Міністерство освіти і науки України

Харківський національний університет імені В.Н. Каразіна

Факультет комп'ютерних наук

Спеціальність 125 «Кібербезпека»

Освітня програма «Безпека інформаційних та комунікаційних систем»

«Допущено до захисту»

В.о. зав. кафедрою БІСТ

Ольга МЕЛКОЗЬОРОВА

_____

« » 2023 р.

Пояснювальна записка

до кваліфікаційної роботи магістра

на тему: «Розробка моделі та методу захисту від кіберзагроз веб-сервісу квантового генератора випадкових чисел»

оцінка « »

Голова ЕК

Олександр ЛЕМЕШКО _____

Керівник: канд. техн. н., доцент

Нарєжній Олексій Павлович

Рецензент: канд. техн. н., старш. викл.

Лисицький Костянтин Євгенійович

Виконавець: студентка групи КБ-61

Осипенко Юлія Сергіївна

Харків – 2023

РЕФЕРАТ

Структура та обсяг роботи. Пояснювальна записка містить 135 сторінок, 15 рисунків, 3 таблиці, 2 додатки, 159 джерел.

Актуальність теми. У дипломній роботі розроблена модель, що дозволяє виявляти та запобігати кібератакам на веб-сервіс. Для цього проведено аналіз загроз безпеці та ідентифікацію слабких місць у веб-сервісі. Розроблена та впроваджена система моніторингу та виявлення аномальної поведінки користувачів веб-сервісу. Крім того, розглянуті можливості використання квантових технологій для забезпечення додаткового рівня безпеки.

Об'єктом розробки є веб-сервіс квантового генератора випадкових чисел, який використовується для забезпечення криптографічної безпеки в різних системах.

Предметом розробки є модель та метод захисту цього веб-сервісу від кіберзагроз.

Основною проблемою, що вирішується, є забезпечення безпеки веб-сервісу квантового генератора випадкових чисел від кібератак та зламів. Квантові генератори випадкових чисел мають важливе значення для криптографічних протоколів, і їх використання повинно бути забезпечено високим рівнем безпеки.

Метою проекту є створення ефективного та надійного методу захисту веб-сервісу квантового генератора від кіберзагроз, що забезпечить безпеку і конфіденційність випадкових чисел, генерованих сервісом.

Основними завданнями, на вирішення яких спрямовано проект, є виявленні потенційних кіберзагроз, що можуть спричинити витік конфіденційної інформації або злам безпеки квантового генератора; розробка методу захисту, який би забезпечував захист від загроз та зберігав надійність генерації випадкових чисел.

Значимість проекту полягає в тому, що він може допомогти у підвищенні рівня кібербезпеки веб-сервісів, які використовують квантові генератори випадкових чисел, що є важливою складовою в безпеці багатьох систем, зокрема фінансових. Проект також може мати значення для розвитку науки, зокрема кібербезпеки, та навчання студентів у цій галузі.

Методи дослідження. Під час дослідження були використані таки методи: аналіз сучасних рішень, аналіз існуючих загроз та існуючих методів протидії, порівняння методів захисту та вибір найбільш актуального з них в умовах української специфіки, аналіз методологій розробки web-ресурсів.

Практична цінність. Дослідження може бути використане під час розробки квантового генератору випадкових чисел, що працює в режимі реального часу, перевірений безпекою, шляхом вимірювання флуктуації вакууму. Запропоновано та реалізовано оптимізований алгоритм випадкового вилучення, щоб подолати розрив у швидкості між швидким генеруванням випадковості та повільним вилученням випадковості. Дані можуть використовуватися в навчальному процесі під час вивчення подібних тем.

Апробація роботи. Основні положення на результати роботи були представлені у статті у фаховому журналі, який входить до категорії Б.

Ключові слова: КІБЕРБЕЗПЕКА, КВАНТОВИЙ ГЕНЕРАТОР ВИПАДКОВИХ ЧИСЕЛ, ВЕБ-РЕСУРС, КІБЕРЗАГРОЗИ, МЕТОДИ АНАЛІЗУ, ІДЕНТИФІКАЦІЯ ЗАГРОЗ, НАСКРІЗНЕ ШИФРУВАННЯ.

ABSTRACT

Structure and scope of work. The explanatory note contains 135 pages, 15 figures, 3 tables, 2 appendices, 159 sources.

Actuality of theme. The thesis developed a model that allows detection and prevention of cyber attacks on a web service. For this, an analysis of security threats and identification of weak points in the web service was carried out. A system for monitoring and detecting abnormal behavior of web service users has been developed and implemented. In addition, the possibilities of using quantum technologies to provide an additional level of security are considered.

The object of development is a web service of a quantum random number generator, which is used to ensure cryptographic security in various systems.

The subject of development is a model and method of protecting this web service against cyber threats.

The main problem to be solved is to secure the quantum random number generator web service from cyber attacks and hacking. Quantum random number generators are essential for cryptographic protocols, and their use must be ensured with a high level of security.

The goal of the work is to create an effective and reliable method of protecting the quantum generator web service from cyber threats, which will ensure the security and confidentiality of random numbers generated by the service.

The main tasks to be solved by the project are the detection of potential cyber threats that can cause the leakage of confidential information or security breaches of the quantum generator; development of a protection method that would provide protection against threats and preserve the reliability of random number generation.

The significance of the work is that it can help increase the level of cyber security of web services that use quantum random number generators, which is an important

component in the security of many systems, including financial ones. The project may also have implications for the development of science, particularly cyber security, and student education in this field.

Research methods. The same methods were used during the research: analysis of modern solutions, analysis of existing threats and existing methods of countermeasures, comparison of protection methods and selection of the most relevant of them in the conditions of Ukrainian specificity, analysis of web resource development methodologies.

Practical value. The research can be used in the development of a real-time, safety-tested quantum random number generator by measuring vacuum fluctuations. An optimized random extraction algorithm is proposed and implemented to overcome the speed gap between fast random generation and slow random extraction. The data can be used in the educational process when studying similar topics.

Approbation of work. The main provisions on the results of the work were presented in an article in a professional journal, which is included in category B.

Keywords: CYBER SECURITY, QUANTUM RANDOM NUMBER GENERATOR, WEB RESOURCE, CYBER THREATS, ANALYSIS METHODS, THREAT IDENTIFICATION, END-TO-END ENCRYPTION.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ ТА СКОРОЧЕНЬ

ADC	Analogue-to-Digital Convertor
BS	Beam Splitter
CPU	Central Processing Generator
DI	Device Independent
E2EE	End to End Encryption
FFT	Fast Fourier Transform
FIFO	First Input First Output
FPGA	Field Programmable Gate Array
GPU	General Processing Generator
H3DH	Extended Triple Diffie-Hellman
IM	Immediate Message
KDF	Key Derivation Function
KS	Kolmogorov-Smirnov
LO	Local Oscillator
MitM	Man in the Middle
OTR	Off the Record
PCIE	Peripheral Component Interconnect Express
RCS	Rich Communication Service
PGV	Pretty Good Privacy
PKI	Public Key Infrastructure
RNG	Random Number Generator
SAS	Short Authentification String
SRTP	Secure Real-time Transport Protocol
QRNG	Quantum Random Number Generator
ZRTP	Zimmerman Real-time Transport Protocol

ВСТУП

Учені з усього світу досліджують проблему захисту квантових генераторів від кіберзагроз, оскільки вони є ключовим елементом в квантовій криптографії. Наприклад, у 2018 році учені з Швейцарії та Китаю запропонували квантово-статистичний підхід до захисту квантових генераторів від кіберзагроз.

У дииломній роботі будуть використані результати попередніх досліджень та розробок з квантової криптографії, квантової стеганографії, квантової інформаційної технології та криптоаналізу квантових систем. Наприклад, дослідження про квантову стеганографію можуть бути корисними для розробки методів захисту від кіберзагроз для квантових генераторів випадкових чисел.

Одним з основних методів є розробка моделі безпеки, яка базується на комплексному підході до вирішення проблем безпеки. Це включає аналіз ризиків, ідентифікацію потенційних загроз та вразливостей системи, розробку алгоритмів та процедур захисту, які враховують характеристики квантового генератора випадкових чисел та його взаємодію з іншими компонентами веб-сервісу.

Розробка методу захисту, який забезпечує цілісність та конфіденційність випадкових чисел, є новим напрямком досліджень. В даній роботі розроблено метод захисту, який базується на використанні криптографічних алгоритмів та квантової криптографії для захисту квантового генератора випадкових чисел від кіберзагроз.

Квантові методи застосовуються для забезпечення безпеки передачі даних. Один з таких методів - квантовий ключовий обмін, який забезпечує безпеку передачі ключів шифрування за допомогою квантових криптографічних протоколів.

Результати роботи можуть бути використані в освітніх цілях в межах підготовки фахівців за напрямом «Кібербезпека». Використання квантового генератора випадкових чисел у навчальному процесі дає студентам можливість практично ознайомитися з принципами роботи такого генератора та навчитися захищати веб-сервіси від кіберзагроз. Це може збільшити їх кваліфікацію та підготувати до роботи в області кібербезпеки.

Доробком за тематикою проекту є стаття: І.Д. Горбенко, О.А. Замула, Ю.С. Осипенко (2022). Концепція оцінки ризиків кібербезпеки інформаційної системи об’єкта критичної інфраструктури, 118-130. Вилучено з: http://rt.nure.ua/article/view/262515/258937

1 НАСКРІЗНЕ ШИФРУВАННЯ (E2EE)

Наскрізне шифрування (E2EE) гарантує, що вміст повідомлення буде незрозумілим для будь-кого, крім відправника та одержувача, запобігаючи прочитанню постачальниками послуг, урядовими програмами стеження або зловмисниками типу «людина посередині» (MitM). обмінялися повідомленнями. Після викриття Сноуденом про урядове стеження в 2013 році [56], більше додатків для обміну миттєвими повідомленнями (IM) заявили, що підтримують E2EE. Однак ці додатки для обміну миттєвими повідомленнями та чутливі до численних форм атак, включаючи атаки MitM і підслуховування [6, 72]. Урядові установи, хакери та навіть постачальники послуг миттєвого обміну повідомленнями можуть контролювати ці додатки, щоб проводити програми стеження або викрадати конфіденційну інформацію [5, 10].

Спільнота дослідників безпеки давно почала розглядати програми для приватного чату та безпечні системи онлайн-зв'язку. У 2004 році для забезпечення E2EE був запропонований протокол не запису (OTR) [4]. Він був реалізований як плагін у звичайних клієнтах миттєвих повідомлень, таких як Pidgin [44], але він не широко використовується через проблеми зручності використання [55, 62]. У 2013 році викриття Сноудена підвищили обізнаність громадськості про основні проблеми конфіденційності [35]. Отже, з'явилися інші альтернативи у вигляді нових систем обміну зашифрованими повідомленнями, які забезпечують зв'язок E2EE шляхом прийняття та розширення протоколу OTR. Open Whisper Systems випустила Signal, новий проривний протокол E2EE, у 2013 році, щоб забезпечити E2EE, а також розширені функції безпеки, такі як пряма секретність і майбутня секретність [7, 16]. Signal був розроблений, щоб забезпечити як синхронне, так і асинхронне середовище обміну повідомленнями [36]. Останніми роками протокол Signal використовувався іншими програмами

обміну миттєвими повідомленнями, зокрема Signal і WhatsApp. Зараз Google впроваджує E2EE для розширених комунікаційних служб (RCS) в Android Messages, а Zoom також нещодавно впровадив його для зустрічей [3, 29]. Незважаючи на те, що численні програми обміну миттєвими повідомленнями включають функції E2EE, вони різняться за характеристиками безпеки та зручності використання, концепціями конфіденційності, моделями загроз і претензіями щодо безпеки [62].

Наш внесок у цю роботу подвійний. Спочатку ми досліджуємо найпопулярніші програми E2EE [11, 14, 15, 20, 27, 32, 33, 39, 40, 51, 53, 54, 58, 60, 66, 69–71, 74] і E2EE, що лежить в їх основі протоколи обміну повідомленнями. Базуючись на поточній дослідницькій літературі [1, 4, 7, 9, 16, 17, 21, 26, 36, 47–50, 57, 64], потім ретельно досліджуються та систематизуються їх характеристики E2EE, включаючи їх основні церемонії аутентифікації. Зокрема, ми перевіряємо найважливіший аспект керування ключами, тобто перевірку та автентифікацію відбитків пальців ключа (церемонія автентифікації), а також те, чи процес перевірки чутливий до людських помилок, які можуть призвести до атак MitM. Ми також досліджуємо та систематизуємо безпеку та зручність використання церемоній автентифікації, які використовуються в програмах E2EE. Незважаючи на те, що було проведено кілька досліджень для вивчення популярних служб обміну повідомленнями з точки зору їх безпеки, зручності використання та впровадження, у цій роботі буде розглянуто ширший набір найпопулярніших програм E2EE та їхніх базових церемоній автентифікації. Результати цього документу про систематизацію можуть надати цінні пропозиції для майбутніх досліджень для посилення поточних реалізацій E2EE та вдосконалення церемоній автентифікації в системах E2EE.

1.1 Сучасне наскрізне шифрування

Сучасна реалізація E2EE гарантує, що повідомлення не можуть бути прочитані ніким, крім кінцевих точок зв’язку. На рисунку 1.1 показано, як Аліса та Боб шифрують повідомлення за допомогою найсучаснішого E2EE. Таким чином, більшість додатків E2EE використовують цю схему E2EE, оскільки вона забезпечує надійну наскрізну конфіденційність даних [62]. Однак ці програми використовують постачальника послуг для зберігання відкритих ключів користувачів, обміну відкритими ключами та передачі зашифрованих даних між кінцевими точками. Цей тип реалізації E2EE, який покладається на сервер для розповсюдження ключів, може завадити пасивному зловмиснику MitM, але не може перешкодити активному зловмиснику MitM, який може замінити ключі та таким чином скомпрометувати весь зв’язок між авторизованими користувачами. Отже, зловмисний або зламаний сервер може легко здійснити атаку, відому як а *атака заміни ключа* під час послуги обміну ключами, скомпрометувавши всю систему E2EE. Багато програм E2EE дозволяють користувачам брати участь у прихованому завданні, яке називається церемонією автентифікації. Під час цього завдання користувачі перевіряють свої ключові відбитки пальців і, якщо вони роблять це правильно, перемагають активних зловмисників MitM.

роблять це правильно, перемагають активних зловмисників MitM.

Рисунок 1.1 – Діаграма високого рівня найсучаснішого наскрізного шифрування

1.2 Властивості систем безпечного обміну повідомленнями та модель загрози

- *Конфіденційність* запобігає розповсюдженню вмісту повідомлення без дозволу. Це означає, що лише відправник і одержувач можуть читати повідомлення.
- *Цілісність* гарантує, що повідомлення не було змінено під час надсилання, тому призначений одержувач отримає оригінальне повідомлення.
- *Автентифікація* розкриває особи відправника та одержувача в приватній розмові, що гарантує, що повідомлення надіслано від заявленого відправника.
- *Ідеальна передня секретність* гарантує, що дані, які вже були зашифровані, не можуть бути розшифровані, навіть якщо всі ключові матеріали скомпрометовані.
- *Майбутня* (*зворотна) секретність* гарантує, що зашифровані дані не можна буде розшифрувати в майбутньому, навіть якщо всі ключові матеріали будуть скомпрометовані.
- *Заперечення*: обидві сторони розмови повинні мати можливість заперечити, що вони надіслали або зробили повідомлення. Це унеможливлює іншим людям довести, що певне повідомлення надіслано певною стороною розмови.

Із опитування щодо безпечного обміну повідомленнями, проведеним Ангером та ін. [62] припускаємо існування наступних зловмисників:

- Місцевий противник:(Активний/пасивний) зловмисник, який може контролювати локальні мережі з будь-якої сторони розмови, наприклад, власники відкритих бездротових точок доступу.
- Глобальний противник:(Активний/пасивний) зловмисник, який може заволодіти багатьма частинами Інтернет-сервісу (наприклад, могутні національні держави чи великі Інтернет-провайдери).

- Постачальники послуг: Усі оператори послуг можуть розглядатися як потенційні зловмисники, якщо програми E2EE використовують централізовану інфраструктуру для розповсюдження відкритих ключів і зберігання чи пересилання повідомлень, наприклад, за допомогою каталогу відкритих ключів.

Як зазначено в [62], ми припускаємо, що зловмисники можуть використовувати програми E2EE, що дозволяє їм створювати облікові записи та надсилати повідомлення як законні користувачі. Ми також припускаємо, що кінцеві точки програм E2EE захищені.

1.3 Протоколи обміну повідомленнями з наскрізним шифруванням

У 2004 році протокол OTR був представлений як криптографічний протокол для забезпечення функції E2EE [4]. Він замінив досить хорошу конфіденційність (PGP), щоб забезпечити повну пряму таємність і заборонену автентифікацію, імітуючи приватне спілкування в реальному світі. Через уразливість базового протоколу обміну ключами Діффі-Хеллмана до атак MitM, протокол OTR використовує різновиди протоколу SIGMA [28] як обмін ключами з автентифікацією для забезпечення автентифікації [45]. Протокол OTR реалізовано як плагін у стандартних клієнтах миттєвих повідомлень, таких як Pidgin; однак дослідники виявили, що ці реалізації мають низку проблем зручності використання [55, 62]. Крім того, протокол OTR не підтримує асинхронне середовище обміну повідомленнями або груповий обмін повідомленнями, оскільки він був розроблений для середовищ синхронного обміну повідомленнями [12].

Протокол Signal був представлений у 2013 році компанією Open Whisper Systems, щоб забезпечити E2EE, а також розширені функції безпеки, такі як пряма секретність і майбутня секретність [7, 16]. Він підтримує як синхронні, так і асинхронні середовища обміну повідомленнями [36]. Signal використовує

протокол узгодження розширеного потрійного ключа Діффі-Хеллмана (X3DH) для встановлення спільного секретного ключа між двома користувачами, які взаємно автентифікують один одного на основі своїх відкритих ключів, таким чином забезпечуючи пряму секретність і криптографічну заборону [37]. Протокол X3DH розроблено для асинхронних середовищ, у яких користувач (Боб) може перейти в режим офлайн після завантаження інформації на сервер, а інший користувач (Аліса) може використовувати цю інформацію для надсилання зашифрованих даних Бобу, таким чином встановлюючи спільний секретний ключ для майбутнє спілкування. Використовуючи спільний секретний ключ, обидва користувачі можуть використовувати алгоритм Double Ratchet для обміну зашифрованими повідомленнями [43]. Алгоритм Double Ratchet використовує ланцюжок функції отримання ключів (KDF) для отримання секретних ключів для шифрування повідомлень. В останні роки протокол Signal було прийнято кількома програмами E2EE. Крім того, деякі протоколи налаштовують власні специфікації, щоб скопіювати певні функції безпеки з протоколу Signal і таким чином реалізувати функцію E2EE. Наприклад, протокол Matrix [38] використовує бібліотеку шифрування Olm, яка базується на протоколі Signal, для реалізації функції E2EE у програмі Element [11].

Кілька додатків E2EE використовують власні власні протоколи, такі як iMessage від Apple, протокол MTProto від Telegram і багато інших додатків E2EE (розглянемо далі в розділі 4). Linphone [33] і Silent Phone [53] використовують транспортний протокол Zimmermann Real-time Transport Protocol (ZRTP) [73] для реалізації функції E2EE для голосового та відеозв’язку. ZRTP — це протокол узгодження ключів, який використовує обмін ключами Діффі-Хеллмана для встановлення спільного секрету між двома кінцевими точками. Цей спільний секрет потім використовується для встановлення безпечних сеансів транспортного протоколу реального часу (SRTP) для програм [73]. Однак відомо, що обмін ключами Діффі-Хеллмана чутливий до атак MitM, і тому ZRTP

використовує механізм, заснований на короткому рядку автентифікації (SAS), щоб запобігти такому типу атак [63]. Цей SAS може бути перевірений кінцевими користувачами, щоб гарантувати відсутність атаки MitM.

Незважаючи на те, що різні аспекти ландшафту захищених повідомлень були систематизовані в попередніх дослідженнях, ця систематизація документів надає унікальну та додаткову перспективу. Попередня робота була зосереджена на захищеному обміні повідомленнями та проводила лише дослідження високого рівня основних концепцій і особливостей протоколів обміну повідомленнями E2EE [4, 7, 16, 45]. Наскільки нам відомо, наша робота є першою, яка вивчає ширший набір найпопулярніших програм E2EE, включаючи їхні базові церемонії автентифікації. Деякі інші статті також досліджують безпеку додатків E2EE та зручність використання базових церемоній автентифікації; однак вони роблять це без проведення систематичного дослідження, яке охоплює велику кількість програм E2EE, натомість зосереджуючись лише на одній або кількох програмах [1, 17, 21, 26, 46, 47, 50, 64, 65]. Ці дослідження також не зосереджені на безпеці E2EE та зручності використання церемонії автентифікації в групових сценаріях. Найтісніше пов’язана робота Herzberg et al. [22], який розкриває проблеми та обмеження поточної церемонії автентифікації в деяких захищених програмах обміну повідомленнями. Ми поділяємо спільний підхід до висвітлення важливості церемонії автентифікації та її зручності використання в поточних програмах E2EE; однак ми охоплюємо велику кількість популярних програм E2EE і зосереджуємося не лише на церемонії автентифікації, але й на реалізації функції E2EE у цих програмах E2EE. Ми також докладаємо більше зусиль для застосування методології для оцінки реалізації функції E2EE та церемоній автентифікації в групових сценаріях.

1.4 Методика систематизації

Нещодавно було зроблено заяви про те, що численні програми для обміну миттєвими повідомленнями забезпечують безпечні рішення для обміну повідомленнями. Однак вони були заражені незрозумілими претензіями щодо безпеки та проблемами зручності використання [62]. Щоб систематизувати знання про найпопулярніші програми E2EE, ми розробили та впровадили підхід, описаний у цьому розділі. Після того, як Сноуден оприлюднив інформацію про широке державне стеження в 2013 році [56], як академічні кола, так і промисловість виявили зростаючий інтерес до розробки безпечних комунікаційних рішень. За останні роки кількість програм E2EE також значно зросла. Базуючись на наявній дослідницькій літературі та загальнодоступних програмах обміну повідомленнями, ми обмежили наш аналіз найпопулярнішими програмами E2EE, зосередившись на систематизації та оцінці того, як вони реалізували свою функціональність E2EE та основні церемонії автентифікації. Ми перевірили відповідні офіційні документи, документацію, дослідницьку літературу та визначення протоколу E2EE. На додаток до вивчення їхніх функціональних можливостей і впровадження E2EE, ми також досліджували їхні базові церемонії автентифікації. Ми ретельно перевірили відомі програми E2EE (див. Розділ 4). Ми обмежили наше дослідження колекцією дуже популярних програм E2EE, сумісних з Android або iOS, на основі кількості встановлень і рейтингів, отриманих із Google Play Store. Apple App Store публічно не розголошує кількість установок програми; однак ми вважаємо, що дані, доступні в Google Play Store, надають достатню інформацію про популярність програми. Таблиця 3 у Додатку A.3 показує 17 дуже популярних програм E2EE, останнє оновлення яких відбулося 25 грудня 2022 року. Ми розглянули програми, у яких реалізовано найсучаснішу функцію E2EE, і надано документацію щодо їх функцій E2EE. Оскільки всі програми, перелічені в таблиці 3, сумісні як з Android, так і з iOS, нам довелося включити в наше дослідження дві додаткові

програми (а саме, FaceTime і Messages від Apple), які підтримуються лише на пристроях Apple як програми за замовчуванням, але не підтримуються на Android пристроїв. Обидві програми також реалізують найсучаснішу функцію E2EE та надають документацію щодо своїх функцій E2EE. Ми розглянули відповідні офіційні документи, документацію E2EE та дослідницьку літературу на основі конференцій найвищого рівня та цитат Google Scholar. Ці академічні та неакадемічні посилання були використані для дослідження того, як функціональність E2EE зараз використовується в програмах E2EE. Ми спеціально шукали основний протокол E2EE, який програма E2EE використовує для реалізації функцій E2EE, і криптографічні примітиви, від яких залежить основний протокол E2EE. Ми також провели практичний аналіз функцій E2EE, які надають програми E2EE, і різні методи перевірки коду, які використовують програми E2EE під час церемоній автентифікації. На цьому етапі ми перевірили зручність використання церемоній автентифікації в програмах E2EE і те, як людські помилки можуть вплинути на зручність використання та призвести до атак MitM на основі наявної дослідницької літератури. Для додатків E2EE, які розглядаються, ми мали намір оцінити кілька критеріїв щодо впровадження в них функції E2EE, включаючи їхні базові протоколи повідомлень E2EE та церемонії автентифікації. Критерії, що оцінюються, можна розділити на дві категорії:

A. Безпека

- Протоколи E2EE, які використовуються програмами E2EE для реалізації функції E2EE.
- Чи надається функція E2EE за умовчанням чи як додаткова властивість.
- Чи підтримує програма E2EE функцію E2EE для обміну текстовими повідомленнями та аудіо/відеодзвінків.
- Чи реалізують програми E2EE функцію E2EE у групових сценаріях, таких як групові повідомлення та групові аудіо- чи відеодзвінки.

- Чи опортуністичний режим E2EE вразливий до активних атак MitM.
- Чи надає програма E2EE спосіб перевірки та автентифікації відбитків ключа (церемонія автентифікації) для запобігання активним атакам MitM.
- Чи є церемонія аутентифікації першочерговим завданням чи ні.

Б. Практичність

- Як користувачі знаходять церемонію автентифікації, щоб виконати її.
- Термінологія, яку програми E2EE використовують для позначення церемонії автентифікації.
- Як відбиток пальця ключа представляється користувачеві для участі в церемонії автентифікації.
- Як користувачам пропонується виконати церемонію автентифікації.
- Як користувачі виконують церемонію автентифікації в групах.
- Чи дозволяє програма E2EE користувачам обмінюватися кодами відбитків пальців через позасмуговий (OOB) канал безпосередньо з програми.
- Чи є церемонія автентифікації вразливою до людських помилок, які можуть призвести до атак MitM.

1.5 Аналіз застосувань E2EE

У цьому підрозділі буде порівняно оцінені програми E2EE щодо критеріїв, пов’язаних із впровадженням функції E2EE. Короткий опис цих реалізацій можна знайти в таблиці 1.1. Результати в основному були взяті з наших експериментів із вивчення програм E2EE, а також документації E2EE та офіційних технічних документів щодо безпеки відповідних програм E2EE. Ми перевіряємо, як функція E2EE зараз реалізована в найпопулярніших програмах E2EE (тільки в програмах для смартфонів), які стверджують, що пропонують рішення для обміну повідомленнями E2EE. У цих програмах функція E2EE увімкнена за замовчуванням або може бути включена користувачем. В обох випадках ці

програми використовують оппортуністичний режим E2EE, що означає, що вони встановлюють безпечний канал між двома сторонами без автентифікації іншої сторони [31]. Цей опортуністичний режим E2EE може перемогти пасивного зловмисника MitM, але він не може перемогти активного зловмисника MitM, який може змінити ключі та поставити під загрозу весь зв'язок між законними користувачами [21].

У наших експериментах ми перевіряли кожну програму E2EE у два етапи. На першому етапі ми проаналізували відповідні офіційні документи та документацію E2EE, щоб визначити, який протокол E2EE використовується кожною програмою E2EE та які криптографічні примітиви реалізовані протоколом E2EE. На другому етапі ми провели власні тести, щоб побачити, як функція E2EE працювала в кожній програмі E2EE і як вона була реалізована як в особистих, так і в групових розмовах. Для цього ми використали чотири різні телефонні пристрої (а саме Apple iPhone X, Apple iPhone 7 Plus, Samsung Android 5 Google Pixel) і встановили на них останню версію кожної програми E2EE. Для сценаріїв «один на один» ми використовували встановлену програму E2EE для надсилання текстового повідомлення з одного телефону на інший. Це дозволило нам побачити, чи було текстове повідомлення зашифровано за замовчуванням у режимі E2EE, чи користувач мав увімкнути додатковий режим E2EE. Ми також дотримувалися тієї ж процедури для аудіо- та відеорозмов між двома окремими смартфони, щоб оцінити, чи програма E2EE пропонує функцію E2EE за замовчуванням або як вибір під час ініціювання аудіо- та відеодзвінків. Для групових сценаріїв ми створили групу з трьох різних смартфонів у програмі E2EE, яка підтримує груповий обмін повідомленнями. Потім ми дотримувалися тих самих процедур для надсилання текстових повідомлень, а також здійснення аудіо- та відеодзвінків у групових сценаріях. Це дало нам змогу визначити, чи групові текстові повідомлення, аудіо- та відеорозмови реалізують функцію E2EE за замовчуванням чи за бажанням. У програмах E2EE будь-яка розмова між

двома користувачами називається *сценарій один на один*, тоді як розмова між більш ніж двома користувачами називається *груповий сценарій*. Тому ми вирішили обмежити наш аналіз розміром групи з трьох різних смартфонів. Це було дуже корисно для отримання результатів і уроків для нашого поточного дослідження. Однак у майбутніх дослідженнях розмір групи може бути збільшений до більш ніж трьох для подальшого вивчення функціональності E2EE у сучасних програмах обміну повідомленнями.

1.6 Програми E2EE, що використовують протокол сигналу

Більшість програм E2EE використовують протокол Signal або значною мірою покладаються на спеціальні протоколи, які копіюють деякі функції безпеки протоколу Signal. Протокол Signal розроблено для роботи як у синхронних, так і в асинхронних середовищах обміну повідомленнями, тому він використовує сервер розповсюдження ключів для зберігання ідентифікаційних даних і тимчасових ключів своїх користувачів. Фрош та ін. [16] і Cohn-Gordon et al. [7] досліджували безпеку протоколу Signal у своїх дослідженнях. Вони виявили, що користувачі повинні були зареєструватися та завантажити свої довгострокові, середньострокові та ефемерні відкриті ключі на сервер розподілу ключів як частину процесу реєстрації. У [7] автори також виявили, що сервер розповсюдження ключів може стати шкідливим сервером і, як наслідок, використовуватися в атаках MitM. Вони виявили, що Signal має церемонію автентифікації, яка дозволяє користувачам перевіряти відкриті ключі через OOB-канал. Однак були сумніви щодо деяких реалізацій протоколу Signal, які могли не вимагати проведення такої церемонії. Це дозволить шахрайському серверу або зловмиснику, який контролює реєстрацію особи, змінити ключі та отримати повідомлення з іншого боку. Герцберг та ін. [21] досліджували, як WhatsApp, Viber, Telegram і Signal використовують E2EE, і виявили, що всі чотири програми підтримують як опортуністичний режим E2EE, так і автентифікований режим

E2EE. Автори заявили, що автентифікований режим E2EE відповідає класичному визначенню E2EE, який захищає користувачів від шахрайського оператора MitM, тоді як опортуністичний режим E2EE сам по собі не захищений від такого типу атак. Виявилено, що більшість користувачів не знають, у чому різниця між цими двома режимами, і не використовують їх ефективно. Далі докладніше представляємо кожну програму E2EE. Також представляємо нашу оцінку, яка докладніше розповідає про функції E2EE, які пропонують ці програми E2EE.

Facebook

Messenger Це програма для обміну миттєвими повідомленнями з можливостями голосових і відеодзвінків, розроблена Meta [14]. Він використовує протокол Signal для реалізації функцій E2EE у чатах і дзвінках за допомогою функції під назвою *Таємна розмова* [13]. Функція *Таємна розмова* не є параметром за замовчуванням, тому користувачі повинні ввімкнути *Таємна розмова* вручну та попросіть одержувачів увімкнути *Таємна розмова* на своїх пристроях. Окрім індивідуальних чатів і дзвінків, програма Facebook Messenger також реалізує функцію E2EE у групових чатах і дзвінках через функцію *Таємна розмова*.

Signal

Це програма для послуг миттєвих повідомлень [51]. Він використовує протокол Signal для реалізації E2EE у всіх індивідуальних і групових чатах за замовчуванням [52]. Він також підтримує E2EE для голосового та відеозв’язку між двома сторонами та групових відеодзвінків. RingRTC, бібліотека відеодзвінків з відкритим кодом, написана на Rust, використовується програмою Signal для надання послуг відео- та голосових викликів на додаток до веб-зв’язку в реальному часі (WebRTC).

WhatsApp

Це програма, що належить Meta для послуг миттєвого обміну повідомленнями [69]. Він використовує протокол Signal для реалізації функції

E2EE за замовчуванням у всіх повідомленнях і викликах для всіх індивідуальних і групових сценаріїв [68]. Під час усіх індивідуальних і групових викликів користувач ініціює голосовий або відеовиклик, встановлюючи зашифровані сеанси з кожним із пристроїв одержувача, наприклад, тих, які використовуються в сценарії обміну повідомленнями. Після здійснення дзвінка SRTP використовується для його захисту за допомогою головних секретних ключів, створених для кожного пристрою одержувача.

Інші програми E2EE

Через обмеження простору інші програми E2EE, які використовують протокол Signal, включено до Додатку А.1. Ці програми E2EE перераховані в таблицях 1.1 і 1.2, але більш детально вони представлені в Додатку А.1.

1.7 Програми E2EE, що використовують власні протоколи

Тут ми представимо додатки E2EE, які реалізують власні протоколи, щоб забезпечити функцію E2EE. Ми також представимо нашу оцінку, у якій більш детально досліджуємо їхні реалізації функції E2EE.

Telegram

Це хмарний месенджер для служб обміну миттєвими повідомленнями [58]. Він використовує свій індивідуальний протокол, який називається протоколом MTProto, для реалізації функції E2EE в чатах і дзвінках один на один [59]. Однак функція E2EE не підтримується в групових сценаріях. У всіх сценаріях «один-на-один» програма Telegram не реалізує функцію E2EE за замовчуванням; таким чином, користувачі повинні ввімкнути *Секретний чат* для захисту своїх комунікацій у режимі E2EE. Для обміну криптографічними ключами в протоколі MTProto використовується протокол Діффі-Хеллмана. Коли *Секретний чат* налаштовано, пристрої, які в ньому беруть участь, обмінюються цими ключами.

