ИССЛЕДОВАНИЕ ЭФФЕКТИВНОГО ИСПОЛЬЗОВАНИЯ БЛОЧНЫХ ШИФРОВ НА БАЗЕ IOT- УСТРОЙСТВА

Аль-Маави Хайдер Муайад Ахмед

магистрант, Белгородский государственный национальный исследовательский университет, РФ, г. Белгород

RESEARCH ON THE EFFECTIVE USE OF BLOCK CIPHERS BASED ON AN IoT DEVICE

Al-Maawi Hayder Muayad Ahmed

Master student, Belgorod State National Research University, Russia, Belgorod

Аннотация. В ближайшие годы ожидается присоединение большого количества устройств, которые приведут к новой форме взаимодействия между миром реального и виртуального. В этом многообещающем сценарии, известном как концепция Интернет Вещей (IoT), взаимодействуют разные объекты, такие как датчики, промышленные роботы, автомобили, бытовая техника, среди прочего, подключены постоянно к сети Интернет. Одна из главных проблем, налагаемых Интернетом Вещей - это взаимосвязь устройств с неоднородными характеристиками в основном, с точки зрения коммуникационных возможностей, используемых устройств и сетевых протоколов. Вот почему модель соединение различных устройств включает в себя промежуточное устройство известный как шлюз. Этот шлюз служит централизованным элементом для управление устройствами, которые составляют приложение IoT. Кроме того, получается необходимо для передачи информации в Интернет.

Abstract. In the coming years, a large number of devices are expected to join, which will lead to a new form of interaction between the real and virtual worlds. In this promising scenario, known as the Internet of Things (IoT) concept, various objects interact, such as sensors, industrial robots, cars, home appliances, among other things, constantly connected to the Internet. One of the main problems imposed by the Internet of Things is the interconnection of devices with heterogeneous characteristics mainly in terms of communication capabilities, devices used and network protocols. This is why the interconnection model of various devices includes an intermediate device known as a gateway. This gateway serves as a central element for managing the devices that make up the IoT application. In addition, it turns out necessary to transmit information to the Internet.

Ключевые слова: блочные шифры; Интернет вещей; криптоанализ; сети Фейстеля, легковесные шифры; SPN; RFID.

Keywords: block ciphers; Internet of things; cryptoanalysis; Feistel; lightweights cipher; SPN; RFID.

В современном высокотехнологичном мире с каждым днем все больше устройств и приборов заменяется их аналогами нового поколения, которые, в сущности, имеют одно и то же базовое

использование, но теперь они «умные». Сам термин «умный» означает, что эти устройства теперь могут подключаться к другим устройствам пользователя и обмениваться информацией для того, чтобы настроить их функциональные возможности в соответствии с потребностями пользователя или даже позволить пользователю контролировать все их из одной точки. Все вышесказанное сходится в одном: все эти «умные» устройства должны быть подключены к большой сети быть доступны из любой точки мира.

Существует важная, но в то же время простая проблема, связанная с концепцией Интернета вещей: безопасность. В связи с тем, что все эти устройства будут подключены к Интернету, должны существовать механизмы безопасности, которые не позволят злонамеренный доступ к ним и одновременно защищают обмениваемые данные. Это уже решенная проблема для современных ПК и мобильных устройств, однако нельзя сказать то же самое для устройств, которые составляют IoT. Такие устройства в большинстве своем имеют очень ограниченный набор ресурсов (небольшие объемы ОЗУ, ПЗУ и питание) и возможностей (низкая вычислительная мощность), которые не могут противостоять реализациям безопасности, используемым на других более мощных устройствах, таких как смартфоны и планшеты.

Блочные шифры являются фундаментальными компонентами примитивов с симметричным ключом; они в основном сосредоточены на функциональности шифрования. Для эффективного шифрования больших файлов данные разбиваются на «блоки» фиксированной длины, обычно 64 или 128 бит. Секретность поставляется с секретным ключом, который используется сторонами связи.

После внедрения AES потребность в новых алгоритмах блочного шифрования резко упала, поскольку в большинстве случаев AES является отличным решением. Однако, несмотря на простоту реализации, AES не подходит для сверхограниченных окружений, типа RFID меток и считывателей.

