КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (29), 2025
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2025.29.886
УДК 342.9:5.08

Клімушин Петро Сергійович
кандидат технічних наук, доцент, доцент кафедри протидії кіберзлочинності
Харківський національний університет внутрішніх справ, Харків, Україна
ORCID ID: 0000-0002-1020-9399
klimushyn@ukr.net

Хруслов Максим Михайлович
кандидат фізико-математичних наук, старший дослідник,
доцент, завідувач кафедри електроніки та управляючих систем
Харківський національний університет імені Каразіна
ORCID ID: 0000-0001-9639-9340
maksym.khruslov@karazin.ua

Гнусов Юрій Валерійович
кандидат технічних наук, доцент, завідувач кафедри кібербезпеки та DATA-технологій
Харківський національний університет внутрішніх справ, Харків, Україна
ORCID ID: 0000-0002-9017-9635
duke6969@i.ua

Мальцев Вадим Віталійович
викладач кафедри протидії кіберзлочинності
Харківський національний університет внутрішніх справ, Харків, Україна
ORCID ID: 0000-0003-0214-8976
alan.kast.95@gmail.com

СИСТЕМИ ГЕНЕРУВАННЯ КРИПТОГРАФІЧНИХ КЛЮЧІВ ДЛЯ МОДУЛІВ БЕЗПЕКИ З АПАРАТНОЮ ПІДТРИМКОЮ ПРИСТРОЇВ IOT

Анотація. Інтернет речей (IoT) є дуже великим джерелом як даних, так й джерелом багатьох вразливостей. У зв'язку з чим постає питання безпеки для захисту ресурсів вузлів IoT та даних, якими вони обмінюються. Цей процес ускладнює недостатність ресурсів цих вузлів з точки зору обчислювальної потужності, розміру пам'яті, ресурсів енергії, дальності та продуктивності бездротового з'єднання. Пристрої IoT можуть розгортатися в критичних середовищах, де будь-який витік інформації для перехоплювача або несанкціоноване проникнення в мережу може стати серйозною загрозою безпеці, особливо в Інтернеті військових речей та медичних речей. У таких мережах для забезпечення безпеки використовуються в основному криптографічні методи. Тут першочерговим завданням є генерування криптографічних ключів для пристроїв IoT, що взаємодіють один з одним. Генерування одного загального (сеансового) ключа для обох сторін дозволяє використання симетричних алгоритмів шифрування. Для розподілу цих ключів може використовуватися криптографія з відкритим ключем (асиметрична криптографія), яка є надто складною з обчислювальної точки зору та енерговитратною, щоб працювати на пристроях IoT з обмеженими ресурсами. Актуальним завданням для реалізації захищених технологій та правил безпеки у мережі IoT є завдання генерації та оновлення симетричних криптографічних ключів з високою ентропією. Наряду с цим, для спрощення системи обміну в мережі IoT криптографічними ключами основним питанням є безпечна доставка даних нового ключа та оновлення ключа при обміні. Більшість запропонованих стратегій генерації ключів застосовані на основі фізичного рівня IoT для загальних бездротових середовищ. У дослідженні надається нова таксономія систем генерації ключів для IoT з класифікацією підходів за апаратним забезпеченням, що демонструє фундаментальну різницю в взаємодії пристроїв IoT за складовими: радіо, аудіо, камери, датчики IMU з інерційно вимірювальних блоків, різне обладнання та гібридні підходи. За допомогою такої таксономії користувачі можуть легко визначити найбільш підходящий метод для своїх сценаріїв застосування. Генерація ключів на основі фізичного рівня IoT отримала широкий дослідницький інтерес і застосовувалася з кількома бездротовими технологіями, такими як Wi-Fi, ZigBee, LoRa/LoRaWAN тощо.

Ключові слова: апаратна підтримка пристроїв IoT; криптографічні ключи; системи генерації ключів; шифрування даних; симетрична та асиметрична криптографія; автентифікація пристроїв IoT; атаки: підслуховування, на передбачуваний канал, по боковому каналу та імітації.

ВСТУП

Постановка проблеми. У застосунках Інтернету речей (*Internet of Things — IoT)* існує багато крихітних недорогих пристроїв, наприклад, сенсорні вузли та імплантовані медичні пристрої. Зазвичай вони живляться від батарейок, які може бути важко замінити. Обмежений розмір та блок живлення забезпечують «лише» достатні обчислювальні ресурси та простір для зберігання даних. Тому розробка IoT була зосереджена головним чином на зниженні енергоспоживання та обчислювальних витрат, а також на підвищенні ефективності апаратного забезпечення. Однак проблеми безпеки IoT часто ігнорувалися, розглядаючись як щось «приємне», а не «обов'язкове».

З іншого боку, дані, що передаються в IoT-застосунках, можуть бути чутливими, приватними та конфіденційними, тому безпека IoT може становити велику соціальну та економічну важливість. Так, медичні пристрої та дані, які вони генерують, є дуже важливими з боку забезпечення життя та здоров'я людини та збереження лікарської таємниці. Наприклад, імплантовані пристрої, такі як кардіостимулятор, життєво важливі для життя пацієнтів, а дані про їхнє здоров'я, такі як частота серцевих скорочень, є дуже конфіденційними. Однак роль IoT в інформаційній безпеці не обмежується лише медичною технікою, так фінансові дані також повинні бути захищені на найвищому можливому рівні, адже такі дані становлять об'єкт підвищеного інтересу для злочинців та потенційних інформаційних диверсій «ворожих країн».

Таким чином в сучасних реаліях питання реалізації безпеки IoT опинилось в центрі уваги та стимулювало значні дослідницькі зусилля. Тим не менш, існують численні недоліки та вразливості безпеки, про що свідчать багато сумнозвісних кібератак. Повертаючись до питання медичних пристроїв можна зазначити, що зловмисниками успішно вдалося зламати імплантовані медичні пристрої останнього покоління, що створює нові загрози для безпеки людей. Як ми вже зазначали подібна ситуація склалася не лише в медицині, але й у інших сферах, наприклад система дистанційного доступу до автомобіля без ключа також була зламана за допомогою дуже недорогих бездротових модулів, що наражає на ризик мільйони автомобілів [**Помилка! Джерело посилання не знайдено.**].

З наведеного вище стає зрозумілим масштаб проблем в IoT, що стало однією з важливих проблем на шляху розвитку даної технології. Численні проблеми виникають через обмежені обчислювальні ресурси та енергопостачання. Отже, слід інвестувати більше дослідницьких зусиль у розробку оптимізованих примітивів безпеки, здатних забезпечити індивідуальну безпеку для застосувань IoT.

Інформаційний аспект безпеки можна реалізувати, головним чином, двома підходами, а саме: сучасною криптографією та безпекою фізичного рівня. Криптографія захищає інформацію за допомогою математичних алгоритмів та протоколів. З іншого боку, методи безпеки фізичного рівня досягають інформаційно-теоретичної безпеки, використовуючи непередбачувані особливості каналу згасання сигналів [**Помилка! Джерело посилання не знайдено.**].

Криптографія була одним з домінуючих рішень інформаційної безпеки з моменту появи відомого протоколу обміну ключами Діффі-Хеллмана в 1976 році. Криптографія не досягає ідеальної секретності, але вона здатна захистити інформацію від атак за

допомогою складних математичних маніпуляцій. Тому її також часто називають обчислювальною безпекою. Оскільки криптографія накладає помірну складність, вона стала фактичним рішенням для захисту передачі інформації. Залежно від того, чи мають два користувача пару різних ключів, чи один і той самий ключ, схеми на основі обчислювальної безпеки називаються асиметричним та симетричним шифруванням.

В асиметричних схемах шифрування сторони мають пару різних відкритих та закритих ключів. Пов'язані протоколи також відомі як криптографія з відкритим ключем (*Public Key Cryptography — PKC*). Спираючись на концепції, успадковані з теорії чисел, такі як дискретний логарифм та цілочисельна факторизація, PKC чудово підходить для шифрування, такого як алгоритм Рівеста-Шаміра-Адлемана (*Rivest-Shamir-Adleman — RSA*), розподілу ключів, такого як обмін ключами Діффі-Хеллмана, та цифрових підписів, таких як криптосистема Ель-Гамаля. З іншого боку, симетричні схеми шифрування вимагають однакового ключа з обох сторін для шифрування та дешифрування. Популярні симетричні схеми включають потоковий шифр RC4, стандарт шифрування даних (*Data Encryption Standard — DES*) та розширений стандарт шифрування (*Advanced Encryption Standard — AES*) тощо.

Класична система шифрування включає розподіл ключів за допомогою PKC та симетричне шифрування. Інфраструктура відкритих ключів (*Public Key Infrastructure — PKI)* спочатку розподіляє один і той самий відкритий ключ між парою легітимних користувачів, назвемо їх Алісою та Бобом. Аліса та Боб мають різні закриті ключі, і вони зможуть отримати один і той самий ключ сеансу на основі деяких складних математичних операцій. Потім ключ сеансу використовується для симетричного шифрування для захисту передачі даних .

Існує багато бездротових методів зв'язку IoT, що спираються на стільниковий зв'язок, рішення IEEE 802.11, WiFi, IEEE 802.15.4, Bluetooth, LoRa/LoRaWAN, вузькосмуговий IoT (NB-IoT), Sigfox [**Помилка! Джерело посилання не знайдено.**] тощо. Але через широкомовну природу бездротового зв'язку інформація стає доступною для всіх користувачів у зоні дії зв'язку. Саме тому, шифрування є життєво важливим для забезпечення конфіденційності та цілісності повідомлень. Зокрема, AES було включено до багатьох стандартів IoT, таких як WiFi, IEEE 802.15.4, Bluetooth та LoRaWAN тощо.

Стандарти IoT утримуються від уточнення способу розподілу ключів для шифрування між законними користувачами. PKC широко використовується в Інтернеті, але може бути оскаржений у контексті IoT через дуже обмежені обчислювальні ресурси таких пристроїв. Використання важких шифрувальних технік в таких системах може призвести до критичного підвищення енергоспоживання пристроїв та як результат значного падіння їх автономності, а також несе ризики падіння їх продуктивності. Нарешті, безпека криптографічних методів, як симетричного шифрування, так і PKC, знаходиться під загрозою через нові квантові комп'ютери.

Хоча це не є небезпечним, неефективним, попередній спільний ключ залишається досить поширеним методом розгортання криптографічних ключів для пристроїв IoT, прикладом чого є програмування ключів у пристрій з ПК через USB-кабель. Однак, оновлювати ключі для пристроїв IoT після їх налаштування та розгортання є складно, враховуючи їхню величезну кількість та типові місця розташування, що є слабкою стороною таких систем.

Підсумовуючи, IoT та пов'язаний з ним Інтернет знаходяться під значною загрозою через слабкі паролі підключених пристроїв. Для недорогих пристроїв IoT терміново потрібна ефективна та легка схема генерування та розподілу ключів.

Окрім вищезгаданих рішень безпеки, існує ще один популярний метод узгодження ключа, отриманого з бездротових каналів, який називається *узгодженням секретного ключа*. Разом із передачею за допомогою безключової безпеки, узгодження секретного ключа також підпадає під поняття безпеки фізичного рівня, яке досягає інформаційно-теоретичної безпеки шляхом використання непередбачуваних особливостей випадкового згасання каналу. Залежно від конкретної реалізації, узгодження секретного ключа має дві моделі, а саме модель каналу та модель джерела.

Узгодження ключа на основі моделі каналу має на меті безпечно передавати ключі між Алісою та Бобом та узгоджувати той самий ключ через двосторонній публічний канал. Однак, воно також стикається з тими ж проблемами, що й безключова безпека, з точки зору її практичної реалізації.

Модель джерела узгодження секретного ключа працює інакше, а саме шляхом генерації ключів з бездротового каналу між Алісою та Бобом, а не шляхом передачі ключів, що називається *генерацією ключів з бездротових каналів*. Філософія генерації ключів бере свій початок у 1993 році, коли Альсведе, Чісар та Маурер заклали її інформаційно-теоретичні основи. Відтоді протягом останніх трьох десятиліть спостерігається дедалі складніше дослідження цієї перспективної методики. Практичний протокол генерації ключів був запропонований у 1995 році. Ідеальна секретність досягається коли згенерований ключ можна використовувати для одноразового шифрування даних [**Помилка! Джерело посилання не знайдено.**]. Тож таким чином нівелюється ризик перехоплення ключа, через те що сам ключ створюється на основі випадкових флуктуацій каналу зв'язку між пристроями, що значно підвищує рівень захищеності каналу.

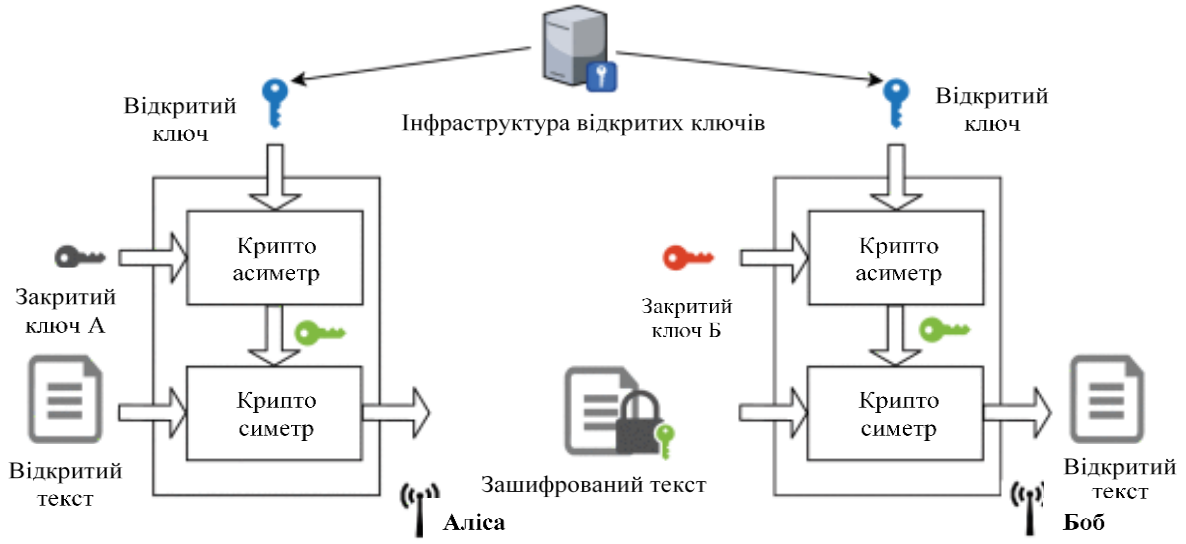


Рис. 1. Класична система шифрування

РКС розповсюджує сеансовий ключ Алісі та Бобу. Потім вони використовують цей сеансовий ключ симетричного шифрування для захисту даних

Класична система шифрування (рис. 1) включає розподіл ключів за допомогою РКС та симетричне шифрування. Інфраструктура відкритих ключів (PKI) спочатку розподіляє один і той самий відкритий ключ між парою легітимних користувачів, Алісою та Бобом. Аліса та Боб мають різні закриті ключі, і вони зможуть отримати один і той

самий ключ сеансу на основі деяких складних математичних операцій. Потім сеансовий ключ використовується для симетричного шифрування для захисту обміну даними.

