Список литературы

1. Шокуров А.В., Кузюрин Н.Н., Фомин С.А. Решетки, алгоритмы и современная криптография. М.: Институт системного программирования РАН, 2011. 130 с.

2. Gentry C. Fully homomorphic encryption using ideal lattices // STOC. 2009. P. 169–178.

3. Micciancio D. Complexity of Lattice Problems. A Cryptgraphic Perspective. Kluwer Academic Publishers, 2002.

АППАРАТНЫЙ МОДУЛЬ ШИФРОВАНИЯ ПОТОКОВЫХ ДАННЫХ

Ю.И. Сапронова

Программные реализации являются более дешевыми и гибкими, однако аппаратные системы имеют выигрыш в производительности и являются гораздо более надежными, за счет использования генератора истинно случайных чисел, а также хранения ключей непосредственно на плате шифратора, а не в оперативной памяти компьютера.

Комбинированный (гибридный) алгоритм шифрования, сочетает в себе симметричный и асимметричный методы шифрования: с помощью симметричного алгоритма шифруется исходная информация, а с помощью асимметричного – сессионный ключ, используемый симметричным алгоритмом. Такой способ устраняет проблему распространения ключей для симметричных алгоритмов, помимо этого, такой способ решает проблему быстродействия асимметричных алгоритмов за счет того, что шифрованию подлежат не передаваемые сообщения, а только сессионный ключ.

Для шифрования данных выбран потоковый шифр Grain, в связи с тем, что он обладает наилучшей производительностью, при этом потребляя меньшее количество ресурсов (по сравнению с AES, MICKEY и Trivium [1]). Кроме того, производительность данного алгоритма может быть увеличена за счет использования дополнительного количества ресурсов FPGA (добавлением параллельных блоков сдвиговых регистров с линейной и нелинейной обратной связью). Для шифрования сессионного ключа выбран алгоритм RSA.

Анализ разработанной системы показал, что достижимая частота работы модуля в режиме шифрования при условии наличия одного блока сдвиговых регистров с линейной и нелинейной обратной связью составила 50 МГц. Для обеспечения достаточного уровня защиты данных синхронизация блоков и, при необходимости, смена сессионного ключа должна производиться каждый час.

Список литературы

1. Efficient FPGA Implementations of High-Dimensional Cube Testers on the Stream Cipher Grain-128 [Электронный ресурс]. URL: https://eprint.iacr.org/2009/218.pdf (дата обращения: 02.05.2019).

ШИФРОВАНИЕ ДАННЫХ НА ОСНОВЕ КВАТЕРНИОНОВ

Ю.И. Сапронова

Алгебра кватернионов представляет собой ассоциативную четырехмерную гиперкомплексную алгебру над полем действительных чисел с уникальными законами умножения. Шифрование, основанное на кватернионах, представленное в [1], использует уникальные свойства кватернионов для поворота векторов данных в трехмерном пространстве. Как известно, вращение вектора представляется в виде результата произведения кватерниона вращения, вектора, представленного в виде кватерниона, и обратного кватерниона вращения.

Умножение кватернионов является затратной вычислительной операцией. Экспериментально было показано, что применение логарифмической системы счисления для вычисления произведения кватернионов может сократить затраты памяти на хранение коэффициентов кватернионов на 14% (при использовании логарифмического полярного