С популярностью IoT небольшие устройства от датчиков до меток RFID могут быть связаны и обмениваться данными друг с другом через сети. При наличии миллиардов таких небольших устройств безопасность и конфиденциальность информации могут быть поставлены на карту из-за различных типов злоумышленников, среди которых могут быть и сами пользователи. Таким образом, информация должна быть должным образом защищена криптографическими схемами.

Задача состоит в том, чтобы найти правильный компромисс между запасом прочности, эффективностью и стоимостью. Несмотря на незначительные размеры устройств, легкая криптография ни в коем случае не является слабой криптографией. Ожидается, что примитивы по-прежнему будут защищены от злоумышленников, хотя злоумышленники в этом контексте могут обладать меньшей вычислительной мощностью или иметь ограниченный доступ к открытым текстам или шифротекстам.

В течение последнего десятилетия большое количество легких примитивов было предложено как научными кругами, так и промышленностью. Среди них один из первых облегченных блочных шифров - Present, который был представлен в CHES 2007, а позже стал стандартом ISO/IEC в 2012 году вместе с Clefia. После этого сообщество стало свидетелем повышение в предложениях новых блочных шифров, включая Prince, Klein, Led, Rectangle, Pride, PRINTcipher, Simon и Speck, Skinny, Present и так далее. Все эти шифры подписано и предназначено специально для чрезвычайно ограниченных сред, таких как RFID метки и сенсорные сети.

Все эксперименты выполняются с использованием двух Raspberry Pi (RPi) - компьютер с 1 ГБ оперативной памяти и беспроводным доступом. Один RPi служит клиентским узлом, а другой RPi служит шлюзом. Настройка соединения для испытательного стенда включает в себя: Raspberry Pi подключается к точке доступа WiFi через WiFi и действует как устройство IoT. Gateway RPi, который подключается к точке доступа через Ethernet и служит шлюзом MQTT-SN.

