УДК 004.056
DOI: 10.31673/2409-7292.2021.045158

**Селедцов Г.М., Перепелиця Л.С.**

# ВАРІАНТ РЕАЛІЗАЦІЇ АЛГОРИТМУ AES В RFID СИСТЕМАХ

В данній роботі приведені основні відомості стосовно RFID систем та побіжний аналіз основних криптографічних алгоритмів, що традиційно в них використовуються. Основна ж робота була проведена над розробкою та апаратною імплементацією AES алгоритму шифрування, що теоретично має допомогти в захисті від більшості з згаданих вище атак.

**Ключові слова:** RFID, AES, радіочастотна ідентифікація.

**Вступ.**

Системи радіочастотної ідентифікації (RFID) використовуються для автоматичного отримання даних про товари, осіб або тварин, чи більш загально: про об'єкт. До об'єкту прикріплюють невелику мікросхему, яка називається RFID-міткою, що довзволяє зберігати та оновлювати інформацію на ній. Ця властивість може бути використана в промисловості для відстеження товарів або в системах контролю доступу. Системи RFID не вимагають прямої видимості між міткою та рідером і працюють безконтактно. Дані та енергія для роботи міток передаються через радіохвилі.

Кожна система RFID складається з міток, які прикріплюється до об'єкта для ідентифікації, і рідера, який здатний отримувати дані з мітки. Рідер також може вміти записувати дані до пам'яті мітки. Додатково, для реалізації безпосередньо програм, що базуються на даних отриманих від міток, використовують хост-компьютер. Команди хосту перетворюються в запити читача і передаються через радіохвилы. Якщо мітка знаходиться в полі дії читача, він вона надсилає відповідь. Відповіді міток обробляються хостом, який використовує дані згідно з діючою програмою.(рис. 1).

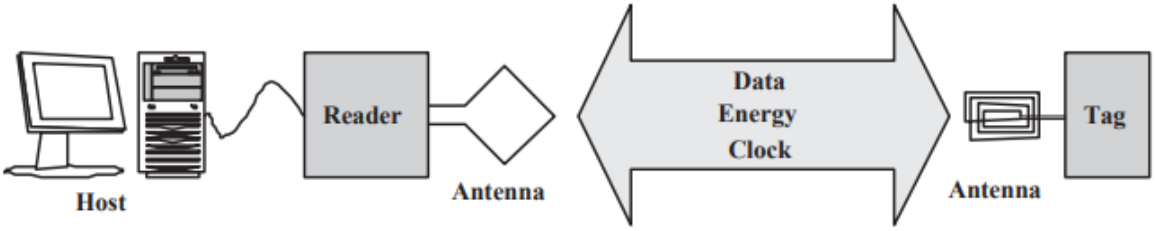


Рис. 1. Програма радіоідентифікації

У цій роботі ми зосередимося на пасивних мітках. Це означає, що вони отримують свою енергію з поля рідера. Інтенсивність поля обмежується національними та міжнародними правилами, тому максимальна енергія доступна для виконання розрахункових операцій завжді обмежена. З цієї причини мікросхеми в RFID мітках мають проектуватися з урахуванням їх енергоефективності. Зменшення енергоспоживання також призводить до збільшення ефктивної площі, в якій мітки можуть працювати користуючись енергією поля рідера. Більше технічних деталей про системи RFID (механізми зв'язку, швидкості передачі даних, кодування даних, модуляція, частота) можна знайти в RFID-Handbook [1] і в стандартах RFID ISO/IEC 18000-3 [6].

Технологія RFID пропонує переконливі переваги в багатьох секторах. Промисловість та роздрібна торгівля заощаджують гроші завдяки розширеній автоматизації виготовлення та складування. Споживачі також можуть скористатися перевагами товару, який може обмінюватися інформацією зі своїм оточенням (наприклад, пральна машина з одягом, молочні пакети з холодильником). Інші застосування систем RFID - це контроль доступу, стеження за тваринами, підтвердження походження товарів, системи плати за проїзд, іммобілізація автомобілів тощо. Існують навіть концепції забезпечення безпеки грошових купюр за допомогою RFID-міток [2]. Так що, схоже, RFID може стати дуже популярною технологією в найближчому майбутньому.

