Семейство криптографических микросхем CryptoAuthentication компании Atmel

с безопасным аппаратным хранением ключей: ATSHA204A, ATECC508A/108A, ATAES132A

Игорь КРИВЧЕНКО,
к. т. н.
ik@efo.ru

В течение многих лет компания Atmel выпускает различные защищенные криптографические устройства индустриального стандарта. Микросхемы семейства CryptoAuthentication — одни из них. Эти недорогие, малогабаритные и простые в использовании устройства предназначены для безопасного хранения данных небольшого объема, генерации и хранения ключей шифрования, а также для выполнения некоторых базовых криптографических операций. Простой и понятный API-интерфейс с небольшим набором функций существенно облегчает их интеграцию в конечные системы. Основные области применения — симметричная и асимметричная аутентификация, шифрование и проверка целостности данных, электронная цифровая подпись.

Ключевыми особенностями микросхем CryptoAuthentication, о которых сегодня пойдет речь, являются безопасное хранение ключей и аппаратные блоки, помогающие противостоять различным внешним атакам, в том числе агрессивным. Эти малопотребляющие устройства поддерживают современные криптографические протоколы, в частности ECDSA для цифровой подписи и ECDH для генерации совместных сеансовых ключей шифрования. Они могут работать с любым внешним микроконтроллером, требуют лишь одну линию ввода/вывода, действуют в широком диапазоне напряжений питания. Все это помогает разработчикам без особых проблем добавлять в свои изделия современный, надежный уровень информационной безопасности за минимальную стоимость.

В настоящее время большое внимание уделяется проблемам безопасности хранимых, обрабатываемых и передаваемых данных, защите от копирования интеллектуальной собственности и цифрового контента, а также защите от клонирования конечных устройств. Хакеры воруют закрытую информацию в основном потому, что для ее хранения и защиты используется программное обеспечение. Переход на аппаратный уровень — более привлекательное решение, но стандартные интегральные микросхемы тоже могут быть легко атакованы с целью прочесть информацию. Поэтому требуется еще более защищенный подход. Секретные данные можно хранить, например, в специализированных микросхемах, у которых на кристалл встроены физические барьеры и реализованы криптографические контрмеры для противодействия хакерским атакам. Такие полупроводниковые устройства выпускают многие известные компании — Inside Secure, Infineon, NXP, STM, Broadcomm и другие.

Защищенные микросхемы CryptoAuthentication фирмы Atmel реализуют набор криптографических алгоритмов и устойчивое к внешним атакующим воздействиям аппаратное окружение массива памяти на кристалле. Это не дает возможности злоумышленнику извлечь ключи и другую секретную информацию — сложно атаковать то, что ты не видишь. Микросхемы данного семейства доступны для рядового пользователя. Они дешевые, не требуют лицензирования при покупке, выпускаются в удобных для применения корпусах. Поскольку компания Atmel постоянно проводит огромную работу по криптографическому инжинирингу своих микросхем, разработчикам нет необходимости быть или становиться экспертами в области криптографии, если они хотят добавить надежный уровень безопасности в конечную систему.

Состав семейства CryptoAuthentication приведен в таблице. В него входят четыре микросхемы, различающиеся как по своим функциям, так и по целевым областям применения.

ATSHA204 A — исторически первый представитель семейства CryptoAuthentication с интегрированным хеш-алгоритмом SHA-256 и защищенным массивом EEPROM-памяти 4,5 кбит. Микросхема является наиболее простым и дешевым устройством в семействе. Обеспечивает надежную аппаратную аутентификацию и защищенное хранение ключей/данных. Основное назначение — различные режимы симметричной аутентификации, конфигурируемой конечным пользователем, защищенное скачивание и загрузка кода, защита от клонирования.

Криптографические акселераторы микросхем ATECC508A и ATECC108A поддерживают 256-битную криптографию на эллиптических кривых. Они содержат защищенный массив EEPROM-памяти 10 кбит и монотонный счетчик числа использований. Доступ к памяти этих микросхем может быть ограничен, а затем созданная пользовательская конфигурация блокируется. Основные отличия ATECC508A состоят в том, что она дополнительно поддерживает алгоритм Диффи — Хеллмана на эллиптических кривых (ECDH) и имеет

улучшенный счетчик числа использований. В остальном микросхемы одинаковы и обратно совместимы с ATSHA204A. Основное назначение — асимметричная аутентификация, безопасность обмена сообщениями, проверка целостности данных. Ключевая особенность — разработчику не нужно организовывать безопасное хранение секретных данных на стороне хоста.

