УДК 004.056.55

А. Н. Каменских, В. Г. Наборщиков
Пермский национальный исследовательский
политехнический университет, г. Пермь

АНАЛИЗ СТРУКТУРНО-ФУНКЦИОНАЛЬНЫХ МОДЕЛЕЙ КРИПТОГРАФИЧЕСКИХ ПРОЦЕССОРОВ ДЛЯ СИСТЕМ «ИНТЕРНЕТА ВЕЩЕЙ»

В данной статье проведен анализ существующих проблем и решений в области проектирования криптопроцессоров для систем «интернета вещей», а также поставлены задачи для достижения целей исследования.

Ключевые слова: информационная безопасность, «Интернет-вещей», криптография, схемотехника, криптопроцессоры.

A.N. Kamenskikh, V.G. Naborshchikov
Perm national research polytechnic university, Perm

ANALYSIS OF STRUCTURAL AND FUNCTIONAL MODELS OF CRYPTOGRAPHIC PROCESSORS FOR THE "INTERNET OF THINGS" SYSTEMS

In this article analyzes the existing problems and solutions in the design of cryptoprocessors for the "Internet of Things" systems, as well as sets out the tasks to achieve the research objectives.

Keywords: information security, "Internet of things", cryptography, circuitry, cryptoprocessors.

Введение. IoT-система является концепцией современной вычислительной системы. Узловые элементы IoT-систем представлены как стандартными персональными компьютерами, так и мобильные телефонами, контроллерами, серверами, датчиками и другими подобными элементами. В ядре современных IoT-систем лежат «облачные вычисления». Следует отметить, что в последнее время активно развивается концепция «туманных вычислений» (англ. fog computing). Этот тренд связан с ростом вычислительных возможностей мобильных устройств, что делает проблему защищенной коммуникации встроенных устройств еще более актуальной [1].

IoT-система оказывается более уязвима относительно классической ЛВС и даже распределенной информационной-управляющей системы (РИУС). Класс РИУС наиболее близок к классу IoT-систем, именно поэтому разрабатываемые сейчас стандарты безопасности IoT-систем опираются на стандарты РИУС (NIST 800-82 и другие).

Одним из методов защиты IoT-систем является шифрование. Так как многие элементы не обладают достаточной вычислительной мощностью для реализации алгоритмов шифрования с современными требованиями безопасности, появляется потребность в специализированных сопроцессорах,

реализующих криптографические функции, или криптопроцессорах (шифропроцессорах).

Анализ архитектуры криптографического процессора. Рассмотрим различные способы безопасной передачи данных между элементами IoT-системы, рисунок 1.

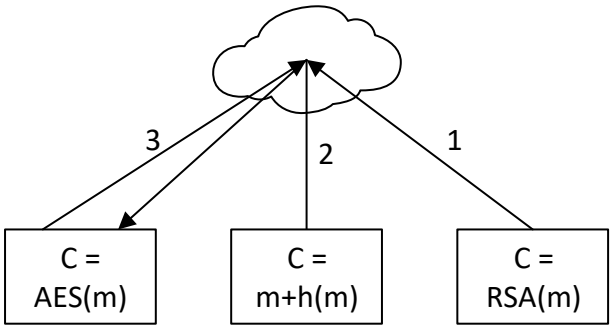

Рисунок 1 – Способы коммуникации конечных устройств с облачной платформой

Способ 1 – данные шифруются при помощи алгоритма RSA открытым ключом сервера, который для этого должен быть загружен в память устройства. Криптопроцессор должен поддерживать алгоритмы ассиметричного шифрования (АШ), например, RSA. Возможные угрозы (вектора атаки) – подмена устройства (англ., man in the middle, MitM), так как сервер не может аутентифицировать источник сообщения. Атаки, направленные на «отказ в обслуживании» (англ., Denial of Service), так как сервер тратит ресурсы на расшифровку данных.

Способ 2 – данные подписываются ключом датчика/контроллера. В этом случае криптопроцессор должен поддерживать хэширование и алгоритм цифровой подписи. Возможные угрозы (вектора атаки) – чтение данных, так как данные идут в открытом виде, то любой злоумышленник может их прочитать, но не изменить. Анализ криптографических алгоритмов и их реализации, для развития вектора атаки злоумышленник будет пытаться скомпрометировать секретные ключи устройства, или напрямую расшифровать их пользуясь тем, что конечные устройства не обладают большими вычислительными ресурсами.

