АРХИТЕКТУРНЫЕ ИННОВАЦИИ В МНОГОЯДЕРНЫХ ИКМ QorIQ

ВЛАДИМИР ЕГОРОВ, к.т.н., в.н.с., Институт проблем информатики РАН

Статья знакомит читателей с интересными архитектурными новшествами в последних многоядерных интегрированных коммуникационных микроконтроллерах (ИКМ) семейства QorIQ компании Freescale Semiconductor.

ВВЕДЕНИЕ

Интегрированные коммуникационные микроконтроллеры, давно выпускаемые компанией Motorola и ее преемницей Freescale Semiconductor, по сей день остаются востребованными на рынке телекоммуникационной микроэлектроники и интегрированных приборов для интеллектуальной пакетной коммутации и маршрутизации. Особенно к месту они пришлись производителям оригинального оборудования OEM (Original Equipment Manufacturers). Особенность рынка OEM заключается в том, что специфическое оборудование производится небольшими сериями и обеспечить экономическую эффективность и прибыльность такого производства можно только при использовании готовых решений и устройств, легко адаптируемых под нужды конкретных заказчиков. ИКМ в полной мере отвечают этим требованиям. Удачное сочетание встроенных высокопроизводительных процессоров с гибко адаптируемыми контроллерами ввода-вывода и системными опциями, ориентированными на самый широкий спектр приложений в области современной телекоммуникации и пакетной коммутации, позволяет создавать оригинальные системы с использованием широко распространенных современных телекоммуникационных стандартов и программировать собственные (proprietary) протоколы.

ИКМ компании Freescale прошли долгий путь эволюции. Сегодня выпускаются четыре их семейства от самых первых IMP (Integrated Multi-protocol Processor) и QUICC (Quadruple Integrated Communications Controller) до современного PowerQUICC в четырех поколениях (PowerQUICC I, PowerQUICC II, PowerQUICC II Pro и PowerQUICC III) и, наконец, последнего семейства QorIQ. Любопытно, что абсолютно нигде, ни на сайте компании Freescale, ни в «Википедии», нет расшифровки этой странной аббревиатуры. Можно лишь предполагать, что буквы **Q** в ней как-то связаны с предтечами этого семейства QUICC и PowerQUICC, а звучание может быть схожим со словом *кворум* (quorum).

Семейство ИКМ QorIQ — совсем молодое. Первые приборы появились на свет в 2008 г., но уже сегодня компания Freescale предлагает в этом семействе пять базовых платформ, включающих по нескольку моделей. И если две младшие платформы P1 и P2 лишь немногими несущественными признаками отличаются от последнего поколения ИКМ семейства PowerQUICC, то благодаря трем старшим платформам — P3, P4 и P5 — разработчики компании Freescale, безусловно, сделали значительный шаг в архитектуре ИКМ и вновь подтвердили лидерство компании в этой области.

Обобщенная структура трех старших платформ ИКМ семейства QorIQ показана на рисунке 1, а в таблице 1 приведены их основные характеристики. Самыми революционными и достойными отдельного рассмотрения являются четыре особенности платформ P3, P4 и P5, определяющие новые подходы компании Freescale к архитектуре современных ИКМ:

- новое процессорное ядро;
- встроенный гипервизор;
- архитектура ускорения в путях данных;
- архитектура доверия.

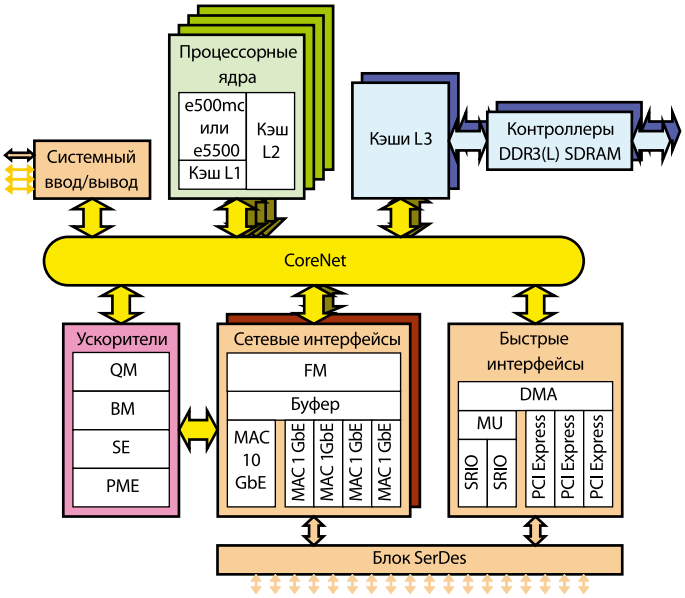


Рис. 1. **Обобщенная структура платформ P3, P4 и P5 семейства QorIQ**

НОВОЕ ПРОЦЕССОРНОЕ ЯДРО

Перманентная тенденция повышения производительности процессоров за счет расширения разрядной сетки не обошла стороной ИКМ. Первое поколение ИКМ, IMP, базировалось на 16-разрядном ядре, все последующие с брендами QUICC и PowerQUICC — уже на 32-разрядных процессорных ядрах. Самое мощное из них, ядро e500, реализованное с проектными нормами 90 нм, стало основой семейства третьего поколения ИКМ в линейке PowerQUICC.

