РЕФЕРАТ

Актуальність теми. Забезпечення криптографічної стійкості інформаційних систем безпосередньо залежить від якості ключового матеріалу, який використовується в алгоритмах шифрування, протоколах автентифікації та механізмах розподілу секретів. Існуючі рішення, зокрема стандартні програмні генератори псевдовипадкових чисел і окремі апаратні RNG, нерідко мають обмеження, пов’язані з якістю реалізації, складністю валідації й чутливістю до деградації фізичних джерел. Розробники вимушені або покладатися на «чорні скриньки» у вигляді вбудованих RNG, або витрачати значні зусилля на комплексну перевірку та комбінування кількох джерел випадковості.

У даній роботі розглядається задача підвищення стійкості ключів шифрування шляхом розробки способу генерації ключового матеріалу, який поєднує фізичну ентропію апаратного генератора істинно випадкових чисел із математично обґрунтованим перетворенням до розподілу Гауса та подальшою криптографічною післяобробкою.

Об’єктом дослідження є процеси формування криптографічного ключового матеріалу в інформаційно-комунікаційних системах із використанням апаратних та програмних генераторів випадкових чисел.

Предметом дослідження є способи підвищення стійкості ключів шифрування за рахунок комбінованих способів генерації випадкових послідовностей, що поєднують фізичну ентропію, нормальний розподіл і криптографічну післяобробку, а також методи статистичної оцінки якості таких послідовностей.

Мета роботи: розробка та обґрунтування способу генерації криптографічних ключів на основі нормального розподілу, який, використовуючи апаратне джерело істинно випадкових чисел і криптографічну післяобробку, забезпечує підвищену статистичну якість і стійкість ключового матеріалу порівняно з типовими способами.

Наукова новизна. Вперше запропоновано новий спосіб генерації ключового матеріалу, який ґрунтується на розподілі Гауса, відрізняється від існуючих поєднанням апаратного джерела випадковості з математичною трансформацією до нормального розподілу та подальшою криптографічною післяобробкою і який дозволяє генерувати криптографічно стійкі випадкові послідовності.

Практична цінність. Запропонований спосіб може бути використаний як окремий модуль генерації ключового матеріалу в програмно-апаратних комплексах захисту інформації, протоколах захищеного обміну даними та вбудованих системах. Реалізація способу в середовищі Linux мовою С з використанням апаратного RNG процесора та стандартних криптографічних бібліотек дозволяє інтегрувати його в існуючу інфраструктуру без істотних змін архітектури. Практичні результати показують, що при коректному налаштуванні та достатній мінімальній ентропії на вході спосіб забезпечує формування ключових послідовностей, які за статистичними характеристиками відповідають вимогам сучасних криптографічних стандартів, що дає змогу підвищити надійність систем безпеки без значного збільшення обчислювальних витрат.

Апробація роботи. Основні положення та результати дослідження були представлені та обговорювалися на XVIII науково конференцій магістрантів та аспірантів «Прикладна математика та комп'ютинг» ПМК-2025 факультету прикладної математики (Київ, 20 листопада 2025 р.).

Публікації. Результати дисертації викладено в наукових працях, у тому числі:

- тези до доповіді на XVIII науково-практичній конференцій магістрантів та аспірантів ПМК-2025 факультету прикладної математики за темою «Аналіз ключів шифрування згенерованих на основі нормального розподілу»

- стаття до наукового, фахового журналу «Вісник Хмельницького національного університету. Серія: Технічні науки», том 360 №6.2 (2025) за темою «Спосіб підвищення надійності ключів шифрування на основі розподілу Гауса»

Структура та обсяг роботи. Магістерська дисертація складається зі вступу, чотирьох розділів та висновків.

У *вступі* обґрунтовано актуальність тематики, сформульовано мету, завдання, об’єкт і предмет дослідження, окреслено наукову новизну та практичну цінність роботи.

У *першому розділі* наведено огляд сучасних способів генерації криптографічних ключів, проаналізовано властивості апаратних та програмних генераторів випадкових чисел, розглянуто поняття стійкості ключового матеріалу та типові вектори атак на RNG.

У *другому розділі* сформульовано теоретичні засади запропонованого способу, описано застосування нормального розподілу в задачі генерації ключів та обґрунтовано вибір математичних і криптографічних примітивів.

У *третьому розділі* викладено особливості програмної реалізації способу, включно з організацією доступу до апаратного джерела ентропії, реалізацією нормалізації до розподілу Гауса та післяобробки.

У *четвертому розділі* подано результати експериментальної оцінки якості ключових послідовностей за допомогою NIST SP 800-22, виконано порівняння з іншими способами генерації та сформульовано практичні рекомендації щодо застосування запропонованого способу.