Однак швидкість генерації ключів недостатньо висока для підтримки передачі даних. Отже, більш поширеним рішенням є побудова гібридної криптосистеми з використанням генерації ключів та симетричного шифрування, як показано на рис. 2 [**Помилка! Джерело посилання не знайдено.**]. Аліса та Боб можуть генерувати ключі безпосередньо зі свого спільного бездротового каналу, без допомоги третьої сторони, такої як PKI. Таким чином, генерація ключів забезпечує значно вищий рівень інформаційної безпеки, тому їй не загрожують нові квантові комп'ютери. Нарешті, цей метод має легкий характер, тому він чудово підходить для недорогих пристроїв IoT. Тобто генерація ключів з спільного бездротового каналу пристроїв IoT є ідеальною альтернативою PKC для створення безпечних сеансових ключів для IoT. Тому систематизований та порівняний аналіз методів та схем генерації таких криптографічних ключів для запровадження у пристроях IoT надається в цьому дослідженні.

Рис. 2. Гібридна криптосистема на основі генерації ключів

Генерація ключів встановлює однаковий сеансовий ключ для Аліси та Боба. Потім вони використовують цей ключ для симетричного шифрування.

Аналіз останніх досліджень і публікацій. Загальний процес генерації ключа з використанням атрибутів фізичного рівня бездротового каналу включає чотири етапи: зондування каналу, квантування, узгодження інформації та посилення конфіденційності [**Помилка! Джерело посилання не знайдено.**]. З точки зору фізичного рівня, більша частина роботи зосереджена на вдосконаленні зондування каналу або етапу квантування. Зондування каналу є ключовим елементом протоколів генерації ключів, який фіксує випадковість каналу шляхом вимірювання параметрів каналу, результатом тут виступає певна інформація про параметри каналу зв'язку в конкретному часовому зрізі.

Система генерації ключів, яка заснована на використанні характеристик каналу результатів вимірювань будується на принципі взаємності від електромагнітного розповсюдження [**Помилка! Джерело посилання не знайдено.**]. Тобто характеристики каналу, отримані відправником і одержувачем, будуть однаковими, якщо вимірювання виконується протягом часу когерентності.

Для покращення подібності вироблених характеристик каналу додають фазу попередньої обробки отриманої інформації про сигнал [**Помилка! Джерело посилання не знайдено.**]. Доведено, що додавання цієї фази веде до збільшення значення коефіцієнта кореляції. Чим вище значення коефіцієнта кореляції характеристик каналу, тим більша ймовірність отримання однакового ключа між двома користувачами. Тим не менш існує

ймовірність отримання різного ключа між двома пристроями, тому необхідна фаза виправлення помилок, щоб створити однаковий ключ.

Деякі дослідники [**Помилка! Джерело посилання не знайдено.**] намагаються подолати цю проблему шляхом модифікації існуючої фази попередньої обробки сигналу. Фаза змінюється шляхом поділу даних вимірювання на кілька блоків даних. Кожен блок даних буде попередньо оброблений за допомогою існуючого методу попередньої обробки сигналу.

Інше дослідження [**Помилка! Джерело посилання не знайдено.**] пропонує модифікувати фазу попередньої обробки сигналу шляхом поєднання методу поліноміальної регресії з модифікованим фільтром Калмана. Результати проведених тестів показують, що використання модифікованого етапу попередньої обробки сигналу здатне виробляти ті самі ключові біти без проходження фази виправлення помилок. Однак фаза попередньої обробки сигналу вимагає значно більшого обчислення, оскільки вона виконується окремо для кожного блоку даних. Чим більший обсяг даних, тим більший час потрібно для обчислення. Частими параметрами для визначення успіху побудованої системи генерації ключів є коефіцієнт кореляції, швидкість розбіжності ключів, швидкість синхронізації ключів і нерегулярність.

Деякі дослідження системи генерації ключів для пристроїв IoT [**Помилка! Джерело посилання не знайдено.**] також зосереджені на використанні цих параметрів для визначення продуктивності побудованої системи генерації ключів. Параметри продуктивності в пристроях IoT повинні бути додані з обчислювальним часом і накладними витратами на зв’язок, які покажуть ефективність системи. Чим менший обчислювальний час і накладні витрати на зв’язок, тим ефективніша система, тому її можна впроваджувати на пристроях з обмеженими ресурсами.

В іншому дослідженні [**Помилка! Джерело посилання не знайдено.**] запропоновано ефективний метод генерації ключів без етапу попередньої обробки сигналу та виправлення помилок, щоб він міг зменшити час обчислення та накладні витрати на зв’язок. Цей метод ґрунтується на синхронізованому квантуванні, який використовує середнє значення, стандартне відхилення та параметр стандартного поділу відхилення. Тобто система синхронізації здатна виробляти однакові ключові біти без проходження етапів попередньої обробки сигналу та виправлення помилок. Порівняно з попередньою системою оцінки продуктивності запропонована система здатна гарантувати значно швидший час обчислення та менші накладні витрати на зв’язок.

Загалом, для визначення успішності встановленої схеми генерації ключа часто використовуються три параметри продуктивності, тобто швидкість генерації ключів (*Key Generation Rate — KGR*), коефіцієнт неузгодженості ключів (*Key Disagreement Rate — KDR*) та випадковість [**Помилка! Джерело посилання не знайдено.**]. KGR показує кількість бітів ключа, згенерованих протягом вимірювання. KDR вказує на невідповідність бітів квантування, тоді як випадковість вказує на значення випадковості згенерованого секретного ключа. Завжди існує компроміс між цими параметрами. Деякі дослідники використовували схему без втрат для збільшення KGR, але результуючий KDR також збільшувався; інші дослідники використовували схему зі зниженим рівнем KDR, однак це тягне за собою зменшення KGR. Оскільки схема генерації секретного ключа має метою генерування ідентичних ключів між двома пристроями, квантування, яке генерує високі KDR, використовується не часто. Деякі дослідники використовували схеми попередньої обробки для покращення каналу взаємності з метою зменшення KDR. Щоб подолати проблему багаторівневих параметрів продуктивності, можна розглянути

використання комбінації схем попередньої обробки з багаторівневим квантуванням для отримання низького KDR, водночас отримавши високий KGR.

Ця стаття пропонує комплексний огляд легких рішень безпеки, розроблених для IoT, що спираються на генерацію ключів з бездротових каналів.

Метою статті є порівняльний огляд методів управління та генерації ключів з бездротових каналів на основі вирішення наступних завдань: розглядання основ управління та генерації ключів; визначення таксономії систем генерації ключів для IoT з класифікацією підходів за апаратним забезпеченням; аналізу типового протоколу генерації ключів для використання випадковості зі спільних каналах між пристроями IoT; порівняння продуктивності систем генерації ключів за трьома метриками: швидкість, коефіцієнт узгодження ключів та випадковість, оцінка відомих атак та засобів захисту від них на системи генерації ключів таких, як атаки підслуховування, на передбачуваний канал, по боковому каналу та імітації.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

1. Системи управління криптографічними ключами IoT.

Управління ключами є критичним компонентом безпеки IoT. Оскільки пристрої IoT взаємодіють через потенційно незахищені мережі, управління криптографічними ключами стає необхідним для захисту конфіденційних даних. Нездатність впровадити ефективне управління ключами може призвести до несанкціонованого доступу, витоків даних та втрати довіри користувачів. Управління ключами включає генерацію, розповсюдження, зберігання та знищення криптографічних ключів.

Система керування ключами (*Key Management System — KMS*) забезпечує єдиний інтерфейс для керування ключами, підвищує безпеку корпоративної мережі, забезпечує масштабованість і мінімізує людські помилки. Криптографічна KMS — це централізована система, яка забезпечує генерацію, зберігання та розповсюдження ключів, а також автоматичне закінчення терміну дії, оновлення, заміну, резервне копіювання та скасування ключів, і все це для широкого кола застосувань.

Спроби знайти компромісне рішення в наведених рамках найчастіше призводили до підходу, у якому велика мережа сенсорних вузлів розбивалася на групи взаємодіючих вузлів, котрим як механізм розподілу ключів використовувалося групове управління ключами (*Group Key Management — GKM*), тобто, ключі спільно використовуються вузлами, що утворюють одну групу [**Помилка! Джерело посилання не знайдено.**]. Наведені підходи знайшли своє застосування в різних типах застосунках: бездротових натільних мереж, бездротових сенсорних мереж, хмарних обчислень, бездротових мереж IPv6 та IoT. Вони надають рішення для окремих груп застосунків GKM, беручи до уваги безліч атрибутів, найбільш важливими з яких є: схеми розподілу ключів, тип криптографії, що використовується, пряма і зворотна секретність (загальний ключ повинен оновлюватися, коли новий вузол IoT приєднується до групи або залишає групу), взаємна незалежність ключа, наявність єдиної точки відмови і масштабованість. Визначення різних стратегій оновлення ключів наведено в табл. 1.

Таблиця 1

Визначення різних стратегій оновлення ключів

Типи оновлення ключів	Визначення стратегій

Періодичне	Це стратегія оновлення ключів, за якої ключі шифрування оновлюються через регулярні проміжки часу. Важливі зміни відбуваються за заздалегідь визначеним графіком, наприклад, щогодинна, щодня, щотижня або будь-яким іншим регулярним інтервалом. Цей метод гарантує регулярне оновлення ключів, мінімізуючи ризик довгострокових компрометацій та зберігаючи безпеку групового зв'язку.
Імовірнісне	Це стратегія, за якої оновлення ключів відбуваються випадковим чином відповідно до розподілу ймовірностей. Ключі оновлюються через випадкові проміжки часу, додаючи аспект непередбачуваності, а не за заздалегідь визначеним графіком або тригером. Цей підхід додає додатковий рівень безпеки, ускладнюючи для потенційних зловмисників прогнозування того, коли будуть впроваджені критичні оновлення.
На вимогу	Це стратегія, за якої значні зміни відбуваються у відповідь на певні запити або тригери від членів групи або системи. Коли член запитує новий ключ, виявляє проблему безпеки або виконуються певні заздалегідь визначені умови, можуть бути ініційовані оновлення ключів. Цей метод забезпечує більшу гнучкість в управлінні ключами, оскільки оновлення впроваджуються за потреби, а не за заздалегідь визначеним графіком.
За сеансами.	Це стратегія, за якої ключі шифрування оновлюються на початку кожного групового сеансу або сеансу зв'язку. Сеанс — це окремий період або фаза групового спілкування. Цей метод гарантує, що кожен сеанс починається з нового набору ключів, тим самим зменшуючи потенційний вплив компрометації ключів або атак на наступні сеанси.
Зміна членства в групі	Це стратегія оновлення ключів у GKM, яка вимагає оновлення ключів шифрування під час зміни членства в групі. Коли учасники приєднуються до групи або виходять з неї, або коли змінюється кількість учасників.

Здебільшого для реалізації групового керування ключами застосовуються виключно симетричні криптоалгоритми, такий підхід здатний забезпечити низькі обчислювальні витрати на одному вузлі, однак це призводить до різкого зниження продуктивності при масштабуванні: зі збільшенням числа пристроїв та частоти змін у складі груп процеси оновлення та розподілу ключів стають вузьким місцем, а загальна масштабованість системи виявляється надто обмеженою. На основі цих випадків в [**Помилка! Джерело посилання не знайдено.**] представлена архітектура гнучкого і добре масштабованого децентралізованого групового керування ключами для контролю доступу в середовищі IoT, яке не викликає сильного навантаження на систему GKM у разі зміни членства вузлів у групі.

GKM є важливим компонентом протоколів безпечного групового зв'язку. Крім того, більшість існуючих схем GKM залежать від криптографії з відкритим ключем, яка є вразливою для квантових комп'ютерів. GKM являє собою фундаментальний елемент в схемах безпечного групового зв'язку, якій використовується всіма членами групи. Спільний груповий ключ використовується для підписання та шифрування групових повідомлень, автентифікації членів групи та повідомлень, а також надання доступу до групових ресурсів та трафіку. Криптографічна стійкість цього групового ключа та протоколу керування ключами визначають стійкість схеми безпечного групового зв'язку [**Помилка! Джерело посилання не знайдено.**], [**Помилка! Джерело посилання не знайдено.**].

Схеми управління груповими ключами можна класифікувати на три категорії: симетричні, асиметричні та гібридні. Хоча асиметричні механізми ключів є потужнішими та служать основою для встановлення безпечних каналів зв'язку між кількома сторонами, вони також споживають більше енергії. Це критично важлива технологія для високо взаємопов'язаних мереж і, як така, є критично важливою для IoT. Проміж іншим були зроблені зміни для полегшення криптографічних примітивів, таких

як криптографія еліптичних кривих (*Elliptic Curve Cryptography — ECC*) та вдосконалені системи шифрування *AES*, шляхом зменшення обчислювального часу та витрат [**Помилка! Джерело посилання не знайдено.**].

Вимоги до безпечного групового спілкування можна розділити на дві категорії: вимоги безпеки та вимоги ефективності. До вимог безпеки відносяться:

Автентифікація. Перш ніж надати вузлам доступ до групи, схема групового зв'язку повинна автентифікувати пристрої IoT. Крім того, в процесі групового спілкування учаснику може бути призначена роль відправника, одержувача або обидві ці ролі. Для захисту від атак, пов'язаних з ідентифікацією, учасники повинні бути автентифіковані. Автентифікацію можна здійснити за допомогою групового ключа, парного ключа або сертифіката [**Помилка! Джерело посилання не знайдено.**].

Цілісність. Правильність та узгодженість групових повідомлень є обов'язковою умовою коректного та безпечного функціонування пристроїв IoT. Повідомлення слід пересилати без модифікацій та коригувань. Для досягнення такого обміну можна використовувати цифрові підписи зі стійкими ключами шифрування [**Помилка! Джерело посилання не знайдено.**].

