КОМП'ЮТЕРНІ НАУКИ, ІНФОРМАЦІЙНІ ТЕХНОЛОГІ, СИСТЕМНИЙ АНАЛІЗ ТА КІБЕРБЕЗПЕКА

DOI 10.31891/2307-5732-2021-301-5-18-21
УДК 004.421.5:004.942

ГУРМАН І. В.
Хмельницький національний університет
ORCID ID: 0000-0002-2282-3484
e-mail: devastator192@gmail.com
ПЕТЛЯК Н. С.
Університет економіки і підприємництва, м.Хмельницький
ORCID ID: 0000-0001-5971-4428
e-mail: npetlyak@khmnu.edu.ua
ЧЕШУН В. М.
Хмельницький національний університет
ORCID ID: 0000-0002-3935-2068
e-mail: cheshunvn@khmnu.edu.ua
ДЖУЛІЙ А. В.
Університет економіки і підприємництва, м.Хмельницький
ORCID ID: 0000-0001-5011-3052
e-mail: kksmkhnu@gmail.com
ЧОРНЕНЬКИЙ В. І.
Університет економіки і підприємництва, м.Хмельницький
ORCID ID: 0000-0002-0576-7097
e-mail: vitnel@ukr.net

ВИЗНАЧЕННЯ ЕНТРОПІЙНОЇ СКЛАДОВОЇ ПОКАЗНИКІВ ДАТЧИКІВ ДЛЯ ГЕНЕРАЦІЇ КРИПТОКЛЮЧІВ МОБІЛЬНОГО ДОДАТКУ СИСТЕМИ КЛІЄНТ-БАНК

В роботі представлено результати дослідження датчиків пристроїв мобільного зв'язку як джерела ентропії для генерації криптоключів мобільного додатку системи клієнт-банк. Результати підтверджують наявність в значеннях показників датчиків складової, придатної для використання в якості джерела первинної ентропії для генераторів псевдовипадкових чисел за криптографічними алгоритмами з подальшим застосуванням в роботі генераторів криптоключів в сервісах мобільного банкінгу системи клієнт-банк.

Ключові слова: датчик, ентропія, генератор псевдовипадкових чисел, мобільний банкінг.

GURMAN IVAN V., CHESHUN VIKTOR.M. PETLIAK NATALIIA S.
Khmelnytsky National University, Khmelnytsky, Ukraine
DZHULIY ANDRII.V., CHORNENKYI VITALII I.
University of Economics and Entrepreneurship, Khmelnytsky, Ukraine

DETERMINATION OF ENTROPY COMPONENT IN SENSOR INDICATORS FOR GENERATION OF CRYPTOGRAPHIC KEYS OF THE MOBILE APPLICATION OF THE CLIENT-BANK SYSTEM

The rapid penetration of the banking market of mobile banking creates not only new opportunities and conveniences, but also new risks and threats, which leads to increased requirements for information security of mobile services. One of the important components of the security of the mobile banking service 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 sources of entropy, for the effective use of which it is necessary to determine the type and capabilities of the source.

The paper presents the results of the study of sensors of mobile communication devices as a source of entropy for generating cryptokeys of a mobile application of the client-bank system. An accelerometer, a temperature sensor, a gyroscope, a light brightness sensor, a magnetic field sensor, an atmospheric pressure sensor, a distance sensor, and a humidity sensor are considered as a source of entropy. The results of the research confirm the presence in the values of the sensors of mobile communication devices of a component suitable for use as a source of primary entropy for generators of pseudo-random numbers by cryptographic algorithms. In turn, pseudo-random number generators built with the use of mobile device sensors can be the basis of high-entropy cryptographic key generators in the client-bank system mobile banking services.

The obtained results are focused on the implementation of algorithms and means of generating high-entropy pseudo-random numbers and can be used to reduce the risks of unauthorized access to customer information in the client-bank system by disclosing cryptokeys in mobile banking services.

