КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (32), 2026
ISSN 2663 – 4023
DOI 10.28925/2663-4023.2026.32.1205
УДК 004.056.5:621.396

Лужецький Володимир Андрійович
д.т.н., професор, завідувач кафедри захисту інформації
Вінницький національний технічний університет, Вінниця, Україна
ORCID: 0000-0001-7466-7738
lva.kzi2002@gmail.com

Селезньов Віталій Ігорович
асистент кафедри захисту інформації
Вінницький національний технічний університет, Вінниця, Україна
ORCID: 0009-0004-0225-9697
seleznov.vitalii@email.com

Хохлачова Юлія Євгеніївна
к.т.н., професор, професор кафедри інженерії програмного забезпечення та кібербезпеки
Київський національний торговельно-економічний університет,
ORCID: 0000-0002-1883-8704
y.khokhlachova@knute.edu.ua

ПРОТОКОЛ АВТЕНТИФІКАЦІЇ ЗАСОБІВ ІНТЕРНЕТУ РЕЧЕЙ З ВИКОРИСТАННЯМ RFID-МІТОК

Анотація. Стрімкий розвиток Інтернету речей та масове впровадження RFID-міток актуалізують задачу розробки протоколів автентифікації та контролю цілісності даних. Переважна більшість існуючих протоколів автентифікації для RFID-міток забезпечує взаємну автентифікацію учасників взаємодії та стійкість до типових мережевих атак, однак серед розглянутих підходів здебільшого відсутні рішення, що також забезпечують цілісність інформації, яка зберігається та передається RFID-міткою. У низці прикладних сценаріїв автентифікація RFID-мітки має супроводжуватися контролем цілісності переданих нею даних, що зумовлює необхідність розробки спеціалізованого протоколу, здатного розв'язувати обидві задачі одночасно в умовах обмежених апаратних ресурсів. У статті запропоновано протокол двосторонньої автентифікації між RFID-міткою та сервером системи, для реалізації якого на стороні RFID-мітки достатньо криптографічної геш-функції з апаратною складністю, що не перевищує 2000 GE, простої функції оновлення псевдовипадкового числа та операції конкатенації. Автентифікація сторін забезпечується на основі одноразових параметрів, що незалежно оновлюються після кожної сесії, а їх початкові значення розподіляються між RFID-міткою та системою на етапі ініціалізації. Для виконання однієї сесії автентифікації на стороні RFID-мітки достатньо трьох обчислень геш-функції та одного виконання функції оновлення псевдовипадкового числа, а кількість обмінів повідомленнями між RFID-міткою та системою скорочено до двох. У роботі показано стійкість розробленого протоколу до атак підробки зчитувача та RFID-мітки, повторного відтворення, активної атаки типу «людина посередині» та порушення синхронізації, а також забезпечення прямої секретності й контролю цілісності даних RFID-мітки. Отримані результати свідчать про доцільність застосування запропонованого протоколу в системах, де дані RFID-мітки не є конфіденційними, але потребують контролю цілісності, зокрема в логістиці, управлінні ланцюгами постачання та суміжних IoT-застосуваннях.

Ключові слова: IoT, RFID-мітка, протокол автентифікації, одноразові параметри, цілісність даних, геш-функція, криптографія.

ВСТУП

Постановка проблеми. Стрімкий розвиток концепції Інтернету речей (IoT) суттєво трансформував підходи до проектування розподілених інформаційних систем, у яких

фізичні об’єкти, сенсори та виконавчі пристрої об’єднані в єдину екосистему для автоматизованого збору, передавання і обробки даних [1]. Кількість підключених пристроїв у глобальному масштабі продовжує зростати, охоплюючи промислове виробництво, транспортну логістику, медицину, роздрібну торгівлю та багато інших галузей. У такому середовищі технології автоматичної ідентифікації відіграють ключову роль, оскільки саме вони забезпечують зв’язок між фізичним станом об’єкта і його цифровим представленням у сервісах IoT. Радіочастотна ідентифікація (RFID) є однією з найбільш поширених технологій автоматичної ідентифікації, що використовується в IoT-інфраструктурі [2]. Технологія RFID ґрунтується на бездротовій взаємодії між RFID-міткою, розміщеною на об’єкті, та зчитувачем, який ініціює сеанс зв’язку і передає отримані дані до системи обробки. RFID технологія не потребує прямої видимості між RFID-міткою та зчитувачем, підтримує масове зчитування великої кількості об’єктів одночасно і дозволяє зчитувати дані на значних відстанях залежно від діапазону частот і типу обладнання. Завдяки цим властивостям технологія RFID знайшла широке практичне застосування в управлінні ланцюгами постачання та логістиці, в охороні здоров’я для ідентифікації пацієнтів і відстеження медикаментів, у системах контролю доступу, транспортних системах, системах бібліотечного обліку та у роздрібній торгівлі [2, 3].

За конструктивними особливостями RFID-мітки поділяють на активні, напівпасивні та пасивні. Активні RFID-мітки оснащені власним джерелом живлення, можуть ініціювати передачу даних і підтримувати відносно складні обчислення. Пасивні RFID-мітки не мають власного джерела живлення і живляться виключно від електромагнітного поля зчитувача. Саме пасивні RFID-мітки отримали найбільш масове поширення завдяки низькій вартості виробництва і малим габаритам та становлять переважну більшість розгорнутих RFID-систем [4, 7]. Обмін даними між RFID-міткою та системою зчитування здійснюється через відкритий радіоканал, що створює суттєві загрози інформаційній безпеці, оскільки повідомлення можуть бути перехоплені, модифіковані або повторно використані зловмисником. Серед типових мережевих атак на RFID-системи виділяють атаки перехоплення, повторного відтворення, підміни пристрою та десинхронізації [4, 5]. Для пасивних EPC Gen2-міток проблема захисту ускладнюється ще й жорсткими обмеженнями обчислювальних ресурсів, відповідно до яких, для криптографічних перетворень в RFID-мітках може бути доступно близько 2000 GE, тоді як реалізація традиційних криптографічних алгоритмів, зокрема AES або класичних геш-функцій, потребує значно більших апаратних витрат. Це обмежує можливість безпосереднього застосування стандартних криптографічних примітивів у дешевих пасивних RFID-мітках і зумовлює необхідність розробки спеціалізованих легких або надлегких протоколів автентифікації.

Важливе практичне значення для сучасних UHF RFID-систем має специфікація EPCglobal Class-1 Generation-2 UHF RFID (EPC Gen2) [6], яка фактично визначає базові принципи взаємодії між зчитувачем і пасивною RFID-міткою та широко використовується в промислових і логістичних застосуваннях. Водночас засоби, передбачені цією специфікацією, не забезпечують повноцінної криптографічно стійкої строгої взаємної автентифікації для пасивних RFID-міток. Як наслідок, у науковій літературі поширеним є підхід, за якого для EPC Gen2-сумісних міток розробляються додаткові малоресурсні протоколи автентифікації, що враховують апаратні обмеження RFID-міток і водночас забезпечують вищий рівень безпеки.

