МИКРОКОНТРОЛЛЕР USIP® ОТ INNOVA CARD: НОВАЯ ПЛАТФОРМА ДЛЯ СИСТЕМ С ВЫСОКИМИ ТРЕБОВАНИЯМИ К БЕЗОПАСНОСТИ

Кирпичников А.П., Киршин Е.А.

Один из авторов прочитал приведённое выше объявление, напечатанное скромно мелким шрифтом, (в “Volt&Nuts”, кажется) и грустно подумал о всех разработчиках с наивной верой закрывающих программу во внутренней флэш любезно предоставленным изготовителем «битом секретности» – «на века». А ведь алгоритмы в современном мире часто много ценнее и долговечнее, чем сами изделия. Недаром с тех пор произошли некоторые сдвиги в области их закрытия – многие солидные фирмы предлагают более серьёзные технологии «секретности» (например, компания Analog Devices ввела механизм Security LockBox® в DSP-процессорах Blackfin, что позволяет использовать двухуровневое шифрование для аутентификации и закрытия кода; Atmel объявил о создании специализированной CryptoMemory® EEPROM и т.д.).

Так существуют ли вообще микропроцессоры, гарантирующие стойкость от всех современных методов взлома (включающих анализ работы внутренних шин по записи электромагнитного фона; принуждение аппаратной части к ошибкам и раскрытию секретов воздействием «рентгена» – как в зубоврачебном кабинете, бесчисленные зонды и щупы для подключения к «интимным» местам кристалла сквозь тонкую «обёртку» корпуса и пр.), и, если да, то насколько специфика сохранения тайны ограничивает при этом реальные возможности такого вычислителя – об этом наша статья.

«Если вы забыли программу своего микроконтроллера и первоисточники утеряны, обратитесь к нам, и мы прочитаем её для вас…»

Объявление в американском журнале конца 90-х

Микроконтроллер USIP®

USIP был разработан во Франции в 2004 году для нужд сохранения информации наиболее ценящейся в Европе – банковской тайны. Причём расчётная стоимость «взлома» самыми современными средствами, экономящими силы и время, и без учёта стоимости оных, по проекту должна составлять не менее € 50 тыс. (а в идеале, достигать €1 млн.), а время, при достаточном количестве образцов, – тысячи человеко-часов. Основным применением микросхемы должны являться различные платёжные терминалы и иные электронные средства идентификации и доступа (ключи, радио ID и пр.). На борту контроллера может быть размещена любая из существующих криптографических систем (наиболее примитивная – AES, даже аппаратно встроена, чтобы не занимать ресурсы процессора). При этом микросхема продолжает являться достаточно мощным вычислительным средством с разветвлёнными интерфейсами, позволяющим автономно решать большинство задач, возникающих при создании компактного интеллектуального прибора обработки информации.

Ядро. В качестве платформы для построения системы было выбрано защищённое ядро MIPS 4KSd, как наиболее отвечающее требованиям защиты информации, как с учётом топологии так и производительности.

Ядро этого типа разрабатывалось для поддержки продуктов с множеством приложений, в частности, базирующихся на высокоэффективных алгоритмах шифрования и виртуальных машинах. 4KSd реализует архитектуру MIPS32 с поддержкой SmartMIPS ASE (для ускорения алгоритмов шифрования, таких как RSA, ECC, DES и AES) и механизмом оптимизации плотности кода MIPS16E. При этом ядро имеет дополнительные блоки, благодаря которым достигается увеличение быстродействия на вышеуказанных алгоритмах. Так, имеется автономный блок умножения/деления 32x16 и 32x32, выполняющий операции умножения и умножения с накоплением за один и два такта частоты ядра соответственно.

MIPS 4KSd имеет пятиступенчатый конвейер с обратной связью и работает на тактовой частоте до 96 МГц (в новых моделях – до 175 МГц) с возможностью выполнения инструкций в каждом такте. За счет наличия дополнительных блоков вычисления пиковая производительность достигает 1,30 MIPS/МГц, что выгодно отличает кристалл от других ядер, имеющих обычно 0.5-0.8 MIPS/МГц. В состав ядра также входят 2 блока кэш-памяти инструкций и данных, по 8 Кбайт каждый.