Конфіденційність. Це набір правил, що обмежують доступ до даних. Групові повідомлення, надіслані групі, повинні бути обмежені цією групою; лише авторизовані групи можуть мати доступ до цих даних. Цього можна досягти за допомогою різних методів шифрування.

Перекодування. Це стосується процесу оновлення ключа сеансу. Кожна зміна членства вимагає перекодування пов'язаних ключів. Груповий ключ слід негайно відкликати, якщо змінюється членство учасника. В іншому випадку, доки груповий ключ не буде оновлено, відкликані вузли можуть продовжувати використовувати групове спілкування. Різні методи оновлення ключів надають можливості для керування життєвим циклом ключів шифрування у сценаріях групового спілкування, як показано в табл. 1.

Незалежність групи. Вузол зберігає профіль для кожної групи, який включає параметри безпеки, такі як адреса контролера групи та ключ групи. Оскільки вузол може бути членом кількох груп, параметри безпеки для кожної з них повинні бути незалежними, щоб скомпрометована група не впливала на інші групи.

Квантова стійкість. Поява та подальший розвиток квантових обчислень може зробити класичні криптографічні рішення вразливими до порушень безпеки. Зазначені виклики вимагають розвитку та адаптації криптографічних систем до протидії атакам з боку квантових систем.

Вимоги до ефективності:

Масштабованість. Ефективність та безпека групового зв'язку може бути якісно реалізована коли мова йде про невеликі групи, однак при збільшені числа учасників ефективне функціонування системи безпеки стає значно складнішим. Алгоритми управління членством повинні бути ефективними при одночасному управлінні кількома запитами, наприклад, приєднання пристрою до активності або його вихід. Доставка групового ключа великим групам повинна здійснюватися в розумні терміни з розумною затримкою, низькими обчислювальними та комунікаційними витратами [**Помилка! Джерело посилання не знайдено.**].

Гнучкість. Схеми безпечного групового зв'язку повинні добре працювати в різних типах середовищ. Підтримувати динамічну поведінку. Дозволяти додавати та видаляти користувача в будь-який час [**Помилка! Джерело посилання не знайдено.**].

Низькі витрати на зберігання, зв'язок та обчислення: Схеми безпечного групового зв'язку повинні бути ефективними з точки зору витрат на зберігання, зв'язок та

обчислення. Кількість ключів, що використовуються для захисту групового зв'язку має бути обмеженою до характеристик пам'яті для зберігання ключів. Обчислювальні витрати не повинні бути дуже високими, оскільки пристрої мають низькоенергетичний процесор. Фактично, щоб уникнути споживання енергії вузлом, схема безпечного групового зв'язку не повинна накладати високі витрати на зв'язок.

Дослідники працюють над створенням архітектури, яка є не тільки безпечною, але й здатною запобігати атакам, навіть якщо зловмисники отримають доступ до системи. Як результат, ефективніше надсилати багатоадресні повідомлення групі пристроїв, ніж надсилати одноадресні повідомлення окремим пристроям у кількох копіях, що споживає більше енергії.

Встановлення безпечного групового ключа є критично важливою функцією для забезпечення цілісності, автентифікації та конфіденційності повідомлень. За безпеку сеансу відповідає контролер групи, який керує автентифікацією, авторизацією та контролем доступу. Сервер ключів управляє потрібним ключовим матеріалом. Головним завданням GKM є забезпечення того, щоб усі авторизовані групи мали оновлені ключі відповідно до існуючих стратегій наведених в табл. 1. Найважливіша схема управління груповими ключами класифікується за п'ятьма параметрами: продуктивність, безпека, якість обслуговування, сервер управління ключами та контролер сеансу групи.

Інноваційним підходом до генерації та розподілу ключів є використання механізму ланцюга блоків в мережах вузлів, якій вимагає наявність вузлів з великим сховищем даних, обчислювальними та комунікаційними можливостями [**Помилка! Джерело посилання не знайдено.**].

Концепція системи генерації та оновлення криптографічних ключів (*Key Generating and Renewing — KGR*) утворює мережу вузлів IoT за доменною структурою для обміну даними захищених криптографічно [**Помилка! Джерело посилання не знайдено.**]. Кожен вузол відіграє роль майстра або репліки в домені. У ресурсах майстра зберігаються актуальні описи домену та опис всіх вузлів домену, а також дані, необхідні для автентифікації вузла домену.

Вузли репліки зберігають у своїх ресурсах копію опису безпечного домену, отриманого від майстер-вузла. У разі виходу з ладу сенсорного вузла, що виступає в ролі майстра, запускається спеціальна процедура вибору нового майстер-вузла з коректно функціонуючих вузлів-реплік. Один із вузлів кожного домену виступає як шлюз для домену. Цей вузол є вузлом-приймачем даних, що надходять з вузлів домену, а також джерелом даних, що відбуваються за межами домену. Вузол шлюзу відповідає за безпечний обмін даними між доменами та є представником домену для системи KGR. Для системи KGR з усіх вузлів домену безпеки важливим є лише вузол-сенсор, який в даний момент виступає як шлюз в домені безпеки вузлів-сенсорів. Джерелом криптографічних ключів для захисту передачі даних буде окремий вузол, до якого матимуть доступ вузли-шлюзи.

У системі KGR буде три типи вузлів: сервер ключів є джерелом криптографічних ключів; вузли — представники доменів, для яких створюватимуться симетричні ключі; вузол — центр авторизації для управління ресурсами сервера ключів, додавання нових ідентифікаторів для авторизованих вузлів і підготовка вузлів к роботі.

Клієнтами служби генерації та оновлення криптографічних ключів є вузли доменів. Кожен такий вузол зберігатиме у своїх ресурсах необхідні дані для встановлення з'єднання та безпечного обміну даними з сервером ключів, а також дані, необхідні для безпечного обміну даними з іншими вузлами.

Створення безпечної системи потребує розробки рішень безпеки для конфігурації програмного та апаратного забезпечення всіх компонентів системи. Важливим елементом для системи KGR цих рішень є створення безпечних процедур: запуску вузла брокер (виступає посередником обміну даними між вузлами системи KGR); ініціювання вузла сервера ключів (створення локальної структури довіри з використанням асиметричних ключів для вузла сервера ключів та створення індивідуальних даних для вузла); підготовки облікових даних для вузла за результатом спільної роботи центра авторизації та сервера ключів; реєстрації вузла в домені; передачі списку авторизованих вузлів у співробітництво; генерації сеансових ключів, яка складається із трьох етапів: запит сеансового ключа, надання сеансового ключа цільовому вузлу, підтвердження доставки сеансового ключа на вузол призначення; безпечного обміну даними між вузлами; оновлення сеансового ключа, яке включає також три етапи: запит — надання — підтвердження доставки оновленого сеансового ключа на вузол призначення.

Обмеження ресурсів і відсутність спільної інфраструктури довіри спонукають дослідників шукати альтернативні підходи до генерації ключів, досліджуючи особливості та функції, що інтегровані в самі пристрої IoT. Існуючі системи генерації ключів засновані на загальному принципі, якщо кілька пристроїв можуть спостерігати загальний сигнал (наприклад, звук, температуру чи рух) із певного каналу, їхні спостереження можна використовувати як дані для генерації випадкових ключів.

Попередні дослідження дали величезну кількість технічно надійних систем, що спираються на різні допоміжні канали, такі як візуальний канал, акустичний канал і сенсорний канал [**Помилка! Джерело посилання не знайдено.**]. Тут виокремлюють схеми безпечного сполучення з трьох аспектів: фізичний канал, взаємодія людини з комп'ютером та класи застосунків. Однак, цю систематизацію нелегко використовувати практично, оскільки значна частина систем лежить на перетині різних категорій.

Актуальним є запровадження таксономії з класифікації підходів за апаратною підтримкою відповідно до апаратного інтерфейсу, що використовуються для генерації ключів, таких як аудіо, сенсор, камера, радіо, біометрія, гібридні з аналізом безпеки та порівнянням продуктивності [**Помилка! Джерело посилання не знайдено.**].

Таким чином, системи генерації ключів ускладняються через різноманітність пристроїв IoT, апаратних можливостей різних платформ та моделей взаємодії між системами, а також між людьми-операторами і машинами.

2. Системи генерування криптографічних ключів IoT.

Пристрої IoT можуть розгортатися в критичних середовищах, де будь-який витік інформації для перехоплювача або проникнення в мережу може стати серйозним порушенням безпеки, особливо в Інтернеті військових або медичних речей. У таких мережах для забезпечення безпеки використовуються в основному криптографічні методи. Тут першочерговим завданням є генерування криптографічного ключа (сеансового ключа) для пристроїв IoT, що взаємодіють один з одним. Генерування одного загального ключа для обох сторін дозволяє використання симетричних алгоритмів шифрування.

Таким чином, актуальним завданням для реалізації захищених технологій та правил безпеки у мережі IoT є завдання генерації та оновлення симетричних криптографічних ключів з високою ентропією (*Key Generating and Renewing — KGR*). Наряду с цим, для спрощення системи обміну в мережі IoT криптографічними ключами основним питанням є безпечна доставка даних ключа та оновлення ключа при обміні.

Асиметрична криптографія використовується для побудови структур довіри, для підпису повідомлень, що пересилаються, і для встановлення безпечного з'єднання з іншою стороною для обміну даними. За допомогою асиметричної криптографії будуються механізми розподілу симетричних ключів. Асиметрична криптографія не використовується для шифрування великих даних, тому що ці алгоритми характеризуються відносно великими накладними витратами щодо зашифрованих даних, забирають багато часу та ресурсів, а для забезпечення достатньої стійкості шифру ці ключі мають бути відносно довгими.

Симетрична криптографія більш ефективна у обчислювальному відношенні та забезпечує достатню стійкість шифру за рахунок використання ключів, які набагато коротші, ніж асиметрична криптографія. Однак існує суттєва проблема із симетричною криптографією, це роздача ключа. Для цього зазвичай використовуються асиметричні алгоритми для встановлення з'єднання та визначення так званого сеансового ключа, який є симетричним ключем, що використовується обома сторонами з'єднання. Подальший обмін даними здійснюється з використанням сеансового ключа.

Кожен криптографічний ключ необхідно час від часу змінювати, щоб зловмисникам було важко згадати ключ. Для цього використовуються різні стратегії оновлення криптографічних ключів. Перша група методів використовує асиметричну криптографію (дуже схожу процедуру встановлення сеансового ключа). У другій групі методів «старий» симетричний криптографічний ключ використовується для підтримки процедури отримання «нового» ключа. У третій групі методів при встановленні сеансового ключа генерується додатковий симетричний ключ, який буде використовуватися тільки для оновлення сеансового ключа.

Асиметрична криптографія використовується тією чи іншою мірою у всіх сценаріях. Ця криптографія вимагає, щоб кожна сторона мала власний асиметричний ключ. Процедура визначення сеансового ключа цих сторін вимагає обміну їх відкритими ключами. Для забезпечення безпечного обміну відкритими ключами між сторонами використовується так звана "третя сторона" довіри, відомий як центр сертифікації. Описані рішення відомі та широко використовуються, але вимагають, щоб кожен вузол мережі мав доступ до мережі, в якій доступний центр сертифікації. Крім того, алгоритми, що використовуються, вимагають відносно великих ресурсів пам'яті для збереження ключів; пристрій повинен мати достатню обчислювальну потужність та досить ефективне джерело енергії. Цим вимогам задовольняють стаціонарні вузли, але вони являють собою серйозну проблему для мобільних, що використовують бездротові канали зв'язку і вузли сенсорної мережі з батарейним живленням, які в даний час складають дуже велику кількість мережевих вузлів IoT [**Помилка! Джерело посилання не знайдено.**].

Для подолання цих перешкод, різні організації створюють кластери мережевих вузлів, в яких застосовуються спеціальні правила безпеки, адаптовані до вимог організації [**Помилка! Джерело посилання не знайдено.**]. Цей підхід призначений для захисту даних, які обмінюються всередині організацій від несанкціонованих дій з зовні. Така організація може бути великою корпорацією, елементами критичної інфраструктури держави, озброєними силами тощо.

Пристрої IoT — це, по суті, інтелектуальні пристрої, які підтримують підключення до Інтернету та можуть обмінюватися даними через Інтернет з іншими пристроями та надати користувачеві віддалений доступ для керування пристроями відповідно до їх потреб [**Помилка! Джерело посилання не знайдено.**]. За умовами застосування, пристрої IoT можна класифікувати за трьома категоріями: портативні/носимі

(смартфони, розумні часи, розумні окуляри, розумний одяг, розумне взуття), стаціонарні (розумний динамік, розумний дисплей, розумна лампочка, розумний перемикач) та мережеві (Wi-Fi, Bluetooth, RFID, ZïgBee, 5G).

Мережеві пристрої — це фізичні пристрої, які необхідні в комп'ютерній мережі для зв'язку та взаємодії з обладнанням. Мережеві пристрої зазвичай не мають вбудованих датчиків, мікрофона та динаміка. Більше того, кожен мережевий пристрій зазвичай має один бездротовий інтерфейс зв'язку. Системи генерації ключів для цих пристроїв зазвичай ґрунтуються на характеристиках фізичного рівня бездротового каналу, таких як індикатор потужності прийнятого сигналу, інформація про стан каналу тощо.

Стаціонарні пристрої, типу розумний будинок, переважно більшість із них не мають датчиків, мікрофона та динаміка. Системи генерації ключів для стаціонарних пристроїв зазвичай використовують загальну контекстну інформацію, яка може бути виміряна різнорідними датчиками [**Помилка! Джерело посилання не знайдено.**].

Портативні/носимі пристрої — це розумні електронні пристрої, які носяться близько до шкіри та/або на її поверхні, або які користувач носить із собою. Ці пристрої часто скорочено називають носимими пристроями, а прикладами таких пристроїв є розумні окуляри, розумний годинник та розумний одяг. Тут також класифікуємо мобільний телефон до цієї категорії.

Ці пристрої зазвичай оснащені різноманітними датчиками, які можуть контролювати, виявляти, аналізувати та передавати інформацію про контекст користувача, таку як місцезнаходження, рух, частота серцевих скорочень тощо. Вони також мають вбудований мікрофон, динамік та різні функції бездротового підключення. Тому, порівняно з двома іншими типами пристроїв, носимі пристрої можуть надавати більше інформації для генерації ключів. Дійсно, значна частина існуючих систем генерації ключів базується на носимих пристроях [**Помилка! Джерело посилання не знайдено.**], [**Помилка! Джерело посилання не знайдено.**], [**Помилка! Джерело посилання не знайдено.**].