Аналіз останніх досліджень і публікацій. У сучасних дослідженнях [3-5], [7], [8], [12-18], присвячених протоколам автентифікації для RFID-систем, простежуються два

основні підходи. Перший ґрунтується на використанні малоресурсних криптографічних примітивів, зокрема геш-функцій, генераторів псевдовипадкових чисел або фізично неклонованих функцій, що дає змогу підвищити рівень безпеки за прийнятних апаратних витрат. Другий підхід орієнтований на максимальне зменшення апаратної складності за рахунок використання лише найпростіших побітових перетворень. Прикладом такого підходу є протокол SASI [12], у якому для реалізації взаємної автентифікації пасивних RFID-міток використовуються лише прості побітові операції та циклічний зсув. Проте подальший криптоаналіз показав, що така спрощена обчислювальна модель не виключає появи суттєвих вразливостей. Дослідження [13-15] продемонстрували вразливість SASI до атак десинхронізації, трасування та повного розкриття секретів.

У праці [7] запропоновано малоресурсний протокол автентифікації для EPC Gen2-сумісних RFID-систем. Автори пропонують використання в якості основного перетворення спеціалізованого генератора псевдовипадкових чисел PRNG. PRNG побудований на основі LFSR, що поєднаний з нелінійною функцією-фільтром. Запропонований PRNG характеризується низькими апаратними витратами і демонструє задовільні статистичні властивості відповідно до вимог специфікації EPC Gen2. Протокол автентифікації використовує лише побітові операції XOR та виклики PRNG, забезпечуючи взаємну автентифікацію і встановлення спільного сесійного ключа з динамічним оновленням ідентифікатора RFID-мітки через синхронізовані виклики PRNG на стороні RFID-мітки та серверу.

У статті [8] розроблено надлегкий протокол взаємної автентифікації UMAP для протидії атакам відтворення в умовах обмежених ресурсів пасивних RFID-міток. Механізм автентифікації та оновлення ключів побудований на основі побітових операцій, зокрема XOR, AND, OR та циклічних зсувів, а також із використанням міток часу, що забезпечує актуальність кожного повідомлення і унеможливлює повторне використання перехоплених даних. Автори підтвердили стійкість протоколу до визначених загроз засобами Scyther та AVISPA, а також здійснили порівняльний аналіз продуктивності, який показав скорочення загального часу виконання в середньому на 78,51% відносно аналогічних протоколів [8].

У роботі [16] запропоновано два варіанти протоколу автентифікації на основі тригерних геш-ланцюгів, спрямовані на усунення недоліків оригінальної схеми Henrici-Müller. У схемі Challenge-Response Triggered Hash для забезпечення взаємної автентифікації та стійкості до атак повторного відтворення використано двосторонній обмін псевдовипадковими значеннями. У схемі Forward-Rolling Triggered Hash додатково введено автентифікований монотонний лічильник на основі геш-ланцюга Лампорта, що дозволяє усунути вразливість до атак зв’язування сесій. Обидві схеми побудовані на основі геш-функцій, що підвищує криптографічну стійкість порівняно з підходами, які використовують лише найпростіші побітові перетворення, однак водночас збільшує обчислювальні витрати на стороні RFID-мітки.

У праці [17] запропоновано схему автентифікації для RFID-систем, у якій поєднано генератор псевдовипадкових чисел, геш-функцію та операції XOR, а автентифікація реалізується в межах трьох раундів обміну між RFID-міткою та зчитувачем. Стійкість до атаки десинхронізації досягається за рахунок зберігання в базі даних сервера поточної та попередньої версій секрету RFID-мітки, що дозволяє відновити коректну автентифікацію після неуспішного сеансу. Автори зазначають, що протокол є стійким до атак повторного відтворення, підміни та перехоплення, зберігаючи при цьому низькі обчислювальні витрати на стороні RFID-RFID-мітки.

У дослідженні [18] запропоновано фреймворк надійної автентифікації під назвою RAFI для IoT-інфраструктури на основі технології RFID, що поєднує криптографічну геш-функцію, операції XOR, використання міток часу, симетричне зашифрування та розшифрування повідомлень між сервером і RFID-міткою на основі сеансових ключів. Відмінною рисою протоколу є встановлення спільного сеансового ключа між RFID-міткою та сервером за результатами успішної автентифікації, а також відсутність необхідності оновлення спільних секретних параметрів після кожного сеансу, що забезпечує стійкість до атаки десинхронізації. Автори також декларують забезпечення взаємної автентифікації, прямої секретності, стійкості до атак повторного відтворення та атак типу «людина посередині». Разом з тим одночасне використання гешування, побітових операцій та симетричного шифрування ускладнює обчислювальну структуру протоколу і обмежує його придатність для реалізації в найпростіших пасивних RFID-мітках із жорстко обмеженими апаратними ресурсами.

Серед розглянутих протоколів автентифікації для RFID-міток переважна більшість забезпечує взаємну автентифікацію сторін взаємодії, стійкість до типових мережевих атак і, в окремих випадках, захист анонімності RFID-мітки. Водночас у прикладних сценаріях, де дані, що передаються від RFID-мітки, не є конфіденційними, але потребують обов'язкового контролю цілісності, цього набору властивостей є недостатньо. Це зумовлює актуальність розроблення протоколу автентифікації для RFID-міток, який, поряд із взаємною автентифікацією та стійкістю до типових атак, забезпечував би також перевірку цілісності інформації, що передається від RFID-мітки. Метою даної роботи є розробка протоколу автентифікації для RFID-міток, що забезпечує зазначені властивості шляхом використання геш-функції як основного криптографічного перетворення.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Запропонований протокол реалізує взаємну автентифікацію між RFID-міткою та системою із застосуванням криптографічної геш-функції $H(\cdot)$ та функцію оновлення псевдовипадкового числа $G(\cdot)$. Безпека протоколу ґрунтується на властивості незворотності та стійкості до колізій обраної геш-функції. Функція $G(\cdot)$ реалізує оновлення псевдовипадкового числа. У подальшому під системою розуміється довірена сторона протоколу, що складається зі серверної частини з базою даних та зчитувача. При цьому вважається, що обмін даними між зчитувачем і сервером здійснюється через захищений канал зв'язку, тому вони розглядаються як єдине ціле. У табл. 1 наведено умовні позначення, що використовуються в описі протоколу.

Таблиця 1

Перелік умовних позначень використаних у протоколі

Позначення	Опис
$H(\cdot)$	Криптографічна геш-функція
$G(\cdot)$	Функція оновлення псевдовипадкового числа
M	Інформація, що зберігається RFID-міткою
$H(M)$	Геш-значення інформації
$P_i^{(с)}, P_i^{(м)}, K_i^{(с)}, K_i^{(м)}, r_i^{(с)}, r_i^{(м)}$	Одноразові параметри для i-ї сесії на стороні системи та RFID-мітки відповідно
σ_i	Одноразові автентифікаційні дані для i-ї сесії
R_i	Відповідь від RFID-мітки для i-ї сесії

Протокол передбачає два етапи: ініціалізацію та автентифікацію. Етап ініціалізації виконується один раз під час додаванні нової RFID-мітки до системи. Основною метою цього етапу є встановлення між RFID-міткою та базою даних системи спільних секретних одноразових параметрів, що використовуватимуться для подальших сесій автентифікації. Для кожної нової RFID-мітки у базі даних сервера додається новий запис, що містить такі поля:

$\{ID,\ M,\ H(M),\ P_0,\ K_0,\ r_0\}$,

де ID – унікальний ідентифікатор RFID-мітки в системі, а P_0, K_0, r_0 – початкові значення одноразових параметрів. Водночас RFID-мітка також зберігає такі параметри: $\{M,\ H(M),\ P_0,\ K_0,\ r_0\}$.

