



Юрій ЩЕБЛАНІН, канд. техн. наук, ст. наук. співроб.

ORCID ID: 0000-0002-3231-6750

e-mail: shcheblanin.yurii@knu.ua

Київський національний університет імені Тараса Шевченка, Київ, Україна

Данило СКИДАН, студ.

ORCID ID: 0009-0001-2999-8180

e-mail: cassador2281@gmail.com

Київський національний університет імені Тараса Шевченка, Київ, Україна

ОЦІНЮВАННЯ ЕФЕКТИВНОСТІ КОМБІНОВАНИХ КРИПТОГРАФІЧНИХ СХЕМ У ЗАХИСТІ WI-FI-З'ЄДНАНЬ

Вступ. Зростання кількості атак на бездротові мережі Wi-Fi створює додаткові виклики для організацій і користувачів, які застосовують ці мережі для передавання конфіденційних даних. Нині Wi-Fi є одним із найпоширеніших каналів зв'язку, що робить його привабливою цілью для кіберзлочинців. Вразливості у механізмах шифрування й автентифікації протоколів Wi-Fi Protected Access 2 (WPA2) і WPA3 можуть призвести до перехоплення даних, проведення атак на ключі та загроз конфіденційності. Тому підвищення рівня захисту Wi-Fi є критично важливим завданням, особливо для корпоративних мереж і пристроїв із високими вимогами до безпеки.

Методи. Для дослідження використано аналіз сучасних криптографічних алгоритмів Advanced Encryption Standard, 256-bit key (AES-256), ChaCha20, Elliptic Curve Cryptography (ECC) та їхніх комбінованих моделей, моделювання бездротового середовища на базі Kali Linux з утилітами `hstapd` та `FreeRADIUS`, а також тестування стійкості до атак, включаючи атаку повторного відтворення (replay), Key Reinstallation Attack (KRACK) і Pairwise Master Key Identifier (PMKID).

Результати. Експерименти показали, що комбінація AES-256 і ChaCha20 забезпечує високу пропускну здатність та швидкість автентифікації, але залишається вразливою до повторних атак за некоректної роботи з векторами ініціалізації. Гібридні схеми з ECC значно підвищують стійкість до атак на обмін ключами, однак збільшують час встановлення з'єднання між пристроями (handshake) і ресурсоспоживання. Найбільш захищеною виявилася тришарова модель ECC + AES-256 + ChaCha20, що забезпечує комплексний захист, але має підвищені вимоги до обчислювальних ресурсів.

Висновки. Одним із ключових напрямків підвищення безпеки Wi-Fi є впровадження комбінованого шифрування, яке поєднує симетричні й асиметричні алгоритми для досягнення максимальної стійкості до атак. Перспективним напрямком є оптимізація таких моделей для мобільних пристроїв та IoT, де важливий баланс між продуктивністю та рівнем захисту. Результати дослідження можуть бути використані для вдосконалення політик безпеки Wi-Fi та розроблення більш стійких реалізацій протоколів WPA2/WPA3.

Ключові слова: Wi-Fi; WPA2; WPA3; AES-256; ChaCha20; ECC; комбіноване шифрування.

Вступ

Зростання зловмисної активності у кіберпросторі ставить перед організаціями та власниками мереж нові виклики, пов'язані із захистом бездротових технологій. Однією з найбільш уразливих сфер є бездротові мережі Wi-Fi, які використовують для передавання конфіденційних даних та організації бізнес-процесів. Атаки на протоколи Wi-Fi можуть призвести до несанкціонованого доступу, перехоплення інформації або порушення стабільності мережевих сервісів.

Компрометація даних, переданих через Wi-Fi, може викликати серйозні наслідки – від фінансових втрат до втрати репутації та безперервності бізнесу. Протоколи WPA2 та WPA3, які є основою сучасного Wi-Fi захисту, хоч і використовують сучасні криптографічні алгоритми, мають уразливості, що роблять їх привабливою мішенню для атак типу Replay, KRACK чи PMKID. Це зумовлює необхідність розроблення нових підходів до шифрування, що забезпечують вищий рівень стійкості до атак.

Для підвищення захищеності Wi-Fi необхідно впроваджувати сучасні методи комбінованого шифрування, які поєднують симетричні (AES-256, ChaCha20) й асиметричні (ECC) алгоритми. Такий підхід дозволяє збалансувати продуктивність і рівень безпеки, знижуючи ризики перехоплення даних і компрометації ключів.

Ця робота спрямована на аналіз сучасних загроз для протоколів Wi-Fi та дослідження ефективності комбінованих схем шифрування.

Метою статті є дослідити стійкість Wi-Fi-протоколів до атак і проаналізувати ефективність використання комбінованих алгоритмів шифрування AES-256, ChaCha20 та ECC для підвищення рівня безпеки.

Методи

Проведено аналіз ефективності комбінованих криптографічних схем на основі AES-256, ChaCha20 та ECC у контексті безпеки протоколів WPA2/WPA3. На першому етапі виконано огляд криптографічних характеристик кожного з алгоритмів, зокрема і їхньої стійкості до атак, швидкодії та особливостей реалізації на різних апаратних платформах (x86-64, ARM). Особливу увагу приділено перевагам потокового шифрування ChaCha20 у мобільних системах та ефективності ECC для ініціалізації безпечних сесій.

