Общая информация

Физический датчик случайных чисел предназначен для формирования случайной последовательности бит, которые используются для инициализации программно криптографически стойкого генератора случайных чисел. Физический датчик случайных чисел работает от фазы шума сигнала сравнения фазы двух нестабильных RC-генераторов. Принцип формирования случайного числа основан на выборке мгновенных значений на выходе генератора варьируемой высокой частоты сигналом стабильной низкой частоты. Генератор высокой частоты подвергается случайной вариации генерируемой частоты. Блок питается от источника с напряжением 1.8В. Выходная последовательность физического датчика требует программно-аппаратной коррекции для повышения энтропии.

Функциональные особенности

- Источник питания: 1.62-1.98 В
- Технология CMOSF8 (4 слоя металлизации)
- Низкий ток потребления:
  - 249 мкА @ 25 МГц
- Температурный диапазон -40°C - 85°C
- Размеры 160 мкм x 26,2 мкм

Информация о СФ-блоке	
Тип СФ-блока	Hard IP
Статус	Проверен в кремнии
Поддерживаемые техпроцессы	CMOSF8
Поддерживаемые интерфейсы	Параллельный
Размеры	
X;Y	160,0 мкм;26,2 мкм
Файлы, сопровождающие СФ-блок	
Документация	Спецификация
Файлы проекта	gds, lef, cdl, drc.summary, lvs.report
Пример проекта	Нет
Тестовый модуль	Нет
Файл ограничений	Нет
Модель	lib, поведенческое описание Verilog
Стоимость СФ-блока и технической поддержки	
По запросу	

Впервые в России реализован и сертифицирован аппаратный физический датчик случайных чисел в составе интегральной микросхемы, предназначенной для использования в качестве средства криптографической защиты.

Физический датчик случайных чисел сертифицирован Центром защиты информации и специальной связи ФСБ России в составе интегральной микросхемы MIK51AD144D (K5016BK02H4)