Семейство микропроцессоров КРОЛИК, версия КМХ

Обновленная архитектура семейства КРОЛИК для микроконтроллерного применения на базе оригинального RISC ядра компании КМ211 представлена ядрами КМХ8 и КМХ32 разрядностью 8 и 32 бита соответственно и предназначена для создания малопотребляющих (обладающих минимальными размерами ядра), начального уровня производительности защищённых микросхем с повышенными требованиями к надёжности. Усовершенствованная архитектура с расширенным набором команд, а также переход на обновлённую версию компилятора GCC позволили улучшить быстродействие и энергоэффективность на 20-25%, при минимальном увеличении размера кристалла и даже сниженном потреблении на МГц.

Области применения

- Микроконтроллеры общего назначения
- Встраиваемые системы
- Смарт-карты
- Банковские карты
- SIM-карты
- Идентификация личности и паспортно-визовые документы
- Бесконтактные метки для товаров
- Модули безопасности
- Контроль доступа, транспорт
- Автомобильная электроника
- Системы управления реального времени (FreeRTOS)
- Портативные устройства
- Ультра-низкопортребляющие микросхемы

Семейство микропроцессоров КРОЛИК ориентировано на высокую эффективность Си-компилированного кода, с повышенными требованиями к стоимости микросхемы и безопасности данных. Ядра проектируются с учётом требований стабильности работы в условиях нестабильного питания, рассинхронизации тактового сигнала и иного рода воздействий. Архитектура и система команд хорошо приспособлены к особенностям языка Си, что даёт выдающуюся плотность кода при минимальных размерах ядра и низком энергопотреблении.

Ориентация на пользователя

- Гибкая система команд, расширение набора команд по требованию клиента
- Высокая степень конфигурируемости ядра
- SDK на базе Eclipse 3.7 (Indigo) and GCC 4.7.2 (доступен на www.km211.ru/ru/downloads)
- Портированные ОС: freeRTOS и др.

Гибкая система команд, собственные средства разработки и собственное RTL описание позволяют КМ211 быстро оценивать изменения в архитектуре для поддержки требований клиентов. Удобство и простота реконфигурации ядра позволяют получать хорошие результаты по энергопотреблению и площади, за счёт исключения не требующихся в конкретном проекте аппаратных ресурсов. Для создания новой версии ядра достаточно отредактировать одностраничный файл конфигурации, что позволяет быстро и без ошибок произвести синтез на основе любой библиотеки, FPGA или ASIC.

Архитектура

- Гарвардского типа, RISC
- 3-ступенчатый конвейер
- Выполнение переходов без задержек в конвейере
- Исполнение большинства команд за 1 такт
- Размер памяти данных и памяти команд до 4ГБ
- Архитектура оптимизирована под Си

Оптимизация затрат

- Малый размер ядра
- Высокая плотность кода
- Гибкое лицензирование
- Варианты изготовления:
  - ASIC
  - FPGA

Удачное сочетание 16 и 32-разрядных команд, которые идут в одном потоке, даёт высокую плотность кода. 90% команд имеют размерность 16 бит.

IP-блоки ядер KMX8 и KMX32 поставляются в виде RTL-описания или в виде топологического примитива. Модульность, простота конфигурации и хорошо комментированное RTL описание позволяет разработчикам легко адаптировать процессор к целям конкретного применения.

Пример реализации

В таблице ниже представлены результаты синтеза ядер максимальной конфигурации адресных пространств с регистровым файлом.

		KMX8	KMX32	ед.изм.
Общие характеристики	Вычислительная эффективность, тест Dhrystone		2,1	DMIPS/МГц
	Вычислительная эффективность, тест Coremark		2,1	Coremark/МГц
	Разрядность операндов	8	32	бит
	Размер кода, генерируемого из Си исходников, в сравнении с ARM Thumb-2 (100%)		97	%
90 нм, оптимизация по площади	Площадь (коэффициент заполнения 70%)	0,026	0,09	мм^2
	Размер в условных вентилях (gatecount)	10	33	тыс. вентилей
	Потребление динамическое	12	28	мкВт/МГц
	Ток потребления в статическом режиме	1,25	2,8	мкА
90 нм, оптимизация по быстродействию	Рабочая частота, не менее	100	100	МГц
	Площадь (коэффициент заполнения 70%)	0,035	0,12	мм^2
	Размер в условных вентилях (gatecount)	13	36	тыс. вентилей
	Потребление динамическое		40	мкВт/МГц
	Ток потребления в статическом режиме		5	мкА
180 нм, оптимизация по площади	Площадь (коэффициент заполнения 70%)	0,178	0,53	мм^2
	Потребление динамическое		192	мкВт/МГц
	Ток потребления в статическом режиме		15	мкА
180 нм, оптимизация по быстродействию	Рабочая частота, не менее	50	50	МГц
	Площадь (коэффициент заполнения 70%)	0,266	0,94	мм^2
	Потребление динамическое		296	мкВт/МГц
	Ток потребления в статическом режиме		33	мкА
Altera Cyclone EP4CE115	Размер ядра (логических элементов)	3000	3500	LE

Примечание. по 90 нм использовался процесс TSMC 90LP,
по 180 нм для KMX8 — МИКРОН CMOSF8; для KMX32 — МИКРОН HCMOS8D.