Viber

Це програма для обміну миттєвими повідомленнями, що належить Rakuten [66]. Він реалізує функцію E2EE, використовуючи ті самі концепції, що й

протокол Signal [67]. Проте програма Viber використовує власну реалізацію для захисту всіх повідомлень і дзвінків у стилі E2EE. У додатку Viber функція E2EE увімкнена за замовчуванням у всіх індивідуальних і групових сценаріях. У дзвінках Viber потік аудіо- та відеодзвінків перетворюється на протокол SRTP і шифрується за допомогою алгоритму Salsa20.

Zoom

Це хмарна платформа для відеозустрічей і командного чату [74]. Нещодавно компанія Zoom додала функцію E2EE до зустрічей Zoom і телефонних дзвінків Zoom між двома кінцевими користувачами [29, 30]. За замовчуванням Zoom-зустрічі та Zoom-телефонні дзвінки між двома кінцевими користувачами не є E2EE. Це означає, що користувачі повинні ввімкнути функцію E2EE через веб-портал Zoom. Щоб реалізувати функцію E2EE, Zoom використовує криптографію з відкритим ключем для розповсюдження сеансового ключа всім користувачам, які беруть участь у зустрічі Zoom [75]. Zoom використовує Diffie-Hellman над Curve25519, алгоритм цифрового підпису Edwards-curve (EdDSA) і розширене шифрування стандарт (AES) у GCMmode для функції E2EE у Zoommeetings. Виведення ключа здійснюється за допомогою функції виведення ключа на основі HMAC (HKDF). Zoom використовує ті самі криптографічні методи та систему керування ключами, що й зустрічі Zoom для функції E2EE під час індивідуальних телефонних дзвінків Zoom.

Інші програми E2EE

Через обмеження простору інші програми E2EE, які використовують власні протоколи E2EE, можна знайти в Додатку А.2. Ці програми E2EE перераховані в таблицях 1.1 і 1.2, але більш детально представлені в Додатку А.2.

1.8 Непрозорість додатків E2EE

Багато програм E2EE вводять користувачів в оману, стверджуючи, що вони зашифровані або безпечні комунікаційні платформи. Згідно з всебічним

опитуванням безпечного обміну повідомленнями, проведеним Unger et al. [62], деякі з цих програм не надають рішень для обміну повідомленнями E2EE, як це рекламується. Не всі програми E2EE підтримують функцію E2EE за умовчанням, і це може заплутати нових користувачів, які використовують ці програми для надсилання конфіденційної інформації. Крім того, як було зазначено раніше, опортуністичний режим E2EE стійкий до пасивних атак MitM, але чутливий до активних атак MitM. Більшість додатків E2EE сповіщають користувачів про те, що режим E2EE активовано та їхні зв'язки є E2EE, використовуючи різні індикатори, як-от спеціальні сповіщення та піктограми замка, щоб вказати, що режим увімкнено (див. рисунок 3 у Додатку А.3). Звичайним користувачам це може ускладнити виявлення активних атак MitM, особливо якщо вони не знають про ризики безпеці, спричинені неперевіркою відбитків пальців. В [1] Abu-Salma et al. провели дослідження за участю 22 учасників (одинадцять із яких були користувачами Telegram) і дослідили кілька елементів безпеки програми Telegram. Автори повідомили, що дизайн інтерфейсу користувача згубно вплинув на поведінку учасників під час церемонії автентифікації через кілька проблем дизайну. Вони також виявили, що всі учасники не знали про корисність відбитків пальців. Крім того, вони помітили, що, незважаючи на попередній досвід роботи з Telegram, жоден з одинадцяти користувачів не використовував відбитки пальців. Тому користувачі повинні брати участь у церемонії автентифікації, щоб перевірити свої відбитки пальців і запобігти активним атакам MitM. Участь у верифікації та автентифікації цих ключових відбитків пальців увімкне автентифікований режим E2EE, який підтримується більшістю програм E2EE.

1.9 Аналіз автентифікації. Церемонія

Після того, як було досліджено поточну реалізацію функції E2EE у багатьох програмах E2EE, цей опис базується на цьому та досліджує зручність

використання церемонії автентифікації в програмах E2EE та те, як користувачі можуть брати участь у такій церемонії автентифікації. Для кожної програми E2EE ми оцінюємо виконання критеріїв, пов’язаних із церемоніями автентифікації. Це надає огляд відмінностей між програмами E2EE, а також їхніми основними церемоніями автентифікації. Ми перевіряємо поточну реалізацію церемонії автентифікації в програмах E2EE на основі відповідних офіційних документів, документації та наукової літератури, а деяку інформацію було зібрано шляхом вивчення програм E2EE. Усі програми E2EE, проаналізовані в цьому дослідженні, використовують однаковий підхід до реалізації церемонії автентифікації, яка складається з виконання цього завдання необов’язковим, покладаючись на те, що користувачі знайдуть і виконають його, і нададуть користувачам подібні представлення коду для порівняння та перевірки своїх відбитків пальців. Таким чином, замість того, щоб зосереджуватися на одній програмі, як у попередньому розділі, у цьому розділі розглядається та оцінюється церемонія автентифікації в цілому, використовуючи знання, отримані в результаті вивчення програм E2EE та відповідних посилань. У наступних підрозділах ми надамо поглиблений аналіз церемонії автентифікації та можливості її використання в усіх програмах E2EE. Зауважте, що на практиці деякі програми E2EE мають ті самі проблеми з зручністю використання та технічні проблеми з церемонією автентифікації. Короткий виклад цього аналізу можна знайти в таблиці 1.2.

Таблиця 1.1 – Безпека впровадження функції наскрізного шифрування в додатках із наскрізним шифруванням

Застосунок	E2EE	Функція E2EE у сценарії «один-на-один».				Функція E2EE у груповому сценарії				Вразливий на Активний	Надання методу
	Протокол	E2EE	У чаті	В аудіо	У відео	E2EE	У чаті	В аудіо	У відео		щоб перейти в режим
		Режим		Телефонуйте	Телефонуйте	Режим		Телефонуйте	Телефонуйте	Атака MitM	автентифікації E2EE
елемент	Власний	Опортуністичний за замовчуванням	✓	✓	✓	Опортуністичний за замовчуванням	✓	✓	✓	Так	Так, це покладається на те, що користувачі можуть виконувати за бажанням церемонія аутентифікації.
Facebook Messenger	Сигнал	Опортуністичний через опцію	✓	✓	✓	Опортуністичний через опцію	✓	✓	✓	Так	Так, це покладається на те, що користувачі можуть виконувати за бажанням церемонія аутентифікації.
FaceTime	Власний	Опортуністичний за замовчуванням	Н.Д.	✓	✓	Опортуністичний за замовчуванням	Н.Д.	✓	✓	Так	Немає

Продовження таблиці 1.1 – Безпека впровадження функції наскрізного шифрування в додатках із наскрізним шифруванням

Google Meet	Сигнал	Опортуністичний за замовчуванням	✓	✓	✓	Опортуністичний за замовчуванням	✓	✓	✓	Так	Немає
KakaoTalk	Власний	Опортуністичний через опцію	✓	✗	✗	Опортуністичний через опцію	✓	✗	✗	Так	Так, це покладається на те, що користувачі можуть виконувати за бажанням церемонія аутентифікації.
LINE	Власний	Опортуністичний за замовчуванням	✓	✓	✓	Опортуністичний за замовчуванням	✓	✗	✗	Так	Так, це покладається на те, що користувачі можуть виконувати за бажанням церемонія аутентифікації.
Linphone	Власний	Опортуністичний через опцію	✓	✓	✓	Опортуністичний через опцію	✓	✗	✗	Так	Так, це покладається на те, що користувачі можуть виконувати за бажанням церемонія аутентифікації.
Повідомлення від Apple	Власний	Опортуністичний за замовчуванням через iMessage	✓	Н.Д.	Н.Д.	Опортуністичний за замовчуванням через iMessage	✓	Н.Д.	Н.Д.	Так	Немає

Продовження таблиці 1.1 – Безпека впровадження функції наскрізного шифрування в додатках із наскрізним шифруванням

Повідомлення від Google	Сигнал	Опортуністичний за замовчуванням в RCS	✓	Н.Д.	Н.Д.	Н.Д.	Н.Д.	Н.Д.	Н.Д.	Так	Так, це покладається на те, що користувачі можуть виконувати за бажанням церемонія аутентифікації.
Signal	Сигнал	Опортуністичний за замовчуванням	✓	✓	✓	Опортуністичний за замовчуванням	✓	✓	✓	Так	Так, це покладається на те, що користувачі можуть виконувати за бажанням церемонія аутентифікації.
Безшумний телефон	Власний	Опортуністичний за замовчуванням	✓	✓	✓	Опортуністичний за замовчуванням	✓	✓	✓	Так	Так, це покладається на те, що користувачі можуть виконувати за бажанням церемонія аутентифікації.
Skype	Сигнал	Опортуністичний через опцію	✓	✓	✗	Н.Д.	Н.Д.	Н.Д.	Н.Д.	Так	Так, це покладається на те, що користувачі можуть виконувати за бажанням церемонія аутентифікації.
Telegram	Власний	Опортуністичний через опцію	✓	✓	✓	Н.Д.	Н.Д.	Н.Д.	Н.Д.	Так	Так, це покладається на те, що користувачі можуть виконувати за бажанням

Продовження таблиці 1.1 – Безпека впровадження функції наскрізного шифрування в додатках із наскрізним шифруванням

											церемонія аутентифікації.
											Так, це покладається на те, що
Threema	Власний	Опортуністичний за замовчуванням	✓	✓	✓	Опортуністичний за замовчуванням	✓	✓	✓	Так	користувачі можуть виконувати за бажанням
											церемонія аутентифікації.
											Так, це покладається на те, що
Viber	Власний	Опортуністичний за замовчуванням	✓	✓	✓	Опортуністичний за замовчуванням	✓	✓	✓	Так	користувачі можуть виконувати за бажанням
											церемонія аутентифікації.
											Так, це покладається на те, що
WhatsApp	Сигнал	Опортуністичний за замовчуванням	✓	✓	✓	Опортуністичний за замовчуванням	✓	✓	✓	Так	користувачі можуть виконувати за бажанням
											церемонія аутентифікації.
											Так, це покладається на те, що
Wickr	Власний	Опортуністичний за замовчуванням	✓	✓	✓	Опортуністичний за замовчуванням	✓	✓	✓	Так	користувачі можуть виконувати за бажанням

Продовження таблиці 1.1 – Безпека впровадження функції наскрізного шифрування в додатках із наскрізним шифруванням

											церемонія аутентифікації.
WIRE	Власний	Опортуністичний за замовчуванням	✓	✓	✓	Опортуністичний за замовчуванням	✓	✓	✓	Так	Так, це покладається на те, що користувачі можуть виконувати за бажанням
											церемонія аутентифікації.
ZOOM	Власний	Опортуністичний через опцію	✓	✓	✓	Опортуністичний через опцію	✓	✓	✓	Так	Так, це покладається на те, що користувачі можуть виконувати за бажанням
											церемонія аутентифікації.

✓ вказує на наявність функції E2EE та✗означає, що функція E2EE не надається, н.д. – немає даних.

1.10 Пошук і проведення церемонії

Участь у церемонії автентифікації та її успішне завершення увімкне автентифікований режим E2EE, який узгоджується з традиційним визначенням E2EE. На відміну від оппортуністичного режиму E2EE, автентифікований режим E2EE гарантує що жодні активні зловмисники MitM не беруть участі в приватній розмові між двома кінцевими користувачами. Щоразу, коли Аліса та Боб хочуть спілкуватися за допомогою програми E2EE, вони обоє використовують постачальника послуг для обміну своїми відкритими ключами шифрування та встановлення секретного спільного ключа для майбутнього спілкування. Цей секретний спільний ключ відомий лише Алісі та Бобу. Ніхто інший, навіть

постачальник послуг, не може дізнатися значення секретного спільного ключа або розшифрувати будь-яке з надісланих повідомлень. Однак ці постачальники послуг можуть використовувати фальшиві відкриті ключі під час служби обміну ключами, щоб уникнути захисту, який пропонують програми E2EE від шахраїв або скомпрометованих постачальників послуг. Наприклад, коли Аліса хоче поговорити з Бобом через програму E2EE, вона отримає його відкритий ключ від постачальника послуг, щоб зашифрувати спільний секретний ключ, а потім надішле його йому через постачальника послуг. Однак зловмисний постачальник може легко встановити *атака заміни ключа* і надати їй фальшивий відкритий ключ під своїм контролем. Зловмисний постачальник тепер може розшифрувати спільний секретний ключ, повторно зашифрувати його за допомогою real Боба відкритий ключ, а потім надішліть його Бобу, стверджуючи, що його надіслала Аліса. Таким чином, шахрайський постачальник став активним зловмисником MitM між Алісою та Бобом. Це означає, що зловмисник може читати або змінювати повідомлення, які Аліса та Боб надсилають один одному, без відома двох атакованих сторін. У реальному світі всі програми E2EE, згадані в Розділі 4, реалізують цей оппортуністичний режим E2EE за замовчуванням, який, як відомо, захищений лише від пасивних атак MitM. Щоб перейти в режим E2EE з автентифікацією та запобігти активним атакам MitM, обидва кінцеві користувачі повинні взяти участь у церемонії автентифікації та успішно її завершити.

Незважаючи на важливість церемонії автентифікації для виявлення активних атак MitM, церемонія автентифікації є необов’язковою для всіх поточних програм E2EE. Отже, користувачі можуть бути вразливими до людських помилок, що може призвести до атак MitM. Таким чином, автентифікований режим E2EE залежить від користувачів і того, як вони взаємодіють під час церемонії автентифікації для встановлення довіри та забезпечення безпечного зв’язку. Також часто користувачі ігнорують процес автентифікації, доки їх не заохотять це зробити, після чого вони можуть

зіткнутися з труднощами та неправильно зрозуміти кроки, залишаючись уразливими для атак MitM. На практиці всі програми E2EE (які забезпечують механізм для виконання церемонії автентифікації), покладаються на те, що кінцеві користувачі активують автентифікований режим E2EE, усвідомлюючи ризики безпеки та важливість автентифікації для запобігання таким атаку, вжиття необхідних заходів для успішної церемонії автентифікації. Це включає навігацію налаштуваннями програми та системою меню, щоб знайти термінологію, яка використовується для позначення церемонії автентифікації. На рисунку 4 у Додатку А.3 зображено деякі програми E2EE та термінологію, яку вони використовують для позначення церемонії автентифікації. Після визначення місця проведення церемонії автентифікації кінцеві користувачі повинні порівняти та перевірити відбитки пальців ключа, перш ніж вирішити, продовжувати спілкування чи ні. Крім того, кінцеві користувачі повинні розуміти значення невдачі (відбитки пальців, що не збігаються), щоб припинити зв’язок. Як показано в таблиці 1.2, усі програми E2EE (які пропонують механізм для виконання церемонії автентифікації) використовують різні термінології та представлення відбитків пальців у своїх церемоніях автентифікації.

1.11 Відбитки пальців

Під час церемонії автентифікації багато програм E2EE використовують текстові (слова та речення), числові, шістнадцяткові та графічні відбитки пальців. Відображення відбитків пальців ключа є важливим компонентом церемонії автентифікації в усіх програмах E2EE, і воно відіграє важливу роль у допомозі користувачам правильно виконати церемонію автентифікації та запобігати активним атакам MitM. У таких церемоніях автентифікації програми E2EE представляють відбитки ключа шифрування або відбитки відкритих ключів інших користувачів, використовуючи різні підходи (див. таблицю 2). Ці відбитки пальців можна порівняти та перевірити особисто або через OOB-канал,

наприклад текстове повідомлення, електронну пошту чи телефонний дзвінок. Такий відбиток пальця кодується в читаний/замінний код для полегшення ручного порівняння та перевірки. У реальному світі всі програми E2EE (які пропонують механізм для виконання церемонії автентифікації), генерують відбиток пальця та представляють його як зрозумілий людині код або обмінний об’єкт.

QR-код

Ключовий відбиток кодується в QR-код, який може бути автоматично захоплений і порівняний додатком E2EE без необхідності втручання кінцевого користувача. Цей метод найкраще працює, коли церемонія автентифікації виконується особисто, а QR-код сканується особисто. Лише 5 додатків E2EE, проаналізованих у цьому дослідженні (Element, Signal, Threema, WhatsApp і Wickr), пропонують цей метод користувачам, які знаходяться неподалік один від одного, дозволяючи їм виконувати церемонію автентифікації особисто. На малюнку 5a в Додатку A.3 показано подання QR-коду для програми Signal.

Числове представлення

Ключовий відбиток представлений у вигляді послідовності числових цифр для полегшення порівняння та перевірки. Щоб зробити довгий код більш читабельним, цей метод організовано у вигляді блоків (або фрагментів) чисел із кількома цифрами. Наприклад, програма WhatsApp, показана на малюнку 5b у Додатку A.3, використовує 60-значний цифровий рядок, який розбивається на 12 блоків п’ятизначних чисел. Цей метод можна використовувати як особисто, так і дистанційно для порівняння та перевірки відбитка ключа. Це корисно для людей, які перебувають у віддалених місцях і навряд чи зустрінуться особисто до спілкування через програму E2EE. Лише 6 додатків E2EE (Messages by Google, Signal, Skype, Viber, WhatsApp і Zoom), пропонують цей метод своїм користувачам, незалежно від того, знаходяться вони поблизу чи віддалено. Однак у реальному світі лише Signal і WhatsApp пропонують функцію для прямого

обміну відбитком ключа з програми через OOB-канал у віддаленому спілкуванні. Інші додатки покладаються лише на те, що користувачі порівнюють і перевіряють відбиток ключа через OOB-канал за вибором. На малюнку 5b у додатку A.3 показано цифровий відбиток ключа програми WhatsApp і значок спільного доступу у верхньому правому куті екрана телефону, який використовується для прямого обміну відбитком ключа з програми WhatsApp через OOB-канал для виконання автентифікації. церемонія дистанційно.

Буквено-цифрове подання

З метою порівняння та перевірки відбиток ключа відображається в цифровому та алфавітному порядку. Цей підхід можна використовувати, щоб розділити рядок символів на фрагменти однакового розміру, покращуючи читабельність тексту. Його можна використовувати в шістнадцятковому форматі, форматі base32 або base64. Лише 7 програм E2EE, проаналізованих у цій роботі (Facebook Messenger, KakaoTalk, LINE, Telegram, Threema, Wickr і Wire), пропонують цей метод для порівняння та перевірки відбитка ключа особисто або віддалено. На практиці всі вищезазначені програми E2EE відображають відбиток ключа в шістнадцяткових символах (на малюнку 5c у Додатку A.3 показано шістнадцяткове представлення для програми Telegram), і жодна з них не пропонує функцію прямого обміну відбитком ключа в програмі. , за винятком програми Wickr, яка відображає відбиток ключа в символах base32 (як показано на малюнку 5d у Додатку A.3). Хоча представлення Base64 також було запропоновано в літературі, жодна з програм E2EE наразі не використовує його.

Графічне представлення

Ключовий відбиток кодується в зображення або послідовність емодзі для порівняння та перевірки. Цей метод можна використовувати для заміни текстових представлень відбитків пальців і було запропоновано для покращення зручності використання в попередній літературі. Лише 3 програми E2EE, проаналізовані в цьому дослідженні (Element, KakaoTalk і Telegram), пропонують

цей метод для порівняння та перевірка відбитка пальця ключа особисто або дистанційно. Наприклад, на малюнку 5e в Додатку А.3 зображено зображення, отримане з ключа шифрування для програми KakaoTalk. Крім того, на малюнку 5f у Додатку А.3 показано емодзі, які програма Element використовує для порівняння та перевірки відбитка ключа.

Короткий рядок автентифікації

Лише дві програми E2EE, проаналізовані в цій роботі (Linphone і Silent Phone), використовують механізм перевірки на основі SAS (наприклад, чотири символи або два слова) замість буквено-цифрових або числових представлень, щоб зробити завдання порівняння та перевірки під час церемоній аутентифікації більш читабельними. На малюнку 5g у Додатку А.3 показано церемонію автентифікації для програми Linphone, яка використовує код SAS із чотирьох символів для перевірки особи користувача. На малюнку 5h у Додатку А.3 показано церемонію автентифікації для програми Silent Phone, яка використовує код SAS із двох слів для перевірки особи користувача.

Підтримка OOB каналів

На жаль, лише 7 програм, проаналізованих у цьому дослідженні (Linphone, Signal, Silent Phone, Threema, Viber, WhatsApp і Wickr), надають функцію для прямого обміну відбитком ключа зсередини програми за допомогою OOB-каналу, наприклад, текстового повідомлення, електронний лист або телефонний дзвінок. Ці програми покладаються на рішення користувачів використовувати інший надійний засіб зв’язку для порівняння та перевірки своїх відбитків пальців. Наявність такого OOB-каналу може полегшити церемонію автентифікації, особливо для користувачів, які не є близькими один до одного. Крім того, деякі програми E2EE використовують числові представлення та не підтримують OOB-канали, за допомогою яких користувачі можуть виконувати церемонію автентифікації. Наприклад, Zoom використовує цифрові представлення для своїх кодів зустрічей E2EE, але не підтримує OOB-канали для виконання церемонії

автентифікації вручну або навіть будь-який автоматизований процес перевірки. Замість цього організатор наради може прочитати код безпеки вголос, і тому користувачі можуть порівняти та перевірити, чи їхні клієнти відображають той самий код безпеки. Однак супротивник може сидіти й копіювати голос організатора наради, коли оголошує рядок цифр 0-9 із попередніх нарад, і, таким чином, здійснити атаку зі зміною порядку голосу, щоб створити будь-які цифри, які забажає супротивник, і таким чином скомпрометувати функцію E2EE у майбутньому. засідання [48].

1.12 Комунікації групи E2EE

Загалом проблеми з безпекою та перешкоди зручності використання програм E2EE у групових сценаріях подібні до тих, що виникають у сценаріях «один на один». У [26] автори провели аналіз безпеки *Запечатування листів*, яка є схемою E2EE для LINE. Вони знайшли це *Запечатування листів* не відповідає одній із фундаментальних вимог безпеки E2EE, якою є цілісність повідомлення. Їх результати продемонстрували доцільність атак з використанням кількох вразливостей у системі E2EE LINE. Ці атаки можуть бути організовані наскрізним противником, членом зловмисної групи або зловмисним користувачем. Наприклад, зловмисний член групи може здійснити атаки з уособленням або підробкою схеми шифрування групових повідомлень, використовуючи вразливість етапу отримання ключа в шифруванні групових повідомлень.

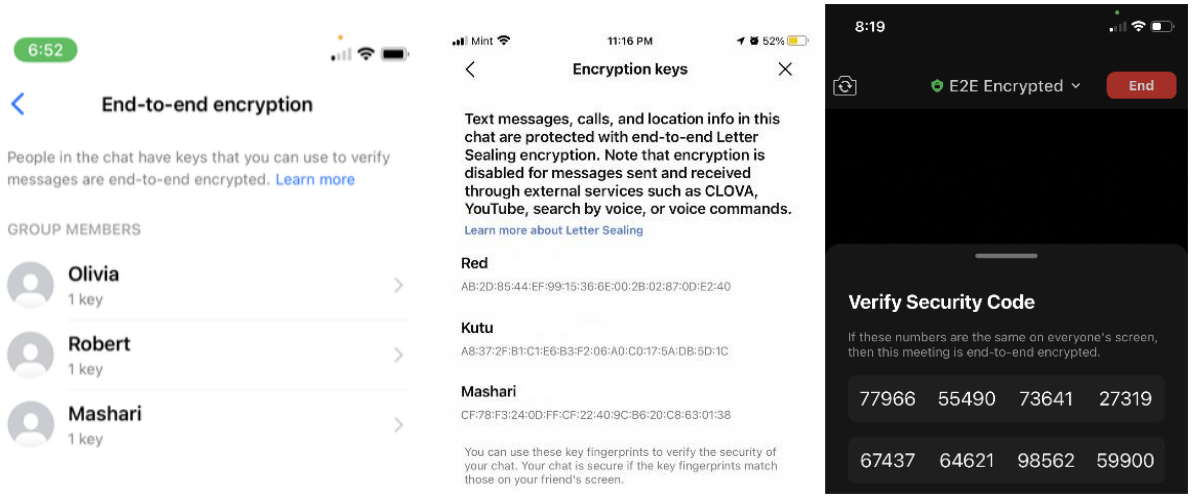

Рисунок 1.2 – Церемонії автентифікації в групових сценаріях E2EE

Більшість додатків E2EE, проаналізованих у цьому дослідженні, підтримують групові комунікації E2EE. Однак участь у церемонії автентифікації не є автентифікацією на основі групи. Це попарна автентифікація, яка схожа на схему автентифікації один-до-одного, таку як церемонія автентифікації для двох сторін. Таким чином, наявність групи з величезною кількістю членів групи зробить церемонію автентифікації надзвичайно проблематичною та більш складною для виконання. Як і в зашифрованому спілкуванні «один-на-один», учасники групи в наскрізному зашифрованому груповому спілкуванні повинні виконати церемонію автентифікації, щоб гарантувати, що розмови між учасниками групи є конфіденційними та автентифікованими, таким чином гарантуючи відсутність атак MitM. Насправді переважна більшість програм E2EE дотримуються однакових процедур для церемонії автентифікації в усіх індивідуальних і групових сценаріях. Наприклад, WhatsApp не дозволяє своїм користувачам під час групового чату автентифікувати один одного груповим способом; швидше, він покладається на попарну індивідуальну автентифікацію. Однак деякі інші програми E2EE відрізняються за налаштуваннями церемонії автентифікації щодо надання ключів своїм користувачам під час церемонії автентифікації, зберігаючи при цьому попарну перевірку відбитків пальців.

Наприклад, програма Facebook Messenger використовує іншу термінологію для позначення церемонії групової автентифікації. Він перераховує всіх учасників групи в одному списку, щоб допомогти користувачам знайти ключ пристрою кожного члена, що може підвищити зручність використання церемонії автентифікації в груповому сценарії. Інша програма перераховує всіх членів групи з їхніми ключами в одному списку, що також може бути корисним для учасників групи з точки зору участі в церемонії автентифікації групи. З іншого боку, є тільки один додаток (Zoom), в якому відбувається церемонія аутентифікації

Таблиця 1.2 – Зручність використання церемонії автентифікації в додатках із наскрізним шифруванням

Застосунок	Термінологія, що використовується для позначення церемонії автентифікації	Відбиток пальця Представництво	Увімкнути церемонію автентифікації автентифікований режим E2EE	Група Церемонія	Підтримуючи Канали OOB	Вразливий до Людські помилки
Element	У індивідуальному та груповому сценаріях: (Перевірити) Одноразовий код	QR код, Екранні емодзі (7 емодзі)	Відскануйте QR-код, Порівняйте емодзі вручну	На основі пар Аутентифікація	Немає	Так, оскільки користувачі вручну порівняти емодзі.

Продовження таблиці 1.2 – Зручність використання церемонії автентифікації в додатках із наскрізним шифруванням

Facebook Messenger	У сценарії 1 до 1: (Клавіші пристрою), У груповому сценарії: (Наскрізне шифрування) Ключі пристрою	66 шістнадцяткових символів для кожного пристрою	Ручне порівняння символів	На основі пар Аутентифікація	Немає	Так, оскільки користувачі вручну порівняти персонажів.
FaceTime	Н.Д.	Н.Д.	Н.Д.	Н.Д.	Н.Д.	Н.Д.
Google Meet	Н.Д.	Н.Д.	Н.Д.	Н.Д.	Н.Д.	Н.Д.
KakaoTalk	У індивідуальному та груповому сценаріях: (Відкритий ключ)	зображення, 32 шістнадцяткові символи для кожної сторони	Порівняти вручну зображення або символи	На основі пар Аутентифікація	Немає	Так, оскільки користувачі вручну порівняти зображення або символів.
LINE	У індивідуальному та груповому сценаріях: (Ключі шифрування)	32 шістнадцяткові символи для кожної сторони	Ручне порівняння символів	На основі пар Аутентифікація	Немає	Так, оскільки користувачі вручну порівняти персонажів.
Linphone	У індивідуальному та груповому сценаріях: (Дзвонити за контактом) Безпека зв'язку	Код SAS з 4 символів	Порівняти SAS вручну через аудіодзвінок	На основі пар Аутентифікація	Так	Так, оскільки користувачі вручну порівняти SAS через аудіодзвінок.

Продовження таблиці 1.2 – Зручність використання церемонії автентифікації в додатках із наскрізним шифруванням

Повідомлення від Apple	Н.Д.	Н.Д.	Н.Д.	Н.Д.	Н.Д.	Н.Д.
Повідомлення від Google	У сценарії 1 до 1: (Перевірити шифрування) Код підтвердження	60-значне число	Порівняти числа вручну	Н.Д.	Немає	Так, оскільки користувачі вручну порівняти числа.
Signal	У індивідуальному та груповому сценаріях: (Переглянути номер безпеки) Перевірте номер безпеки	QR код, 60-значне число	Відскануйте QR-код, Порівняти числа вручну	На основі пар Аутентифікація	Так	Так, оскільки користувачі вручну порівняти числа.
Безшумний телефон	У індивідуальному та груповому сценаріях: (Дзвонити за контактом) Перевірити SAS	Два слова	Порівняйте слова вручну через аудіодзвінок	На основі пар Аутентифікація	Так	Так, оскільки користувачі вручну порівняти слова через аудіодзвінок.
Skype	У сценарії 1 до 1: (Код безпеки)	60-значне число	Порівняти числа вручну	Н.Д.	Немає	Так, оскільки користувачі вручну порівняти числа.

Продовження таблиці 1.2 – Зручність використання церемонії автентифікації в додатках із наскрізним шифруванням

Telegram	У сценарії 1 до 1: (Ключ шифрування)	зображення, 64 шістнадцяткові символи	Порівняти вручну зображення або символи	Н.Д.	Немає	Так, оскільки користувачі вручну порівняти зображення або символів.
Threema	У індивідуальному та груповому сценаріях: (Відбиток ключа)	QR код, 32 шістнадцяткові символи	Відскануйте QR-код, Ручне порівняння символів	На основі пар Аутентифікація	Так	Так, оскільки користувачі вручну порівняти персонажів.
Viber	У індивідуальному та груповому сценаріях: Увімкнути (Довірені контакти) (Зателефонуйте своєму контакту) Перевірте секретний ідентифікаційний ключ	48-значне число	Порівняти числа вручну через аудіодзвінок	На основі пар Аутентифікація	Так	Так, оскільки користувачі вручну порівняти числа через аудіодзвінок.
WhatsApp	У індивідуальному та груповому сценаріях: (Шифрування) Перевірте код безпеки	QR код, 60-значне число	Відскануйте QR-код, Порівняти числа вручну	На основі пар Аутентифікація	Так	Так, оскільки користувачі вручну порівняти числа.

Продовження таблиці 1.2 – Зручність використання церемонії автентифікації в додатках із наскрізним шифруванням

Wickr	У індивідуальному та груповому сценаріях: (Перевірка безпеки) Порівняйте код безпеки	QR код, 51 символ за схемою Base32	Відскануйте QR-код, Ручне порівняння символів	На основі пар Аутентифікація	Так	Так, оскільки користувачі вручну порівняти персонажів.
WIRE	У індивідуальному та груповому сценаріях: (Пристрої) Перевірте відбиток пальця пристрою	64 шістнадцяткові символи для кожного пристрою	Ручне порівняння символів	На основі пар Аутентифікація	Немає	Так, оскільки користувачі вручну порівняти персонажів.
ZOOM	У індивідуальному та груповому сценаріях: (Шифрування) Перевірте код безпеки	40-значне число	Порівняти числа вручну	Груповий Аутентифікація	Немає	Так, оскільки користувачі вручну порівняти числа.

є груповим. Програма Zoom, як показано на малюнку 2c, використовує лише один код безпеки для налаштування наради Zoom, щоб перевірити код безпеки для всіх учасників наради Zoom у поточному сеансі. Тут Zoom дозволяє користувачам порівнювати та перевіряти 40-значне число, представлене у вигляді 8 блоків п’ятизначних чисел, щоб перевірити безпечне з’єднання їхнього сеансу Zoom. Тому організатор наради може прочитати код безпеки вголос, а потім усі користувачі зможуть порівняти та переконатися, що їхні клієнти відображають той самий код безпеки.

Деякі програми E2EE, проаналізовані в цьому дослідженні (Facebook Messenger, KakaoTalk, Linphone, Skype, Telegram і Zoom), не реалізують функцію E2EE за замовчуванням. Користувачам доведеться вручну ввімкнути функцію E2EE, щоб забезпечити безпеку своїх розмов. Це може викликати плутанину у користувачів, які не знайомі зі схемою E2EE. Абу-Салма та ін. [2] досліджували досвід користувачів з різними комунікаційними інструментами та їх сприйняття функцій безпеки цих інструментів. Вони виявили, що користувачі надсилають конфіденційну інформацію за допомогою чату Telegram за замовчуванням, який не є E2EE. На практиці звичайні користувачі можуть почуватися введеними в оману заявами E2EE. Тому ми пропонуємо, щоб будь-яка програма, яка має на меті запропонувати безпечне рішення для обміну повідомленнями E2EE, реалізувала функціональність E2EE за замовчуванням, а не як функцію вибору. Ми також пропонуємо, щоб програми E2EE просили своїх користувачів виконувати церемонію автентифікації як основне завдання. Усі програми E2EE, проаналізовані в цій роботі, реалізують функцію E2EE в оппортуністичному режимі E2EE, чи то за замовчуванням, чи як опцію підключення. На практиці цей опортуністичний режим E2EE сприйнятливий до активних атак MitM; отже, користувачі повинні пройти церемонію автентифікації, щоб активувати автентифікований режим E2EE. Однак церемонія автентифікації є необов’язковою для всіх існуючих програм E2EE. Це може ускладнити виявлення активних MitM-атак, особливо для звичайних користувачів, які не знають про ризики безпеки, пов’язані з пропуском або клацанням через церемонію автентифікації.

