ЛЕГКОВІСНА КРИПТОГРАФІЯ ВБУДОВАНИХ СИСТЕМ

Дорофєєва К. І., Ляшенко О. С., Мартиненко Я. А.
Харківський національний університет радіоелектроніки, Харків, Україна

В алгоритмах, які використовуються у звичайній криптографії, виникають проблеми в роботі у вбудованих системах, оскільки мають значну процесорну потужність та споживають велику кількість енергії. Тому сьогодні набуває популярності легковісна криптографія, яка використовується у вбудованих системах, радіочастотній ідентифікації та у сенсорних мережах. На відміну від систем, які можуть повноцінно функціонувати, вбудовані системи мають внутрішні обмеження, такі як: потужність, пам'ять, зберігання енергії. Саме легка криптографія призначена для таких видів систем. Вона є простішою і швидшою за звичайну, хоча менш захищеною. Тому дослідження низкоресурсної криптографії є важливою складовою для функціонування вбудованих систем [1]. Для них характерно зберігання, доступ і передача приватної, конфіденційної інформації. Таким чином, конфіденційність і цілісність ресурсів і послуг зазначених пристроїв є важливою проблемою, яку необхідно враховувати під час їх проєктування.

Метою доповіді є дослідження легкої криптографії у вбудованих системах, завдяки якій ці системи можуть функціонувати на рівні з системами, які мають значну потужність, енергію та пам'ять.

У доповіді наводяться приклади використання алгоритмів для забезпечення належного функціонування у вбудованих системах. Прикладами можуть бути Elliptic Curve Cryptography (ECC) і Hyperelliptic Curve Cryptography (HECC), DES, 3DES і Clefia. ECC та HECC мають меншу довжину операндів і відносно нижчі обчислювальні вимоги. Крім цього у них ключова пара коротша за алгоритм RSA. З підвищенням рівня безпеки розміри ключів RSA ростуть набагато швидше, ніж ECC [2]. Хоча DES, 3DES і Clefia добре працюють у системах, які мають належну потужність обробки та пам'яті, вони можуть бути призначені для легковісної криптографії на вбудованих системах і підтримувати високий рівень безпеки.

Отже, для подолання багатьох проблем, які виникають у традиційної криптографії, пропонуються полегшені методи криптографії. Вони включають обмеження, пов'язані з фізичним розміром, вимогами до обробки, обмеженням пам'яті та витратою енергії.

Список літератури

1. Joaquin Garcia-Alfaro, Georgios Lioudakis. Data Privacy Management and Autonomous Spontaneous Security. 2013. P. 333–349. DOI: https://dl.acm.org/doi/10.1007/978-3-642-54568-9_21

2. William J. Buchanan, Shancang Li, Rameez Asif. Lightweight cryptography methods. 2017. P. 187–201. DOI: https://doi.org/10.1080/23742917.2017.1384917