З поширенням пристроїв IoT безпечний зв'язок між пристроями (*Device-to-Device — D2D*) стає все більш важливим, оскільки пристрої IoT часто необхідно об'єднувати в пари для синхронізації та обміну даними. Узгодження криптографічного ключа є фундаментальною вимогою для безпечного зв'язку D2D для досягненні конфіденційності. Щоб подолати ці проблеми, захист фізичного рівня (*Physical Layer Security — PLS*) отримав серйозних досліджень.

Характеристики бездротових каналів залежать від розташування середовища, наприклад матеріалів розсіювача, їх мобільності та розподілу. Ці характеристики роблять канал між вузлами унікальним, випадковим і непередбачуваним для перехоплювачів. Тому запропоновано схеми розподілу безпечних ключів, які використовують характеристики фізичного рівня радіоканалу пристроїв зв'язку. Ці характеристики фізичного рівня зазвичай включають потужність отриманого сигналу (*Received Signal Strength — RSS*) та інформацію про стан каналу (*Channel State Information — CSI*), як характеристики радіоканалів [**Помилка! Джерело посилання не знайдено.**]. Ці характеристики каналу є найбільш доступними характеристиками в бездротових пристроях з різними стандартами. Комбінація вищезазначених атрибутів може бути використана для підвищення рівня безпеки.

Однак, незважаючи на вищезазначені переваги, PLS стикається з кількома проблемами, пов'язаними зі змінним у часі характером фізичного каналу та недосконалими оцінками на сторонах зв'язку. Тут пропонують схеми як на основі

генерування ключів з атрибутів фізичного рівня так реалізують методи для пом'якшення впливу недосконалих оцінок каналу. Крім того, більшість запропонованих стратегій генерації ключів на основі фізичного рівня розроблені для загальних бездротових середовищ, які можуть бути незастосовними безпосередньо до багатьох середовищ IoT. У цьому дослідженні надається порівняний аналіз схем генерування ключів для використання у пристроях IoT.

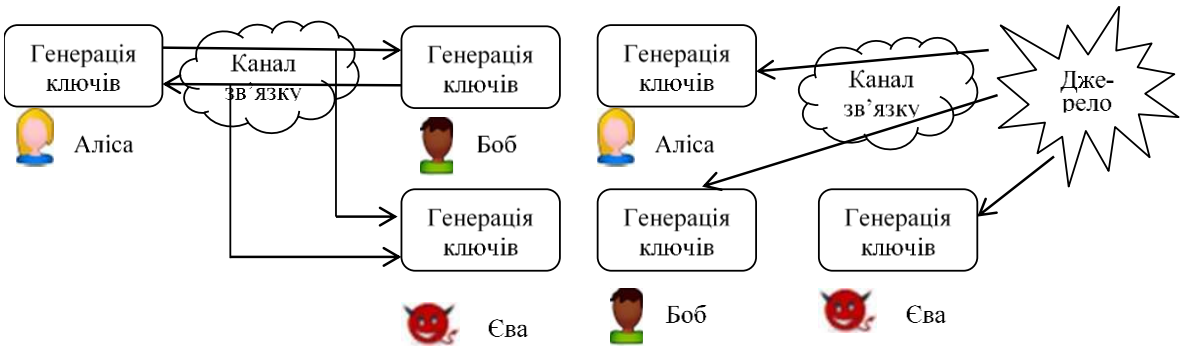
Зокрема, дослідження [**Помилка! Джерело посилання не знайдено.**] використовує нову таксономію для систем генерації ключів, яка включає таки складові: радіо, аудіо, камери, датчики IMU з інерційно вимірювальних блоків (*Inertial Measurement Unit*), різне обладнання та гібридні підходи (рис. 3). Тобто обґрунтуванням цієї таксономії є класифікація підходів за апаратним забезпеченням.

Перш ніж обговорювати системи генерації ключів, спочатку коротко розглянемо потенційні атаки. Це пояснюється тим, що системи безпеки завжди супроводжуються атаками. Маючи на увазі атаки, читачі можуть краще зрозуміти вразливості різних підходів. Без втрати загальності використовуємо позначення, які зазвичай використовуються в цій галузі: Аліса та Боб представляють два легітимні пристрої, які прагнуть згенерувати один і той самий ключ, а Єва представляє зловмисника, який намагається отримати один і той самий ключ за допомогою різних типів атак. Метою Єви завжди є підрив системи сполучення пристроїв, і вона може розпочати атаки на автентичність, конфіденційність та цілісність. Зосередимося на деяких поширених атаках, таких як атака «людина посередині» (MITM), атака повторення, атака підслуховування. Ці атаки матимуть різний ступінь загрози для різних схем.

Рис. 3. Таксономія систем генерації ключів для IoT

Радіо/аудіо системи. Радіозв'язок використовується для обміну інформацією між пристроями. Водночас його також можна використовувати для генерації криптографічних ключів. Генерація ключів за допомогою радіозв'язку отримала значний інтерес в останні десятиліття [**Помилка! Джерело посилання не знайдено.**]. Залежно від розташування Аліси та Боба, генерацію ключів на основі радіозв'язку можна розділити на схеми на основі взаємності каналу та схеми на основі близькості, як показано на рис. 4.

ISSN 2663 - 4023



1. а) на основі взаємності каналу б) на основі близькості

Рис. 4. Модель системи для генерації ключів на основі радіо та аудіо

У схемі на основі взаємності каналу Аліса та Боб хочуть згенерувати той самий ключ зі свого спільного бездротового каналу та захистити ключ від підслуховування. Як показано на рис. 4.а, Аліса та Боб розташовані на певній відстані один від одного. Потім вони використовуватимуть взаємний канал між собою для генерації ключів.

Генерація ключів на основі радіозв'язку, яку також називають генерацією ключів фізичного рівня, спирається на три принципи, а саме: часову варіацію, взаємність каналу та просторову декореляцію:

- *Часова варіація* пов'язана з поширенням сигналу в часі і залежить від відбиття, заломлення та розсіювання. Ці зміні сигналу є непередбачуваними, а їх випадковість забезпечує формування криптографічних ключів з високою ентропією.
- *Взаємність каналу* визначається одної несучій частотою передачі сигналів, тобто вплив каналу на обох кінцях каналу буде взаємним. Ця особливість гарантує, що Аліса та Боб можуть отримувати висококорельовані вимірювання каналу та генерувати однакові ключі.
- *Просторова декореляція* проявляється, коли Єва знаходиться на відстані більше половини довжини хвилі від будь-якого з легітимних користувачів і вона відчуває некорельовані впливи каналу згідно з теорією зв'язку. Ця властивість є важливою для гарантії того, що ключі, згенеровані Алісою та Бобом, не можуть бути вгадані Євою, отже, ключі є безпечними.

Ці принципи були проаналізовані та підтверджені експериментально у [**Помилка! Джерело посилання не знайдено.**]. Типовий протокол генерації ключів на основі взаємності каналу складається з наступних чотирьох кроків: зондування каналу, квантування, узгодження інформації та посилення конфіденційності (рис. 5).

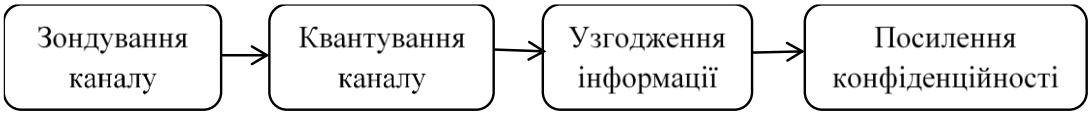


Рис. 5. Типовий протокол генерації ключів на основі взаємності каналів

Зондування каналу вимагає двонаправленої передачі між Алісою та Бобом. Зокрема, Аліса спочатку передає сигнал Бобу, який вимірює інформацію про канал за допомогою деяких параметрів каналу, наприклад, індикатору потужності прийнятого сигналу (*Received Signal Strength Indicator RSSI*), імпульсної характеристики каналу

(*Channel Impulse Response — CIR*) та частотної характеристики каналу (*Channel Frequency Response — CFR*). Потім Боб відповідає сигналом Алісі, яка вимірює той самий параметр. Це завершує пару вимірювань. Аліса та Боб продовжують зондування, доки не зберуть достатню кількість вимірювань.

Вибір параметра каналу залежить від прийнятих бездротових технологій. Хоча RSSI передбачено майже у всіх бездротових стандартах, CIR та CFR доступні лише в широкосмугових системах.

Квантування може виконуватися на основі середнього значення та стандартного відхилення.

Узгодження інформації використовується для того, щоб Аліса та Боб узгодили однакові ключі, чого можна досягти за допомогою кодів корекції помилок (*Error-Correcting Code — ECC*).

Посилення конфіденційності застосовується для зменшення загрози витоку інформації під час узгодження інформації. Це робиться за допомогою екстрактора, універсальних хеш-функцій або криптографічних хеш-функцій.

Після цього кроку генерація ключів завершується. Аліса та Боб отримують однаковий захищений ключ, і вони можуть використовувати цей ключ із симетричними алгоритмами шифрування, такими як AES-128, для захисту своїх подальших комунікацій.

З точки зору фізичного рівня, більша частина досліджень зосереджена на вдосконаленні зондування каналу або етапів квантування. Зондування каналу є ключовим елементом протоколів генерації ключів, який фіксує випадковість каналу шляхом вимірювання параметрів каналу.

Генерація ключів на основі взаємності каналів отримала широкий дослідницький інтерес і застосовувалася з кількома бездротовими технологіями, такими як ZigBee, Wi-Fi, LoRa [**Помилка! Джерело посилання не знайдено.**], [**Помилка! Джерело посилання не знайдено.**] тощо.

Підходи на основі близькості використовують властивість спільного розташування мобільних пристроїв для створення ключів, коли два пристрою фізично розташовані в одному місці, їх радіосигнали будуть дуже близькі один до одного (рис. 4, b).

Схеми, засновані на близькості, ґрунтуються на наступному спостереженні: якщо найближчий відправник переміщається дуже близько до однієї з антен приймача, приймач може спостерігати велику зміну показника, наприклад, *RSSI*, що приймається приймачем. Натомість, якщо далекий відправник наближається до одержувача, дві антени не побачать великої різниці RSSI [**Помилка! Джерело посилання не знайдено.**].

Підходи, що базуються на спільному розміщенні, використовують фізичну близькість для автентифікації пристроїв. Однак ці підходи мають спільну проблему: відстань між двома легітимними пристроями повинна бути близькою до кілька десятків сантиметрів [**Помилка! Джерело посилання не знайдено.**]. Отже, практичність таких підходів низька, оскільки бездротові приймачі вбудовані в мобільні пристрої, і в деяких сценаріях складно розмістити дві антени на такій короткій відстані.

Акустичні хвилі мають багато подібних властивостей до радіохвиль, таких як затухання, багатопроменеве поширення, відбиття та дифракція. Відповідно, значна частина існуючих робіт досліджувала, як використовувати аудіосигнали для сполучення пристроїв IoT. Так само, як і генерація ключів на основі радіо, більшість робіт можна розділити на два класи: на основі взаємності каналу та на основі близькості. Ідея схеми на основі близькості полягає в тому, що звук, записаний мікрофонами, не надто сильно відрізняється в межах близькості, але суттєво відрізняється, коли два пристрої

знаходяться далеко один від одного. В даний час мікрофони та динаміки інтегровані в багато пристроїв IoT, такі як смартфони, Google Assistant, Amazon Echo та ноутбуки.

Перші дослідження з перевірки взаємності акустичного каналу на діапазоні частот 18k-22kHz проведені в [**Помилка! Джерело посилання не знайдено.**], де автори впровадили на кількох смартфонах та оцінили його продуктивність у чотирьох середовищах: статичне середовище у приміщенні, мобільне середовище у приміщенні, статичне зовнішнє середовище та мобільне середовище на вулиці. Результати показали, що взаємність каналів для генерації ключів працює добре, коли два пристрою знаходяться на відстані не більше 60 см. Вони підтвердили випадковість згенерованих ключів, а також проаналізували безпеку від можливих атак.

Автори [**Помилка! Джерело посилання не знайдено.**] також запропонували систему узгодження ключів, засновану на взаємності акустичних каналів, де використовувала рівні звукового тиску як характеристики фізичного рівня акустичного каналу. У запропонованій системі прийнято звичайну процедуру генерації ключів для бездротової генерації ключів: зондування каналу, квантування, узгодження та посилення конфіденційності. Автори реалізували запропоновану систему на смартфоні Samsung Galaxy та провели оцінку у різних середовищах, включаючи класну кімнату, конференц-зал та коридор. Результати визначили можливість досягти швидкості генерації ключа 80 біт/с і коефіцієнта бітових помилок 25% до узгодження.

Система для встановлення загального криптографічного ключа працює в такий спосіб. По-перше, обидва пристрої повинні виконати метод синхронізації на основі протоколу мережного часу (*Network Time Protocol — NTP*), щоб встановити достатню синхронізацію. По-друге, обидва пристрої витягують двійкове уявлення записаного звуку, яке називається аудіовідбитком. Результати досліджень показали, що їхній протокол добре працює в офісному середовищі.

Основним обмеженням вищезгаданих систем є те, що обидва пристрої потребують точної синхронізації, що іноді нереально, особливо для пристроїв, які зустрічаються один з одним уперше. Для розв’язання цього обмеження в роботі [**Помилка! Джерело посилання не знайдено.**] наданий спосіб поєднання двох смарт-годинників заснований на ідеї двохфакторної автентифікації, коли два користувача обмінюються рукостисканням, що усуває вимогу синхронізації.

Робочий процес виглядає так. Процес сполучення запускається шляхом виявлення першого негативного піку під час процесу рукостискання. Спостереження полягає в тому, що сигнали прискорення, виміряні двома смарт-годинниками, повинні слідувати одній і тій же схемі і досягати піку майже в той самий час, коли дві руки щільно стиснуті. Система витягує послідовність двійкових ключів як із функцій часової області, і з функцій частотної області. Потім використовується двійковий код Голея для лінійної попередньої корекції помилок між двома розумними годинниками. Результати показали, що швидкість генерації бітів може досягти 13,4 біт/с, а ступень узгодженості ключів 96,7% для 128-бітного ключа.

В роботі [**Помилка! Джерело посилання не знайдено.**] наданий спосіб також заснований на близькості акустичного сигналу. Спосіб будується на ідеї, що відклик акустичного каналу є унікальним для даного пристрою в даному місці. Запропонована схема включає два основних кроки: двонаправлену початкову автентифікацію та узгодження ключа.

На першому кроці вони використовують час проходження акустичного сигналу між двома пристроями для автентифікації один одного. Зокрема, якщо інтервал часу

відповіді перевищує попередньо визначене порогове значення, пристрій вважатиметься зловмисником.