У *висновках* підсумовано основні результати дослідження та окреслено перспективи подальшого розвитку роботи.

Дисертація представлена на 84 аркуші, містить 3 таблиці, 4 додатки та посилання на список використаних літературних джерел.

Ключові слова: криптографічний ключ, стійкість ключів, генератор випадкових чисел, апаратний RNG, псевдовипадковий генератор, нормальний розподіл, метод Бокса–Мюллера, тестовий комплекс NIST SP 800-22, ентропія, післяобробка випадкових послідовностей.

ABSTRACT

Actuality of theme. Ensuring the cryptographic strength of information systems directly depends on the quality of the key material used in encryption algorithms, authentication protocols and secret-sharing mechanisms. Existing solutions, in particular standard software pseudorandom number generators and some hardware RNGs, often have limitations related to implementation quality, complexity of validation and sensitivity to the degradation of physical sources. Developers are forced either to rely on "black box" embedded RNGs, or to spend significant effort on comprehensive verification and combining several sources of randomness.

In this work, the problem of increasing the robustness of encryption keys is considered by developing a method for generating key material that combines the physical entropy of a hardware true random number generator with a mathematically grounded transformation to the Gaussian distribution and subsequent cryptographic post-processing.

The object of the research is the processes of forming cryptographic key material in information and communication systems using hardware and software random number generators.

The subject of the research is the methods of increasing the robustness of encryption keys by means of combined methods of generating random sequences that integrate physical entropy, normal (Gaussian) distribution and cryptographic post-processing, as well as methods of statistical quality assessment of such sequences.

The purpose of the work is the development and justification of a method for generating cryptographic keys based on the normal distribution which, using a hardware source of true random numbers and cryptographic post-processing, provides increased statistical quality and robustness of key material compared to typical methods.

Scientific novelty. For the first time, a new method for generating key material based on the Gaussian distribution is proposed. It differs from existing approaches by combining a hardware source of randomness with a mathematical transformation to the normal distribution and subsequent cryptographic post-processing, and makes it possible to generate cryptographically secure random sequences.

Practical value. The proposed method can be used as a separate key-material generation module in hardware–software information security systems, in secure data exchange protocols and in embedded systems. Implementation of the method in the Linux environment in the C programming language, using the processor hardware RNG and standard cryptographic libraries, makes it possible to integrate it into existing infrastructure without significant changes to the architecture. Practical results show that with correct configuration and sufficient minimal entropy at the input, the method provides key sequences whose statistical characteristics meet the requirements of modern cryptographic standards, which allows increasing the reliability of security systems without a significant increase in computational costs.

Approbation of work. The main provisions and results of the research were presented and discussed at the XVIII scientific conference of master's and postgraduate students "Applied Mathematics and Computing" PMK-2025 of the Faculty of Applied Mathematics (Kyiv, November 20, 2025).

Publications. The results of the thesis are presented in scientific publications, including:

– theses for the report at the XVIII scientific and practical conference of master's and postgraduate students PMK-2025 of the Faculty of Applied Mathematics on the topic "Analysis of encryption keys generated on the basis of the normal distribution";

– an article submitted to the scientific professional journal "Herald of Khmelnytskyi National University. Series: Technical Sciences", vol. 360, No. 6.2 (2025) on the topic "Method of increasing the reliability of encryption keys based on the Gaussian distribution".

Structure and scope of work. The master's thesis consists of an introduction, four chapters and conclusions.

The introduction substantiates the relevance of the topic, formulates the aim, tasks, object and subject of the research, and outlines the scientific novelty and practical value of the work.

The first chapter provides an overview of modern methods of generating cryptographic keys, analyses the properties of hardware and software random number generators, considers the concept of key material robustness and typical attack vectors on RNGs.

The second chapter formulates the theoretical foundations of the proposed method, describes the use of the normal distribution in the problem of key generation and justifies the choice of mathematical and cryptographic primitives.

The third chapter presents the features of the software implementation of the method, including the organization of access to the hardware entropy source, implementation of normalization to the Gaussian distribution and post-processing.

The fourth chapter presents the results of experimental evaluation of the quality of key sequences using NIST SP 800-22, provides a comparison with other generation methods and formulates practical recommendations on the application of the proposed method.

The conclusions summarize the main results of the research and outline the prospects for further development of the work.

The thesis is presented on 84 pages, contains 3 tables, 4 appendices and references to the list of used literary sources.

Keywords: cryptographic key, key robustness, random number generator, hardware RNG, pseudorandom generator, normal distribution, Box–Muller method, NIST SP 800-22 test suite, entropy, post-processing of random sequences.