Через цю популярність суспільство почало думати про питання безпеки та конфіденційності, у питиання що стосуються цієї технології.

Першим серйозним приводом для занепокоїння стали випадкати стаження за споживачами : здатність RFID рідерів ідентифікувати всі незахіщенні мітки в межі дії свого поля, може бути використана щоб відстежувати переміщення споживача, чи збирати інформацію про нього на основі даних в RFID мітках. Іншою проблемою безпеки є підробка міток, коли вони використовуються для контролю доступу, контролю втрат, або для підтвердження походження обєкту. Третя проблема безпеки, про яку слід згадати, - це несанкціонований доступ до вмісту пам'яті міток. Якщо в пам'яті зберігаються чутливі дані, це серйозна проблема для безпеки всієї системи.

Покращення рівня безпеки завжди відбувається за рахунок додаткових витрат. Незважаючи на те, що промисловість/бізнес хоче використовувати мітки що мають мінімальну вартість, використання RFID у повсякденному житті вимагає вирішення проблем з безпекою технологіх. У даній роботі пропонується реалізація методу аутентифікації для систем RFID з використанням стійкого шифрування. Розширений стандарт шифрування (AES) використовується як криптографічний примітив, оскільки він стандартизований і вважається безпечним. В роботі буде представлений протокол аутентифікації і як він може бути інтегрований в існуючі стандарти. Крім того, представляється реалізація AES з низьким енергоспоживанням, яка підходить для RFID-міток з точки зору споживання енергії та розміру чіпа(кристалу)(die-size).

Системи RFID сприйнятливі до атак: оскільки вони працюють без нагляду і безконтактно, зловмисник може працювати віддалено і пасивні атаки не будуть помічені. Деякі з основних проблем стосуються (небажаного) відстеження споживачів, підробки міток та несанкціонованого доступу до вмісту їх пам'яті. Це основні вразливості які мають бути виправленні для того, щоб технологія RFID могла отримати широке визнання користувачів.

**Аналіз дотичних робіт.** Деякі наукові роботи вже намагалися виправити вразливості RFID систем. У [3] пропонують так звані «blocker tags» для захисту споживачів від відстеження. Одна мітка імітує широкий діапазон ідентифікаційних номерів, тому рідер не може однозначно його ідентифікувати, а відстеження стаж неможливим. Цей підхід пропонувався як ріщення для міток нижнього цінового діапазону, які коштували менше 0,05 доларів США.

У [4] розглянуто питання безпеки та конфіденційності систем RFID так само, які і в [7]. Тут пропонується хеш-блокування, як механізм для контролю доступу і його рандомізовану версію для боротьби з стежкою за споживачем. Також пропонуються й інші ідеї для підвищення безпеки, але припущення які вони роблять про середовище в яких ці систмеи будуть працювати, наприклад, про те, що сигнал від мітки неможливо буде підслухати, роблять його пропозиції непридатними для практичної реалізації.

У [8] також звертають увагу на проблему стеження за споживачами і рекомендують стирати ідентифікаційний номер мітки на місці продажу. Вони також розглядають захист вмісту міток і вводять концепцію контролю доступу шляхом взаємної аутентифікації міток і рідеру.

У [9] автори мають на меті виправити одразу декілька різних вразливостей безпеки-конфіденційність споживачів, підробка купюр і її виявлення. Вони пропонують систему, яка задовольняє вимогам для всіх чотирьох основних суб'єктів: центрального банку, торговців, виконавчої влади та споживача. Пропозиція в цій публікації - система RFID з використанням асиметричної криптографії в поєднанні з деякими методами, які вимагають фізичного доступу до мітки.

Нарешті, «RFID-Handbook» [1] намагється вирішити проблеми безпеки в RFID системах за допомогою механізмів аутентифікації. Це також є предметом цієї роботи. Для автентифікації мипропонуємо використовувати стійкі криптографічні алгоритми.