Память. Контроллер содержит в себе три типа памяти: ROM (128 Кб), RAM (128 Кб) и Flash (256 Кб). Память ROM содержит загрузчик Secure Boot Loader (предназначен для обновления прошивки и записи ключей для алгоритмов шифрования) и библиотеку низкоуровневого доступа к периферии Hardware Abstraction Layer (HAL).

Доступ к памяти ROM и RAM осуществляется в режимах 8-, 16- и 32- бит за один такт частоты ядра.

В USIP® имеется контроллер внешней памяти, поддерживающий память SDRAM (32 Мб, максимальная частота 96 МГц) и до четырех слотов памяти SRAM (4x32Мб).

Адресное пространство памяти линейное и составляет 4Гб. Имеется механизм MMU, с использованием которого возможно разграничение доступа к памяти по страницам (размером от 1 Кб до 16 Мб) с режимом доступа чтение/запись/выполнение. Это достигается с использованием конфигурируемых блоков TLB.

Достаточно быстрая встроенная Flash осуществляет запись страницы (2048 бит) за 1 мс, есть дополнительные возможности приостановки записи/стирания, проверки содержимого по 128-бит и 16-бит сигнатурам. Чтение Flash возможно в двух режимах (синхронный и асинхронный), отличающихся скоростью и энергопотреблением.

Прерывания и DMA. Ядро MIPS 4KSd имеет шесть уровней приоритетов внутренних прерываний, что позволяет создавать системы с гибким распределением и иерархией процессов. Для каждого уровня в USIP® жестко закреплен определённый набор периферии. Для обработки внешних прерываний имеется отдельный вход для быстрого обслуживания. Кроме того, есть возможность настроить каждый из 32-х имеющихся выводов GPIO в качестве источника внешнего прерывания. Отдельное прерывание – NMI, которое используется в системе безопасности для генерации сброса микросхемы в случае атаки.