Ефективність церемонії автентифікації в сучасних програмах обміну повідомленнями була в центрі уваги численних опублікованих наукових досліджень. Було доведено, що через недоліки зручності використання та людські помилки користувачі не можуть виконати церемонію автентифікації і, отже, є вразливими до атак MitM. У дослідженні, проведеному Schröder et al. [47],

автори виявили, що користувачі не змогли завершити церемонію автентифікації в додатку Signal і тому були сприйнятливі до атак MitM через проблеми з зручністю використання. У дослідженні Vaziripour та ін. [64], автори досліджували легкість визначення місцезнаходження та завершення церемонії автентифікації в WhatsApp, Viber і Facebook Messenger. Вони виявили, що через брак знань про безпеку та різні недоліки дизайну інтерфейсу користувача учасникам було важко знайти та виконати церемонію автентифікації. Крім того, дослідження, проведені Herzberg et al. [21] і Shirvanian et al. [50] досліджували зручність виконання церемонії автентифікації в WhatsApp, Viber, Telegram і Signal і виявили, що учасники були вразливі до атак MitM.

У [21] автори показали, що більшість учасників не змогли пройти автентифікацію, навіть коли їм показали, як це зробити. У [50] автори продемонстрували, що учасники не виконували церемонії віддаленої автентифікації належним чином через труднощі з зручністю використання та людські помилки. Щоб допомогти користувачам знайти та знайти церемонію автентифікації, ми пропонуємо, щоб програми E2EE надсилали сповіщення на початку розмови. Це повідомлення може допомогти поінформувати користувачів про важливість завершення церемонії автентифікації для запобігання атакам MitM. Крім того, ми пропонуємо, щоб програми E2EE надавали користувачам можливість переходу до церемонії автентифікації з інтерфейсу розмови, якщо вони хочуть. Це пов’язано з тим, що основним завданням користувачів у всіх поточних програмах E2EE є продовження розмови, а церемонія автентифікації є лише необов’язковим завданням. З іншого боку, багато, але не всі програми E2EE, проаналізовані в цьому дослідженні, не забезпечують функцію для прямого обміну відбитком ключа зсередини програми за допомогою OOB-каналу, наприклад, текстового повідомлення або електронної пошти. Ця функція може допомогти користувачам завершити церемонію автентифікації, особливо якщо вони не знаходяться поблизу. Тому ми вважаємо, що всі програми E2EE

повинні мати цю функцію, щоб користувачі могли обмінюватися своїми відбитками пальців ізсередини програми через OOB-канал.

Більшість додатків E2EE, згаданих у Розділі 4, досі використовують цифрове або шістнадцяткове представлення відбитків пальців, хоча багато досліджень показали, що інші представлення, наприклад слова та речення, краще допомагають користувачам виявляти атаки. Дечанд та ін. [9] провели дослідження користувачів, щоб дослідити продуктивність і зручність використання шести текстових представлень ключів і відбитків пальців. Вони виявили, що учасники були більш стійкими до атак, коли використовували слова та речення, порівняно з цифровими або буквено-цифровими (шістнадцятковими та Base32) представленнями. Автори повідомили, що схема шістнадцяткового представлення показала себе значно гірше, ніж інші схеми представлення з точки зору виявлення атак і оцінки зручності використання. Подібним чином інша робота Tan et al. [57] досліджували зручність використання та безпеку восьми текстових і візуальних представлень відбитків пальців. Вони виявили, що візуальні відбитки пальців були більш вразливі до атак, ніж інші методи, навіть якщо вони були простими у використанні та швидкими для обробки. У [64] автори досліджували церемонію автентифікації в WhatsApp, Viber і Facebook Messenger. Під час цього дослідження автори помітили, що багато учасників відчували, що рядок цифр і шістнадцятковий рядок, який використовується для представлення відбитків пальців, був надмірно довгим. Крім того, деякі дослідження показали, що телефони E2EE сприйнятливі до атак MitM через людські помилки. Наприклад, дослідження Shirvanian et al. [49] досліджували безпеку та зручність використання телефонів E2EE. У завданнях на порівняння контрольної суми та перевірку мовця автори розглядали два слова та чотири слова. Вони виявили, що користувачі були вразливі до атак MitM через їхні збої в завданнях порівняння контрольної суми та перевірки мовця. Крім того, більшість сучасних програм E2EE використовують числові представлення у своїх

механізмах автентифікації, на що користувачі скаржилися, згідно з дослідницькою літературою. Тому ми рекомендуємо, щоб програми E2EE використовували текстові та візуальні представлення, які полегшують процес автентифікації для користувачів. Однак необхідні додаткові дослідження для вивчення вразливості безпеки цих уявлень.

2 КВАНТОВИЙ ГЕНЕРАТОР ВИПАДКОВИХ ЧИСЕЛ У РЕАЛЬНОМУ ЧАСІ ЗІ ШВИДКІСТЮ 8 ГБІТ/С ІЗ ВИБІРКАМИ, НЕ ПОВ'ЯЗАНИМИ З IID

Випадкові числа всюдисущі в сучасному суспільстві. Вони використовуються в багатьох програмах, починаючи від криптографії, симуляції та азартних ігор до фундаментальних тестів фізики. Для більшості цих програм якість випадкових чисел має величезне значення. Якщо, наприклад, криптографічні ключі, що походять від випадкових чисел, є передбачуваними, це матиме серйозні наслідки для безпеки інтернету. Для забезпечення безпеки криптографічного шифрування випадкові числа мають бути справді випадковими, тобто абсолютно непередбачуваними для всіх і, отже, приватними, а їх випадковість має бути засвідчена [76, 77].

Справжньої непередбачуваності та конфіденційності згенерованих чисел можна досягти за допомогою процесу квантового вимірювання: виконуючи проективне вимірювання на чистому квантовому стані та гарантуючи, що стан не є власним станом вимірювального проектора, результат є непередбачуваним і, отже, справжнім випадковим. можна генерувати числа. Крім того, оскільки чистий стан не можна співвіднести з будь-яким іншим станом у всесвіті, згенеровані числа будуть приватними. Сертифікація дає користувачеві гарантію того, що отримані випадкові числа дійсно є випадковими. Оскільки абсолютно ідеальна випадковість не може бути створена, сертифікація приходить у формі невеликої ймовірності помилки, яка описує, наскільки далекі згенеровані випадкові числа від ідеальних умов.

Незалежні від пристрою (DI) QRNG, засновані на порушенні нерівності Белла, дають найсильнішу сертифікацію випадковості з найменшою кількістю припущень. Однак на сьогоднішній день вони є дуже непрактичними в реальних програмах через їх високу складність і дуже низьку швидкість: наразі перевірені

DI-QRNG базуються на сплутанні атомів [78] або фотонів [79, 80] і створюють випадкові числа приблизно 10^{-5} та 1 біт/с відповідно. Тим не менш, можна зменшити складність системи, замінивши її припущеннями щодо пристрою. Отже, важливим завданням у розробці RNG є оптимізація компромісу між практичністю (технічна складність і швидкість) і надійністю (випадковість сертифікації, непередбачуваність і конфіденційність).

Тут ми розглядаємо дуже практичну систему, залежну від пристрою, яка базується на гомодинному виявленні (чистого) квантово-механічного вакуумного стану. Така проста система є однією з абсолютних передових технологій QRNG, оскільки вона поєднує в собі простоту, економічну ефективність, інтегрованість чіпа та надзвичайно високу швидкість. У порівнянні з попередніми реалізаціями ми зменшили кількість припущень, зокрема тих, які недостатньо обґрунтовані практичними компонентами. Таким чином, наш QRNG ідеально підходить для таких додатків, як класичний і, зокрема, квантовий розподіл ключів, які вимагають найвищих гарантій безпеки та високої швидкості [81].

Є чотири критичні проблеми, пов’язані з продуктивністю залежного від пристрою QRNG, які ще не були враховані в одній реалізації. Більшість попередніх QRNG розглядали всі інформаційні побічні канали як класичні, а не квантові [82–90]. Лише обробляючи їх квантово, випадкові числа можна захистити від супротивника з квантовою підтримкою. Нещодавно цю проблему було вирішено для незалежного від джерела QRNG [91], який вимагає більш складного вимірювального приладу. Крім того, часто вважалося, що вимірювання не корельовані в часі [82–91], але кінцева смуга пропускання будь-якої реальної системи виявлення вводить кореляції, які можна видалити лише приблизно за допомогою методів постобробки (зазвичай зі зниженням швидкості). У більшості попередніх реалізацій також не використовується консервативний і строгий підхід – метрологічний підхід [92] – для визначення

параметрів, важливих для виділення кількості випадковості шляхом обліку недосконалостей і невизначеностей калібрування. Нарешті, нещодавно було продемонстровано високошвидкісне виділення випадковості з використанням теоретично безпечного екстрактора випадковості [90, 93].

За допомогою нашого QRNG ми вирішуємо всі вищезазначені проблеми одночасно: ми обчислюємо нижню межу витягуваної квантової випадковості, включаючи можливість отримання квантової інформації супротивником через бічні канали. Ми враховуємо корельовані вибірки, що є результатом кінцевої смуги пропускання вимірювального пристрою. Ми проводимо метрологічну характеристику вимірювальної гомодинної детекторної системи, щоб кількісно визначити їх безпеку. Нарешті, як наслідок, ми створюємо випадкові числа в режимі реального часу зі швидкістю 8 Гбіт/с за допомогою екстрактора випадковості Тепліца на швидкому програмованому полем вентильному масиві (FPGA), перевищуючи попередній рекорд швидкості реального часу більш ніж на коефіцієнт два. Схема нашого QRNG показана на рис. 2.1. Довільна квадратура вакуумного стану вимірюється за допомогою збалансованого гомодинного детектора, що складається з яскравого опорного пучка, симетричного розщеплювача променя та двох фотодіодів [94]. В ідеалі результати вимірювання є випадковими з розподілом Гауса, пов’язаним лише з функцією Гауса Вігнера квантового стану вакууму [95]. Однак фактично виміряний гаусівський розподіл містить два додаткових незалежних джерела гаусового шуму; надлишок оптичного шуму та електронного шуму, таким чином сприяючи двом бічним каналам. Це необхідно враховувати при оцінці мінімальної ентропії джерела.

Рівень квантової випадковості, який можна витягти з гомодинного вимірювання флуктуацій вакууму, визначається залишковою хеш-лемою [96, 97]

$$\ell \leq N H_{\min}(X \mid E) - \log \frac{1}{\epsilon_{\text{hash}}^2} \tag{2.1}$$

Тут $H_{\min}(X \mid E)$ — мінімальна ентропія результату окремого вимірювання, отриманого з випадкової величини X, обумовленої квантовою побічною інформацією E, яку має супротивник, N — кількість агрегованих вибірок, ϵ_{hash} — відстань між ідеально рівномірний випадковий рядок і рядок, створений екстрактором випадковості. Тому зрозуміло, що нам потрібно знайти міні-ентропію нашої практичної – отже, недосконалої – реалізації, щоб обмежити кількість випадковості. Ми досягаємо цього за допомогою двоетапного підходу: спочатку ми теоретично виводимо межу мінімальної ентропії за допомогою реалістичної моделі безпеки та виражаємо її в термінах експериментально доступних параметрів. Далі ми експериментально виводимо ці параметри за допомогою метрологічної характеристики [92]. Використовуючи такий підхід, ми знаходимо мінімальну ентропію в найгіршому випадку, сумісну з довірчими інтервалами наших вимірювань характеристики та калібрування, таким чином отримуючи рядок випадкових бітів, які заслуговують на довіру з однаковим рівнем довіри.

Для виведення мінімальної ентропії ми припускаємо, що вихідний стан представлено гауссовою квантовою функцією Вігнера, симетричною у фазовому просторі, а квантовий процес є стаціонарним. Зокрема, наша модель безпеки включає квантову побічну інформацію та ефекти кінцевої пропускної здатності.

Спочатку ми розглянемо сценарій iid, де сигнали в різний час розподіляються однаково та незалежно (таким чином нехтуючи ефектами пропускної здатності). Ми враховуємо квантову побічну інформацію, розглядаючи джерело, що випромінює теплове світло із середнім числом фотонів n, і зловмисного супротивника, який проводить очищення цього теплового стану. Без втрати загальності очищений стан можна припустити як двомодовий стиснутий вакуумний стан, позначений як ρ_{XE}. Вихідний результат X ідеального гомодинного виявлення має розподіл щільності ймовірності $p_X(x) = G(x; 0, g^2(1 + 2n))$, тобто гауссове значення з нульовим середнім і дисперсією

$g^2(1 + 2\ n)$, де g – коефіцієнт посилення. Нижня межа мінімальної ентропії отримана як $H_{\min}(X \mid E) \geq -\log\|\gamma^{-1/2}\rho_{XE}\gamma^{-1/2}\|_\infty$ [98], де $\|\cdot\|_\infty$ — норма оператора, а γ є заданим станом Гаусса. Однак на практиці аналого-цифровий перетворювач (ADC) відображає неперервні змінні X у дискретні та обмежені змінні $\bar{X}$ з розміром біну Δx. Оптимізуючи динамічний діапазон ADC, ми знаходимо нижню межу мінімальної ентропії (подробиці наведено в Додатковому матеріалі):

$$H_{\min}(\bar{X} \mid E)_\rho \geq -\log\left(\frac{\Delta x}{g}\frac{\sqrt{2}(2n+1)}{\sqrt{\pi(4n+3)}}\right) \tag{2.2}$$

Виходячи за рамки iid, ми тепер розглянемо більш реалістичний сценарій, де виміряний сигнал має кінцеву смугу пропускання. Ми розрізняємо сигнал, тобто гомодинне вимірювання квантового стану, включаючи всі адитивні шумові процеси, і надлишковий шум, тобто всі джерела шуму, присутні у вимірюванні, окрім чистих флуктуацій вакууму, наприклад, електронний шум детектора та інтенсивність шуму гетеродина лазера. Давайте спочатку розглянемо ідеальне гомодинне виявлення флуктуацій вакууму, що дає сигнал X. За його спектром потужності $f_X(\lambda)$ можна оцінити коефіцієнт ентропії сигналу $h(X) = \frac{1}{2}\log(2\pi e\sigma_X^2)$, де $\sigma_X^2 = \frac{1}{2\pi e}2^{\int_0^{2\pi}\frac{d\lambda}{2\pi}\log[2\pi e f_X(\lambda)]}$ [99] є умовною дисперсією. Зауважте, що якщо сигнал не є iid, ${\sigma_X}^2$ є строго меншим за дисперсію сигналу, позначену σ^2. Аналогічно, зі спектру потужності надлишкового шуму $f_U(\lambda)$ отримуємо коефіцієнт ентропії шуму $h(U) = \frac{1}{2}\log(2\pi e\sigma_U^2)$.

Через кінцеву смугу пропускання вимірювального пристрою як сигнал X_t і надлишковий шум U_t в заданий момент часу t співвідносяться з їх значеннями в попередні моменти часу.

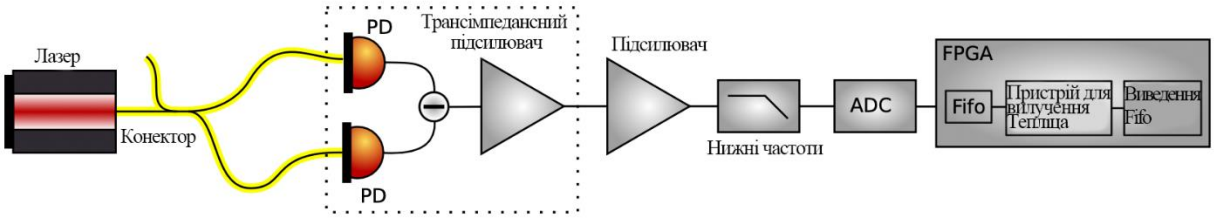

Рисунок 2.1 – Схема QRNG. Лазерний промінь 1,6 мВт 1550 нм був розділений на дві частини за допомогою 3 дБ волоконного конектора та виявлений саморобним гомодинним детектором на основі мікрохвильового підсилювача MAR-6 від Minicircuits і двох 120 мкм InGaAs фотодіодів (PD). Вихідний сигнал детектора був посилений за допомогою мікрохвильового підсилювача, відфільтрований низькими частотами на 400 МГц і оцифрований за допомогою 16-бітного аналого-цифрового перетворювача (ADC) 1 G виборка/с. ADC зчитувався Xilinx Kintex UltraScale FPGA. ADC і FPGA були розміщені на карті PCI Express від 4DSP (Abaco). FPGA використовувалася для вилучення випадковості в реальному часі на основі хешування Тепліца. Fifo: буфер першим прийшов першим вийшов.

Щоб відфільтрувати вплив цих кореляцій, ми розглядаємо розподіл щільності ймовірності X_t залежно від усіх минулих значень сигналу, $p_{X_t}(x_t \mid x_{<t}) = G(x_t; \mu_t, \sigma_X^2)$, де $x_{<t}$ позначає набір значень усіх сигналів у момент часу $t' < t$. Зверніть увагу, що середнє значення μ_t залежить від $x_{<t,}$ тоді як умовна дисперсія σ_X^2 не залежить. Цей опис узгоджується з припущенням про стаціонарний гаусівський процес [99]. Умовна змінна в момент часу *t* практично не залежить від попередніх значень сигналу, тому ми можемо застосувати ті ж міркування, що й для випадку iid вище, і ідентифікувати $\sigma_X^2 \equiv g^2(1 + 2n)$, що, у свою чергу, передбачає$\sigma^2 = g^2(1 + 2n) + \zeta$, де $\zeta = \sigma^2 - \sigma_X^2$ – це дисперсія додаткового класичного шуму, який зміщує середнє значення на μ_t.

Для надлишкового шуму U_t ми подібним чином отримуємо розподіл щільності ймовірності, обумовлений минулими значеннями, тобто $p_{U_t}(u_t \mid u_{<t}) = G(u_t; \nu_t, \sigma_U^2)$. Величиною, яка цікавить, є умовна дисперсія надлишкового шуму σ_U^2, яка представляє дисперсію надлишкового шуму, яка практично не залежить від попередніх значень шуму. Тому ототожнюємо $\sigma_U^2 \equiv 2g^2 n$. аким чином, використовуючи умовні розподіли, ми відобразили налаштування без iid у описану вище модель iid з ідентифікацією $g^2 \equiv \sigma_X^2 - \sigma_U^2$ та $n \equiv \frac{1}{2}\frac{\sigma_U^2}{\sigma_X^2 - \sigma_U^2}$. Нарешті, щоб отримати нижню оцінку, ми розглядаємо класичний шум ζ як квантовий шум. Це робиться шляхом заміни $n \to n + \frac{\zeta}{2g^2} = \frac{1}{2}\left(\frac{\sigma^2}{\sigma_X^2 - \sigma_U^2} - 1\right)$. Потім нижню межу можна знайти, вставивши g і n у рівняння (2.2), яке зображено на рис. 2.2 для різного надлишкового шуму, роздільної здатності ADC і часових кореляцій.

Використовуючи наведені вище результати, ми тепер можемо оцінити мінімальну ентропію за допомогою метрологічної характеристики нашої установки. Відповідно до аналізу безпеки мінімальна ентропія може бути знайдена шляхом визначення дисперсії σ^2, а також умовних дисперсій гомодинного сигналу σ_X^2 і надлишкового шуму σ_U^2. Щоб отримати консервативну, а отже, надійну оцінку мінентропії, важливо, щоб визначення цих параметрів не покладалося на будь-які припущення щодо ідеальності гомодинного детектора.

У попередніх дослідженнях гомодинного QRNG було підтверджено наявність єдиного дробового шуму шляхом визначення його масштабування за допомогою оптичної потужності. Однак недосконале відхилення синфазного сигналу, шум високої інтенсивності лазера або проникнення розсіяного світла в сигнальний порт – імовірно, це проблема з інтегрованими фотонними чіпами – може без потреби обмежувати вилучення випадкових чисел. Крім того, цей метод визначення характеристик безпосередньо не сумісний із визначенням метрологічного рівня, оскільки важко пов’язати похибку оцінки рівня дробового

шуму з довірчим інтервалом. Щоб уникнути цих припущень і проблем, ми проводимо незалежну, надійну та метрологічну характеристику вимірювального пристрою.

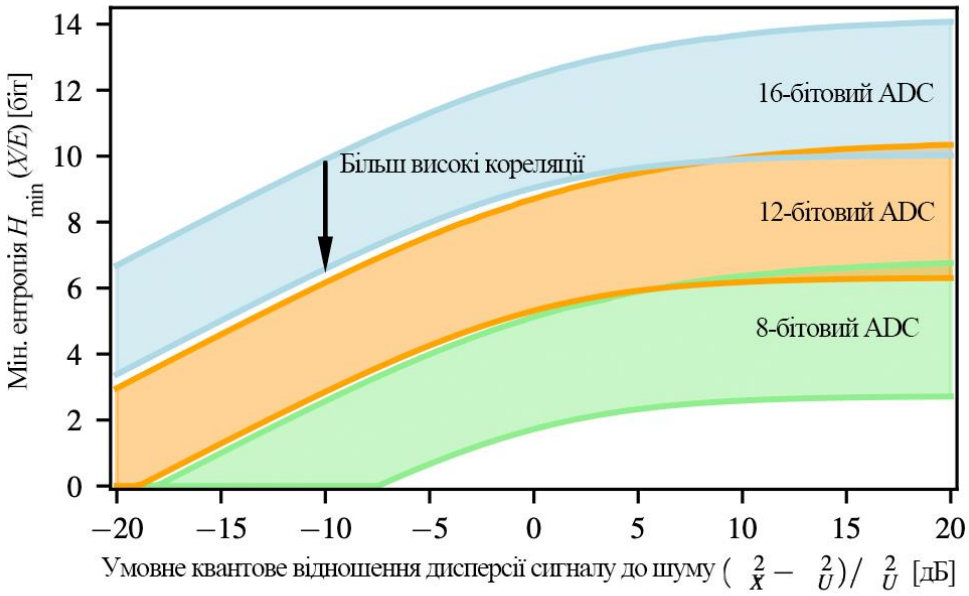

Рисунок 2.2 – Мінімальна ентропія для роздільної здатності 8-, 12- і 16-бітових ADC в залежності від співвідношення умовної дисперсії флуктуацій вакууму та умовної дисперсії надлишкового шуму, $(\sigma_X^2 - \sigma_U^2)/\sigma_U^2$. Заштриховані області вказують на області між низькими кореляціями $(\sigma_X^2/\sigma^2 = 0{,}99)$, верхній слід, і високими кореляціями $(\sigma_X^2/\sigma^2 = 0{,}1)$, нижній слід. Дисперсію сигналу було оптимізовано для отримання найвищої мінімальної ентропії.

В основному ми розглядаємо гомодинний детектор як коробку з входом і виходом з мінімальними припущеннями щодо його внутрішньої роботи (див. рис. 2.3а). Таким чином, наша стратегія полягає в тому, щоб виміряти функцію передачі коробки та використовувати цей результат для консервативного калібрування спектральної щільності потужності (PSD) флуктуацій вакууму. Цей консер потім оцінений результат порівнюється з PSD фактичного вимірювання шуму, з якого ми виводимо умовні дисперсії шуму сигналу та надлишкового шуму, і, нарешті, мінімальну ентропію.

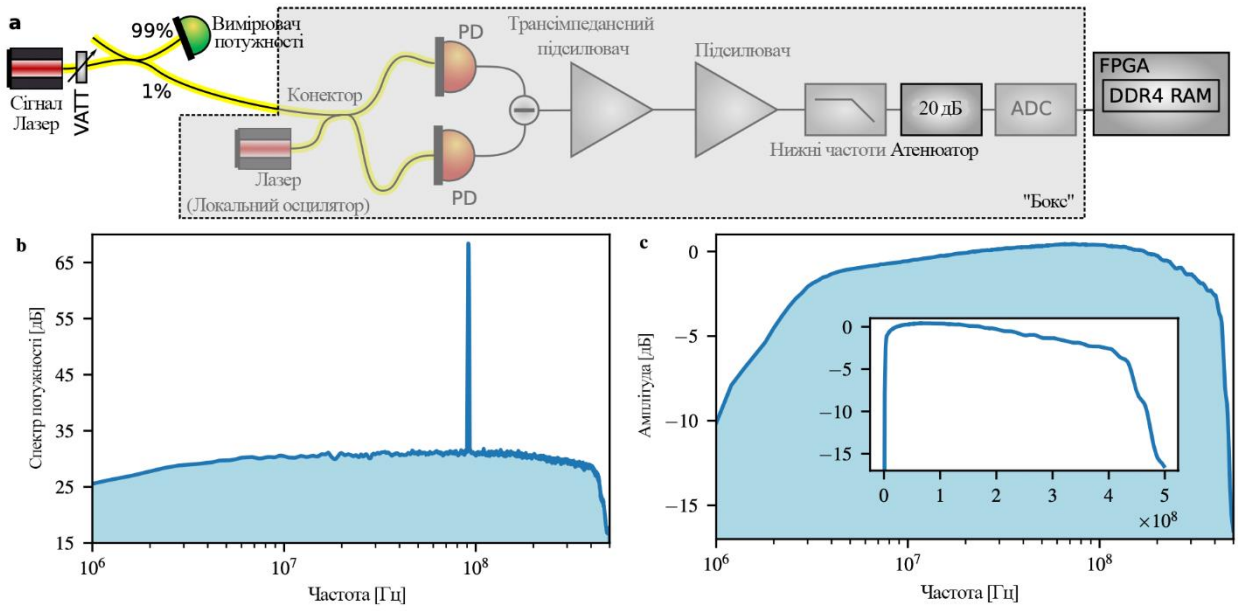

Рисунок 2.3 – Характеристика передатної функції системи детектування для отримання рівня шуму флуктуацій вакууму. a) Експериментальна установка для визначення характеристик. b) Спектр потужності типового вимірювання. Передатна функція визначається амплітудою вузла биття. c) Передатна функція гомодинного детектора та електроніки, включаючи аналого-цифровий перетворювач. Вставка: функція передачі з лінійною шкалою частот.

Передавальна функція коробки вимірюється шляхом введення когерентного стану у формі другого лазерного променя (незалежного від лазера локального осцилятора) з малою потужністю P_{sig} у сигнальний порт дільника променя, як показано на рис. 2.3a. Типовий сигнал биття показаний на рис. 2.3b, отриманий шляхом обчислення усередненої періодограми з дискретизованого сигналу. Ми реєструємо передаточну функцію $\text{TF}(\nu)$ шляхом сканування частоти сигнального лазера. На кожній різницевій частоті ν визначаємо потужність сигналу биття і нормалізуємо її на P_{sig}. При високому відношенні сигнал/шум середньоквадратична потужність сигналу биття є чисто функцією амплітуди когерентного стану (тобто потужності лазерного сигналу) і не залежить від шумових властивостей двох лазерів і детектора.

Передатна функція включає ефективність перешкод, оптичні втрати та квантову ефективність фотодіодів, а також залежне від частоти посилення всіх підсилювачів, фільтра низьких частот і аналогову смугу пропускання ADC. Оскільки вакуумний шум був посилений для оптимального заповнення діапазону ADC, ми використали електричний аттенюатор на 20 дБ з рівним загасанням у смузі частот, що цікавить, щоб уникнути насичення, див. рис. 3a. Результат характеристики передатної функції, нормалізований до максимального посилення 1, показано на рис. 2.3b. Припускаючи лінійність детектора, ми отримуємо PSD флуктуацій вакууму шляхом множення функції передачі TF(v) на енергію дробового шуму $\hbar\omega_L$, що міститься в смузі пропускання 1 Гц, де $\hbar$ — постійна Планка, а ω_L — кутова частота локального осциляторного лазеру. Моделюючи внутрішню роботу сірого ящика, ми підтверджуємо в додатковому матеріалі, що використовуючи цю процедуру, ми справді отримуємо нижню межу PSD коливань вакууму.

Консервативно оцінений PSD флуктуацій вакууму показаний на рис. 2.4a разом із фактично виміряним PSD сигналу. Спектри чітко «забарвлені», що вказує на те, що вибірки даних є корельованими і, отже, не iid. Це додатково підтверджено на рис. 2.4b, де зображено автокореляцію сигналу. Це обґрунтовує важливість використання співвідношення мінентропії, пов’язаного з вибірками, які не є iid.

З PSD ми обчислюємо три параметри для отримання мінімальної ентропії, які підсумовані в таблиці 2.1. Мінімізація мінімальної ентропії за довірчим набором оцінених параметрів дала 10,7 біт на 16-бітну вибірку для ймовірності помилки нашої характеристики параметра (тобто $\epsilon_{\mathrm{PE}} = 10^{-10}$ ймовірність того, що фактичні параметри знаходяться за межами довірчих інтервалів). Щоб перевірити припущення Гауса в нашому доказі безпеки, ми розрахували квантилі ймовірності виміряних зразків і порівняли їх із теоретичними квантилями розподілу Гауса, див. рис. 2.4c.

Після обчислення мінімальної ентропії наступним кроком є вилучення випадкових чисел. Це робиться за допомогою сильного екстрактора на основі алгоритму хешування матриці Тепліца, у якому вихідне число можна повторно використовувати [15, 18, 25].

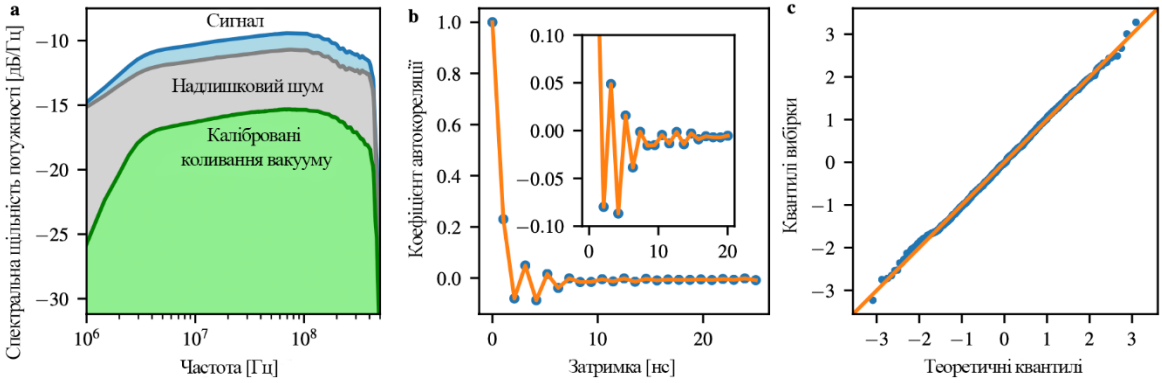

Рисунок 2.4 – Результати експерименту. a) На рисунку показано спектральну щільність потужності сигналу, калібровані флуктуації вакууму (отримані шляхом визначення характеристик) і надлишковий шум (отриманий шляхом віднімання PSD флуктуацій вакууму з PSD сигналу. b) Коефіцієнти автокореляції, розраховані за виміряні зразки та усереднені 1000 разів. На вставці показано збільшення. c) Графік Q-Q, що вказує гаусівство виміряних зразків. Дисперсію зразків було нормалізовано до 1. Обмежений діапазон ADC скорочує хвости розподілу Гауса, що призводить до невеликих відхилень від теоретичних квантилів до кінців.

Ми вибрали розміри матриці n = 1280 біт і m = 640 біт, що відповідає 80 вхідним зразкам із глибиною 16 біт і вихідною довжиною $m < \ell$ вибрано clS cL, кратне 128 біт, таке, що рівняння. 1 було виконано з $H_{\min} = 10{,}7$ біт та $\epsilon_{\text{hash}} < 10^{-33}$. Записані зразки від ADC були передані у буфер першим прийшов – першим вийшов (FIFO) в FPGA з використанням 64-розрядної шини з тактовою частотою 250 МГц. Потім було реалізовано виділення випадковості з тактовою частотою 125 МГц і одночасно оброблено 128-бітні слова: ми розбили повну матрицю Тепліца по стовпцях на підматриці розміром (стовпця) 128. На кожному

етапі конвеєра 128-бітний вхідний вектор помножили на n рядків-векторів підматриці паралельно.

Таблиця 2.1 – Підсумок параметрів, визначених метрологічною характеристикою, з їх довірчими інтервалами для $\epsilon_{\mathrm{PE}} = 10^{-10}$: дисперсії сигналу σ^2, дисперсії умовного сигналу σ_X^2 та дисперсії умовного надлишкового шуму σ_U^2. Розрахована мінімальна мінімальна ентропія за довірчими інтервалами, безпечна довжина відповідно до залишкової геш-леми та довжина витягнутої випадкової послідовності в експерименті.

Параметр	Середнє	Довірчий інтервал
σ^2	$3{,}96 \times 10^7$	$0{,}09 \times 10^7$
σ_X^2	$3{,}29 \times 10^7$	$0{,}07 \times 10^7$
σ_U^2	$2{,}49 \times 10^7$	$0{,}06 \times 10^7$
Умовне відношення кванта до надлишкового шуму	-4,9 дБ	
Мінімальна ентропія	10,7 біт	
Розраховано безпечна довжина	640,7 біт	
Вилучена довжина	640 біт	

Начальний елемент із $n + m - 1$ біт зберігався у швидких логічних тригерах FPGA, а підматриці генерувалися на ходу через обмежені логічні ресурси. Множення було виконано за допомогою порозрядного I та наступного XOR усіх 128 біт, які були реалізовані в 3-ступінчастому конвеєрі для виконання часових обмежень. Отримані m бітів зберігаються в регістрі накопичувача. Досягнута пропускна здатність склала 8 Гбіт/с.