Более подробно о самих микросхемах ATSHA204A и ATECC508A/108A, режимах их работы, системе команд, особенностях конфигурирования и персонализации, примерах потенциальных приложений и средствах поддержки разработок мы планируем рассказать в последующих публикациях.

Особняком в семействе CryptoAuthentication стоит ATAES132A — микросхема защищенной последовательной EEPROM объемом 32 кбит. Она позволяет осуществлять аутентификацию и конфиденциальное хранение данных, поддерживает стандарт симметричного шифрования AES. Ограничения доступа для каждой из 16 зон пользователя конфигурируются независимо, и любой ключ может быть использован с любой зоной. Ключи также могут применяться и для задач аутентификации. Подобная гибкость позволяет применять микросхему ATAES132A в широком спектре конечных приложений.

Криптографический акселератор AES-128 устройства работает в режиме AES-CCM для аутентификации, шифрования данных и вычисления MAC. Шифроваться могут как данные в памяти микросхемы, так и внешние пакеты данных небольшого объема (зависит от конфигурации). Расширенные криптографические функции реализуются путем обмена с ATAES132A дополнительными командными пакетами при помощи стандартных операций чтения и записи. Безопасная персонализация облегчает серийное производство на сторонних фабриках. Устройство содержит 16 монотонных счетчиков числа использований, тоже расположенных в EEPROM. Регистры конфигурационной памяти управляют доступом к пользовательской памяти, а также ограничением функциональности ключей и счетчиков. Пользовательская память устройства может быть доступна и непосредственно, при помощи стандартных SPI- или I²C-команд. Полная повыводная совместимость с микросхемами последовательной EEPROM различных производителей и идентичный набор интерфейсных команд облегчает замену на ATAES132A в уже существующих проектах.

Вернемся к проблемам аутентификации, так как именно для этой области были разработаны микросхемы семейства CryptoAuthentication. Бурно развивающиеся облачные сервисы, решения для «Интернета вещей» (IoT), распределенные системы измерения, управления и контроля, интенсивный рост количества мобильных и носимых устройств уже значительно повлияли на темпы развития смарт-решений и платформ. Соответственно, количество точек входа для хакерских атак тоже постоянно увеличивается. Например, только в 2014 году уязвимости Heartbleed, Shellshock и Poodle позволили вскрыть миллиарды паролей по всему миру. Поэтому требуется устойчивая и надежная защита конечных приложений: устройства должны точно «понимать», что они действительно «разговаривают» с тем, с кем было намечено.

Нетрудно догадаться, что без доверия к данным, которыми обмениваются между собой конечные устройства, рынок распределенных систем контроля, управления и сбора данных, и особенно IoT, развиваться не будет. А потому строгая аутентификация в таких областях стала действительно насущной проблемой, ключевым фактором. Каждый раз разработчики должны себя спрашивать, нужна ли криптография в их системах. И если не нужна, то почему.

Для выполнения определенных задач информационной безопасности, которые в настоящее время требуются и могут понадобиться различным пользователям, микросхемы семейства CryptoAuthentication компании Atmel реализуют следующие криптографические функции:

- высококачественный генератор псевдослучайных чисел;
- функции хеширования;
- алгоритмы цифровой подписи;
- алгоритмы формирования сеансового ключа.

Это позволяет применять данные микросхемы для встраиваемых устройств аутентификации и сетевого взаимодействия (например, счетчики энергии, удаленные медицинские терминалы, автомобильные сигнализации, блоки распределенного управления ответственным оборудованием на производстве, игровые устройства и т. п.). Перечислим некоторые из потенциальных приложений:

- Защита от клонирования — аутентификация уникального идентификационного номера клиента на предмет его подлинности (системные аксессуары, дочерние электронные карты, картриджи принтеров, медицинские одноразовые упаковки, узлы IoT и т. п.).
- Обеспечение целостности передаваемых сообщений. Поддержка схемы открытого распределения ключей для создания общих сеансовых ключей с целью последующего шифрования передаваемых данных.
- Защита встроенного ПО или медиаданных — проверка достоверности кода на этапе загрузки во Flash-память на предмет несанкционированных модификаций. Шифрование программных файлов при широковещательной рассылке общего вида. Уникальное шифрование образов программного кода для применения только на определенной конечной системе.
- Безопасный и быстрый обмен сеансовыми ключами шифрования для управления конфиденциальным коммуникационным каналом, зашифрованной загрузкой и другими подобными операциями.