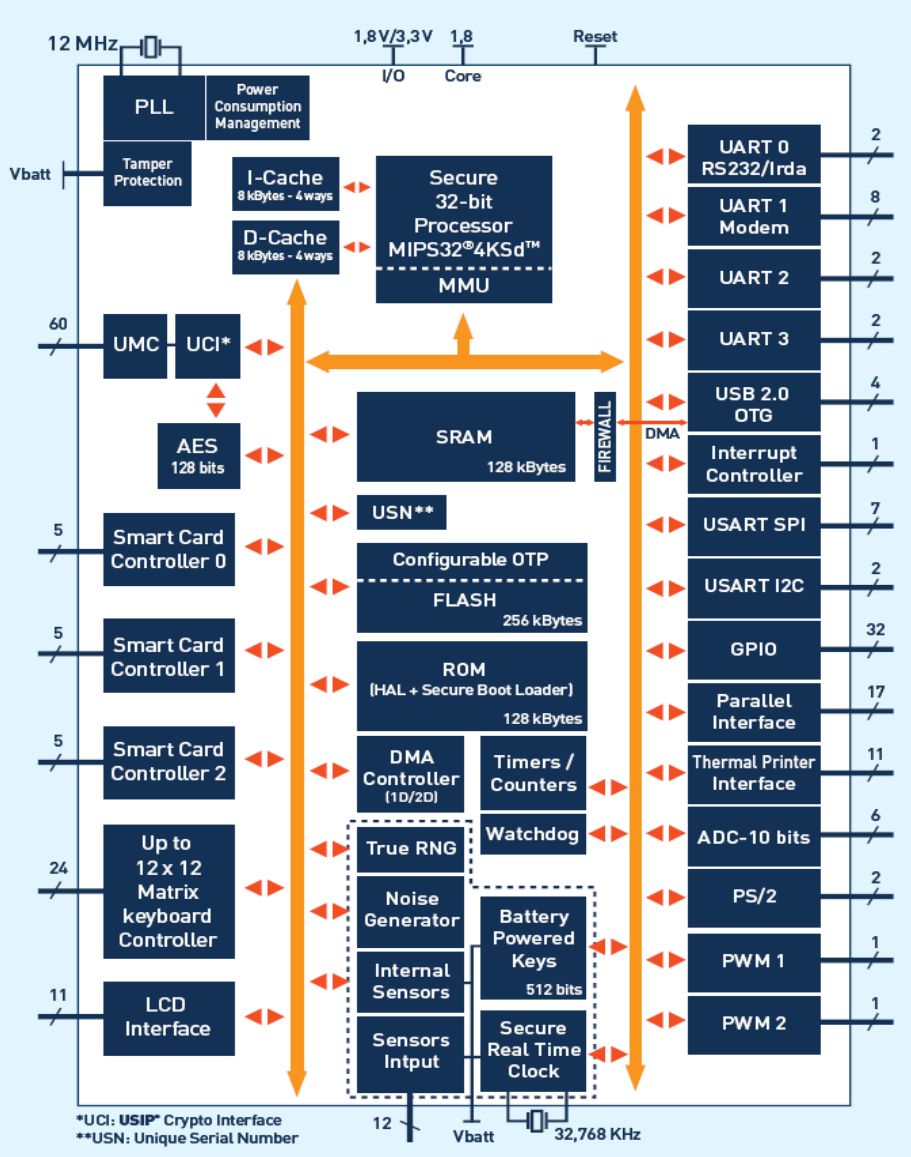

Рис. 1. Структурная схема микроконтроллера USIP®.

Благодаря достаточно развитому механизму DMA существует возможность передачи данных память - память, память - периферийные устройства (кроме тех устройств, в которых в качестве базовой используется частота, отличная от частоты PLL). Режимы 1D и 2D с положительным и отрицательным шагом позволяют организовать «разворот» буферов в памяти, а также упаковку/распаковку без использования ресурсов процессора. Эти возможности могут значительно повысить быстродействие при различных преобразованиях форматов данных. При обмене данными с периферией существует возможность упаковки/распаковки данных на лету. Еще одна возможность контроллера DMA – приостановка передачи с последующим возобновлением.

Периферия. USIP представляет собой систему на кристалле, поэтому большинство интерфейсов передачи данных – внешние, такие как UART и USB. Интерфейсы обмена в пределах устройства ограничены минимумом: SPI и I^2C.

Из коммуникационных интерфейсов в USIP® присутствуют UART (2 двухпроводных, один с поддержкой IrDA и один с полным набором сигналов для подключения модема, до 2 Мбит/с, имеются буфера FIFO), USB 2.0 OTG (16 конечных точек), I^2C (Philips 2.1, 100/400 КГц), SPI (1.5 МГц, настраиваемый режим Motorola и изменяемая длина слов), SPP (IEEE1284, совместимый с IBM PC Centronix), PS2 (для подключения клавиатуры и мыши IBM PC).

Интерфейсы, обеспечивающие ввод-вывод: интерфейс смарт-карт (три интерфейса, работающих в синхронном и асинхронном (ISO-7816 UART) режимах, есть режим эмуляции смарт-карты), интерфейс термо-принтера, контроллер клавиатуры (для подключения матриц с размером до 12x12 линий), LCD-интерфейс.

В USIP® также присутствует набор таймеров: Watchdog с системой защиты, два 32-битных PWM и четыре 16-битных таймера общего назначения.

Для ввода аналоговых сигналов имеется 10-бит АЦП (разрядность может изменяться от 2 до 10 бит) с максимальной частотой дискретизации 400 КГц, использующий в качестве опоры одно из питаний: 1.8 В или 3.3 В.

Питание, тактовая частота и энергопотребление. Кристалл имеет несколько вводов питания 3.3 В и 1.8 В: линии питания ядра, периферии, памяти, аналоговых устройств и устройств защиты. USIP® довольно экономичен: на частоте 96 МГц, при всех включенных периферийных устройствах, микросхема потребляет около 160 mA (90% по линии ядра (1.8 В) и 10% по линии IO (3.3В)).