**Автентифікація.** У [10] розрізняють три методи автентифікації: системи що базуються на паролях (слабка автентифікація), аутентифікація виклик-відповідь (сильна

аутентифікація) (challenge-response authentication), а також автентифікацію з нульовим пізнанням (zero-knowledge authentication). Системи паролів пропонують слабкий рівень безпеки, а методи нульового пізнання часто пов'язані з «сильними» математичними проблемами, які є дуже “дорогими” для розрахунку та реалізації. Таким чином, найоптимальнішими є техніки виклик-відповідь.

Існують асиметричні та симетричні техніки типу виклик-відповідь. Недоліком асиметричних методів автентифікації є те, що вони дуже трудомісткі і дорогі для реалізації в апаратній частині. Тому незважаючи на їх теоретичну ефективність, вони не є оптимальним вибором для систем RFID. Були спроби розробити ресурсозберігаючі алгоритми асиметричної автентифікації. Для іх реалізації в RFID системах було запропоновано NTRU [11], але було доведено, що він має деякі недоліки безпеки [12].

Симетричні алгоритми працюють з одним секретним ключем який знають всі автентифіковані пристрої. Автентифікація здійснюється шляхом перевірки володіння цим секретним ключем. Проблемою при використанні симетричних методів автентифікації є ефективний розподіл ключів і їх керування. Кожне оновлення ключа має бути повідомлено всім учасникам. Компрометація тільки одного пристрою, що тримає ключ, впливає на всю систему. Ці проблеми і деякі рішення були розглянуті в Handbook of Applied Cryptography.

Симетрична автентифікація може бути виконана використовуючи алгоритми шифрування або хеш-функції. Є цілий ряд причин що сприяли обранню AES як криптографічного примітиву. Цей алгоритм шифрування був обраний у 2001 році як стандарт шифрування в США і вважається дуже безпечним. Крім того, він добре підходить для апаратних реалізацій.

Протоколи для використання в системах відповідей на виклики, засновані на шифруванні, визначені в стандарті ISO/IEC 9798-2. Одностороння автентифікація працює наступним чином: існує два партнери A і B. Обидва мають один і той же приватний ключ K. B посилає випадкове число rB до A. A шифрує число rB використовуючи ключ K і відправляє назад до B. B також виконує шифрування rBi прівнюючи результат своєї роботи і роботи A може робити висновки про те чи володіє A секретним ключом K

$$\begin{aligned} A \leftarrow B: &\qquad r_B \\ A \rightarrow B: &\qquad E_K(r_B) \end{aligned}$$

Протокол взаємної аутентифікації працює аналогічно. B посилає до A випадкове число. A шифрує rB і самостійно згенероване віпадкове число rA спільним ключем K і пересилає його B. B розшифровує повідомлення і може довести, що rB є правильним і отримуєrA. B змінює послідовність випадкових чисел, та зашифровує її за допомогою K, і передає її A. A підтверджує результат і перевіряє ідентичність B.

$$\begin{aligned} A \leftarrow B: &\qquad r_B \\ A \rightarrow B: &\qquad E_K(r_A, r_B) \\ A \leftarrow B: &\qquad E_K(r_B, r_A) \end{aligned}$$

Для того, щоб мінімізувати споживання електроенергії та розмір мікросхеми, було вирішено розробити схему призначену тільки для шифрування AES. Використовуючи модифіковані протоколи, можна виконувати односторонню аутентифікацію, а також взаємну автентифікацію, навіть якщо не доступна розшифровка AES. Протоколи взаємної автентифікації вимагають додаткового генератора випадкових чисел, тому вони більш дорогі для реалізації.

**Дизайн протоколу безпеки.** У системі RFID з підвищеною безпекою рівень безпеки спирається не тільки на силу використовуваних криптографічних алгоритмів. Протоколи що відповідають за реалізацію алгоритмів автентифікації відіграють головну роль в тому, чи може зловмисник успішно проникнути в систему чи ні. Навіть якщо ми використовуємо

сильні криптографічні алгоритми, ми повинні забезпечити безпеку протоколу. Протокол, представлений далі, дозволяє RFID системам використовувати AES як криптографічний примітив. У системах RFID обмежена обчислювальна потужність і доступна для міток енергія, що накладає великі обмеження на можливий протокол. На додаток до необхідної пропускної здатності для передачі даних, слід звернути увагу на сумісність з існуючими стандартами, такими як ISO/IEC 18000 або електронний код продукту (EPC).