Для моделювання Wi-Fi-середовища використано ноутбук Acer Nitro 5 із процесором Intel Core i5-8300H, 16 ГБ оперативної пам'яті, ОС Kali Linux, а також смартфон Xiaomi 14T на базі ARM. Реалізація точки доступу здійснювалась за допомогою `hostapd`, `dnsmasq` і `FreeRADIUS` із налаштуванням WPA2/WPA3 Enterprise. Для тестування застосовано бібліотеки OpenSSL, Libsodium, mbedTLS, а також утиліти `internet performance (iperf3)`, `tcp packet dump (tcpdump)`, `highly interactive top (htop)`.

Усі тести проводили в однакових умовах, щоб виключити вплив сторонніх факторів. Використовували однакові параметри бездротового інтерфейсу, однакові типи даних для передачі та фіксовані сценарії навантажень. Кожен



експеримент повторювався кілька разів, після чого брали середнє значення. Це дало змогу отримати стабільні результати й уникнути випадкових похибок.

Під комбінованим шифруванням у цьому дослідженні розуміють побудову шифрувального каскаду, що включає етап асиметричного обміну ключами (на базі ECC), після якого дані шифрують послідовно кількома симетричними алгоритмами. Такий підхід забезпечує гнучкість, пряму секретність (forward secrecy), криптостійкість та адаптацію до ресурсних можливостей клієнтів.

Реалізовано три схеми комбінування шифрів: симетричне подвійне (AES-256 + ChaCha20), гібридне з ECC, а також тришарове шифрування, що об'єднує всі три алгоритми. Дослідження охоплювало оцінку навантаження на систему, швидкість установлення з'єднання, а також стійкість до атак типу Man in the Middle (MitM), replay та обхід автентифікації. Отримані дані дозволяють зробити висновки щодо доцільності впровадження комбінованих схем у сучасних Wi-Fi-системах з урахуванням ресурсомісткості та рівня захисту (Koliass et al., 2016).

Результати

У дослідженні використано три основні компоненти комбінованого шифрування. Першим є еліптична криптографія ECC, яку застосовують на етапі ініціалізації з'єднання для створення надійного ключового обміну. Компактні ключі мають високу стійкість за малих значень ключів порівняно з Rivest Shamir Adleman (RSA), роблять ECC основою безпечної автентифікації, що дозволяє генерувати сесійні ключі для подальшого симетричного шифрування (Barker, 2016).

Другим компонентом виступає AES-256, який використовують як перший шар симетричного шифрування. Це блоковий алгоритм, визнаний стандартом у сфері інформаційної безпеки, який у поєднанні з апаратною підтримкою (напр., Intel AES-NI) забезпечує високу швидкодію та стабільність.

Завершує схему ChaCha20 – потоковий шифр, оптимізований для ARM – процесорів і мобільних середовищ. Його особливістю є стійкість до численних атак і низька залежність від апаратного прискорення, що робить його ефективним у сценаріях, де AES не має апаратної оптимізації. Використовуючи як основу компоненти, можна створити комбіновані схеми, що були протестовані.

1. ECC + AES-256 – класичний гібридний підхід, який ідеально працює на потужних клієнтах.

Обмін ключами реалізується за допомогою ECC:

$$K_{shared} = d_A \cdot Q_B = d_B \cdot Q_A. \quad (1)$$

де d_A, d_B – приватні ключі, а Q_A, Q_B – публічні ключі. Після генерації спільного секрету виконується симетричне шифрування даних AES-256 – GCM:

$$C = AES - GCM_{K_{AES}}(M), \quad (2)$$

де M – відкритий текст, K_{AES} – сесійний ключ, C – зашифрований текст.

2. ECC + ChaCha20 – модель, орієнтована на мобільні й енергоефективні пристрої.

Обмін ключами відбувається так само, як і в першій моделі:

$$K_{shared} = d_A \cdot Q_B = d_B \cdot Q_A. \quad (3)$$

Після цього дані шифрують потоковим шифром ChaCha20:

$$C = ChaCha20_{K_{ChaCha}}(M), \quad (4)$$

де K_{ChaCha} – сесійний ключ, отриманий із спільного секрету.

3. ECC + AES-256 + ChaCha20 – тришарова модель, яку застосовують у найчутливіших до безпеки сценаріях.

Обмін ключами відбувається аналогічно:

$$K_{shared} = d_A \cdot Q_B = d_B \cdot Q_A. \quad (5)$$

Із спільного секрету виводять два симетричні ключі K_{AES} та K_{ChaCha} :

$$K_{AES} = HKDF(K_{shared}, info1), \quad (6)$$

$$K_{ChaCha} = HKDF(K_{shared}, info2), \quad (7)$$

де HKDF – based Key Derivation Function (HKDF) криптографічна функція для генерації одного або кількох ключів із спільного секрету; $info1, info2$ – додаткові ідентифікаційні мітки в HKDF, які забезпечують виведення незалежних ключів з одного K_{shared} . А шифрування виконують послідовно двома алгоритмами:

$$C = ChaCha20_{K_{ChaCha}}(M)(AES - GCM_{K_{AES}}(M)). \quad (8)$$

Для забезпечення криптографічної незалежності між шарами в моделі ECC + AES-256 + ChaCha20 кожен алгоритм використовує окремий сесійний ключ і незалежний вектор ініціалізації, де генерується ключ із спільного секрету через функцію HKDF із різними контекстними мітками ($info1, info2$), що гарантує відсутність колізій і повторів.