Початкові значення P_0, K_0, r_0 генеруються сервером незалежно одне від одного псевдовипадковим чином. Передача початкових параметрів до RFID-мітки здійснюється шляхом фізичної прошивки її пам'яті, що унеможливлює перехоплення початкових параметрів по радіоканалу:

Система→RFID: $\{M,\ H(M),\ P_0,\ K_0,\ r_0\}$. (1)

Обов'язковою умовою коректності протоколу є $P_0 \neq K_0$, що забезпечує незалежність двох ланцюгів, які використовуються в протоколі, а саме ланцюжка підтвердження автентичності системи RFID-міткою з використанням одноразового параметра $P_i^{(\text{м})}$ та ланцюжка підтвердження автентичності RFID-мітки системою на основі одноразового параметра $K_i^{(\text{с})}$.

Перед початком кожної нової сесії автентифікації RFID-мітка проходить процедуру радіочастотної ідентифікації, за результатами якої система отримує ідентифікатор *ID* RFID-мітки та завантажує відповідний запис із бази даних. Ця процедура не є складовою протоколу і тому не розглядається в його межах.

Схему протоколу автентифікації наведено на рис. 1. Процес автентифікації для *i*-ї сесії передбачає виконання декількох кроків.

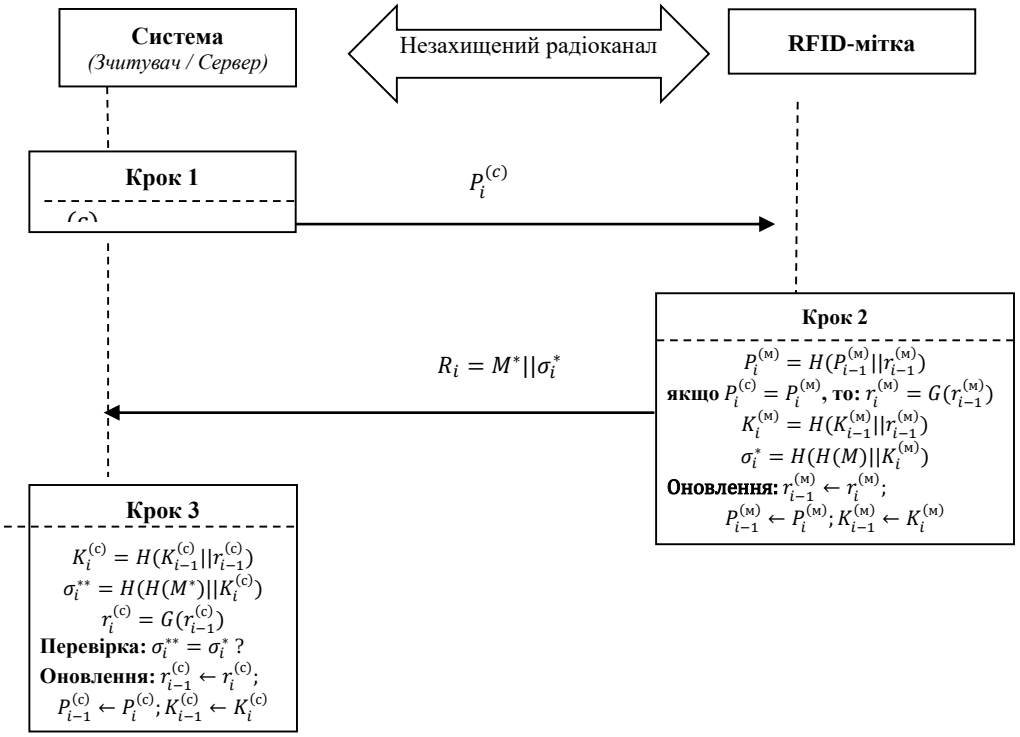

Рис. 1. Схема протоколу автентифікації

Крок 1. Система обчислює значення одноразового параметру $P_i^{(с)}$ та надсилає його до RFID-мітки:

$$P_i^{(с)} = H(P_{i-1}^{(с)} || r_{i-1}^{(с)}). \quad (2)$$

Значення $P_i^{(с)}$ забезпечує підтвердження автентичності системи для RFID-мітки, оскільки його обчислення передбачає знання одноразових параметрів $P_{i-1}^{(с)}, r_{i-1}^{(с)}$ попередньої сесії.

Крок 2. RFID-мітка обчислює очікуване значення параметра $P_i^{(м)}$:

$$P_i^{(м)} = H(P_{i-1}^{(м)} || r_{i-1}^{(м)}) \quad (3)$$

на основі збережених у неї значень $(P_{i-1}^{(м)}, r_{i-1}^{(м)})$ з попередньої сесії. RFID-мітка здійснює перевіряє виконання умови: $P_i^{(с)} = P_i^{(м)}$?

Якщо $P_i^{(с)} \neq P_i^{(м)}$, то RFID-мітка ігнорує запит і не надсилає жодної відповіді.

Якщо $P_i^{(с)} = P_i^{(м)}$, то RFID-мітка переконалася в автентичності системи, після чого виконує обчислення параметра $K_i^{(м)}$ на основі якого формує одноразові автентифікаційні дані:

$$r_i^{(м)} = G(r_{i-1}^{(м)}) \quad (4)$$

$$K_i^{(м)} = H(K_{i-1}^{(м)} || r_{i-1}^{(м)}) \quad (5)$$

$$\sigma_i = H(H(M) || K_i^{(м)}) \quad (6)$$

Значення σ_i пов'язує разом автентичність RFID-мітки та цілісність її даних M. RFID-мітка надсилає системі відповідь $R_i = M || \sigma_i$ та оновлює значення одноразових параметрів $(P_{i-1}, K_{i-1}, r_{i-1})$:

$$r_{i-1}^{(м)} \leftarrow r_i^{(м)}; P_{i-1}^{(м)} \leftarrow P_i^{(м)}; K_{i-1}^{(м)} \leftarrow K_i^{(м)} \quad (7)$$