На завершення ми продемонстрували QRNG на основі вимірювання флуктуацій вакууму з вилученням у реальному часі зі швидкістю 8 Гбіт/с. Наш QRNG має сильну гарантію безпеки з ймовірністю відмови $N' \cdot \epsilon_{\mathrm{hash}} + \epsilon_{\mathrm{PE}} + \epsilon_{\mathrm{seed}} = N' \cdot 10^{-33} + 10^{-10} + \epsilon_{\mathrm{seed}}$, де N' — це кількість циклів QRNG у минулому, ϵ_{hash} — це параметр безпеки, пов'язаний із видаленням додаткової інформації (див. рівняння 2.1), $\epsilon_{\mathrm{PE}} = 10^{-10}$ – параметр безпеки оцінки параметра

метрологічної оцінки, ϵ_{seed} описує безпеку використовуваних випадкових бітів. для заповнення екстрактора випадковості. Оскільки супротивник може мати доступ до всієї квантової побічної інформації з минулого, ϵ_{hash} зростає з часом [76]. Ми вибрали значення 10^{-33}, щоб мати можливість генерувати випадкові числа Гауса з безпекою $\epsilon = 2 \times 10^{-10}$ для QKD-прогону з 10^{10} зразками, які вимагають повторного заповнення QRNG лише раз на 10 років. У нашому експерименті початкові біти вибиралися за допомогою генератора псевдовипадкових чисел, що не дозволяло нам дати гарантію безпеки для ϵ_{seed}. Згенеровані випадкові числа пройшли статистичні тести на випадковість Dieharder [101] і NIST [102].

Швидкість нашого QRNG у реальному часі була обмежена 8 Гбіт /с через невеликий розмір вхідних даних екстрактора Тепліца, який вимагає наша реалізація FPGA. З у 5 разів більшим розміром вхідних даних пропускна здатність понад 10 Гбіт /с була б можливою з тим самим параметром безпеки. Тим не менш, наш QRNG ідеально підходить для використання у високошвидкісних QKD-з'єднаннях, наприклад, у дискретній змінній із тактовою частотою ГГц [103], а також у високошвидкісній безперервній змінній QKD [104]. Для модульованого за Гаусом CVQKD рівномірний розподіл випадкових чисел потрібно перетворити на розподіл Гаусса, що вимагає більшої швидкості генерації випадкових чисел. Крім того, QKD вимагає кількісної безпеки та гарантії конфіденційності випадкових чисел, як це надає наша система. Подальші розробки, щоб гарантувати надійну роботу протягом тривалого часу та відповідати вимогам органів сертифікації, повинні включати самотестування під час увімкнення живлення та онлайн-тестування параметрів підтвердження безпеки, а також згенерованих випадкових чисел.

2.1 Попередні додаткові матеріали

Ми описуємо n-модові стани електромагнітного поля в представленні функції Вігнера. Ми маємо справу з гауссовими станами, у яких функція Вігнера повністю характеризується першим і другим моментами поля квадратури. Користувач нашого квантового генератора випадкових чисел вимірює за допомогою гомодинного виявлення бозонну моду, пов'язану з квадратурними операторами q і p. Без втрати загальності ми припускаємо, що супротивник (також званий підслуховувачем) тримає очисну систему E, визначену однією бозонною модою з квадратурними операторами q_e, p_e. Ми припускаємо, що виміряна мода знаходиться в тепловому стані з n середнім числом фотонів. Це означає, що середні значення квадратур дорівнюють нулю, а коваріаційна матриця (CM) є

$$V_{\text{thermal}} = \begin{pmatrix} \langle \hat{q}^2 \rangle & \frac{1}{2}\langle \hat{q}\hat{p} + \hat{p}\hat{q} \rangle \\ \frac{1}{2}\langle \hat{p}\hat{q} + \hat{q}\hat{p} \rangle & \langle \hat{p}^2 \rangle \end{pmatrix} \tag{2.3}$$

$$= \begin{pmatrix} 1+2n & 0 \\ 0 & 1+2n \end{pmatrix}, \tag{2.4}$$

де ми прийняли угоду про те, що дисперсія вакууму дорівнює 1.

Добре відомо, що очищення термічного стану – це двомодовий стиснутий вакуум (TMSV), стан Гауса з нульовим середнім і CM [20]

$$V_{\text{TMSV}} = \begin{pmatrix} \langle \hat{q}^2 \rangle & \frac{1}{2}\langle \hat{q}\hat{p} + \hat{p}\hat{q} \rangle & \langle \hat{q}\hat{q}_e \rangle & \langle \hat{q}\hat{p}_e \rangle \\ \frac{1}{2}\langle \hat{p}\hat{q} + \hat{q}\hat{p} \rangle & \langle \hat{p}^2 \rangle & \langle \hat{p}\hat{q}_e \rangle & \langle \hat{p}\hat{p}_e \rangle \\ \langle \hat{q}_e\hat{q} \rangle & \langle \hat{q}_e\hat{p} \rangle & \langle \hat{q}_e^2 \rangle & \frac{1}{2}\langle \hat{q}_e\hat{p}_e + \hat{p}_e\hat{q}_e \rangle \\ \langle \hat{p}_e\hat{q} \rangle & \langle \hat{p}_e\hat{p} \rangle & \frac{1}{2}\langle \hat{p}_e\hat{q}_e + \hat{q}_e\hat{p}_e \rangle & \langle \hat{p}_e^2 \rangle \end{pmatrix} \tag{2.5}$$

$$= \begin{pmatrix} 1+2n & 0 & 2\sqrt{n(n+1)} & 0 \\ 0 & 1+2n & 0 & -2\sqrt{n(n+1)} \\ 2\sqrt{n(n+1)} & 0 & 1+2n & 0 \\ 0 & -2\sqrt{n(n+1)} & 0 & 1+2n \end{pmatrix} \quad (2.6)$$

Якщо користувач вимірює квадратуру $\hat{q}$ за допомогою гомодинного виявлення, вихід вимірювання є безперервною дійсною змінною *X із* розподілом щільності ймовірності

$$p_X(x) = G(x; 0, g^2(1+2n)), \quad (2.7)$$

де g є фактором посилення і

$$G(x; \mu, v^2) = \frac{1}{\sqrt{2\pi}v} e^{-\frac{(x-\mu)^2}{2v^2}} \quad (2.8)$$

позначає Гаусс із середнім μ і дисперсією v^2.

Кореляції між результатом *X* ідеального гомодинного виявлення та квантовою побічною інформацією, що зберігається підслухувачем, описуються класично-квантовим (CQ) станом

$$\rho_{XE} = \int dx p_X(x) |x\rangle\langle x| \otimes \rho_E^x \quad (2.9)$$

де інтеграл по дійсній прямій, а p E є станом Гауса з першим моментом

$$\begin{pmatrix} \langle \hat{q}_e \rangle \\ \langle \hat{p}_e \rangle \end{pmatrix} = \begin{pmatrix} \frac{2\sqrt{n(n+1)}}{g(1+2n)} x \\ 0 \end{pmatrix} \quad (2.10)$$

і коваріаційна матриця

$$\begin{pmatrix} \frac{1}{1+2n} & 0 \\ 0 & 1+2n \end{pmatrix} \quad (2.11)$$

У нашому QRNG безперервна змінна X відображається в дискретній і обмеженій змінній *X* шляхом застосування аналого-цифрового перетворювача (ADC). Тому ми розглядаємо модель, у якій X замінено дискретною змінною $\bar{X}$ такий як

$$p_{\bar{X}}(k) = \int_{I_k} dx p_X(x) \quad (2.12)$$

де I_k є d інтервалами, які дискретизують результат гомодинного виявлення. У типових умовах ці d неперекривні інтервали I_k мають форму

$$I_1 =]-\infty, -R] \tag{2.13}$$

$$I_d =]R, \infty[\tag{2.14}$$

а при k = 2,..., d — 1

$$I_k =]a_k - \Delta x/2, a_k + \Delta x/2] \tag{2.15}$$

з $a_k = -R + (k-1)\Delta x/2$ та $\Delta x = 2R/(d-2)$. Цей вибір інтервалів відображає спосіб, у який ADC з діапазоном R і розміром біну Δx працює при відображенні безперервної змінної в дискретну.

У термінах дискретної змінної $\bar{X}$, кореляції з повністю квантовим перехоплювачем описуються станом

$$\rho_{\bar{X}E} = \sum_k p_{\bar{X}}(k)|k\rangle\langle k| \otimes \rho_E^{(k)} \tag{2.16}$$

з

$$\rho_E^{(k)} = \frac{1}{p_{\bar{X}}(k)} \int_{I_k} dx p_X(x) \rho_E^x \tag{2.17}$$

2.2 Нижні межі мінімальної ентропії з квантовою побічною інформацією

Враховуючи стан $\rho_{\bar{X}E}$ у рівнянні (2.16), мінімальна ентропія XX обумовлювала Е зчитувані дані [98-105]

$$H_{\min}(\bar{X} \mid E)_\rho = \sup_\gamma \left[-\log \left\| \gamma_E^{-\frac{1}{2}} \rho_{\bar{X}E} \gamma_E^{-\frac{1}{2}} \right\|_\infty \right] \tag{2.18}$$

Першу нижню межу мінімальної ентропії можна отримати шляхом обчислення $\left\| \gamma_E^{-1/2} \rho_{\bar{X}E} \gamma_E^{-1/2} \right\|_\infty$ для заданого вибору стану γ:

$$H_{\min}(\bar{X} \mid E)_\rho \geq -\log \left\| \gamma_E^{-1/2} \rho_{\bar{X}E} \gamma_E^{-1/2} \right\|_\infty \tag{2.19}$$

$$= -\log\left[\sup_k p_{\bar{X}}(k)\left\|\gamma_E^{-1/2}\rho_E^{(k)}\gamma_E^{-1/2}\right\|_\infty\right] \tag{2.20}$$

де остання рівність виконується, оскільки $\rho_{\bar{X}E}$ є станом CQ. Тут ми дорівнюємо γ однорежимному гауссовому стану з нульовим середнім і CM

$$\begin{pmatrix} 1+2(n+\delta) & 0 \\ 0 & 1+2(n+\delta) \end{pmatrix} \tag{2.21}$$

де параметр δ буде оптимізовано *апостериорно* для отримання жорсткої межі. Друга нижня межа отримана шляхом застосування трикутної нерівності,

$$p_{\bar{X}}(k)\left\|\gamma_E^{-1/2}\rho_E^{(k)}\gamma_E^{-1/2}\right\|_\infty = \left\|\gamma_E^{-1/2}\left(\int_{I_k} dx p_X(x)\rho_E^x\right)\gamma_E^{-1/2}\right\|_\infty \tag{2.22}$$

$$\leq \int_{I_k} dx p_X(x)\left\|\gamma_E^{-\frac{1}{2}}\rho_E^x\gamma_E^{-\frac{1}{2}}\right\|_\infty \tag{2.23}$$

що має на увазі

$$H_{\min}(\bar{X}\mid E) \geq -\log\left[\sup_k \int_{I_k} dx p_X(x)\left\|\gamma_E^{-1/2}\rho_E^x\gamma_E^{-1/2}\right\|_\infty\right] \tag{2.24}$$

Зверніть увагу, що ρ_E^x та γ_E обидва є станами Гаусса, і тому наведену нижню межу можна обчислити за допомогою методів представлення Гіббса, розроблених у [106] і методів [81] для відносної ентропії між двома довільними станами Гауса. Ці попередні методи можуть бути використані для виведення формули для відносної ентропії Реньї (див. теорему 5 у посиланні [107]). Застосовуючи цю формулу, отримуємо

$$\left\|\gamma_E^{-1/2}\rho_E^x\gamma_E^{-1/2}\right\|_\infty = (n+\delta)(1+n+\delta)\sqrt{\frac{1+2n}{\delta(2n(n+1+\delta)+\delta)}}\exp\left[\frac{x^2}{2g^2(1+2n)}\frac{4n(n+1)}{4n(n+1+\delta)+2\delta}\right] \tag{2.25}$$

Цей останній вираз дозволяє нам писати

$$\int_{I_k} dx p_X(x)\left\|\gamma_E^{-1/2}\rho_E^x\gamma_E^{-1/2}\right\|_\infty = \frac{1}{g}\frac{(n+\delta)(1+n+\delta)}{\sqrt{2\pi\delta(2n(n+1+\delta)+\delta)}}\int_{I_k} dx\exp\left[\frac{-x^2}{2g^2}\frac{\delta}{2n(n+1+\delta)+\delta}\right] \tag{2.26}$$

Супремум над k можна обчислити для будь-якого заданого набору інтервалів I_k. Для інтервалів, як у рівняннях (2.13)-(2.15) отримуємо

$$\sup_k \int_{I_k} dx p_X(x) \left\| \gamma_E^{-1/2} \rho_E^x \gamma_E^{-1/2} \right\|_\infty \leq \frac{(n+\delta)(1+n+\delta)}{\delta} \max\left\{ \operatorname{erf}\left(\sqrt{\frac{\delta}{4n(n+1+\delta)+2\delta}} \frac{\Delta x}{2g} \right), \frac{1}{2} \operatorname{erfc}\left(\sqrt{\frac{\delta}{4n(n+1+\delta)+2\delta}} \frac{R}{g} \right) \right\} \tag{2.27}$$

що для оптимального вибору R дає нашу третю нижню межу

$$H_{\min}(\bar{X} \mid E)_\rho \geq -\log\left[\frac{(n+\delta)(1+n+\delta)}{\delta} \operatorname{erf}\left(\sqrt{\frac{\delta}{4n(n+1+\delta)+2\delta}} \frac{\Delta x}{2g} \right) \right] \tag{2.28}$$

Ми зауважимо, що це фактично сімейство нижніх меж, параметризованих δ, тоді слід знайти оптимальне значення δ, для якого межа є більш жорсткою.

При найнижчому порядку в Δx нижня межа в рівнянні (2.28) спрощується до

$$H_{\min}(\bar{X} \mid E)_\rho \geq -\log\left(\frac{\Delta x}{g} \right) - \log\left(\frac{(n+\delta)(1+n+\delta)}{\sqrt{2\pi\delta[2n(n+1+\delta)+\delta]}} \right) \tag{2.29}$$

і поклавши, наприклад, $\delta = n$, отримаємо

$$H_{\min}(\bar{X} \mid E)_\rho \geq -\log\left(\frac{\Delta x}{g} \right) - \log\left(\frac{\sqrt{2}(2n+1)}{\sqrt{\pi(4n+3)}} \right) \tag{2.30}$$

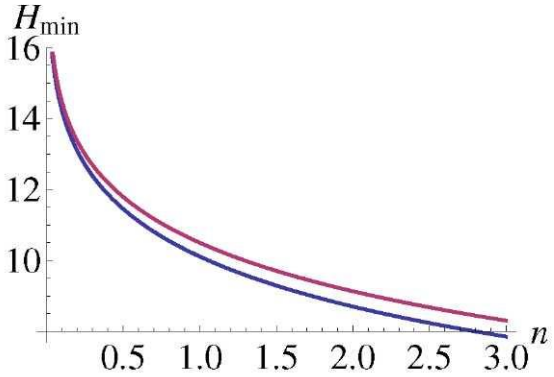

Рисунок 2.5 – Гомодинна верхня межа $H_{\min}(\bar{X} \mid C)$ як у рівнянні (2.33) [червона лінія] і нижня межа в рівнянні (2.28) (синя лінія) від середнього числа фотонів n, для $\delta = n$ та Δx =≈ n/1000.

2.3 Порівняння з класичною додатковою інформацією

Ми можемо порівняти нижні межі, обчислені в попередніх розділах, із верхньою межею, отриманою за припущення, що підслуховувач виконує ідеальне гомодинне виявлення.

Якщо користувач і підслуховувач застосовують гомодинне виявлення, вони генерують пару корельованих гаусових змінних X і Y так, що

$$p_Y(y) = G(y; 0{,}1 + 2n) \tag{2.31}$$

$$p_X(x \mid y) = G\left(x; \frac{2g\sqrt{n(n+1)}}{1+2n} y, \frac{g^2}{1+2n}\right) \tag{2.32}$$

Потім змінна X відображається в дискретну та обмежену змінну $\bar{X}$, як описано в розділі. Використовуючи оптимальний вибір діапазону R ADC, мінімальна ентропія $\bar{X}$ обумовлювлена на Y є

$$H_{\min}(\bar{X} \mid C) = -\log \operatorname{erf}\left(\frac{\Delta x}{g}\frac{\sqrt{2+4n}}{4}\right) \tag{2.33}$$

або до виправлення порядку вище ніж Δx,

$$H_{\min}(\hat{X} \mid C) \simeq -\log\left(\frac{\Delta x}{g}\right) - \log\left(\sqrt{\frac{1+2n}{2\pi}}\right) \tag{2.34}$$

На рис. 2.5 показано гомодинну верхню межу в рівнянні (2.33) разом із нижньою межою у рівнянні (2.28) як функція n, для $\delta = n$ та $\Delta x = n/1000$. На рис. 2.6 показано різницю між приблизною гомодинною верхньою межею в рівнянні (2.34) і приблизну нижню межу в рівнянні (2.29), знову для δ =n (зверніть увагу, що різниця не залежить від Δx). Графік показує, що різниця така мала, як частка біта.

2.4 Оцінка дисперсій і коефіцієнта ентропії

У цьому додатку ми обговорюємо оцінку дисперсії, швидкості ентропії та умовної дисперсії шуму та сигналу. Щоб зробити речі більш конкретними, ми зосереджуємось на оцінці дисперсії сигналу variance σ^2, рівня ентропії $h(X)$ та дисперсії умовного сигналу σ_X^2. Припустимо, що T є часом виконання експерименту, і n вимірювань сигналу виконуються через регулярні інтервали часу $\delta t = T/n$. Спектральна щільність, обчислена на основі цих даних, є

функцією n дискретних частот, позначених як ω_j 's, які приймають значення від $2\pi/T$ до $2\pi n/T$. Нижче ми працюємо з дискретною змінною λ_j, визначеною як $\lambda_j \equiv T\omega_j/n$, яка може бути апроксимована безперервною змінною λ, що приймає значення з областю визначення $[0,2\pi]$.

Ми оцінюємо спектральну густину $f(\lambda)$, застосовуючи метод Велча, згідно з яким дані спочатку розбиваються на M блоків (можливо, що перекриваються), а потім у кожному блоці обчислюється періодограма, тобто дискретне перетворення даних Фур'є, що містяться в цьому самому блоці. Потім оцінюється спектральна щільність, беручи середнє значення за періодограмами.

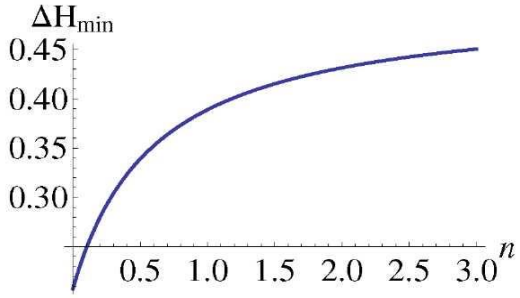

Рис. 6. Різниця між наближеною гомодинною верхньою межею в рівнянні (2.34) і приблизною нижньою межею в рівнянні (2.29) проти середнього числа фотонів n, для для δ =n.

Ми припускаємо, що періодограми, як випадкові величини, є незалежними та однаково розподіленими, і що кожна періодограма розподілена як квадрат гауссової змінної. Тоді оцінка Велча спектральної щільності розподіляється як (перемасштабована) $\chi^2(k)$ змінна з M ступенями свободи. Позначивши як $f_0(\lambda_j)$ оцінку Велча для спектральної щільності та як $f(\lambda_j)$ її реальне значення, тоді ми можемо отримати довірчий інтервал, застосовуючи хвостову межу змінної $\chi^2(k)$. Наприклад, ми можемо використати межі хвоста (див. наприклад [108])

$$\Pr\left\{f(\lambda_j) < \frac{f_0(\lambda_j)}{1+t}\right\} \le e^{-\frac{Mt^2}{8}},$$
$$\Pr\left\{f(\lambda_j) > \frac{f_0(\lambda_j)}{1-t}\right\} \le e^{-\frac{Mt^2}{8}} \qquad (2.35, 2.36)$$

Для $t \ll 1$ це дає, аж до членів вищого порядку,

$$\Pr\{f(\lambda_j) \notin [(1-t)f_0(\lambda_j), (1+t)f_0(\lambda_j)]\} = P(t) \quad (2.37)$$

з

$$P(t) \leq 2e^{-Mt^2/8}. \quad (2.38)$$

Давайте спочатку обговоримо оцінку рівня ентропії

$$h(X) = \frac{1}{2}\int_0^{2\pi} \frac{d\lambda}{2\pi} \log[2\pi e f(\lambda)] \quad (2.39)$$

як наближено кінцевою сумою

$$h(X) \simeq \frac{1}{2}\sum_{j=1}^{n} \frac{1}{n} \log[2\pi e f(\lambda_j)] \quad (2.40)$$

Для кожного заданого $j, 1 - P(t)$ — це ймовірність того, що $f(\lambda_j) \in [(1-t)f_0(\lambda_j), (1+t)f_0(\lambda_j)]$, тоді випливає (з застосування пов'язаного сполучення), що

$$\Pr\{\exists j \mid f(\lambda_j) \notin [(1-t)f_0(\lambda_j), (1+t)f_0(\lambda_j)]\} \leq nP(t) \quad (2.41)$$

Це еквівалентно тому, що з імовірністю, більшою за $1 - nP(t), f(\lambda_j)$ лежить між $(1-t)f_0(\lambda_j)$ та $(1+t)f_0(\lambda_j)$ для всіх j = 1,..., n. Тому

$$h(X) \in \left[\frac{1}{2}\sum_{j=1}^{n} \frac{1}{n} \log[2\pi e f_0(\lambda_j)] + \frac{1}{2}\log(1-t), \frac{1}{2}\sum_{j=1}^{n} \frac{1}{n} \log[2\pi e f_0(\lambda_j)] + \frac{1}{2}\log(1+t)\right] \quad (2.42)$$

з імовірністю не менше $1 - nP(t) = 1 - 2ne^{-Mt^2/8}$. Подальша лінійна апроксимація для $t \ll 1$ дає довірчий інтервал

$$h(X) \in \left[\frac{1}{2}\sum_{j=1}^{n} \frac{1}{n} \log[2\pi e f_0(\lambda_j)] - \frac{\log e}{2} t, \frac{1}{2}\sum_{j=1}^{n} \frac{1}{n} \log[2\pi e f_0(\lambda_j)] + \frac{\log e}{2} t\right] \quad (2.43)$$

Нарешті, щоб врахувати перекриття між сусідніми періодограмами, ми замінюємо $M \to \gamma M$, для $\gamma < 1$. Наприклад, якщо періодограма має 50% перекриття, ми ставимо $\gamma = 1/2$. На закінчення, з перекриттям 50%, ми отримуємо, що для будь-якого заданого $\epsilon > 0$, швидкість ентропії лежить в інтервалі

$$h(X) \simeq \frac{1}{2}\sum_{j=1}^{n} \frac{1}{n} \log[2\pi e f_0(\lambda_j)] \pm 2\log e \sqrt{\frac{1}{M}\ln\left(\frac{2n}{\epsilon}\right)} \quad (2.44)$$

з ймовірністю не більшою за ϵ.

З рівня ентропії ми отримуємо довірчий інтервал для умовної дисперсії, $\sigma_X \in [\sigma_X^-, \sigma_X^+]$, де

$$\sigma_X^{\pm} = \frac{1}{2\pi e} 2^{\sum_{j=1}^{n} \frac{1}{n} \log[2\pi e f_0(\lambda_j)]} 2^{\pm 4 \log e \sqrt{\frac{1}{M} \ln \frac{2n}{\epsilon}}}. \quad (2.45)$$

Аналогічно отримуємо оцінку дисперсії сигналу σ^2 використовуючи відношення

$$\sigma^2 = \int_0^{2\pi} \frac{d\lambda}{2\pi} f(\lambda) \quad (2.46)$$

з якого ми отримуємо довірчий інтервал

$$\sigma^2 \simeq \left(1 \pm 4\sqrt{\frac{1}{M} \ln \frac{2n}{\epsilon}}\right) \sum_{j=1}^{n} \frac{1}{n} f_0(\lambda_j) \quad (2.47)$$

Таким же чином ми отримуємо довірчий інтервал для дисперсії умовного шуму, $\sigma_U \in [\sigma_U^-, \sigma_U^+]$ (це має додатково включати систематичні помилки). Щоб отримати найгіршу оцінку мінімальної ентропії, ми розглядаємо менше значення для дисперсії сигналу, σ_X^-, а більший для шуму, σ_U^+.

2.5 Характеристика спектральної густини потужності флуктуацій вакууму

Тут ми відкриваємо чорну скриньку гомодинного детектора та показуємо, включивши недоліки, що межа, наведена в основному тексті, справді є нижньою межею флуктуацій вакууму. Як описано в основному тексті, ми б'ємо двома лазерами гетеродина з потужністю P_{LO} і допоміжний сигнальний лазер з потужністю P_{sig}, яка є частотою, розстроєною відносно локального осцилятора на ν. Промені інтерферують на дільнику променя з коефіцієнтом розщеплення $R(\nu)$: $1 - R(\nu)$, де частотна залежність v враховує залежне від частоти відхилення загального режиму гомодинної електроніки. Крім того, ми беремо до уваги видимість інтерференції $\chi \in (0,1]$ та квантові ефективності η_1 та $\eta_2 \in (0,1]$ двох фотодіодів.

Після фотодетектування та віднімання струму зчитується струм сигналу биття в момент часу t

$$i_{\text{beat}}(t) = 2\chi^2(\eta_1 + \eta_2)\sqrt{R(\nu)(1-R(\nu))}\,\frac{e}{\hbar\omega}\sqrt{P_{\text{LO}}P_{\text{sig}}}\cos(2\pi\nu t) \qquad (2.48)$$

Тут ω – абсолютна кутова частота гетеродина лазера. Квадрат середньоквадратичної (RMS) амплітуди сигналу биття, оцифрованого аналого-цифровим (ADC) перетворювачем, отриманого за спектром потужності отриманих зразків, тоді визначається як

$$\widetilde{\text{TF}}(\nu) := \left(\sqrt{2}\chi^2(\eta_1 + \eta_2)\sqrt{R(\nu)(1-R(\nu))}\,\frac{e}{\hbar\omega}\right)^2 P_{\text{LO}}P_{\text{sig}}G(\nu) \qquad (2.49)$$

де $G(\nu)$ описує загальне посилення гомодинного детектора, можливих фільтрів і аналогового входу ADC, а також включає оцифровку в цілі числа. Ми називаємо $\text{TF} := \widetilde{\text{TF}}/P_{\text{sig}}$ передаточна функція.

Спектральна щільність потужності (PSD) флуктуацій вакууму після фотодетектування та оцифруваних зчитувань

$$\text{PSD}_{\text{vac}} = 2e(i_{\text{dc1}} + i_{\text{dc2}})G(\nu) = 2\frac{e^2}{\hbar\omega}(\eta_1(1-R(\nu)) + \eta_2 R(\nu))P_{\text{LO}}G(\nu) \qquad (2.50)$$

де i_{dc1} та i_{dc2} є прямими фотострумами, що генеруються фотодіодами. Використовуючи характеристику передавальної функції з рівняння 2.49 отримуємо

$$\text{PSD}_{\text{vac}} = \hbar\omega\frac{1}{\chi^2}\frac{\eta_1(1-R(\nu))+\eta_2 R(\nu)}{(\eta_1+\eta_2)^2 R(\nu)(1-R(\nu))}\frac{\widetilde{\text{TF}}(\nu)}{P_{\text{sig}}} \geq \hbar\omega\frac{\widetilde{\text{TF}}(\nu)}{P_{\text{sig}}} \qquad (2.51)$$

На останньому кроці ми обмежили PSD вакуумних флуктуацій знизу, використовуючи $1/\chi \geq 1$ та $\left(\eta_1\left(1-R(\nu)\right) + \eta_2 R(\nu)\right) / \left((\eta_1+\eta_2)^2 R(\nu)\left(1-R(\nu)\right)\right) \geq 1$, де рівність виконується для $\eta_1 = \eta_2 = 1, R = 0{,}5$.

3 ОПТИЧНИЙ КВАНТОВИЙ ГЕНЕРАТОР ВИПАДКОВИХ ЧИСЕЛ У РЕАЛЬНОМУ ЧАСІ 6 Гбіт/С НА ОСНОВІ ФЛУКТУАЦІЇ ВАКУУМУ

Випадкові числа є основою для застосування в статистиці, моделюванні [109], криптографії [110] і фундаментальній науці [111]. Випадковість випадкових чисел безпосередньо впливатиме на загальну безпеку відповідних прикладних систем. Класичні методи генерації випадкових чисел, наприклад, генератори псевдовипадкових чисел (RNG) на основі визначених алгоритмів [112], забезпечують економічно ефективний і портативний метод створення псевдовипадкових чисел з високою швидкістю, що задовольняє попит на випадкові числа більшості програм. Однак, через детерміновані та передбачувані особливості алгоритмів, псевдо RNG не підходять для певних програм, де потрібна справжня випадковість. У програмах криптографії випадкові числа з ненадійною випадковістю призведуть до проблем із безпекою, оскільки хакери можуть отримати доступ до інформації випадкових чисел і таким чином зламати системи шифрування [113]. Швидкий розвиток технологій квантової криптографії, таких як квантовий розподіл ключів [114-118], яка вимагає безпечної генерації випадкових чисел у режимі реального часу та високої швидкості, безперечно прискорює дослідження справжньої генерації випадкових чисел.

Засновані на внутрішній випадковості фундаментальних квантових процесів, гарантовано виробляють недетерміновані та непередбачувані випадкові числа [119-121]. Такі переваги привертають увагу дослідників, і запропоновано багато відповідних протоколів генератора. Було продемонстровано, що практичні протоколи QRNG реалізують високошвидкісну генерацію випадкових чисел з відносно низькою вартістю, включаючи вимірювання шляху фотона [122, 123], часу прибуття фотона [124-128], розподіл

кількості фотонів [129-133], флуктуація вакууму [134-140], фазовий шум [141-148] та підсилений спонтанний шум квантових станів [149-154] і т.д. Як правило, протокол, заснований на вимірюванні флуктуації вакууму, є більш прикладним і цінним протоколом QRNG через його зручність підготовки стану, нечутливість ефективності виявлення та високу швидкість генерації.

QRNG, засновані на вимірюванні флуктуації вакууму, зазвичай реалізуються шляхом застосування гомодинної схеми [134-140], які реалізують вимірювання квадратурної амплітуди вакуумного стану, щоб генерувати справжні випадкові числа. Їх безпека в кінцевому підсумку гарантується законами квантової фізики і може бути досягнута шляхом застосування ідеальних пристроїв. Але насправді обладнання практичних пристроїв у системах QRNG не завжди може задовольнити вимоги, що неминуче призведе до появи класичного шуму та, зрештою, призведе до зниження безпеки системи.

Сімейства універсальних хеш-функцій, включаючи хешування Тепліца [47,48], виявилися теоретично безпечними, і вони широко використовуються для усунення впливу класичного шуму, який ставить під загрозу безпеку згенерованих випадкових чисел [157]. Процес постобробки зазвичай називається вилученням випадковості. Матрицю хешування Тепліца часто вибирають як алгоритм вилучення випадковості через її низьку складність обчислення та реалізації. Дотепер існує багато реалізацій хешування Тепліца, реалізованих на різних платформах, включаючи пристрої центрального процесора (CPU), пристрої загального процесора (GPU) і пристрої програмованої вентильної матриці (FPGA) тощо. Реалізації на пристроях CPU перетворюють Тепліца алгоритм хешування до алгоритму швидкого перетворення Фур'є (FFT), тоді як їх швидкість обмежена відносно малими значеннями, такими як 441 Кбіт/с [157] та 1,6 Мбіт/с [145]. Реалізація графічного процесора реалізує паралельне обчислення багатьох потоків FFT у пристрої графічного процесора і таким чином досягає швидкості вилучення в реальному часі 1,35 Гбіт/с [158]. Однак ці

швидкості все ще не відповідають вимогам практичної квантової системи розподілу ключів щодо високошвидкісної генерації випадкових чисел у реальному часі.

Враховуючи переваги FPGA з паралельними обчисленнями, реалізація хешування Тепліца в пристроях FPGA може бути найбільш перспективним методом досягнення швидкої швидкості вилучення випадкових чисел, щоб підтримувати високу швидкість генерації випадкових чисел у реальному часі. Робота в реф. [147] представляє QRNG, заснований на вимірюванні флуктуацій фази лазера, і реалізує 3,36 Гбіт/с виділення випадкових чисел у реальному часі та, нарешті, підтримує 3,2 Гбіт/с генерацію випадкових чисел у реальному часі через обмеження швидкості підключається інтерфейсу малого форм-фактора. Алгоритм вилучення випадковості, застосований у цій роботі, перетворює всю матрицю Тепліца на підматриці та виконує операцію множення між підматрицями та вхідними необробленими даними, що покращує продуктивність вилучення випадковості. У той час як операція множення між підматрицями та вхідними необробленими даними все одно споживатиме певні обчислювальні ресурси, що значно обмежуватиме кінцеву швидкість вилучення випадковості на даному пристрої, де обчислювальні ресурси обмежені. Щоб вирішити цю проблему, потрібен оптимізований алгоритм хешування Тепліца, щоб зменшити споживання обчислювальних ресурсів і, нарешті, підтримувати більш високу швидкість вилучення.

Ми представляємо QRNG у реальному часі 6 Гбіт/с, заснований на вимірюванні флуктуації вакууму за гомодинною схемою. Щоб заповнити прогалину між швидкою генерацією випадковості та повільним виділенням випадковості, ми реалізуємо оптимізований алгоритм хешування Тепліца для підтримки реалізації високошвидкісних генераторів. Швидкість випадкового вилучення в реальному часі, яку ми зрозуміли, досягає 12 Гбіт/с, займаючи менше обчислювальних ресурсів, і алгоритм має здатність підтримувати сотні Гбіт/с

вилучення випадкових даних, що швидше, ніж коли-небудь повідомлялося про метод вилучення випадкових даних 3,36 Гбіт/с [147]. Припускаючи, що перехоплювач має повне знання класичного шуму, наш генератор має швидкість генерації випадкової інформації 6,83 Гбіт/с, і це підтримує генерацію інформаційно-теоретично підтверджених квантових випадкових чисел 6 Гбіт/с, які виводяться в реальному часі через периферійний компонент Interconnect Express (PCIE) інтерфейс із параметром безпеки $1.03e^{-128}$.

