УДК 004.056
О. Ганайчук
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

ВИКОРИСТАННЯ ОПТИМІЗОВАНИХ АЛГОРИТМІВ АСИМЕТРИЧНОЇ КРИПТОГРАФІЇ (CL-PKE) ДЛЯ ПРИСТРОЇВ ІЗ ОБМЕЖЕНИМИ РЕСУРСАМИ

UDC 004.056
O. Hanaichuk

USE OF OPTIMIZED ALGORITHMS OF ASYMMETRIC CRYPTOGRAPHY (CL-PKE) FOR RESOURCE CONSTRAINED DEVICES

Пристрої з обмеженими ресурсами, такі як датчики та RFID, використовуються в багатьох областях застосування для визначення, зберігання та передачі конфіденційних даних. Ці дані мають бути зашифровані для забезпечення конфіденційності. Реалізація традиційних методів шифрування з відкритим ключем цими пристроями завжди є складною, оскільки вони мають дуже обмежені обчислювальні ресурси.

Щоб подолати загрозу атаки, необхідна інфраструктура відкритих ключів (PKI), яка керує сертифікатами, щоб створити захищену систему в традиційних налаштуваннях криптографії з відкритим ключем. Однак на практиці PKI стикається з багатьма проблемами, особливо з масштабованістю інфраструктури. Ідея, що стоїть за шифруванням із відкритим ключем без сертифікатів (CL-PKE), полягає в тому, що навіть якщо супротивник успішно замінює відкритий ключ жертви своїм власним вибором, він все одно не може розшифрувати повідомлення, зашифроване відкритим ключем, який він опублікував. Хоча ця ідея є досить непоганою, вона не підходить для традиційної системи відкритих ключів, в якій закритий ключ суб'єкта відповідає лише відкритому ключу суб'єкта.

Також PKI вимагає постійного онлайн-сервера сертифікації. Ця проблема вирішується тим, що CL-PKE залежить від офлайн-довіреної третьої сторони (TTP) для видачі повних приватних ключів (IBE) або часткових приватних ключів (CL-PKE) користувачам у мережі. Однак IBE страждає від проблеми депонування ключів, при якій усі приватні ключі користувачів розкриваються, якщо TTP скомпрометований або стає шкідливим. CL-PKE не страждає від проблеми депонування ключів і кваліфікується як безпечна схема шифрування. Однак алгоритм шифрування всіх існуючих схем IBE і CL-PKE вимагає обчислення модульного піднесення до степеня та операцій дволінійного створення пари над адитивною еліптичною кривою, які є обчислювально дуже дорогими криптографічними операціями. У контексті цього була розроблена полегшена оптимізована схема CL-PKE, в якій операції експонування та створення пари повністю виключаються під час шифрування і передбачає лише обчислення простих операцій додавання та множення на еліптичній кривій.

Література.

1. Dent, A., Libert, B., and Paterson, K.: "Certificateless Encryption Schemes Strongly Secure in the Standard Model"; To appear in Proc. PKC 2008, LNCS, Springer-Verlag (2008)
2. Ian Blake, Gadiel Seroussi, and Nigel Smart. 1999. Elliptic cur ves in cryptography.Vol. 265. Cambridge University Press.