Крок 3. Отримавши $R_i^* = M^* || \sigma_i^*$, система обчислює:

$$K_i^{(с)} = H(K_{i-1}^{(с)} || r_{i-1}^{(с)}) \quad (8)$$

$$\sigma_i^{**} = H(H(M^*) || K_i^{(с)}) \quad (9)$$

$$r_i^{(с)} = G(r_{i-1}^{(с)}) \quad (10)$$

Якщо $\sigma_i^{**} = \sigma_i^*$, то автентичність RFID-мітки підтверджено системою, а отримані дані M є цілісними. Система оновлює значення $(P_{i-1}^{(с)}, K_{i-1}^{(с)}, r_{i-1}^{(с)})$ в базі даних:

$$r_{i-1}^{(с)} \leftarrow r_i^{(с)}; P_{i-1}^{(с)} \leftarrow P_i^{(с)}; K_{i-1}^{(с)} \leftarrow K_i^{(с)} \quad (11)$$

Якщо $\sigma_i^{**} \neq \sigma_i^*$ або зафіксовано відсутність відповіді на крок 1 протягом відведеного часу очікування, то значення $(P_{i-1}^{(с)}, K_{i-1}^{(с)}, r_{i-1}^{(с)})$ в базі даних залишаються незмінними. Відсутність відповіді від RFID-мітки свідчить про можливу десинхронізацію. RFID-мітка могла оновити значення $(P_{i-1}^{(м)}, K_{i-1}^{(м)}, r_{i-1}^{(м)})$ на крок уперед

після попередньої сесії, відповідь якої не дійшла до системи. Оскільки різниця станів у такому разі завжди складає рівно одну сесію, протокол передбачає механізм відновлення синхронізації, що полягає в додатковій спробі автентифікації. Схему протоколу автентифікації у разі порушення синхронізації наведено на рис. 2.

Кроки спроби 1 завершуються інформацією про порушення синхронізації. Спроба 2 (відновлення синхронізації) передбачає реалізацію кроків 4-6.

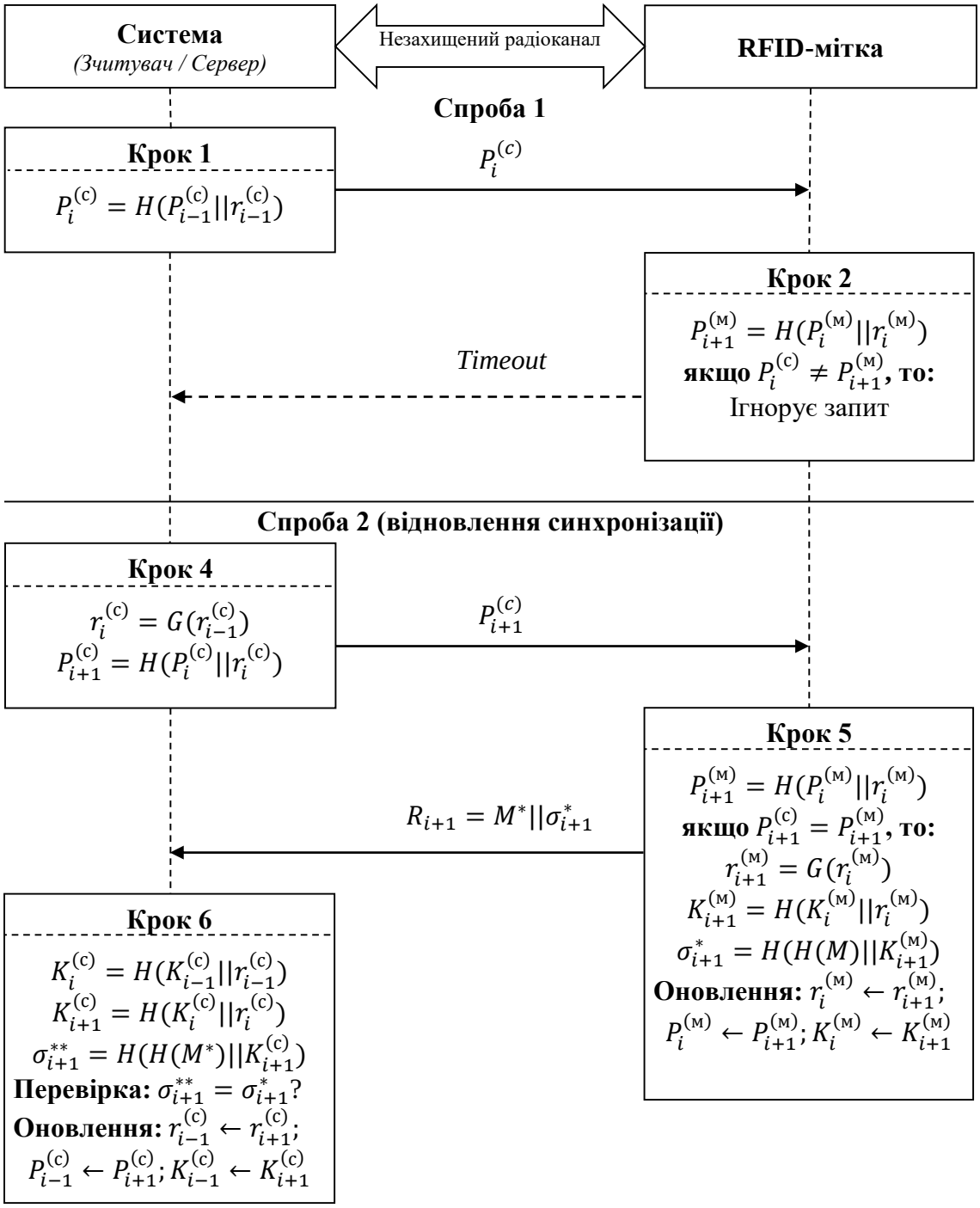

Рис. 2. Схема протоколу автентифікації у разі порушення синхронізації

Крок 4. Система обчислює одноразовий параметр $P_{i+1}^{(с)}$ для наступної сесії, використовуючи обчислений на кроці 1 попередні значення $P_i^{(с)}$ та $r_i^{(с)}$, обчислені за формулами (3), (10):

$$P_{i+1}^{(с)} = H(P_i^{(с)} || r_i^{(с)}), \tag{12}$$

та надсилає $P_{i+1}^{(с)}$ до RFID-мітки.

Крок 5. При порушенні синхронізації в пам'яті RFID-мітки збережені значення $(P_i^{(м)}, K_i, r_i)$, що є результатом завершення i-ї сесії. Тоді RFID-мітка обчислює очікуване значення $P_{i+1}^{(м)}$ за формулою (3) та порівнює з параметром $P_{i+1}^{(с)}$ отриманим від системи. У разі успішної перевірки RFID-мітка здійснює обчислення відповідно до формул (4), (5), (6) для значення i+1, формує результат $R_{i+1} = M||\sigma_{i+1}$ та надсилає до системи. Після цього RFID-мітка виконує оновлення значень:

$$r_i^{(м)} \leftarrow r_{i+1}^{(м)}; P_i^{(м)} \leftarrow P_{i+1}^{(м)}; K_i^{(м)} \leftarrow K_{i+1}^{(м)} \tag{13}$$

Крок 6. Отримавши від RFID-мітки $R_{i+1}^* = M^*||\sigma_{i+1}^*$, система обчислює:

$$K_{i+1}^{(с)} = H(K_i^{(с)} || r_i^{(с)}) \tag{14}$$

$$\sigma_{i+1}^{**} = H(H(M^*)||K_{i+1}^{(с)}). \tag{15}$$

Якщо $\sigma_{i+1}^{**} = \sigma_{i+1}^*$, то автентифікація є успішною та синхронізацію відновлено. Система оновлює значення в базі даних до $(P_{i+1}^{(с)}, K_{i+1}^{(с)}, r_{i+1}^{(с)})$, де $r_{i+1}^{(с)} = G(r_i^{(с)})$. Якщо друга спроба завершилась відсутністю відповіді або помилкою при перевірці, то протокол завершується з помилкою автентифікації, а оновлення значень в базі даних системи не відбувається і наступна сесія розпочнеться з тих самих значень $(P_{i-1}^{(с)}, K_{i-1}^{(с)}, r_{i-1}^{(с)})$.

