. Ghrabenko, D. V. Zhujkov // *Zbirnyk naukovykh pracj Kharkiv's'kogho universytetu Povitrjanykh Syl*. – 2017. – # 4. – S. 115–118.
14. Sun Y. Random number generation using inertial measurement unit signals for on-body IoT devices / Y. Sun and B. Lo // in *Proc. Living Internet Things, Cybersecur. IoT*. – 2018. – P. 1–9.
15. Toward sensorbased random number generation for mobile and IoT devices / K. Wallace, K. Moran, E. Novak, G. Zhou, K. Sun // *IEEE Internet Things J*. – Dec. 2016. – Vol. 3, # 6. – P. 1189–1201.
16. Dem'skyi O.O. Metod realizatsii heneratora vypadkovykh chysel / O.O. Dem'skyi, V.O. Boichuk // «*Intelektualnyi potentsial – 2018*» - zbirnyk naukovykh prats molodykh naukovtsiv i studentiv z nahody 30-richchia pidhotovky IT-fakhivtsiv v KhNU. – Khmelnytskyi: PVNZ UEP, 2018. – Ch.3: Kiberbezpeka ta aktualni problemy kompiuternykh system i mrezezh. – S. 40–44.
17. Lane Wagner, How SHA-2 Works Step-By-Step (SHA-256) / Published July 8, 2020. [Elektronnyj resurs]. – URL: <https://qvault.io/2020/07/08/how-sha-2-works-step-by-step-sha-256>.
18. Cheshun V. M. Ocinka efektyvnosti roboty gheneratora kryptokljuchiv pidvyshhenoji entropiji dlja systemy kljent-bank / V. M. Cheshun, V. I. Chornen'kyj, V. V. Jackiv // *Zbirnyk naukovykh pracj molodykh naukovtsiv i studentiv «Intelektual'nyj potentsial – 2020»*. – Khmelnyckyj: PVNZ UEP, 2020. – Chastyna 2. – S. 84–93.

Надійшла / Paper received: 16.10.2020

Надрукована / Paper Printed : 01.12.2020