Keywords: sensor, entropy, pseudo-random number generator, mobile banking.

Постановка проблеми

Сучасна банківська система – складний механізм з підвищеними вимогами щодо надійності, який базується на використанні різноманітних сервісів організації доступу до банківських послуг. До типових сервісів банківських послуг належить комп'ютерний банкінг (PC banking), телефонний банкінг (Phone banking), SMS-банкінг (SMS banking), WAP-банкінг (WAP banking), мобільний банкінг (Mobile banking), Internet-банкінг (Internet banking, WEB banking, Online banking) тощо [1, 2]. Особливою популярністю

останнім часом користується мобільний банкінг, який набуває все більшого поширення через повсюдне розповсюдження пристроїв мобільного зв'язку (ПМЗ), повсюдну доступність і зручність сервісу.

Стрімке вторгнення на ринок банківських послуг мобільного банкінгу створює не лише нові можливості і зручності, але і нові ризики та загрози, що зумовлює підвищені вимоги до інформаційної безпеки мобільного сервісу. Для захисту сервісів системи клієнт-банк використовуються механізми електронного цифрового підпису, хеш функцій, розповсюдження ключів сесії із застосуванням алгоритмів асиметричного шифрування, симетричне шифрування та захищений протокол передачі і автентифікації [2, 3]. 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. Вибір засобів і методу формування псевдовипадкових чисел з високим показником ентропії є однією із основних проблем у вирішенні завдань формування криптоключів високої надійності, оскільки генерація якісної випадкової послідовності чисел – найскладніша частина багатьох криптографічних операцій [4,5,6].

Аналіз останніх досліджень і публікацій

Генераторам псевдовипадкових чисел (ГПВЧ) присвячена велика кількість наукових досліджень і публікацій, що зумовило появу великої кількості видів та моделей генераторів, а також їх модифікацій. В спеціалізованих криптографічно сильних ГПВЧ в якості джерел ентропії використовується радіоактивний розпад, фізичні явища оптично-квантової механіки, електричні шуми тощо [5,6], але для масового використання в системах мобільного банкінгу такі ГПВЧ непридатні. Базисом ГПВЧ електронних систем, як правило, є програмні або апаратні методи генерації та їх комбінації [4], але окремий клас ГПВЧ утворюють криптографічні генератори [7], що найчастіше використовуються в електронних банківських сервісах.

Робота криптографічних ГПВЧ базується на методах та алгоритмах сучасної криптографії, стартові значення для яких формуються із застосуванням явищ або засобів, оцінювані параметри яких можуть розглядатися як випадкові. Ці явища використовуються для збільшення ентропії генерованих в різних сеансах послідовностей чисел і розглядаються як джерела первинної ентропії [4,5].

Згідно із презентованими в [8] результатами досліджень, ефективними джерелами ентропійних значень можуть бути широко розповсюджені в сучасному електронному середовищі датчики різного типу, в тому числі датчики IoT. В [9.10] відзначається перспективність застосування в якості джерел ентропії датчиків сучасних ПМЗ, але особливості їх використання в конкретних застосуваннях потребують подальших досліджень і детального аналізу [10].

Метою роботи є дослідження властивостей датчиків пристроїв мобільного зв'язку як джерела ентропії для генерації криптоключів мобільного додатку системи клієнт-банк.

Виклад основного матеріалу

Спосіб застосування датчиків пристроїв мобільного зв'язку як джерела ентропії для генерації криптоключів мобільного додатку системи клієнт-банк базується на математичній моделі, запропонованій в [11]. Трирівнева модель процесу генерації псевдовипадкових чисел підвищеної ентропії відображує розподіл типових функцій цього процесу за загальним цільовим призначенням, що є характерними етапам процесу формування криптоключів на основі показників датчиків: етап зчитування показників датчиків; етап обробки отриманих значень з виділенням ентропійної складової і представленням їх у форматі, придатному для застосування в роботі криптографічного ГПВЧ; етап генерації криптоключів криптографічним ГПВЧ.