Протокол не прив'язаний до конкретної геш-функції. Будь-яка функція, що задовольняє вимогам незворотності та стійкості до колізій, є прийнятною. Єдиним практичним обмеженням до геш-функції є складність її апаратної реалізації, оскільки для пасивних RFID-міток обсяг логічних вентилів, що відводиться на криптографічну складову, як правило, не перевищує 2000 GE [4]. Як приклад сумісної геш-функції може бути використана геш-функція HDG, запропонована авторами у роботах [19, 20], апаратна складність якої задовольняє зазначеному обмеженню навіть при обчисленні геш-значень довжиною 256 біт. Функція $G(\cdot)$ повинна бути відома обом сторонам протоколу. Найпростішим варіантом є реалізація у вигляді лічильника $G(r) = r + 1$, однак для більшого рівня безпеки бажано, щоб значення r_i суттєво відрізнялось від попереднього r_{i-1} для кожної сесії. Тому рекомендованим є використання конструкцій на основі регістрів зсуву з лінійним зворотнім зв'язком (LFSR), що є простими при апаратній реалізації та забезпечують краще оновлення псевдовипадкового числа між сесіями. Безпека протоколу не залежить від непередбачуваності $G(\cdot)$, оскільки значення r_i ніколи не передається каналом зв'язку у відкритому вигляді, а захист повністю забезпечується незворотністю $H(\cdot)$.

АНАЛІЗ БЕЗПЕКИ ПРОТОКОЛУ

Виконано теоретичний аналіз стійкість запропонованого протоколу до основних атак на RFID-системи. Аналіз базується на структурних властивостях протоколу та криптографічних властивостях геш-функції $H(\cdot)$.

Протокол забезпечує взаємну автентифікацію сторін. Система підтверджує свою автентичність RFID-мітці за допомогою одноразового параметра $P_i^{(\text{с})}$. Лише легітимна система, що зберігає параметри попередньої сесії $(P_{i-1}^{(\text{с})}, r_{i-1}^{(\text{с})})$ здатна обчислити коректне значення одноразового параметра для i-ї сесії. У свою чергу, RFID-мітка підтверджує свою автентичність системі через автентифікаційні дані $\sigma_i = H(H(M)||K_i^{(\text{м})})$. Лише легітимна RFID-мітка, що володіє одноразовим параметром $K_i^{(\text{м})}$, може сформувати коректне значення σ_i.

Стійкість до атаки підробки зчитувача забезпечується тим, що для ініціювання i+1 сесії система повинна надіслати RFID-мітці коректне значення $P_{i+1}^{(c)} = H(P_i^{(\text{с})}||r_i^{(\text{с})})$. Хоча значення $P_i^{(\text{с})}$ передається каналом зв'язку відкрито і може бути перехоплене під час попередньої i-ї сесії, для обчислення наступного значення ланцюжка необхідно знати $r_i^{(\text{с})} = G(r_{i-1}^{(\text{с})})$, яке ніколи не передається каналом зв'язку. Задача знаходження значення $r_{i-1}^{(\text{с})}$ із перехопленого повідомлення $P_i^{(c)} = H(P_{i-1}^{(\text{с})}||r_{i-1}^{(\text{с})})$ зводиться до задачі знаходження прообразу геш-функції. За умови криптографічної стійкості $H(\cdot)$ така задача є обчислювально нездійсненною, тому зловмисник не може сформувати коректне значення $P_{i+1}^{(c)}$.

Стійкість до атаки підробки RFID-мітки випливає з необхідності формування коректного автентифікаційного значення $\sigma_i = H(H(M)||K_i^{(\text{м})})$ для і-ї сесії. Хоча повідомлення M передається відкритим каналом зв'язку і може бути перехоплене під час попередньої сесії, значення одноразового параметра $K_i^{(\text{м})}$ ніколи не передається під час реалізації протоколу. Його обчислення здійснюється рекурсивно відповідно до співвідношення $K_i^{(\text{м})} = H(K_{i-1}^{(\text{м})}||r_{i-1}^{(\text{м})})$, де значення $r_{i-1}^{(\text{м})}$ також не передається каналом зв'язку. Таким чином, формування коректного значення σ_i без знання параметрів $(K_{i-1}^{(\text{м})}, r_{i-1}^{(\text{м})})$, використаних у попередній сесії, є неможливим. Відновлення цих параметрів із перехоплених повідомлень також зводиться до задачі знаходження прообразу геш-функції, тому зловмисник не може сформувати коректну відповідь RFID-мітки.

Протокол є стійким до атаки повторного відтворення, оскільки кожна і-та сесія використовує власні значення $P_i^{(c)}, K_i^{(\text{м})}$ та σ_i, які оновлюються після кожної успішної автентифікації. Повторне використання перехопленої відповіді $R_i = M||\sigma_i$ у сесії i+1 буде відхилено системою, оскільки перевірка виконуватиметься із використанням оновленого параметра $K_{i+1}^{(\text{с})}$ для якого формується нове значення автентифікаційних даних, що буде відрізнятися від σ_i.

Пряма секретність забезпечується тим, що компрометація параметрів $(P_i^{(\text{с})}, K_i^{(\text{с})}, r_i^{(\text{с})}, P_i^{(\text{м})}, K_i^{(\text{м})}, r_i^{(\text{м})})$, які використовувались у i-й сесії, не дозволяє відновити параметри попередніх сесій. Зокрема, відновлення значення $K_{i-1}^{(\text{м})}$ зі співвідношення $K_i^{(\text{м})} = H(K_{i-1}^{(\text{м})}||r_{i-1}^{(\text{м})})$ зводиться до задачі знаходження прообразу геш-функції, що

унеможливлює ретроспективне розкриття повідомлень, перехоплених у попередніх сесіях.

Протокол забезпечує контроль цілісності інформації M, що зберігається і передається RFID-міткою. Автентифікаційне значення $\sigma_i = H(H(M)||K_i^{(м)})$ криптографічно пов'язує інформацію M з одноразовим параметром $K_i^{(м)}$, який використовується у відповідній i-й сесії. Будь-яка зміна M під час передачі призведе до невиконання умови $\sigma_i^{**} \neq \sigma_i^*$, при перевірці на стороні системи. Формування іншого повідомлення M', для якого $H(M') = H(M)$, зводиться до задачі знаходження колізії геш-функції і є обчислювально нездійсненним.