На другому кроці Аліса і Боб спочатку створюють характеристики акустичних каналів. Потім біти 1 і 0 кодуються в акустичному сигналі методом імпульсного кодування на основі синусоїдальної хвилі. Припустимо, що Аліса кодує послідовність бітів в акустичний сигнал і передає модульований сигнал Бобу. Боб може декодувати той самий симетричний ключ на основі відповіді акустичного каналу між Алісою та Бобом. Таким чином, і Аліса, і Боб встановлюють той самий ключ для захисту свого зв'язку. Результати оцінювання показали, що запропонована система може досягти високого рівня відповідності але при розтушуванні один до одного менше 3 см.

Датчики IMU (Inertial Measurement Unit) в пристроях IoT надають їм можливість збирати інформацію про навколишнє середовище. Датчики IMU — це інерційний вимірювальний пристрій, який вимірює та повідомляє питому силу тіла, кутову швидкість, а іноді й орієнтацію об'єкта, використовуючи комбінацію акселерометрів, гіроскопів і іноді магнітометрів. Серед цих типів датчиків акселерометр є найбільш широко використовуваним датчиком розробки системи сполучення пристроїв. Це пов'язано з тим, що він забезпечує хороше джерело ентропії для початкового завантаження безпечного каналу зв'язку в автономних та спонтанних взаємодіях між мобільними пристроями, які мають загальний контекст. Цей контекст зазвичай представляє собою повсякденну діяльність, таку як тряска, ходьба, жести тощо.

Останнім часом інтерес дослідників також приваблює іншу щоденну дію — рукостискання є звичайною практикою, коли дві людини зустрічаються, щоб висловити довіру та повагу. Перша ідея була запропонована та продемонстрована в [**Помилка! Джерело посилання не знайдено.**]. Результати оцінки показали, що рукостискання може генерувати 128-бітові ключі приблизно за 1 секунду з ймовірністю успіху більш 99%. Інша ідея сполучення на основі прискорення для наручних пристроїв за рахунок використання удосконаленої схеми запропоновано в [**Помилка! Джерело посилання не знайдено.**]. Але їхній результат було отримано шляхом моделювання, а не реалізації системи на реальних наручних пристроях.

Останніми роками дослідники виявили ще одну поширену повсякденну діяльність — ходьба, яку можна використовувати при генерації ключів. Хода відноситься до моделей ходьби людей. Як і інші біометричні дані, такі як обличчя та відбитки пальців, хода є біометричною характеристикою, і дослідження в галузі психології та біометрії показали, що у різних людей є відмінні та унікальні моделі ходьби. Отже, мобільні пристрої, надіті на тіло одного і того ж користувача, можуть вимірювати той самий шаблон ходи, в той час як пристрої на тілі іншого користувача мають різні вимірювання. Цей факт закладає основу схем генерації ключів з урахуванням ходьби [**Помилка! Джерело посилання не знайдено.**].

Системи генерації ключів на основі ходьби забезпечують автономний і спонтанний спосіб сполучення пристроїв, що носяться на тілі одного і того ж користувача. Недавнє дослідження показало, що в бінарних бітових рядках, що згенерували, є зміщення [**Помилка! Джерело посилання не знайдено.**]. Вони також вказали, що зловмисник може створити дуже схожий ключ за допомогою аналізу відео. На жаль, у літературі не було робіт, які могли б запобігти такого роду атакам. Тож це може бути цікавою темою майбутніх досліджень.

Крім рухів, описаних вище, інші рухи також використовуються для полегшення безпечного сполучення пристроїв. Синхронні жести, такі як удари, використовувалися для пар двох мобільних пристроїв, оснащених акселерометрами. Інтуїція полягає в тому,

що удари створюють рівні та протилежні сили жорсткого контакту, які одночасно сприймаються акселерометром. Отже, сигнал акселерометра може надати достатньо інформації, щоб визначити, чи взаємодіють два пристрої фізично чи ні.

Різне обладнання. Досягнення в мікроелектроніці, вбудованих системах та бездротових технологіях призвели до швидкого розвитку нових типів мініатюрних датчиків IoT, що, у свою чергу, створює багато нових можливостей для контекстного сполучення пристроїв IoT. Слід зазначити, що через різноманітність різного обладнання класифікуємо ці роботи на основі сигналу, який вони використовували для сполучення пристроїв.

Системи, що ґрунтуються на руханні, підтверджені на невеликому наборі даних у контрольованому середовищі. Однак інша фізіологічна біометрія людини, серцебиття, не має такої проблеми і було перевірено на великих наборах даних.

Традиційно біометрія — це метод, широко відомий як автоматична ідентифікація або верифікація особи за її фізіологічними або поведінковими характеристиками. У контексті генерації ключів біометричні ознаки використовуються як ключові матеріали для генерації випадкових ключів через такі ознаки: 1) відмінність, щоб ключі, згенеровані від різних суб'єктів, були різними; 2) часова мінливість та невразливість тобто змінюватися з часом та мати високий ступінь випадковості, щоб біометричні характеристики, записані в різний час, не генерували однаковий ключ, навіть якщо вони отримані від однієї й тієї ж особи.

Зокрема, дослідники виявили, що міжімпульсний інтервал (*Interpulse Interval — IPI*), тобто інтервал між піками сигналу серцебиття, є надзвичайно випадковим і може використовуватися як випадкове джерело для генерації ключів (рис. 6) [**Помилка! Джерело посилання не знайдено.**].

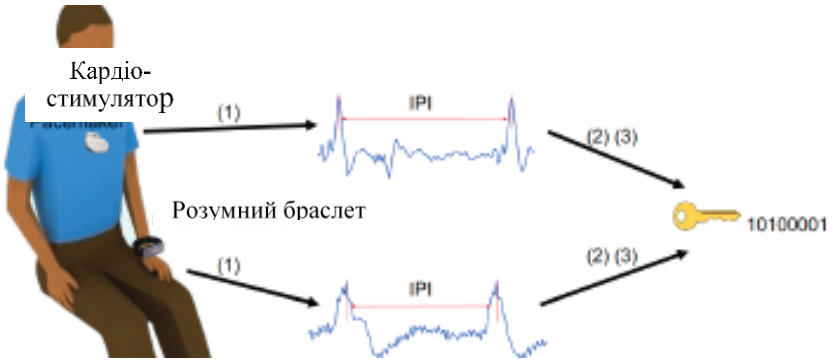


Рис. 6. Система генерації ключів на основі сигналу серцебиття

Запропонована система працює наступним чином. Спочатку біосенсори, розташовані в різних місцях тіла, фіксували серію IPI. Потім для досягнення кращої продуктивності накопичували кілька IPI, а потім виконували операцію по модулю для рандомізації монотонно зростаючих мульти-IPI для формування кінцевої двійкової послідовності. Однак, через обмежену ентропію джерела інформації, така схема не може досягти високої швидкості генерації ключів.

Згадані схеми сполучення пристроїв на основі ходьби використовують акселерометр для запису моделей ходьби користувача. Однак основною проблемою сенсорних систем на основі акселерометра є те, що безперервна вибірка акселерометра швидко розряджає акумулятор пристроїв IoT з обмеженими ресурсами. Щоб вирішити цю проблему, нещодавня тенденція полягає у використанні пристроїв збору кінетичної енергії (*Kinetic Energy Harvesting — KEH*) для заміни акселерометра. KEH — це процес перетворення руху та вібрацій в електричну енергію для живлення електронних

пристроїв. Діяльність людини є найважливішими джерелами, оскільки носимі пристрої можуть збирати енергію безпосередньо від діяльності користувача. Тому КЕН є перспективною технологією для застосувань у носимих та імплантованих датчиках, де використання батарей недоцільне [**Помилка! Джерело посилання не знайдено.**].

Для сполучення двох смартфонів, що знаходяться поблизу, запропоновано систему на основі магнітометра з обміну показниками магнітних полів. Результати оцінки показали, що магнітометри двох смартфонів може сполучити два пристрої протягом 4,5 секунд з показником успішності понад 90% [**Помилка! Джерело посилання не знайдено.**].

З появою нових датчиків дослідники [**Помилка! Джерело посилання не знайдено.**] запропонували першу систему генерації ключів на основі п'єзоелектричних датчиків для натільних та імплантованих пристроїв. Ці датчики використовують п'єзоелектричний ефект для вимірювання змін тиску, прискорення, температури, деформації або сили шляхом їх перетворення в електричний заряд. Результати оцінки показали, що вони можуть поєднувати два пристрою, що носяться на тілі одного і того ж користувача з ймовірністю успіху 95,6%. Аналіз безпеки також показав їх стійкість до пасивних та активних атак.

Камери. Використовуючи переваги камер у пристроях, дослідники розробили багато підходів до генерації ключів. Оскільки камери є практично у всіх смартфонах, дослідники розробили безліч підходів до генерації ключів, які використовують переваги камер у пристроях. Пристрій із однією камерою може сфотографувати двовимірний штрих-код, який кодує криптографічний ключ іншого пристрою. Змінивши ролі і повторивши вищеописаний процес, обидва пристрою можуть досягти автентифікованого обміну ключами. Порівняння цієї схеми з іншими системами обміну ключами, які використовують інші канали, такі як ультразвук, аудіо тощо, показує, що вона безпечніша і зручніша у використанні, оскільки користувач може візуально визначити сполучений пристрій. Однак вона має кілька обмежень. Наприклад, обидва пристрої повинні бути оснащені камерою для взаємної автентифікації. Крім того, ці підходи вимагають взаємодії людини з смартфоном для полегшення процесу сполучення пристроїв.

Гібридні підходи. Вищезазначені контекстно-орієнтовані підходи до сполучення покращують ефективність сполучення пристроїв IoT, усуваючи будь-яке втручання людини в сполучення. Використовуючи вбудовані датчики з однаковими способами сприйняття, можна фіксувати певний фізичний фон, такий як характеристики фізичного рівня одного бездротового каналу, сигнал руху одного користувача та навколишній звук від однієї й тієї ж події. Тим не менш, через гетерогенність пристроїв IoT, у деяких сценаріях непрактично припускати, що всі пристрої мають спільний спосіб сприйняття. Це обмеження спонукає до деяких нових досліджень, спрямованих на сполучення гетерогенних пристроїв IoT, використовуючи різні способи сприйняття.

До цієї підкатегорії належіть контекстно-орієнтований протокол сполучення з нульовою взаємодією для носимих пристроїв, використовуючи навколишній звук та освітленість. Система використовує контекстні відбитки пальців для розробки згенерованого ключа, що можливо лише тоді, коли два пристрої знаходяться поблизу один одного протягом тривалого періоду часу. Інтуїтивно, це базується на тому факті, що пристрої, що належать одному користувачеві, можуть спостерігати подібну контекстну інформацію протягом тривалішого часу, ніж інші пристрої. Ці схеми не передбачають взаємодії з користувачем, але для накопичення достатньої ентропії для завершення автентифікації потрібен тривалий час.

Інша контекстно-орієнтована схема сполучення для пристроїв IoT, оснащених різними типами датчиків, використовує час як спільний фактор для різних типів датчиків. Вона створює відбитки подій, які можна порівнювати на різних пристроях IoT, зосереджуючись на часі події, а не на даних окремих датчиків подій. Принцип полягає в тому, що пристрої, розташовані всередині фізично захищеного простору (наприклад, розумний дім), зможуть виявляти більш типові події з часом, на відміну від сторонніх. Результати оцінки показали, що легітимні пристрої в одній кімнаті можуть досягти середньої подібності відбитків пальців 94,9%, тоді як зовнішній зловмисник може досягти лише 68,9% подібності.

Крім того, деякі інші системи використовують різні комбінації модальностей датчиків для сполучення пристроїв. Наприклад, розроблено система автентифікації, використовуючи комбінацію чотирьох різних модальностей датчиків, а саме: температури навколишнього середовища, прецизійного газу, вологості та висоти.

Схеми генерації ключів з використанням мультимодального зондування мають дві переваги. З одного боку, їх можна використовувати для сполучення гетерогенних пристроїв IoT, які мають різні датчики, форми та розміри. З іншого боку, це підвищує безпеку схем сполучення від зловмисників, оскільки вимагає від зловмисника одночасного моніторингу різних властивостей фізичного середовища. Водночас, вони також мають деякі недоліки. По-перше, такі схеми можуть зайняти багато часу для завершення сполучення пристроїв, оскільки частота деяких подій низька. По-друге, через гетерогенність даних датчиків, метод обробки зазвичай є більш складним і дорогим, оскільки сигнали, виміряні в різних просторах станів датчиків, неможливо безпосередньо порівняти.

Загалом, система генерації ключів на основі радіо є хорошим вибором, оскільки вона досягає високої стійкості, зручності використання, практичності та повсюдності. Хоча рівень безпеки такої системи є середнім через широкомовний характер бездротового радіозв’язку.

Системи на основі аудіо мають низьку дальність передачі та залежать від мікрофона та динаміка, які не завжди доступні на пристроях IoT. Тому зручність використання та практичність є відносно низькими.

Зручність використання схем на основі датчиків IMU низька, оскільки вони також вимагають від користувачів виконання певних дій, таких як ходьба, струшування, удари, для створення загальної контекстної інформації. Але їхня практичність висока завдяки широкій доступності датчиків IMU на сучасних пристроях IoT.

Системи на основі різних датчиків, через їхню залежність від спеціального обладнання, мають низьку зручність використання, практичність та повсюдність. Однак, безпека, у свою чергу, виграє від цих недоліків. Це пояснюється тим, що сигнали таких різних датчиків, як біометричні дані користувача, зазвичай важко скопіювати, виготовити, імітувати та підслухати. Подібно до різних датчиків, підходи до багатомодальних датчиків також мають низьку зручність використання, практичність та повсюдність.

3. Атаки та контрзаходи протидії для вирішення проблем безпеки.

Через відкритий характер бездротового зв’язку, здатність зловмисника спостерігати за пристроями та витік інформації по бічних каналах, існують різні атаки на систему генерації ключів IoT. Через різноманітність апаратного забезпечення та принципів проєктування різні системи генерації ключів стикаються з багатьма атаками. Тому зосереджуємося лише на атаках, з якими стикається більшість систем генерації ключів.

Атака підслуховування є одним із типових підходів до атаки в бездротових мережах. Вона отримала значну увагу, оскільки багато атак з боку противника часто слідують за діяльністю підслуховування. Зловмисник, Єва, може просто знаходитися десь на шляху поширення та підслуховувати весь відповідний мережевий трафік для подальшого аналізу. Отже, це легко виконати та важко виявити.