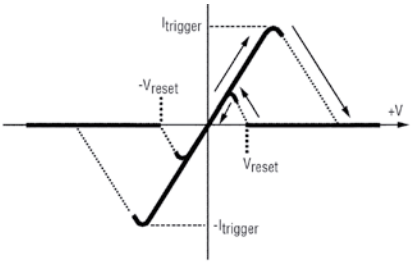
Платформы ИКМ семейства QorIQ с P1 по P4 тоже имеют 32-разрядные процессорные ядра, причем в платформах P1 и P2 — это все то же ядро e500, разве что выполненное с проектными нормами 45 нм. Для платформ P3 и P4 это ядро было доработано с целью эффективного использования гипервизора в многоядерных ИКМ, вследствие чего получило шифр e500mc (e500 multicore). Однако в самой последней платформе P5

Honeywell
Infineon technologies
EPCOS
SICK
VISHAY
BOURNS Reliable Electronic Solutions
IOR
Tyco Electronics
Panasonic ideas for life
CRYDOM
DATA VISION
MITSUBISHI ELECTRIC
Kingbright
muRata Innovator in Electronics
velleman

УСТРОЙСТВА ЗАЩИТЫ ОТ ИМПУЛЬСНЫХ ПОМЕХ TBU

BOURNS® Reliable Electronic Solutions

- реализация защиты от перенапряжения и высокого тока в одном устройстве
- высокая скорость срабатывания (устранение импульса за 100 нс)
- высокий уровень напряжения и тока блокировки
- прецизионное ограничение выходного тока и напряжения
- широкая полоса пропускания без вносимых помех (до 3 ГГц)
- малые габаритные размеры
- лучшее соответствие требованиям Telcordia GR-1089 и ITU K.20/K.21



www.platan.ru ПЛАТАН
Офисы в Москве: м. Молодежная: ул.Ивана Франко, 40, стр.2, (495) 97-000-99, e-mail: platan@aha.ru;
м. Новослободская: 1-й Щемиловский пер., 16, стр.2 (495) 744-70-70, platan@platan.ru
Офис в Санкт-Петербурге: ул. Зверинская, 44 (812) 232 88 36, baltika@platan.spb.ru

наконец появилось новое 64-разрядное ядро e5500, изначально предназначенное для мощных многоядерных ИКМ семейства QorIQ.

Новое 64-разрядное ядро и вся платформа P5 ориентированы на вычислительно интенсивные приложения, такие как обработка изображений и видео или статистическая обработка больших массивов данных. И по-прежнему в центре внимания компании Freescale находятся приложения, связанные с телекоммуникацией и пакетной обработкой, где 32-разрядная сетка вносила естественное ограничение на длину адреса и, тем самым, допустимые размеры виртуальной оперативной памяти. Переход на 64-разрядное ядро позволил увеличить сквозной непрерывный объем виртуальной памяти в 16 раз — с 4 до 64 Гбайт.

Архитектурно ядро e5500 с суперскалярной организацией и двумя семиступенными конвейерами в основном не отличается от ядра e500mc за исключением расширения машинного слова с 32 до 64 разрядов и повышения рабочей частоты с 1,5 до 2,5 ГГц, что дает в сумме более чем трехкратное повышение производительности отдельного ядра. Менее значительные особенности ядра e5500 по сравнению с ядром e500 заключаются в организации блока плавающей запятой, кэша второго уровня и поддержки гипервизора.