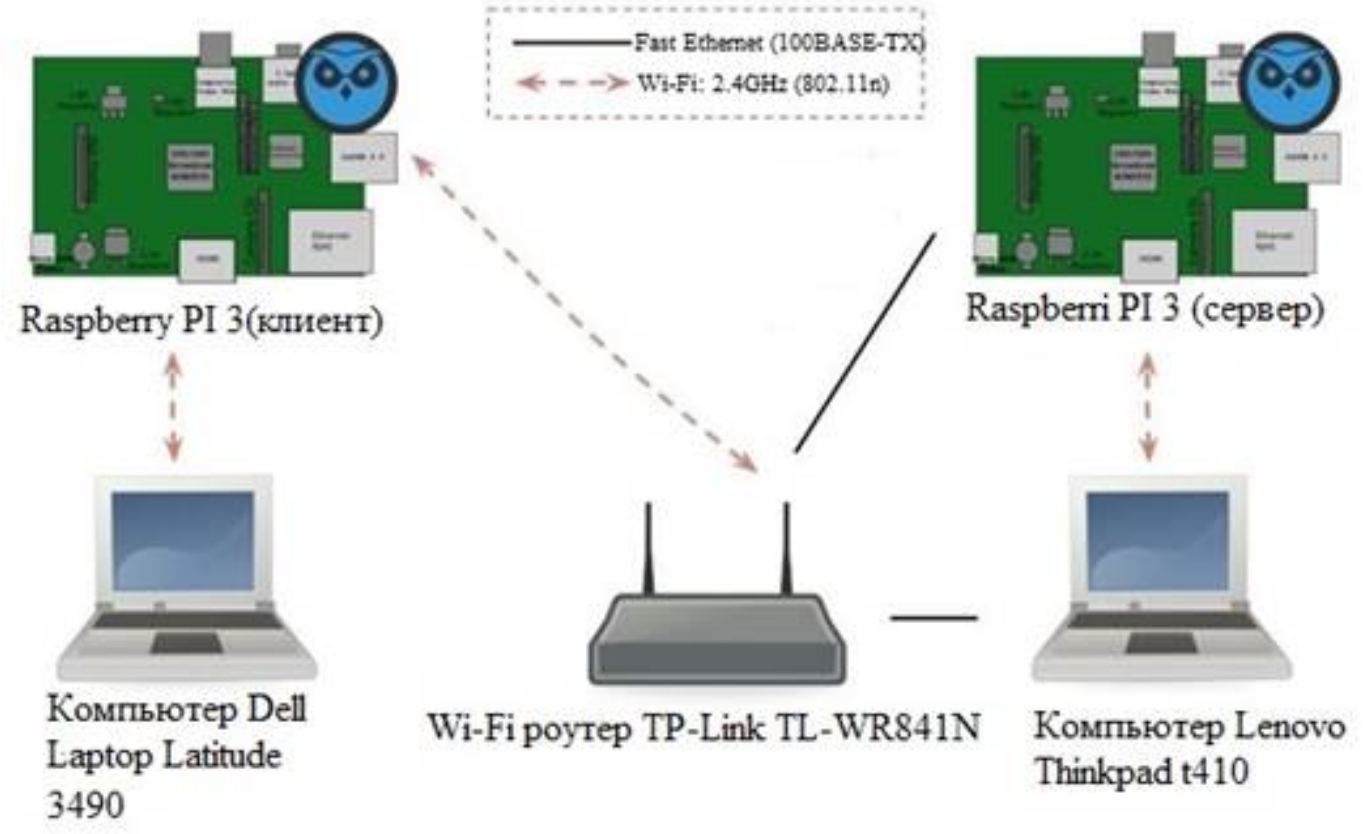

Рисунок 1. Схема реализации

Эксперимент заключается в проверке производительности зашифрованной связи за определенное время. Это делается путем шифрования сообщения на клиент и отправку пакетов по сети на шлюз на две секунды. Через две секунды программа покажет, как много пакетов за этот период было отправлено. Этот процесс повторяется несколько раз, чтобы убедиться, что цифры незначительно варьируются. Средний результат записывается и сравнивается среди разных шифров. Шифрование выполняется в режиме цепочки блоков шифрования (CBC).

Этот режим объединяет блоки данных, зашифрованные с помощью блока шифры, приводящие к случайным символам шифротекста. Поскольку используются блочные шифры, открытый текст должен быть дополнен быть равным размеру блока, который является 64-битным для всех упомянутые блочные шифры за исключением AES (128-бит).

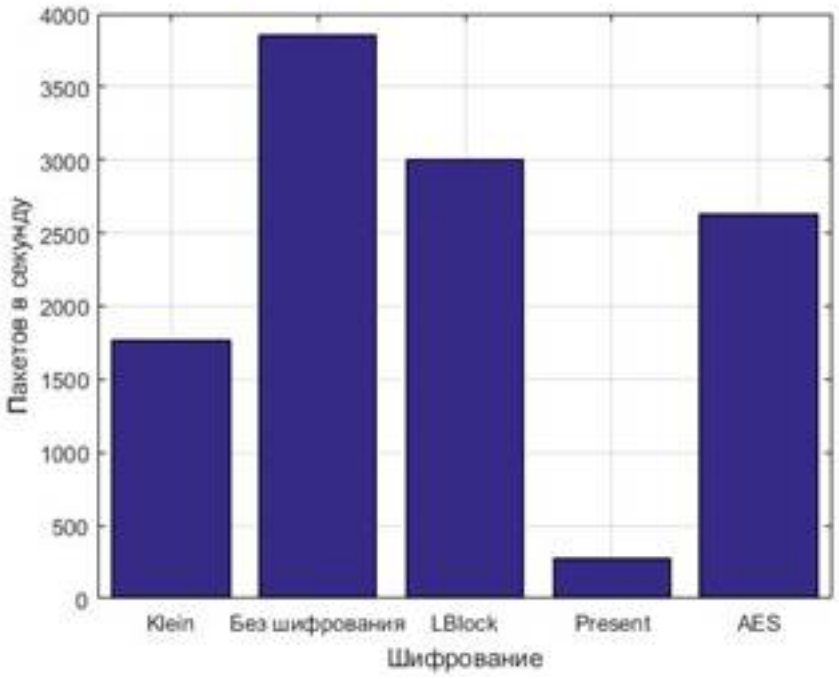

Рисунок 2. Средняя скорость с использованием максимальной полезной нагрузки

На рисунке 2показано, что LBLOCK показал наилучшие результаты с точки зрения скорости по сравнению с AES и другими блочными шифрами в тесте максимальной полезной нагрузки, сумев посылать 3004 пакета в секунду, что на 16,5% больше по сравнению с AES.