Об'єктом дослідження даної роботи є другий етап, який визначає можливість формування на підставі показників датчиків ПМЗ значення високої ентропії, потрібного для реалізації алгоритму роботи ГПВЧ, а саме з виділення ентропійної складової в значеннях показників датчиків ПМЗ.

При виборі датчиків ПМЗ в якості потенційних джерел ентропії з розгляду були виключені ті, що є залежними від поведінки користувача (датчики початку руху, пульсу, серцевої активності тощо), датчики з бінарним виходом і віртуальні датчики (реалізуються програмно, їх робота базується на показниках інших датчиків, через що додаткової ентропії вони генерувати не можуть) [12].

Таким чином був сформований перелік датчиків, потенційно перспективних в якості джерел ентропії: Type_Accelerometer – акселерометр; Type(_Ambient*)_Temperature – датчик температури; Type_Gyroscope – гіроскоп; Type_Light – датчик яскравості світла; Type_Magnetic_Field – датчик магнітного поля; Type_Pressure – датчик атмосферного тиску; Type_Proximity – датчик відстані; Type_Relative_Humidity – датчик вологості.

За результатами 20 послідовних вимірювань показників датчика температури Samsung Galaxy A22 отримано наступні значення (фрагмент пулу вибірки з 10000 значень): 24.375045, 24.425790, 24.381837, 24.315987, 24.435728, 24.359723, 24.370825, 24.356152, 24.391004, 24.386701, 24.379900, 24.411879, 24.424070, 24.339089, 24.436872, 24.420948, 24.448370, 24.426860, 24.368145, 24.372090. З аналізу показників датчика температури можна визначити високу стабільність цілої частини числа, низьку змінюваність десятих долей і фактично хаотичну змінюваність розрядів починаючи від сотих долей числа.

За аналогічними результатами 20 послідовних вимірювань показників акселерометра отримано наступні значення: 9.753255, 9.698901, 9.690168, 9.775196, 9.817273, 9.752594, 9.737145, 9.788312, 9.770896, 9.768726, 9.671298, 9.732452, 9.712309, 9.813275, 9.740949, 9.784542, 9.785174, 9.704438. В роботі акселерометра також можна визначити високу стабільність цілої частини числа, низьку змінюваність десятих долей і фактично хаотичну змінюваність розрядів починаючи від сотих долей числа.

Нестабільність значень молодших розрядів дробової частини показників датчиків в сталих умовах проведення експерименту зумовлена похибкою вимірювань, яка утворюється через недосконаліть самого датчика та можливі внутрішні і зовнішні впливи на роботу ПМЗ. При цьому похибка є статистично непередбачуваною, що свідчить на користь зазначеної частини числа як носія ентропії.

Аналіз виділених в якості джерела ентропії розрядів числа навіть на такій невеликій вибірці дозволяє зробити висновок про відносно рівномірний розподіл значень десяткових цифр в числах від 17 до 26 повторів для окремих значень 0-9.

Для унаочнення результату експерименту були сформовані гістограми статистики появи окремих десяткових цифр в молодших розрядах дробової частини числа для повного пулу з 10000 значень. На рис. 1 наведено гістограми, побудовані за проказниками акселерометра.

Статистичний аналіз отримуваних в експерименті результатів і їх гістограм свідчить про відсутність будь-якої залежності між наявними в окремих розрядах значеннями цифр, а також про відносно рівномірний розподіл вказаних значень між розрядами. Аналогічний висновок можна зробити за результатами дослідження різних моделей ПМЗ в стаціонарному і рухомому режимах. Крім того, багатократне повторення експерименту дає подібні середньостатистичні результати зі змінюваними статистичними даними за усередненими показниками, але демонструє відсутність залежності в характері відхилення статистики появи цифр в будь-якому розряді від усередненого значення 10% щодо окремих розрядів.

