ZUC1

Ultra-Compact 3GPP Cipher Core

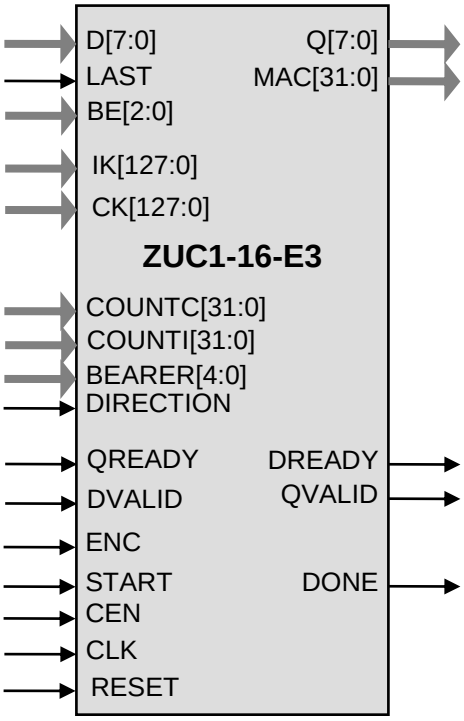
General Description

The ZUC1 core implements ZUC stream cipher in compliance with the 3GPP Confidentiality and Integrity Algorithms 128-EEA3 & 128-EIA3 version 1.6. It produces the keystream that consists of 32-bit blocks using 128-bit key and IV.

Multiple configurations of ZUC1 core are available; the number after dash indicates the throughput in bits per clock, so ZUC1-32 version is 4 times faster than ZUC1-8. Enhanced –E3 version is available that supports both EEA3 and EIA3 confidentiality and integrity algorithms. Compact ZUC1-2-E3 core is very small (12K gates).

The design is fully synchronous and available in both source and netlist form. Test bench includes the ETSI/SAGE test vectors.

Symbol



Base Core Features

Keystream generation using the ZUC Algorithm version 1.6 (ZUC-2011)

High throughput: up to 40 Gbps in 65 nm process, 10 Gbps in Altera Stratix III

Small size: from 7.5K ASIC gates

Satisfies ETSI SAGE ZUC and EAE3/EIA3 specifications

Outputs keystream in 32-bit data blocks

Uses 128-bit key and IV

Completely self-contained: does not require external memory

Available as fully functional and synthesizable Verilog, or as a netlist for popular programmable devices and ASIC libraries

Deliverables include test benches

Applications

- Secure mobile communications
- 3GPP Confidentiality and Integrity Algorithm 128-EEA3 & 128-EIA3

Pin Description

Name	Type	Description
CLK	Input	Core clock signal
RESET	Input	Core reset signal
CEN	Input	Synchronous enable signal. When LOW the core ignores all its inputs and all its outputs must be ignored.
START	Input	When goes HIGH, a cryptographic operation is started
ENC	Input	HIGH corresponds to the encryption operation, LOW to decryption. Typically fixed at either HIGH or LOW.
DREADY	Output	When HIGH, core is expecting data on the D bus
QVALID	Output	When HIGH, output data is valid on the Q bus
QREADY	Input	When HIGH, external circuitry is ready to accept data on the Q bus
DVALID	Input	When HIGH, data is valid on the D bus
DONE	Output	When HIGH, message processing completed, MAC data is valid
CK[127:0]	Input	Encryption Key
IK[127:0]	Input	Integrity Key
COUNTC[31:0]	Input	Encryption packet counter
COUNTI[31:0]	Input	Integrity packet counter
BEARER[4:0]	Input	Bearer information
DIRECTION	Input	Link direction. HIGH for uplink, LOW for downlink. Typically fixed at either HIGH or LOW.
Q[7:0]	Output	Output ciphertext or plaintext data (width depends on the configuration)
D[7:0]	Input	Input plaintext or ciphertext data (width depends on the configuration)
LAST	Input	When HIGH, indicates the last word of input data on the D bus
BE[2:0]	Input	Number of valid bits in the last word minus 1. Sampled by the core at the same time LAST is sampled HIGH (width depends on the configuration)
MAC[31:0]	Output	Calculated MAC value

Function Description

A ZUC operation produces a keystream in 32-bit data blocks as defined by ETSI/SAGE “Specification of the 3GPP Confidentiality and Integrity Algorithms 128-EEA3 & 128-EIA3. Document 2: ZUC Specification” Version: 1.6.

A EEA3/EIA3 (-E3) option includes operation per ETSI/SAGE “Specification of the 3GPP Confidentiality and Integrity Algorithms EEA3 & EIA3. Document 1: EEA3 and EIA3 Specification”. The input data shall be zero-padded to 64 bits.

Operation

A rising input on the START port triggers the beginning of a cryptographic operation, using the KEY and IV inputs to initialize the keystream. The core then starts to output the keystream per ZUC algorithm..

When all the rounds are completed, the READY signal is raised and the next unit of keystream is available on the output Q.

The core continues to produce the keystream as long as START is kept high. To throttle the output, at any time the CEN input can be brought low to pause the core.

A cryptographic operation can be aborted at any time by lowering the START signal for at least one clock cycle.

-E3 option

With the -E3 option, the core performs the encryption and authentication using the EEA3 and EIA3 algorithms. The input data shall be zero-padded to D/Q bus width. LAST input shall be asserted along with the last word of the input data. After calculating the MAC, the core will assert the DONE output and output the calculated MAC value onto the MAC[31:0] bus.

Export Permits

See the IP Cores, Inc. licensing basics page, http://ipcores.com/exportinformation.htm, for links to US government sites and more details.

Deliverables

HDL Source Licenses

- Synthesizable Verilog RTL source code
- Testbench (self-checking)
- Test vectors
- Expected results
- User Documentation

Netlist Licenses

- Post-synthesis EDIF
- Testbench (self-checking)
- Test vectors
- Expected results

Contact Information

IP Cores, Inc.
3731 Middlefield Rd.
Palo Alto, CA 94303, USA
Phone: +1 (650) 815-7996
E-mail: info@ipcores.com
www.ipcores.com