УДК 004.056
Л. Сава
Тернопільський національний технічний університет імені Івана Пулюя

РОЗРОБЛЕННЯ АЛГОРИТМІВ НЕСИМЕТРИЧНОГО ШИФРУВАННЯ ДЛЯ МОБІЛЬНИХ ЗАСОБІВ ЗВ'ЯЗКУ

L. Sava

DEVELOPMENT OF ASYMMETRIC ENCRYPTION ALGORITHMS FOR MOBILE COMMUNICATIONS

Розвиток інтернет-технологій разом із мобільними, комп'ютерними технологіями сформували смарт-технології, які дозволяють формувати як кіберфізичні, а й соціокіберфізичні системи. Основою смарттехнологій є комплексування стандартів бездротових каналів із мобільними та комп'ютерними протоколами. Крім цього, технології 4G/5G комплексують із різними веб-платформами з урахуванням цифровізації послуг у кіберпросторі. Для забезпечення послуг безпеки автентичності та цілісності, як правило (шифруються понад 80% трафіку Хром), використовується мережевий протокол SSL/TLS, заснований на гібридизації симетричних алгоритмів шифрування з алгоритмами гешування (режим AEAD), що забезпечує досконалу пряму секретність. Однак, цей протокол піддається не тільки атакам "Зустріч на середині", POODLE, BEAST, CRIME, BREACH, а з появою повномасштабного квантового комп'ютера може бути зламаний.

Створення сучасних синтезованих мереж ґрунтується на гібридизації технологій бездротових мобільних та соціо-кіберфізичних систем на основі Інтернету речей. Класичні комп'ютерні системи та технології інтегрують елементи Інтернет речей та формують принципово нові напрямки розвитку IT-індустрії –smart-технології, які поєднують досягнення мобільних, бездротових та соціо-кіберфізичних систем.

Однак стрімке розширення mesh-, сенсорних мереж з використанням стандартів бездротових каналів: мобільних технологій LTE, IEEE802.16, IEEE802.16e, IEEE802.15.4, IEEE802.11, Bluetooth не забезпечує безпеку інформаційних потоків. У гонитві за надшвидкістю в таких каналах не надаються послуги конфіденційності та цілісності. Протокол Diameter забезпечує взаємодію між клієнтами з метою аутентифікації, авторизації та обліку різних сервісів, проте має суттєві недоліки до сучасних кібератаків.

Для забезпечення безпеки в кіберфізичних системах на основі інтернет-речей використовується стандарт KNX (ISO/IEC 14543) на основі використання VPN-каналів (шифрування AES-128, -256). Проте, всі наявні механізми безпеки не забезпечать необхідний рівень безпеки в постквантовий період (поява повномасштабного квантового комп'ютера). Фахівці NIST США висувають сумніви у стійкості сучасних симетричних та несиметричних криптосистем (включаючи алгоритми та на еліптичних кривих). У таких умовах постквантові криптоалгоритми на основі синтезу теорій завадостійкого кодування та захисту інформації – крипто-кодові конструкції можуть розглядатися як альтернативний механізм забезпечення безпеки.

Крім цього, виникає необхідність розгляду концепції двох контурів безпеки (внутрішнього – безпосередньо інфраструктура мережі та зовнішнього – хмарні платформи – сервера управління кіберфізичними системами) в умовах інтеграції мереж та хмарних технологій.

Для забезпечення безпеки у постквантовий період, спеціалістами NIST пропонується використати постквантові алгоритми. Такі алгоритми вимагають для симетричних криптосистем збільшення до 512 біт ключових послідовностей (при цьому забезпечується безпечний час близько 60 років) або використання постквантових несиметричних криптосистем (PQAS – post-quantum asymmetric cryptosystems). Серед конкурсантів третього туру конкурсу виділяються алгоритми, побудовані на комплексуванні теорії завадостійкого кодування та криптографії. Крипто-кодові конструкцій Мак-Еліса та Нідеррайтера на еліптичних кодах, які забезпечують захист від атаки Сидельникова та зниження енергоємності. Крім цього вони інтегровано забезпечують виправлення помилок в інформаційній послідовності. Таким чином, використання для безпеки постквантових криптосистем-крипто-кодових конструкцій забезпечує своєчасний перехід на алгоритми постквантового періоду.