Стійкість до активної атаки типу «людина посередині» забезпечується тим, що будь-яка модифікація переданих повідомлень призводить до порушення перевірок автентичності. Підміна значення $P_i^{(c)}$ призведе до його невідповідності з $P_i^{(м)}$, незалежно обчисленому на стороні RFID-мітки для тієї ж i-ї сесії, внаслідок чого запит буде відхилено. Аналогічно, підміна $R_i = M||\sigma_i$ призведе до невідповідності автентифікаційних даних при перевірці на стороні системи.

Протокол є стійким до атаки з порушення синхронізації, що може бути наслідком, наприклад, блокування відповіді RFID-мітки. Для запобігання цьому система виконує повторну спробу автентифікації (див. рис. 2), переходячи до параметрів $(P_{i+1}^{(c)}, K_{i+1}^{(c)}, r_{i+1}^{(c)})$ та повторюючи запит. Оскільки різниця між параметрами, що використовуються сторонами після одиночного збою, становить один крок ланцюжка, синхронізація відновлюється автоматично.

Особливістю запропонованого протоколу є його орієнтація на застосування, у яких інформація M не є конфіденційною, але важливим є забезпечення її цілісності. З цієї причини в протоколі не передбачено додаткових механізмів приховування або шифрування M, а основну увагу зосереджено на забезпеченні автентичності сторін та виявленні будь-якої модифікації M під час передавання. Атаки фізичного клонування RFID-мітки та атаки ретрансляції виходять за межі розглянутої моделі загроз і потребують застосування додаткових апаратних механізмів захисту. Зазначені властивості безпеки протоколів автентифікації для RFID-міток наведено у табл. 2.

Таблиця 2

Властивості безпеки протоколів автентифікації для RFID-міток

Властивість	SA SI [12]	CR-Triggered Hash [16]	Dass & Om scheme [17]	EPC Gen2 PRNG [7]	ULMAP [8]	RAFI [18]	Запропо-нований протокол
Взаємна автентифікація	так	так	Так	так	так	так	так
Стійкість до підробки зчитувача	так	так	Так	так	так	так	так
Стійкість до підробки RFID-мітки	так	так	так	так	так	так	так
Стійкість до replay-атак	так	так	так	так	так	так	так
Стійкість до активної MITM	так	так	так	так	так	так	так
Пряма секретність	ні	так	так	так	так	так	так
Контроль цілісності даних	ні	ні	ні	ні	ні	так	так
Стійкість до порушення синхронізації	ні	так	так	ні	так	так	так

Як видно з табл. 2, запропонований протокол задовольняє усім переліченим властивостям. Варто відзначити, що лише протокол RAFI [18] і запропонований авторами протокол автентифікації забезпечують контроль цілісності даних. Це визначає перевагу запропонованого протоколу для застосувань, у яких передані дані RFID-мітки не є конфіденційними, але потребують обов'язкового контролю цілісності даних.

АНАЛІЗ ОБЧИСЛЮВАЛЬНИХ ВИТРАТ

Обчислювальні витрати запропонованого протоколу на стороні RFID-мітки визначаються кількістю базових криптографічних операцій, що виконуються протягом однієї сесії автентифікації. В запропонованому протоколі для звичайної сесії на стороні RFID-мітки виконуються перевірка одноразового параметра $P_i^{(\text{с})}$, оновлення параметрів $(P_i^{(\text{м})}, K_i^{(\text{м})}, r_i^{(\text{м})})$ та формування автентифікаційних даних σ_i. З урахуванням формул (3), (4), (5) та (6), зазначена послідовність операцій передбачає три обчислення геш-функції $H(\cdot)$ та одне обчислення $G(\cdot)$. Тому обчислювальні витрати на стороні RFID-мітки для однієї сесії автентифікації визначаються виразом $C_{\text{м}} = 3C_H + C_G$, де C_H – витрати на одне обчислення геш-функції, а C_G – витрати на одне обчислення функції $G(\cdot)$. Для порівняння з відомими протоколами у табл. 3 наведено перелік операцій, що виконуються на стороні RFID-мітки, їх узагальнену оцінку у вигляді обчислювальних витрат, а також кількість обмінів між RFID-міткою та системою в межах однієї сесії автентифікації.

Таблиця 3

Оцінки обчислювальних витрат для автентифікації на стороні RFID-мітки

Протокол	Операції	Оцінки обчислювальних витрати	Кількість обмінів повідомленнями
SASI [12]	XOR, ADD, ROT, OR	$8C_{XOR} + 3C_{ADD} + 2C_{ROT} + C_{OR}$	4
CR-Triggered Hash [16]	H, RNG	$3C_H + C_{RNG}$	3
Dass & Om scheme [17]	H, RNG, XOR	$2C_H + 4C_{RND} + C_{XOR}$	3
EPC Gen2 PRNG scheme [7]	$PRNG, XOR$	$4C_{PRNG}^{EPC} + 6C_{XOR}$	3
ULMAP [8]	XOR, AND, OR, ROT	$17C_{XOR} + 4C_{AND} + 4C_{ROT} + 2C_{OR}$	3
RAFI [18]	$H, XOR, E/D$	$2C_H + 6C_{XOR} + C_{E/D}$	2
Запропонований	H, G	$3C_H + C_G$	2

Примітка: C_H – витрати на одне обчислення геш-функції; C_G – витрати на одне обчислення функції $G(\cdot)$; C_{RNG} – витрати на генерацію випадкового числа; C_{PRNG}^{EPC} – витрати на спеціалізований генератор псевдовипадкових чисел, сумісний з EPC Gen2; C_{XOR} – витрати на одну операцію додавання за модулем два; C_{ROT} – витрати на одну операцію циклічного зсуву; $C_{E/D}$ – витрати на одну операцію зашифрування або розшифрування.

Як видно з табл. 3, запропонований протокол характеризується помірними обчислювальними витратами на стороні RFID-мітки та потребує лише двох взаємодій у межах звичайної сесії автентифікації. На відміну від надлегких протоколів [8] та [12], запропонований протокол забезпечує вищий рівень криптографічної стійкості за рахунок використання геш-функції. Водночас, порівняно з [7], [17] та [18], протокол

має простішу обчислювальну структуру, оскільки не потребує генератора випадкових чисел, додаткових елементів XOR або блоку зашифрування чи розшифрування на стороні RFID-мітки. Таким чином, запропонований протокол можна розглядати як компромісне рішення для пасивних RFID-міток, у яких необхідно поєднати помірні обчислювальні витрати, малу кількість взаємодій та контроль цілісності переданих даних.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

У статті розроблено протокол взаємної автентифікації системи та RFID-міток, у якому, як основне криптографічне перетворення використовується геш-функція. Запропонований протокол орієнтований на застосування, у яких дані RFID-мітки не є конфіденційними, але потребують обов'язкового контролю цілісності. Конструкція протоколу ґрунтується на двох незалежних геш-ланцюгах, один із яких використовується для підтвердження автентичності системи перед RFID-міткою, а інший – для підтвердження автентичності RFID-мітки системою та перевірки цілісності переданих даних.