3.1 Алгоритм випадкового виділення в реальному часі

Для практичної системи QRNG електричний шум, який існує в реальній системі, впливатиме на безпеку необроблених даних, тому відповідна операція вилучення випадкових чисел дуже важлива для усунення впливу класичного шуму. Операція випадкового вилучення зазвичай виконується на основі оцінки мінімальної ентропії, яка допомагає охарактеризувати випадковість, яку можна витягти, і справжні випадкові числа будуть згенеровані після вилучення випадковості. Для системи реального часу швидкість вилучення зазвичай є вузьким місцем усієї системи. Тому дуже важливо розробити високошвидкісний алгоритм випадкового вилучення, щоб покращити загальну продуктивність системи.

Як одну з універсальних хеш-функцій, матрицю хешування Тепліца часто вибирають як алгоритм вилучення через її низьку складність обчислення та реалізації. Двійкову матрицю Тепліца T розміром $j \times k$ можна побудувати за допомогою $j + k - 1$ випадкових бітів з тієї причини, що кожна спадна діагональ матриці Тепліца однакова. Імовірність зіткнення такої матриці Тепліца, яка вказує на ймовірність отримання однакового виходу для різних вхідних вихідних даних, визначається кількістю рядків і кількістю стовпців у матриці Тепліца. Імовірність зіткнення певного гешу Тепліца дорівнює $k \cdot 2^{(-j+1)}$, де кількість стовпців k дорівнює довжині вхідних даних, а кількість рядків j вказує на

довжину вихідних даних. Отже, відносно невелику ймовірність зіткнення можна отримати за допомогою вибору відповідних значень k і j.

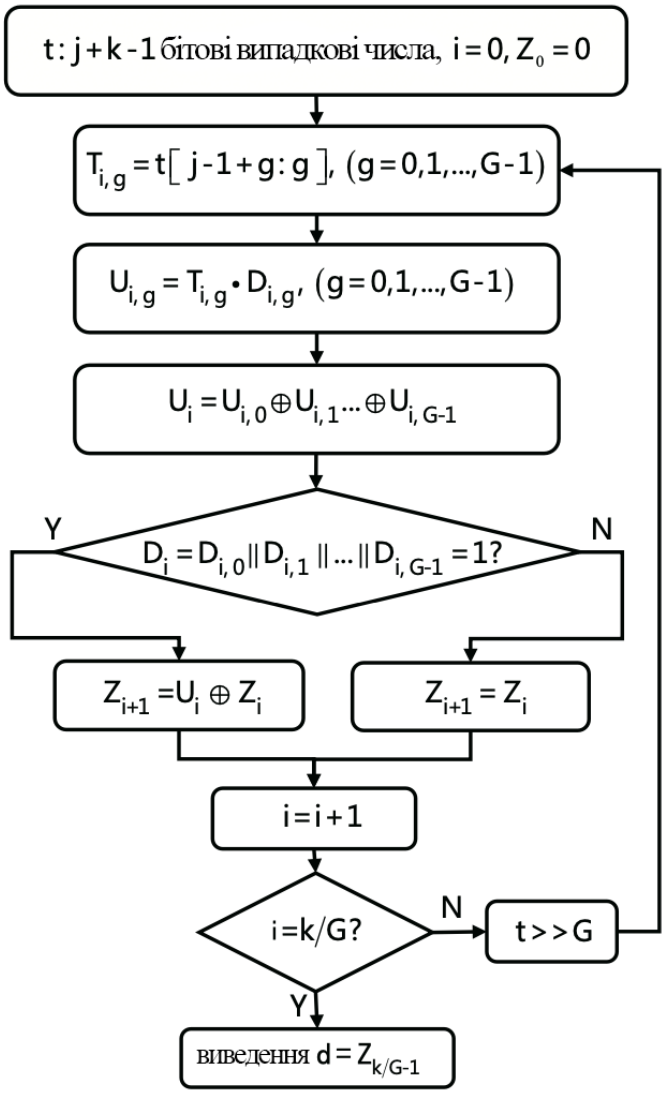

Рисунок 3.1 – Алгоритм вилучення випадковості кожного блоку розрахунку в реальному часі.

Переваги паралельних обчислень FPGA роблять його широко використовуваним у високошвидкісних обчислювальних програмах. Однак FPGA важко безпосередньо виконувати масштабні матричні обчислення через обмеження ресурсів FPGA. Алгоритм вилучення випадковості в реальному часі, застосований у [147] перетворює всю матрицю Тепліца на підматриці та виконує

операцію множення між підматрицями та вхідними необробленими даними. Хоча операція множення між підматрицями та вхідними необробленими даними все одно споживатиме певні обчислювальні ресурси, якщо підматриці великі. Враховуючи переваги FPGA із паралельним обчисленням, ми оптимізуємо алгоритм хешування Тепліца шляхом перетворення множення між підматрицями та вхідними необробленими даними на виключну операцію або операцію (XOR) між стовпцями матриці хешування Тепліца, що може значно зменшити споживання ресурсів і підтримує більш високу швидкість вилучення. Операцію множення матриці Тепліца T і необроблених даних D можна перетворити на операцію XOR між стовпцями T.

Як показано на рис. 3.1, $j + k - 1$ випадкових бітів використовуються як вихідні числа випадкового числа. Кожні G стовпці годинника матриці Тепліца можна окремо представити як $T_{i,g} = t[j - 1 + g: g], g = 0,1,2, \dots, G - 1$. G необроблені біти даних $D_{i,g} = 1$ або 0 одночасно приведуть до відповідної проміжної змінної $U_{i,g} = T_{i,g}$ або $U_{i,g} = 0$, та $U_i = U_{i,0} \oplus U_{i,1} \dots \oplus U_{i,G-1}$буде досягнуто. Якщо$D_i = D_{i,0} \| D_{i,1} \| \dots \| D_{i,G-1} = 1$, інша проміжна змінна $Z_{i+1} = U_i \oplus Z_i$. В іншому випадку, якщо $D_i = D_{i,0} \| D_{i,1} \| \dots \| D_{i,G-1} = 0$, тоді $Z_{i+1} = Z_i$. Значення лічильника і збільшується на 1 за раунд. Якщо i дорівнює k/G, результат розрахунку $d = Z_{k/G-1}$ виведень. В іншому випадку t зрушить G бітів праворуч і перезапустить присвоєння $T_{i,g}$. Результатом d є остаточні витягнуті j бітові випадкові числа. Примітно, що номер стовпця для кожної операції XOR може бути не тільки G, але й цілим числом, кратним G. Зазвичай ми встановлюємо значення G, що дорівнює інтегральній частоті точності вибірки n, щоб спростити процес обчислення. Якщо припустити, що частота обчислення екстрактора дорівнює C, такий модуль випадкового вилучення може реалізувати обробку необроблених даних у реальному часі зі швидкістю CG.

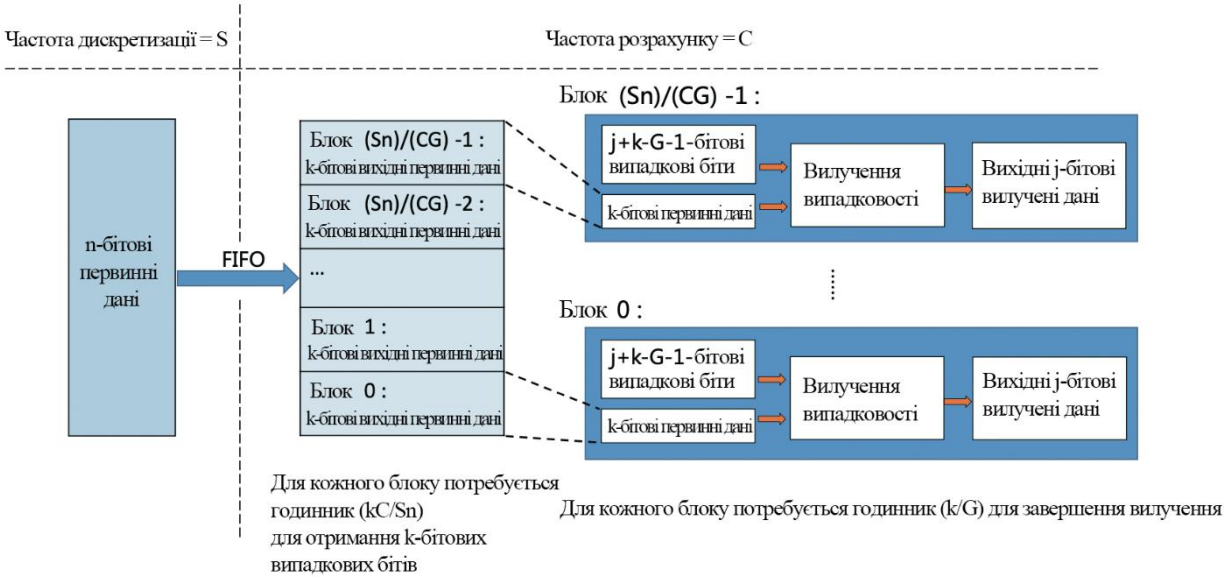

Рисунок 3.2 – Процес алгоритму вилучення випадковості, де кілька блоків працюють паралельно. Щоб подолати розрив у швидкості, відібрані високошвидкісні n-бітні первинні дані передаються в кілька низькошвидкісних попередньо оброблених k-бітових блоків даних через один або кілька модулів черги пам'яті, які називаються First Input First Out (FIFO). Блоки обчислення *(Sn)/(CG)* на основі алгоритму, представленого на рис. 1, циклічно викликаються з блоку 0 до блоку *(Sn)/(CG)*-1, як тільки кожний блок завершує отримання необроблених даних. Причина того, що випадкове вилучення працює на частоті *C*, а не *S*, полягає в тому, що загальна плата розробки FPGA не підтримує занадто швидку тактову частоту.

Однак платформа FPGA підтримує швидкість обчислення *C*, яка є набагато нижчою за частоту дискретизації *S*. Тому необхідно перетворити дискретизовані високошвидкісні *n*-бітні необроблені дані в кілька низькошвидкісних попередньо оброблених *k*-бітних блоків даних за допомогою середовища кешування під назвою First Input First Вихід (FIFO).

Як показано на рис. 3.2 ці блоки послідовно пронумеровані як 0, 1, 2, ..., *(Sn)/(CG)*-1. Хід перетворення можна розділити на два етапи. По-перше, ми використовуємо FIFO для перетворення *n*-розрядних даних із частотою *S* у бітові

дані Sn/C із частотою C. Через обмеження FPGA значення S/C зазвичай встановлюється як 2', а значення з i можна встановити як -3, -2, -1, 0, 1, 2 або 3. Якщо значення S/C має бути більше 8, більше FIFO буде каскадовано для реалізації такої функції. Після першого кроку бітрейт на вихідній стороні FIFO дорівнює Sn, що набагато вище, ніж швидкість вилучення випадковості, CG, кожного блоку. Отже, по-друге, ми будемо розподіляти $(Sn)/C$ бітові дані з вихідного порту FIFO до $(Sn)/(CG)$ незалежних блоків обчислень послідовно, керуючи вихідним сигналом дозволу. Таким чином, кожен блок потребуватиме $(kC)/(Sn)$ годинників для послідовногоотримання k бітових даних. Слід зауважити, що частота бітових даних Sn/C, які отримує кожен блок, дорівнює C замість S. Наступна обробка також працюватиме на частоті з C.

Після того як один блок закінчить зберігати k-бітові дані, цей блок припинить зберігання даних, а наступний блок почне зберігати наступні k-бітові дані. Коли останній блок, блок $(Sn)/(CG)$-1, завершує зберігання даних, перший блок, блок 0, знову починає зберігання даних, що являє собою цикл зберігання даних. Для послідовного зберігання даних для всіх $(Sn)/(CG)$ блоків знадобиться тактовий сигнал k/G.

Нарешті, ми застосуємо алгоритм вилучення випадковості, представлений на рис. 3.3 в кожному блоці. Кожен годинник G бітові необроблені дані використовуватимуться для контролю прогресу вилучення, так що кожен блок із k бітовими вхідними необробленими даними потребуватиме k/G тактів для виконання вилучення випадковості та виведення j біт вилучених випадкових чисел. Операція вилучення кожного блоку починається, як тільки блок закінчує зберігання даних, і вони обчислюються незалежно. Як правило, значення G можна встановити як ціле число, кратне точності вибірки n, і в наших налаштуваннях це значення дорівнює n для спрощення процесу обчислення.

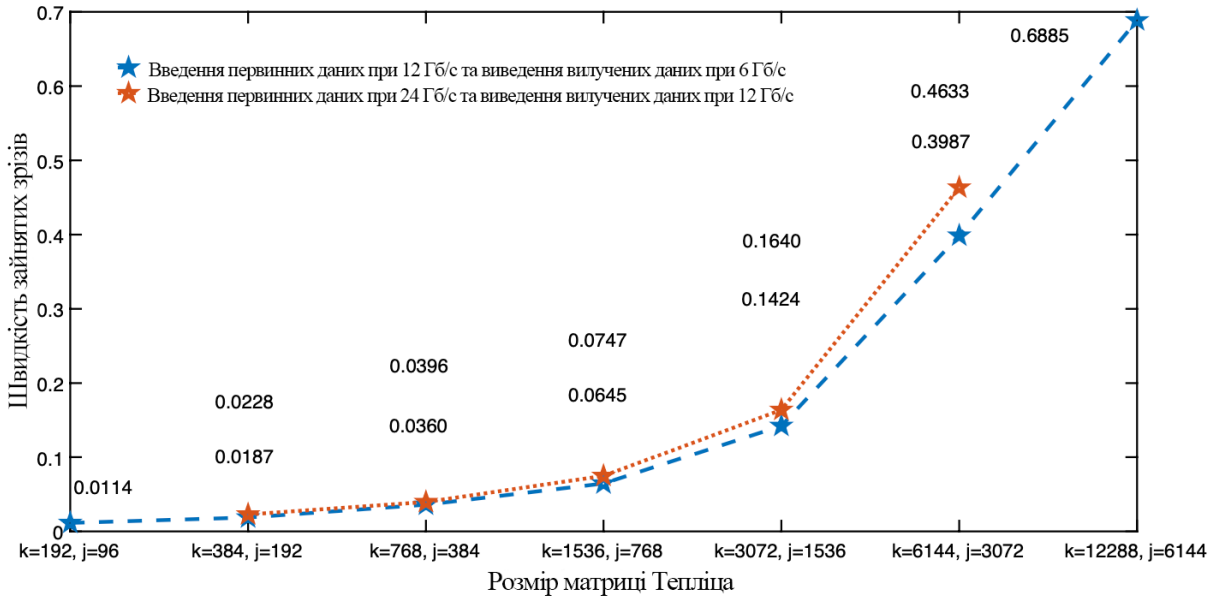

Рисунок 3.3 – Результат перевірки споживання обчислювальних ресурсів алгоритму. Ми зосереджуємося на ресурсі зрізу, який становить основну логічну одиницю FPGA. Тест проводиться на оціночній платі Xilinx KC705, яка має 50950 зрізів. k дорівнює довжині вхідних даних і номеру стовпця матриці T. j вказує довжину вихідних даних разом із номером рядка матриці T. Синя лінія є результатом тесту, який використовує різні матриці Тепліца для обробки вхідних необроблених даних 12 Гбіт/с. Вхідні дані розділені на 8 блоків, які обчислюються окремо. Червона лінія показує результати обробки вхідних необроблених даних 24 Гбіт/с, які розділені на 16 блоків, які обчислюються окремо.

Перевірка споживання обчислювальних ресурсів алгоритму виконується на платі оцінювання Xilinx KC705, щоб знайти відповідну схему конфігурації параметрів. Легко зрозуміти, що швидкість вилучення екстрактором пов’язана з кількістю блоків, що працюють паралельно, разом із апаратним ресурсом обчислювальної платформи. Швидкість вилучення випадковості зростає лінійно зі збільшенням кількості блоків при заданій частоті обчислень, у той час як зайняті обчислювальні ресурси також збільшаться. Результати тесту показані на

рис. 3.3. Ми встановлюємо $j/k = 1/2$ і $G=n=12$, щоб перевірити, як різні значення k і j впливають на зайнятість обчислювальних ресурсів. Для заданого номера блоку та частоти обчислення C, чим більше значення k і j, тим більше обчислювальних ресурсів буде споживано, а збільшення значень k і j безпорадно для швидкості обчислення. Тоді як більші значення k і j допомагають отримати менший параметр безпеки, коли визначається значення випадковості, яке можна витягти, яке буде детально проаналізовано в наступному розділі. Примітно, що якщо ми використовуємо матрицю Тепліца з невеликим розміром, тобто 192 x 384, за допомогою цього алгоритму можна реалізувати обробку сотень Гбіт/с необроблених даних у реальному часі. У цьому експерименті ми гарантуємо, що обчислений параметр безпеки є достатньо малим, вибираючи відповідні k і j, і в той же час менше використовуємо обчислювальні ресурси. Екстрактори випадковості, що підтримують 24 Гбіт/с і 12 Гбіт/с вхідних необроблених даних у реальному часі, реалізовані, і результати споживання їх фрагментів показані на рис. 3 , де зріз становить основну логічну одиницю FPGA. Взявши для прикладу один із екстракторів, він займатиме 16,40% фрагментів, коли розмір матриці хешування Тепліца становить 1536 x 3072 і 16 блоків викликаються для реалізації випадкового вилучення в реальному часі необроблених даних у реальному часі 24 Гбіт/с, що означає, що наш алгоритм є дуже перспективним для підтримки ще швидшого вилучення випадковості на нашій платформі, тобто платі оцінки KC705.

3.2. Експериментальне впровадження

Щоб реалізувати практичний безпечний високошвидкісний QRNG у режимі реального часу, ми реалізуємо оптоволоконну установку з декількома готовими пристроями та платою аналого-цифрового перетворювача (ADC) власної розробки та застосовуємо оптимізований екстрактор випадковості в

реальному часі для генерації справжніх випадкових чисел шляхом вимірювання флуктуації вакууму. Блок-схема показана на рис. 4 .

1550-нм волоконний лазер (NKT Basic E15, ширина лінії 100 Гц) служить гетеродином (LO) і підключений до одного вхідного порту 50:50 дільника променя (BS). У той час як інший вхідний порт заблокований для забезпечення стану вакууму. Два вихідних порти дільника променя оптично з'єднані з двома вхідними портами збалансованого гомодинного детектора (Thorlabs PDB480C, смуга пропускання обмежена 1 ГГц фільтром низьких частот). Результати вимірювань збалансованого гомодинного детектора остаточно дискретизуються 12-розрядною картою АЦП (ADS5400, частота дискретизації 1 ГГц, точність дискретизації 12 бітів і діапазон вхідної напруги $2R$, зменшений з 2 VPP до 1,5 VPP за допомогою попереднього підсилювача плати ADC) щоб отримати необроблені дані в режимі реального часу. Наступний екстрактор випадковості на основі оптимізованого алгоритму використовується для виконання екстракції одночасно з отриманням необроблених даних.

Припускаючи в гіршому випадку, що супротивник може слухати і контролювати класичний шум, Haw та інші [137] встановили максимальну мінімальну ентропію дискретизованого сигналу вимірювання.

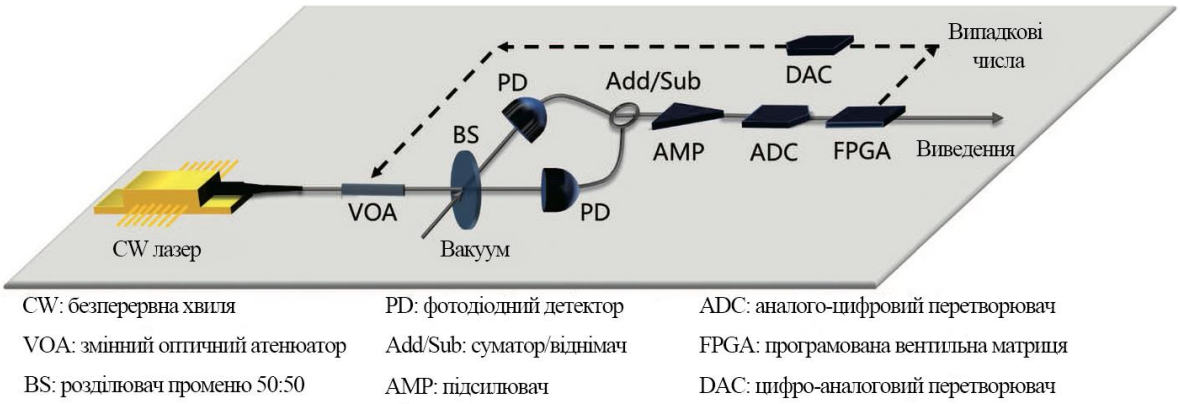

Рисунок 3.4 – Експериментальна демонстрація оптичного QRNG в реальному часі на основі флуктуації вакууму. Промені CW, випромінювані лазерним діодом, надходять на один вхідний порт 50:50 BS. Інший вхідний порт BS заблокований для забезпечення стану вакууму. Наступна операція вимірювання реалізується гомодинним детектором і ADC. Результат вимірювання остаточно обробляється екстрактором випадковості для виділення остаточних випадкових бітів.

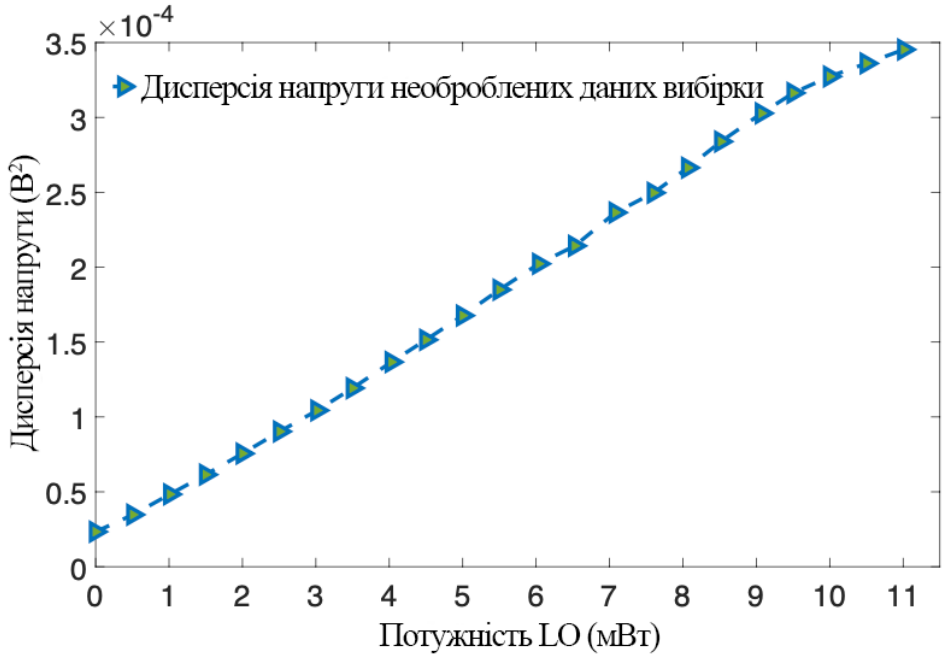

Рисунок 3.5 – Дисперсія в залежності від потужності LO. На цьому рисунку показано дисперсію напруги вихідних даних вибірки як функцію потужності LO. Потужність LO збільшується шляхом регулювання змінного аттенюатора від 0 мВт до мВт з розміром кроку 0,5 мВт. Дисперсія напруги необроблених даних збільшується лінійно з потужністю LO в діапазоні від 0 мВт до 9,5 мВт. Нахил кривої тенденції буде зменшуватися, коли потужність LO буде більшою за 9,5 мВт.

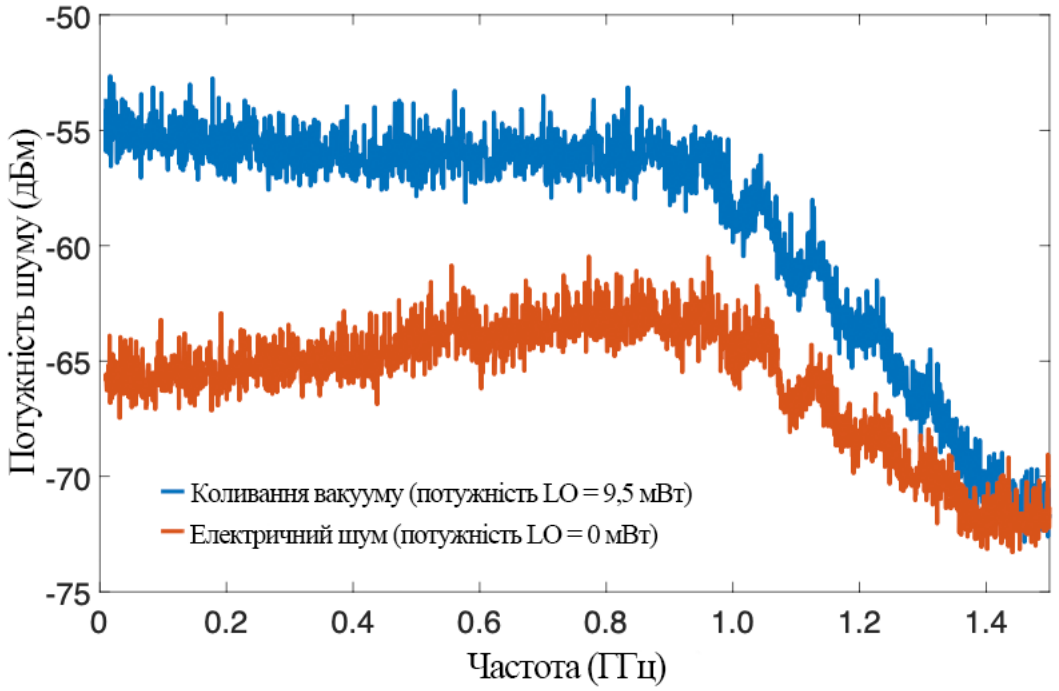

Рисунок 3.6 – Щільність спектру потужності флуктуацій вакууму, коли потужність LO становить 9,5 мВт (синя лінія), і електричного шуму, коли потужність гетеродина становить 0 мВт (червона лінія). Діапазон смуги пропускання 3 дБ f0 становить приблизно 0-1 ГГц. Відповідний результат отримується за допомогою аналізатора спектру для виявлення вихідного сигналу детектора.

M_{dis} обумовлений класичним шумом E, який є

$$H_{\min}(M_{dis} \mid E) = -\log_2[\max(c_1, c_2)] \tag{3.1}$$

де $c_1 = \frac{1}{2}\left[\operatorname{erf}\left(\frac{e_{\max} - R + 3\delta/2}{\sqrt{2}\sigma_Q}\right) + 1\right], c_2 = \operatorname{erf}\left(\frac{\delta}{2\sqrt{2}\sigma_Q}\right),$ (3.2)

і значення M є суперпозицією квантового шуму Q і класичного шуму E. R дорівнює половині діапазону вхідної напруги карти ADC і $\delta = 2R/(2^n)$, де n — точність вибірки карти ADC. σ_Q вказує на значення стандартного відхилення квантової флуктуації. Цей результат базується на припущенні, що квантова

випадковість не залежить від класичного шуму, а значення класичного шуму знаходиться в межах кінцевого інтервалу, тобто $-5\sigma_E \leq e \leq 5\sigma_E$, що є дійсним для 99,9999%.

Ми спрощуємо хід аналізу та гарантуємо, що система працює в безпечних умовах, які $c_1 \leq c_2$, у якому порівняння між c_1 і c_2 вкаже, чи оцінка мінімальної ентропії використовує правильну максимальну ймовірність вгадування. У цьому випадку ми можемо спростити умовну мінімальную ентропію як

$$H_{\min}(M_{dis} \mid E) = -\log_2\left[\operatorname{erf}\left(\frac{\delta}{2\sqrt{2}\sigma_Q}\right)\right] \tag{3.3}$$

в якій ми знаходимо, що $H_{\min}(M_{dis} \mid E)$ збільшується при зменшенні δ і збільшенні σ_Q. Для даної системи QRNG, її точність вибірки δ визначається, тому ми розглядаємо, як побудовані компоненти впливають на значення σ_Q.

Відповідна потужність LO покращує значення σ_Q^2 як посилання [138] введено. Потужність LO збільшується шляхом регулювання змінного аттенюатора від 0 мВт із кроком 0,5 мВт для пошуку оптимального σ_Q^2. Одночасно розраховується та записується дисперсія напруги кожного виміряного вихідного даних, як показано на рис. 3.5. Коли потужність LO встановлена на 0 мВт, виміряна дисперсія напруги 10^8 послідовних необроблених даних розглядається як σ_E^2, що має середнє розрахункове значення 3,13e^{-5} В ^{2}. Рис. 3.5 вказує на те, що дисперсія напруги необроблених даних збільшується лінійно з потужністю LO в діапазоні від 0 мВт до 9,5 мВт. У той час як нахил кривої тенденції буде зменшуватися, коли потужність LO буде більшою за 9,5 мВт.

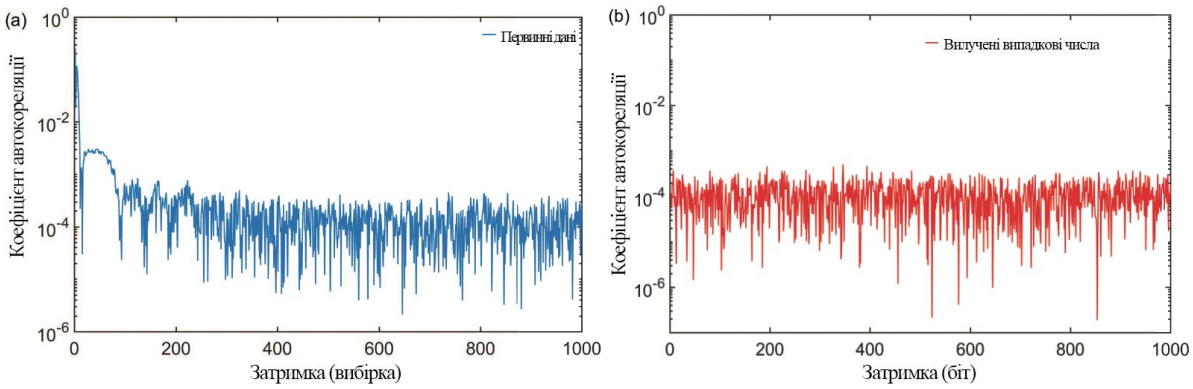

Рисунок 3.7 – Автокореляція 10^7 первинних даних (a) і 10^7 біт вилучених випадкових чисел (b). Недосконалий гомодинний детектор без крутої бічної смуги неминуче погіршить продуктивність автокореляції, що призводить до вищих значень автокореляції низького порядку. Автокореляція, яка існує в необроблених даних, добре усувається процесом хешування Тепліца.

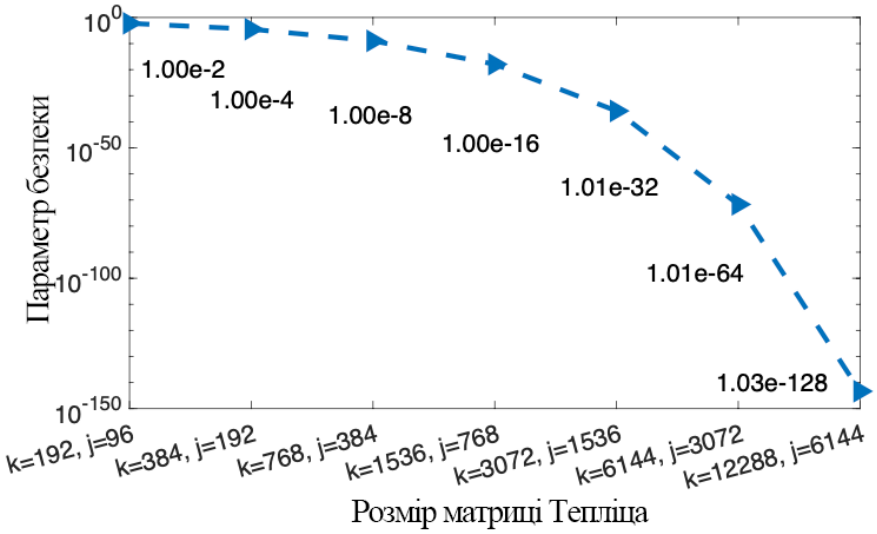

Рисунок 3.8 – Розраховані значення параметрів безпеки для різних розмірів матриці Тепліца, коли вилучена випадковість вхідних первинних даних становить 56,92%.

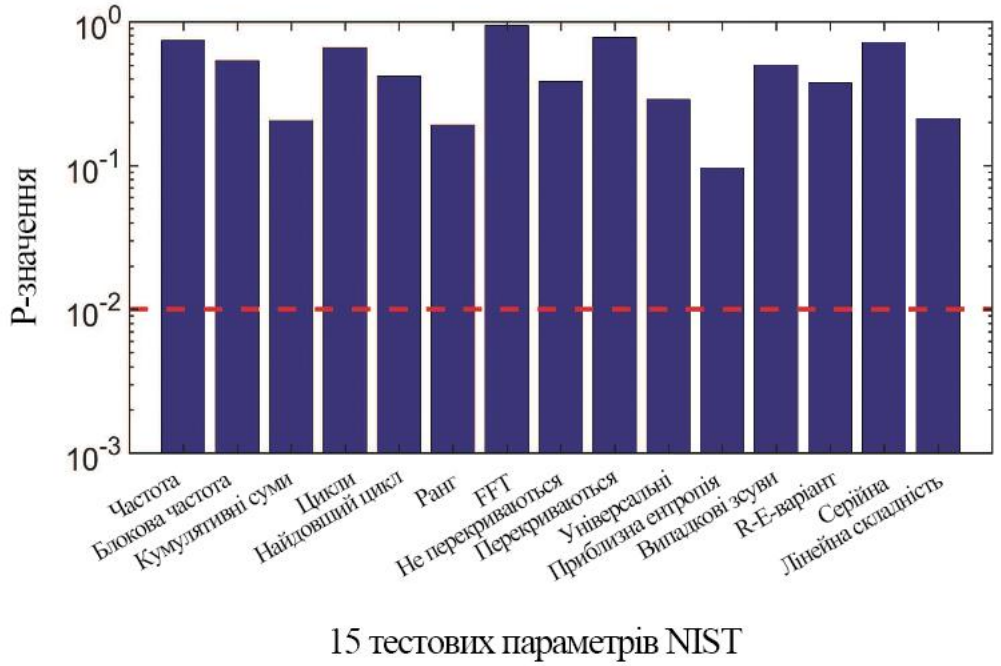

Рисунок 3.9 – Результати набору статистичних тестів NIST. Стандартні набори тестів NIST містять 15 тестових параметрів. Критерій Колмогорова-Смірнова використовується для отримання кінцевого p-значення для випадків кількох p-значень. Тест вважається успішним, якщо всі кінцеві p-значення задовольняють 0,01≤p-значення≤0,99.