Естественно, ядро e5500 сохраняет полную программную совместимость с ядром e500 за исключением форматов данных с плавающей запятой. Ядро e5500 поддерживает широко распространенные форматы представления чисел с плавающей запятой, соответствующие стандарту IEEE 754, включая двойную точность. Его блок плавающей запятой обеспечивает по сравнению с аналогичным блоком ядра e500 удвоение производительности при одинарной точности и учетверение при двойной на одной и той же рабочей частоте. Новые возможности использовать не обязательно: пользователю предоставлена возможность искусственно установить традиционный 32-разрядный режим для прикладных программ, где разрядность имеет принципиальное значение, но, разумеется, с потерей свойственного новому ядру выигрыша по производительности. По сравнению с ядром e500 изменились также максимальный размер и дисциплина использования кэша второго уровня. Если в предыдущих ядрах такой кэш находился между оперативной памятью и кэшами первого уровня (front-side L2 cache) и по объему не превышал 128 Кбайт, то в ядре e5500 максимально возможный размер кэша L2 вырос до 512 Кбайт, и он был перенесен с шины памяти на отдельную шину (back-side L2 cache). Последнее позволило повысить быстродействие и снизить паразитный трафик в системе, вызванный необходимостью поддерживать когерентность кэша. Кроме того, более гибкая организация кэша L2 предоставила возможность пользователю произвольно его конфигурировать, в частности:

– блокировать отдельные линейки кэша для ускорения выполнения некоторых часто повторяющихся программ-

Таблица 1. **Характеристики платформ ИКМ семейства QorIQ**

Характеристика	P1	P2	P3	P4	P5
Процессорное ядро	e500	e500	e500mc	e500mc	e5500
Разрядность	32	32	32	32	64
Число ядер	1 или 2	2 или 4	4	4 или 8	1 или 2
Рабочая частота, ГГц	до 0,8	до 1,2	до 1,5	до 1,5	до 2,2
Скорость Ethernet, Гбит/с	до 1	до 1	до 10	до 10	до 10
Архитектура DPAA	нет	нет	есть	есть	есть
Архитектура TA	нет	нет	есть	есть	есть

ных действий, например, обработки прерываний;

– организовывать ассоциативный кэш с восемью записями в линейке (eight-way cache);

– использовать весь кэш или его части в качестве сверхбыстрой «подручной» (scratch-pad) оперативной памяти с произвольным доступом.

ВСТРОЕННЫЙ ГИПЕРВИЗОР

Существенным отличием ядер e500mc и e5500, безусловно, стал встроенный гипервизор с полноценной аппаратной поддержкой, что обеспечило возможность более эффективного использования многоядерных ИКМ. Многие приложения предполагают организацию на одном ИКМ нескольких относительно независимых и взаимно изолированных вычислительных доменов, в ряде случаев даже с различными операционными средами. Очевидно, что самое простое и эффективное решение в таких случаях — построение системы на основе ИКМ с многоядерным процессором. Но одной многоядерности процессора недостаточно. Между изолированными вычислительными доменами помимо распределения процессорных ядер необходимо надежно разделить массив наличной памяти и встроенный ввод-вывод. При этом механизмы разделения должны не только гарантировать взаимную изоляцию вычислительных доменов, но и обеспечить максимально эффективную работу операционных систем и всех вычислительных процессов внутри каждого отдельного домена. К типичным приложениям из области телекоммуникации, пакетной коммутации и маршрутизации, естественно воспринимающим гетерогенную мультипроцессорность и вследствие этого эффективно реализуемым на многоядерных ИКМ QorIQ, можно отнести:

– программные коммутаторы пакетов (soft switches) с явно выраженными раздельными задачами коммутации (data plane) и управления (control plane);

– комбинированные системы, использующие наряду с универсальной операционной средой, например Linux, оригинальные операционные системы, в частности, системы реального времени;

– сложные программные комплексы, включающие либо специальное особо охраняемое, либо, наоборот, стороннее недостаточно апробированное и достоверное программное обеспечение.

В многоядерных ИКМ семейства QorIQ функции разделения наличных ресурсов между вычислительными доменами выполняет встроенный гипервизор — специальная привилегированная программа низкого уровня. Находясь «под операционной системой» домена, гипервизор предоставляет ей некую виртуальную машину с набором ресурсов, отнесенных к данному домену. Гипервизор способен параллельно управлять множеством виртуальных машин как на одном процессорном ядре, так и на нескольких ядрах. Механизм управления виртуальными машинами схож с механизмом переключения процессов операционной системой. В результате разделения каждая виртуальная машина работает независимо от других, даже не подозревая об их существовании.

Поскольку гипервизор непосредственно взаимодействует с операционными системами вычислительных доменов, следует предположить, что эти операционные системы должны знать о наличии гипервизора и понимать его интерфейс. Это значит, что использование любой операционной системы в многоядерных ИКМ требует внесения в нее определенных корректив, объем и сложность которых зависят, в первую очередь, от качества реализации гипервизора. Следует отметить, что компания Freescale предоставляет версию стандартной системы Linux, работающую над гипервизором. Ряд поставщиков широко используемых операционных сред, в том числе систем реального времени, также дорабатывает свои продукты для совместной работы с гипервизором ИКМ семейства QorIQ.

