Общая информация

Сопроцессор предназначен для поддержки шифрования RSA и шифрования при помощи эллиптических кривых (elliptic curve cryptography, ECC). Сопроцессор работает как ведомое устройство на шине APB и может использоваться, например, в СнК с ЦПУ архитектур ARM или RISC-V.

Функциональные особенности

- Операнды размещаются в ОЗУ;
- Поддерживаемый размер операндов - до 4098 бит включительно;
- Поддержка модулярного и не модулярного умножения;
- Поддержка модулярного и не модулярного сложения;
- Поддержка модулярного и не модулярного вычитания;
- FIFO команд для задания командных последовательностей;
- Установка адресных смещений указателей на операнды, размещаемые в ОЗУ.

Тип СФ-блока	Soft IP
Статус	Используется в проектах для массового производства
Поддерживаемые техпроцессы	Только RTL-код, поддерживается любой техпроцесс. Требуется подключение к модулю ОЗУ.
Поддерживаемые интерфейсы	AMBA APB (32 бита)
Результат логического синтеза	
Количество эквивалентных вентилей	57667
Файлы, сопровождающие СФ-блок	
Документация	Спецификация
Файлы проекта	Исходное описание на языках Verilog+VHDL
Пример проекта	Нет
Тестовый модуль	Нет
Файл ограничений	Нет
Модель	Не требуется
Программное обеспечение, работающее с СФ-блоком	
Моделирование	Любой инструмент для моделирования Verilog+VHDL (например, Cadence Incisive Enterprise Simulator)
Инструмент синтеза	Любой инструмент синтеза для RTL (например, Cadence Genus Synthesis Solution, Cadence Innovus Implementation System)
Стоимость СФ-блока и технической поддержки	
По запросу	

Информация о СФ-блоке