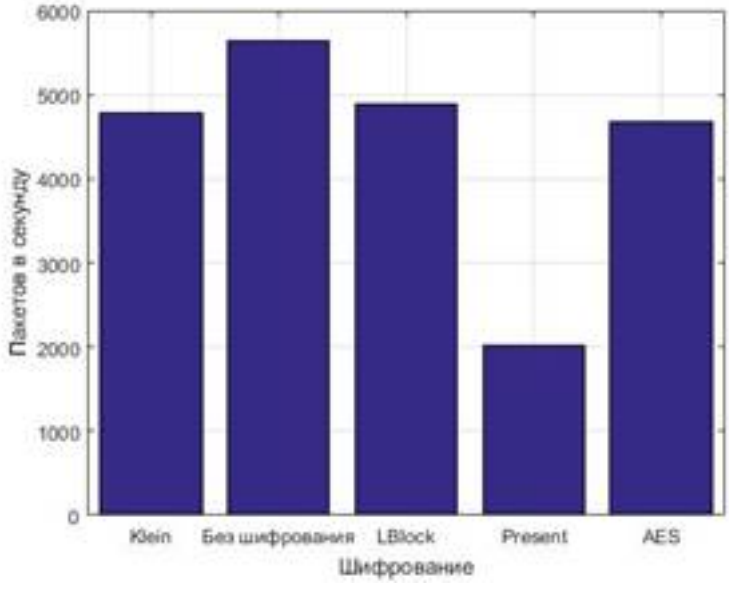

Рисунок 3. Средняя скорость для минимальной полезной нагрузки

На рисунке 3показано, что в тесте минимальной полезной нагрузки LBLOCK, AES и KLEIN демонстрируют практически одинаковую производительность. Тем не менее, LBLOCK - самый быстрый с 4889 пакетами в секунду, уступая только без шифрования. Предыдущие два рисунка показывают различные характеристики алгоритмов шифрования при настройке

минимальной и максимальной полезной нагрузки. Это показывает, что при настройке минимальной полезной нагрузки время обработки для шифрования не является значительным по сравнению со временем передачи.

Был также проведен второй анализ, который измеряет энергопотребление RPi во время шифрованной связи. В этом анализе та же процедура повторяется с добавлением амперметра, подключенного к кабелю электропитания RPi, для измерения силы тока и расчета потребляемой мощности. Также выполняется режим обратной связи, в котором RPi шифрует и отправляет сообщения самому себе. Обратная связь была добавлена, чтобы изолировать потребление энергии между процессом шифрования и процессом передачи.

На рисунке 4 показано энергопотребление на зашифрованный пакет, отправленный через WiFi, а на рисунке 5 показано энергопотребление для режима обратной связи или шифрования без передачи. Разницу между этими двумя показателями можно рассматривать как мощность, потребляемую для связи WiFi. Оба рисунка показывают, что PRESENT потребляет очень много электроэнергию. Это результат очень небольшого числа пакетов, отправленных за период 10 секунд, по сравнению с другими шифрами. Это может быть связано с тем фактом, что PRESENT считается оптимизированным для аппаратной реализации, а не для программного обеспечения, используемого в эксперименте.

