FIQ-OpenAES-128e Datasheet

Overview

This datasheet refers to FIQ-OpenAES-128e, a sample RTL implementation of RAMBAM AES according to the article Redundancy AES Masking Basis for Attack Mitigation (RAMBAM), presented in this repository.

Features

- Low latency
- AES-128 encryption only
- Redundancies 8 (the original and alternative implementations) and 13 only
- Fully synthesizable

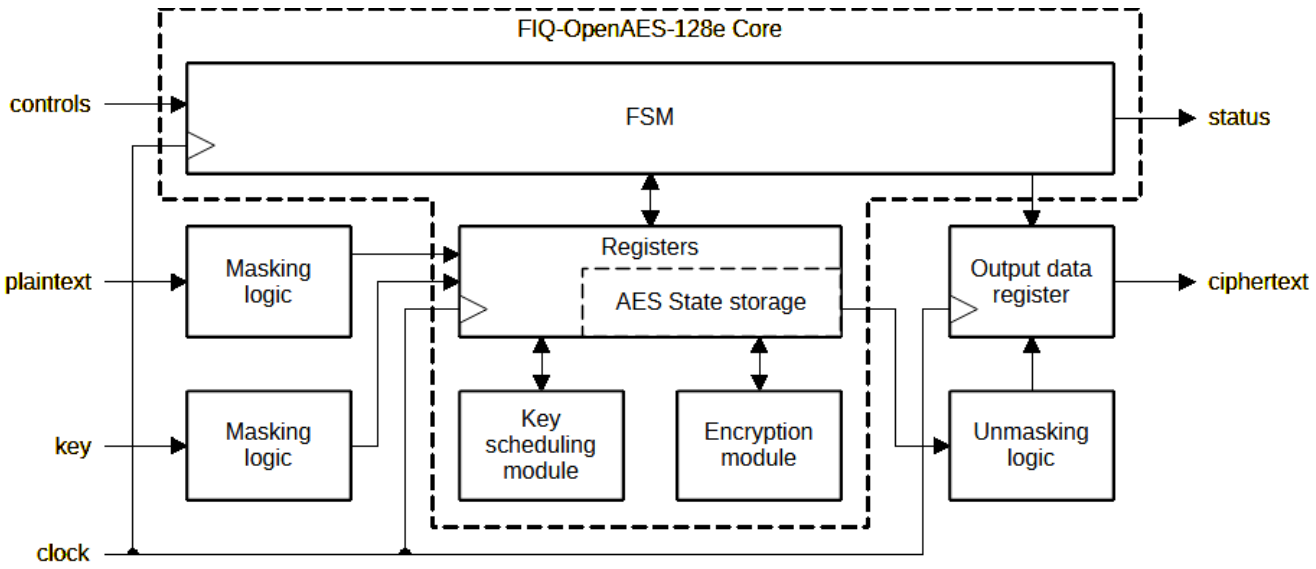

Figure 1: FIQ-OpenAES-128e High Level Block Diagram

Table 1: Document History

Issue	Date	Changes/Comments
1.0	August 13, 2023	Initial version

Contents

1 Configuration Options

FIQ-OpenAES-128e comes with limited configurable capabilities. The parameters are summarized below. The values of the parameters are immaterial, as long as they are defined.

Table 2: User-controlled Configuration

Configuration parameter	Description
REDUNDANCY_8 **REDUNDANCY_13**	There parameters define the redundancy to be used. Either REDUNDANCY_8 or REDUNDANCY_13, but not both, must be defined
NEW_LA_EN	Alternative implementation of redundancy 8 (does not matter if REDUNDANCY_13 is defined)

2 Functional Description

FIQ-OpenAES-128e implements AES-128 encryption only with a bare-core (native) interface.

FIQ-OpenAES-128e processes one cipher block at a time. A single block cipher operation takes 13 clock cycles.

3 Integration Guide

FIQ-OpenAES-128e implements only the native core interface (a hardware state machine). It needs to be connected to a state machine, implementing the flow control.

3.1 Native Interface

Table 3 provides the signal list for the native interface.

