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

УДК 004.056.53

Войтехович
Сергей Андреевич

Устройства криптографической защиты информации для датчиков и исполнительных устройств «умного дома»

АВТОРЕФЕРАТ

на соискание степени магистра техники и технологии
по специальности 1-39 81 03 «Информационные радиотехнологии»

Научный руководитель
Власова Галина Александровна
Кандидат технических наук,
доцент

Минск 2018 г.

ВВЕДЕНИЕ

В последние годы сетевые технологии всё более активно проникают в нашу жизнь. Производители электроники стараются встраивать средства для коммуникации и мониторинга во многие вещи, ранее обходившиеся без этой опции. Концепция сети физических объектов, оснащенных встроенными технологиями, позволяющими ощущать или взаимодействовать с их внутренним состоянием или окружающей средой без участия человека в большинстве операций, получила название «Internet of Things» — «интернет вещей».

Типичными примерами реализации и развития данной концепции можно назвать системы автоматизации, телеметрии и контроля на предприятиях, а также активно развиваемые и рекламируемые в наше время системы «умный дом». Если первые из них используются и совершенствуются уже давно, то приход в гражданский сектор, сопровождающийся появлением вторых — явление новое и перспективное. «Умный дом» представляет собой современный тип жилья с высокой степенью автоматизации и применения высокотехнологичных устройств. Данная система должна обеспечивать безопасность, комфорт и ресурсосбережение для всех жителей дома, подкрепляя это таким важным фактором, как удобство использования. «Умный дом» может включать в себя такие системы: как вентиляция, кондиционирование, отопление, замки дверей и ворот, отдельные электроприборы и др.

Как «умный дом», так и системы автоматизации на предприятиях, представляют собой начальную стадию развития данной концепции, поскольку даже законченные и самостоятельные системы на объектах пока что остаются локальными примерами, тогда как концепция «интернет вещей» подразумевает создание глобальной коммуникационной сети подобных систем, охватывающих большинство аспектов жизни человека.

К технологиям, позволяющим реализовать данную идею, можно отнести средства автоматической идентификации (радиочастотная идентификация, оптические метки, идентификатор единицы оборудования сети), средства измерения (датчики, приборы учета, интегрированные измерительные системы) и средства передачи данных (как беспроводные, так и проводные сети). Чаще всего система реализуется в виде сети датчиков и исполнительных устройств, преимущественно беспроводных, собирающих и передающих в центральный узел информацию о контролируемых ими параметрах. Обычно для связи устройств используется радиоканал, и получающаяся структура обозначается аббревиатурой БСС — беспроводная сеть сенсоров.

Для оконечных устройств и датчиков, входящих в состав БСС, важны такие качества, как эффективность в условиях низких скоростей передачи данных, отказоустойчивость, адаптивность, возможность самоорганизации,

низкое энергопотребление. В первую очередь, именно требование максимальной автономности системы накладывает жесткие ограничения на использование определенных технологий и архитектур. Система должна обладать максимальной устойчивостью и надежностью, а также достаточной для выполнения требуемых задач вычислительной мощностью при минимальном энергопотреблении. Для организации систем, удовлетворяющих этим требованиям, обычно применяют в качестве базы микроконтроллеры, основанные на архитектуре RISC (Reduced Instruction Set Computer — компьютер с сокращённым набором команд), преимущественно 32-битные ARM (Advanced RISC Machine — усовершенствованная RISC-машина) и 8-битные AVR (Advanced Virtual RISC — расширенный виртуальный RISC). Несмотря на активное развитие и внедрение в последние годы архитектуры ARM, микроконтроллеры AVR продолжают удерживать достаточно важные позиции благодаря простоте, более низкой стоимости и энергопотреблению. Также популярны AVR-совместимые клоны, основанные на FPGA (Field-Programmable Gate Array — программируемая пользователем вентильная матрица), устройствах, конфигурируемых разработчиком после изготовления при помощи исходного кода на языке проектирования, описывающего логику работы микросхемы. Основным преимуществом ПЛИС-клонов является возможность обеспечить лучшее быстродействие выполняемых алгоритмов за счет намного более высокой верхней границы возможной тактовой частоты ЦП и возможность эффективно выполнять параллельные вычисления.

С увеличением количества БСС, вопрос их информационной защиты становится всё более важным. Злоумышленники могут как просто перехватить требующуюся им информацию, так и подавить её поток или внести изменения в передаваемые данные. Любая из этих угроз при реализации в определенных условиях может привести к нежелательным последствиям или вовсе спровоцировать критическую ситуацию.