У протоколі генерації ключів Алісі та Бобу часто потрібно обмінюватися деякою інформацією, щоб виправити невідповідності між їхніми початковими ключами (узгодженням інформації). Тож Єва може підслуховувати цю інформацію та використовувати її для підвищення рівня успіху. Існує два способи вирішення цієї проблеми: розробити протокол генерації ключів, який не обмінюється жодною інформацією; протокол генерації ключів повинен гарантувати, що Єва все одно не зможе відновити правильний ключ навіть за умови обміну інформацією.

Атака на передбачуваний канал означає, що зловмисники можуть навмисно виконувати деякі регулярні дії, щоб спричинити передбачувані зміни в отриманому сигналі легітимних пристроїв. Виявлено, що більшість систем генерації ключів на основі RSSI страждають від такої атаки. Нещодавно дослідники виявили, що CSI може протидіяти цій атаці, оскільки вона може витягувати інформацію про канал з різних піднесучих, а рух зловмисника має різний вплив на різні піднесучі. Щоб протидіяти передбачуваній атаці каналу для системи генерації ключів на основі RSSI, дослідники запропонували різноманітні методи, вводячи різні види випадковості в канали, такі як використання кількох антен, обертання антен, передача випадкових сигналів та інші схеми.

Під час *атаки імітації* Єва має можливість спостерігати, як користувач ходить, трясеться та рухається. Потім вона може повторити дії користувача з метою генерації подібного сигналу, щоб вона могла витягти той самий ключ. Атака імітації є серйозною загрозою для систем генерації ключів на основі руху, оскільки рухи користувача легко спостерігати та імітувати.

Традиційно вважається, що біометричні дані користувача важко скопіювати та підробити. Однак нещодавні дослідження показали, що зловмисники можуть зламати систему автентифікації на основі біометики, генеруючи дуже схожі біометричні дані. Синтетичні сигнали ЕКГ дуже близькі до ЕКГ доброякісного користувача, а рівень успішності злому сягає 81%. Тобто ця технологія явно становить загрозу для систем генерації ключів на основі ЕКГ.

Щоб пом’якшити атаку імітації, потрібно використовувати сигнали від кількох датчиків. Єві важко отримати подібні сигнали від різних датчиків шляхом підслуховування та імітації. Але вартість та практичність використання багатомодального зондування викликають занепокоєння.

Атаки по боковому каналу можливі з використанням запропонованої технології відновлення звуку з відео. За допомогою цієї технології зловмисники можуть зламати системи генерації ключів на основі вібрації або акустики. Недавні дослідження також показали, що відео можна використовувати для відновлення даних про рухи людей. Таким чином, схеми генерації ключів на основі руху або вібрації є вразливими до атаки відеоаналізу. Для захисту від таких атак одним із рішень є введення випадкового сигналу в процес генерації ключів. Іншим можливим рішенням є запозичення ідеї з системи розпізнавання облич із системою виявлення живості. Мета виявлення живості полягає у визначенні того, чи є обличчя «живим», чи це просто шахрайське відтворення. Таким чином, завдяки включенню виявлення активності, система генерації ключів може захистити від таких атак, коли вони відтворюють подібний сигнал з інформації побічного каналу.

В системах генерації ключів використовуються три метрики порівняння:

- *Швидкість створення ключів (Key Generation Rate — KGR),* яка виміряє кількість бітів за одиницю часу, яку може генерувати система. Вона вказує, як швидко система генерації ключів може генерувати або оновлювати ключі. Для процесу генерації ключів у реальному часі бажаний високий KGR.
- *Швидкість узгодження ключів (Key Agreement Rate — KAR)*, яка означає кількість узгоджених бітів по відношенню до загальної кількості згенерованих бітів. Високий показник успіху чи KAR може значно підвищити ефективність протоколу сполучення пристроїв. В ідеалі він має бути однаковим для двох законних пристроїв і найменшим для зловмисника.
- *Випадковість ключа* має першорядне значення у криптографічному протоколі, оскільки ключ із низькою ентропією може бути легко зламаний зловмисником.

У системі пари пристроїв випадковість згенерованих ключів оцінюється за допомогою популярного набору тестів NIST (*National Institute of Standards and Technology*). Набір тестів NIST надає 15 тестів з метою оцінки різних функцій випадковості. Наприклад, метою частотного (монобітного) тесту є оцінка частки нулів та одиниць у ключовій послідовності. Мета рангового тесту двійкової матриці — перевірити наявність лінійної залежності між рядками фіксованої довжини в рядку двійкового ключа.

4. Апаратні модулі безпеки та довірені платформи.

Довірені обчислення, засновані на апаратному корені довіри, були розроблені галуззю для захисту обчислювальної інфраструктури та мільярдів кінцевих вузлів IoT. Застосування апаратних модулів безпеки (*Hardware Security Module — HSM*) є одним з ефективних контрзаходів забезпечення безпеки IoT.

Використання HSM дозволяє зберігати та генерувати ключі безпечним способом. HSM повинен виконувати різні завдання безпеки: підписання, перевірку підпису, шифрування, дешифрування або хешування, а також безпечне зберігання та генерацію довірених випадкових чисел. Коротше кажучи, HSM забезпечує кореневу платформу довіри. У цьому сенсі HSM пропонують рішення, яке спирається на: генерацію випадкових чисел з високою ентропією; захист від несанкціонованого доступу, забезпечуючи безпечне зберігання закритих криптоключів та конфіденційної інформації; тим самим перешкоджаючи фізичним атакам; резервне копіювання та відновлення ключів.

Для забезпечення економічно ефективної архітектури безпеки існує щонайменше три різні варіанти HSM — повний, середній та легкий — кожен з яких зосереджений на різних варіантах використання безпеки з різними вимогами до вартості, функціональності та безпеки [].

Повний модуль забезпечує максимальний рівень функціональності, безпеки та продуктивності, застосовуючи, серед іншого, дуже потужний апаратно-прискорений асиметричний криптографічний структурний блок.

Середній модуль не має асиметричної криптографії в апаратному забезпеченні, він тим не менш здатний виконувати деякі некритичні за часом операції асиметричної криптографії (наприклад, протоколи обміну ключами), використовуючи внутрішній процесор та прошивку. Практично весь захист внутрішнього зв’язку базується на симетричних криптографічних алгоритмах.

Легкий модуль здатний виконувати суворі вимоги до вартості та ефективності. Порівняно з середнім модулем, легкий модуль містить лише апаратно-прискорений симетричний криптографічний механізм, апаратний генератор випадкових чисел, годинник світового координованого часу разом з деякими дуже невеликими додатковими енергозалежними та енергонезалежними модулями пам’яті.

Модулі довіреної платформи (*Trusted Platform Modules — TPM*), як підгрупи пристроїв HSM, забезпечують певну поведінку та захищають систему від несанкціонованих змін і атак, таких як шкідливе програмне забезпечення. Дійсно, ключі, згенеровані в пристрої, не можуть бути вилучені за межі TPM. Отже, дані, захищені цими ключами, не будуть розкриті. У цьому сенсі TPM забезпечує корінь довіри.

TPM визначається як апаратний пристрій, що включає енергозалежне та енергонезалежне сховище даних, а також набір криптографічних алгоритмів, реалізованих в апаратному забезпеченні. Крім того, різні стандарти TPM включають специфікацію API для взаємодії. Коротше кажучи, TPM — це апаратний компонент, який забезпечує безпечне зберігання криптографічно захищених даних (ключів, сертифікатів, паролів та інших даних, пов’язаних з внутрішніми механізмами TPM) та дозволяє генерувати ключі всередині TPM за допомогою TRNG [**Помилка! Джерело посилання не знайдено.**], шифрування з приватним/відкритим ключем та операцій підпису.

На рис. 7 показано архітектуру пристрою TPM2.0 [**Помилка! Джерело посилання не знайдено.**], де різні компоненти з’єднані між собою загальною шиною, яка також підключається до інтерфейсу вводу/виводу. Окрім вищезгаданого TRNG та енергонезалежної пам’яті, де розташовані регістри конфігурації платформи, існують інші важливі модулі, такі як механізми симетричних та асиметричних ключів, а також механізм генерації ключів.

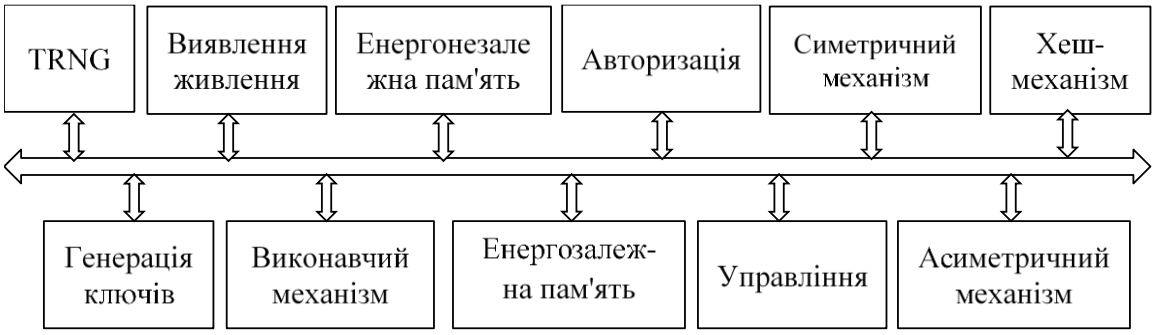


Рис. 7. Архітектура модуля довіреної платформи TPM2.0

Крім того, процес шифрування/дешифрування даних в TPM виконуються за допомогою ключа даного TPM. Використання апаратного TPM — це підхід, який дозволяє уникнути більшості видів атак.

У контексті кібербезпеки, особливо для IoT, високий рівень випадковості є важливим для захисту криптографічних протоколів. Квантові обчислення створюють значні ризики для традиційних методів шифрування. Щоб вирішити ці проблеми, в [**Помилка! Джерело посилання не знайдено.**] запропоновано квантово-безпечне рішення для обчислень, довірених IoT. Зокрема, реалізовано практична інтеграція квантового генератора випадкових чисел (*Quantum Random Number Generator — QRNG*) TPM для створення прототипу квантового модуля довіреної платформи (*Quantum Trusted Platform Module — QTPM*) для систем IoT з метою покращення криптографічних

можливостей. Запропонована структура квантової ентропії як послуги (*Quantum Entropy as a Service — QEaaS*) ще більше розширює доступ квантової ентропії до застарілих пристроїв IoT з обмеженими ресурсами.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Загалом, система генерації ключів на основі радіо є хорошим вибором, оскільки вона досягає високої стійкості, зручності використання, практичності та повсюдності. Хоча рівень безпеки такої системи є середнім через широкомовний характер бездротового радіозв'язку.

Системи на основі аудіо мають низьку дальність передачі та залежать від мікрофона та динаміка, які не завжди доступні на пристроях IoT. Тому зручність використання та практичність є відносно низькими.

Зручність використання схем на основі датчиків IMU низька, оскільки вони також вимагають від користувачів виконання певних дій, таких як ходьба, струшування, удари, для створення загальної контекстної інформації. Але їхня практичність висока завдяки широкій доступності датчиків IMU на сучасних пристроях IoT.

Системи на основі різних датчиків, через їхню залежність від спеціального обладнання, мають низьку зручність використання, практичність та повсюдність. Однак, безпека, у свою чергу, виграє від цих недоліків. Це пояснюється тим, що сигнали таких різних датчиків, як біометричні дані користувача, зазвичай важко скопіювати, виготовити, імітувати та підслухати. Подібно до різних датчиків, підходи до багатомодальних датчиків також мають низьку зручність використання, практичність та повсюдність.

Таким чином, різні системи генерації ключів мають різні рівні вразливості до атак. Дослідники повинні розглянути потенційні атаки, особливо ті, які використовують витік інформації по побічному каналу. Крім того, всі дослідження зосереджені на розробці нових систем генерації ключів, але дуже мало робіт було зроблено для аналізу вразливостей існуючих систем. Деякі складні дослідження важко провести, але вони мають велику цінність [**Помилка! Джерело посилання не знайдено.**].

Комплексна безпека вузлів IoT повинна захищати рівномірно від усіх загроз. Вкрай важливо використовувати випробувану методологію — генерування, зберігання та використовування криптографічних ключів протягом усього циклу їх життя в зашифрованому вигляді і в захищеному обладнанні, тобто апаратних модулях безпеки HSM та модулях довіреної платформи TPM . Апаратні модулі HSM та TPM забезпечують виконання всіх операцій шифрування і розшифрування даних всередині модулю, тобто криптографічні ключі не залишають захищений периметр модулю.

Перевагами апаратних засобів захисту мережі IoT є: апаратний спосіб формування випадкових послідовностей; методологія апаратних модулів безпеки та довірених платформ — виконання криптографічних операцій в середовищі захищених криптографічних мікросхем (безпека на кристалі); розмежування та розвантажування функцій центрального процесора вузла IoT за допомогою спеціалізованого криптопроцесора для виконання криптографічних перетворень; гарантування цілісності криптографічних перетворень даних; підвищення швидкості криптографічних перетворень даних. Ці переваги визначили розвиток апаратних засобів захисту IoT: вбудованих генераторів випадкових послідовностей та криптографічних ключів, криптографічних прискорювачів (криптоакселераторів) та криптографічних модулів у

мікропроцесорних комплектах загального призначення [**Помилка! Джерело посилання не знайдено.**].

Наряду з розглянутими досягненнями систем генерації ключів IoT є проблеми подальшого дослідження у цьому напрямку.

Генерація ключів в сценаріях низької взаємності каналів залишається відкритою проблемою дослідження. Дослідження генерації ключів 5G все ще спирається на моделювання, а практичні системи генерації ключів ще не розроблені. Ці нові комунікаційні технології створюють не лише виклики, а й нові можливості.

Більшість існуючих систем генерації ключів працюють в режимі однорангового зв'язку. Дослідження систем групової генерації ключів показує, що вони страждають або від проблем ефективності, або від практичності. Традиційні протоколи генерації парних ключів не можна безпосередньо розширити до сценаріїв генерації групових ключів. Це пов'язано з тим, що секретна інформація між парою легітимних пристроїв не може бути ефективно та безпечно поширена на інші пристрої IoT. Тому питання про те, як розробити ефективний і практичний протокол генерації групового ключа, залишається відкритим.

Користувач відіграє вирішальну роль у деяких системах генерації ключів, таких як введення випадковості шляхом струшування або ходьби, порівняння результатів. Тобто, як розробити швидку та практичну систему генерації ключів з невеликою залученістю користувача, вимагає подальшого дослідження.