Середнє σ_M^2 значення відповідних 10^8 послідовних даних можна отримати як 3,16e^{-4} В^2 шляхом встановлення потужності LO на 9,5 мВт. Для нашого ADC із 12-розрядною точністю дискретизації та діапазоном вхідної напруги 1,5 VPP його дисперсія помилок квантування обчислюється як $(\delta/12)^2 = (1.5/(4096 \cdot 12))^2 = 9{,}3132\text{e}^{-10}$ В^2. У дискретизації M і E існують помилки квантування, тому надійна верхня межа of σ_Q^2 може бути розрахована як $\sigma_M^2 - \sigma_E^2 - 2(\delta/12)^2 = 2{,}8457\text{e}^{-4}\text{В}^2$ при розгляді впливу помилок квантування ADC. Замініть σ_Q^2 в рівнянні (2) і $H_{\min}(M_{dis} \mid E)$ таким чином обчислюється як 6,83 біта на вибірку, що означає, що 56,92% випадкових бітів можна згенерувати з кожної вибірки, а

швидкість генерації квантової випадковості в реальному часі досягає 6,83 Гбіт/с. Варто відзначити, що власно розроблений збалансований гомодинний детектор 1,2 ГГц використовується для побудови системи квантового генератора випадкових чисел, і він досяг мінімального значення ентропії 6,53 біта на вибірку [159].

Квантовий шум значно перевищує класичний шум на вихідному кінці гомодинного детектора, коли потужність гетеродина встановлена на 9,5 мВт, як показано на рис. 6. Наступний 12-розрядний ADC із частотою дискретизації 1 ГГц перетворює сигнали в цифрові дані. 8 блоків операцій вилучення із синхронізованою частотою обчислення C 125 МГц виконуються паралельно на FPGA в реальному часі. Для нашої реалізації гешування Тепліца ми встановлюємо $j = 6144$ і $k = 12288$, щоб коефіцієнт вилучення становив $j/k = 50\%$, що є меншим за 56,92%, як отримано з обчисленої $H_{\min}(M_{dis} \mid E)$.

Таким чином, теоретичний параметр безпеки інформації ε, який означає статистичну відстань між вилученою випадковою послідовністю та рівномірною послідовністю, може бути обчислений за допомогою залишкової геш-леми, $j = k \cdot H_{\min}(M_{dis} \mid E)/n - 2 \cdot \log_2(1/\varepsilon)$. Розраховане ε становить приблизно 1,03e^{-128} у нашій установці. З такою конфігурацією швидкість генерації випадкових чисел у реальному часі може досягти 6 Гбіт/с. Примітно, що для різних розмірів матриці Тепліца розраховані значення параметрів безпеки досить різні, як показано на рис. 8. Для виконання вилучення можна вибрати різні матриці Тепліца відповідно до фактично доступних ресурсів і різних вимог безпеки.

Щоб перевірити випадковість згенерованих у реальному часі випадкових чисел, витягнуті випадкові числа завантажуються на комп'ютер. через інтерфейс PCIE для автономного тестування на випадковість. Максимальна теоретична швидкість PCIE для передачі витягнутих випадкових чисел досягає 13,66 Гбіт/с, коли плата KC705 налаштована на роботу в 8 смугах у режимі швидкості

з’єднання 2,5 Гбіт/с і може ефективно підтримувати нашу передачу даних 6 Гбіт/с.

Тести автокореляції виконуються для порівняння якості необроблених даних і витягнутих випадкових чисел, як показано на рис. 7. Ми випадковим чином вибираємо 10^7 послідовних необроблених даних і 10^7 послідовних витягнутих випадкових чисел. Причина відносно великої автокореляції, яка існує в необроблених даних, полягає в тому, що недосконалий гомодинний детектор без крутої бічної смуги неминуче погіршить продуктивність автокореляції [135], що призводить до вищих значень автокореляції низького порядку. Автокореляція може бути значно зменшена після операції хешування Тепліца.

Ми також застосовуємо стандартний набір тестів NIST для перевірки отриманих випадкових чисел. Двійкові дані розміром 1 гігабіт зчитуються та діляться на 1000 підпослідовностей по 1 мегабіту. Для обробки результатів тесту ми застосовуємо критерій Колмогорова-Смирнова (KS), щоб отримати кінцеве значення p для випадків, коли кожен елемент тесту отримає кілька значень p. Як правило, тест вважається успішним, якщо всі кінцеві значення p задовольняють 0,01<P-значення<0,99. Результати тестування показані на рис. 3.9, який вказує на те, що згенерована випадкова бітова послідовність пройшла всі тести NIST.

ВИСНОВКИ

У дииломній роботі використані результати попередніх досліджень та розробок з квантової криптографії, квантової стеганографії, квантової інформаційної технології та криптоаналізу квантових систем. Одним з основних методів є розробка моделі безпеки, яка базується на комплексному підході до вирішення проблем безпеки. Це включає аналіз ризиків, ідентифікацію потенційних загроз та вразливостей системи, розробку алгоритмів та процедур захисту, які враховують характеристики квантового генератора випадкових чисел та його взаємодію з іншими компонентами веб-сервісу.

Розробка методу захисту, який забезпечує цілісність та конфіденційність випадкових чисел, є новим напрямком досліджень. В даній роботі розроблено метод захисту, який базується на використанні криптографічних алгоритмів та квантової криптографії для захисту квантового генератора випадкових чисел від кіберзагроз.

У дипломній роботі розглянуто найпопулярніші програми E2EE, включаючи їхні базові протоколи обміну повідомленнями E2EE та церемонії автентифікації. Незважаючи на те, що церемонія автентифікації відіграє важливу роль у запобіганні активним атакам MitM, деякі програми E2EE не пропонують жодної церемонії автентифікації своїм користувачам. Виявлено, що поточні реалізації функції E2EE в різних програмах E2EE, зокрема в опортуністичному режимі E2EE, можуть перемогти пасивного зловмисника MitM, але не можуть перемогти активного зловмисника MitM. Також виявлено, що фактична реалізація функції E2EE в режимі автентифікації E2EE значною мірою залежить від того, чи користувачі успішно виконають і завершать церемонію автентифікації. Однак кілька досліджень показали, що користувачі не можуть успішно виконати та завершити церемонію автентифікації і, отже, стають

уразливими до активних атак MitM через проблеми з зручністю використання та людські помилки. Ця систематизація відкриває шляхи, які потребують подальшого дослідження. По-перше, необхідні подальші дослідження для автоматизації церемонії автентифікації або впровадження напівавтоматизованої церемонії автентифікації, щоб зменшити зусилля з боку користувача під час виконання церемонії автентифікації. Крім того, необхідні додаткові дослідження, щоб поширити дослідження на контекст групового спілкування. Більшість дослідницьких досліджень зосереджено лише на двосторонньому E2EE, але наявність більше двох сторін ускладнить виконання церемонії автентифікації. Нарешті, нові дослідження можуть бути зосереджені на роботі протоколу E2EE лише через аудіоканал. Більшість досліджень зосереджено лише на телефонах, які завжди мають два канали (канал даних і аудіоканал). Тому необхідні нові дослідження, щоб продемонструвати, як встановити цей протокол E2EE на лінійних телефонах, які мають лише аудіоканали.

Запропоновано та експериментально продемонстровано високошвидкісний квантовий генератор випадкових чисел, що працює в режимі реального часу, перевірений безпекою, шляхом вимірювання флуктуації вакууму. Запропоновано та реалізовано оптимізований алгоритм випадкового вилучення, щоб подолати розрив у швидкості між швидким генеруванням випадковості та повільним вилученням випадковості. Операція вилучення усуває потенційні проблеми безпеки, спричинені класичним шумом.

Оскільки це квантовий генератор випадкових чисел, у майбутньому буде цікаво застосувати повністю квантовий метод аналізу для кількісної оцінки випадковості, яку можна витягнути. Тим часом можна провести подальші дослідження, запропонувавши різні методи захисту від хакерських атак, наприклад моніторинг мінімальної ентропії в реальному часі, для підвищення практичної безпеки квантових генераторів випадкових чисел.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. R. Abu-Salma, K. Krol, S. Parkin, V. Koh, K. Kwan, J. Mahboob, Z. Traboulsi, and M A. Sasse. 2017. The Security Blanket of the Chat World: An Analytic Evaluation and a User Study of Telegram. Internet Society. https://doi.org/10.14722/eurousec.2017.23006 (дата звернення: 14.11.23).

2. R. Abu-Salma, M. Angela Sasse, J. Bonneau, A. Danilova, A. Naiakshina, and M. Smith. 2017. Obstacles to the Adoption of Secure Communication Tools. In 2017 IEEE Symposium on Security and Privacy (SP). IEEE, 137-153. https://doi.org/10.1109/SP.2017.6 (дата звернення: 14.11.23).

3. D. Bohn. 2020. Google is rolling out end-to-end encryption for RCS in Android Messages beta, https://www.theverge.com/2020/11/ 19/21574451/android-rcs-encryption-message-end-to-end-beta (дата звернення: 10.11.23).

4. N. Borisov, I. Goldberg, and E. Brewer. 2004. Off-the-Record Communication, or, Why Not to Use PGP. In Proceedings of the 2004 ACM Workshop on Privacy in the Electronic Society (WPES '04). Association for Computing Machinery, New York, NY, USA, 77-84. https://doi.org/10.1145/1029179.1029200 (дата звернення: 14.11.23).

5. Pew Research Center. 2017. Most Americans think the government could be monitoring their phone calls and emails, https: //pewrsr.ch/3nI8hIf (дата звернення: 10.11.23).

6. D. Clark. 2015. Microsoft to Alert Users to Suspected Government Snooping, https://www.wsj.com/articles/microsoft-to-alertusers-to-suspected-government-snooping-1451528624 (дата звернення: 10.11.23).

7. K. Cohn-Gordon, C. Cremers, B. Dowling, L. Garratt, and D. Stebila. 2020. A formal security analysis of the signal messaging protocol. Journal of Cryptology 33, 4 (2020), 1914-1983. https://doi.org/10.1007/s00145-020-09360-1

8. LINE Corporation. 2021. LINE Encryption Overview, https://d.line-scdn.net/stf/linecorp/en/csr/line-encryptionwhitepaper-ver2.1.pdf (дата звернення: 10.11.23).

9. S. Dechand, D. Schürmann, K. Busse, Y. Acar, S. Fahl, and M. Smith. 2016. An Empirical Study of Textual Key-Fingerprint Representations. In Proceedings of the 25th USENIX Conference on Security Symposium (SEC'16). USENIX Association, USA, 193-208.

10. K. Donaldson and M. Burton. 2019. Facebook, WhatsApp Will Have to Share Messages With U.K., https://www.bloomberg.com/news/articles/2019-09-28/facebook-whatsappwill-have-to-share-messages-with-u-k-police (дата звернення: 10.11.23).

11. Element 2022. https://element.io/. (дата звернення: 14.11.23).

12. K. Ermoshina, F. Musiani, and H. Halpin. 2016. End-to-End Encrypted Messaging Protocols: An Overview. In International Conference on Internet Science. Springer, 244-254. https://doi.org/10.1007/978-3-319-45982-0_22

13. Facebook. 2017. Messenger Secret Conversations. Technical Whitepaper, https://about.fb.com/wp-content/uploads/2016/07/messengersecret-conversations-technical-whitepaper.pdf (дата звернення: 10.11.23).

14. Facebook Messenger 2022. https://www.messenger.com/. (дата звернення: 14.11.23).

15. FaceTime 2022. https://support.apple.com/en-us/HT204380. (дата звернення: 14.11.23).

16. T. Frosch, C. Mainka, C. Bader, F. Bergsma, J. Schwenk, and T. Holz. 2016. How Secure is TextSecure?. In 2016 IEEE European Symposium on Security and Privacy (EuroSP). IEEE, 457-472. https: //doi.org/10.1109/EuroSP.2016.41

17. C. Garman, M. Green, G. Kaptchuk, I. Miers, and M. Rushanan. 2016. Dancing on the Lip of the Volcano: Chosen Ciphertext Attacks on Apple Imessage. In

Proceedings of the 25th USENIX Conference on Security Symposium (SEC'16). USENIX Association, USA, 655-672.

18. Wire Swiss GmbH. 2021. Wire Security Whitepaper, https://wire-docs.wire.com/download/WireSecurityWhitepaper.pdf. (дата звернення: 10.11.23).

19. Google. 2022. Messages End-to-End Encryption Overview, https://www.gstatic.com/messages/papers/messages_e2ee.pdf (дата звернення: 10.11.23).

20. Google Meet 2022. https://apps.google.com/meet/. (дата звернення: 14.11.23).

21. A. Herzberg and H. Leibowitz. 2016. Can Johnny Finally Encrypt? Evaluating E2E-Encryption in Popular IM Applications. In Proceedings of the 6th Workshop on Socio-Technical Aspects in Security and Trust (STAST '16). Association for Computing Machinery, New York, NY, USA, 17-28. https://doi.org/10. 1145/3046055.3046059 (дата звернення: 14.11.23).

22. A. Herzberg, H. Leibowitz, K. Seamons, E. Vaziripour, J. Wu, and D. Zappala. 2021. Secure Messaging Authentication Ceremonies Are Broken. IEEE Security & Privacy 19, 2 (2021), 29-37. https://doi.org/10.1109/ MSEC.2020.3039727

23. C. Howell, T. Leavy, and J. Alwen. 2017. Wickr Messaging Protocol. TECHNICAL PAPER, https://wickr.com/wpcontent/uploads/2019/12/WhitePaper_WickrMessagingProtocol.pdf (дата звернення: 10.11.23).

24. Apple Inc. 2021. Apple Platform Security. iMessage security overview, https://support.apple.com/guide/security/imessage-securityoverview-secd9764312f/web (дата звернення: 10.11.23).

25. Apple Inc. 2022. Apple Platform Security. FaceTime security, https://support.apple.com/guide/security/facetime-security-seca331c55cd/ web (дата звернення: 10.11.23).

26. T. Isobe and K. Minematsu. 2018. Breaking Message Integrity of an End-to-End Encryption Scheme of LINE. In European Symposium on Research in Computer Security, Javier Lopez, Jianying Zhou, and Miguel Soriano (Eds.). Springer, Springer International Publishing, Cham, 249-268. https://doi.org/10. 1007/978-3-319-98989-1_13 (дата звернення: 14.11.23).

27. KakaoTalk 2022. https://www.kakaocorp.com/service/KakaoTalk?lang=en. (дата звернення: 14.11.23).

28. H. Krawczyk. 2003. SIGMA: The ?SIGn-and-MAc'approach to authenticated Diffie-Hellman and its use in the IKE protocols. In Annual International Cryptology Conference. Springer, 400-425. https://doi.org/10.1007/978-3-540-45146-4_24

29. M. Krohn. 2020. Zoom Rolling Out End-to-End Encryption Offering, https://blog.zoom.us/zoom-rolling-out-end-to-endencryption-offering/ (дата звернення: 10.11.23).

30. M. Krohn. 2022. End-to-End Encryption Expands to Zoom Phone and Breakout Rooms, https://blog.zoom.us/end-to-endencryption-zoom-phone-breakout-rooms/ (дата звернення: 10.11.23).

31. A. Langley. 2009. Opportunistic encryption everywhere. In W2SP (2009). (дата звернення: 14.11.23).

32. Line 2022. https://line.me/en/. (дата звернення: 14.11.23).

33. Linphone 2020. https://www.linphone.org/. (дата звернення: 14.11.23).

34. Linphone. 2020. LIME, https://www.linphone. org/technical-corner/lime (дата звернення: 10.11.23).

35. M. Madden. 2014. Public Perceptions of Privacy and Security in the PostSnowden Era, https://www.pewresearch.org/ internet/2014/11/12/public-privacy-perceptions/ (дата звернення: 10.11.23).

36. M. Marlinspike. 2013. Advanced cryptographic ratcheting, https://signal.org/blog/advanced-ratcheting/ (дата звернення: 10.11.23).

37. M. Marlinspike and T. Perrin. 2016. The x3dh key agreement protocol. Open Whisper Systems (2016). (дата звернення: 14.11.23).

38. Matrix 2022. https://matrix.org/. (дата звернення: 14.11.23).

39. Messages by Apple 2022. https://support.apple.com/explore/messages. (дата звернення: 14.11.23).

40. Messages by Google 2022. https://messages.google.com/. (дата звернення: 14.11.23).

41. Microsoft. 2018. Skype Private Conversation. Technical white paper, https://az705183.vo.msecnd.net/onlinesupportmedia/onlinesupport/media/skype/documents/skype-private-conversation-whitepaper.pdf (дата звернення: 10.11.23).

42. E. Omara. 2020. Google Duo End-to-End Encryption Overview, https://www.gstatic.com/duo/papers/duo_e2ee.pdf (дата звернення: 10.11.23).

43. T. Perrin and M. Marlinspike. 2016. The double ratchet algorithm. GitHub wiki (2016). (дата звернення: 14.11.23).

44. Pidgin 2020. https://pidgin.im/. (дата звернення: 14.11.23).

45. M. Di Raimondo, R. Gennaro, and H. Krawczyk. 2005. Secure Offthe-Record Messaging. In Proceedings of the 2005 ACM Workshop on Privacy in the Electronic Society (WPES '05). Association for Computing Machinery, New York, NY, USA, 81-89. https://doi.org/10.1145/1102199.1102216

46. D. Schmidt. 2016. A security and privacy audit of KakaoTalk's end-to-end encryption. Master's thesis.

47. S. Schröder, M. Huber, D. Wind, and C. Rottermanner. 2016. When SIGNAL hits the Fan: On the Usability and Security of State-of-the-Art Secure Mobile Messaging. In European Workshop on Usable Security. IEEE. 1-7. https://doi.org/10.14722/eurousec.2016.23012 (дата звернення: 14.11.23).

48. M. Shirvanian and N. Saxena. 2014. Wiretapping via Mimicry: Short Voice Imitation Man-in-the-Middle Attacks on Crypto Phones. In Proceedings of the

2014 ACM SIGSAC Conference on Computer and Communications Security (CCS '14). Association for Computing Machinery, New York, NY, USA, 868-879. https://doi.org/10.1145/2660267.2660274

49. M. Shirvanian and N. Saxena. 2015. On the Security and Usability of Crypto Phones. In Proceedings of the 31st Annual Computer Security Applications Conference (ACSAC '15). Association for Computing Machinery, New York, NY, USA, 21-30. https://doi.org/10.1145/2818000.2818007

50. M. Shirvanian, N. Saxena, and J. J. George. 2017. On the Pitfalls of End-to-End Encrypted Communications: A Study of Remote Key-Fingerprint Verification. In Proceedings of the 33rd Annual Computer Security Applications Conference (ACSAC '17). Association for Computing Machinery, New York, NY, USA, 499-511. https://doi.org/10.1145/3134600.3134610

51. Signal 2022. https://signal.org/. (дата звернення: 14.11.23).

52. Signal. 2022. Technical information, from https://signal. org/docs/ (дата звернення: 10.11.23).

53. Silent Phone 2022. https://www.silentcircle.com/products-and-solutions/silentphone/. (дата звернення: 14.11.23).

54. Skype 2022. https://www.skype.com/en/. (дата звернення: 14.11.23).

55. R. Stedman, K. Yoshida, and I. Goldberg. 2008. A User Study of Off-theRecord Messaging. In Proceedings of the 4th Symposium on Usable Privacy and Security (SOUPS '08). Association for Computing Machinery, New York, NY, USA, 95-104. https://doi.org/10.1145/1408664.1408678

56. P. Szoldra. 2016. This is everything Edward Snowden revealed in one year of unprecedented top-secret leaks, https://www. businessinsider.com/snowden-leaks-timeline-2016-9 (дата звернення: 10.11.23).

57. J. Tan, L. Bauer, J. Bonneau, L. Faith Cranor, J. Thomas, and B. Ur. 2017. Can Unicorns Help Users Compare Crypto Key Fingerprints?. In Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems (CHI '17). Association

for Computing Machinery, New York, NY, USA, 3787-3798. https://doi.org/10.1145/3025453.3025733

58. Telegram 2022. https://telegram.org/. (дата звернення: 14.11.23).

59. Telegram. 2022. End-to-End Encryption, Secret Chats, https://core.telegram.org/api/end-to-end (дата звернення: 10.11.23).

60. Threema 2022. https://threema.ch/en. (дата звернення: 18.11.23).

61. Threema. 2022. Cryptography Whitepaper, https://threema.ch/press-files/2_documentation/cryptography_whitepaper.pdf (дата звернення: 10.11.23).

62. N. Unger, S. Dechand, J. Bonneau, S. Fahl, H. Perl, I. Goldberg, and M. Smith. 2015. SoK: Secure Messaging. In 2015 IEEE Symposium on Security and Privacy. IEEE, 232-249. https://doi.org/10.1109/SP.2015.22

63. Serge Vaudenay. 2005. Secure Communications over Insecure Channels Based on Short Authenticated Strings. In Annual International Cryptology Conference. Springer, 309-326. https://doi.org/10.1007/11535218_19

64. E. Vaziripour, J. Wu, M. O'Neill, R. Clinton, J. Whitehead, S. Heidbrink, K. Seamons, and D. Zappala. 2017. Is That You, Alice? A Usability Study of the Authentication Ceremony of Secure Messaging Applications. In Proceedings of the Thirteenth USENIX Conference on Usable Privacy and Security (SOUPS '17). USENIX Association, USA, 29-47.

65. S. R. Verschoor and Tanja Lange. 2016. (In-)Secure messaging with the Silent Circle instant messaging protocol. Cryptology ePrint Archive, Paper 2016/703. https://eprint.iacr.org/2016/703 (дата звернення: 18.11.23).

66. Viber 2022. https://www.viber.com/en/. (дата звернення: 18.11.23).

67. Rakuten Viber. 2022. Viber Encryption Overview. https://www.viber.com/app/uploads/viber-encryption-overview.pdf (дата звернення: 10.11.23).

68. WhatsApp. 2021. WhatsApp Encryption Overview. Technical white paper. https://scontent-iad3-1.xx.fbcdn.net/v/t39.8562-

6/326130579_868561330899040_2694856431949694281_n.pdf?_nc_cat=107&ccb=1-7&_nc_sid=ae5e01&_nc_ohc=GiHwGuhmURAAX_u-okb&_nc_ht= scontent-iad3-1.xx&oh=00_AfDBUqimHHncuLDOeqED0EJOAeSSwksocCWXdIkabxGPA&oe=63DDCC24 (дата звернення: 10.11.23).

69. WhatsApp 2022. https://www.whatsapp.com/. (дата звернення: 18.11.23).

70. Wickr 2022. https://wickr.com/. (дата звернення: 18.11.23).

71. Wire 2022. https://wire.com/en/. (дата звернення: 18.11.23).

72. R. Zhang, X. Wang, R. Farley, X. Yang, and X. Jiang. 2009. On the Feasibility of Launching the Man-in-the-Middle Attacks on VoIP from Remote Attackers. In Proceedings of the 4th International Symposium on Information, Computer, and Communications Security (ASIACCS '09). Association for Computing Machinery, New York, NY, USA, 61-69. https://doi.org/10.1145/ 1533057.1533069

73. Ph. Zimmermann, A. Johnston, and J. Callas. 2011. ZRTP: Media path key agreement for unicast secure RTP. Internet Engineering Task Force (IETF) (2011), 2070-1721.

74. Zoom 2022. https://zoom.us/. (дата звернення: 18.11.23).

75. Zoom. 2022. Zoom End-to-End Encryption Whitepaper, https://github.com/zoom/zoom-e2e-whitepaper (дата звернення: 10.11.23).

76. D. Frauchiger, R. Renner, and M. Troyer, arXiv, 1311.4547 (2013). (дата звернення: 18.11.23).

77. A. Acin and L. Masanes, Nature 540, 213 (2016). (дата звернення: 18.11.23).

78. S. Pironio, A. Acin, S. Massar, A. B. De La Giroday, D. N. Matsukevich, P. Maunz, S. Olmschenk, D. Hayes, L. Luo, T. A. Manning, and C. Monroe, Nature 464, 1021 (2010). (дата звернення: 18.11.23).

79. Y. Liu, X. Yuan, M.-H. Li, W. Zhang, Q. Zhao, J. Zhong, Y. Cao, Y.-H. Li, L.-K. Chen, H. Li, T. Peng, Y.-A. Chen, C.-Z. Peng, S.-C. Shi, Z. Wang, L. You,

X. Ma, J. Fan, Q. Zhang, and J.-W. Pan, Physical Review Letters 120, 010503 (2018). (дата звернення: 18.11.23).

80. P. Bierhorst, E. Knill, S. Glancy, Y. Zhang, A. Mink, S. Jordan, A. Rommal, Y. K. Liu, B. Christensen, S. W. Nam, M. J. Stevens, and L. K. Shalm, Nature 556, 223 (2018). (дата звернення: 18.11.23).

81. S. Pirandola, R. Laurenza, C. Ottaviani, and L. Banchi, Nature Communications 8, 15043 (2017). (дата звернення: 18.11.23).

82. C. Gabriel, C. Wittmann, D. Sych, R. Dong, W. Mauerer, U. L. Andersen, C. Marquardt, and G. Leuchs, Nature Photonics 4, 711 (2010). (дата звернення: 18.11.23).

83. M. Fuerst, H. Weier, S. Nauerth, D. G. Marangon, C. Kurtsiefer, and H. Weinfurter, Optics Express 18, 13029 (2010). (дата звернення: 18.11.23).

84. T. Symul, S. M. Assad, and P. K. Lam, Applied Physics Letters 98, 231103 (2011). (дата звернення: 18.11.23).

85. F. Xu, B. Qi, X. Ma, H. Xu, H. Zheng, and H.-K. Lo, Optics Express 20, 12366 (2012). (дата звернення: 18.11.23).

86. J. Y. Haw, S. M. Assad, A. M. Lance, N. H. Y. Ng, V. Sharma, P. K. Lam, and T. Symul, Physical Review Applied 3, 054004 (2015). (дата звернення: 18.11.23).

87. Y.-Q. Nie, L. Huang, Y. Liu, F. Payne, J. Zhang, and J.-W. Pan, Review of Scientific Instruments 86, 063105 (2015). (дата звернення: 18.11.23).

88. Y. Shi, B. Chng, and C. Kurtsiefer, Applied Physics Letters 109, 041101 (2016). (дата звернення: 18.11.23).

89. C. Abellan, W. Amaya, M. Jofre, M. Curty, A. Acin, J. Capmany, V. Pruneri, and M. W. Mitchell, Optics Express 22, 1645 (2014). (дата звернення: 18.11.23).

90. X.-G. Zhang, Y.-Q. Nie, H. Zhou, H. Liang, X. Ma, J. Zhang, and J.-W. Pan, Review of Scientific Instruments 87, 076102 (2016). (дата звернення: 18.11.23).

91. M. Avesani, D. G. Marangon, G. Vallone, and P. Villoresi, arXiv, 1801.04139 (2018). (дата звернення: 18.11.23).

92. M. W. Mitchell, C. Abellan, and W. Amaya, Physical Review A 91, 012314 (2015). (дата звернення: 18.11.23).

93. X. Zhang, Y. Q. Nie, H. Liang, and J. Zhang, IEEE-NPSS Real Time Conference, RT 2016, 1 (2016). (дата звернення: 18.11.23).

94. J. H. Shapiro, IEEE Journal of Quantum Electronics QE-21, 237 (1985). (дата звернення: 18.11.23).

95. C. Weedbrook, S. Pirandola, R. Garcaa-Patraon, N. J. Cerf, T. C. Ralph, J. H. Shapiro, and S. Lloyd, Reviews of Modern Physics 84, 621 (2012). (дата звернення: 18.11.23).

96. R. Renner, Security of Quantum Key Distribution, Ph.D. thesis, ETH Zürich (2005).

97. M. Tomamichel, C. Schaffner, A. Smith, and R. Renner, IEEE Transactions on Information Theory 57, 5524 (2011). (дата звернення: 18.11.23).

98. M. Tomamichel, A framework for non-asymptotic quantum information theory, Ph.D. thesis, ETH Zurich (2012).

99. R. M. Gray, Foundations and Trends in Communications and Information Theory 2, 155 (2006). (дата звернення: 18.11.23).

100. M. N. Wegman and J. L. Carter, Journal of Computer and System Sciences 22, 265 (1981). (дата звернення: 18.11.23).

101. R. G. Brown, "http://www.phy.duke.edu/ rgb/General/dieharder.php," (2018). (дата звернення: 18.11.23).

102. A. Rukhin, J. Soto, J. Nechvatal, M. Smid, E. Barker, S. Leigh, M. Levenson, M. Vangel, D. Banks, A. Heckert, J. Dray, and S. Vo, NIST Special Publication 800-22 (2001). (дата звернення: 19.11.23).

103. A. R. Dixon, Z. L. Yuan, J. F. Dynes, A. W. Sharpe, and A. J. Shields, Optics Express 16, 18790 (2008). (дата звернення: 19.11.23).

104. D. Huang, P. Huang, D. Lin, C. Wang, and G. Zeng, Optics Letters 40, 3695 (2015). (дата звернення: 19.11.23).

105. Here log stands for the logarithm in base 2 and ln for the natural logarithm. (дата звернення: 19.11.23).

106. L. Banchi, S. L. Braunstein, and S. Pirandola, Physical Review Letters 115, 260501 (2015). (дата звернення: 19.11.23).

107. K. P. Seshadreesan, L. Lami, and M. M. Wilde, Journal of Mathematical Physics 59, 072204 (2018). (дата звернення: 19.11.23).

108. C. Lupo, C. Ottaviani, P. Papanastasiou, and S. Pirandola, Physical Review A 97, 052327 (2018). (дата звернення: 19.11.23).

109. A. M. Ferrenberg, D. P. Landau, and Y. J. Wong, "Monte Carlo simulations: Hidden errors from "good" random number generators", Phys. Rev. Lett. 69, 3382 (1992). (дата звернення: 19.11.23).

110. R. Gennaro, "Randomness in cryptography", IEEE Secur. Priv. 4(2), 64-67 (2006).

111. N. Brunner, D. Cavalcanti, S. Pironio, V. Scarani, and S. Wehner, "Bell nonlocality", Rev. Mod. Phys. 86, 419 (2014). (дата звернення: 19.11.23).

112. N. Nisan, "Hardness vs. Randomness", J. Comput. Syst. Sci. 49, 149-167 (1994).

113. J. Bouda, M. Pivoluska, M. Plesch, and C. Wilmott, "Weak randomness seriously limits the security of quantum key distribution", Phys. Rev. A. 86(6), 062308 (2012). (дата звернення: 19.11.23).

114. N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography", Rev. Mod. Phys. 74, 145 (2002). (дата звернення: 19.11.23).

115. V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dusek, N. Lutkenhaus, and M. Peev, "The security of practical quantum key distribution", Rev. Mod. Phys. 81, 1301 (2009). (дата звернення: 19.11.23).

116. C. Weedbrook, S. Pirandola, R. Garcfa-Patron, N. J. Cerf, T. C. Ralph, J. H. Shapiro, and S. Lloyd, "Gaussian quantum information", Rev. Mod. Phys. 84, 621 (2012). (дата звернення: 19.11.23).

117. E. Diamanti, H. Lo, B. Qi, and Z. Yuan, "Practical challenges in quantum key distribution", npj Quantum Inf. 2, 16025 (2016). (дата звернення: 19.11.23).

118. Y. Zhang, Z. Li, Z. Chen, C. Weedbrook, Y. Zhao, X. Wang, C. Xu, X. Zhang, Z. Wang, M. Li, X. Zhang, Z. Zheng, B. Chu, X. Gao, N. Meng, W. Cai, Z. Wang, G. Wang, S. Yu, and H. Guo, "Continuous-variable QKD over 50km commercial fiber", arXiv:1709.04618 (2017). (дата звернення: 19.11.23).

119. X. Ma, X. Yuan, Z. Cao, B. Qi and Z. Zhang, "Quantum random number generation", npj Quantum Inf. 2, 16021 (2016). (дата звернення: 19.11.23).

120. M. Herrero-Collantes and J. C. Garcia-Escartin, "Quantum Random Number Generators", Rev. Mod. Phys. 89, 015004 (2017). (дата звернення: 19.11.23).

121. M. N. Bera, A. Acfn, M. Kus, M. W. Mitchell, and M. Lewenstein, "Randomness in Quantum Mechanics: Philosophy, Physics and Technology", Rep. Prog. Phys. 80, 124001 (2017). (дата звернення: 19.11.23).

122. T. Jennewein, U. Achleitner, G. Weihs, H. Weinfurter, and A. Zeilinger, "A fast and compact quantum random number generator," Rev. Sci. Instrum. 71, 1675 (2000). (дата звернення: 19.11.23).

123. A. Stefanov, N. Gisin, O. Guinnard, L. Guinnard, and H. Zbinden, "Optical quantum random number generator", J. Mod. Opt. 47, 595 (2000).

