Министерство образования Республики Беларусь
Учреждение образования
Белорусский государственный университет
информатики и радиоэлектроники

УДК 004.056.5

Филиппов
Николай Сергеевич

КОДЕК КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ НА БАЗЕ *RASPBERRY PI*

АВТОРЕФЕРАТ

на соискание степени магистра техники и технологии

по специальности 1-39 81 03 Информационные радиотехнологии

Научный руководитель
Саломатин Сергей Борисович
кандидат технических наук, доцент

Минск 2020

КРАТКОЕ ВВЕДЕНИЕ

Вопросы защиты информации становятся все более актуальными с развитием сетевых технологий. Сегодня нас окружает все большее количество гаджетов, способных обмениваться друг с другом данными с участием пользователя или без него. По мере того, как Интернет становится более коммерциализированным, большее внимание уделяется защите персональных данных, финансовых операций и противостоянию киберугрозам. Учитывая особенности устройств, а также их различную природу, вопросы безопасности сетевого взаимодействия требуют рассмотрения новых аспектов. Исследования последних лет показывают, что семь из десяти популярных смарт-устройств уязвимы для потенциальных атак. Большинство выявленных угроз безопасности были связаны с незашифрованными данными, сбором персональных данных, уязвимыми пользовательскими интерфейсами и небезопасными соединениями. Основные проблемы обеспечения безопасности обусловлены тем, что существующие методы и средства защиты изначально разрабатывались для настольных компьютеров, и не учитывали особенности и ограничения устройств Интернета вещей.

Цели безопасности для интернета вещей остаются такими же, как и в других компьютерных сетях, однако появляются и некоторые уникальные проблемы, связанные с использованием криптографии с открытым ключом, которая необходима для защиты связи между узлами датчиков. Криптографические алгоритмы с открытым ключом обычно реализуются сложным образом, что приводит к значительным накладным расходам по отношению к времени выполнения и энергопотреблению.

Одним из наиболее популярных криптографических алгоритмов в настоящее время является *RSA*. Для обеспечения достаточного уровня криптостойкости, используя данный алгоритм, рекомендуется использовать как минимум 2048-битные ключи, что в свою очередь увеличивает занимаемую память устройства, время генерирования, шифрования и дешифрования.

В данной работе рассматривается реализация алгоритмов, основанных на эллиптических кривых, анализируется их производительность по сравнению с алгоритмом *RSA* в контексте устройства интернета вещей *raspberry pi*, а также вопрос удовлетворения условиям ограниченности памяти и вычислительной мощности устройств интернета вещей.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Цель и задачи исследования.

Основной целью магистерской диссертации является разработка кодека на основе анализа криптографических алгоритмов, основанных на эллиптических кривых с целью использования их в устройствах с ограниченными ресурсами. Задачами работы являются: анализ существующих решений криптографической защиты информации в сети интернета вещей; реализация криптографических алгоритмов цифровой подписи и шифрования с использованием эллиптических кривых на языке программирования *Python*, сравнительный анализ с наиболее популярным алгоритмом *RSA* в контексте устройств интернета вещей, анализ криптостойкости данных алгоритмов, увеличение производительности криптографических алгоритмов в устройствах интернета вещей с использованием облачных веб-сервисов; внедрение скрытого управляющего сигнала в передаваемое сообщение с использованием алгоритмов, основанных на эллиптических кривых.

Объектом исследования является система защиты информации в сети интернета вещей. Предметом исследования является криптосистемы *ECDSA* и *ECDH*, работающие в условиях ресурсных ограничений.

Новизна полученных результатов.

В ходе работы были реализованы алгоритмы криптографической защиты информации, основанные на эллиптических кривых, на языке программирования *Python* для устройства интернета вещей *raspberry pi*, позволяющие гибко изменять свою конфигурацию, в отличие от существующего протокола *TLS*. Впервые реализовано внедрение скрытого управляющего сигнала с использованием данных криптографических алгоритмов, а также увеличена производительность данных алгоритмов с использованием облачного сервиса *Heroku* для устройств интернета вещей в 2 раза.

Положения, выносимые на защиту.

Алгоритмы, основанные на эллиптических кривых, имеют повышенную производительность в устройствах интернета вещей и других устройствах, имеющих ограниченные ресурсы, такие как память и вычислительная мощность, по сравнению с наиболее популярным криптографическим алгоритмом *RSA*.

Облачные веб-сервисы, такие, как *Heroku*, позволяют получить увеличение производительности криптографических алгоритмов, используемых в сети интернета вещей в 2 раза.

Алгоритмы, основанные на эллиптических кривых, в комбинации с стеганографическими алгоритмами, такими, как *LSB,* позволяют реализовать алгоритм внедрения управляющего сигнала в устройствах с ограниченными ресурсами, не увеличивая размер передаваемого сообщения.

Апробация результатов диссертации.

Результаты исследований были представлены на 55 и 56 научных конференциях аспирантов, магистрантов и студентов.

Опубликованность результатов исследования.

Результаты исследований были опубликованы в виде тезисов 55 и 56 научных конференций аспирантов, магистрантов и студентов, а также материалах международного научно-технического семинара «Телекоммуникации: сети и технологии, алгебраическое кодирование и безопасность данных».