Проведене дослідження характеру розподілу 0 і 1 в двійкових векторах ентропійної складової показників датчиків ПМЗ також свідчить про відсутність будь-якої залежності між отримуваними в окремих розрядах значеннями цифр, а також про рівномірний розподіл вказаних значень між розрядами.

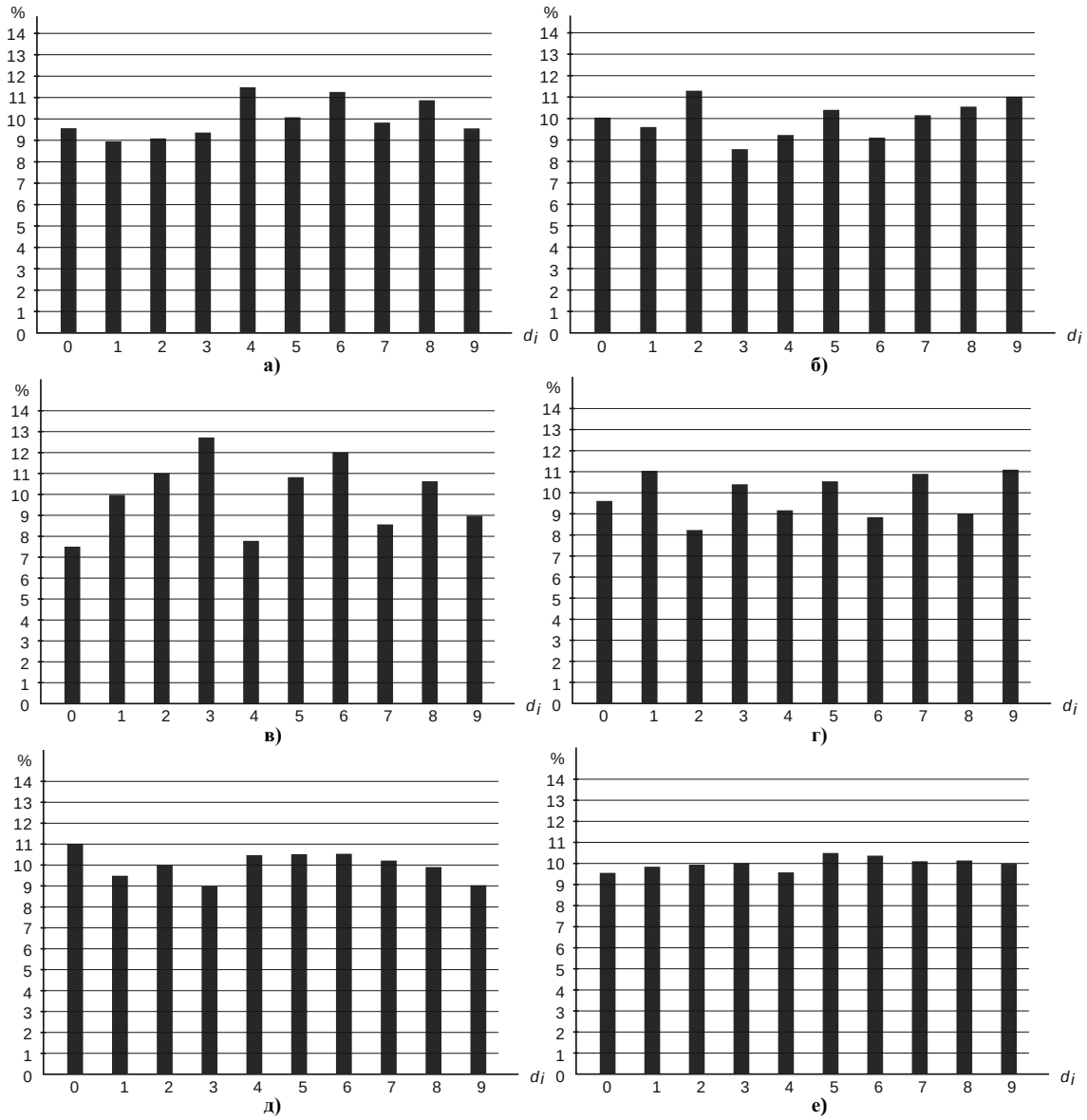

Рис. 1. Гістограми порозрядного аналізу ентропійної складової значень показників акселерометра: а) розряд X_{-2}; б) розряд X_{-3}; в) розряд X_{-4}; г) розряд X_{-5}; д) розряд X_{-6}; е) усереднені показники розрядів X_{-2}–X_{-6}

Дослідження властивостей датчиків температури, магнітометра, освітленості, барометра та ряду інших

датчиків дозволило дійти висновку, що в показниках кожного з них в дробовій частині можна знайти вектор з якісною ентропійною складовою, придатною для використання в якості джерела ентропії в реалізації ГПВЧ.

Висновки

Результати проведених досліджень підтверджують наявність в значення показників датчиків пристроїв мобільного зв'язку складової, придатної для використання в якості джерела первинної ентропії для генераторів псевдовипадкових чисел за криптографічними алгоритмами. В свою чергу, побудовані з використанням датчиків мобільних пристроїв генератори псевдовипадкових чисел можуть бути основою генераторів криптоключів підвищеної ентропії в сервісах мобільного банкінгу системи клієнт-банк.

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. Система «iBank 2» для корпоративних клієнтів. [Електронний ресурс]. – Режим доступу: https://ibank.otpbank.ru/Corporate_Internet–Banking_Guide.pdf.

3. 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.