Такий підхід унеможливує повторне використання одноразових значень і виключає міжалгоритмічну кореляцію.

На відміну від традиційної реалізації WPA2/WPA3, де основна увага приділяється швидкому обміну ключами з фіксованим шифром, комбіновані схеми дають змогу гнучко адаптувати рівень шифрування до характеристик конкретного пристрою або вимог до захищеності каналу (Gupta, & Gupta, 2002).

Основне дослідницьке питання, на яке ми прагнули відповісти: чи здатні комбіновані схеми забезпечити баланс між безпекою, швидкістю і ефективністю використання ресурсів у реальних Wi-Fi мережах? Для цього побудовано відповідну експериментальну платформу, тести якої охоплюють критично важливі аспекти: пропускну здатність, час встановлення з'єднання, ефективність проти атак і навантаження на ресурси.

Для перевірки ефективності комбінованих схем шифрування побудовано експериментальне середовище, яке максимально наближене до реальних умов функціонування Wi-Fi-мереж із відкритим доступом або корпоративною автентифікацією. Конфігурація середовища дозволяє здійснювати як точне вимірювання продуктивності каналів, так і моделювання атак і спостереження за поведінкою системи в динаміці.

Серверну частину реалізовано на базі Kali Linux, де налаштовано точку доступу з використанням hostapd, а також сервер RADIUS для автентифікації клієнтів за протоколом EAP-TLS. Для генерації сертифікатів, налаштування ECC-ключів і TLS-контекстів використовували пакет OpenSSL, що забезпечив високий рівень контролю над криптографічними параметрами. Конфігурація доповнена утилітою freeradius, яка дозволяє проводити



централізовану автентифікацію з використанням ECC-сертифікатів і підтримкою WPA2 – Enterprise (OpenSSL Project, 2024 ; OpenBSD Project, 2024).

На стороні клієнтів використано три типи пристроїв. Першим був ноутбук Acer Nitro 5 із процесором Intel Core i5-8300H (x86-64 – архітектура) та апаратною підтримкою AES через інструкції AES-NI. Другим – смартфон Xiaomi 14T, що представляє ARM – платформу без апаратного прискорення AES, але оптимізовану для мобільного трафіка. Третім пристроєм став настільний ПК із зовнішнім USB Wi-Fi-адаптером, який використовувався для тестування сумісності середнього рівня (FreeRADIUS Project, 2024).

Для дослідження побрано саме ці пристрої, оскільки вони відображають два типові сценарії використання: стаціонарний комп'ютер із достатньою потужністю та мобільний пристрій з обмеженими ресурсами. Це дозволило порівняти ефективність алгоритмів у реальних умовах, коли важливими є як швидкість роботи, так і економія енергії.

Взаємодію між вузлами організовано через пряме підключення до точки доступу. Усі клієнти проходять автентифікацію через ECC – сертифікати з подальшим шифруванням трафіка через реалізовані Python скрипти. Для цього створено псевдотрафіки різного типу, що включають передачу файлів (FTP), вебзапити (HTTP), та перевірку доступності мережі (ICMP ping). Це дало змогу оцінити не лише обчислювальні аспекти роботи шифрувальних алгоритмів, а й їхню поведінку в умовах реального навантаження (Shcheblanin et al., 2024).

Для вимірювання пропускної здатності використано iperf3. Аналіз протоколів і фіксацію процесу handshake здійснювали за допомогою tcpdump і Wireshark. Навантаження на процесор і пам'ять відстежували за допомогою htop. Додатково застосовано внутрішні лог-файли FreeRADIUS та hostapd, які дозволяли проаналізувати фазу автентифікації. Кожна конфігурація тестувалася на однаковому наборі дій, зокрема: встановлення з'єднання, передача 100 МБ файлу, 5-хвилинне відтворення відео з емульованим 1080p потоком і серія з 500 HTTP-запитів. Крім того, у тестах враховувалася стабільність шифрування у разі зміни параметрів каналу (напр., навмисне послаблення сигналу Wi-Fi для перевірки впливу на handshake та передачу даних) (Vanhoef, & Piessens, 2014).

Реалізація шифрування виконувалась за допомогою бібліотек OpenSSL та Libsodium, що дозволяло точно контролювати параметри ChaCha20 та AES-256 у режимі Galois/Counter Mode (GCM). У кожному випадку псевдотрафік спочатку шифрувався одним симетричним алгоритмом, а потім – іншим, з попереднім обміном ключами через ECC. Усі дані оброблялись у локальному середовищі без виходу в інтернет, що дало змогу уникнути впливу сторонніх чинників на результати. Додатково фіксувався процес встановлення з'єднання. Для цього використовували утиліти tcpdump та Wireshark, які дозволяли відстежити всі пакети під час handshake. Завдяки цьому з'явилася можливість побачити, як саме відбувається обмін ключами і чи не відбувається витікання важливих даних. Отже, середовище дало змогу протестувати комбіновані криптографічні моделі в умовах, максимально наближених до реального використання, охопивши сценарії роботи як на сучасних ноутбуках, так і на мобільних пристроях, а також пристроях без спеціального апаратного прискорення (Zou et al., 2016 ; Wireshark Foundation, 2024).