Гипервизор, имеющийся в многоядерных приборах QorIQ, в наибольшей степени затрагивает три архитектурных компонента процессоров ИКМ:

– режимы и состояния процессора;

– диспетчер памяти;

– механизм прерываний.

В ядрах e500mc и e5500 для гипервизора введен специальный высокопривилегированный режим и отдельный комплект критических для производительности и реактивности процессорных регистров, причем переключение на эти регистры происходит сугубо аппаратно так, что эта добавка совершенно незаметна операционной системе и прикладному ПО.

Специально для гипервизора 64-разрядное ядро e5500 предусматривает, а 32-разрядное ядро e500mc дополнительно вводит пространство виртуальных адресов добавлением отдельного идентификатора логического подразделения. Кроме того, в многоядерные ИКМ семейства QorIQ включен дополнительный блок диспетчера памяти для доступа от периферии PAMU (Peripheral Access Management Unit). Это важный компонент разделения и защиты памяти за счет трансляции виртуальных адресов прямого доступа в физические адреса памяти, выполняемой через программно конфигурируемые таблицы. Любое встроенное в ИКМ устройство ввода-вывода, обладающее способностью прямого доступа в память, может быть сконфигурировано для работы исключительно через PAMU.

Механизм прерываний в многоядерных ИКМ семейства QorIQ устроен таким образом, что гипервизор может либо «замкнуть» некоторое прерывание на себя, либо «переключить» его на тот или другой вычислительный домен. В первом случае он оставляет контроль над данным прерыванием за собой, во втором — отдает его операционной системе домена, причем без каких-либо задержек и накладных расходов. Примером таких «переключаемых» прерываний могут быть критические, с точки зрения реактивности, системы прерывания от приданных домену сетевых интерфейсов, обрабатываемые операционной системой реального времени данного домена.

Гипервизор поддерживает два механизма обслуживания программ в отдельных доменах: явный и прозрачный. Явный механизм базируется на специальных программных запросах гипервизору для выполнения определенных специфических действий. Прозрачный механизм работает так, что операционная система или прикладная программа вообще не замечают посредничества гипервизора. Например, выполнение операционной системой некоторой привилегированной инструкции вызывает прерывание процесса и переключение на гипервизор, который после соответствующего контроля может заблокировать выполнение данной инструкции или выполнить ее «от своего имени» и вернуть, если требуется, результат операционной системе.

Равноправные изолированные между собой домены, тем не менее, имеют возможность обмена информацией через гипервизор. Другая интересная особенность гипервизора — возможность создавать неравноправные домены. Например, один домен может быть назначен управляющим, а другой — управляемым. При этом управляющий домен имеет возможность запускать в работу управляемый домен, останавливать его, получать доступ к его данным и реагировать на соотнесенные с ним прерывания.

В результате гипервизор в ИКМ семейства QorIQ обеспечивает в комплексе:

– организацию множества вычислительных доменов и разделение между ними имеющихся в ИКМ процессорных ядер и встроенных контрол-

леров ввода-вывода, а также наличной внешней памяти системы;

– надежную изоляцию доменов друг от друга;

– выделение двум или нескольким доменам общих разделенных ресурсов, в частности общих массивов памяти;

– небольшие накладные расходы на свою работу и в пределе полное исключение потерь производительности и реактивности для критических процессов реального времени;

– минимум изменений в устанавливаемых «поверх него» операционных системах.

АРХИТЕКТУРА УСКОРЕНИЯ В ПУТЯХ ДАННЫХ

Поскольку ИКМ семейства QorIQ ориентированы, в частности, на интеллектуальную высокоскоростную обработку телекоммуникационных данных, программную коммутацию (soft switching) и маршрутизацию (routing) в современных пакетных сетях, для них компания Freescale разработала специализированную фирменную архитектуру ускорения путей данных DPAA (Data Path Acceleration Architecture). При обработке пакетов DPAA затрагивает все основные компоненты ИКМ:

– процессорные ядра;

– интеллектуальные контроллеры ввода-вывода и сетевые интерфейсы;

– аппаратные ускорители обработки пакетов;

– инфраструктуру диспетчеризации внутреннего трафика, обеспечивающую эффективное движение пакетов между всеми названными выше компонентами архитектуры.

В отношении процессорных ядер DPAA весьма толерантна и может быть использована как в одноядерных, так и в многоядерных ИКМ со встроенными кэшами двух уровней. Однако в последнем случае архитектура предоставляет дополнительные уникальные возможности, не типичные для универсальных многоядерных процессоров.

Интеллектуальный ввод-вывод как средство выхода в пакетные сети помимо привычных в ИКМ Freescale универсальных MAC-контроллеров, поддерживающих в семействе QorIQ скорости передачи данных до 10 Гбит/с, включает такой принципиально новый компонент как диспетчер кадров FM (Frame Manager).

