Колосов В.О., Дербуновіч Л.В., Укаїна, Харків

НОВІ АРХІТЕКТУРИ З ВИКОРИСТАННЯМ АЛГОРИТМУ МНОЖЕННЯ МОНТГОМЕРІ

У доповіді розглянуті нові об'єднання архітектури, в яких використовується алгоритм множення Монтгомері для реалізації модульного множення для цілих і бінарних многочленів. Уніфікований підхід, сприяючий підтримці більшості криптосистем з відкритими ключами таких як RSA, Diffie-Hellman, криптосистем на елептичних кривих і інших. До того ж архітектура високо ефективна по апаратним витратам і швидкодії.

Колосов В. А., Дербунович Л.В., Украина, Харьков

НОВЫЕ АРХИТЕКТУРЫ С ИСПОЛЬЗОВАНИЕМ АЛГОРИТМА УМНОЖЕНИЯ МОНТГОМЕРИ

В докладе рассмотрены новые объединение архитектуры в которых используется алгоритм умножения Монтгомери для реализации модульного умножения для целых и бинарных многочленов. Унифицированный подход, способствующий поддержке большинству криптосистем с открытыми ключами таких как RSA, Diffie-Hellman, криптосистем на элептических кривых и других. К тому же архитектура высоко эффективна по аппаратным затратам и быстродействию.

Kolosov V. O., Derbunovich L.V., Ukraine, Kharkov

NEW ARCHITECTURES WITH THE USE OF ALGORITHM OF INCREASE OF MONTGOMERI

We propose a new unified architecture that utilizes the Montgomery Multiplication algorithm to perform a modular multiplication for both integers and binary polynomials and NTRU’s polynomial multiplications. The unified design is capable of supporting a majority of public-key cryptosystems such as NTRU, RSA, Diffie-Hellman key exchange, and Elliptic Curve schemes, among others. Furthermore, the architecture is highly efficient in terms of area and speed.