4. Горицький В.М. Генерація випадкових послідовностей для систем управління ключами / В.М. Горицький, О.В. Снєжок, М.С. Височіненко // Сучасний захист інформації, 2012. – №4. – С. 88–95.

5. Гріненко Т. О. Квантові генератори випадкових чисел в криптографії / Т. О. Гріненко, О. П. Нарєжній // Системи обробки інформації. – 2015. – Вип. 10. – С. 86–89.

6. Heat transfer and entropy generation in a microchannel with longitudinal vortex generators using nanofluids / Amin Ebrahimia, Farhad Rikhtegarb, Amin Sabaghana, Ehsan Roohia Energy // Energy. – Volume 101, 15 April 2016. – P. 190–201.

7. Фауре Е. В. Синтез і аналіз псевдовипадкових послідовностей на основі операцій криптографічного перетворення / Е. В. Фауре, С. В. Сисоєнко, Т. В. Миронюк // Системи управління, навігації та зв'язку. – 2015. – Вип. 4. – С. 85–87.

8. Florin Răstoceanu,Răzvan Rughinis, Stefan-Dan Ciocîrlan, Mihai Enache. Sensor-Based Entropy Source Analysis and Validation for Use in IoT Environments. Electronics, 10, 1173. – 2021 – 28 p.

9. Christine Hennebert, Hicham Hossayni, Cédric Lauradoux. Entropy harvesting from physical sensors. Proceedings of the sixth ACM conference on Security and privacy in wireless and mobile networks, 2013. P. 149–154.

10. Na Lv, Tianyu Chen, Yuan Ma. Analysis on Entropy Sources based on Smartphone Sensors. ICCNS 2020: The 10th International Conference on Communication and Network Security, November 2020. P. 21–31.

11. Модель генератора криптоключів з джерелами ентропії для системи клієнт-банк / В. С. Орленко, В. М. Чешун, О. С. Андрощук, А. І. Катаєва // Міжнародний науково-технічний журнал «Вимірювальна та обчислювальна техніка в технологічних процесах» – 2020. – № 2. – С. 103–112.