Для управления энергопотреблением в USIP® реализовано четыре режима. Два настраиваемых рабочих режима задают набор включенной периферии, режим переключения частоты ядра и режим Ultra-low power (например, для приостановки устройства в режим ожидания по USB).

Механизмы обеспечения безопасности

Механизмы защиты в USIP® присутствуют на различных уровнях и практически в каждом функциональном блоке. Можно выделить следующие уровни защиты: физический, логический и уровень организации процесса разработки и производства.

В качестве пассивной физической защиты используется специальный металлический экран на поверхности кристалла, к нему же подключён дополнительный активный датчик «на вскрытие» кристалла.

Активную защиту обеспечивает набор внешних и внутренних датчиков системы. Задача внутренних датчиков – постоянный мониторинг параметров системы и выполнение необходимых мер (сброс микросхемы, генерация прерывания NMI, стирание защищённой области памяти т.п.) при обнаружении выхода параметров за допустимые пределы. Среди параметров слежения – входная частота PLL, напряжение питания ядра, температура корпуса, доза облучения и др. Внешние датчики позволяют разработчику подключать их по своему усмотрению для отслеживания угрозы внешнего проникновения.

Микроконтроллер USIP® имеет вход резервного питания, использующегося для питания механизмов защиты в случае отключения основного источника.

Ядро MIPS 4KSd также обладает функциями защиты данных. Например, имеются механизмы рандомизации заполнения кэша и его скремблирование. Передача данных по внутренним шинам также осуществляется в режиме скремблирования, что защищает от утечки данных путем анализа электромагнитного излучения (ЭМИ) схемы.

Внешняя память защищена механизмом USIP® Crypto Interface. При его включении все данные, передаваемые по шине аппаратно, шифруются алгоритмом AES-128. Шифрование происходит «прозрачно» для программы микроконтроллера, не занимая ресурсов процессора и не добавляя задержек в передачу данных. К интерфейсу UCI возможно также подключение контроллера Ethernet, что позволяет пересылать зашифрованные данные с большой скоростью на большие расстояния.

Для организации защиты данных на логическом уровне в ядре 4KSd предусмотрен механизм MMU, который, с использованием конфигурируемых TLB (Translation Lookaside Buffers) обеспечивает разграничение доступа к областям памяти процессора.

Для реализации алгоритмов эффективного шифрования и скремблирования в USIP® имеется блок генерации случайных чисел, соответствующий стандартам NIST 800-22 и DIEHARD.

Разработчики позаботились также о защите периферии. Многие периферийные устройства и интерфейсы имеют встроенные механизмы защиты, устраняющие уязвимые места схемы. Так, например, интерфейс USB имеет встроенный файервол, а контроллер клавиатуры защищён от сканирования ЭМИ.

Одним из видов вторжения является злонамеренный доступ к разрабатываемому устройству со стороны самих разработчиков одной из стадий разработки. К примеру, у Innova Card, как разработчика аппаратной части имелась бы потенциальная возможность проникнуть в микросхему после того, как устройство на базе USIP уже создано и получить доступ к «защищённой» информации. Однако разработчики предусмотрели защиту «от себя» и других участников разработки. Механизм защиты на уровне процесса разработки и производства состоит в следующем: в USIP® дополнительно предусмотрен механизм смены фаз жизненного цикла микроконтроллера. При переходе от предыдущей стадии к последующей производится смена набора ключей шифрования, что предотвращает возможность доступа к микросхеме со стороны участников предыдущих стадий жизненного цикла.

Для обеспечения безопасного обновления программного обеспечения и загрузки ключей защиты в USIP® реализован загрузчик Secure bootloader с динамической аутентификацией на основе алгоритма AES.

Средства разработки

Средства разработки традиционно представлены программным обеспечением для PC, отладочной платой и эмулятором. Для системы Windows имеется набор программного обеспечения USIP® HDE – среда разработки Eclipse с набором средств компиляции MIPS.

Особый интерес для разработчиков может представлять платформа Linux. Разработчики компании Innova Card портировали ядро Linux на USIP® и создали комплект «Linux Development Environment», включающий в себя гибкую систему конфигурирования компиляции ядра, файловой системы и библиотек, а также среду отладки. Установка и настройка платформы для Linux на USIP происходит довольно быстро, что позволяет выпустить продукцию на рынок за достаточно краткие сроки, обеспечив при этом большую функциональность устройства.