Протокол що ґрунтується на односторонньому механізмі автентифікації з використанням випадкових чисел був представлених у вище. Але інтеграція цього протоколи яка б враховувала ISO / IEC 18000 вимагає додаткових міркувань. На додаток до обов'язкових команд, які повинні виконувати всі мітки, можна вказати спеціальні команди. Дві команди, інтегровані для автентифікації, надсилають виклик до мітки і запитують зашифроване значення. Ці команди розширюють існуючий стандарт, хоча основна функціональність залишається незмінною. Через обмеження малої потужності, внутрішня тактова частота мітки RFID повинна бути розділена від 13,56 до 100 кГц. Стандарт вимагає від мітки, відповідь не більш ніж через 320 мкс після запиту. В іншому випадку мітка не може надсилати відповідь. Це означає що нам доступний час в 32 тактових циклів на частоті 100 кГц, якого недостатньо для реалізації AES.

Рішення цієї проблеми полягає у зміні протоколу, як показано на рис. 2. Ми розділяємо шифрування та надсилання відповіді. Як правило, в полі рідера існує багато RFID-міток що потребують автентифікації. Після отримання всіх унікальних ідентифікаторів за допомогою запиту інвентаризації рідер посилає виклик C1 до Tag1. Цей тег негайно починає шифрування виклику без надсилання відповіді. У той же час рідер відправляє виклики до міток Tag2 і Tag3. Вони також починають шифрувати своїх ключів. Після завершення шифрування EK (C1), Tag1 чекає на запит на відправку зашифрованого значення R1 назад рідеру. Коли рідер надіслав ці три завдання, він надсилає запит на отримання відповіді від Tag1. Отримане значення R1 перевіряється шляхом шифрування виклику C1 і порівняння результату з прийнятим значенням. Два інші невирішені виклики отримані за допомогою того ж методу. . Цей протокол оцінювався за допомогою моделей високого рівня і є концепцію для майбутніх досліджень протоколів аутентифікації в системах RFID.

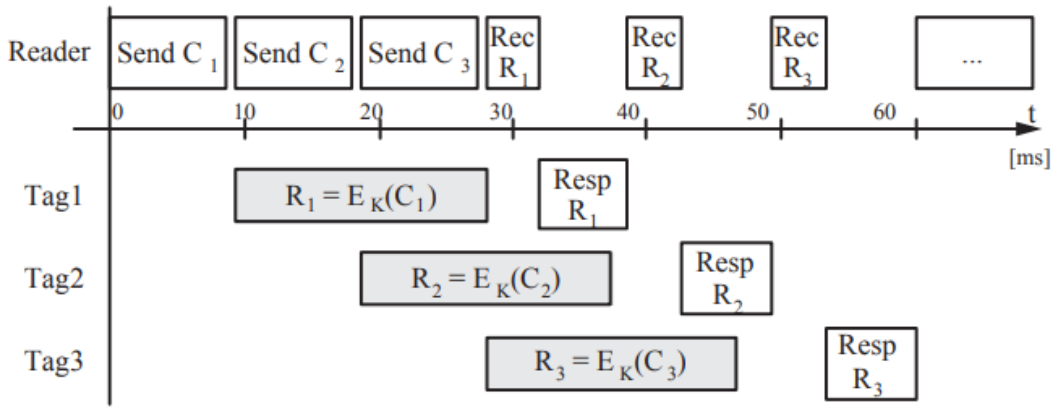


Рис. 2. Протокол автентифікації

Цей протокол забезпечую кожну мітку принаймні 18 мс (1800 тактових циклів на тактовій частоті 100 кГц) для шифрування, що означає що можна автентифікувати до 50 тегів на секунду

**Архітектура міток RFID.** Архітектура мітки RFID (рис. 3) з розширеною безпекою замальована на малюнку. Вона складається з чотирьох частин: аналогового інтерфейсу, цифрового контролера, EEPROM та модуля AES. Аналоговий інтерфейс відповідає за живлення тега, яке передається від рідера до мітки через радіохвилі. Іншими завданнями

