УДК 621.391

ЛЕГКОВАГОВЕ ШИФРУВАННЯ ДЛЯ СИСТЕМ ІЗ ОБМЕЖЕНИМИ РЕСУРСАМИ

В.Б. Дудикевич[1], І.С. Собчук[1], Л.М. Ракобовчук[1], П.І. Гаранюк[1], І.П.Гаранюк[2].

1. Кафедра захисту інформації, Національний університет "Львівська політехніка", УКРАЇНА, м. Львів, вул. С.Бандери, 12,
2. Кафедра комп'ютеризованих систем автоматики, Національний університет "Львівська політехніка", УКРАЇНА, м. Львів, вул. С.Бандери, 12

В статті розглянуто тенденції використання систем з обмеженими ресурсами. Проведено аналіз літературних джерел з проблеми ефективності використання легковагої криптографії. Проведено порівняння класичних і сучасних алгоритмів шифрування. В роботі зроблено порівняння блокових симетричних алгоритмів AES, CAST5, Camelia, MARS та Serpent за критеріями продуктивність/пам'ять при реалізації на 8-бітних доступних мікроконтролерах з архітектурою AVR на мові С. Показана ефективність симетричних алгоритмів легковагої криптографії. Створено антиколізійний протокол, який базується на особливостях будови пакетів даних карток EM4100.

Ключові слова – *криптографія, lightweight криптографія, легковагове шифрування, стійкість легковагової криптографії, ефективність легковагової криптографії, програмні шифри, AVR-мікроконтролери, продуктивність алгоритму, анти колізійний протокол..*

Постановка проблеми. Незважаючи на широке використання систем з обмеженими ресурсами, до яких відносяться RFID-мітки, більшість міток мають слабкий криптозахист або не мають його взагалі, що дає можливість зловмиснику зчитати необхідні дані, підробити радіомітку загалом.

Для пасивних RFID-міток в яких використовується легковагове шифрування основною проблемою є те, що надзвичайно важко в готовому пристрої оптимізувати рівень безпеки, ціну та продуктивність – три основні умови, які повинні виконуватись для успішного впровадження проекту. Попри зростаючу, згідно емпіричного закону Мура, продуктивність та степінь інтеграції обчислювальних засобів потреба у lightweight-криптографії залишається актуальною. Це викликано тим, що одночасно ускладнюються та розширюються функції вбудованих систем, протоколи обміну даними, зростають вимоги щодо енергоспоживання і габаритів, тому ресурси для реалізації захисту інформації в цих системах залишаються досить обмеженими [1, 2, 3].

Аналіз останніх досліджень та публікацій. У лютому 2007 року Hitachi

представила RFID-пристрій, що має розміри 0,05 х 0,05 мм, і товщиною, достатньою для вбудовування в лист паперу (7.5 мкм). Такого рівня інтеграції дозволяє досягти технологія «кремній-на-ізоляторі» (SOI). μ-Chip може передавати 128-бітовий унікальний ідентифікаційний номер, записаний в мікросхему на етапі виробництва. Даний номер не можна змінити, що гарантує високий рівень достовірності і означає, що він буде жорстко прив'язаний (асоційований) з тим об'єктом, до якого приєднується або в який вбудовується цей чіп. μ-Chip від Hitachi має типовий радіус зчитування 30 см [4]. Активні RFID-мітки мають власне джерело живлення і не залежать від енергії зчитувача, внаслідок чого зчитуються на великій відстані, мають великі розміри і можуть бути обладнані додатковою електронікою. Проте, такі мітки найбільш дорогі, а у батарей обмежений час роботи. Активні мітки в більшості випадків більш надійні і забезпечують найвищу точність зчитування на максимальній відстані [5]. Пасивні RFID-мітки мають практично необмежений термін експлуатації. RFID-мітка може використовуватися для виконання інших завдань, крім функції носія даних [6]. Основними недоліками пасивних міток є те, що вартість системи вище вартості системи обліку, заснованої на штрих-кодах. Складність самостійного виготовлення. Штрих-код можна надрукувати на будь-якому принтері. Вразливість до перешкод у вигляді електромагнітних полів. Встановлена технічна база для зчитування штрих-кодів істотно перевершує за обсягом рішення на основі RFID, недостатня відкритість вироблених стандартів, слабкий крипто-захист, або взагалі його відсутність [6].