Innova Card предоставляет отладочный комплект UEK – USIP® Essential Kit. Это плата с установленной микросхемой USIP®, содержащая память SDRAM, SRAM, 2 FLASH, 2 интерфейса RS-232, Ethernet, USB OTG, JTAG, дополнительные разъемы для подключения внешнего оборудования (клавиатура, мышь и т.п.) и плат расширения. Кроме того, контакты ввода-вывода USIP® выведены на специальные площадки, к которым имеются две платы-защелки для внешнего доступа. Также компанией разработан комплект “EZ-Cert for EMV L1 Type Approval”. Это комплект, состоящий из платы, подключаемой к UEK и позволяющей получить доступ к двум смарт-картам и четырём модулям безопасного доступа (Security Access Modules (SAMs)) одновременно.

Для отладки программного обеспечения по JTAG используется эмулятор FS2 компании First Silicon. Имеется две версии этого эмулятора: с интерфейсами LPT и USB. Скорость доступа составляет 10 МГц.

Программное обеспечение

Имеется множество решений для USIP® от Innova Card и третьих фирм. Рассмотрим некоторые из них:

- UCL Crypto-library от Innova Card. Библиотека включает следующие алгоритмы шифрования: RSA (до 2048 бит), DES, 3DES, AES-128, SHA-1, SHA-256, RIPEMD-160, MD5, HMAC, TRNG/PRNG, ECC, генерация ключей и Diffie-Helmann.
- SmartSoft EMV Level 2 approved kernel – библиотека, которая предоставляет интерфейс для работы со смарт-картами. Библиотека написана с учетом требований стандарта EMV L2, поэтому её использование упрощает процесс сертификации. Эту библиотеку рекомендуют использовать совместно с пакетом Innova Card EZ-Cert L1. EMV L2 Kernel представляет собой один из уровней иерархии программного обеспечения для USIP®,

устанавливающийся поверх операционной системы (если она имеется) и библиотек Innova Card EMV L1 и HAL. В свою очередь, библиотека состоит из трех уровней: обмена данными между терминалом и смарт-картой; функций парсинга и конвертации данных с карты; функций поддержки требований стандарта EMV2000 4.1. Пакет EZ-Cert2 – это программная часть EMV L2 Kernel, поддержка при интеграции EMV L2 Kernel на систему разработчика и помощь при прохождении сертификации EMV L2.

- Trango – "гипервизор" – одна из перспективных разработок фирмы Trango Systems. Так, если вам требуется защита системы с большой функциональностью и при этом выпустить продукцию необходимо в кратчайшие сроки, то можно за основу вашей платформы взять Linux, «закрыв» его системой Trango.

Trango – система, подобная виртуальной машине, которая устанавливается на USIP®. Эта система создает необходимое количество «виртуальных окружений» для запуска в них операционных систем либо отдельных программ. Главная задача гипервизора – разграничение доступа к отдельным ресурсам микроконтроллера. Например, возможно разрешить использование USB для окружения, в котором выполняется Linux, а доступ к какому-либо UART открыть только для Windows CE. По заявлению разработчиков, накладные расходы на гипервизор Trango составляют не более 3%. Применение этой системы – интеграция открытых (заведомо незащищенных) операционных систем наподобие Линукс в системы со специальными требованиями к безопасности. Ранее задача разграничения доступа к защищённым данным решалась за счет установки двух микроконтроллеров. Использование Trango позволяет это сделать на одной микросхеме.

- jTOP® for Terminals фирмы Trusted Logic – межплатформенное ПО (middleware), совместимое со стандартами GPD и STIP, с набором программных средств и сервисов. Состав библиотек включает в себя: функции стандарта EMV L2, алгоритмы шифрования, стеки коммуникации USB и TCP/IP, поддержка виртуальной машины java.