В число «штатных» для DPAA аппаратных блоков ускорения обработки пакетов входят криптографический ускоритель SE (Secure Engine) и ускоритель распознавания образов PME (Pattern Matching Engine), в основе своей заимствованные из предыдущего семейства коммуникационных микроконтроллеров PowerQUICC. Для инфраструктуры DPAA обязательны диспетчеры буферов BM (Buffer Manager) и очередей QM (Queue Manager) .

Общее представление о взаимоотношении и взаимодействии компонентов архитектуры DPAA дает рисунок 2, на котором цветом выделены основные группы компонентов архитектуры. Несколько особняком стоит неокрашенная коммутационная структура высокоскоростного обмена данными и когерентности CoreNet. Она, строго говоря, не является компонентом DPAA, т.к. помимо ИКМ используется в большинстве многоядерных процессоров компании Freescale для обеспечения обмена данными между процессорными ядрами, оперативной памятью и периферией систем на кристалле с требуемой пропускной способностью при поддержке когерентности кэшей всех уровней. Однако без нее архитектура DPAA не только выглядела бы бессмысленной, но и оказалась просто неработоспособной.

Механизм диспетчеризации пакетов в DPAA существенно отличается от такого же механизма в предыдущих семействах ИКМ. Если раньше для каждого контроллера ввода-вывода, в том числе контроллеров сетевых интерфейсов, пользователь создавал две линейные очереди, по одной на ввод и вывод, и каждая очередь контролировалась простой цепочкой описателей буферов, то в DPAA диспетчеризация пакетов более диверсифицирована и гибка.

В DPAA для каждого контроллера сетевых интерфейсов может быть организовано множество приоритетных очередей на прием и передачу, причем управление очередями и буферами разделено и выполняется разными аппаратными блоками, соответственно QM и BM. Очереди не привязаны к процессорным ядрам: одно ядро может обрабатывать несколько очередей, и одна очередь может обрабатываться несколькими ядрами. Для ускорения обработки критических трафиков возможно буферирование данных непосредственно в кэше L2.

Главная отличительная черта DPAA — конвейерная обработка пакетов, причем в конвейер могут быть включены процессорное ядро или даже несколько ядер, а также аппаратные ускорители в разнообразных сочетаниях. После организации конвейера продвижение пакетов по нему выполняется аппаратурой QM и не требует оперативного вмешательства программ.