Таблица. Состав семейства CryptoAuthentication и его основные особенности

	ATSHA204A	ATECC508A	ATECC108A	ATAES132A
Описание	Криптографическое устройство для безопасной симметричной аутентификации	Высокоскоростные криптографические устройства для криптографии на эллиптических кривых и асимметричной аутентификации PKI (обратно совместимы с ATSHA204A)		Микросхема защищенной последовательной памяти EEPROM, обеспечивающая аутентификацию и конфиденциальное хранение данных в энергонезависимой памяти
Счетчик числа использований	1K	2 счетчика ×2M	1K	16 счетчиков ×2M
Основная функция	Аутентификация	Аутентификация и обмен ключами по ECDH FIPS SP800-56A для конфиденциальности и целостности данных	Аутентификация	Шифрование/аутентификация
Корпус	UDFN8, SOIC8, SOT23-3, 3-контактный (RBH)	UDFN8, SOIC8, 3-контактный (RBH)		UDFN8, SOIC8
Аутентификация	SHA, HMAC (симметричная)	SHA, HMAC (симметричная), ECC (асимметричная)		AES-CCM (взаимная, симметричная)
Криптографические алгоритмы	SHA-256	SHA-256, ECC-P256	SHA-256, ECC-P256, ECC-B283, ECC-K283	AES-128
Длина ключа	256	SHA = 256, ECC = P256	SHA = 256; ECC = P256, = K283, = B283	128
Интерфейсы ввода/вывода	Однопроводной; I²C	Однопроводной; I²C		I²C, SPI
Размер EEPROM	4,5 кбит	10 кбит		32 кбит (пользовательская), 2 кбит (ключи)
Спящий режим	<150 нА	<150 нА		<250 нА
Максимальное энергопотребление	3 мА	16 мА		26 мА
Напряжение питания	2–5,5 В	2–5,5 В		2,5–5,5 В
Извлечение и перезагрузка ключей	Нет	Нет		Да
Уникальный идентификационный номер	72 бит	72 бит		128 бит
Зашифрованное чтение/запись	SHA/XOR	SHA/XOR		AES-CCM
Целевые приложения	Чувствительные к стоимости приложения. Системы, в которых все компоненты принадлежат одному OEM	Асимметричная аутентификация, сложные системы распределенного доступа и управления, «Интернет вещей» (IoT)		Прямая замена стандартных последовательных EEPROM. Системы, в которых требуется безопасно хранить до 4 кбайт данных

- Хранение ключей шифрования для последующего использования аппаратными или программными криптоакселераторами в стандартных хост-микропроцессорах и микроконтроллерах. Безопасное хранение небольших объемов данных — образов конфигурации, калибровочных коэффициентов, учета числа использований или расхода потребляемого материала и т. п.
- Проверка пользовательских паролей — корректность вводимых пользователем паролей без раскрытия ожидаемого значения; отображение запоминаемых паролей на случайное число; безопасный обмен паролями с удаленными системами.

Важно отметить, что в отличие от конкурентных решений (в основном это микросхемы для смарт-карт) устройства CryptoAuthentication могут эффективно работать как в приложениях «хост-клиент», так и в приложениях «равный с равным» (peer-to-peer). Это особенно актуально в связи с расширением рынка IoT и сферы обмена данными в M2M. Например, IoT будет требовать использования обоих типов отношений. Такая гибкость семейства CryptoAuthentication представляет набор ценных возможностей для разработчиков.

Информационная безопасность системы зависит от того, насколько хорошо в ней хранятся ключи шифрования и насколько защищенным является механизм использования этих ключей без риска раскрыть их. Микросхемы семейства CryptoAuthentication решают обе системные задачи: безопасное хранение ключей и встроенные криптоакселераторы, которые выполняют стандартные криптографические процедуры. Такая однокристальная комбинация — находка для разработчика: обеспечиваются низкая стоимость решения, повышенный уровень информационной безопасности и легкость в применении.

Девиз семейства CryptoAuthentication — «безопасность на кристалле». Микросхемы содержат датчики напряжения, частоты и температуры, защитный металлический экран над всей поверхностью кристалла и другие методы противодействия различным атакам. При определении попыток проникновения в микросхему содержащиеся в ней секретные данные уничтожаются. Гарантами здесь также могут служить многолетний опыт компании Atmel и ее репутация в данной области, сертификаты FIPS и Common Criteria, ведущие позиции в хранении торговых секретов и интеллектуальной собственности, а также многочисленные патенты и ноу-хау.

Литература

1. www.atmel.com
2. Материалы технических тренингов Atmel 2014–2015 гг.