Проведений аналіз безпеки запропонованого протоколу показав, що цей протокол забезпечує стійкість до атак підробки зчитувача та RFID-мітки, повторного відтворення, активної атаки типу «людина посередині» та порушення синхронізації, а також підтримує пряму секретність і цілісність даних RFID-мітки. Стійкість до порушення синхронізації досягається завдяки вбудованому механізму відновлення синхронізації після одиничного збою зв'язку без повторної ініціалізації параметрів RFID-мітки.

Результати порівняльного аналізу з протоколами SASI, CR-Triggered Hash, Dass-Om, EPC Gen2 PRNG scheme, ULMAP показують, що запропонований протокол забезпечує не лише взаємну автентифікацію, а й контроль цілісності даних RFID-мітки та стійкість до порушень синхронізації. На стороні RFID-мітки в межах однієї штатної сесії виконуються три обчислення геш-функції та одне обчислення функції оновлення псевдовипадкового числа при двох обмінах повідомленнями, що свідчить про конкурентоспроможність протоколу за обчислювальними витратами. У разі використання геш-функції HDG, складність апаратної реалізації якої не перевищує 2000 GE, забезпечується можливість застосування запропонованого протоколу не лише у активних RFID-мітках, але й пасивних RFID-мітках згідно специфікації EPC Gen2.

Подальші дослідження будуть спрямовані на формальну верифікацію протоколу засобами автоматизованого аналізу безпеки, зокрема з використанням ProVerif або Scyther, а також на розширення протоколу для підтримки анонімності RFID-мітки в застосуваннях із підвищеними вимогами до конфіденційності.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Atzori, L., Iera, A., & Morabito, G. (2010). The Internet of Things: A survey. *Computer Networks, 54*(15), 2787–2805. https://doi.org/10.1016/j.comnet.2010.05.010
2. Want, R. (2006). An introduction to RFID technology. *IEEE Pervasive Computing, 5*(1), 25–33. https://doi.org/10.1109/MPRV.2006.2
3. Scott, D. (2024). A survey of RFID authentication protocols. *TechRxiv*. https://doi.org/10.36227/techrxiv.171216642.23764824/v1
4. Zhu, F., Li, P., Xu, H., & Wang, R. (2019). A lightweight RFID mutual authentication protocol with PUF. *Sensors, 19*(13), 2957. https://doi.org/10.3390/s19132957
5. Baashirah, R., & Abuzneid, A. (2018). Survey on prominent RFID authentication protocols for passive tags. *Sensors, 18*(10), 3584. https://doi.org/10.3390/s18103584

6. EPCglobal. (2015). *EPC radio-frequency identity protocols Class-1 Generation-2 UHF RFID specification (Version 2.0.1)*. GS1. https://www.gs1.org/sites/default/files/docs/epc/Gen2_Protocol_Standard.pdf
7. Caballero-Gil, P., Caballero-Gil, C., & Molina-Gil, J. (2022). RFID authentication protocol based on a novel EPC Gen2 PRNG. *arXiv*. https://doi.org/10.48550/arXiv.2208.05345
8. Abd Alhasan, A. Q., Rohani, M. F., & Abuali, M. S. (2024). Ultra-lightweight mutual authentication protocol to prevent replay attacks for low-cost RFID tags. *IEEE Access, 12*. https://doi.org/10.1109/ACCESS.2024.3386100
9. Mudra, G., Cui, H., & Johnstone, M. N. (2023). Survey: An overview of lightweight RFID authentication protocols suitable for the maritime Internet of Things. *Electronics, 12*(13), 2990. https://doi.org/10.3390/electronics12132990
10. Shariq, M., Singh, K., Maurya, P. K., Ahmadian, A., & Ariffin, M. R. K. (2021). URASP: An ultralightweight RFID authentication scheme using permutation operation. *Peer-to-Peer Networking and Applications, 14*, 3737–3757. https://doi.org/10.1007/s12083-021-01192-5
11. Shariq, M., Singh, K., Lal, C., Conti, M., & Khan, T. (2022). ESRAS: An efficient and secure ultra-lightweight RFID authentication scheme for low-cost tags. *Computer Networks, 217*, 109360. https://doi.org/10.1016/j.comnet.2022.109360
12. Chien, H.-Y. (2007). SASI: A new ultralightweight RFID authentication protocol providing strong authentication and strong integrity. *IEEE Transactions on Dependable and Secure Computing, 4*(4), 337–340. https://doi.org/10.1109/TDSC.2007.70226
13. Hernandez-Castro, J. C., Tapiador, J. M. E., Peris-Lopez, P., & Quisquater, J.-J. (2008). Cryptanalysis of the SASI ultralightweight RFID authentication protocol with modular rotations. *arXiv*. https://doi.org/10.48550/arXiv.0811.4257
14. Phan, R. C. W. (2009). Cryptanalysis of a new ultralightweight RFID authentication protocol—SASI. *IEEE Transactions on Dependable and Secure Computing, 6*(4), 316–320. https://doi.org/10.1109/TDSC.2008.33
15. Sun, H.-M., Ting, W.-C., & Wang, K.-H. (2011). On the security of Chien's ultralightweight RFID authentication protocol. *IEEE Transactions on Dependable and Secure Computing, 8*(2), 315–317. https://doi.org/10.1109/TDSC.2009.26
16. Lim, T.-L., Li, T., & Gu, T. (2008). Secure RFID identification and authentication with triggered hash chain variants. In *2008 IEEE International Conference on Parallel and Distributed Systems (ICPADS)* (pp. 583–590). https://doi.org/10.1109/ICPADS.2008.46
17. Dass, P., & Om, H. (2016). A secure authentication scheme for RFID systems. *Procedia Computer Science, 78*, 100–106. https://doi.org/10.1016/j.procs.2016.02.017
18. Kumar, V., Kumar, R., Khan, A. A., Kumar, V., Chen, Y.-C., & Chang, C.-C. (2022). RAFI: Robust authentication framework for IoT-based RFID infrastructure. *Sensors, 22*(9), Article 3110. https://doi.org/10.3390/s22093110
19. Seleznov, V., & Luzhetskyi, V. (2023). Method of low-resource hashing type "data–generator". *Cybersecurity: Education, Science, Technique, 28*, 84–95. https://doi.org/10.28925/2663-4023.2023.22.8495
20. Luzhetskyi, V., & Seleznov, V. (2025). Hardware implementation of the HDG hash function. *Bulletin of Cherkasy State Technological University, 30*(2), 10–21. https://doi.org/10.62660/bcstu/2.2025.22

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (32), 2026
ISSN 2663 – 4023

Luzhetskyi Volodymyr Andriiovych
Doctor of Technical Science, Professor, Head of Information Security Department
Vinnytsia National Technical University, Vinnytsia, Ukraine
ORCID: 0000-0001-7466-7738
lva.kzi2002@gmail.com

Seleznov Vitalii Ihorovych
post-graduate student of the Information Security Department
Vinnytsia National Technical University, Vinnytsia, Ukraine
ORCID: 0009-0004-0225-9697
seleznov.vitalii@email.com

