УДК 004.056

Цопа В. Ю.
Кирилащук Т. Г.

ВИКОРИСТАННЯ ЛЕГКИХ БЛОЧНИХ ШИФРІВ ДЛЯ ЗАХИСТУ ІНТЕРНЕТУ РЕЧЕЙ

Вінницький національний технічний університет

Анотація

Розглянуто особливості архітектур легких блочних шифрів (SPN, структури Фейстеля та ARX-алгоритми) у контексті їхнього використання в IoT-системах. Охарактеризовано їхні переваги й недоліки, а також критерії ефективності, зумовлені лімітованими ресурсами мікроконтролерів.

Ключові слова: Інтернет речей, легка криптографія, блочний шифр, SPN, мережа Фейстеля, ARX.

Abstract

The architectures of lightweight block ciphers, including Substitution-Permutation Networks (SPN), Feistel structures, and ARX algorithms, for use in Internet of Things (IoT) devices are analyzed. Their advantages, disadvantages, and efficiency criteria are determined considering the hardware and software limitations of microcontrollers.

Keywords: Internet of Things, lightweight cryptography, block cipher, SPN, Feistel network, ARX.

Вступ

Сьогодні Інтернет речей (IoT) поєднує фізичні об'єкти за допомогою датчиків і мереж, пере–носячи їх у кіберпростір [2]. Забезпечення конфіденційності, цілісності та автентифікації передачі даних є критично важливим. Однак IoT-пристрої, як правило, базуються на 8-бітних або 4-бітних мікроконтролерах. Вони мають жорсткі обмеження щодо обсягу оперативної (RAM) та пос–тійної (ROM) пам'яті, розрядності регістрів та енергоспоживання. Традиційні алгоритми безпеки, такі як AES чи DES, мають занадто велику кількість логічних вентилів і високе розсіювання потужності, що робить їхнє використання в IoT практично неможливим. Ці обмеження зумовили розвиток нової галузі — легкої криптографії (Lightweight Cryptography) [1].

Результати дослідження

Блочні шифри вважаються основними робочими інструментами в криптографічному середовищі, оскільки вони є ефективнішими та досягають вищого рівня дифузії порівняно з потоковими шифрами . Вони оперують блоками даних, створюючи складні зв'язки за допомогою операцій конфузії (плутанини) та дифузії (розсіювання). Архітектурно легкі блочні шифри класифікуються на кілька основних типів. Важливою відмінністю легких шифрів від традиційних є зменшений розмір блоку даних. Зазвичай вони оперують блоками по 64 біти (на відміну від 128 біт у стандартному алгоритмі AES) та використовують ключі довжиною 80 або 128 біт. Такого рівня криптографічної стійкості цілком достатньо для захисту більшості базових IoT-додатків, але при цьому досягається суттєва економія обчислювальних ресурсів та пам'яті мікроконтролера. Структура Фейстеля оперує лише з половиною блоку даних за один раунд, тому вимагає більшої кількості раундів для забезпечення надійності. Її головна перевага полягає в тому, що функція розшифрування не вимагає великих додаткових витрат на реалізацію, оскільки для обох процесів використовується однаковий програмний код. Це суттєво зменшує вимоги до пам'яті. Типовими представниками є алгоритми CLEFIA, SIMON, SPECK та PICCOLO. Підстановочно-перестановочні мережі (SPN) використовують нелінійні шари підстановки (S-box) для конфузії та лінійні матриці перестановки (P-box) для дифузії. Ця архітектура має високий рівень внутрішнього паралелізму. Серед популярних

SPN-шифрів виділяють PRESENT (оптимізований для апаратних рішень), KLEIN та LED [3]. Проте SPN вимагає оборотності S-блоків для процесу розшифрування [1]. Для зменшення впливу атак побічними каналами та економії ресурсів також застосовуються ARX-архітектури (Addition-Rotation-XOR). Вони дозволяють мінімізувати кількість виконуваних операцій і часто не використовують класичні табличні S-блоки, що забезпечує високу швидкість програмної реалізації (наприклад, шифри LEA та Chaskey). Проектування якісного легкого шифру вимагає дотримання низки критеріїв: низької обчислювальної складності, високої пропускної здатності, мінімальних вимог до RAM/ROM, малого енергоспоживан–ня, а також стійкості до лінійного та диференціального криптоаналізу [1, 3].

Висновки

Програмні реалізації легких шифрів мають меншу вартість і забезпечують більшу гнучкість в обслуговуванні систем IoT. Вибір архітектури залежить від конкретних апаратних обмежень пристрою. Для економії пам'яті мікроконтролерів доцільніше використовувати структури Фейстеля або ARX-алгоритми, тоді як для забезпечення високої швидкості за рахунок паралелізму краще підходять SPN-шифри. Подальші дослідження мають бути спрямовані на оптимізацію таблиць розширення ключів та підвищення стійкості шифрів до сучасних методів криптоаналізу.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Sehrawat D., Gill N. S. Lightweight Block Ciphers for IoT based applications: A Review // International Journal of Applied Engineering Research. 2018. Vol. 13, No. 5. P. 2258-2270.

2. Madakam S., Ramaswamy R., Tripathi S. Internet of Things (IoT): A literature review // Journal of Computer and Communications. 2015. Vol. 3, No. 5. P. 164.

3. Bogdanov A. PRESENT: An ultra-lightweight block cipher / Bogdanov A., Knudsen L. R., Leander G. та ін. // Cryptographic Hardware and Embedded Systems (CHES 2007). 2007. Vol. 4727. P. 450-466.

Цопа Владислав Юрійович – студент 2 курсу, група 2БС-24Б, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, м. Вінниця, e-mail: vladtsopa58@gmail.com

Науковий керівник: ***Кирилащук Т.Г.*** – асистент кафедри захисту інформації факультет інформаційних технологій та комп’ютерної інженерії, Вінницький національний технічний університет, м. Вінниця, e-mail: kgt0998@gmail.com

Tsopa Vladyslav Y. – student of group 2BS-24B, Faculty of Information Technology and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, e-mail: vladtsopa58@gmail.com

Supervisor: ***Kyrylashchuk T***. – assistant of the department of information protection of the faculty of information technologies and computer engineering, Vinnytsia National Technical University, Vinnytsia, e-mail: kgt0998@gmail.com