124. H. Ma, Y. Xie and L. Wu, "Random number generation based on the time of arrival of single photons", Appl. Opt. 44, 7760 (2005). (дата звернення: 19.11.23).

125. J. F. Dynes, Z. Yuan, A. W. Sharpe, and A. J. Shields, "A high speed, postprocessing free, quantum random number generator", Appl. Phys. Lett. 93(3), 031109 (2008). (дата звернення: 19.11.23).

126. M. Wayne, E. Jeffrey, G. Akselrod, and P. Kwiat, "Photon arrival time quantum random number generation", J. Mod. Opt. 56, 516-522 (2009).

127. M. Wahl, M. Leifgen, M. Berlin, T. Rohlicke, H. Rahn and O. Benson, "An ultrafast quantum random number generator with provably bounded output bias based on photon arrival time measurements", Appl. Phys. Lett. 98, 171105 (2011). (дата звернення: 19.11.23).

128. Y. Nie, H. Zhang, Z. Zhang, J. Wang, X. Ma, J. Zhang, and J. Pan, "Practical and fast quantum random number generation based on photon arrival time relative to external reference", Appl. Phys. Lett. 104, 051110 (2014). (дата звернення: 19.11.23).

129. W. Wei and H. Guo, "Bias-free true random-number generator", Opt. Lett. 34, 1876 (2009). (дата звернення: 19.11.23).

130. H. Fürst, H. Weier, S. Nauerth, D. G. Marangon, C. Kurtsiefer, and H. Weinfurter, "High speed optical quantum random number generation," Opt. Express 18, 13029-13037 (2010).

131. M. Ren, E Wu, Y. Liang, Y. Jian, G. Wu, and H. Zeng, "Quantum random-number generator based on a photon-number-resolving detector", Phys. Rev. A. 83, 023820 (2011). (дата звернення: 19.11.23).

132. Q. Yan, B. Zhao Q. Liao, and N. Zhou, "Multi-bit quantum random number generation by measuring positions of arrival photons", Rev. Sci. Instrum. 85, 103116 (2014). (дата звернення: 19.11.23).

133. M. J. Applegate, O. Thomas, J. F. Dynes, Z. Yuan, D. A. Ritchie, and A. J. Shields, "Efficient and robust quantum random number generation by photon number detection", Appl. Phys. Lett. 107, 071106 (2015). (дата звернення: 19.11.23).

134. C. Gabriel, C. Wittmann, D. Sych, R. F. Dong, W. Mauerer, U. L. Andersen, C. Marquardt, and G. Leuchs, "A generator for unique quantum random numbers based on vacuum states", Nat. Photonics 4, 711 (2010). (дата звернення: 19.11.23).

135. Y. Shen, L. Tian, and H. Zou, "Practical quantum random number generator based on measuring the shot noise of vacuum states", Phys. Rev. A 81, 063814 (2010). (дата звернення: 19.11.23).

136. T. Symul, S. M. Assad, and P. K. Lam, "Real time demonstration of high bitrate quantum random number generation with coherent laser light", Appl. Phys. Lett. 98, 231103 (2011). (дата звернення: 19.11.23).

137. J. Y. Haw, S. M. Assad, A. M. Lance, N. H. Y. Ng, V. Sharma, P. K. Lam, and T. Symul, "Maximization of Extractable Randomness in a Quantum Random Number Generator", Phys. Rev. Appl. 3, 054004 (2015). (дата звернення: 19.11.23).

138. B. Xu, Z. Li, J. Yang, S. Wei, Q. Su, W. Huang, Y. Zhang, and H. Guo, "High Speed Continuous Variable Source-Independent Quantum Random Number Generation", Quantum Sci. Technol. 4, 025013 (2019). (дата звернення: 19.11.23).

139. Q. Zhou, R. Valivarthi, C. John, and W. Tittel, "Practical quantum random number generator based on sampling vacuum fluctuations", arXiv:1703.00559 (2017). (дата звернення: 19.11.23).

140. F. Raffaelli, G. Ferranti, D. H Mahler, P. Sibson, J. E. Kennard, A. Santamato, G. Sinclair, D. Bonneau, M. G Thompson, and J. C F Matthews, "A homodyne detector integrated onto a photonic chip for measuring quantum states and generating random numbers", Quantum Sci. Technol. 3, 025003 (2018). (дата звернення: 19.11.23).

141. B. Qi, Y. Chi, H. Lo, and L. Qian, "High-speed quantum random number generation by measuring phase noise of a single-mode laser", Opt. Lett. 35, 312-314 (2010).

142. H. Guo, W. Tang, Y. Liu, and W. Wei, "Truly random number generation based on measurement of phase noise of a laser", Phys. Rev. E 81, 051137 (2010). (дата звернення: 19.11.23).

143. F. Xu, B. Qi, X. Ma, H. Xu, H. Zheng, and H. Lo "Ultrafast quantum random number generation based on quantum phase luctuations", Opt. Express 20, 12366 (2012). (дата звернення: 19.11.23).

144. C. Abellán, W. Amaya, M. Jofre, M. Curty, A. Acín, J. Capmany, V. Pruneri, and M. W. Mitchell, "Ultra-fast quantum randomness generation by accelerated phase diffusion in a pulsed laser diode," Opt. Express 22, 1645-1654 (2014).

145. Y. Nie, L. Huang, Y. Liu, F. Payne, J. Zhang, and J. Pan, "The generation of 68 Gbps quantum random number by measuring laser phase fluctuations", Rev. Sci. Instrum. 86, 063105 (2015). (дата звернення: 19.11.23).

146. J. Yang, J. Liu, Q. Su, Z. Li, F. Fan, B. Xu, and H. Guo, "5.4 Gbps real time quantum random number generator with compact implementation", Opt. Express 24, 27475 (2016). 39X. Zhang, Y. Nie, H. Zhou, H. Liang, X. Ma, J. Zhang, and J. Pan, "Fully integrated 3.2 Gbps quantum random number generator with real-time extraction", Rev. Sci. Instrum. 87, 076102 (2016). (дата звернення: 19.11.23).

147. J. Liu, J. Yang, Q. Su, Z. Li, F. Fan, B. Xu, and H. Guo, "117 Gbits/s quantum random number generation with simple structure", IEEE Photon. Technol. Lett. 29, 1109 (2017). (дата звернення: 19.11.23).

148. C. R. S. Williams, J. C. Salevan, X. Li, R. Roy, and T. E. Murphy, "Fast physical random number generator using amplified spontaneous emission", Opt. Express 18, 23584 (2010). (дата звернення: 19.11.23).

149. X. Li, A. B. Cohen, T. E. Murphy, and R. Roy, "Scalable parallel physical random number generator based on a superluminescent LED", Opt. Lett. 36, 1020 (2011). (дата звернення: 19.11.23).

150. W. Wei, G. Xie, A. Dang, and H. Guo, "High-speed and bias-free optical random number generator", IEEE Photon. Technol. Lett. 24, 437 (2012). (дата звернення: 19.11.23).

151. Y. Liu, M. Zhu, B. Luo, J. Zhang, and H. Guo, "Implementation of 1.6 Tbs-1 truly random number generation based on a super-luminescent emitting diode", Laser Phys. Lett. 10, 045001 (2013). (дата звернення: 19.11.23).

152. B. Qi, "True randomness from an incoherent source," Rev. Sci. Instrum. 88, 113101 (2017). (дата звернення: 19.11.23).

153. A. Martin, B. Sanguinetti, C. C. W. Lim, R. Houlmann, and H. Zbinden, "Quantum random number generation for 1.25-GHz quantum key distribution systems", J. Lightwave Technol. 33, 2855 (2015). (дата звернення: 19.11.23).

154. R. Impagliazzo, L. A. Levin, and M. Luby, "Pseudo-random generation from one-way functions", in Proceedings of the 21st Annual ACM Symposium Theory of Computing (STOC) (ACM, 1989), pp.12-24.

155. Y. Mansour, N. Nisan, and P. Tiwari, "The computational complexity of universal hashing", in Proceedings of the 22nd Annual ACM Symposium Theory Computing (STOC) (ACM, 1990), pp. 235-243.

156. X. Ma, F. Xu, H. Xu, X. Tan, B. Qi, and H. Lo, "Postprocessing for quantum random-number generators: Entropy evaluation and randomness extraction", Phys. Rev. A 87, 062327 (2013). (дата звернення: 19.11.23).

157. X. Wang, Y. Zhang, S. Yu, and H. Guo, "High-Speed Implementation of Length-Compatible Privacy Amplification in Continuous-Variable Quantum Key Distribution", IEEE Photonics Journal, 10(3), 7600309 (2018). (дата звернення: 19.11.23).

158. X. Zhang, Y. Zhang, Z. Li, S. Yu and H. Guo, "1.2-GHz Balanced Homodyne Detector for Continuous-Variable Quantum Information Technology", IEEE Photonics Journal, 10(5), 6803810 (2018). (дата звернення: 19.11.23).

159. H. Zhou, P. Zeng, M. Razavi, and X. Ma, "Randomness quantiication of coherent detection", Phys. Rev. A 98, 042321 (2018). (дата звернення: 19.11.23).

ДОДАТОК А

А.1 Додаткові програми E2EE, що використовують протокол сигналу

А.1.1 Google Meet

Це програма, розроблена Google для відеозустрічі та дзвінків [20]. Google оновив додаток Google Duo та об’єднав його з додатком Google Meet, щоб включити відеодзвінки та зустрічі в один додаток. Таким чином, програма Google Meet стверджує, що надає функцію E2EE під час відеодзвінків один на один і групових за допомогою наскрізного шифрування Google Duo [42]. Додаток Google Meet використовує протокол Signal для реалізації протоколу E2EE. Він використовує режим E2EE за замовчуванням для всіх голосових і відеоповідомлень і дзвінків у всіх розмовах один на один і групових розмовах. Під час дзвінків один на один програма Google Meet використовує WebRTC, який підтримує E2EE для індивідуальних дзвінків із використанням DTLS-SRTP. Безпека транспортного рівня дейтаграм (DTLS) використовується для встановлення безпечного з’єднання між двома учасниками виклику, тоді як SRTP використовується для забезпечення зашифрованих медіа-потоків у реальному часі. З іншого боку, зустрічі в додатку Google Meet не шифруються наскрізно. Замість E2EE програма Google Meet використовує хмарне шифрування для своїх зустрічей.

А.1.2 Повідомлення від Google

Це програма, розроблена Google для надсилання повідомлень за допомогою служби коротких повідомлень (SMS)/служби обміну мультимедійними повідомленнями (MMS) і чату за допомогою RCS [40]. Google надає служби чату RCS через програму Android Messages. Нещодавно Google почав розгортати функцію E2EE для RCS у програмі Android Messages [3]. Додаток Google Messages використовує протокол Signal для реалізації функції

E2EE для повідомлень RCS [19]. Тільки Google пропонуючи функцію E2EE в чатах один на один за умовчанням, якщо обидва учасники розмови використовують програму Google Messages. Однак, щоб скористатися функцією E2EE у програмі Google Messages, і відправник, і одержувач повинні використовувати програму Google Messages на своїх телефонах, увімкнути функції чату та використовувати дані або Wi-Fi для повідомлень RCS.

A.1.3 Skype

Це додаток для обміну миттєвими повідомленнями [54]. Використовуючи протокол Signal, він реалізує функцію E2EE як додаткову властивість [41]. Тому за замовчуванням усі повідомлення та дзвінки Skype не є E2EE. Користувачі можуть захистити свої аудіодзвінки або повідомлення, увімкнувши відповідну опцію *Приватна розмова*, який підтримує схему E2EE на основі протоколу Signal. Цей параметр підтримує лише функцію E2EE у чатах і аудіодзвінках між двома користувачами. Немає захисту E2EE ні для відеодзвінка, ні для групового сценарію. Під час аудіодзвінків один на один програма Skype використовує наявний *Приватна розмова* сеансу між двома користувачами для створення ключа шифрування та ініціювання аудіовиклику E2EE. Після налаштування аудіовиклику E2EE медіа-пакети шифруються за допомогою SRTP за допомогою попередньо згенерованого ключа шифрування.

A.2 Додаткові програми E2EE, що використовують власні протоколи

A.2.1 Element.

Додаток для обміну миттєвими повідомленнями та незалежний комунікаційний система підключення через Matrix [11]. Програма Element побудована на основі протоколу Matrix і використовує шифрування, реалізоване у відкритому стандарті Matrix [38]. У всіх індивідуальних і групових чатах і дзвінках програма Element використовує бібліотеку шифрування Olm, яка

базується на протоколі Double Ratchet, популяризованому Signal, для реалізації функції E2EE за замовчуванням.

A.2.2 FaceTime

Це сервіс відео- та аудіодзвінків, розроблений компанією Apple [15]. Компанія Apple стверджує, що аудіо- та відеоконтент викликів FaceTime за замовчуванням шифрується E2EE у всіх індивідуальних і групових сценаріях. FaceTime використовує службу Apple Push Notification (APN) для встановлення першої точки підключення до зареєстрованих пристроїв користувача [25]. Ця перша точка підключення здійснюється через інфраструктуру сервера Apple, яка передає пакети даних між зареєстрованими пристроями користувачів. Зареєстровані пристрої користувачів перевіряють їх ідентифікаційні сертифікати та встановлюють спільний секрет для кожного сеансу за допомогою APN і утиліт проходження сеансу для повідомлень NAT (STUN) через ретрансляційне з'єднання. За допомогою SRTP спільний секрет використовується для отримання ключів сеансу для потокових медіаканалів.

A.2.3 KakaoTalk

Це програма для обміну миттєвими повідомленнями, створена компанією Kakao у Південній Кореї [27]. Це дозволяє користувачам реалізувати функціональні можливості E2EE як функцію вибору. Таким чином, програма KakaoTalk не вмикає функцію E2EE за замовчуванням, і користувачі повинні вибрати відповідну опцію*Секретний чат*спілкуватися в режимі E2EE. Функцію E2EE було додано до програми KakaoTalk на додаток до протоколу обміну повідомленнями LOCO [46]. Протокол обміну повідомленнями LOCO E2EE використовує захист транспортного рівня (TLS), центральний сервер каталогу відкритих ключів, алгоритм шифрування AES і пару ключів RSA. При використанні *Секретний чат* усі повідомлення E2EE в кімнатах чату один на один і групових чатів. Однак аудіо- та відеодзвінки недоступні під час використання *Секретний чат* функція.

А.2.4 LINE. Це програма для обміну миттєвими повідомленнями, популярна у Східній Азії [32]. Він реалізує функціональні можливості E2EE за замовчуванням під назвою функції безпеки *Запечатування* листів[8]. Тому *Запечатування листів* Ця функція ввімкнена за умовчанням для всіх текстових повідомлень, інформації про місцезнаходження, голосових і відеодзвінків між двома користувачами в сценаріях «один на один». Однак лише текстові повідомлення та інформація про місцезнаходження за замовчуванням є E2EE у групових чатах. Програма LINE не підтримує голосові або відеодзвінки E2EE у групових сценаріях. Щоб реалізувати функцію E2EE, програма LINE використовує протокол еліптичної кривої Діффі-Хеллмана (ECDH) через Curve25519 і AES-256 у режимі GCM. Однак у голосових і відеодзвінках «один на один» програма LINE використовує криву secp256r1 для протоколу шифрування, AES для симетричного шифрування та HKDF для отримання симетричних ключів.

А.2.5 Linphone

Це програма для аудіо- та відеодзвінків, яка підтримує миттєві повідомлення [33]. Він реалізує функціональність E2EE як функцію вибору для особистих і групових повідомлень, а також для аудіо- та відеодзвінків. Щоб реалізувати E2EE у функціях індивідуальних і групових миттєвих повідомлень, програма Linphone використовує власний протокол E2EE, який називається шифруванням миттєвих повідомлень Linphone (LIME) [34]. Цей протокол LIME натхненний протоколом Signal, що дозволяє користувачам надсилати й отримувати повідомлення приватно й асинхронно. З іншого боку, програма Linphone реалізує функцію E2EE для індивідуальних аудіо- та відеодзвінків за допомогою ZRTP і SRTP-DTLS, які сумісні з WebRTC. Однак функція E2EE недоступна для голосових або відеодзвінків у групових сценаріях.

А.2.6 Повідомлення від Apple

Це програма для обміну миттєвими повідомленнями, розроблена компанією Apple для надсилання повідомлень за допомогою iMessage та SMS/MMS [39]. Програма Apple Messages використовує протокол iMessage для реалізації функції E2EE за замовчуванням у всіх індивідуальних і групових сценаріях [24]. Після ввімкнення iMessage на пристрої пристрій генерує пари ключів шифрування та підпису для використання зі службою. Протокол Apple iMessage використовує 1280-бітний ключ шифрування RSA та 256-бітний ключ шифрування EC на кривій NIST P-256 для шифрування, тоді як з алгоритмом цифрового підпису еліптичної кривої (ECDSA) використовуються 256-бітні ключі підпису за підписи. Він також використовує Apple Identity Service (IDS) для зберігання відкритих ключів і підтримки відповідності між ними та номером телефону або адресою електронної пошти користувача, а також адресою APN пристрою, тоді як приватні ключі зберігаються в брелоку пристрою. Потім APN використовуються для доставки зашифрованого тексту повідомлення, ключа зашифрованого повідомлення та цифрового підпису відправника.

А.2.7 Беззвучний телефон

Це додаток для обміну миттєвими повідомленнями, розроблений Silent Circle [53]. Він стверджує, що всі повідомлення та дзвінки E2EE за замовчуванням у всіх індивідуальних і групових сценаріях. Він використовує власний протокол, заснований на протоколі Signal, для реалізації E2EE у функціях IM [65]. З іншого боку, ZRTP використовується для реалізації функції E2EE в аудіо- та відеодзвінках [73] ZRTP використовує обмін ключами Діффі-Хеллмана та SRTP для встановлення спільного ключа сеансу та шифрування даних.

А.2.8 Treema

Це програма для обміну миттєвими повідомленнями, яка також дозволяє користувачам здійснювати голосові та відеодзвінки [60]. Він стверджує, що всі

повідомлення та дзвінки E2EE за замовчуванням у всіх індивідуальних і групових сценаріях. Він використовує власний протокол для реалізації функції E2EE у повідомленнях і дзвінках [61]. Коли програма Threema встановлена на телефоні користувача, вона генерує для кожного користувача унікальну асиметричну пару ключів, що складається з відкритого та закритого ключів на основі еліптичних крива криптографія. Додаток Threema використовує протокол ECDH для створення спільного секрету. Потім він використовує потоковий шифр XSalsa20 для шифрування відкритого тексту, тоді як код автентифікації повідомлення (MAC) обчислюється за допомогою Poly1305-AES. У викликах Threema WebRTC використовується для встановлення безпечного однорангового (P2P) з'єднання. Аудіопотік шифрується за протоколом SRTP, а обмін ключами здійснюється за протоколом DTLS-SRTP.

A.2.9 WickrWickr [70] розробив додаток Wickr Me та Wickr Pro для індивідуального та бізнес-використання відповідно. Щоб забезпечити функцію E2EE, Wickr використовує власний протокол під назвою протокол безпечного обміну повідомленнями Wickr, який базується на стандартних криптографічних примітивах [23]. Він використовує обмін ключами ECDH з парами ключів P521, ECDSA з парами ключів P521, AES 256 у режимі GCM і KDF. Усі повідомлення та аудіо/відеодзвінки за замовчуванням є E2EE у всіх індивідуальних і групових сценаріях. Коли Wickr генерує ключі для користувачів та їхніх перших пристроїв, він зберігає відкриті ключі та кореневі ідентифікатори на серверах Wickr.

A.2.10 Wire

Це додаток для обміну миттєвими повідомленнями, створений компанією Wire Swiss GmbH [71]. Він стверджує, що всі повідомлення та дзвінки E2EE за замовчуванням у всіх індивідуальних і групових сценаріях. Wire використовує протокол Proteus для реалізації функції E2EE, яка копіює деякі функції протоколу Signal [18]. Однак протокол Proteus був налаштований як незалежна реалізація протоколу Signal. Протокол Proteus використовує такі криптографічні примітиви:

потоковий шифр ChaCha20, HMAC-SHA256 як MAC, обмін ключами ECDH і HKDF для отримання ключів. Під час проводових викликів медіа-сеанс виклику шифрується протоколом SRTP, тоді як рукостискання DTLS використовується для узгодження алгоритму шифрування SRTP, ключів і параметрів. Щойно клієнт генерує матеріал ключа, клієнт завантажує попередні ключі разом зі своїм відкритим ідентифікаційним ключем на сервер Wire, який може використовуватися іншими клієнтами для асинхронного ініціювання розмови E2EE.

А.3 Додаткові таблиці та рисунки

Таблиця А.3 – Рейтинг програм із наскрізним шифруванням і огляди в Google Play Store

Застосунок	Встановлюється на Google Play	Рейтинг	Відгуки
WhatsApp	5000000000+	4,3	172000000
Facebook Messenger	5000000000+	4,1	85900000
Google Meet	5000000000+	4,6	9810000
Viber	1000000000+	4,5	16200000
Телеграма	1000000000+	4,3	11800000

Продовження таблиці А.3 – Рейтинг програм із наскрізним шифруванням і огляди в Google Play Store

Skype	1000000000+	4,1	11500000
Повідомлення від Google	1000000000+	4,2	9150000
LINE	500000000+	4,1	13700000
Zoom	500000000+	4,2	3980000
KakaoTalk	100000000+	4,3	3160000
Signal	100000000+	4,4	2190000
Wickr Me	10000000+	4,8	89000
Threema	1000000+	4,1	70800
Wire	1000000+	2,9	35100
Linphone	500000+	3,8	5350
Element	500000+	4,1	4570
Silent Phone	500000+	3,8	1830

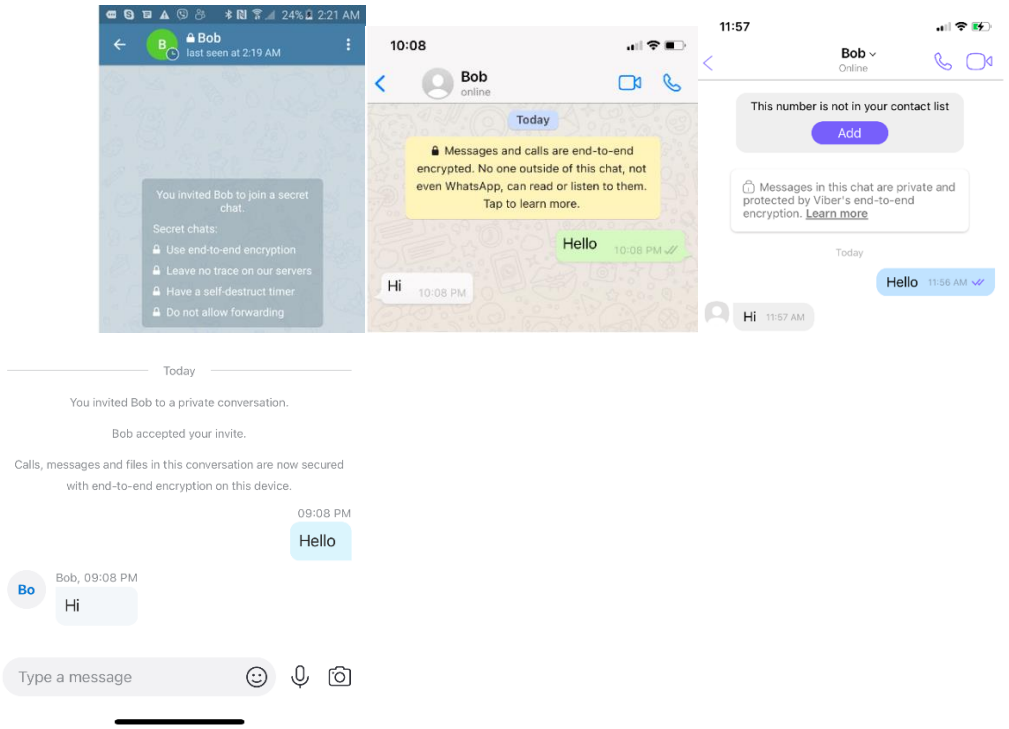

Рисунок А.1 – Сповіщення користувачів про те, що оппортуністичний режим E2EE увімкнено, а їхні повідомлення наскрізно шифруються за допомогою різних індикаторів, таких як спеціальні сповіщення та значки замка.

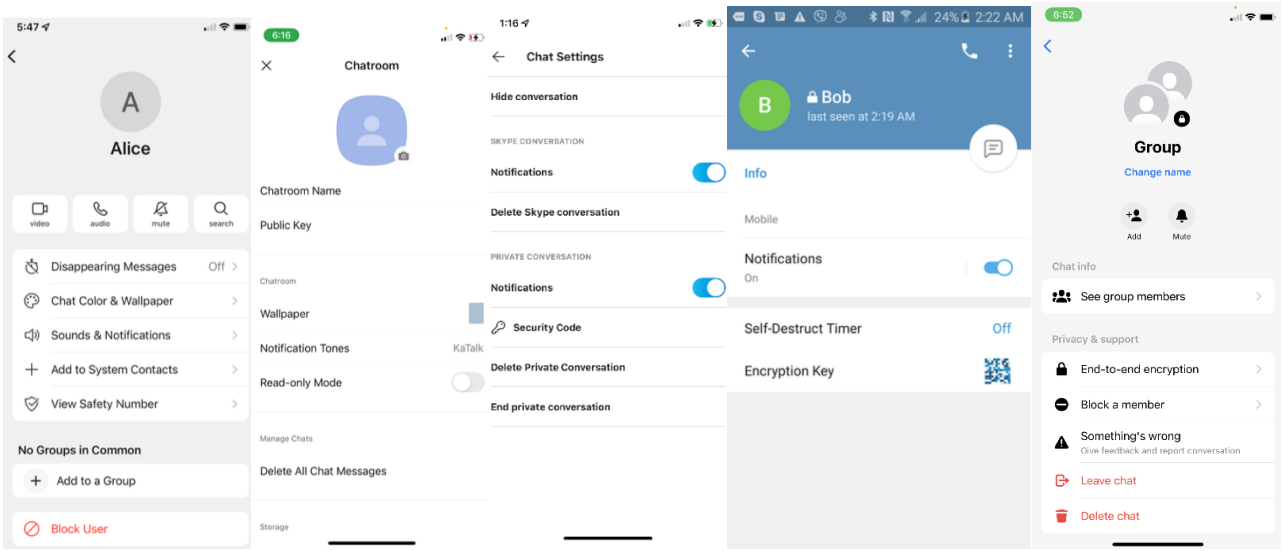

Рисунок А.2 – Деякі програми E2EE посилаються на церемонію автентифікації, використовуючи наведену вище термінологію.

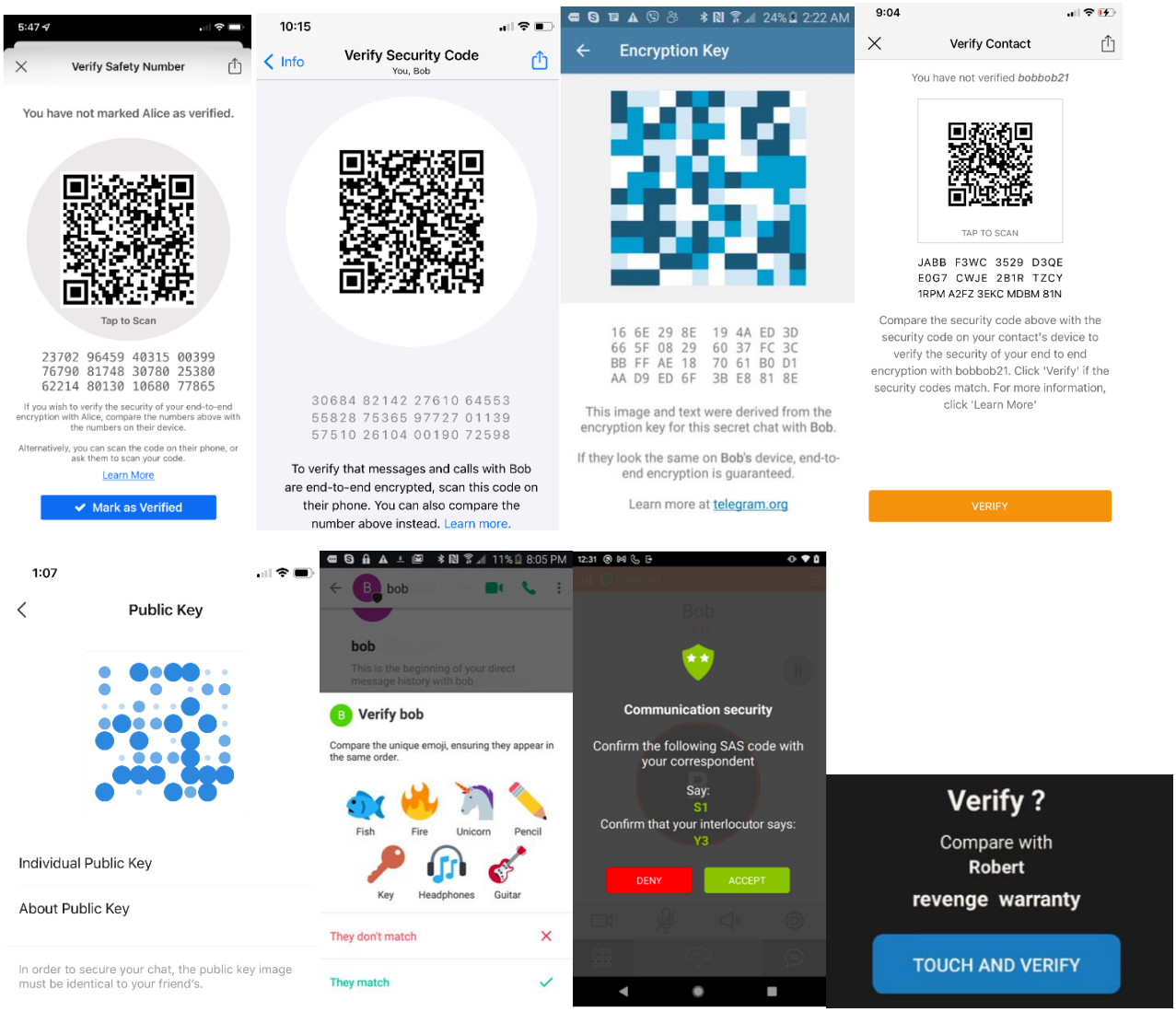

Рисунок А.3 – Представлення відбитків пальців у програмах E2EE

ДОДАТОК Б

Власна публікація (стаття в фаховому журналі категорії Б)

MINISTRY OF EDUCATION AND SCIENCE OF UKRAINE

KHARKIV NATIONAL
UNIVERSITY OF RADIO ELECTRONICS

RADIOTEKHNIKA

All-Ukrainian
interdepartmental scientific and technical collection

ISSN 0485-8972
eISSN 2786-5525

Founded in 1965

ISSUE 209

Kharkiv
Kharkiv National
University of Radio Electronics
2022

UDC 621.3

The collection is included in the List of scientific professional publications of Ukraine, category «Б», technical and physical-mathematical sciences (approved by orders of the Ministry of Education and Science from 17.03.2020 № 409; from 02.07.2020 № 886; from 24.09.2020 № 1188) by specialties: 171 – Electronics; 172 – Telecommunications and Radio Engineering; 173 – Avionics; 125 – Cybersecurity; 151 – Automation and Computer-Integrated Technologies; 152 – Metrology and Information-Measuring Equipment; 153 – Micro- and Nanosystem Technology; 163 – Biomedical Engineering; 105 – Applied Physics and Nanomaterials.

Website: rt.nure.ua

Registration certificate KV № 12098-969 PR dated 14. 12. 2006.

The authors are responsible for the content of the article.

Responsible for the issue: *I.V. Svyd, PhD, Assoc. prof., I.D. Gorbenko, Dr. Sc. (Tech.), prof.*
Technical Secretary: *O.S. Polyakova.*

Recommended by the Scientific and Technical Council of Kharkiv National University of Radio Electronics, protocol № 5 від 24.06.2022.

Address of the editorial board: Kharkiv National University of Radio Electronics (NURE), ave. Nauky, 14, Kharkiv, 61166, tel. (0572) 7021-397.

Journal "Radiotekhnika" is included in the Catalog of subscription editions of Ukraine, subscription index **08391**.

УДК 621.3

Збірник включено до Переліку наукових фахових видань України, категорія "Б", технічні та фізико-математичні науки (затверджено наказами МОНУ від 17.03.2020 № 409; від 02.07.2020 № 886; від 24.09.2020 № 1188) за спеціальностями: 171 – Електроніка; 172 – Телекомунікації та радіотехніка; 173 – Авіоніка; 125 – Кібербезпека; 151 – Автоматизація та комп'ютерно-інтегровані технології; 152 – Метрологія та інформаційно-вимірювальна техніка; 153 – Мікро- та наносистемна техніка; 163 – Біомедична інженерія; 105 – Прикладна фізика та наноматеріали.

Сайт: rt.nure.ua

Реєстраційне свідоцтво КВ № 12098-969 ПР від 14. 12. 2006.

За зміст статті відповідальні автори.

Відповідальні за випуск: *І.В. Свид, канд. техн. наук, доц., І.Д. Горбенко, д-р техн. наук, проф.*
Технічний секретар: *О.С. Полякова.*

Рекомендовано Науково-технічною радою Харківського національного університету радіоелектроніки, протокол № 5 від 24.06.2022.

Адреса редакційної колегії: Харківський національний університет радіоелектроніки (ХНУРЕ), просп. Науки, 14, Харків, 61166, тел. (0572) 7021-397.

Збірник «Радіотехніка» включено до Каталогу передплатних видань України, передплатний індекс **08391**.