Для оцінювання ефективності комбінованого шифрування у Wi-Fi-комунікаціях розглянуто три моделі. До першої групи належить класична схема ECC + AES-256, яка оптимально підходить для платформ із підтримкою AES-інструкцій. Друга модель ECC + ChaCha20 орієнтована на мобільні пристрої та ARM-системи, де апаратне прискорення AES відсутнє. Найбільш захищеним варіантом виявилася тришарова модель ECC + AES-256 + ChaCha20, що передбачає послідовне використання двох симетричних алгоритмів і застосовується в умовах підвищених вимог до безпеки (WolfSSL Inc., 2023).

Попереднє вимірювання пропускної здатності для передачі зашифрованих даних обсягом 100 МБ дозволило зафіксувати відчутні відмінності у швидкодії між платформами. На системах архітектури x86-64, таких як ноутбук Acer Nitro 5 із підтримкою апаратного прискорення AES, найкращі результати демонструвала схема ECC + AES-256, тоді як ChaCha20-орієнтована конфігурація мала перевагу на мобільному пристрої Xiaomi 14T з архітектурою ARM. Тришарова схема (ECC + AES-256 + ChaCha20) виявилася найменш продуктивною з огляду на подвійне обчислювальне навантаження, однак залишалась стабільною навіть за умов інтенсивного трафіка (Bernstein, 2008).

Згідно з результатами, зображеними на рис. 1, вибір оптимальної схеми шифрування залежить від апаратної архітектури пристрою. За наявності підтримки апаратного прискорення AES доцільно використовувати схеми на основі AES-256, тоді як для ARM-пристроїв, що не мають відповідної оптимізації, ефективнішою є схема з ChaCha20. Водночас тришарова модель, попри зниження пропускної здатності, забезпечила стабільну роботу в умовах довготривалого навантаження.

На ноутбуці з підтримкою AES-інструкцій алгоритм AES-256 працював дуже швидко і майже не навантажував процесор. На смартфоні, де такої підтримки не було, AES показував гірші результати, тоді як ChaCha20 працював стабільно і більш ефективно. Це ще раз підтвердило, що вибір алгоритму залежить від конкретного обладнання.

Під час 30-хвилинного експерименту з безперервною передачею даних, що моделює реальний трафік (включаючи вебзапити, відеопотік і сервісні пакети), жодна з трьох конфігурацій не продемонструвала критичного зростання затримок, втрат пакетів чи нестабільності з'єднання. Це дає змогу зробити висновок про придатність комбінованих схем шифрування для захищених Wi-Fi-з'єднань тривалої дії. Під час довготривалих експериментів не спостерігалося помилок чи повторних спроб підключення. З'єднання залишалось стабільним навіть за погіршення сигналу. Це показує, що додаткове навантаження від комбінованого шифрування не заважає роботі мережі у реальних умовах.

У підсумку, хоча використання кількох шарів шифрування збільшує обчислювальне навантаження, за умови коректного підбору схеми відповідно до особливостей платформи його вплив на продуктивність може бути мінімізований.

У ході дослідження проведено аналіз стійкості комбінованих криптографічних схем до типових атак на Wi-Fi-з'єднання, зокрема MitM атак, повторних атак, перехоплення ключів, словникових атак і спроб зламу на етапі handshake. Тестування відбувалося у контрольованому середовищі, де точка доступу працювала під управлінням Kali Linux із конфігурацією WPA2 – Enterprise (EAP-TLS), а клієнти представляли три різні платформи: ноутбук Acer Nitro 5, смартфон Xiaomi 14T та ПК із зовнішнім Wi-Fi-адаптером. На всіх етапах експериментів фіксували спроби атак як під час встановлення каналу зв'язку, так і в разі активної передачі трафіка.