аналогового інтерфейсу є модуляція і демодуляція даних і відновлення тактової частоти з несучої частоти. Цифровий контролер є скінченним автоматом, який відповідає за зв'язок з рідером, реалізує механізм уникнення зіткнень і виконує команди протоколп. Крім того, він реалізує читання і запис в EEPROM і модуль AES. EEPROM зберігає специфічні для мітки дані, такі як унікальний ідентифікатор і криптографічний ключ. Ці дані повинні зберігатися при втраті джерела живлення.

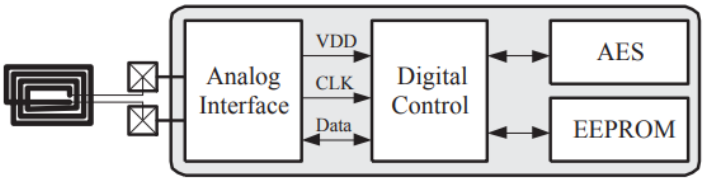


Рис. 3. Архітектура мітки RFID

**Архітектура AES.** Advanced Encryption Standard (AES) - це симетричний алгоритм шифрування, який був обраний у 2001 році Національним інститутом стандартів і технологій (NIST) як Федеральний стандарт обробки інформації FIPS-197. Він працює на блоках даних, так званих State, які мають фіксований розмір 128 біт. State організовано у вигляді матриці з чотирьох рядків і чотирьох стовпців байтів. Визначені довжини ключів - 128 біт, 192 біт або 256 біт. Запропонована реалізація використовує фіксований розмір ключа в 128 біт. Як більшість симетричних шифрів, AES шифрує вхідний блок, застосовуючи ітеративну функцію. Десять ітерацій функцій змінюють State шляхом застосування нелінійних, лінійних і залежних від ключових перетворень. Кожена ітерація перетворює 128-бітний State в модифікований 128-бітний State. З кожним байтом матриці State виконують ці перетворення:

1. SubBytes замінює кожний байт State. Ця операція є нелінійною. Вона часто реалізується у вигляді таблиці. Іноді перетворення SubBytes називається операцією S-Box.

2. ShiftRows зміщує кожен рядок State. Фактичне значення зміщення дорівнює індексу рядків, напр. перший ряд взагалі не зміщується; останній рядок зміщується на три байти вліво.

3. MixColumns перетворює стовпці State. Це множення на постійний поліном у полі GF (28).

4. AddRoundKey об'єднує 128-бітовий State з 128-бітним ключем шляхом додавання відповідних бітів за модулем 2. Це перетворення відповідає операції XOR над State та ключем.

Додатково при кожній ітерації значення що використовується як ключ змінюється. Якщо на першій ітерації ключ завжди дорівнює секретному ключу К, то надалі значення змінюється. Конкретні зміни залежать від конкретної реалізації.

AES - гнучкий алгоритм для апаратних реалізацій. Апаратні реалізації AES можуть бути пристосовані до вимог до розміру мікросхем або можуть бути оптимізовані для високої пропускної здатності в серверних додатках. Ця гнучкість алгоритму AES була однією з цілей при його створенні. Було приділено велику увагу тому , що алгоритм може бути реалізований на системах з різними розмірами шин. Ефективні реалізації можливі на 8-бітних, 32-бітних, 64-бітних і 128-бітних платформах.

Хоча було запропоновано багато апаратних архітектур AES, жодна з описаних архітектур не відповідає вимогам модуля AES для RFID-міток щодо низьких розмірів і низького споживання енергії. Майже всі ці архітектури як мету оптимізації мають швидкість пропускної спроможності. Такі оптимізації нічого не значать для RFID систем. Лише кілька опублікованих архітектур AES не оптимізують пропускну здатність. Але навіть вони не розраховані для ситуацій в яких важливо мінімізувати розмір чіпу та споживану енергію. Чим більше S-Box-ів використовуються, тим менше циклів потрібно для шифрування.

