**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

представления кватерниона в форме Кэли-Диксона), тем самым можно увеличить количество блоков обработки информации.

Процесс шифрования заключается в применении нескольких вращений к каждому из блоков шифруемой информации. При этом начальными значениями для алгоритма является порядок вращения вектора, а также кватернион вращения и синхропосылка, представленная в виде кватерниона инициализации. Рассмотренный метод шифрования можно считать симметричным потоковым алгоритмом с размером единицы шифруемой информации равной четырем машинным слова. Важно отметить, что при использовании такого алгоритма количество возможных ключей фактически безгранично из-за возможности установки порядка вращения и четырех параметров кватерниона вращения и синхропосылки. Однако, ввиду высокой сложности вычислений произведения кватернионов невозможно добиться высокой производительности данного алгоритма.

**Список литературы**

1. A new Quadripartite Public-Key Cryptosystem / T. Nagase [et al.] // ISCIT 2004. Sapporo, 26–29 October 2004. P.74–79.

## ПОДГОТОВКА СПЕЦИАЛИСТОВ ДЛЯ БЕЛОРУССКОЙ АЭС

С.М. Сацук

Подготовка высококвалифицированных кадров – один из самых важных факторов безопасной и эффективной эксплуатации атомной электростанции. Государственная программа подготовки кадров для ядерной энергетики Республики Беларусь на 2008–2020 годы была утверждена в связи с принятием решения о строительстве Белорусской атомной электростанции согласно Постановлению Совета Министров № 1329 от 10 сентября 2008 г. С 2016 года задача подготовки кадров осуществляется в рамках Государственной программы «Образование и молодежная политика» на 2016-2020 годы (Подпрограмма 10 «Подготовка кадров для ядерной энергетики»), утвержденной Постановлением Совета Министров Республики Беларусь № 250 от 28 марта 2016 г.

В соответствии с рекомендациями Международного агентства по атомной энергии (МАГАТЭ) система подготовки кадров для ядерной энергетики должна базироваться на принципах применения системного подхода к подготовке персонала, основанного на соответствующих документах МАГАТЭ, международном опыте, а также на соответствии системы подготовки персонала требованиям законодательства в области ядерной и радиационной безопасности.

В этой связи ряд стран, членов МАГАТЭ, как с развитой ядерной инфраструктурой, так и с развивающейся, выразили желание о сотрудничестве для обмена опытом в области ядерной энергетики и обеспечения стабильного развития ядерного сектора. В 2015 году была создана Региональная сеть STAR-NET.

Основной целью сети STAR-NET является улучшение качества подготовки кадров для ядерной энергетики. Основными направлениями деятельности сети являются: образовательная деятельность и учебно-методическая работа; профессиональная подготовка и взаимодействие с атомной промышленностью; исследовательская и научно-техническая деятельность; информационные системы поддержки деятельности сети.

Региональная сеть образования и подготовки кадров в области ядерных технологий STAR-NET является связующим звеном для реализации научно-образовательных проектов в области подготовки кадров для ядерной энергетики.