Khokhlachova Yuliia Yevheniivna
Candidate of Technical Sciences, Professor, Professor of the Department of Software Engineering and Cybersecurity, Kyiv National University of Trade and Economics, Kyiv, Ukraine
ORCID: 0000-0002-1883-8704
y.khokhlachova@knute.edu.ua

AUTHENTICATION PROTOCOL FOR INTERNET OF THINGS DEVICES USING RFID TAGS

Abstract. The rapid growth of the Internet of Things and the widespread adoption of RFID tags have intensified the need for authentication protocols that also ensure data integrity. Most existing RFID authentication protocols provide mutual authentication and resistance to common network attacks, but they generally do not address the integrity of the data stored on and transmitted by the RFID tag. In many practical scenarios, tag authentication must be complemented by verification of the integrity of the transmitted data, which creates the need for a specialized protocol capable of solving both tasks simultaneously under severe hardware constraints. This paper proposes a mutual authentication protocol for communication between an RFID tag and a system server. On the tag side, the protocol requires only a cryptographic hash function with hardware complexity not exceeding 2000 GE, a simple pseudo-random number update function, and a concatenation operation. Mutual authentication is achieved using one-time parameters that are updated independently after each session, with their initial values distributed between the RFID tag and the system during the initialization phase. A single authentication session on the RFID tag side requires only three hash computations and one execution of the pseudo-random number update function, while the number of message exchanges between the RFID tag and the system is reduced to two. The paper shows that the proposed protocol is resistant to reader impersonation, tag impersonation, replay, active man-in-the-middle, and desynchronization attacks, while also providing forward secrecy and RFID tag data integrity control. The obtained results indicate that the proposed protocol is suitable for systems in which RFID tag data are not confidential but require integrity assurance, particularly in logistics, supply chain management, and related IoT applications.

Keywords: IoT, RFID tag, authentication protocol, one-time parameters, data integrity, hash function, cryptography.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Atzori, L., Iera, A., & Morabito, G. (2010). The Internet of Things: A survey. *Computer Networks, 54*(15), 2787–2805. https://doi.org/10.1016/j.comnet.2010.05.010
2. Want, R. (2006). An introduction to RFID technology. *IEEE Pervasive Computing, 5*(1), 25–33. https://doi.org/10.1109/MPRV.2006.2
3. Scott, D. (2024). A survey of RFID authentication protocols. *TechRxiv*. https://doi.org/10.36227/techrxiv.171216642.23764824/v1
4. Zhu, F., Li, P., Xu, H., & Wang, R. (2019). A lightweight RFID mutual authentication protocol with PUF. *Sensors, 19*(13), 2957. https://doi.org/10.3390/s19132957

5. Baashirah, R., & Abuzneid, A. (2018). Survey on prominent RFID authentication protocols for passive tags. *Sensors, 18*(10), 3584. https://doi.org/10.3390/s18103584
6. EPCglobal. (2015). *EPC radio-frequency identity protocols Class-1 Generation-2 UHF RFID specification (Version 2.0.1)*. GS1. https://www.gs1.org/sites/default/files/docs/epc/Gen2_Protocol_Standard.pdf
7. Caballero-Gil, P., Caballero-Gil, C., & Molina-Gil, J. (2022). RFID authentication protocol based on a novel EPC Gen2 PRNG. *arXiv*. https://doi.org/10.48550/arXiv.2208.05345
8. Abd Alhasan, A. Q., Rohani, M. F., & Abuali, M. S. (2024). Ultra-lightweight mutual authentication protocol to prevent replay attacks for low-cost RFID tags. *IEEE Access, 12*. https://doi.org/10.1109/ACCESS.2024.3386100
9. Mudra, G., Cui, H., & Johnstone, M. N. (2023). Survey: An overview of lightweight RFID authentication protocols suitable for the maritime Internet of Things. *Electronics, 12*(13), 2990. https://doi.org/10.3390/electronics12132990
10. Shariq, M., Singh, K., Maurya, P. K., Ahmadian, A., & Ariffin, M. R. K. (2021). URASP: An ultralightweight RFID authentication scheme using permutation operation. *Peer-to-Peer Networking and Applications, 14*, 3737–3757. https://doi.org/10.1007/s12083-021-01192-5
11. Shariq, M., Singh, K., Lal, C., Conti, M., & Khan, T. (2022). ESRAS: An efficient and secure ultra-lightweight RFID authentication scheme for low-cost tags. *Computer Networks, 217*, 109360. https://doi.org/10.1016/j.comnet.2022.109360
12. Chien, H.-Y. (2007). SASI: A new ultralightweight RFID authentication protocol providing strong authentication and strong integrity. *IEEE Transactions on Dependable and Secure Computing, 4*(4), 337–340. https://doi.org/10.1109/TDSC.2007.70226
13. Hernandez-Castro, J. C., Tapiador, J. M. E., Peris-Lopez, P., & Quisquater, J.-J. (2008). Cryptanalysis of the SASI ultralightweight RFID authentication protocol with modular rotations. *arXiv*. https://doi.org/10.48550/arXiv.0811.4257
14. Phan, R. C. W. (2009). Cryptanalysis of a new ultralightweight RFID authentication protocol—SASI. *IEEE Transactions on Dependable and Secure Computing, 6*(4), 316–320. https://doi.org/10.1109/TDSC.2008.33
15. Sun, H.-M., Ting, W.-C., & Wang, K.-H. (2011). On the security of Chien's ultralightweight RFID authentication protocol. *IEEE Transactions on Dependable and Secure Computing, 8*(2), 315–317. https://doi.org/10.1109/TDSC.2009.26
16. Lim, T.-L., Li, T., & Gu, T. (2008). Secure RFID identification and authentication with triggered hash chain variants. In *2008 IEEE International Conference on Parallel and Distributed Systems (ICPADS)* (pp. 583–590). https://doi.org/10.1109/ICPADS.2008.46
17. Dass, P., & Om, H. (2016). A secure authentication scheme for RFID systems. *Procedia Computer Science, 78*, 100–106. https://doi.org/10.1016/j.procs.2016.02.017
18. Kumar, V., Kumar, R., Khan, A. A., Kumar, V., Chen, Y.-C., & Chang, C.-C. (2022). RAFI: Robust authentication framework for IoT-based RFID infrastructure. *Sensors, 22*(9), Article 3110. https://doi.org/10.3390/s22093110
19. Seleznov, V., & Luzhetskyi, V. (2023). Method of low-resource hashing type "data–generator". *Cybersecurity: Education, Science, Technique, 28*, 84–95. https://doi.org/10.28925/2663-4023.2023.22.8495
20. Luzhetskyi, V., & Seleznov, V. (2025). Hardware implementation of the HDG hash function. *Bulletin of Cherkasy State Technological University, 30*(2), 10–21. https://doi.org/10.62660/bcstu/2.2025.22

Отримано редакцією журналу / Received: 21.01.26
Прорецензовано / Revised: 15.02.26
Схвалено до друку / Accepted: 26.03.26