Общая информация

Сопроцессор предназначен для шифрования/дешифрования блоков данных размером 128 бит по алгоритму ГОСТ Р 34.12—2015. Сопроцессор работает как ведомое устройство на шине APB и может использоваться, например, в СнК с ЦПУ архитектур ARM или RISC-V.

Функциональные особенности

- Размер блока данных – 128 бит;
- Размер ключа – 256 бит;
- Длительность операции шифрования – 1898 тактов системного тактового сигнала;
- Длительность операции расшифрования – 3499 тактов системного тактового сигнала;

Информация о СФ-блоке	
Тип СФ-блока	Soft IP
Статус	Проверен на ПЛИС-прототипе
Поддерживаемые техпроцессы	Только RTL-код, поддерживается любой техпроцесс
Поддерживаемые интерфейсы	AMBA APB (32 бита)
Результат логического синтеза	
Количество эквивалентных вентилей	7965
Файлы, сопровождающие СФ-блок	
Документация	Спецификация
Файлы проекта	Исходное описание на языке Verilog
Пример проекта	Нет
Тестовый модуль	Да
Файл ограничений	Нет
Модель	Не требуется
Программное обеспечение, работающее с СФ-блоком	
Моделирование	Любой инструмент для моделирования verilog (например, Cadence Incisive Enterprise Simulator) с поддержкой UVM
Инструмент синтеза	Любой инструмент синтеза для verilog RTL (например, Cadence Genus Synthesis Solution, Cadence Innovus Implementation System)
Стоимость СФ-блока и технической поддержки	
По запросу	