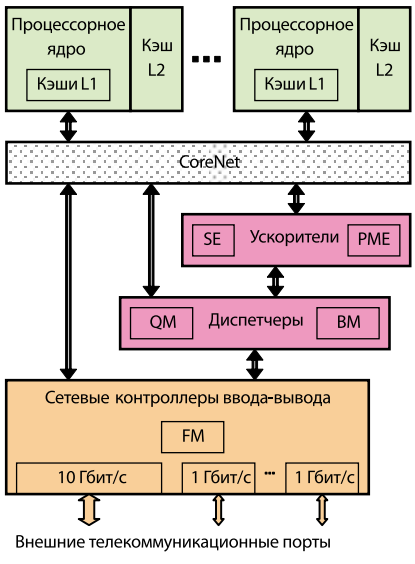


Рис. 2. **Компоненты DPAA и их взаимодействие**

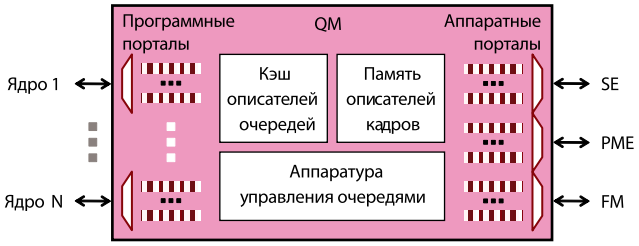


Рис. 3. **Организация QM**

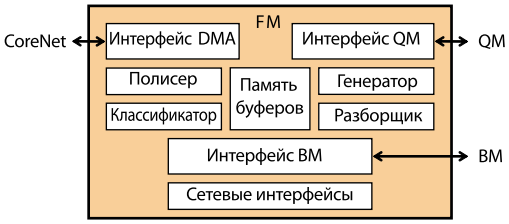


Рис. 4. **Организация FM**

Упрощенно организация аппаратного ускорителя QM показана на рисунке 3. Ускоритель оперирует с описателями кадров FD (Frame Descriptors). Каждый FD описывает некий блок данных, кадр или пакет, хранящийся в памяти в одном или нескольких буферах. В последнем случае к описателю привязана таблица сборки/разборки кадра. Основная структура нижнего уровня, поддерживаемая QM, это очередь кадров FQ (Frame Queue). Все кадры в одной очереди FQ обрабатываются одинаковым образом. Структура более высокого уровня — рабочая очередь WQ (Work Queue), которая образуется из очередей кадров. Все кадры в одной WQ имеют одинаковый приоритет. До восьми рабочих очередей разных приоритетов могут образовать канал, обеспечивающий определенный класс диспетчеризации и привязанный к тому или иному порталу. Порталы делятся на аппаратные, связанные с FM, SE или PME, и программные, соотнесенные с процессорными ядрами. Через свой портал соотнесенный с ним аппаратный ресурс может поставлять в QM кадры для постановки их на очередь и получать следующие, находящиеся во главе соответствующей очереди, кадры.

Требования качества обслуживания поддерживаются в QM приоритетами рабочих очередей и использованием в управлении ими алгоритма взвешенного случайного раннего обнаружения WRED (Weighted Random Early Detection).

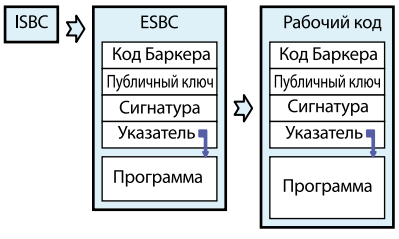


Рис. 5. **Процесс двухэтапной загрузки рабочего кода**

Ускоритель BM работает параллельно с QM и имеет аналогичные порталы. Он поддерживает до 64 пулов буферов, причем в каждом пуле должны быть собраны буферы с идентичными характеристиками. BM аппаратно назначает и освобождает буферы и следит за заполнением пулов с динамическим порогом, имеющим гистерезис.

Конвейер обработки пакетов начинается еще внутри сетевых интерфейсов, где входящие кадры и пакеты после буферирования подвергаются предварительной обработке в FM. Обработка включает разбор и анализ заголовка кадра с поддержкой сетевых протоколов L2, L3 и L4. Стандартный набор протоколов включает стек TCP/UDP/IP, но также возможно добавление пользовательских протоколов. Организация FM показана на рисунке 4.

Суммарная пропускная способность FM составляет 12 Гбит/с в обоих направлениях. Основные возможности буферирования и разбора в FM:

– различные методы буферирования с выбором буферов оптимального размера;

– двухскоростной трехцветный полисинг с маркировкой (two-rate three-color policing and marking);

– принудительное ограничение выходных потоков на сетевом интерфейсе;

– метки времени по стандарту IEEE 1588;

– сбор статистики RMON.

Ускоритель шифрования SE имеет помимо выхода в структуру CoreNet прямые интерфейсы на QM и BM, что позволяет включать SE в аппаратный конвейер прохождения кадров и пакетов по DPAA и выполнять шифрование и дешифрование пакетов «на лету», не отвлекая процессорные ядра. Ускоритель поддерживает практически все широко применяемые в телекоммуникации криптографические алгоритмы, а также выполняет ряд вспомогательных функций, таких как подсчет кодов CRC (Checksum Redundancy Code), генерацию случайных чисел и аппаратное формирование/контроль заголовков и хвостовиков пакетов широко применяемых протоколов безопасности (IPSec, 802.1ae, SSL/TLS, SRTP, 802.11i, 802.16e). Укрупненный перечень поддерживаемых в SE алгоритмов шифрования:

– алгоритмы с публичным ключом (RSA, Диффи-Хеллман, эллиптические);

– стандартные DESA и AESA (с ключом до 256 бит);

– SHA-xx (до 512 бит);

– MD5 (128 бит), HMAC;

– RC4/ARC4;

– Kasumi-F8/F9, A5/3, GEA-3;

– SNOW 3G.

Ускоритель распознавания образов PME выполняет типичные функции распознавания регулярных выражений RegEx (Regular Expressions) при суммарной пропускной способности 9,6 Гбит/с. Подобно SE, он способен встраиваться в конвейер DPAA и обрабатывать пакеты «на лету». В PME могут одновременно распознаваться до 32 K образцов длиной до 128 бит каждый. Образцы могут быть иерархически организованы в 256 наборов с 16 подмножествами в каждом. Основные особенности PME:

– быстрая компиляция и наращивание базы данных;

– использование ограниченных объемов системной памяти;