Способ 3 – данные шифруются симметричным блочным шифром. Криптопроцессор и вся система должны поддерживать соответствующий алгоритм шифрования – AES, DES, «Кузнечик» и другие. Возможные угрозы (вектора атаки) – анализ криптографических алгоритмов и их реализации.

В современных системах указанные способы, как правило, используются в комбинации, так, как только это обеспечивает достаточный уровень защищенности системы и доверия к передаваемым данным. Ярким примером являются реализации протоколов SSH, IKE и его производные. Тем не менее в прикладных задачах с целью снижения затрат ресурсов могут использовать отдельные способы защиты информаци.

Таким образом, современный криптографический процессор для IoT-систем должен иметь возможность работать в трех основных режимах – подпись данных, ассиметричное шифрование, симметричное шифрование. Причем архитектура должна обеспечивать связанность режимов работы, таблица 1. Примерный алгоритм работы устройства управления приведен на рисунке 2.

Таблица 1 – Таблица истинности устройства управления криптографическим процессором

$x_1x_2x_3$	Алгоритм шифрования
000	НЕТ
001	RSA/ECC
01-	AES/ГОСТ
1-0	SHA256/ГОСТ
1-1	Подпись + шифрование

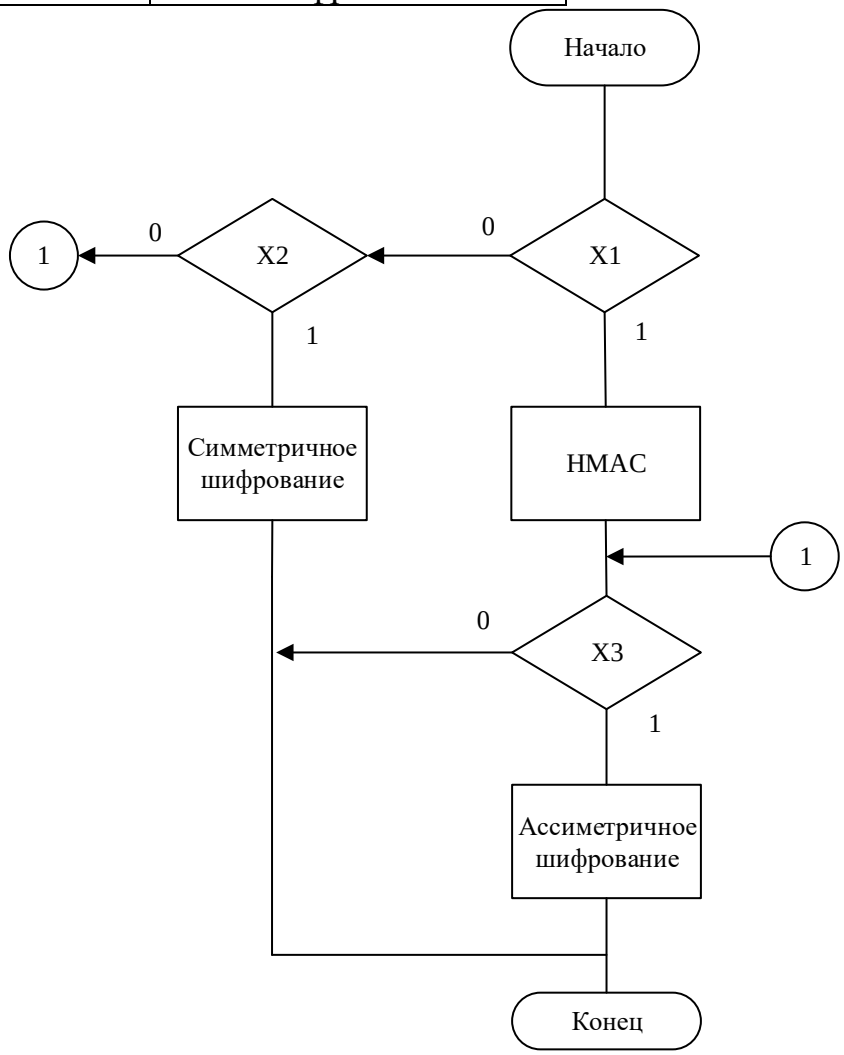

Рисунок 2 – Алгоритм управления криптографическим процессором

Аппаратная реализация алгоритмов симметричного шифрования хорошо изучена, многие решения доведены до промышленного производства. Так же,

аппаратные реализации ассиметричных алгоритмов шифрования представлены значительно меньше, в частности не хватает анализа надежности предлагаемых аппаратных узлов.

