

Новый микроконтроллер Espressif

для Wi-Fi- и Bluetooth-связи

Компания Espressif представила комбинированный чип ESP32-C3. Это новый экономичный микроконтроллер на основе RISC-V, который поддерживает Wi-Fi и Bluetooth LE 5.0 и создан специально для обеспечения защищенных соединений в «Интернете вещей».

Алексей Орешников
alexey.oreshnikov@euroml.ru

Компания Espressif выпустила на рынок Wi-Fi-чип ESP8266 в 2014 году, а ESP32 — в 2016-м. ESP8266, оснащенный только Wi-Fi, обеспечивает простые сценарии применений, в то время как ESP32 позволяет реализовывать решения, где требуется подключение по двум каналам связи — Wi-Fi и Bluetooth/Bluetooth LE, при этом он имеет значительно большую вычислительную мощность и надежные инструменты защиты передачи данных. Оба чипа бесспорно стали лидерами рынка IoT в своих сегментах, обеспечивая подключение огромному количеству устройств по всему миру.

Между тем сам рынок «Интернета вещей» не только стал массовым, но и повзрослел с точки зрения функциональности и ожидаемых затрат. Учитывая потребности и современные тенденции IoT, компания Espressif одной из основных ценностей считает соблюдение баланса между функциональностью устройства и его стоимостью. Фактически очевидно, что универсальная

модель нежизнеспособна, так как должно быть несколько продуктов для различных нужд. Поэтому Espressif представила ESP32-C3 (рис. 1) — комбинированный SoC-модуль, созданный для простых и защищенных соединений.

ESP32-C3 может решать наиболее востребованные задачи, так как при его создании были учтены следующие критерии:

- Безопасность имеет первостепенное значение. Даже самое недорогое решение для передачи данных должно обеспечивать соответствующий уровень защиты от распространенных угроз.
- Поддержка Bluetooth Low Energy.
- Несмотря на то, что стоимость является очень важным параметром, не менее важно и наличие достаточного объема памяти для типовых случаев использования. Это позволит оптимизировать настройки и обновления устройств в полевых условиях.

ESP32-C3 имеет одноядерный, 32-бит, основанный на RISC-V процессор с памятью SRAM 400 кбайт и работающий на частоте 160 МГц (рис. 2). Новый модуль совмещает в себе стандарты 2,4 ГГц Wi-Fi и Bluetooth LE 5.0 с поддержкой большого радиуса действия (long-range support). Имеет 22 настраиваемых GPIO с поддержкой ADC, SPI, UART, I²C, I²S, RMT, TWAI и PWM.

Безопасность

DDoS-атаки на подключенные устройства обычно преследуют следующие цели:

- получение доступа к конфиденциальным данным;
- получение несанкционированного доступа к устройству;
- кража идентификационных данных устройства и впоследствии получение несанкционированного доступа к облаку с данными.

Существуют различные способы проведения этих атак: либо удаленно, используя уязвимости программного обеспечения и протокола, либо физически, получив доступ к устройству через флэш-память и внедрение ошибок. Впоследствии атаки можно сделать постоянными, установив на устройство вредоносное ПО-прошивку по умолчанию. Важно, чтобы платформа подключения обеспечивала достаточную защиту от атак такого типа.

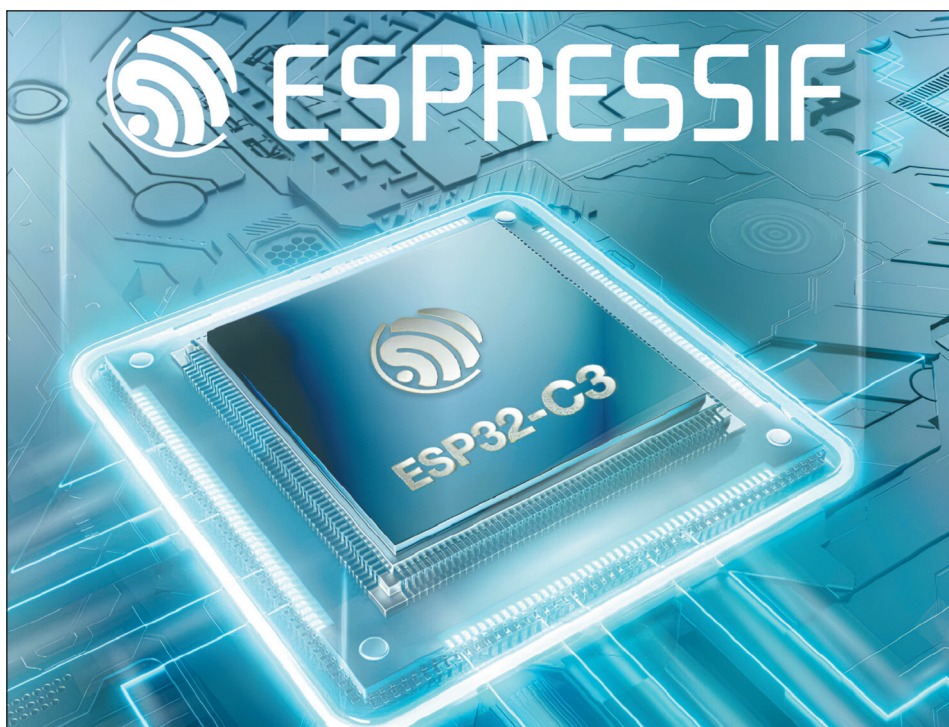


Рис. 1. Модуль ESP32-C3

ESP32-C3 разработан для устранения этой модели угроз.