Реалізація алгоритму AES на 32-розрядної архітектурі дозволяє в чотири рази зменшити необхідні апаратні ресурси порівняно з 128-бітовою архітектурою. Це відбувається за рахунок чотириразового збільшення часу для шифрування. Зменшення апаратних ресурсів має позитивний ефект на споживання енергії: чверть апаратних ресурсів споживає лише чверть енергії. Це важлива особливість для бездротових пристроїв, де середнє споживання енергії є ще більш важливим аспектом якості, ніж загальна енергія, необхідна для шифрування одного блоку. Загальне споживання енергії 32-бітовою архітектурою може бути гірше, ніж для 128-бітових архітектур. Але RFID-мітки не пропонують ні кремнієвого простору, ні електромагнітного поля, достатньо сильного для живлення 128-бітової архітектури.

Архітектура запропонованого 8-бітного модуля AES зображена на рис. 4. Модуль складається в основному з трьох частин: контролера, оперативної пам'яті та основний канал для даних(datapath). Контролер обмінюється даними з іншими модулями на мітці, та контролює послідовність всіх десяти раундів шифрування необхідних для AES. Саме він є інтерфейсом до помяті та каналу данних. Оперативна пам'ять зберігає 128-бітовий State і 128-бітний ключ. Ці 256 бітів організовані як 32 байти, щоб максимально відповідати 8-розрядній архітектурі. 32 байти - це найменша можлива кількість пам'яті для AES. Всі операції перепусують існуючі дані. Оскільки не існує вільної пам'яті для зберігання проміжних значень, контролер повинен гарантувати, що не буде перезаписано жодного байтового стану або байтового ключа, якщо вони потрібно знову під час шифрування. Реалізація оперативної пам'яті здійснюється на основі регістрів. Це дозволяє використовувати clock gating, щоб мінімізувати споживання енергії. Канал даних реалізує логіку для обчислення перетворень AES SubBytes, MixColumns і AddRoundKey. Перетворення ShiftRows здійснюється контролером. Під час виконання SubBytes контролер звертається до оперативної пам'яті таким чином, що виконується операція ShiftRows.

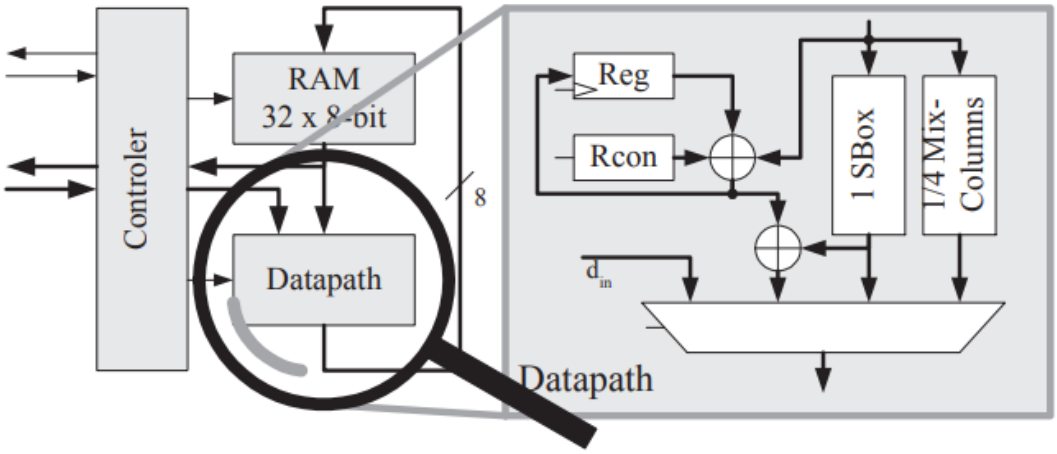


Рис. 4. Архітектура 8-бітного модуля AES

Найбільшою частиною каналу данних AES є S-Box. Існує кілька варіантів реалізації AES S-Box. Найбільш очевидним варіантом є 256 × 8-бітна ROM для реалізації 8-бітного пошуку в таблиці. На жаль, не існують ROM що були б оптимізовані для роботи з малою потужність. Варіантом що відповідав би нашим обмеженням є обчислення значень заміщення за допомогою комбінаційної логіки, як було запропоновано в [13]. За рахунок нехтування можливістю дешифрації ми можемо адаптувати запропонований комбінаційний S-Box. Крім того, регістри використовується як проміжне сховище для конвеєрної операції SubBytes: під час заміни одного байта наступний байт зчитується з пам'яті. Заміщений байт записується в поточну адресу зчитування. Вибравши належним чином адреси для читання,

ця процедура ефективно поєднує операції SubBytes і ShiftRows. ShiftRows просто зводиться до правильної адресації.