Производительность

- 100 МГц при 90 нм техпроцессе.
- Быстрое переключение контекста программных процессов.
- Время реакции на прерывание 1-3 периода тактовой частоты.
- Однотактное умножение 8x8/16x16/опционально32x32.
- Расширяемость сопроцессорами: MAC, крипто-ускорители, видео и др.

Ядро микропроцессора показывает высокую энергоэффективность при достаточной для многих задач производительности. Успешное применение в приложениях реального времени достигается за счёт быстрого переключения контекста программных процессов, благодаря использованию виртуальных регистровых файлов в качестве регистров общего назначения и за счёт малого времени реакции на прерывание. Имеется набор опциональных ускорителей и широкий ряд периферийных блоков: таймеры, ШИМ, CRC, контроллеры памяти FLASH, LCD, GPIO и другие.

Стабильность ядра

- Устойчивость при работе:
  - в широком диапазоне температур,
  - питающих напряжений,
  - в условиях помех.
- Корректная отработка попыток взлома.
- Отлаженный синтез из RTL.

Одной из главных целей разработки ядра было обеспечение удобства повторного использования за счёт минимизации ошибок при создании новых конфигураций ядра. Мы постарались защитить ядро от нарушения синхронизации и нестабильности шин, от сбоев и нештатных ситуаций. Специализированное дерево синхронизации сохраняет работоспособность ядра при нестабильном синхросигнале.

Защищенность ядра

- Два режима работы ядра с различными правами доступа к ресурсам (только KMX32).
- Ограничение доступа к памяти и защита исполняемого кода программ.
- Заказной ремапинг системы команд.
- Средства защиты по требованиям банковских и идентификационных смарт-карт.

Средства, обеспечивающие надёжную защиту внутренних данных, кода и аппаратных структур являются основным отличием от конкурирующих микропроцессоров. Возможность работы ядра в двух режимах: системном и пользовательском, с различными правами доступа к ресурсам, обеспечивает конфиденциальность кода и данных, что даёт дополнительную защиту от взлома. Предусмотрены биты блокировки кода системной и пользовательской областей от дампа через интерфейс отладчика. Переключение между режимами не вызывает потери производительности. Заказной ремапинг набора команд является дополнительной защитой исполняемого кода.

Возможности защиты данных

- EC-DSA (160-2048)
- RSA (512-4096)
- AES-128/256
- DES/3DES
- ГОСТ 28147-89
- ГОСТ 34.10
- ГОСТ 34.11

Для реализации функций безопасности KM211 предлагает большой набор аппаратных ускорителей с поддержкой международных и российских стандартов, что резко увеличивает производительность системы при решении подобных задач.

Смарт-карты

- Бесконтактный интерфейс ISO14443A
- Контактный интерфейс ISO7816
- Оптимизация энергопотребления для беспроводных решений

Ориентирование ядра на использование в бесконтактных смарт-картах позволило достигнуть отличных показателей потребления и защищённости. Низкая потребляемая мощность полностью удовлетворяет требованиям к питанию беспроводных устройств.

Инструменты разработки и отладки

- Мультиплатформенная (Windows-Linux) интегрированная среда разработки на основе Eclipse 3.7 (Indigo):
  - компилятор языка Си GCC 4.7.2.,
  - отладчик GDB
    - трассировщик,
    - профилировщик,
  - покомандный симулятор ядра (ISS),
  - потактовый симулятор ядра (CAS)
    - внешние блоки через LUA скрипты,
  - JTAG,
  - встроенные средства отладки,
  - FPGA платформа прототипирования,
  - тестовое окружение на VERILOG для проверки и создания новых проектов.

Набор средств разработки базируется на среде Eclipse и постоянно обновляемом компиляторе GNU GCC. Поддержана переконфигурация SDK под новые периферийные блоки и размеры встроенной памяти, подключение моделей новой периферии реализовано посредством LUA скриптов. Возможности интерфейса отладки являются опциональными, не идут вразрез с требованиями защиты и имеют ряд битов блокировки, ограничивающих при необходимости доступ через функции отладки.

Контактная информация

Головной офис и разработка:

ООО «КМ211»

Адрес: Россия
124498, г. Москва, Зеленоград,
проезд 4806, дом 5, строение 23

Email: info@km211.ru

Телефон: +7 (499) 940-03-56

Факс: +7 (499) 940-03-57

Сайт: www.km211.ru

Представитель в США:

alexey.makhalov@km211.ru

тел: +1 425 9987756

Компания КМ211 является резидентом свободной экономической зоны ОЭЗ Зеленоград (www.oez-zel.com)