Теоретична та практична підтримка досліджень ґрунтуються на теоретичному аналізі та моделюванні оцінки, тоді як багато інших досліджень ґрунтуються на реальних вимірюваннях з використанням стандартного обладнання. Лише невелика частина досліджень у літературі містить як теоретичний аналіз, так і практичну перевірку [**Помилка! Джерело посилання не знайдено.**]. Тому потрібна ретельна робота над теоретичними і практичними перевірками систем генерування криптографічних ключів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Bala, D. Q., & Raman, B. (2020). PHY-based key agreement scheme using audio networking. *2020 International Conference on Communication Systems & Networks (COMSNETS)*, Bengaluru, India, 129–136. https://doi.org/10.1109/COMSNETS48256.2020.9027340
2. Bala, D. Q., Raman, B., Anees, A., & Chen, Y.-P. P. (2018). Discriminative binary feature learning and quantization in biometric key generation. *Pattern Recognition, 77,* 289–305.
3. Bansal, S., & Kumar, D. (2020). IoT ecosystem: A survey on devices, gateways, operating systems, middleware and communication. *International Journal of Wireless Information Networks, 27*(4), 1–25. https://doi.org/10.1007/s10776-020-00483-7
4. Bruesch, A., Le, N., Schürmann, D., Sigg, S., & Wolf, L. C. (2019). Security properties of gait for mobile device pairing. *IEEE Transactions on Mobile Computing, 19*(3).
5. Bruesch, A., Nguyen, L., Schürmann, D., Sigg, S., & Wolf, L. C. (2019). Security properties of gait for mobile device pairing. *IEEE Transactions on Mobile Computing, 19*(3). https://doi.org/10.1109/TMC.2019.2897933
6. Cabrera-Gutierrez, A. J., Castill, E., Escobar-Molero, A., Álvarez-Bermejo, J. A., Morales, D. P., & Parrilla, L. (2022). Integration of hardware security modules and permissioned blockchain in industrial IoT networks. *IEEE Access,* 10, 114331–114345. https://doi.org/10.1109/ACCESS.2022.3217815
7. Cheng, Q., Hsu, C., & Harn, L. (2020). Lightweight noninteractive membership authentication and group key establishment for WSNs. *Mathematical Problems in Engineering, 2020,* 1–9.
8. Dammak, M., Senouci, S. M., Messous, M. A., Elhdhili, M. H., & Gransart, C. (2020). Decentralized lightweight group key management for dynamic access control in IoT environments. *IEEE Transactions on Network and Service Management, 17*(3), 1742–1757.

9. Fomichev, M., Álvarez, F., Steinmetzer, D., Gardner-Stephen, P., & Hollick, M. (2017). Survey and systematization of secure device pairing. *IEEE Communications Surveys & Tutorials, 20*(1), 517–550.
10. Frustaci, M., Pace, P., Aloi, G., & Fortino, G. (2018). Evaluating critical security issues of the IoT world: Present and future challenges. *IEEE Internet of Things Journal, 5,* 2483–2495. https://ieeexplore.ieee.org/document/8086136
11. Furtak, J. (2020). Cryptographic keys generating and renewing system for IoT network nodes: A concept. *Sensors, 20*(17), 5012. https://doi.org/10.3390/s20175012
12. Furtak, J., Zieliński, Z., & Chudzikiewicz, J. (2019). A framework for constructing a secure domain of sensor nodes. *Sensors, 19*(12), 2797. https://www.mdpi.com/1424-8220/19/12/2797
13. Han, J., Chung, A. J., Sinha, M. K., Harishankar, M., Pan, S., Noh, H. Y., Zhang, P., & Tague, P. (2018). Do you feel what I hear? Enabling autonomous IoT device pairing using different sensor types. *2018 IEEE Symposium on Security and Privacy (SP),* San Francisco, CA, USA, 836–852. IEEE.
14. Jiang, Q., Huang, X., Zhang, N., Zhang, K., Ma, X., & Ma, J. (2019). Shake to communicate: Secure handshake acceleration-based pairing mechanism for wrist-worn devices. *IEEE Internet of Things Journal, 6*(3), 5618–5630.
15. Klimushyn, P., Solianyk, T., Mozhaiev, O., Gnusov, Y., Manzhai, O., & Svitlychny, V. (2022). Crypto-resistant methods and random number generators in Internet of Things (IoT) devices. *Innovative Technologies and Scientific Solutions for Industries, 2*(20), 22–34. https://doi.org/10.30837/ITSSI.2022.20.022
16. Li, G., Zhang, Z., Zhang, J., & Hu, A. (2020). Encrypting wireless communications on the fly using one-time pad and key generation. *IEEE Internet of Things Journal.* https://doi.org/10.1109/JIOT.2020.3004451
17. Li, Z., Pei, Q., Markwood, I., Liu, Y., & Zhu, H. (2018). Secret key establishment via RSS trajectory matching between wearable devices. *IEEE Transactions on Information Forensics and Security, 13,* 802–817. https://doi.org/10.1109/TIFS.2017.2768020
18. Lin, Q., Xu, W., Lan, G., Cui, Y., Jia, H., Hu, W., Hassan, M., & Seneviratne, A. (2020). KEHKey: Kinetic energy harvester-based authentication and key generation for body area network. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies, 4*(1), 1–26.
19. Lin, Q., Xu, W., Liu, J., Khamis, A., Hu, W., Hassan, M., & Seneviratne, A. (2019). H2B: Heartbeat-based secret key generation using piezo vibration sensors. *Proceedings of the 18th International Conference on Information Processing in Sensor Networks,* Montreal, Quebec, Canada, 265–276. ACM.
20. Lu, Y., Wu, F., Tang, S., Kong, L., & Chen, G. (2019). FREE: A fast and robust key extraction mechanism via inaudible acoustic signal. *Proceedings of the 20th ACM International Symposium on Mobile Ad Hoc Networking and Computing*, Catania, Italy, 311–320. ACM.
21. Moara-Nkwe, K., Shi, Q., Lee, G. M., & Eiza, M. H. (2018). A novel physical layer secure key generation and refreshment scheme for wireless sensor networks. *IEEE Access, 6,* 11374–11387. https://doi.org/10.1109/ACCESS.2018.2806423
22. Piccoli, A., Pahl, M.-O., Fries, S., & Sel, T. (2020). Ensuring consistency for asynchronous group-key management in the industrial IoT. *Proceedings of the 16th International Conference on Network and Service Management (CNSM),* Izmir, Turkey, 1–5. https://doi.org/10.23919/CNSM50824.2020.9269080
23. Pierson, T. J., Liang, X., Peterson, R., & Kotz, D. (2016). Wanda: Securely introducing mobile devices. *Proceedings of IEEE INFOCOM 2016,* San Francisco, CA, USA, 1–9. IEEE.
24. Prantl, T., Prantl, D., Bauer, A., Iffländer, L., Dmitrienko, A., Kounev, S., & Krupitzer, C. (2021). Benchmarking of pre- and post-quantum group encryption schemes with focus on IoT. *Proceedings of the IEEE International Performance, Computing, and Communications Conference (IPCCC),* 1–10.
25. Prantl, T., Zeck, T., Bauer, A., Ten, P., Prantl, D., Yahya, A. E. B., Iffländer, L., Dmitrienko, A., Krupitzer, C., & Kounev, S. (2022). A survey on secure group communication schemes with focus on IoT communication. *IEEE Access, 10,* 99944–99962. https://doi.org/10.1109/ACCESS.2022.3206451
26. Ruotsalainen, H., Zhang, J., & Grebeniuk, S. (2020). Experimental investigation on wireless key generation for low power wide area networks. *IEEE Internet of Things Journal, 7*(3), 1745–1755.
27. Samiullah, F., Gan, M.-L., Akleylek, S., & Aun, Y. (2023). Group key management: A systematic literature review. *IEEE Access, 11,* 77464–77491. https://doi.org/10.1109/ACCESS.2023.3298024
28. Shang, J., & Wu, J. (2020). AudioKey: A usable device pairing system using audio signals on smartwatches. *International Journal of Security and Networks, 15*(1), 46–58.
29. Shen, Y., Yang, F., Du, B., Xu, W., Luo, C., & Wen, H. (2018). Shake-n-Shack: Enabling secure data exchange between smart wearables via handshakes. *2018 IEEE International Conference on Pervasive Computing and Communications (PerCom),* 1–10. IEEE.

30. Sudarsono, A., Yuliana, M., Kristalina, P., & Barakbah, A. R. (2018). An implementation of shared key generation extracted from received signal strength in vehicular ad-hoc communication. *Proceedings of the 2018 Sixth International Symposium on Computing and Networking (CANDAR)*, Takayama, Japan, 57–65.
31. Tian, Y., Wang, Z., Xiong, J., & Ma, J. (2020). A blockchain-based secure key management scheme with trustworthiness in DWSNs. *IEEE Transactions on Industrial Informatics, 16*, 6193–6202. https://doi.org/10.1109/TII.2020.2965975
32. Wang, Q., Kang, M., Wu, G., Ren, Y., & Su, C. (2020). A practical secret key generation scheme based on wireless channel characteristics for 5G networks. *IEICE Transactions on Information and Systems, 103*(2), 230–238.
33. Wu, Y., Lin, Q., Jia, H., Hassan, M., & Hu, W. (2020). Auto-Key: Using autoencoder to speed up gait-based key generation in body area networks. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies, 4*(1), 1–23.
34. Xi, W., Qian, C., Han, J., Zhao, K., Zhong, S., Li, X.-Y., & Zhao, J. (2016). Instant and robust authentication and key agreement among mobile devices. *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, Vienna, Austria, 616–627. ACM.
35. Xie, P., Feng, J., Cao, Z., & Wang, J. (2018). GeneWave: Fast authentication and key agreement on commodity mobile devices. *IEEE/ACM Transactions on Networking, 26*(4), 1688–1700.
36. Xu, G., Adetifa, O., Mao, J., Sakk, E., & Wang, S. (2025). Developing quantum trusted platform module (QTPM) to advance IoT security. *Future Internet, 17*(5), 193. https://doi.org/10.3390/fi17050193
37. Xu, W., Jha, S., & Hu, W. (2019). LoRa-Key: Secure key generation system for LoRa-based network. *IEEE Internet of Things Journal, 6*(4), 6404–6416.
38. Xu, W., Zhang, J., Huang, S., Luo, C., & Li, W. (2022). Key generation for Internet of Things: A contemporary survey. *ACM Computing Surveys, 14*, 1–37. https://doi.org/10.1145/3429740
39. Yuliana, M., Wirawan, & Suwadi. (2019). A simple secret key generation by using a combination of pre-processing method with a multilevel quantization. *Entropy, 21*, 192. https://doi.org/10.3390/e21020192
40. Yuliana, M., Wirawan, & Suwadi. (2019). An efficient key generation for the Internet of Things based synchronized quantization. *Sensors, 19*(12). https://doi.org/10.3390/s19122674
41. Yuliana, M., Wirawan, & Suwadi. (2019). Performance analysis of loss level quantization on the secret key generation scheme in indoor wireless environment. *International Journal of Advanced Science, Engineering and Information Technology, 9*, 100–108. https://doi.org/10.18517/ijaseit.9.1.7583
42. Zhan, F., Yao, N., Gao, Z., & Yu, H. (2018). Efficient key generation leveraging wireless channel reciprocity for MANETs. *Journal of Network and Computer Applications, 103*, 18–28. https://doi.org/10.1016/j.jnca.2017.11.014
43. Zhang, J., Ding, M., López-Pérez, D., Marshall, A., & Hanzo, L. (2019). Design of an efficient OFDMA-based multi-user key generation protocol. *IEEE Transactions on Vehicular Technology, 68*(9), 8842–8852.
44. Zhang, J., Li, G., Marshall, A., Hu, A., & Hanzo, L. (2020). A new frontier for IoT security emerging from three decades of key generation relying on wireless channels. *IEEE Access, 8*, 138406–138446. https://doi.org/10.1109/ACCESS.2020.3012006
45. Zhang, J., Rajendran, S., Sun, Z., Woods, R., & Hanzo, L. (2019). Physical layer security for the Internet of Things: Authentication and key generation. *IEEE Wireless Communications, 26*(5), 92–98.
46. Zhang, J., Wang, Z., Yang, Z., & Zhang, Q. (2017). Proximity-based IoT device authentication. *Proceedings of IEEE INFOCOM 2017*, Atlanta, GA, USA, 1–9. IEEE.
47. Zhang, J., Woods, R., Duong, T. Q., Marshall, A., Ding, Y., Huang, Y., & Xu, Q. (2016). Experimental study on key generation for physical layer security in wireless communications. *IEEE Access, 4*, 4464–4477.
48. Klimushyn, P. S. (2025). Communication technologies and specialised communication protocols for ensuring cybersecurity of the Internet of Things. *Law and Safety, 2*(97), 52–68. https://doi.org/10.32631/pb.2025.2.05
49. Klimushyn, P. S. (2025). Problematic aspects of IoT cybersecurity standardisation. *Law and Safety, 1*(96), 53–66. https://doi.org/10.32631/pb.2025.1.05
50. Klimushyn, P., Svitlychnyi, V., Gnusov, Y., & Onyshchenko, Y. (2025). Automotive electronics and cybersecurity: A systematic review of security attacks and countermeasures. *Cybersecurity: Education, Science, Technology, 4*(28), 115–136. https://doi.org/10.28925/2663-4023.2025.28.760

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (29), 2025
ISSN 2663 - 4023

Petro Klimushyn
PhD, Associate Professor of the Department of Counteracting Cybercrime
Kharkiv National University of Internal Affairs, Kharkiv, Ukraine
ORCID ID: 0000-0002-1020-9399
klimushyn@ukr.net

Maksym Khruslov
PhD, Senior Researcher, Associate Professor,
Head of the Department of Electronics and Control Systems
Kharkiv National University named after Karazin
ORCID ID: 0000-0001-9639-9340
maksym.khruslov@karazin.ua

Yuriy Gnusov
PhD, Associate Professor,
Head of the Department of Cybersecurity and DATA-Technologies
Kharkiv National University of Internal Affairs, Kharkiv, Ukraine
ORCID ID: 0000-0002-9017-9635
duke6969@i.ua

Vadym Maltsev
Teacher of the Department of Counteracting Cybercrime
Kharkiv National University of Internal Affairs, Kharkiv, Ukraine
ORCID ID: 0000-0003-0214-8976
alan.kast.95@gmail.com

CRYPTOGRAPHIC KEY GENERATION SYSTEMS FOR SECURITY MODULES WITH HARDWARE SUPPORT OF IOT DEVICES

Abstract. The Internet of Things (IoT) is a very large source of both data and many vulnerabilities. In this regard, the issue of security arises for protecting the resources of IoT nodes and the data they exchange. This process is complicated by the insufficiency of the resources of these nodes in terms of computing power, memory size, energy resources, range and wireless connection performance. IoT devices can be deployed in critical environments where any information leakage to an interceptor or unauthorized penetration into the network can become a serious security threat, especially in the Internet of Military Things and Medical Things. In such networks, cryptographic methods are mainly used to ensure security. Here, the primary task is to generate cryptographic keys for IoT devices interacting with each other. Generating one common (session) key for both parties allows the use of symmetric encryption algorithms. To distribute these keys, public-key cryptography (asymmetric cryptography) can be used, which is too computationally complex and energy-intensive to run on resource-constrained IoT devices. A pressing task for implementing secure technologies and security rules in the IoT network is the task of generating and updating symmetric cryptographic keys with high entropy. Along with this, to simplify the system of exchange of cryptographic keys in the IoT network, the main issue is the secure delivery of new key data and key update during exchange. Most of the proposed key generation strategies are applied based on the physical layer of IoT for general wireless environments. The study provides a new taxonomy of key generation systems for IoT with a classification of approaches by hardware, which demonstrates the fundamental difference in the interaction of IoT devices by components: radio, audio, cameras, IMU sensors with inertial measurement units, various hardware and hybrid approaches. With this taxonomy, users can easily identify the most suitable method for their application scenarios. IoT physical layer-based key generation has received extensive research interest and has been applied with several wireless technologies such as Wi-Fi, ZigBee, LoRa/LoRaWAN, etc.