12. Функціональна реалізація генератора криптоключів з джерелами ентропії для мобільного банкінгу / О. С. Андрощук, Ю. П. Кльоц, В.С. Орленко, В. М. Чешун // Вісник Хмельницького національного університету. Технічні науки. – 2021. – № 1. – С. 7–11.

References

1. Gheseleva N.V. Informacijna systema pidtrymky elektronnykh platezhiv cherez Internet / N.V. Gheseleva, Gh.V. Pronjuk, V.V. Dobrovoljsjkyj// Ekonomika i suspiljstvo, 2018. – Vypusk #14. – S. 1005–1010.

2. Systema «iBank 2» dlja korporatyvnykh klijentiv. [Elektronnyj resurs]. – URL: https://ibank.otpbank.ru/Corporate_Internet–Banking_Guide.pdf.

3. Bezpeka Internet–bankinghu v Ukrajini: praktychni aspekty [Elektronnyj resurs]. – URL: https://bankchart.com.ua/e_banking/statti/bezpeka_internet_bankingu_v_ukrayini_praktichni_aspekti.

4. Ghorycjkyj V.M. Gheneracija vypadkovykh poslidovnostej dlja system upravlinnja kljuchamy / V.M. Ghorycjkyj, O.V. Snjezhok, M.S. Vysochinenko // Suchasnyj zakhyst informaciji, 2012. – #4. – S. 88–95.

5. Ghrinenko T. O. Kvantovi gheneratory vypadkovykh chysel v kryptoghrafiji / T. O. Ghrinenko, O. P. Narjezhnij // Systemy obrobky informaciji. – 2015. ¬– Vyp. 10. – S. 86–89.

6. Heat transfer and entropy generation in a microchannel with longitudinal vortex generators using nanofluids / Amin Ebrahimia, Farhad Rikhtegarb, Amin Sabaghana, Ehsan Roohia Energy // Energy. – Volume 101, 15 April 2016. – P. 190–201.

7. Faure E. V. Syntez i analiz psevdovypadkovykh poslidovnostej na osnovi operacij kryptoghrafichnogho peretvorennja / E. V. Faure, S. V. Sysojenko, T. V. Myronjuk // Systemy upravlinnja, navighaciji ta zv'jazku. – 2015. – Vyp. 4. – S. 85–87.

8. Florin Răstoceanu,Răzvan Rughinis, Stefan-Dan Ciocîrlan, Mihai Enache. Sensor-Based Entropy Source Analysis and Validation for Use in IoT Environments. Electronics, 10, 1173. – 2021 – 28 p.

9. Christine Hennebert, Hicham Hossayni, Cédric Lauradoux. Entropy harvesting from physical sensors. Proceedings of the sixth ACM conference on Security and privacy in wireless and mobile networks, 2013. P. 149–154.

10. Na Lv, Tianyu Chen, Yuan Ma. Analysis on Entropy Sources based on Smartphone Sensors. ICCNS 2020: The 10th International Conference on Communication and Network Security, November 2020. P. 21–31.

11. Modelj gheneratora kryptokljuchiv z dzherelamy entropiji dlja systemy klijent-bank / V. S. Orlenko, V. M. Cheshun, O. S. Androshhuk, A. I. Katajeva // Mizhnarodnyj naukovo-tekhnichnyj zhurnal «Vymirjuvaljna ta obchysljuvaljna tekhnika v tekhnologhichnykh procesakh» – 2020. – # 2. – S. 103–112.

12. Funktsionalna realizatsiia heneratora kryptokliuchiv z dzherelamy entropii dlia mobilnoho bankinhu / O. S. Androshchuk, Yu. P. Klots, V.S. Orlenko, V. M. Cheshun // Herald of Khmelnytskyi National University. Technical sciences. – 2021. – № 1. – S. 7–11.

Рецензія/Peer review : 07.09.2021 р. Надрукована/Printed :10.10.2021 р.