Общая информация

Сопроцессор симметричной криптографии предназначен для шифрования/дешифрования блоков данных по симметричным алгоритмам DES, AES, ГОСТ 28147-89. Сопроцессор работает как ведомое устройство на шине APB и может использоваться, например, в СнК с ЦПУ архитектур ARM или RISC-V.

Функциональные особенности

- Шифрование/расшифровка 64-битных блоков данных в соответствии с ГОСТ 28147-89;
- Возможность программирования значения таблицы замен для ГОСТ 28147-89;
- Работа алгоритма шифрования/расшифровки ГОСТ 28147-89 в режиме 16 или 32 шагов;
- Шифрование/расшифровка по алгоритму DES за 28 тактов системной частоты;
- Поддержка Triple DES с двойным или тройным ключом;
- Шифрование/расшифровка 128-битных блоков данных при помощи алгоритма AES;
- Поддерживаемые длины ключей для алгоритма AES – 128, 192 или 256 бит.

Информация о СФ-блоке	
Тип СФ-блока	Soft IP
Статус	Проверено на ПЛИС-прототипе
Поддерживаемые техпроцессы	Только RTL-код, поддерживается любой техпроцесс
Поддерживаемые интерфейсы	AMBA APB (32 бита)
Результат логического синтеза	
Количество эквивалентных вентилей	11597
Файлы, сопровождающие СФ-блок	
Документация	Спецификация
Файлы проекта	Исходное описание на языке 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	