Keywords: hardware support for IoT devices; cryptographic keys; key generation systems; data encryption; symmetric and asymmetric cryptography; IoT device authentication; attacks; eavesdropping; on the intended channel; on the side channel and imitation.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Bala, D. Q., & Raman, B. (2020). PHY-based key agreement scheme using audio networking. *2020 International Conference on Communication Systems & Networks (COMSNETS)*, Bengaluru, India, 129–136. https://doi.org/10.1109/COMSNETS48256.2020.9027340
2. Bala, D. Q., Raman, B., Anees, A., & Chen, Y.-P. P. (2018). Discriminative binary feature learning and quantization in biometric key generation. *Pattern Recognition, 77*, 289–305.
3. Bansal, S., & Kumar, D. (2020). IoT ecosystem: A survey on devices, gateways, operating systems, middleware and communication. *International Journal of Wireless Information Networks, 27*(4), 1–25. https://doi.org/10.1007/s10776-020-00483-7
4. Bruesch, A., Le, N., Schürmann, D., Sigg, S., & Wolf, L. C. (2019). Security properties of gait for mobile device pairing. *IEEE Transactions on Mobile Computing, 19*(3).
5. Bruesch, A., Nguyen, L., Schürmann, D., Sigg, S., & Wolf, L. C. (2019). Security properties of gait for mobile device pairing. *IEEE Transactions on Mobile Computing, 19*(3). https://doi.org/10.1109/TMC.2019.2897933
6. Cabrera-Gutierrez, A. J., Castill, E., Escobar-Molero, A., Álvarez-Bermejo, J. A., Morales, D. P., & Parrilla, L. (2022). Integration of hardware security modules and permissioned blockchain in industrial IoT networks. *IEEE Access*, 10, 114331–114345. https://doi.org/10.1109/ACCESS.2022.3217815
7. Cheng, Q., Hsu, C., & Harn, L. (2020). Lightweight noninteractive membership authentication and group key establishment for WSNs. *Mathematical Problems in Engineering, 2020*, 1–9.
8. Dammak, M., Senouci, S. M., Messous, M. A., Elhdhili, M. H., & Gransart, C. (2020). Decentralized lightweight group key management for dynamic access control in IoT environments. *IEEE Transactions on Network and Service Management, 17*(3), 1742–1757.
9. Fomichev, M., Álvarez, F., Steinmetzer, D., Gardner-Stephen, P., & Hollick, M. (2017). Survey and systematization of secure device pairing. *IEEE Communications Surveys & Tutorials, 20*(1), 517–550.
10. Frustaci, M., Pace, P., Aloi, G., & Fortino, G. (2018). Evaluating critical security issues of the IoT world: Present and future challenges. *IEEE Internet of Things Journal, 5*, 2483–2495. https://ieeexplore.ieee.org/document/8086136
11. Furtak, J. (2020). Cryptographic keys generating and renewing system for IoT network nodes: A concept. *Sensors, 20*(17), 5012. https://doi.org/10.3390/s20175012
12. Furtak, J., Zieliński, Z., & Chudzikiewicz, J. (2019). A framework for constructing a secure domain of sensor nodes. *Sensors, 19*(12), 2797. https://www.mdpi.com/1424-8220/19/12/2797
13. Han, J., Chung, A. J., Sinha, M. K., Harishankar, M., Pan, S., Noh, H. Y., Zhang, P., & Tague, P. (2018). Do you feel what I hear? Enabling autonomous IoT device pairing using different sensor types. *2018 IEEE Symposium on Security and Privacy (SP)*, San Francisco, CA, USA, 836–852. IEEE.
14. Jiang, Q., Huang, X., Zhang, N., Zhang, K., Ma, X., & Ma, J. (2019). Shake to communicate: Secure handshake acceleration-based pairing mechanism for wrist-worn devices. *IEEE Internet of Things Journal, 6*(3), 5618–5630.
15. Klimushyn, P., Solianyk, T., Mozhaiev, O., Gnusov, Y., Manzhai, O., & Svitlychny, V. (2022). Crypto-resistant methods and random number generators in Internet of Things (IoT) devices. *Innovative Technologies and Scientific Solutions for Industries, 2*(20), 22–34. https://doi.org/10.30837/ITSSI.2022.20.022
16. Li, G., Zhang, Z., Zhang, J., & Hu, A. (2020). Encrypting wireless communications on the fly using one-time pad and key generation. *IEEE Internet of Things Journal.* https://doi.org/10.1109/JIOT.2020.3004451
17. Li, Z., Pei, Q., Markwood, I., Liu, Y., & Zhu, H. (2018). Secret key establishment via RSS trajectory matching between wearable devices. *IEEE Transactions on Information Forensics and Security, 13*, 802–817. https://doi.org/10.1109/TIFS.2017.2768020
18. Lin, Q., Xu, W., Lan, G., Cui, Y., Jia, H., Hu, W., Hassan, M., & Seneviratne, A. (2020). KEHKey: Kinetic energy harvester-based authentication and key generation for body area network. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies, 4*(1), 1–26.
19. Lin, Q., Xu, W., Liu, J., Khamis, A., Hu, W., Hassan, M., & Seneviratne, A. (2019). H2B: Heartbeat-based secret key generation using piezo vibration sensors. *Proceedings of the 18th International Conference on Information Processing in Sensor Networks*, Montreal, Quebec, Canada, 265–276. ACM.
20. Lu, Y., Wu, F., Tang, S., Kong, L., & Chen, G. (2019). FREE: A fast and robust key extraction mechanism via inaudible acoustic signal. *Proceedings of the 20th ACM International Symposium on Mobile Ad Hoc Networking and Computing*, Catania, Italy, 311–320. ACM.

21. Moara-Nkwe, K., Shi, Q., Lee, G. M., & Eiza, M. H. (2018). A novel physical layer secure key generation and refreshment scheme for wireless sensor networks. *IEEE Access, 6,* 11374–11387. https://doi.org/10.1109/ACCESS.2018.2806423
22. Piccoli, A., Pahl, M.-O., Fries, S., & Sel, T. (2020). Ensuring consistency for asynchronous group-key management in the industrial IoT. *Proceedings of the 16th International Conference on Network and Service Management (CNSM)*, Izmir, Turkey, 1–5. https://doi.org/10.23919/CNSM50824.2020.9269080
23. Pierson, T. J., Liang, X., Peterson, R., & Kotz, D. (2016). Wanda: Securely introducing mobile devices. *Proceedings of IEEE INFOCOM 2016*, San Francisco, CA, USA, 1–9. IEEE.
24. Prantl, T., Prantl, D., Bauer, A., Iffländer, L., Dmitrienko, A., Kounev, S., & Krupitzer, C. (2021). Benchmarking of pre- and post-quantum group encryption schemes with focus on IoT. *Proceedings of the IEEE International Performance, Computing, and Communications Conference (IPCCC)*, 1–10.
25. Prantl, T., Zeck, T., Bauer, A., Ten, P., Prantl, D., Yahya, A. E. B., Iffländer, L., Dmitrienko, A., Krupitzer, C., & Kounev, S. (2022). A survey on secure group communication schemes with focus on IoT communication. *IEEE Access, 10,* 99944–99962. https://doi.org/10.1109/ACCESS.2022.3206451
26. Ruotsalainen, H., Zhang, J., & Grebeniuk, S. (2020). Experimental investigation on wireless key generation for low power wide area networks. *IEEE Internet of Things Journal, 7*(3), 1745–1755.
27. Samiullah, F., Gan, M.-L., Akleylek, S., & Aun, Y. (2023). Group key management: A systematic literature review. *IEEE Access, 11,* 77464–77491. https://doi.org/10.1109/ACCESS.2023.3298024
28. Shang, J., & Wu, J. (2020). AudioKey: A usable device pairing system using audio signals on smartwatches. *International Journal of Security and Networks, 15*(1), 46–58.
29. Shen, Y., Yang, F., Du, B., Xu, W., Luo, C., & Wen, H. (2018). Shake-n-Shack: Enabling secure data exchange between smart wearables via handshakes. *2018 IEEE International Conference on Pervasive Computing and Communications (PerCom)*, 1–10. IEEE.
30. Sudarsono, A., Yuliana, M., Kristalina, P., & Barakbah, A. R. (2018). An implementation of shared key generation extracted from received signal strength in vehicular ad-hoc communication. *Proceedings of the 2018 Sixth International Symposium on Computing and Networking (CANDAR)*, Takayama, Japan, 57–65.
31. Tian, Y., Wang, Z., Xiong, J., & Ma, J. (2020). A blockchain-based secure key management scheme with trustworthiness in DWSNs. *IEEE Transactions on Industrial Informatics, 16,* 6193–6202. https://doi.org/10.1109/TII.2020.2965975
32. Wang, Q., Kang, M., Wu, G., Ren, Y., & Su, C. (2020). A practical secret key generation scheme based on wireless channel characteristics for 5G networks. *IEICE Transactions on Information and Systems, 103*(2), 230–238.
33. Wu, Y., Lin, Q., Jia, H., Hassan, M., & Hu, W. (2020). Auto-Key: Using autoencoder to speed up gait-based key generation in body area networks. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies, 4*(1), 1–23.
34. Xi, W., Qian, C., Han, J., Zhao, K., Zhong, S., Li, X.-Y., & Zhao, J. (2016). Instant and robust authentication and key agreement among mobile devices. *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, Vienna, Austria, 616–627. ACM.
35. Xie, P., Feng, J., Cao, Z., & Wang, J. (2018). GeneWave: Fast authentication and key agreement on commodity mobile devices. *IEEE/ACM Transactions on Networking, 26*(4), 1688–1700.
36. Xu, G., Adetifa, O., Mao, J., Sakk, E., & Wang, S. (2025). Developing quantum trusted platform module (QTPM) to advance IoT security. *Future Internet, 17*(5), 193. https://doi.org/10.3390/fi17050193
37. Xu, W., Jha, S., & Hu, W. (2019). LoRa-Key: Secure key generation system for LoRa-based network. *IEEE Internet of Things Journal, 6*(4), 6404–6416.
38. Xu, W., Zhang, J., Huang, S., Luo, C., & Li, W. (2022). Key generation for Internet of Things: A contemporary survey. *ACM Computing Surveys, 14,* 1–37. https://doi.org/10.1145/3429740
39. Yuliana, M., Wirawan, & Suwadi. (2019). A simple secret key generation by using a combination of pre-processing method with a multilevel quantization. *Entropy, 21,* 192. https://doi.org/10.3390/e21020192
40. Yuliana, M., Wirawan, & Suwadi. (2019). An efficient key generation for the Internet of Things based synchronized quantization. *Sensors, 19*(12). https://doi.org/10.3390/s19122674
41. Yuliana, M., Wirawan, & Suwadi. (2019). Performance analysis of loss level quantization on the secret key generation scheme in indoor wireless environment. *International Journal of Advanced Science, Engineering and Information Technology, 9,* 100–108. https://doi.org/10.18517/ijaseit.9.1.7583
42. Zhan, F., Yao, N., Gao, Z., & Yu, H. (2018). Efficient key generation leveraging wireless channel reciprocity for MANETs. *Journal of Network and Computer Applications, 103,* 18–28. https://doi.org/10.1016/j.jnca.2017.11.014
43. Zhang, J., Ding, M., López-Pérez, D., Marshall, A., & Hanzo, L. (2019). Design of an efficient OFDMA-based multi-user key generation protocol. *IEEE Transactions on Vehicular Technology, 68*(9), 8842–8852.

44. Zhang, J., Li, G., Marshall, A., Hu, A., & Hanzo, L. (2020). A new frontier for IoT security emerging from three decades of key generation relying on wireless channels. *IEEE Access, 8*, 138406–138446. https://doi.org/10.1109/ACCESS.2020.3012006
45. Zhang, J., Rajendran, S., Sun, Z., Woods, R., & Hanzo, L. (2019). Physical layer security for the Internet of Things: Authentication and key generation. *IEEE Wireless Communications, 26*(5), 92–98.
46. Zhang, J., Wang, Z., Yang, Z., & Zhang, Q. (2017). Proximity-based IoT device authentication. *Proceedings of IEEE INFOCOM 2017,* Atlanta, GA, USA, 1–9. IEEE.
47. Zhang, J., Woods, R., Duong, T. Q., Marshall, A., Ding, Y., Huang, Y., & Xu, Q. (2016). Experimental study on key generation for physical layer security in wireless communications. *IEEE Access, 4*, 4464–4477.
48. Klimushyn, P. S. (2025). Communication technologies and specialised communication protocols for ensuring cybersecurity of the Internet of Things. *Law and Safety*, *2*(97), 52–68. https://doi.org/10.32631/pb.2025.2.05
49. Klimushyn, P. S. (2025). Problematic aspects of IoT cybersecurity standardisation. *Law and Safety, 1*(96), 53–66. https://doi.org/10.32631/pb.2025.1.05
50. Klimushyn, P., Svitlychnyi, V., Gnusov, Y., & Onyshchenko, Y. (2025). Automotive electronics and cybersecurity: A systematic review of security attacks and countermeasures. *Cybersecurity: Education, Science, Technology, 4*(28), 115–136. https://doi.org/10.28925/2663-4023.2025.28.760