сети предполагает, что легитимные пользователи и подслушивающие аналитики случайным образом расположены на большой географической территории в соответствии с некоторыми вероятностными распределениями.

Рассматривается децентрализованная беспроводная сеть в двумерном пространстве на основе гомогенной модели однородного точечного пуассоновского процесса PPP. Местоположения легитимных передатчиков соответствуют однородному PPP с интенсивностью λ. Каждый передатчик имеет предполагаемый приемник на фиксированном расстоянии r в случайном направлении [1, 2].

Определяются следующие основные показатели системы защиты.

Граф защищенности. Используется для изучения свойств связности среди легитимных пользователей сети и характеризует существование связи с полной защитой между любыми двумя легитимными пользователями.

Пропускная способность защищенной сети. Учитывает одновременные передачи между всеми допустимыми линиями связи и дает математически поддающийся измерению показатель достижимой пропускной способности сети с заданным требованием защиты на основе перколяционной модели.

Отключение соединения. Событие, когда пропускная способность канала от передатчика для предполагаемого приемника ниже скорости кодового слова. Вероятность этого события называется вероятностью отказа соединения, обозначается как Pco

Сбой в работе системы защиты. Событие, когда пропускная способность канала от передатчика, по крайней мере, к одному перехватчику превышает структурную избыточность. Вероятность того, что это событие произойдет, называется вероятностью отключения секретности, обозначаемой как Pso.

Список литературы

1. Franceschetti R. Random Networks for Communication: from Statistical Physics to Information Systems. Cambridge University Press, 2008.

2. Vaze R. Random Wireless Networks, Cambridge University Press, 2015.

РЕШЕТЧАТАЯ КРИПТОСИСТЕМА НА ОСНОВЕ МНОГООБРАЗИЯ БАЗИСОВ

С.Б. Саломатин, В.В. Панькова

Криптографические механизмы используют библиотеки решетчатого кодирования с масштабируемой реализации примитивов гомоморфного преобразования [1, 2].

Базовая структура решетчатых криптосистем соответствует архитектуре криптосистемы Мак-Элиса с секретной функцией на основе решеток [3]. Исходная криптосистема описывается следующим образом:

Генерация ключей. Формируется удобный с вычислительной точки зрения базис решетки R. Базис R преобразуется в трудно обратимый базис Q с помощью унимодулярного преобразования.. Базис Q используется в качестве открытого ключа (открытого базиса), а базис R – в качестве секретного ключа шифрования (закрытого базиса).

Процедура зашифрования. Выбирается любой вектор решетки **w**, используя открытый базис Q, и к нему добавляется вектор открытого текста **p**. Вектор $\mathbf{c} = \mathbf{w} + \mathbf{p}$ представляет собой зашифрованный текст.

Расшифрование. Используя закрытый базис, решается задача вычисления ближайшего вектора решетки **nw** к зашифрованному тексту **c**. Найденный ближайший вектор решетки **nw** вычитается из зашифрованного текста для получения открытого текста $\mathbf{p} = \mathbf{c}–\mathbf{nw}$.

Безопасность криптосистемы основывается на следующих трех предположениях. Легко вычислить неудобный базис Q из базиса R, но вычислительно трудно решить обратную задачу. Легко создать случайный вектор решетки даже с неудобным базисом Q. Легко найти ближайший вектор с удобным базисом R, но трудно это сделать с открытым базисом Q.

Дополнительное усиление системы состоит в использовании нормальной формы Эрмита для базиса открытого ключа, базисов генераторных матриц алгебро-геометрических структур и построения семейств PRF на основе решеток, через задачи обучения с ошибками (LWE).

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