В роботах [7, 8] було досліджено такі класичні криптоалгоритми як DES (Data Encryption Standard), DESX (DES Extension), AES (Advanced Encryption Standard), IDEA (International Data Encryption Algorithm), TEA (Tiny Encryption Algorithm), XTEA (Extended TEA), SEA (Scalable Encryption Algorithm), та відносно нові алгоритми спеціально розроблені для lightweight-криптографії DESL (DES Lightweight Extension), HIGHT та PRESENT.

У роботі [8] здійснено порівняння блокових симетричних алгоритмів AES, CAST5, Camelia, MARS та Serpent за критеріями продуктивність/пам'ять при реалізації на 8-бітних недорогих мікроконтролерах з архітектурою AVR на мові C. Результати досліджень підтвердили високу ефективність алгоритму AES, який випередив усіх конкурентів.

В статті [9] наведено результати порівняння алгоритмів Skipjack, TEA, XTEA, XXTEA, XXTEAO з точки зору використання їх в якості lightweight-алгоритмів у безпровідних сенсорних мережах з різними протоколами роботи на базі платформи MICA2 з AVR-ядром і перевагу віддано алгоритму XXTEAO.

Основні результати щодо використання асиметричних алгоритмів у lightweight-криптографії можна знайти в роботах [3, 8].

Мета статті - аналіз різних типів криптоалгоритмів, дослідження можливості використання легковагового шифрування для захисту персональних даних між ідентифікатором та зчитувачем.

Виклад основного матеріалу досліджень.

1. Легковаговагове шифрування для пасивних **RFID-міт**ок.

Для систем, де ціна та витрати енергії виходять на перший план, обчислювальна потужність сконцентрована в малих, недорогих центральних процесорах, серед яких домінують 8-бітні мікроконтролери.

Серед особливостей AVR-мікроконтролерів, важливих в контексті lightweight-криптографії варто відзначити, що пам'ять організована за Гарвардською архітектурою з 8-бітною пам'яттю даних типу SRAM (1-8 Кбайт) та 16-бітною пам'яттю програм типу Flash (8-128 Кбайт). Регістровий файл містить 32 регістри загального призначення безпосередньо підключених до АЛП. Система команд складається з понад 130 команд, більшість з яких виконуються за один такт. Алгоритми тестувалися для моделі ATmega128.

Розробку програмного забезпечення на мові асемблера, відлагодження, симуляцію та оцінку кількості тактів і розміру коду здійснено з використанням безкоштовного інтегрованого середовища розробки AVR Studio 4.

Результати порівняння вимог до пам'яті наших реалізацій алгоритму Gossamer з відомими реалізаціями інших lightweight-алгоритмів представлені на рис. 1.

Продуктивність – це параметр, який дозволяє оцінити швидкість шифрування і розшифрування даних в бітах за секунду, і коректно порівняти алгоритми, адже в конкретних пристроях швидкість роботи залежить і від тактової частоти мікроконтролера, і від довжини блоку вхідних даних, і від кількості тактів, необхідних для шифрування чи розшифрування цього блоку. Результати порівняння за продуктивністю алгоритму Gossamer з відомими реалізаціями інших lightweight-алгоритмів зображені на рис.2.

При цьому алгоритм Gossamer у варіанті максимальної швидкодії демонструє достатньо високу продуктивність, поступаючись лише алгоритму AES і випереджаючи всі інші алгоритми.