Table 3: FIQ-OpenAES-128e Native Interface Signal List

Port name	Width	Direction	Description
Synchronization and reset			
clk_i	1	input	Clock input
srst_i	1	input	Synchronous reset input
Data and control inputs			
start_i	1	input	Start pulse.
key_destruct_i	1	input	Key destruct pulse. Write 1 to erase the protected internal key and round key storage
state_i	128	input	Share 1 of the plaintext
state_share2_i	128	input	Share 2 of the plaintext
key_i	128	input	Share 1 of the key

key_share2_i	128	input	Share 2 of the key
rand_i	Configuration dependent	input	Random data input
Control and status outputs			
ready_o	1	output	Indicates that the core is ready to start a new operation and is waiting for a new command
done_o	1	output	Single-clock pulse, asserted when **state_o** receives valid data.
Data output			
state_o	128	output	Share 1 of the ciphertext
state_share2_o	128	output	Share 2 of the ciphertext

3.2 Native Interface Protocol

Figure 2 illustrates the protocol of the native interface.

A new operation is initiated by asserting the `start_i` input to the core as soon as `ready_o` is activated (at the same cycle). The input data, the key and the type of operation are indicated via the signals `state_i`, `key_i`, `encode_i` and `mode_i`. The `done_o` output is asserted for one cycle when `state_o` contains a valid result of the operation. Note that it is not necessary to wait for the `ready_o` assertion in order to read the output data. When working with shares, signals corresponding to both shares follow the same protocol.

The `rand_i` input should receive fresh random data at least at the start of each AES encryption.

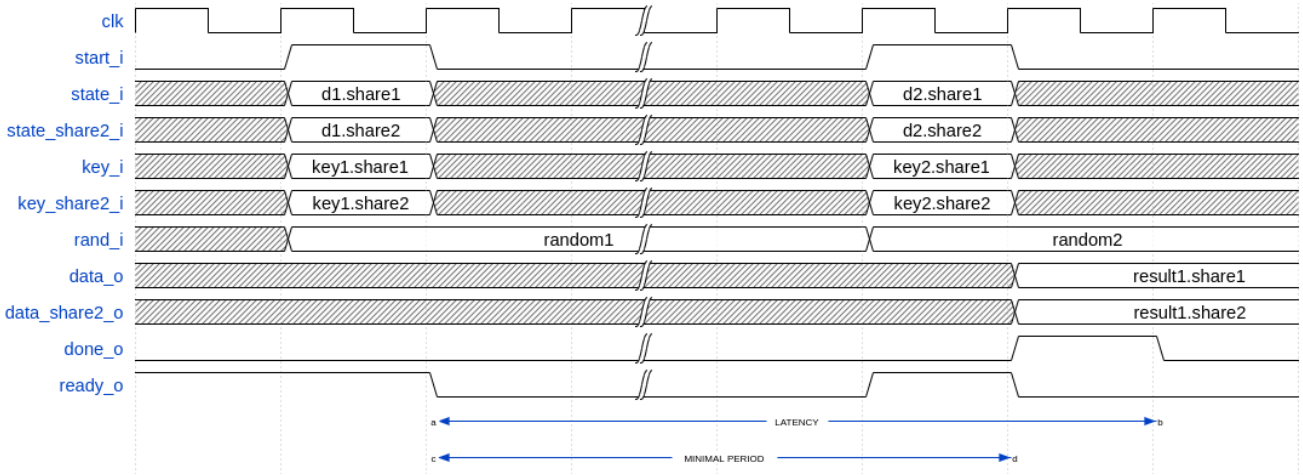

Figure 2: FIQ-OpenAES-128e Native Interface Protocol Diagram

4 Area and Performance in Numbers

Table 4 provides the numbers for area and performance for FIQ-OpenAES-128e configurations. The numbers for ASIC area (gate equivalent count) were obtained using the Yosys logical synthesis flow and the NanGate open source library for the 45nm process node.

Table 4: Area and performance for typical configurations of the AES core

Defined configuration parameters	Gate count (kGE)	Xilinx 7-series		Throughput bits/cycle
		LUT	FF	
REDUNDANCY_8	113	15600	1166	10.6
REDUNDANCY_8, NEW_LA_EN	114	15800	1173	10.6
REDUNDANCY_13	165	24400	1361	10.6