Часть разработанных устройств и методов их синтеза засекречены – следовательно их схемы не опубликованы и нельзя оценить наличие в них аппаратных уязвимостей, что потенциально влияет на общую безопасность. Таким образом, актуально исследование надежности аппаратных узлов, реализующих алгоритмы ассиметричного шифрования.

Следует отметить, что постоянный рост вычислительных ресурсов приводит к тому, что алгоритм RSA становится уязвимым. В основе этого процесса лежит фактор экспоненциального роста затрат времени/памяти при увеличении длины ключа. Решением этой проблемы является переход на использование криптографии на основе эллиптических кривых (ECC). Длина ключа в алгоритмах ECC на порядок ниже, чем в алгоритме RSA, при той же криптографической стойкости. Поэтому при разработке методов синтеза стоит опираться именно на те блоки и узлы, которые используются в процессорах ECC [2].

В основе ECC лежат следующие базовые операции:

1. Алгебраическое сложение двух точек, которое заключается в решении следующих уравнений 1-3 [2]:

$$m = (Y_p - Y_q) / (X_p - X_q) \quad (1)$$

$$X_r = m^2 - X_p – X_q \quad (2)$$

$$Y_r = Y_p + m * (X_r - X_p) \quad (3)$$

2. Скалярное умножение алгоритмом умножения-сложения:

$$I = I + A \quad (4)$$

$$A = A * 2 \quad (5)$$

3. Логарифмирование:

Наибольшее количество операций выполняет схема сложения/вычитания. Поэтому именно над ее оптимизацией и следует работать в первую очередь.

Постановка частных задач исследования. Для достижения цели исследования – разработать отказоустойчивый криптографический процессор на основе метода комбинированного резервирования для глобально-асинхронных локально-произвольных (ГАЛП) схем, необходимо решить следующие задачи:

I. Разработать структурно-функциональную модель ГАЛП криптопроцессора;

II. Разработать модели энергонадежности синхронных и асинхронных узлов криптографического процессора:

a. Сумматор (надежность, быстродействие, энергопотребление).

b. Умножитель (надежность, быстродействие, энергопотребление).

с. Сложение по модулю два (надежность, быстродействие, энергопотребление).

III. Разработать формальную систему вывода оптимальных участков синхронных и асинхронных схем;

Заключение. «Интернет-вещей» активно внедряется в повседневную жизнь общества, научные основы этой технологии уже заложены и достаточно хорошо изучены. Однако, на практике разработчики систем «Интернета-вещей» часто пренебрегают обеспечением надежности и безопасности своих систем, происходит это зачастую из-за высоких затрат на технологии обеспечения безопасности и надежности. Следовательно, появляется проблема, которая требует дополнительного изучения и поиска специализированных решений, оптимальных для «Интернета-вещей».

Список литературы

1. Что такое интернет вещей? кривых [Электронный ресурс]. – URL: https://trends.rbc.ru/trends/industry/5db96f769a7947561444f118

2. Доступно о криптографии на эллиптических кривых [Электронный ресурс]. – URL: https://habr.com/ru/post/335906/ (дата обращения 10.12.2020)

Сведения об авторах

Каменских Антон Николаевич – кандидат технических наук, доцент кафедры «Автоматика и телемеханика» Пермского национального исследовательского политехнического университета, Пермь, e -mail: antoshkinoinfo@yandex.ru

Наборщиков Владимир Георгиевич – студент Пермского национального исследовательского политехнического университета, Пермь, e-mail: naborshikov_vladimir@mail.ru

About the authors

Kamenskikh Anton Nikolaevich – Ph.D. in Technical Sciences, Associate Professor Department of Automation and remote control, Perm National Research Polytechnic University, Perm, e-mail: antoshkinoinfo@yandex.ru

Naborshchikov Vladimir Georgievich – Student Perm National Research Polytechnic University, Perm, e-mail: naborshikov_vladimir@mail.ru