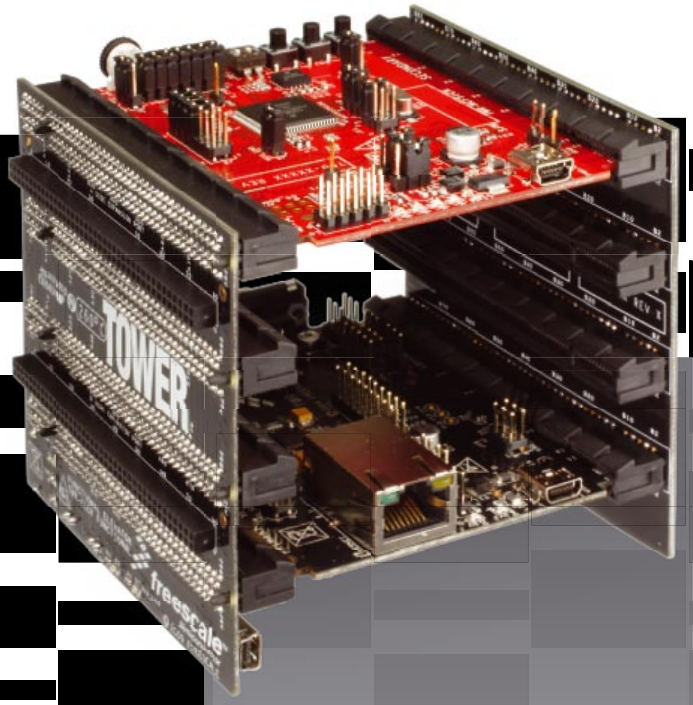
– блокировка «взрывного» размножения образцов.

В целом благодаря разумно организованному аппаратному конвейеру DPAA радикально сокращаются программные накладные расходы на обработку отдельного пакета и, соответственно, затрачиваемое на нее время. По оценкам компании Freescale, типовая обработка пакета в процессорном ядре может потребовать не более сотни инструкций. Таким образом, при рабочей частоте в 1 ГГц одно ядро способно в пределе обрабатывать до десяти миллионов пакетов в секунду. В многоядерных ИКМ эта величина кратно возрастает.

АРХИТЕКТУРА ДОВЕРИЯ

В ИКМ семейства QorIQ реализована так называемая архитектура доверия TA (Trust Architecture). Она включает уникальные средства, аппаратные и программные, обеспечения информационно безопасного функционирования систем на основе

freescale™
semiconductor



www.towersystem.ru

Присоединяйся.
Общайся.
Воплощай.

freescale@symmetron.ru

Симметрон
ГРУППА КОМПАНИЙ

Москва (495) 797-5545
moscow@symmetron.ru

Санкт-Петербург (812) 449-4000
spb@symmetron.ru

Новосибирск (383) 211-9295
sibir@symmetron.ru

Киев +38 (044) 239-2065
kiev@symmetron.ua

Харьков +38 (057) 750-8022
kharkov@symmetron.ua

Донецк +38 (062) 337-1183
donetsk@symmetron.ua

Минск +375 (17) 209-8020
minsk@symmetron.ru

таких ИКМ. Безопасное функционирование подразумевает защиту системы от различных угроз, поддержание ее целостности, конфиденциальность пользовательских данных и аутентификацию системных средств, таких как конфигурационные данные или криптографические ключи, а также защиту системного и прикладного ПО.

ТА способна решать следующие задачи обеспечения безопасности в системе:

– обнаружение неавторизованных изменений ПО или системной конфигурации и аппаратный запрет использования неавторизованно измененных компонентов;

– защиту от похищения конфиденциальных программ, установленных частных или сессионных ключей, равно как и прочих секретных данных;

– взаимную изоляцию вычислительных доменов друг от друга;

– запрет исполнения программ из областей данных.

Все средства ТА по умолчанию не активированы, и приложение, не требующее специальных мер обеспечения безопасности, может их просто игнорировать, хотя даже полномасштабное задействование таких средств в очень небольшой степени влияет на время разработки и создания информационно безопасных систем.

В ИКМ семейства QorIQ предусмотрена внутренняя, недоступная извне постоянная память, в которой хранится безопасный начальный загрузчик ISBC (Internal Secure Boot Code). Этот загрузчик предельно прост, и его основная функция заключается в удостоверении возможности следующего этапа загрузки проверкой сигнатуры внешнего пользовательского безопасного загрузчика ESBC (External Secure Boot Code). Корректность загружаемого кода удостоверяется специальной «подписью» первичного разработчика ПО с использованием алгоритма хеширования SHA 256. На рисунке 5 проиллюстрирован процесс двухэтапной загрузки рабочего кода для последующей работы в режиме безопасности.

В типичном случае в качестве первичного разработчика ПО выступает изготовитель оборудования OEM. В удостоверяемый его «подписью» загрузчик ESBC входят как собственно выполняемые программы, так и различного рода информация о конфигурации аппаратуры и ПО. «Подпись» первичного разработчика исключает возможность несанкционированной подмены внешнего загрузчика, например, заменой микросхемы полупостоянной памяти в устройстве вне ИКМ.