CONTENT

ЗМІСТ

УДК 681.3.06 **DOI:10.30837/rt.2022.2.209.12**

І.Д. ГОРБЕНКО, д-р техн. наук, О.А. ЗАМУЛА, д-р техн. наук, Ю.С. ОСИПЕНКО

КОНЦЕПЦІЯ ОЦІНКИ РИЗИКІВ КІБЕРБЕЗПЕКИ ІНФОРМАЦІЙНОЇ СИСТЕМИ ОБ'ЄКТА КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Вступ

Вважається, що основним підходом до забезпечення кібер- і інформаційної безпеки інформаційної системи є стратегія захисту на основі ризику [1]. Одним з головних завдань управління інформаційними ризиками є об'єктивно ідентифікувати і оцінити найбільш значущі для об'єкта критичної інфраструктури ризики. В [2] визначені критерії підходів до вибору методів оцінки і управління ризиками безпеки. Саме тому, на наш погляд, актуальним є пошук методів оцінки і управління ризиками безпеки, які в певній мірі відповідають визначеним критеріям. У цьому дослідженні використано один з відомих підходів до моделювання, – «дерево атак» [3]. Метод «дерева атак» є систематичним методом визначення характеристик безпеки системи на основі всіх атак, яким піддається інформаційна система. Виявлення всіх можливих атак полегшує аналіз можливих шляхів реалізації кібератак та вибір адекватних контрзаходів і їх оптимальне використання. Дерево атаки складається з вузлів, ребер та з'єднувальних елементів, де кожен вузол відповідає кроку атаки. Кореневий вузол є кінцевою метою зловмисника, а дочірні вузли даного вузла представляють підцілі. Ребра представляють зміну стану, спричинену діями зловмисника. З'єднувальний елемент – це шлях для просування до мети атаки: АБО (диз'юнктивне), чи І (кон'юнктивне) для вузлів із двома або більше дочірніми елементами.

Основні результати досліджень

Архітектура інформаційної системи

Інформаційна система компанії, відповідно до її компонентів, може бути розділена на дві частини: компоненти, які доступні користувачеві (наприклад, термінал), і компоненти, які доступні тільки постачальнику послуг, такі як сервер центрального офісу компанії. Можливі сценарії загроз безпеки, засновані на потоці інформації через зазначені компоненти, наведені нижче [4, 5] (рис. 1):

1) Поширення шкідливого коду у обладнанні, порушення бар'єру безпеки, доступ до конфіденційної інформації користувача та отримання доступу до основного сервера через сенсорний пристрій.

2) Виток інформації або підробка даних у процесі передачі даних.

3) Виявлення (вимірювання) ризиків витоку даних через вразливості у персональному комп'ютері (ПК), смарт-пристрої чи шлюзі, який використовується для передачі даних сховищем або персоналом.

4) Ризики кібератак через вразливість основного сервера та репозиторію в зоні дії провайдера.

Виявлення та ідентифікація загроз інформаційної системи компанії

Для того щоб виявити загрози, що можуть бути використані для побудови дерева атак інформаційної системи компанії, доцільно обрати типові та засновані на відповідних сценаріях загрози безпеки відповідно до ISO/IEC 27005 [6, 7]. Нарешті, щоб визначити вразливості інформаційної системи компанії, доцільно структурувати використані загрози, щоб зробити їх придатними для середовища інформаційної системи компанії відповідно до ISO/IEC 27005. Отримані дані використовувалися як компоненти дерева атак інформаційної системи компанії. Відповідно до архітектури системи, виявлених загроз безпеки та уразливостей, пропонується виділити сім областей загроз безпеці інформаційної системи компанії (рис. 2).

Рис. 1. Архітектура інформаційної системи компанії

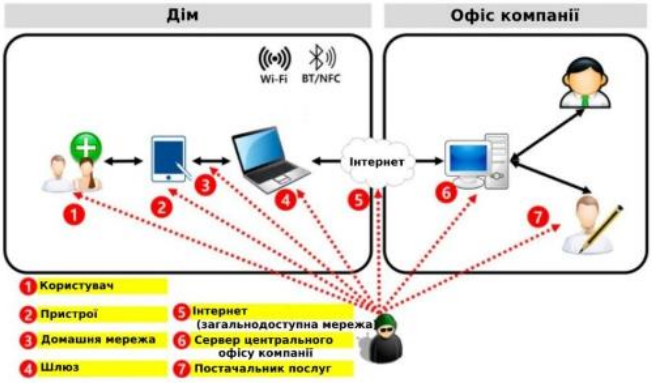

Рис. 2. Області, що пов'язані із загрозами безпеки

Варіанти використання областей загроз безпеки інформаційної системи

З а г р о з а 1 : Користувач

При використанні користувачами терміналів часто виникають загрози безпеці, що пов'язані з помилками використання пристроїв, слабкими паролями, втратою пристроїв, фішингом тощо.

З а г р о з а 2 : Пристрої

Термінали засновані або на операційній системі загального призначення (GPOS) або на вбудованій операційній системі реального часу (RTOS). Пристрої на базі RTOS захищені від несанкціонованого доступу, оскільки вони оптимізовані для конкретних функцій на етапах проектування та виробництва. І навпаки, пристрої на основі GPOS, такі як смартфони, вразливі для загроз безпеки, оскільки вони використовують зовнішні програми. Використання терміналів у таких умовах робить їх вразливими для загроз безпеки через функції збереження та обміну даними цих пристроїв, а також ризик втрати/крадіжки пристрою, уразливості додатків та передачі відкритого тексту.

З а г р о з а 3 : Домашня мережа (мережа філіалу компанії)

Передача інформації між терміналом в особистому просторі користувача (вдома або в офісі) та до серверу центрального офісу компанії відбувається переважно бездротовою мережею. Як показано на рис. 3, типи мереж, що використовуються в домашніх умовах, включають LAN (локальна обчислювальна мережа), Wi-Fi, Bluetooth, NFC (комунікація ближнього радіусу дії) та мережі довгострокової еволюції. У той час як деякі пристрої вбудованого типу повинні бути підключені до локальних мереж, інтелектуальні пристрої на основі GPOS можуть зв'язуватися із сервером центрального офісу компанії. У таких умовах сервісні

системи на базі домашніх мереж піддаються загрозам безпеці, пов'язаним із наскрізною передачею відкритого тексту та атаками посередника (MITM-атаками) (рис. 3) [8].

З а г р о з а 4 : Шлюз, наприклад, VPN

Шлюз відіграє роль посередника між користувачем та сервером центрального офісу компанії, піддаючи систему загрозам безпеці, пов'язаними з шахрайськими шлюзами, а також втратою/крадіжкою шлюзів та MITM атаками [8].

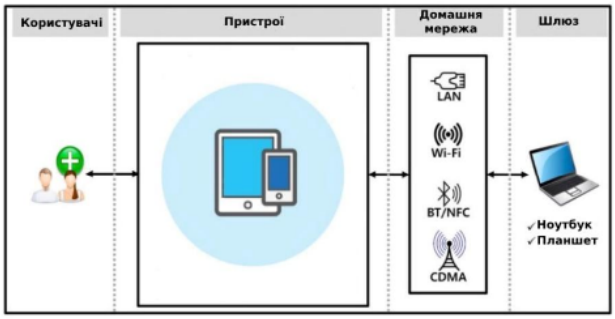

Рис. 3. Домашня мережа

З а г р о з а 5 : Інтернет (загальнодоступна мережа)

Зв'язок між користувачем та сервером центрального офісу компанії відбувається через мережу загального користування (Інтернет). Оскільки особиста інформація передається через загальнодоступний Інтернет, важливо встановити наскрізні правила безпеки. Крім того, потрібна зашифрована передача даних. У таких умовах інформаційна система компанії вразлива для загроз безпеки, пов'язаних з перехопленням даних, підробкою/зміною та підвищенням привілеїв [8].

З а г р о з а 6 : Сервер центрального офісу компанії

Сервер центрального офісу компанії знаходиться у місці розташування постачальника послуг. Він складається з ПК та програмного забезпечення, необхідного для віддалених консультацій, а його користувачами є персонал та системні адміністратори (співробітник служби безпеки та інший допоміжний персонал). Ця система дуже важлива, тому що вона опрацьовує всі дані користувачів. Крім того, якщо сервер центрального офісу компанії підключений до відповідних установ через урядовий мережевий концентратор, необхідні суворі правила безпеки для запобігання проникненню в державну систему. У таких умовах інформаційна система компанії може піддаватися загрозам безпеки, пов'язаним з MITM-атаками, шкідливим кодом, підробкою/зміною застосунків та незаконним доступом до мережі за допомогою обходу перевірок фізичної безпеки [8].

З а г р о з а 7 : Реалізація послуг, що надаються центральним офісом – постачальником послуг

У таких умовах інформаційна система компанії може приваблювати загрози безпеки, пов'язані з MITM-атаками, шкідливим кодом, підробкою/зміною застосунків та незаконним доступом до Korea-Net, оминаючи наявні перевірки фізичної безпеки [8]. Ця область також може бути вразливою для загроз безпеки, пов'язаних з помилками використання пристрою, витоком важливих даних та прослуховуванням телефонних розмов.

Метод дерева атак

Першим кроком в оцінці ризику безпеки є визначення задіяних активів та розрахунок їхньої вартості. Дерево атак використовується для оцінки всіх загроз безпеці, з якими може зіткнутися кожен актив, як визначено у кожній із семи областей загроз безпеці. Як показано на рис. 5, ймовірність виникнення атаки обчислюється з використанням з'єднувальних елементів АБО та І, які є входом для кожного вузла, що представляє просування атаки до мети.

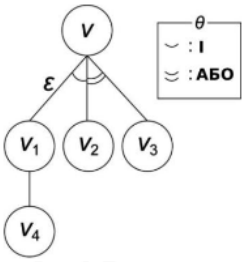

Рис. 5. Дерево атак

Теоретично, ймовірність успіху потенційної атаки збільшується прямо пропорційно до мотивації зловмисника і обернено пропорційно до зусиль, необхідних для організації атаки. У цьому дослідженні вартість активів, ймовірність виникнення атаки та ймовірність успіху атаки використовувалися як параметри оцінки ризиків безпеки, пов'язаних з інформаційною системою компанії.

На рис. 6 наведено приклад того, як проводиться оцінка ризиків. Методика оцінки ризику може бути стисло викладена наступним чином.

1. Оцінка вартості активів інформаційної системи компанії (див. табл. 1 – 3).

Таблиця 1

Критерії оцінки вартості активів

Розподіл	Низький	Помірний	Високий
Конфіденційність	1	2	3
Цілісність	1	2	3
Доступність	1	2	3
Внесок активів	1	2	3

Таблиця 2

Класифікація вартості активів

Мета безпеки	Потенційна дія	Опис
Конфіденційність	Високий	Повинний бути доступним усередині лише уповноваженим особам; несанкціоноване розкриття інформації може призвести до порушення конфіденційності особи та/або фатального пошкодження інформаційної системи компанії.
	Помірний	Може бути розкритий усередині, але у разі зовнішнього впливу може викликати серйозні проблеми щодо конфіденційності та інформаційної системи компанії.
	Низький	При впливі зовнішніх осіб матиме незначний вплив на приватне життя та інформаційну систему компанії.
Цілісність	Високий	Випадкові або навмисні зміни можуть завдати серйозної шкоди приватному життю або інформаційній системі компанії.
	Помірний	Випадкові або навмисні зміни можуть завдати значної шкоди особистому життю або інформаційній системі компанії.
	Низький	Випадкові або навмисні зміни матимуть незначний вплив на особисте життя або інформаційну систему компанії.
Доступність	Високий	Переривання обслуговування може призвести до фатального пошкодження інформаційної системи компанії.
	Помірний	Переривання обслуговування може призвести до значного пошкодження інформаційної системи компанії.
	Низький	Переривання обслуговування завдасть незначної шкоди інформаційній системі компанії.
Внесок активів	Високий	Актив необхідний для послуг інформаційної системи компанії.
	Помірний	Актив частково потрібний для обслуговування інформаційної системи компанії.
	Низький	Актив відіграє допоміжну роль у послугах інформаційної системи компанії.

Таблиця 3

Класифікація вартості активів

Шкала важливості	Сумарна оцінка	Опис
1	4-5	Може завдати шкоди активам, однак майже не впливає на інформаційну систему компанії.
2	6-7	Пошкоджений актив незначно впливає на пов'язаний домен або систему.
3	8-9	Пошкодження активів призводить до значних втрат для бізнесу.
4	10-11	Пошкодження активів призводить до дуже значних втрат для бізнесу.
5	12	Пошкодження активів призводять до великих втрат для бізнесу, який може перестати функціонувати.

2. Оцінка ймовірності виникнення внутрішніх та зовнішніх атак на інформаційну систему компанії (див. табл. 4).

Таблиця 4

Критерії оцінки ймовірності виникнення атаки

Розподіл	Низький	Помірний	Високий
	1	2	3
Ймовірність виникнення атаки	1-50%	51-80%	81-100%

3. Оцінка ймовірності успіху внутрішніх та зовнішніх атак на інформаційну систему компанії (див. табл. 5 – 7).

Таблиця 5

Оцінки різних аспектів потенціалу атаки

Фактор	Рівень	Значення
Витрачений час	≤ 1 день	0
	≤ 1 тиждень	1
	≤ 1 місяць	4
	≤ 3 місяці	10
	≤ 6 місяців	17
	>6 місяців	19
	недоцільно	∞
Експертиза	Непрофесіонал	0
	Досвідчений	3
	Експерт	6
	Численні експерти	8
Знання системи	Відкритий	0
	Обмежений	3
	Секретний	7
	Критичний	11
Можливість доступу	Непотрібний/необмежений	0
	Легкий	1
	Помірний	4
	Важкий	10
	Відсутній	∞
Обладнання	Стандартний	0
	Спеціалізований	4
	Індивідуальний	7
	Ряд індивідуальних	9

Таблиця 6

Оцінки ймовірності успіху атаки

Значення	Потенціал атаки, необхідний для виявлення та використання сценарію атаки	Ймовірність успіху атаки
0-9	Базовий	5
10-13	Розширений базовий	4
14-19	Помірний	3
20-24	Високий	2
≥ 25	За межами високого	1

Таблиця 7

Приклади оцінок ймовірності успіху атаки

Атака	Витрачений час	Експертиза	Знання системи	Можливість доступу	Обладнання	Потрібний потенціал атаки	
						Сума	Оцінка
Витік інформації про клієнта з пристрою	0	6	7	4	4	21	Високий
Підробка шляхом прослуховування телефонних розмов та спуфінг	0	3	0	4	4	11	Помірний
MITM-атаки з використанням шахрайської точки доступу	0	6	3	10	4	23	Високий
Підбір інформації	0	0	0	4	4	8	Базовий

4. Вибір пріоритетної мети для забезпечення безпеки інформаційної системи компанії (див. табл. 8 та 9).

Таблиця 8

Оцінки значення ризику

Значення	Рівень
1-12	Низький
13-32	Помірний
≥33	Високий

Таблиця 9

Оцінки значення ризику

Актив		Вартість активу	Проблема	Ймовірність виникнення атаки AOP)	Ймовірність успіху атаки (ASP)	Значення ризику (RV)	
Пристрій	RTOS	5	Витік інформації про користувачів	1	2	10	H
	GPOS	5	Ненадійний пароль	2	5	50	B
	Шлюз	5	Критична інформація, що передається через помилки в роботі пристрою	3	4	60	B
		5	Збитки через неправильне поводження з пристроєм	2	5	50	B

Продовження табл. 9

		5	Доступ до внутрішньої системи та розкриття важливої нформації через вразливість застосунків пристрою	2	4	40	В
		5	Пристрій: передача відкритого тексту між внутрішньою системою	3	5	75	В
		5	Пристрій: передача відкритого тексту між інформаційною системою компанії	3	5	75	В
		5	Пристрій: MITM-атаки між інформаційною системою компанії	3	1	15	П
		5	Шлюз: передача відкритого тексту між внутрішньою системою	3	3	27	П
		5	Витік інформації через зараження шкідливе ПЗ	1	2	10	Н
		5	Розкриття важливої інформації шляхом зламування шлюзу	2	1	10	Н
		5	MITM-атаки з використанням шахрайського шлюзу	2	1	10	Н
		5	Значний витік інформації з втраченого/викраденого шлюзового пристрою	2	3	30	П
ПК	ПК	4	Підробка шляхом прослуховування телефонних розмов та спуфінгу	3	5	60	В
		4	Несанкціонований доступ через MITM-атаки	2	3	24	П
		4	Шлюз: передача відкритого тексту між інформаційною системою компанії	3	5	60	В
		4	MITM-атаки з використанням шахрайської точки доступу	2	1	8	Н
		4	Витік інформації через зараження шкідливим ПЗ	1	2	8	Н
		4	Розкриття важливої інформації через злам шлюзу	1	1	4	Н
		5	Доступ до внутрішньої системи, що використовується незатвердженим пристроєм	1	1	5	Н
		5	Витік інформації з пристрою через зараження шкідливим ПЗ	1	1	5	Н
		5	Збереження важливої інформації у пристрої	2	4	40	В
		5	Витік важливої інформації з втраченого/викраденого пристрою	2	4	40	В

ISSN 0485-8972 Radiotekhnika No. 209 (2022)
eISSN 2786-5525

Закінчення табл. 9

		4	Внутрішній доступ до національних мереж зв'язку шляхом засобів фізичного захисту	1	1	4	Н
		4	Внутрішній доступ до національних мереж зв'язку шляхом використання вразливості бездротової мережі	1	1	4	Н
		4	Залишення робочого місця на тривалий час після входу в систему	2	5	40	В
		4	Збій безвідмовності через відсутність збереження записів, до яких здійснюється доступ	1	5	20	П
		4	Аварія через помилки в роботі інформаційної системи компанії	1	5	20	П
ПЗ	ПЗ для передачі даних	3	Доступ до внутрішньої системи та розкриття важливої інформації шляхом експлуатації вразливості програми, що використовується	1	1	3	Н
	ПЗ для моніторингу	2	Доступ до внутрішньої системи через файли оновлень для ПЗ	2	1	4	Н
Інформація	Особиста інформація	4	Підбір	3	3	36	В

Вартість активів

Національний інститут стандартів та технологій США (NIST) розробив концепцію управління ризиками: Risk Management Framework for Information Systems and Organizations для захисту комп'ютерних мереж від кібератак [2]. Керівні принципи NIST-RMF поділяють дії з управління ризиками на наступні етапи життєвого циклу: 1) підготовка організації до впровадження концепції RMF. 2) категоріювання інформації та інформаційних систем; 2) вибір (на основі таких факторів, як мінімальні вимоги безпеки та аналіз витрат) заходів захисту; 3) впровадження заходів безпеки); 4) оцінювання безпеки; 5) авторизація безпеки; 6) постійний моніторинг безпеки. Зазначені елементи концепції RMF запропоновані і гармонійно відповідають моделі побудови системи управління інформаційною безпекою організації: ПВПД (плануй, виконуй, перевіряй, дій), яка визначена у стандарті ISO/IEC 27005 [6], і яка, у свою чергу, є частино системи управління організацією. Публікація FIPS PUB 199 [9] визначає критерії категоризації інформації та безпеки інформаційних систем (на основі потенційного впливу системи). FIPS PUB 199 встановлює три цілі безпеки (конфіденційність, цілісність та доступність) та визначає рівні потенційного впливу порушень безпеки на окремих осіб та організації як низький, помірний та високий. При категоризації загальна вартість кожного активу (рис. 6), що підлягає захисту, розраховується наступним чином:

$$AV_a = \sum_{i=1}^{n} A_i\,, \tag{1}$$

де AV_a – сума значень активів (3–12) активу a, розрахована як сума коефіцієнтів, пов'язаних із значеннями активів (1–3: вклад конфіденційності, цілісності та доступності).

У табл. 1 наведено критерії оцінки вартості активів. Вартість активів кожного з чотирьох елементів (цілей безпеки) оцінюється за трибальною шкалою. Загальна оцінка вартості активів розраховується шляхом додавання всіх індивідуальних оцінок, а клас вартості активів

визначається на основі обчисленого результату. Вартість активів оцінюється по відношенню до кожної з цілей безпеки за допомогою трьох рівнів, що відповідають потенційним наслідкам кожної мети безпеки, як описано в табл. 2, і варіюються від 3 до 12. Підставляючи розраховане значення рівняння (1) можна отримати ступінь важливості активу, залежну від вартості активу, яка варіюється від 1 до 5.

У табл. 3 представлені визначення кожного зі ступенів важливості активів, класифікованих вище. Оцінені вартості активів аналізуються з використанням положень, визначених у ISO/IEC 27005 [6] та ISO 31000 RM [10] та перевіряються з використанням методу оцінки ризику, заснованого на урахуванні конфіденційності, цілісності та доступності, відповідно до NIST 800–37 RMF, FIPS PUB 199, виду відмови, наслідків загроз та аналізу критичності активу.

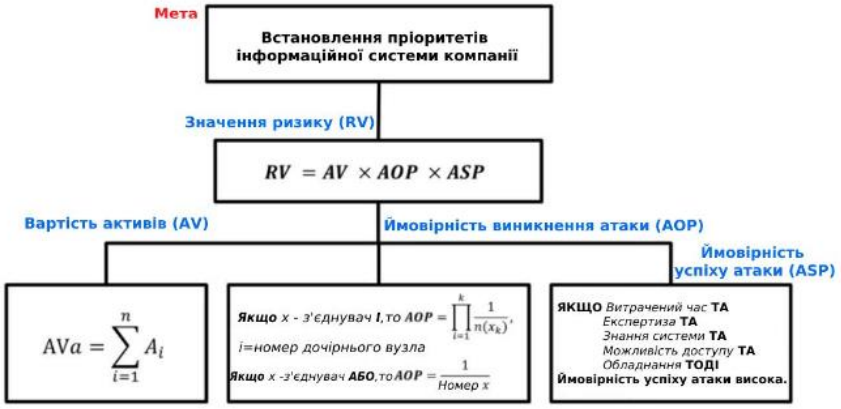

Рис. 6. Етапи оцінки ризиків інформаційної системи компанії

Ймовірність виникнення атаки

Ймовірність виникнення атаки (AOP – Attack occurrence probability) визначається як відношення кількості подій атаки всіх вузлів до кількості дочірніх вузлів атаки, пов'язаних із кореневим вузлом із ціллю досягнення мети атаки кореневого вузла. Нехай один з вузлів – X буде кінцевим вузлом, тоді AOP = 1 (див. рівняння (2), (3)).

$$\text{Якщо } x - \text{з}'\text{єднувальний елемент I, то } AOP = \prod_{i=1}^{k} \frac{1}{n(x_k)}, \quad i = \text{номер вузла}. \tag{2}$$

$$\text{Якщо } x - \text{з}'\text{єднувальний елемент АБО, то } AOP = \frac{1}{\text{Номер } x}. \tag{3}$$

Однак у цьому випадку дерево атак має два основних обмеження. По-перше, вузлам не привласнюється вага, хоча кожен вузол має різний рівень ризику та його потенційна загроза може призвести до різного ступеня збитків. По-друге, замість порівняння ймовірностей появи вузлів вказується лише ймовірність досягнення мети верхнього вузла без урахування частоти появи вузла та рівня ризику кожного вузла, що ускладнює кількісну оцінку вразливостей загроз для безпеки пристроїв. Ймовірність виникнення атаки розраховується шляхом розробки дерева атак для кожного сценарію загроз безпеки відповідно до сімох областей загроз безпеки, як показано на рис. 7. Ймовірність виникнення атаки для прикладу на рис. 7 можна розрахувати в такий спосіб. Оскільки для досягнення v_4 можна вибрати v_8 або v_9, v_2 має ймовірність виникнення атаки 1/2. Крім того, оскільки для досягнення v_4 необхідно вибрати один з методів, представлених v_4, v_5, v_6 і v_7, його ймовірність виникнення атаки становить 1/4. Оскільки для досягнення v_1 обрано єдиний вузол v_3, його ймовірність виникнення

атаки дорівнює 1. Отже, якщо метою атаки є користувач, ймовірність виникнення атаки для витоку інформації про користувача становить 6,25%, як показано нижче:

$$AOP = \frac{1}{2} \times \frac{1}{4} \times \frac{1}{2} = \frac{1}{16} \times 100. \quad (4)$$

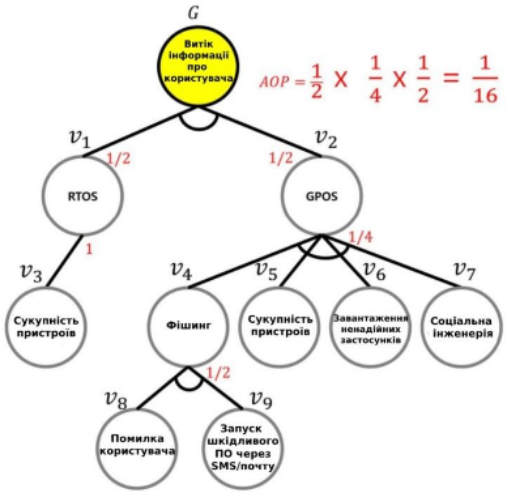

Рис. 7. Приклад дерева атак сценарію загроз безпеки для користувача

Після побудови дерева атак для кожної із семи областей загроз безпеки розраховується ймовірність виникнення атаки кожного дерева атак і, відповідно, кожній області надається оцінка. Оцінка надається кожній області на основі трибальної шкали відповідно до значення ймовірність виникнення атаки, розрахованого за рівнянням (4) та відповідно до критеріїв оцінки (табл. 4).

Ймовірність успіху атаки

Ймовірність успіху атаки (ASP–Attack success probability), визначена у ISO/IEC 15408 [11] та ISO/IEC 18045 [12], і оцінюється на основі наступних факторів [12]:

- Час, що витрачається зловмисником на виявлення вразливості, розробку методу атаки та проведення атаки;
- Необхідні спеціальні експертні знання;
- Знання досліджуваної системи;
- Можливість доступу до мети атаки;
- IT-апаратне/програмне забезпечення або інше обладнання, необхідне для виявлення та використання вразливості.

Ці фактори, що впливають на ймовірність успіху атаки, не є незалежними, а скоріше взаємозамінні з різних точок зору. Наприклад, необхідні знання та обладнання можуть бути замінені витраченим часом (див. табл. 5).

Ймовірність успіху атаки розраховується шляхом застосування значення коефіцієнта (табл. 5) відповідно до сценарію атаки для семи областей загроз безпеки. Потім надається оцінка на основі значення потенціалу атаки (див. таблицю 6), а категоризація виконується на основі рівня потенціалу атаки (див. табл. 7). Для розрахунку ймовірності успіху атаки кожної загрози безпеці рівні ймовірності успіху атаки порівнюються з кінцевими вузлами дерева атак. Наприклад, кожен вузол на рис. 7 відображається на призначеному йому рівні ймовірності успіху атаки відповідно до оцінок ймовірності успіху атаки (див. табл. 7).

Розрахунок значення ризиків

Значення ризику (RV – Risk value) є добутком вартості активів (AV – Asset value), ймовірності виникнення атаки (AOP – Attack occurrence probability) та ймовірності успіху атаки (ASP – Attack success probability):

$$RV = AV \times AOP \times ASP\,. \tag{5}$$

Розраховані значення ризиків оцінюються на трьох рівнях: низькому, помірному та високому (див. табл. 8). При інтерпретації результатів оцінки ризику чим вище вартість активів, ймовірність виникнення атаки і ймовірність успіху атаки, тим вище значення ризику.

Результати аналізу ризиків інформаційної системи компанії відображають рівні ризику загроз безпеці і можуть бути інтерпретовані з погляду відносного ефекту даної атаки. Необхідно встановити відповідні рекомендації щодо безпеки на основі вартості активів кожної загрози з урахуванням її ймовірності виникнення атаки та ймовірності успіху атаки (див. табл. 10).

Таблиця 10

Результати аналізу ризиків

RV = AV × AOP × ASP						
Вартість активів (AV)	Ймовірність виникнення атаки (AOP)	Ймовірність успіху атаки(ASP)				
		За межами високої	Помірна	Висока	Розширена базова	Базова
Оцінка 5	Низька	5	10	15	20	25
	Помірна	10	20	30	40	50
	Висока	15	30	45	60	75
Оцінка 4	Низька	4	8	12	16	20
	Помірна	8	16	24	32	40
	Висока	12	24	36	48	60
Оцінка 3	Низька	3	6	9	12	15
	Помірна	6	12	18	24	30
	Висока	9	18	27	36	45
Оцінка 2	Низька	2	4	6	8	10
	Помірна	4	8	12	16	20
	Висока	6	12	18	24	30
Оцінка 1	Низька	1	2	3	4	5
	Помірна	2	4	6	8	10
	Висока	3	6	9	12	15

Висновки

1. Метод «дерева атак» є систематичним методом визначення характеристик безпеки системи на основі всіх атак, яким піддається інформаційна система. Виявлення всіх можливих атак полегшує аналіз можливих шляхів реалізації кібератак та вибір адекватних контрзаходів і їх оптимальне використання.

2. Щоб виявити загрози, що можуть бути використані для побудови дерева атак інформаційної системи компанії, доцільно обрати типові та засновані на відповідних сценаріях загрози безпеки відповідно до ISO/IEC 27005, а щоб визначити вразливості інформаційної системи компанії, доцільно структурувати враховані загрози та зробити їх придатними для середовища інформаційної системи компанії також відповідно до ISO/IEC 27005.

3. Основними варіантами загроз безпеки інформаційної системи є: користувач; пристрої; домашня мережа (мережа філіалу компанії); шлюз, наприклад, VPN; інтернет (загальнодоступна мережа); сервер центрального офісу компанії; загрози безпеки, пов'язані з MITM-атаками, шкідливим кодом, підробкою/зміною застосунків та незаконним доступом до KoreaNet, оминаючи наявні перевірки фізичної безпеки.

4. Запропонована концепція припускає визначення: областей загроз безпеки інформаційної системи; задіяних інформаційних активів та розрахунок їхньої вартості; оцінку ймовірності виникнення атак на інформаційну систему; оцінку ймовірності успіху атак на інформаційну систему та інше.

5. Основна перевага метода «дерева атак» в тому, що він дозволяє спеціалістам з захисту ідентифікувати потенційні атаки та впроваджувати відповідні контрзаходи. Недоліки цього підходу полягають у тому, що при його впровадженні важко врахувати всі дії і, при цьому, відсутня можливість для моделювання атак, що включають одночасні дії зловмисників.

6. Обгрунтовані методи оцінки ризику, включаючи урахування ймовірності успіху атаки та ймовірності виникнення атаки, дозволяють усунути зазначені недоліки та забезпечити більш точну ідентифікацію методів атаки, пов'язаних із поведінкою зловмисника.

7. Концепція оцінки ризиків кібербезпеки і методика аналізу та оцінки загроз безпеки, які використані, відповідають підходам до побудови ризикоорієнтованих систем управління інформаційною безпекою і можуть стати основою для розробки системи безпеки інформації в інформаційній системі об'єкта критичної інфраструктури.

Список літератури:

1. Schneier B. Attack trees. Dr Dobbs J. 1999;24:21–29. doi: 10.1002/9781119183631.ch21. [CrossRef] [Google Scholar]
2. NIST SP800–37 Rev. 2. Risk Management Framework for Information Systems and Organizations, 2018.
3. Потій О.В., Горбенко І.Д., Замула О.А., Ісірова К.В. Аналіз методів оцінки і управління ризиками кібер і інформаційної безпеки // Радіотехніка. 2021. Вип. 206. С. 5-23.
4. Maji A, Mukhoty A, Majumdar A, Mukhopadhyay J, Sural S, Paul S, et al. Security analysis and implementation of web-based telemedicine services with a four-tier architecture // Proceedings of the Second International Conference on Pervasive Computing Technologies for Healthcare. Tampere; 2008. p. 46–54. 10.4108/icst.pervasivehealth2008.2518.
5. She H, Lu Z, Jantsch A, Zheng LR, Zhou D. A network-based system architecture for remote medical applications. Asia-Pac Adv Netw. 2007;1:27–31. [Google Scholar].
6. International Organization for Standardization. Information security risk management. (second edition). ISO/IEC 27005:2011. 2011. [Google Scholar].
7. International Organization for Standardization . Health informatics – Information security management in health using ISO/IEC 27002. ISO/DIS 27799:2014(E) 2015. [Google Scholar].
8. Camara C., Peris-Lopez P., Tapiador JE. Security and privacy issues in implantable medical devices: a comprehensive survey. J Biomed Inf. 2015;55:272–289. doi: 10.1016/j.jbi.2015.04.007. [PubMed] [CrossRef] [Google Scholar].
9. Stine KM, Kissel RL, Barker WC, Lee A, Fahlsing J, Gulick J. Guide for mapping types of information and information systems to security categories. NIST SP800–64 Rev. 4. 2008. [Google Scholar].
10. International Organization for Standardization. Risk management. ISO 31000:2018. 2018. [Google Scholar].
11. International Organization for Standardization. Information technology – Security techniques – Evaluation criteria for IT security Part 1: Introduction and general model. ISO/IEC 15408–1:2009. 2009. [Google Scholar].
12. International Organization for Standardization. Refining software vulnerability analysis under ISO/IEC 15408 and ISO/IEC 18045. ISO/IEC 18045. 2015. [Google Scholar].

Надійшла до редколегії 22.05.2022

Відомості про авторів:

Горбенко Іван Дмитрович – д-р техн. наук, професор, професор кафедри безпеки інформаційних систем і технологій, факультет комп'ютерних наук, Харківський національний університет імені В.Н. Каразіна, головний конструктор АТ «Інститут інформаційних технологій», Україна; e-mail: Gorbenkol@iit.kharkov.ua, ORCID: https://orcid.org/0000-0003-4616-3449

Замула Олександр Андрійович – д-р техн. наук, професор, професор кафедри безпеки інформаційних систем і технологій, факультет комп'ютерних наук, Харківський національний університет імені В.Н. Каразіна, Україна; e-mail: zamylaaa@gmail.com, ORCID: http://orcid.org/0000-0002-8973-6190

Осипенко Юлія Сергіївна – магістрант кафедри безпеки інформаційних систем і технологій, факультет комп'ютерних наук, Харківський національний університет імені В.Н. Каразіна, Україна; e-mail: julie.osipenko17@gmail.com