Таким образом, для передаваемой в БСС информации обязательно требуется криптографическая защита данных. Нельзя при этом забывать об ограничениях платформы AVR — невысокой вычислительной мощности, малом объеме памяти, как постоянной, так и оперативной. Также, как уже говорилось, необходимо снижение энергопотребления. Для работы в подобных ограниченных условиях подходят алгоритмы перспективного и активно развивающегося в последнее время направления криптографии — криптографии на эллиптических кривых (Elliptic Curve Cryptography, ECC) в конечных полях.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Цель данной работы: реализация криптографического модуля на эллиптических кривых на AVR-совместимого устройства для защиты исполнительных устройств системы «умный дом».

Задачи исследования: обзор подходов к эффективному использованию ограниченных вычислительных возможностей микроконтроллеров для применения криптоалгоритмов на эллиптических кривых; моделирование возможных угроз информационной безопасности в системах с применением микроконтроллеров серии AVR и им подобных и обозначение путей противодействия им; выбор криптографических алгоритмов для применения в микроконтроллере; выбор и адаптация ECC-библиотеки под задачи исследования; проведение сравнительных измерений параметров работы криптографических алгоритмов средствами симулятора микроконтроллера.

Объект исследования работы: криптографическая защита передачи данных на устройствах, основанных на архитектуре AVR для защиты исполнительных устройств системы «умный дом».

Предмет исследования работы: реализация эффективных алгоритмов асимметричного шифрования, основанных на эллиптических кривых, на устройствах, основанных на архитектуре AVR для защиты исполнительных устройств системы «умный дом».

КРАТКОЕ СОДЕРЖАНИЕ РАБОТЫ

Во введении показано, в чём актуальность работы.

В главе 1 описываются основные системы «умного дом», угрозы безопасности передаваемой с микроконтроллера и на него информации, распространенные средства защиты и тенденции развития.

В главе 2 описываются микроконтроллеры архитектуры AVR, рассмотрены их особенности, а также проведен анализ возможностей использования алгоритмов эллиптической криптографии как средства обеспечения информационной безопасности в системе «умный дом».

В главе 3 были представлены основные модели угроз для микроконтроллеров архитектуры AVR, были сделаны и обоснованы выборы языка описания аппаратуры, интегрированной среды разработки, ПЛИС для запуска клона ядра AVR, а также самого ядра и запускаемой на нем крипто библиотеки.

В главе 4 приводится программная реализация исследуемых алгоритмов, сделан выбор между средами симуляции, описаны методы проведения измерений, а также приведены результаты всех измерений и произведен их краткий анализ.

В приложении приложена программная реализация криптографический алгоритм.

ВЫВОДЫ

Количество датчиков и исполнительных устройств для «умного дома» с каждым днём растёт и образуют свою систему, такие системы так же нуждаются в построении грамотной и надежной криптографической защиты. Таким образом, основной задачей для криптографической защиты «умного дома» является реализация и оптимизация надежных алгоритмов шифрования и аутентификации на устройствах с микроконтроллером. Асимметричные алгоритмы на эллиптических кривых являются самым перспективным направлением развития данной области.

В данной работе была проведена симуляция работы микроконтроллера с обоснованием выбора симулятора и модели микроконтроллера. Для этого микроконтроллера были реализованы алгоритмы шифровании, основанные на идеях эллиптической криптографии, а также произведены замеры производительности алгоритмов и использования ими доступной памяти.

Как показали сравнительные измерения с неэллиптическими асимметричными алгоритмами и симметричными алгоритмами, использование алгоритмов эллиптической криптографии для повышения уровня информационной безопасности на микроконтроллерах архитектуры AVR в исполнительных системах умного дома возможно, несмотря на высокую вычислительную сложность, но только в составе систем, не требующих передачи данных чаще одного раза в 30 секунд. Применение традиционных асимметричных алгоритмов шифрования на подобных микроконтроллерах возможно только при использовании моделей с 32 КБ памяти данных по причине высокого её потребления этими алгоритмами.

СПИСОК ОПУБЛТКОВАННЫХ РАБОТ

[1-А.]Войтехович С.А., Власова Г.А. Обучение-необходимое условие обеспечения информационной безопасности в период цифровизации. / Войтехович С.А., Власова Г.А.// 10-я международная научно-методическая конференция «Дистанционное обучение – образовательная среда 21 века» - Минск, 2017.

[2-А.] Войтехович С.А., Власова Г.А. Особенности применения криптографических методов для датчиков и исполнительных устройств в системе «умный дом». / Войтехович С.А., Власова Г.А.// 54-я научная конференция аспирантов, магистрантов и студентов БГУИР. Минск, 2018.