USIP® в ряду других микроконтроллеров

Глубокая специализация кристалла в области обеспечения безопасности не настолько драматически повлияла на его характеристики как обычного контроллера или вычислителя системы, что позволяет сравнивать его с наиболее успешными образцами из обычного ряда контроллеров. Например, USIP® имеет достаточно схожую структуру с 32-битными микроконтроллерами на базе ядра ARM9. В качестве примера для сравнения был рассмотрен достаточно новый микроконтроллер от STMicroelectronix – STR912FAW44.

Механизмы организации памяти, прерываний и DMA выполнены аналогично. Отличия имеются лишь в деталях реализации. Выборка из Flash организована также, как и в других микроконтроллерах: имеется 128-битный регистр предвыборки, заполняющийся за 4 такта частоты процессора, что позволяет в каждом такте получать одно 32-разрядное слово при условии последовательного расположения во Flash.

В USIP® имеется достаточно развитый набор функциональных устройств и периферии. При этом отдельно взятые периферийные устройства лишь незначительно уступают в функциональной насыщенности микроконтроллерам на базе ARM9. Так, фиксированный множитель PLL не позволяет плавно настраивать частоту, что затрудняет управление энергопотреблением, однако в какой-то степени это компенсируется сравнительно низким общим потреблением микросхемы и возможностью использовать четыре режима управления питанием. Несмотря на то, что контроллер в общении с периферией ориентирован на защиту информации, присутствуют также и некоторые достоинства периферийных устройств. Например, имеется возможность достаточно гибко изменять приоритеты устройств на внутренней шине микроконтроллера; устройство DMA предоставляет дополнительные возможности (режим 2D, положительный и отрицательный шаг, приостановка передачи и пр.).

Поскольку специфика микросхемы – обеспечение безопасности, в USIP® сделан упор на увеличение производительности именно алгоритмов шифрования. Так, например, благодаря дополнительным вычислительным блокам, производительность алгоритмов AES, 3DES и SHA-1 на 50-100% выше, чем на микроконтроллере STR912FAW44, имеющем аналогичную тактовую частоту 96 МГц. Для сравнения: генерация 1024-битной сигнатуры RSA занимает менее 35мс.

Следующая версия кристалла USIP2 будет работать на частотах до 175 МГц, что позволит сравнивать этот микроконтроллер с процессорами ARM и MIPS, работающими на частотах до 300 МГц.

Главное достоинство USIP® в сравнении с другими микроконтроллерами – это, несомненно, его защищённость, заложенная в концепцию микроконтроллера изначально. Недостатки же, связанные с некоторыми ограничениями в периферийных устройствах, - лишь временное явление (добавить функциональность в периферию гораздо проще, чем изменять сами принципы архитектуры!). Подобные недостатки могут быть легко исправлены в следующих ревизиях микросхемы, и можно говорить о достаточно высоком потенциале этого кристалла.

Заключение

USIP®, представляя собой готовую платформу для создания платёжных терминалов (POS) и других устройств обеспечения банковской тайны, является одновременно современным высокопроизводительным кристаллом с разветвлённой периферией и может являться базой для построения самых разных устройств, защищающих ноу-хау разработчика на самом высоком уровне.

Обладая низкой стоимостью (€12-15), микросхема, при достаточно высокой производительности, предоставляет широкий набор периферии, позволяющий дополнительно сократить число внешних микросхем и уменьшить стоимость изделия в целом. Основное же преимущество данного кристалла – это система защиты, заложенная в архитектуру системы изначально, что позволяет совместить производительность, гибкость и защищенность в одном корпусе и обеспечить соответствие всем современным требованиям безопасности.

К настоящему времени на основе USIP уже выпущено несколько продуктов, успешно прошедших сертификацию на соответствие современным стандартам безопасности (EMV, PCI и др.)

Ссылки

1. Официальный сайт компании Innova Card: http://www.innova-card.com.

2. Официальный сайт компании Analog Devices: http://www.analog.com

3. Официальный сайт компании Trusted Logic: http://www.trusted-logic.com.

4. Официальный сайт компании Trango Systems: http://www.trango-systems.com.

5. Официальный сайт компании SmartSoft: http://www.smartsoft-it.com.