ОПТИМАЛЬНІ ДЕКОМПОЗИЦІЇ БАГАТОРОЗРЯДНИХ ЦІЛИХ ЧИСЕЛ

Просолов В.В., Мельникова О.А.
Харківський національний університет радіоелектроніки, Харків, Україна

Загальним завданням у впровадженні багатьох криптосистем з відкритим ключем є піднесення до степеню в деякій комутативній групі G, тобто оцінка продукту. Приклад груп включає (Z / nZ) для деякого цілого числа n, наприклад для перевірки підписів ElGamal або DSA; групи раціональних точок на еліптичних кривих над кінцевими полями, наприклад для перевірки підписів ECDS; і класові групи уявних-квадратичних порядків, наприклад для перевірки RDSA підписів [1 - 2]. Ми маємо k = 2 для верифікації DSA та ECDSA і k = 3 для верифікації ElGamal і RDSA. Більші значення k з'являються в протоколах фірмових знаків. У цій роботі ми допускаємо також k = 1 для алгоритмів; міркування ефективності можуть ігнорувати цей випадок. Добре відомо, що взагалі надмірно неефективно обчислювати повноваження g_i^{ei} окремо, а потім перемножувати їх. Натомість зазвичай застосовуються специфічні алгоритми для однократного піднесення до степеню.

Звичайний підхід для однократного піднесення до степеню поєднує всі елементи вхідної групи g_i один з одним на етапі попереднього обчислення, потім етап оцінки одночасно переглядає всі показники. У цій роботі ми обговорюємо альтернативний підхід, коли на етапі попередньої обчислювальної дії показники обробляються окремо. У цьому підході на етапі оцінювання використовується переплетення генераторів та експонентів для різних і, а не обробка декількох і одночасно.

Метою доповіді є вивченні та вдосконаленню методів n-кратної декомпозиції багаторозрядних числових значень.

В роботі розглянуто існуючі методи швидкого піднесення до степеню по модулю, які використовуються в сучасних криптоалгоритмах та алгоритми однократного піднесення до степеню по модулю. Проводиться порівняння алгоритмів піднесення до степеню для знаходження їх переваг та недоліків. Результатом дослідження розробленого алгоритму піднесення до степеню з декомпозицією є те, що він ефективніший за свої аналоги, якщо використовується фіксована основа, цю властивість можливо використовувати у деяких сучасних криптосистемах.

Список літератури

1. American National Standards Institute (ANSI). Public key cryptography for the financial services industry: The elliptic curve digital signature algorithm (ECDSA). ANSI X9.62, 1998.

2. Federal Information Processing Standards Publication 186 – 4 (FIPS PUB 186 - 4). Digital Signature Standard (DSS) // U.S. Department of Commerce. Technology Administration, National Institute of Standards and Technology (NIST). — 2013. — 130 p.