Іншим інноваційним рішенням є розрахунок операції MixColumns. Ми досягли побудови підмодуля, який обчислює лише одну четверту операції MixColumns. За допомогою доступу до підмодулю чотири рази виконується повна операція MixColumns для одного стовпця State. Операція MixColumns для одного стовпця показана в рівнянні нижче. Рівняння показують, що всі вихідні байти qi в MixColumns обчислюються за тією ж самою функцією - тільки порядок вхідного стовпця bytes відрізняється.

Шифрування блоку відкритого тексту працює наступним чином. Перед запуском шифрування, блок відкритого тексту необхідно завантажити в ОЗУ модуля AES. У мітці RFID блок відкритого тексту - це 128-бітний текст-виклик, який був отриманий від рідера. Зв'язок між читачем і тегом байт-орієнтована, що добре вписується в 8-бітну архітектуру модуля AES: кожен прийнятий байт може зберігатися в модулі AES. Проміжної пам'яті не потрібно. Криптографічний ключ отримується аналогічним чином з EEPROM мітки. Тепер алгоритм AES може бути виконаний. Він починається з модифікації стану операцією AddRoundKey з використанням незміненого ключа шифру. Наступні десять раундів AES, застосовуючи перетворення SubBytes, ShiftRows, MixColumns і AddRoundKey.

**Результат.** Ця реалізація шифрування AES-128 споживає 7,23 мкА на КМОП-процесорі 0,35 мкм. Він працює на частоті 100 кГц і потребує 1010 тактових циклів для шифрування 128-бітового блоку даних. Необхідна апаратна складність оцінюється в 3,434 еквівалентних логічних елементах(GE). Всі представлені результати виходять з моделювання на транзисторному рівні. Складність кожного компонента наведена в таблиці 1. У таблиці 2 представлено порівняння нашого підходу з 32-бітовою реалізацією S. Mangard і 128-бітний процесор AES для шифрування від Verbauwhede.. З результатів очевидно, що тільки рішення представленне в данній роботі досягає високих вимог до інтеграції криптографічних компонентів у мітки RFID. Ці вимоги - низьке енергоспоживання та низький розмір чіпу,а також вимог щодо швидкості шифрування.

Таблиця 1

Характеристика данної імплементації AES

| Компонент | мкА при 100кГц | GE | Тактових циклів |
|---|---|---|---|
| S-Box | 0.67 | 395 | 450 |
| MixColumns | 0.41 | 252 | 390 |
| AddRoundKey | 0.53 | 90 | 170 |
| RAM | 4.64 | 2337 | |
| Контролер | 0.98 | 360 | |
| Всього | 7.23 | 3434 | 1010 |

Таблиця 2

Порвняння різних імплементацій AES

| AES-128 шифрування | мкА при 100кГц | GE | Тактових циклів |
|---|---|---|---|
| Цей алгоритм | 7.23 | 3434 | 1010 |
| Мангард | 47 | 10700 | 64 |
| Вербавед | 307 | 173000 | 10 |

**Висновки**

На данний момент криптографічни методи захисту в RFID-системах мають балансувати між ефективністю захисту і вартістю впровадження. Вибір кінцевого рішення залежить перш за все від потреб користувача, але ми віримо, що чим більщ росповсюдженною буде ця технологія тим гостріше стоятиме питання безпеки данних. Ця робота представляє систему безпеки RFID, що дозволяє підвищити рівень криптографічного захисту. Завдяки цим RFID-системам підвищеної безпеки ми відкриваємо шлях до повсякденного використання технології RFID.