Структура и объем диссертации.

Работа представлена в 5 разделах. В материалах магистерской диссертации отражены следующие вопросы: обзор существующих методов криптографической защиты информации в сети интернета вещей; обзор устройства *raspberry pi*; краткие теоретические сведения об эллиптических кривых; алгоритмы, основанные на алгебре эллиптических кривых; криптоанализ данных алгоритмов; практическая реализация алгоритмов в устройстве *raspberry pi*; сравнительный анализ с алгоритмом *RSA*; практическое приложение внедрения скрытого управляющего сигнала в передаваемое сообщение; способ увеличения производительности криптографических алгоритмов, основанных на эллиптических кривых с помощью облачных веб-сервисов.

Общий объем работы составил 80 страниц, 54 иллюстрации, 7 таблиц.

В ходе написания магистерской диссертации использовалось 20 библиографических источников.

КРАТКОЕ СОДЕРЖАНИЕ РАБОТЫ

В первом разделе диссертации рассматриваются функции устройства *raspberry pi zero w* в сети интернета вещей, обзор существующих решений криптографической защиты информации в сети интернета вещей, симметричные и асимметричные криптографические алгоритмы.

Во втором разделе рассматриваются общие теоретические сведения об эллиптических кривых, а также производится выбор эллиптических кривых для практической реализации алгоритмов цифровой подписи и шифрования.

В третьем разделе рассматриваются криптографические алгоритмы, основанные на эллиптических кривых, а именно алгоритм цифровой подписи *ECDSA* и алгоритм шифрования, основанный на алгоритме обмена ключами *ECDH*, их принцип работы, а также представлены блок-схемы данных алгоритмов.

В четвертом разделе рассматривается процесс конфигурации устройства *raspberry pi*, практическая реализация криптографических алгоритмов, основанных на эллиптических кривых на языке программирования *Python* и анализ их производительности на устройстве *raspberry pi*, производится сравнительный анализ производительности алгоритмов *ECDSA* и *RSA*, рассматривается реализация способа внедрения скрытого управляющего сигнала с использованием данных алгоритмов и стеганографического алгоритма *LSB*, рассмотрена возможность увеличения производительности криптографических алгоритмов в устройствах интернета вещей с использованием облачной платформы *Heroku*.

В пятом разделе рассматривается анализ устойчивости данных алгоритмов к различным атакам, таким как атака перебором, алгоритм «baby step giant step» и алгоритм ρ Полларда, представлены блок-схемы алгоритмов, а также их реализация на языке программирования *Python*.

ЗАКЛЮЧЕНИЕ

В ходе исследований был разработан кодек на основе сравнительного анализа производительности алгоритмов, основанных на эллиптических кривых, с алгоритмом *RSA* на устройстве *raspberry pi*. Было выявлено, что алгоритмы, основанные на эллиптических кривых, имеют чем больший требуемый уровень криптостойкости, тем большую производительность при генерации пар ключей и подписи сообщения, однако *RSA* имеет практически константное время верификации цифровой подписи, равное 0.01 с, в то время, как затраченное время для алгоритма на эллиптических кривых увеличивается по мере увеличения размера ключа. В связи с этим было принято решение воспользоваться облачным веб-сервисом *Heroku* для увеличения производительности данной части алгоритма. После реализации веб-сервиса, скорость верификации подписи увеличилась в 2 раза, однако осталась ниже, чем у *RSA*.

Показано, что ключи, генерируемые алгоритмами, основанными на эллиптических кривых, имеют длину, равную удвоенному значению требуемого уровня криптостойкости. Это позволяет получить выигрыш в занимаемой ключом памяти устройства тем больший, чем выше требуемый уровень криптостойкости.

В ходе работы, на устройстве *raspberry pi,* были реализованы алгоритм цифровой подписи *ECDSA* и метод шифрования, основанный на алгоритме обмена ключами *ECDH* с помощью языка программирования *Python,* а также практическое приложение по внедрению скрытого управляющего сигнала в аудиофайл с использованием алгоритмов *LSB, ECDH* и *ECDSA.*

Также был произведен сравнительный анализ криптостойкости алгоритмов с использованием трех атак: перебором, алгоритм «*baby step, giant step*» и алгоритм ρ Полларда, алгоритмы которых были также реализованы на языке программирования *Python*. Результаты экспериментов показали, что алгоритм «*baby step, giant step*» имеет максимальную скорость взлома закрытого ключа, однако требует большего объема памяти, в то время, как алгоритм ρ Полларда требует меньше памяти, но скорость взлома ниже, чем у алгоритма «*baby step, giant step*».

Алгоритмы, основанные на эллиптических кривых, имеют повышенную производительность, а также меньшие размеры ключей, что удовлетворяет современным требованиям криптографической защиты информации устройств с ограниченными ресурсами, используемые в сети интернета вещей. Использование облачных веб-сервисов позволяет повысить производительность отдельных частей алгоритмов.

Также, в настоящее время, до практического использования квантовых компьютеров, можно сказать, что данные алгоритмы являются оптимальным решением криптографической защиты информации в устройствах с ограниченными ресурсами.