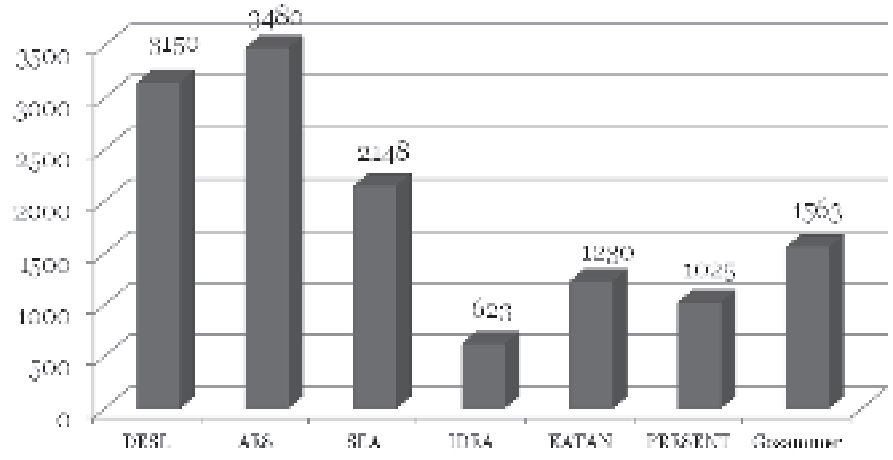

Рис. 1. Необхідний об'єм пам'яті даних в байтах для алгоритмів

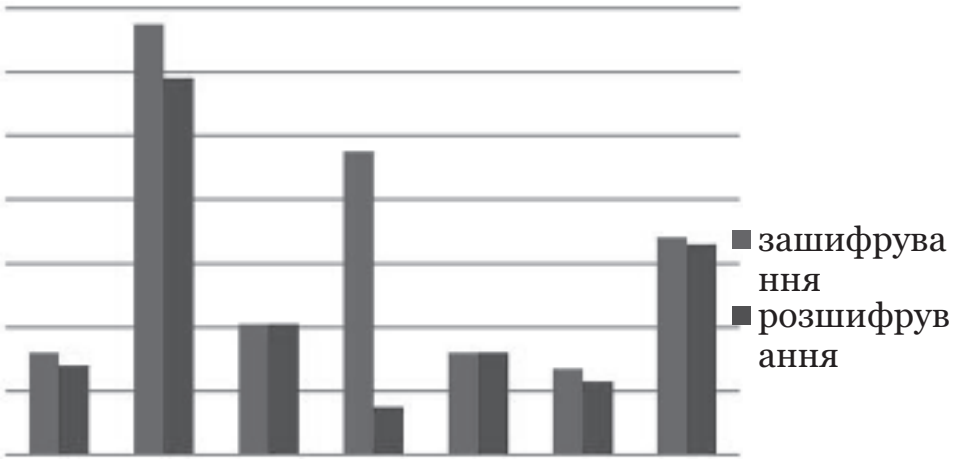

Рис. 2. Продуктивність реалізації алгоритмів (кбіт/с)

2. Підвищення швидкодії та живучості зчитувача**.** Наступним основним параметром системи RFID є швидкодія, яка залежить від застосування та конфігурації системи.

Характеризується: швидкістю передачі даних та швидкістю ідентифікації. Швидкість передачі даних є власне швидкістю передачі бітів даних, тоді як швидкість ідентифікації визначається характеристиками антиколізійних алгоритмів при визначенні індивідуального номера мітки.

Швидкість передачі даних в основному залежить від періоду повторення бітів інформації. Чим менший період, тим більша швидкість передавання даних. З точки зору апаратної реалізації можна зазначити, що для даної схеми кодування та модуляція призводить до розширення спектру. З врахуванням обмежень за шириною спектру це призведе до зниження потужності, що надається мітці. З цього спостерігаємо взаємозв'язок між швидкістю передавання даних і дальністю дії.

Швидкодія ідентифікації залежить від використаного антиколізійного протоколу. Антиколізійні протоколи впливають на витрати при проектуванні апаратури, які у свою чергу, помітно впливають на вартість. Існує взаємозв'язок між швидкістю ідентифікації та вартістю. Крім того, протоколи впливають на потужність споживання – чим більше інтенсивність обробки, тим більше споживається потужність [10].

Надійність зв'язку в системах RFID також сильно пов'язана з антиколізійними алгоритмами. Так, в прямому каналі зв'язку надійність є вищою, тому що в ньому простіше забезпечити велике відношення сигнал/шум. Натомість надійність зворотного каналу зв'язку значно нижча, тому більш надійними є протоколи, які вимагають передачі меншого обсягу даних від мітки до зчитувача. Застосування процедур виявлення і корекції помилок призводить до зниження швидкості передавання даних, ускладнює апаратуру, вимагає великих витрат потужності і, отже, зменшує дальність. Як зазначалося раніше, у міру

наближення до зчитувача напруженість поля зростає, сигнал стає більш помітним і, отже, зростає надійність зв'язку. Надійність каналів зв'язку пов'язана як з дальністю дії, так і з швидкодією системи [11].