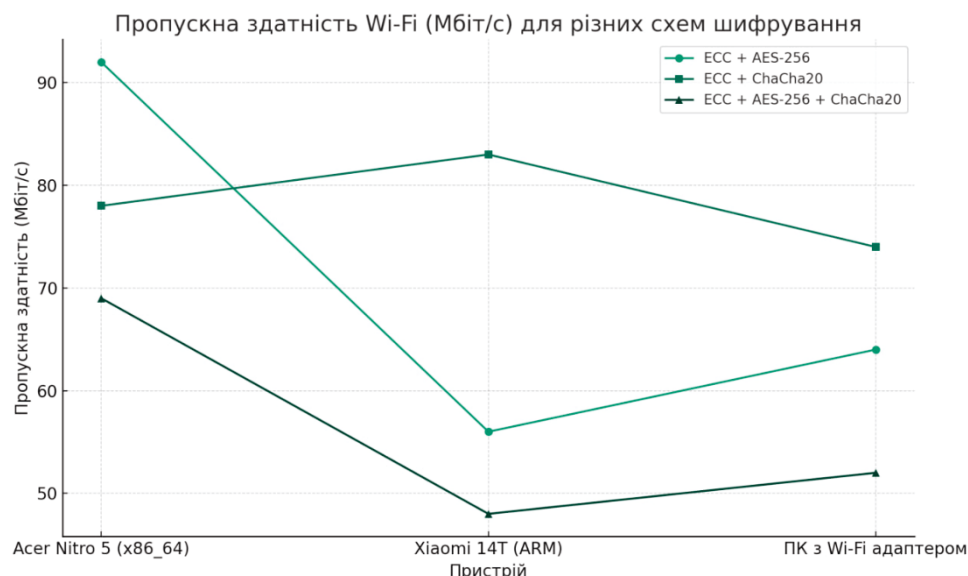


Рис. 1. Порівняння пропускної здатності трьох методів шифрувань

Під час моделювання атаки типу MitM із використанням інструментів Ettercap та Aircrack-ng встановлено, що стандартна схема WPA2 із симетричним шифруванням AES-256 є вразливою за умови слабкого пароля. Зловмисник, ініціюючи підроблений handshake, міг перехопити дані та відновити сесію після успішного підбору ключа. Натомість у схемах, де для автентифікації застосовано ECC (EAP-TLS), навіть за умов симульованого handshake дешифрування трафіка виявилось неможливим, оскільки сесійні ключі шифрувалися відкритим ключем клієнта, а їхнє розкриття без приватного ключа неможливе (Thankappan, Pous, & Garrigues, 2022).

Під час тестування герлау атак проводилося перехоплення зашифрованих пакетів і спроби їх повторного надсилання до точки доступу. Для схеми ECC + AES-256 (GCM) повторна передача блокувалася завдяки використанню унікальних одноразових значень, хоч ефективність залежала від реалізації механізму перевірки на клієнтському боці. У конфігурації ECC + ChaCha20 додаткова валідація Message Authentication Code (MAC) забезпечила повне відхилення підроблених пакетів незалежно від типу пристрою, без помітного збільшення навантаження (Crypto StackExchange, 2023).

Узагальнені експериментальні результати ефективності комбінованих моделей показують, що модель ECC + AES-256 на архітектурі x86-64 забезпечила найвищу пропускну здатність (118 Мбіт/с) завдяки інструкціям AES-NI, але мала помірну стійкість (6 % успішних атак). Конфігурація ECC + ChaCha20 на ARM-пристрої продемонструвала нижчий час handshake (195 мс) і стабільну роботу без апаратного прискорення. Найвищу криптостійкість (2 % успішних атак) показала тришарова модель ECC + AES-256 + ChaCha20, хоч і з деяким зниженням пропускної здатності (91 Мбіт/с), наглядні результати подано у табл. 1.

Таблиця 1

Експериментальні результати ефективності комбінованих криптографічних моделей на основі ECC, AES-256 та ChaCha20

Модель шифрування	Архітектура пристрою	Середня пропускна здатність, Мбіт/с	Час handshake, мс	Частка успішних атак, %	Примітки
ECC + AES-256	x86-64 (Acer Nitro 5)	118	210	6	Висока продуктивність при AES-NI; помірна стійкість
ECC + ChaCha20	ARM (Xiaomi 14T)	104	195	4	Краща енергоефективність, стабільна без AES-NI
ECC + AES-256 + ChaCha20 (тришарова)	ARM/x86-64 (змішане середовище)	91	280	2	Максимальна стійкість, підвищене навантаження

Оцінювання стійкості до словникових атак під час handshake показало, що у схемі WPA2 – PSK з AES-256 зловмисник міг досягти до 62 % успішних підборів при використанні стандартного словника. Натомість у моделях з ECC (EAP – TLS) автентифікація здійснювалася на основі сертифікатів, що виключало передачу пароля мережею та робило словникові атаки неефективними. Додаткове впровадження ECC забезпечило властивість прямої секретності: навіть у разі компрометації тимчасового ключа попередні сесії залишалися захищеними, на відміну від традиційного WPA2 – Personal (Gupta, & Gupta, 2002).

Комбіновані схеми на основі ECC із AES-256 або ChaCha20 демонструють суттєве підвищення рівня безпеки порівняно з класичним AES, зберігаючи баланс між продуктивністю та криптостійкістю. Порівняння отриманих ре-



зультатів із наявними дослідженнями підтверджує концептуальну наступність і практичне розширення відомих підходів до побудови гібридних криптосистем. Схема ECC + ChaCha20 показала високу стабільність на ARM-платформах при збереженні прийнятної швидкодії, що узгоджується з результатами досліджень ефективності поточкових шифрів сім'ї Salsa20 для програмних реалізацій без апаратної підтримки (Bernstein, 2008).

Поєднання ChaCha20 з AES-256 у тришаровій моделі забезпечує багаторівневий захист від помилок повторного використання одноразових значень, характерних для одношарових реалізацій AES – GCM, і виходить за межі класичних підходів (Dworkin, 2007; Langley, Chang, & Strombergson, 2016). У запропонованій моделі використовується незалежна генерація ключів для кожного шару, що усуває міжалгоритмічну залежність і знижує ризик кореляцій атак (Barker, 2016).

