SIMON Encryption/Decryption Engine

1.0 Reference Design Datasheet

Description

For many applications the data link must be secure to protect it from unintended exposure. This operation is achieved by encrypting the data using a publicly available block cipher. However, in SWaP constrained systems it may be challenging to use most popular, industry ciphers. The SIMON Encryption Block Cipher overcomes this gap. The National Security Agency (NSA) performed the development work and defined the standard configuration for round encoding/decoding and secret key expansion.

Altera has implemented encryption/decryption engines that are compliant with NSA specifications. Customers can use these engines to implement secure links for their systems. The user can define any desired engine configuration from the NSA-defined list. These engines were implemented efficiently, preserving the algorithms' lightweight characteristics. The user can easily integrate the IP into their existing system using Altera's Qsys system integration tool or using an HDL flow.

Features

- SIMON Encryption/Decryption Block Ciphers
- Flexible Cipher Configuration Support
- Integrated Key Expansion
- Qsys Compliant
- Supported in all Altera® FPGA Families

Applications

- Digital Communication
- Industrial Control
- Military Systems

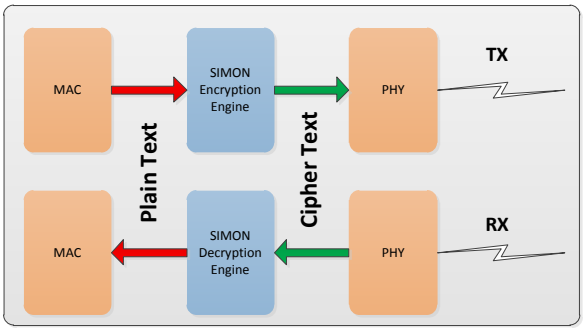

Figure 1: Encrypted Communication System

Block Size	Key Size	ALMs	Data Rate [MB/s]
32	64	64	51
48	72	80	65
48	96	95	64
64	96	105	66
64	128	122	65
96	96	130	77
96	144	153	79
128	128	177	79
128	192	205	78
128	256	237	71

Figure 2: SIMON Encryption/Decryption Engine Performance in Cyclone® V FPGA

101 Innovation Drive
San Jose, CA 95134
www.altera.com