Одним із найефективніших методів підвищення живучості є резервування, тобто введення в систему надлишковості. При виході бази даних комп'ютера з ладу дані будуть залишатися на самому пристрої. Система залишається живучою навіть у випадку відключення напруги живлення за рахунок вчасного під'єднання апаратного резерву [11].

3. Антиколізійний протокол. RFID-мітка є простим носієм ідентифікаційного номера, тому постає проблема точного зчитування цього номера. Якщо в робочій зоні зчитувача знаходиться безліч міток, що відповідають одночасно, їхні сигнали інтерферуються.

Таблиця

Структура пакету EM4100

9 біт заголовку		
8 біт номер серії		
або ID корпоративної		
32 біт даних		

Таке накладення сигналів називається колізією, а результати зчитування найчастіше виявляються втраченими. Для уникнення колізій система RFID вимагає формування команд, які базуються на протоколах, що отримали назву антиколізійних[20]. Багато антиколізійних протоколів вимагають виявлення факту виникнення конфлікту сигналів. Найбільш загальноприйнятий метод виявлення колізій базується на використанні властивостей кодування сигналів. Кодування сигналу лише за рівнем, принципово не придатне для виявлення колізії, проте, в цей самий час код Манчестера в якому інформація пов'язана з переходом сигналу від одного рівня до іншого має таку властивість. Саме тому протокол-алгоритм за яким працює запропонований зчитувач має антиколізійну властивість. Дана властивість реалізована на апаратному рівні.

Крім цього для підвищення швидкодії, зменшення помилкових зчитувань та перевірки цілісності даних створено антиколізійний протокол, який базується на особливостях будови пакетів даних карток EM4100 (див.табл.(пакет

даних)), за рахунок пошуку заголовку, преамбули пакету, врахування затримок під час передачі між частинами пакету та підрахунку контрольних сум по рядках та стовпцях «на льоту» при прийомі даних від мітки. Блок схема алгоритму представлено на рис. 3.

Висновки. Результати даних досліджень підтверджують перспективність та доцільність застосування lightweight-криптографії у пасивних RFID-мітках для захисту даних при передачі через канал «мітка-приймач». Оскільки розглянуті оптимізації алгоритму при реалізації на 8-бітних вбудованих платформах дозволяють досягнути компромісу між параметрами ціна/енергоспоживання в залежності від конкретного застосування. На основі існуючого протоколу передавання EM4100 вдосконалено метод обміну інформацією (конфіденційною або, що містить персональні дані), який на відміну від існуючих використовує алгоритм шифрування та антиколізійний протокол для захисту даних при передачі через канал «мітка-приймач».