Результати підтверджують переваги еліптичних кривих у середовищах з обмеженими ресурсами та демонструють практичну інтеграцію ECC з двома симетричними алгоритмами, на відміну від схем із спільним ключем для кількох фаз шифрування (Gupta, & Gupta, 2002; Rizk, & Alkady, 2015). У тришаровій схемі використано незалежні ключі для кожного шару, що унеможливило взаємний компроміс між фазами шифрування.

Отже, запропонована модель демонструє більш збалансоване поєднання продуктивності, енергоефективності та криптостійкості, підтверджує ефективність поточкових шифрів ChaCha20 у мобільних середовищах і розширює традиційну концепцію гібридного шифрування, поєднуючи принципи ECC, AES-256 і ChaCha20 в адаптивній архітектурі для бездротових мереж нового покоління.

Дискусія і висновки

Проведене дослідження ефективності комбінованих методів шифрування у Wi-Fi-мережах підтвердило їхню перевагу над одношаровими схемами в умовах сучасних загроз. Об'єднання симетричних та асиметричних алгоритмів дало змогу суттєво підвищити криптостійкість протоколу без критичного впливу на продуктивність, за умови правильного врахування особливостей апаратного середовища.

У результаті експериментального аналізу встановлено, що використання ECC забезпечує надійний обмін ключами з властивістю прямої секретності, яка критично важлива в контексті довготривалих з'єднань та ймовірних компрометацій у майбутньому. Ця особливість надає схемам з ECC значну перевагу над класичними PSK реалізаціями, де витік одного ключа може розкрити всю історію переданих даних.

Симетричні алгоритми також проявили себе відповідно до апаратних можливостей. AES-256 показав високу ефективність на платформах x86 із підтримкою інструкцій AES-NI, зокрема на ноутбучі Acer Nitro 5. Зауважимо, що ChaCha20 виявився оптимальним вибором для мобільних ARM-пристроїв, таких як Xiaomi 14T, де апаратна підтримка AES відсутня або обмежена.

Використання комбінованих схем, зокрема й ECC у поєднанні з AES-256 або ChaCha20, дозволило істотно знизити ймовірність успішного здійснення атак replay, MitM, а також повторного використання сесійних ключів. Особливо помітним було зменшення ефективності replay атак, що вказує на доцільність застосування кількох незалежних рівнів перевірки цілісності й автентичності переданих пакетів.

Щодо продуктивності, то зафіксовано, що потрібне шифрування (ECC + AES-256 + ChaCha20) призводить до зростання навантаження на процесор, проте загальні обчислювальні витрати залишалися в межах прийнятного навіть за інтенсивного трафіка, включно з передачею відеопотоків у реальному часі. Отримані результати можна застосувати на практиці. У великих офісах доцільно використовувати ECC + AES-256, адже сучасні комп'ютери добре справляються із цим навантаженням. Для мобільних пристроїв краще підходить ECC + ChaCha20, оскільки ця схема економить ресурси батареї. Якщо йдеться про критично важливі системи, то найвищий рівень захисту дає тришарова модель, навіть якщо вона сповільнює роботу. Для пристроїв з обмеженими ресурсами найефективнішою виявилася конфігурація ECC + ChaCha20, яка поєднує високу безпеку з енергоефективністю.

Окрему увагу приділено часу встановлення з'єднання. Додавання ECC і каскадного симетричного шифрування помітно подовжувало фазу handshake. Проте сумарна затримка не перевищувала кількох сотень мілісекунд і не мала відчутного впливу на якість з'єднання в умовах типового використання.

Отже, отримані результати підтверджують перспективність комбінованих методів шифрування для захисту Wi-Fi- мереж. Їхня реалізація дозволяє адаптувати криптографічну конфігурацію під конкретне апаратне середовище та характер трафіка. Подальший розвиток концепції може включати автоматизовані механізми динамічного вибору шифрувальних схем, що реагуватимуть на поточні навантаження, тип даних і контекст середовища. У довгостроковій перспективі такі підходи можуть стати основою нових стандартів захисту бездротового зв'язку, що поєднують високу стійкість до атак із широкою сумісністю та прийнятною продуктивністю.

У майбутньому подібні комбіновані схеми можуть стати частиною нових стандартів Wi-Fi. Це дасть змогу підвищити захист без зміни звичних сценаріїв використання для користувачів, оскільки всі додаткові операції виконуватимуться автоматично на рівні протоколу.

Внесок авторів: Данило Скидан – концептуалізація, методологія, аналіз сучасних криптографічних алгоритмів, проведення експериментів у Kali Linux, інтерпретація результатів; Юрій Щєбланін – огляд літератури, підготовка рукопису, редагування тексту, участь у розробленні методології дослідження.

Джерела фінансування. Це дослідження не отримало жодного гранту від фінансової установи в державному, комерційному або некомерційному секторах.