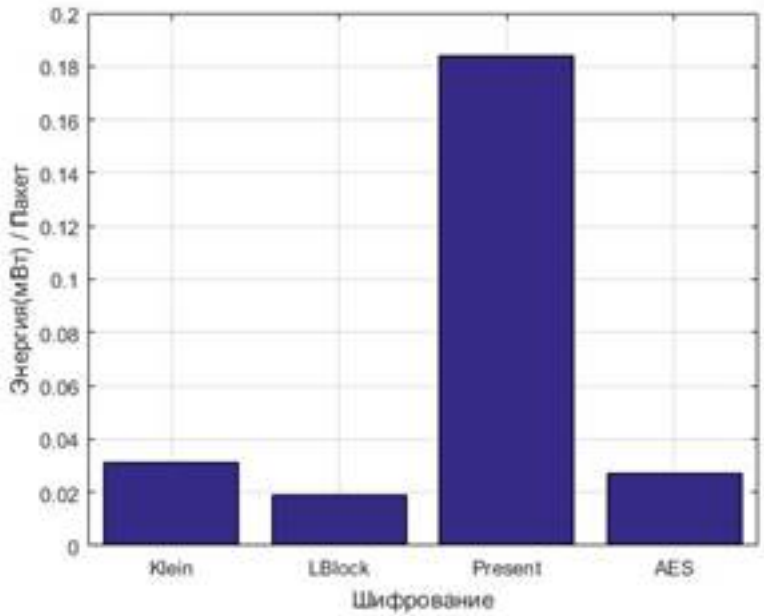

Рисунок 4. Потребляемая мощность при передаче

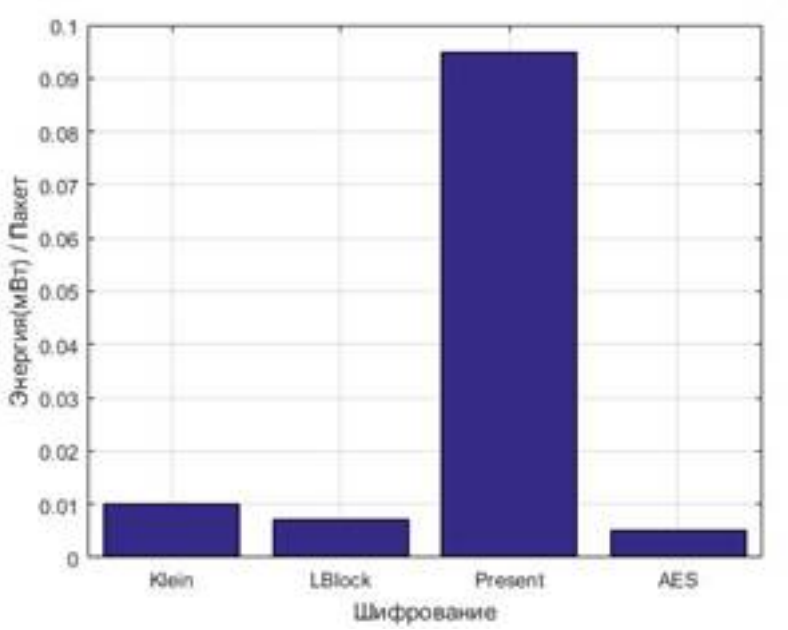

Рисунок 5. Потребляемая мощность без передачи

Процесс обычно ниже по сравнению с процессом передачи, за исключением PRESENT. Для AES, KLEIN и LBLOCK мощность, потребляемая процессом шифрования, находится в диапазоне одной трети всего процесса. Это показывает, что стоимость передачи по Wi-Fi значительно выше, чем стоимость шифрования данных с использованием блочного шифра.

Список литературы:

1. Черемушкин А. В. Криптографические протоколы. Основные свойства и уязвимости. — М.: Изд. дом "Академия", 2009. — 272 с. Шеннон К. Работы по теории информации и кибернетике. — М.: Иностранная литература, 1963. — 832 с.

2. Фомичев В. М. Методы дискретной математики в криптологии: учеб. пособие. М.:Диалог МИФИ, 2010 — 216 с.

3. IPC2U: Что такое MQTT и для чего он нужен в IIoT? Описание протокола MQTT [Электронный ресурс]: Режим доступа: https://ipc2u.ru/articles/prostyeresheniya/chto-takoe-mqtt/

4. Баричев С. Криптография без секретов. – М.: Горячая Линия – Телеком, 2004 – 54 с.

5. Poschmann A. Lightweight Cryptography: Cryptographic Engineering for a Pervasive World. Ph.D. Thesis. Ruhr University Bochum, 2009.

6. Жуков А.Е. Легковесная криптография. Часть 1 [Электронный ресурс] / Вопросы кибербезопасности. 2015. №1 (9). - Режим доступа: https://cyberleninka.ru/article/n/legkovesnaya-kriptografiya-chast-1

7. Поляков А.С. Простой способ разработки «Легких» алгоритмов шифрования [Электронный ресурс] / Доклады БГУИР. 2017. №2 (104). - Режим доступа: https://cyberleninka.ru/article/n/prostoy-sposob-razrabotki-legkih-algoritmov-shifrovaniya