- Защищенная загрузка данных (Secure Boot). ESP32-C3 реализует стандартную схему аутентификации на основе RSA-3072, чтобы гарантировать, что на платформе могут использоваться только доверенные приложения. Эта функция защищает от запуска вредоносного приложения, запрограммированного во флэш-памяти. Безопасная загрузка должна быть эффективной, чтобы устройства мгновенного включения (например, лампочки) могли использовать эту функцию. Реализация безопасной загрузки ESP32-C3 добавляет менее 100 мс к процессу загрузки.
- Флэш-шифрование. ESP32-C3 использует флэш-шифрование на базе AES-128-XTS, благодаря которому приложение, а также данные настроек могут оставаться зашифрованными во флэш-памяти. Контроллер флэш-памяти поддерживает выполнение зашифрованного микропрограммного обеспечения приложения. Это не только обеспечивает необходимую защиту конфиденциальных данных, хранящихся во флэш-памяти, но и защищает от изменений встроенного ПО во время выполнения, которые представляют собой атаки «время проверки — время использования».

- Цифровая подпись и HMAC-периферия. ESP32-C3 имеет периферийное устройство для цифровой подписи, которое может генерировать цифровые подписи с закрытым ключом, защищающим от несанкционированного доступа к встроенному ПО. Точно так же периферийное устройство HMAC может генерировать криптографический ключ, защищающий от доступа к встроенному ПО. Большинство облачных сервисов IoT используют аутентификацию на основе сертификатов X.509,

а периферийное устройство цифровой подписи защищает закрытый ключ устройства, который определяет его подлинность. Это обеспечивает надежную защиту идентификации устройства, даже если в ПО присутствуют уязвимости.

- World Controller.

В модуль ESP32-C3 внедрено новое периферийное устройство: world controller. Он представляет собой полностью изолированные друг от друга две среды. В зависимости от настроек world controller может использоваться для реализации доверенной среды выполнения (TEE) или схемы разделения приоритетов. Если ПО приложения получает задачу, связанную с конфиденциальными данными (например, цифровое управление правами (DRM)), то оно может воспользоваться преимуществом world controller и изолировать выполнение.

Bluetooth LE 5.0 с поддержкой Long-Range

Обычно подключенные устройства используют Wi-Fi для соединения с облачными сервисами. Однако устройства, работающие только по Wi-Fi, создают определенные трудности для сетевых настроек, поскольку не могут обеспечить надежную обратную связь провайдеру, в то время как у провайдеров iOS и Android возникают дополнительные сложности при подключении к сети. Наличие в устройстве радиомодуля Bluetooth LE упрощает настройку.

Кроме того, Bluetooth LE обеспечивает легкое обнаружение и управление в локальной среде. Предыдущие версии протокола Bluetooth LE имели меньший радиус действия, что делало его не очень подходящим протоколом для локального управления на больших пространствах, например

в многоэтажных домах. ESP32-C3 поддерживает протокол Bluetooth LE 5.0 с кодированными функциями PHY и расширенной рекламой, а также обеспечивает избыточность данных для пакетов, тем самым увеличивая дальность действия (обычно до 100 м). Кроме того, он поддерживает протокол Bluetooth LE Mesh. Это делает его отличным инструментом для управления устройствами в локальной сети и для соединения напрямую с другими сенсорными устройствами Bluetooth LE 5.0.

Достаточный объем памяти

При большом разнообразии вариантов использования и требований к памяти часто сложно определить наиболее подходящий ее размер для SoC-систем. Однако, опираясь на свой предыдущий опыт, компания Espressif пришла к выводу, что важно поддерживать варианты использования с одним, а иногда и с двумя TLS-подключениями к облаку, которые постоянно активны по Bluetooth LE, поэтому оптимальный запас для приложения в ESP32-C3 — это 400 кбайт. При этом стоимость нового модуля осталась приемлемой. Кроме того, ESP32-C3 имеет динамическое разделение для памяти хранения команд (IRAM) и хранения данных (DRAM). Таким образом, полезная память максимально увеличена. Здесь также важно отметить, что Espressif оптимизировали требования к памяти подсистемы Bluetooth по сравнению с ESP32.

Стабильное программное обеспечение

ESP32-C3 будет поддерживаться через популярную платформу Espressif ESP-IDF, которая уже поддерживает миллионы подключенных устройств и выпускается при тщательном контроле и строгом тестировании. Зрелость ESP-IDF, а также знакомство с API и инструментами облегчат разработчикам создание приложений для ESP32-C3. Благодаря доступности ESP-IDF другие программные компоненты, такие как облачные агенты, можно использовать на ESP32-C3 без каких-либо изменений. Помимо этого, ESP32-C3 поддерживает режим работы хоста, чтобы обеспечить возможность подключений по Wi-Fi и Bluetooth LE для внешних микроконтроллеров или микропроцессоров через ESP-AT и SDK, размещенных на ESP.

Также доступна модель ESP32-C3F, которая поставляется со встроенной флэш-памятью для упрощения проектирования. Espressif активно развивает линейку экономичных модулей, предназначенных для легкого создания подключенных устройств. В связи с этим компания выпустила модуль ESP32-C3-MINI-1, который выполнен в мини-формате (13×16,6 мм) и поддерживает работу при температуре до -105 °C. Для простоты миграции модуль ESP32-C3-WROOM-1 по контактам совместим с модулями ESP-WROOM-02D и ESP-WROOM-02. ESP32-C3-WROOM-1 также поддерживает максимальную температуру -105 °C. Как упоминалось ранее, ESP32-C3 ориентирован на наиболее распространенные варианты использования подключенных устройств. Однако Espressif продолжает создавать решения, которые будут учитывать дополнительные варианты использования.

Официальным дистрибьютором Espressif в России и странах СНГ является компания «ЕвроМобайл». ■