Список використаних джерел

- Barker, E. (2016). *Recommendation for Key Management, Part 1: General (NIST Special Publication 800-57 Part 1, Rev. 4)*. National Institute of Standards and Technology. <https://doi.org/10.6028/NIST.SP.800-57pt1r4>
- Bernstein, D. J. (2008). The Salsa20 family of stream ciphers. In *New Stream Cipher Designs* (pp. 84–97). Springer. https://doi.org/10.1007/978-3-540-68351-3_8
- Crypto StackExchange. (2023). *For AES–GCM, why do protocols not use the nonce to prevent replay attacks?* <https://crypto.stackexchange.com/questions/114926>



- Dworkin, M. (2007). *Recommendation for block cipher modes of operation: Galois/Counter Mode (GCM) and GMAC*. NIST Special Publication 800–38D. <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-38d.pdf>
- FreeRADIUS Project (2024). FreeRADIUS Technical Documentation. <https://wiki.freeradius.org>
- Gupta, V., & Gupta, S. (2002). Elliptic Curve Cryptography (ECC) and its applications. In *Proceedings of the 6th IEEE International Symposium on Consumer Electronics* (pp. 209–212). Association for Computing Machinery New York NY United States. <https://doi.org/10.1145/570681.570691>
- Langley, A., Chang, W.-T., & Strombergson, J. (2016). *ChaCha20 and Poly1305 for IETF protocols.RFC 8439*. <https://datatracker.ietf.org/doc/html/rfc8439>.
- Kolias, C., Kambourakis, G., Stavrou, A., & Gritzalis, S. (2016). Intrusion detection in 802.11 networks: Empirical evaluation of threats and a public dataset. *IEEE Communications Surveys & Tutorials*, 18(1), 184–208. <https://doi.org/10.1109/COMST.2015.2402161>
- OpenBSD Project. (2024). *Libsodium – A modern and easy-to-use crypto library*. <https://doc.libsodium.org>
- OpenSSL Project. (2024). *OpenSSL: Cryptography and SSL/TLS Toolkit Documentation*. <https://www.openssl.org/docs/>
- Rizk, R. & Alkady, Y. (2015). Two-phase hybrid cryptography algorithm for wireless sensor networks. *Journal of Electrical Systems and Information Technology*, 2(3), 296–313. <https://doi.org/10.1016/j.jesit.2015.11.005>
- Shcheblanin, Y., Zahynei, A., Kurchenko, O., Melnyk, I., & Smirnov, S. (2024). Analysis of identification and access management models in the context of fog computing. In *CPITS-II 2024: Workshop on Cybersecurity Providing in Information and Telecommunication Systems II* (Vol. 3826, pp. 288–293). SEUR-WS.org. <https://ceur-ws.org/Vol-3826/short19.pdf>
- Thankappan, M., Rifà-Pous, H., & Garrigues, C. (2022). Multi-Channel Man-in-the-Middle Attacks Against Protected Wi-Fi Networks: A State of the Art Review. *Expert Systems with Applications*, 210, 118401. <https://doi.org/10.1016/j.eswa.2022.118401>
- Vanhoe, M., & Piessens, F. (2014). Advanced Wi-Fi attacks using commodity hardware. In *Proceedings of the Annual Computer Security Applications Conference (ACSAC)* (pp. 256–265). <https://doi.org/10.1145/2664243.2664260>
- Wireshark Foundation (2024). *Wireshark User Guide*. https://www.wireshark.org/docs/wsug_html_chunked/
- WolfSSL Inc. (2023). *What is the difference between AES and ECC?* <https://www.wolfssl.com/what-is-the-difference-between-aes-and-ecc>
- Zou, Y., Zhu, J., Wang, X., & Hanzo, L. (2016). A survey on wireless security: Technical challenges, recent advances, and future trends. *Proceedings of the IEEE*, 104(9), 1727–1765. <https://doi.org/10.1109/JPROC.2016.2558521>