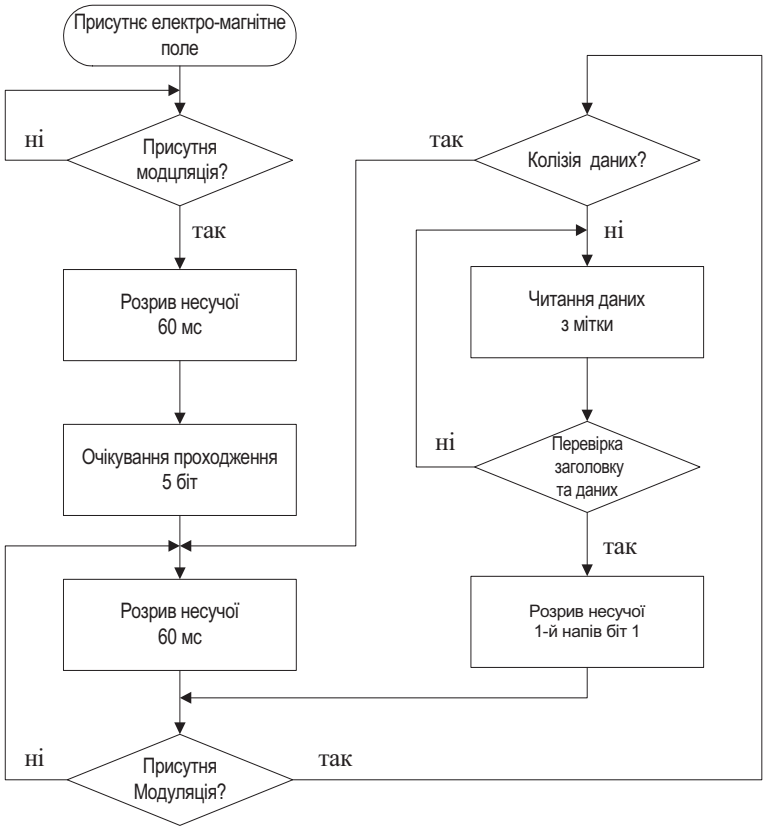

Рис. 3. Блок-схема антиколізійного протоколу

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Konidala D. M. RFID Tag-Reader Mutual Authentication Scheme Utilizing Tag's Access Password/. M. Konidala and K. Kim// Auto-ID Labs White Paper WP-HARDWARE-033, Jan 2007. – С 25-86.
2. Jinwala D., Patel D., Dasgupta K. Investigating and Analyzing the Light-weight ciphers for Wireless Sensor Networks // INFOCOMP Journal of Computer Science, Vol. 8, Issue 2, pp. 39-50, 2009.
3. Rinne S., Eisenbarth T., Paar C. Performance Analysis of Contemporary Light-Weight Block Ciphers on 8-bit Microcontrollers // ECRYPT Workshop Software Performance Enhancement for Encryption and Decryption, June 11-12, 2007, Amsterdam, NL, pp. 33-43.
4. Проблемы и их решения в RFID технологии [Електронний ресурс]. Режим доступу: http://www.itsec.ru/articles2/Inf_security.
5. Фролова Г. Технология RFID. Проблемы и решения / Г. Фролова // Журнал «Склад и техника», 2007. – № 1.
6. Keith E. Mayes. Smart cards, tokens, security and applications/ Keith E. Mayes Konstantinos Markantonakis // Springer Science+Business Media, 2008. – С. 416.
7. Eisenbarth, S. Kumar, C. Paar, A. Poschmann, L. Uhsadel. A Survey of Lightweight Cryptography Implementations // IEEE Design & Test of Computers - Special Issue on Secure ICs for Secure Embedded Computing Vol. 24, Nr. 6, pp. 522-533, November 2007.
8. Çakiroğlu M. Software implementation and performance comparison of popular block ciphers on 8-bit low-cost microcontroller // International Journal of the Physical Sciences Vol. 5(9), pp. 1338-1343, 18 August, 2010.
9. Пуля П.А. Аспекти захищеної передачі даних в системах радіочастотної ідентифікації / П.А. Пуля, Т. Б. Крет// Матеріали першої Міжнародної наукової конференції студентів та молодих науковців «Сучасні інформаційні технології 2011». – Одеса, 2011. – Том 2. – С. 104-105.
10. Пуля П. Розроблення RFID-системи контролю доступу на основі легковагового шифрування / П. Пуля // Збірник тез доповідей секції кафедр «Захист інформації» та «Безпека інформаційних технологій» 69-ої студентської науково-технічної конференції. – Львів, 2011. – С. 17.
11. Гарасим Ю. Р. Метод загального резервування для забезпечення живучості системи захисту інформації / Дудикевич В. Б., Гарасим Ю. Р. // Науково-технічний журнал «Захист інформації» №2, 2010. – С. 74-84.