Була представленна концепція алгоритму автентифікації, що може використовувати AES шифрування, навіть на найдешевших з можливих міток, що означає можливість його використання в товарах та послугах повсякденного життя не нехтуючи безпокою споживача або його данних. Подальша робота буде полягати у вивченні просунутих протоколів аутентифікації для односторонньої та взаємної аутентифікації. Інші методи аутентифікації (наприклад, асиметричні методики) повинні бути проаналізовані для придатності для систем RFID.

**Перелік посилань**

1. RFID Handbook: Fundamentals and Applications in Contactless Smart Cards and Identification, Second Edition, Klaus Finkenzeller, Copyright 2003 John Wiley & Sons, Ltd.
2. A. Juels and R. Pappu Squealing Euros: Privacy protection in RFID-enabled banknotes. In Financial Cryptography, 7th International Conference, Revised Papers, volume 2742 of Lecture Notes in Computer Science, pages 103–121. Springer, 2003.
3. A. Juels, R. L. Rivest, and M. Szydlo. The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy. In Proceedings of the 10th ACM Conference on Computer and Communication Security, pages 103–111.
4. S. A. Weis. Security and Privacy in Radio-Frequency Identification Devices. Master's thesis, Massachusetts Institute of Technology, Cambridge, MA 02139, May 2003.
5. International Organization for Standardization. ISO/IEC 9798-2: Information Technology - Security techniques – Entity Authentication Mechanisms Part 2: Entity authentication using symmetric techniques. ISO/IEC, 1993.
6. International Organization for Standardization. ISO/IEC 18000-3. Information Technology AIDC Techniques – RFID for Item Management, March 2003.
7. S. A. Weis, S. E. Sarma, R. L. Rivest, and D. W. Engels. Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems. In Security in Pervasive Computing, 1st Annual Conference on Security in Pervasive Computing, Boppard, Germany, March 12-14, 2003, Revised Papers, volume 2802 of Lecture Notes in Computer Science, pages 201–212. Springer, 2004
8. S. E. Sarma, S. A. Weis, and D. W. Engels. RFID Systems and Security and Privacy Implications. In Cryptographic Hardware and Embedded Systems – CHES 2002, 4th International Workshop, Redwood Shores, CA, USA, August 13-15, 2002, Revised Papers, volume 2523 of Lecture Notes in Computer Science, pages 454–470. Springer, 2002
9. A. Juels and R. Pappu. Squealing Euros: Privacy protection in RFID-enabled banknotes. In Financial Cryptography, 7th International Conference, FC 2003, Guadeloupe, French West Indies, January 27-30, 2003, Revised Papers, volume 2742 of Lecture Notes in Computer Science, pages 103–121. Springer, 2003
10. A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone. Handbook of Applied Cryptography. CRC Press, 1997. Available online at http://www.cacr.math.uwaterloo.ca/hac/
11. J. Hoffstein, J. Pipher, and J. H. Silverman. NTRU: A Ring-Based Public Key Cryptosystem. In Algorithmic Number Theory, Third International Symposium, ANTS-III, Portland, Oregon, USA, June 21-25, 1998, Proceedings, volume 1423 of Lecture Notes in Computer Science, pages 267–288. Springer, 1998.
12. A. May. Cryptanalysis of NTRU. preprint, (unpublished), February 1999.
13. J. Wolkerstorfer, E. Oswald, and M. Lamberger. An ASIC implementation of the AES SBoxes. In Topics in Cryptology - CT-RSA 2002, The Cryptographer's Track at the RSA Conference, 2002, San Jose, CA, USA, February 18-22, 2002, volume 2271 of Lecture Notes in Computer Science, pages 67–78. Springer, 2002.
14. Alex Biryukov. Related-key Cryptanalysis of the Full AES-192 and AES-256 [Електронний ресурс] / Alex Biryukov, Dmitry Khovratovich // University of Luxembourg. – 2009. – Режим доступу до ресурсу: http://www.impic.org/papers/Aes-192-256.pdf

Надійшла: 19.10.2021 Рецензент: д.т.н., доцент Ахрамович В.М.