References

- Barker, E. (2016). *Recommendation for Key Management, Part 1: General (NIST Special Publication 800-57 Part 1, Rev. 4)*. National Institute of Standards and Technology. <https://doi.org/10.6028/NIST.SP.800-57pt1r4>
- Bernstein, D. J. (2008). The Salsa20 family of stream ciphers. In *New Stream Cipher Designs* (pp. 84–97). Springer. https://doi.org/10.1007/978-3-540-68351-3_8
- Crypto StackExchange. (2023). *For AES-GCM, why do protocols not use the nonce to prevent replay attacks?* <https://crypto.stackexchange.com/questions/114926>
- Dworkin, M. (2007). *Recommendation for block cipher modes of operation: Galois/Counter Mode (GCM) and GMAC*. NIST Special Publication 800–38D. <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-38d.pdf>
- FreeRADIUS Project (2024). FreeRADIUS Technical Documentation. <https://wiki.freeradius.org>
- Gupta, V., & Gupta, S. (2002). Elliptic Curve Cryptography (ECC) and its applications. In *Proceedings of the 6th IEEE International Symposium on Consumer Electronics* (pp. 209–212). Association for Computing Machinery New York NY United States. <https://doi.org/10.1145/570681.570691>
- Langley, A., Chang, W.-T., & Strombergson, J. (2016). *ChaCha20 and Poly1305 for IETF protocols.RFC 8439*. <https://datatracker.ietf.org/doc/html/rfc8439>.
- Kolias, C., Kambourakis, G., Stavrou, A., & Gritzalis, S. (2016). Intrusion detection in 802.11 networks: Empirical evaluation of threats and a public dataset. *IEEE Communications Surveys & Tutorials*, 18(1), 184–208. <https://doi.org/10.1109/COMST.2015.2402161>
- OpenBSD Project. (2024). *Libsodium – A modern and easy-to-use crypto library*. <https://doc.libsodium.org>
- OpenSSL Project. (2024). *OpenSSL: Cryptography and SSL/TLS Toolkit Documentation*. <https://www.openssl.org/docs/>
- Rizk, R. & Alkady, Y. (2015). Two-phase hybrid cryptography algorithm for wireless sensor networks. *Journal of Electrical Systems and Information Technology*, 2(3), 296–313. <https://doi.org/10.1016/j.jesit.2015.11.005>
- Shcheblanin, Y., Zahynei, A., Kurchenko, O., Melnyk, I., & Smirnov, S. (2024). Analysis of identification and access management models in the context of fog computing. In *CPITS-II 2024: Workshop on Cybersecurity Providing in Information and Telecommunication Systems II* (Vol. 3826, pp. 288–293). SEUR-WS.org. <https://ceur-ws.org/Vol-3826/short19.pdf>
- Thankappan, M., Rifà-Pous, H., & Garrigues, C. (2022). Multi-Channel Man-in-the-Middle Attacks Against Protected Wi-Fi Networks: A State of the Art Review. *Expert Systems with Applications*, 210, 118401. <https://doi.org/10.1016/j.eswa.2022.118401>
- Vanhoe, M., & Piessens, F. (2014). Advanced Wi-Fi attacks using commodity hardware. In *Proceedings of the Annual Computer Security Applications Conference (ACSAC)* (pp. 256–265). <https://doi.org/10.1145/2664243.2664260>
- Wireshark Foundation (2024). *Wireshark User Guide*. https://www.wireshark.org/docs/wsug_html_chunked/
- WolfSSL Inc. (2023). *What is the difference between AES and ECC?* <https://www.wolfssl.com/what-is-the-difference-between-aes-and-ecc>
- Zou, Y., Zhu, J., Wang, X., & Hanzo, L. (2016). A survey on wireless security: Technical challenges, recent advances, and future trends. *Proceedings of the IEEE*, 104(9), 1727–1765. <https://doi.org/10.1109/JPROC.2016.2558521>

Отримано редакцією журналу / Received: 04.11.25

Прорецензовано / Revised: 08.11.25

Схвалено до друку / Accepted: 21.12.25

Yurii SHCHEBLANIN, PhD (Engin.), Senior Researcher
ORCID ID: 0000-0002-3231-6750
e-mail: shcheblanin.yurii@knu.ua
Taras Shevchenko National University of Kyiv, Kyiv, Ukraine

Danylo SKYDAN, Student
ORCID ID: 0009-0001-2999-8180
e-mail: cassador2281@gmail.com
Taras Shevchenko National University of Kyiv, Kyiv, Ukraine

EVALUATING THE EFFECTIVENESS OF COMBINED CRYPTOGRAPHIC SCHEMES IN SECURING WI-FI CONNECTIONS

Background. The growing number of attacks targeting wireless Wi-Fi networks poses significant challenges for organizations and users relying on these networks to transmit confidential data. Today, Wi-Fi is one of the most widely used communication channels, making it an attractive target for cybercriminals. Vulnerabilities in the encryption and authentication mechanisms of Wi-Fi Protected Access 2 (WPA2) and WPA3 protocols can lead to data interception, key – related attacks, and serious privacy risks. Therefore, enhancing the security of Wi-Fi networks is a critical task, particularly for corporate environments and devices with high security requirements.

Methods. This study involved analyzing modern cryptographic algorithms Advanced Encryption Standard, 256 – bit key (AES-256), ChaCha20, Elliptic Curve Cryptography (ECC) and their combined implementations, modeling a wireless



environment based on Kali Linux using hostapd and FreeRADIUS, and testing resistance to attacks such as Replay, Key Reinstallation Attack (KRACK), and PMKID.

Results. *Experiments demonstrated that the AES-256 and ChaCha20 combination ensures high throughput and fast authentication performance but remains vulnerable to replay attacks if initialization vectors are improperly managed. Hybrid schemes involving ECC significantly improve resistance to key exchange attacks but increase handshake time and resource consumption. The most secure configuration proved to be the three – layer ECC + AES-256 + ChaCha20 model, which provides comprehensive protection at the cost of increased computational demands.*

Conclusions. *One of the key directions for improving Wi-Fi security is the adoption of combined encryption approaches that integrate both symmetric and asymmetric algorithms to achieve maximum resilience against modern attacks. A promising area of further development is the optimization of such schemes for mobile and IoT devices, where a balance between performance and security is essential. The findings of this study may contribute to enhancing Wi-Fi security policies and developing more robust WPA2/WPA3 protocol implementations.*

Key words: *Wi-Fi; WPA2; WPA3; AES-256; ChaCha20; ECC; combined encryption.*

Автори заявляють про відсутність конфлікту інтересів. Спонсори не брали участі в розробленні дослідження; у зборі, аналізі чи інтерпретації даних; у написанні рукопису; в рішенні про публікацію результатів.

The authors declare no conflicts of interest. The funders had no role in the design of the study; in the collection, analyses or interpretation of data; in the writing of the manuscript; in the decision to publish the results.