REFERENCES

1. Konidala D. M. (2007). RFID Tag-Reader Mutual Authentication Scheme Utilizing Tag's Access Password/. M. Konidala and K. Kim// Auto-ID Labs White Paper WP-HARDWARE-033, Jan– pp 25-86.
2. Jinwala D., Patel D., Dasgupta K. (2009). Investigating and Analyzing the Light-weight ciphers for Wireless Sensor Networks // INFOCOMP Journal of Computer Science, Vol. 8, Issue 2, pp. 39-50.
3. Rinne S., Eisenbarth T., Paar C. (2007). Performance Analysis of Contemporary Light-Weight Block Ciphers on 8-bit Microcontrollers // ECRYPT Workshop Software Performance Enhancement for Encryption and Decryption, June 11-12, Amsterdam, NL, pp. 33-43.
4. Problemy y ykh reshenyya v RFID tekhnolohyy [Elektronnyy resurs]. Rezhym dostupu: http://www.itsec.ru/articles2/Inf_security. (in Russian)

5. Frolova H. (2007). Tekhnolohyya RFID. Problemы y reshenyya / H. Frolova // Zhurnal «Sklad y tekhnyka»– Vol 1. (in Russian)
6. Keith E. Mayes. (2008). Smart cards, tokens, security and applications/ Keith E. Mayes Konstantinos Markantonakis // Springer Science+Business Media– pp. 416.
7. Eisenbarth, S. Kumar, C. Paar, A. Poschmann, L. Uhsadel. (2007). A Survey of Lightweight Cryptography Implementations // IEEE Design & Test of Computers - Special Issue on Secure ICs for Secure Embedded Computing Vol. 24, Nr. 6, pp. 522-533, November.
8. Çakiroğlu M. (2010). Software implementation and performance comparison of popular block ciphers on 8-bit low-cost microcontroller // International Journal of the Physical Sciences Vol. 5(9), pp. 1338-1343, 18 August.
9. Pulya P.A. (2011). Aspekty zakhyshchenoyi peredachi danykh v systemakh radiochastotnoyi identyfikatsiyi / P.A. Pulya, T. B. Kret// Materialy pershoyi Mizhnarodnoyi naukovoyi konferentsiyi studentiv ta molodykh naukovtsiv «Suchasni informatsiyni tekhnolohiyi 2011». – Odesa– Vol 2. – pp. 104-105.(in Ukrainian)
10. Pulya P. (2011). Rozroblennya RFID-systemy kontrolyu dostupu na osnovi lehkovahovoho shyfruvannya / P. Pulya // Zbirnyk tez dopovidey sektsiyi kafedr «Zakhyst informatsiyi» ta «Bezpeka informatsiynykh tekhnolohiy» 69-oyi student·s'koyi naukovo-tekhnichnoyi konferentsiyi. – L'viv– pp. 17. (in Ukrainian)
11. Harasym Yu. R. (2010.) Metod zahal'noho rezervuvannya dlya zabezpechennya zhyvuchosti systemy zakhystu informatsiyi / Dudykevych V. B., Harasym Yu. R. // Naukovo-tekhnichnyy zhurnal «Zakhyst informatsiyi» №2– pp. 74-84. (in Ukrainian)

LIGHTWEIGHT ENCRYPTION FOR SYSTEMS WITH LIMITED RESOURCES

V.B. Dydukevych[1], I.S. Sobchuk[1], L.M. Rakobovchuk[1], P.I. Garaniuk[1], I.P. Garaniuk[2].

1. Department of Information Security, National University "Lviv Polytechnic", Ukraine, Lviv city, S.Bandera St., 12, E-mail: Igorpolitech@gmail.com

2. Computerized Automation Systems, National University «Lviv Polytechnic», UKRAINE,. Lviv,. S.Bandera St., 12

The article considers the trends of the use of systems with limited resources. The analysis of the literature sources on the issue of efficiency of the use of lightweight cryptography has been conducted. A comparison of classical and modern encryption algorithms has been conducted. The paper has made a comparison of block symmetric algorithms AES, CAST5, Camelia, MARS and Serpent on such criteria: performance / memory with the implementation on available 8-bit microcontrollers with the AVR architecture in language C. The efficiency of symmetric algorithms of lightweight cryptography has been shown. An anticollision protocol has been created, which is based on the features of the data packets structure of EM4100 cards.

Key words– *cryptography, lightweight cryptography, lightweight encryption, stability of lightweight cryptography, efficiency of lightweight cryptography, software codes, AVR-microcontrollers, algorithm performance, anticollision protocol.*

Стаття надійшла до редакції 12.09.2016
Received 12.09.2016