# Заключение

В начале работы ставились цели исследования легковесных криптографических алгоритмов с позиции таких характеристик, как требования к оперативной памяти устройства, энергопотребление, производительность.

В процессе изучения литературы по теме сформулированы основные (впрочем, уже классические) положения криптографии. Определены основные угрозы безопасности систем интернета вещей, они свои для каждого слоя таких систем. Для дальнейшего анализа выбираются те из них, которые направлены на сенсорный уровень. Основными из них являются подслушивание, введение фальшивого узла, атака повторного воспроизведения.

Вводится определение легковесного криптографического алгоритма, формулируются требования к нему.

Выделяются задачи, которые необходимо выполнить для противодействия указанным атакам. Это подтверждение достоверности и целостности пакета (аутентификация) – подтверждение, что пакет данных отправил законный отправитель, и пакет не был изменен по пути (блокирует введение фальшивого узла отправителя или ретранслятора данных). Это подтверждение подлинности пакета (что это пакет, отправленный сейчас, а не отправленный ранее и перехваченный) – блокирует атаку повторного воспроизведения. Это, наконец, обеспечение конфиденциальности пакета данных – защита от подслушивания. При этом важно, чтобы процедура аутентификации была простой и однократной, так как интернет-соединение устройства может быть нестабильным и/или непостоянным.

Далее выделяются оптимальные подходы к решению данных задач. Для решения первой задачи наилучшим решением является применение цифровой подписи, которая, к тому же, гарантирует целостность сообщения. Подписывать рекомендуется не весь текст сообщения, а его хэш, это позволит ускорить процесс. Для реализации ЭЦП необходимо знание секретного ключа, который может быть, например, вшит при изготовлении устройства. Для подтверждения подлинности пакета наиболее разумным представляется добавление к сообщению метки времени. Так как сообщение будет хэшировано, ее не удастся изменить злоумышленнику. Необходимо наличие защищенного системного таймера.

Ключевой, главной задачей является третья – шифрование. Между блочными и потоковыми алгоритмами, более предпочтительными являются блочные алгоритмы, в особенности для устройств IoT (в силу небольших объемов передаваемых пакетов). Асимметричное шифрование подходит в наименьшей степени.

Далее описывается предлагаемая методология тестирования производительности и энергопотребления программной реализации легковесного криптоалгоритма. Главная задача такого тестирования – сравнения реализаций и алгоритмов. Описываются возможные препятствия и искажения такого тестирования, приводятся меры по их учету и преодолению.

Затем предложенная методология тестирования производительности применяется на практике. Сравниваются три различные реализации алгоритма AES. Результатом тестирования являются несколько серий измерений. Затем по ним вычисляются параметры алгоритмов.

Следует отметить, что расположение точек хорошо соответствует теоретическим прогнозам. Это свидетельствует главным образом об удачно построенном эксперименте, т.е. порядке вызова тестируемых функций. Полученные результаты являются достаточно стабильными, т.е. на всем исследованном промежутке (10-600 блоков) восстанавливается практически одинаковая производительность (разница не превышает 5%). Это также говорит об удачной методике, однако пока рано с уверенностью говорить о стабильности, для этого следует протестировать реализации бОльшего числа различных алгоритмов.

В процессе проведения работы возникло несколько «побочных» вопросов, которые могут лечь в основу дополнительных исследований. Насколько предсказуемо время выполнения команд процессором в каждом конкретном месте кода? Другими словами, как на время исполнения команды влияют соседние команды? Осталась непроверенной на практике описанная методика тестирования энергопотребления, в будущем её следует реализовать и проверить.

Таким образом, в результате работы достигнута поставленная цель – исследовать легковесные криптографические алгоритмы, а также выполнены задачи – определение перспективных видов легковесных криптоалгоритмов, формулирование рекомендаций по их применению. Создана методология тестирования производительности и энергопотребления алгоритмов, для сравнения алгоритмов. Тестирование производительности проверено, тестирование энергопотребления ожидает проверки в будущем.