Внутренняя недоступная извне постоянная память обслуживается процессором прожига безопасности SFP (Security Fuse Processor), который решает в ИКМ три основные задачи:

– физически однократно пережигает определенные перемычки внутри кристалла ИКМ;

– предоставляет прожженные данные для их использования во время процедуры начальной загрузки;

– гарантированно безопасным образом доставляет установленные ключи и иную секретную информацию другим аппаратным блокам, когда система находится в рабочем режиме обеспечения безопасности.

Пользователь, желающий применить ТА, обязан соответствующим образом пережечь перемычки SFP. Для этого необходимо подать напряжение 1,5 В на определенный вывод ИКМ и сообщить SFP информацию прожига, записав требуемые параметры безопасности в его адресуемые регистры. Эти параметры могут в типичном случае включать единожды программируемый главный ключ OTPMK (One-time Programmable Master Key), хешированный публичный сверхкорневой ключ (Public Super Root Key) и пароль для диалога со средствами отладки. Записанные в SFP секретные данные уже не могут быть считаны или изменены.

В процессе работы ИКМ встроенный в него монитор безопасности (security monitor) контролирует корректность использования при шифровании ключа OTPMK и инициализируемого случайным образом ключа ключевого шифрования KEK (Key Encryption Key). Ключи OTPMK и KEK доступны исключительно в специальном режиме безопасности, который может быть включен только после правильно выполненных этапов начальной загрузки ISBC и ESBC. Для отладки пользовательских программ, предназначенных для работы в режиме безопасности, предусмотрен специальный режим аппаратной подмены OTPMK и KEK тестовыми ключами с фиксированными значениями.

В качестве компонента архитектуры безопасности может рассматриваться также встроенный в SE контролёр целостности в процессе работы RTIC (Run-time Integrity Checker), который периодически отслеживает возможные нарушения выделенной для SE системной памяти. Контроль осуществляется хешированием этой памяти на нескольких уровнях, максимально четырех, по алгоритму SHA 256. Хеш-код вырабатывается в процессе загрузки памяти. Контролёр RTIC запускается как фоновая программа специальным таймером и периодически производит проверку памяти.

В последние ИКМ семейства QorIQ помимо OTPMK был введен дополнительный обнуляемый секретный ключ ZSK (Zeroizable Secret Key) с батарейным питанием. В отличие от OTPMK, который блокируется при любых нарушениях безопасности, но вновь становится доступным после успешной начальной загрузки ESBC и при переходе системы в рабочий безопасный режим, ключ ZSK исчезает и больше никогда не восстанавливается, делая тем самым невозможным дальнейшее функционирование системы. Отдельное батарейное питание позволяет обнаруживать вторичные попытки внешнего вмешательства даже при выключенном основном питании ИКМ.

В целом ТА позволяет предотвратить любые попытки несанкционированного изменения сертифицированного безопасного ПО на всех уровнях и надежно защитить от похищения пользовательские данные, файлы, пароли, ключи шифрования и другую конфиденциальную и секретную информацию.

Кратковременная защита текущей информации, например IP-пакетов по протоколу IPSec, может осуществляться с использованием ключей KEK, при этом ключи генерируются и сохраняются в пределах SE внутри ИКМ и никоим образом не могут быть извлечены оттуда и похищены. Для защиты долговременно хранимой информации предусмотрен ключ OTPMK, однократно устанавливаемый первичным пользователем путем прожига перемычек в SFP, т.е. также внутри ИКМ и, следовательно, тоже не доступный извне. Особо секретная информация может быть защищена ключом ZSK.

Весьма существенно, что ТА делает первичного пользователя более независимым, с одной стороны, от изготовителя ИКМ, т.е. компании Freescale, а, с другой стороны, от вторичных пользователей систем OEM, построенных на основе ИКМ семейства QorIQ.

Автором уже не раз отмечались преимущества использования ИКМ в отечественных разработках аппаратуры пакетной коммутации и маршрутизации. И появление ИКМ семейства QorIQ, несомненно, дает дополнительный толчок к их использованию в России.

ЛИТЕРАТУРА

1. В. Егоров. Интегрированные коммуникационные процессоры компании Freescale Semiconductor//Электронные компоненты. №8. 2007.

2. В. Егоров. Интегрированные коммуникационные микроконтроллеры Freescale Semiconductor: из прошлого в будущее//Электронные компоненты. №7. 2008.

3. В. Егоров. Многоядерные интегрированные сетевые процессоры высокой пропускной способности//Электронные компоненты. №7. 2009.