

The CLP-43 MULTI2 Flow-Through core implements the MULTI2 encryption and decryption algorithms for all key sizes via a FIFO based data interface. The algorithm is based on the ISO 9979/0009 Algorithm Register Entry and supports ECB, CBC, OFB and CFB block cipher modes of operation as specified by NIST Special Publication 800-38A.

Key Features:

- MULTI2 encryption and decryption flow-through core
- Steady state throughput is 64 bits/cycle/round
- Maximum clock frequency: 300 MHz in 90nm
 - 600 Mbps of throughput with 32 rounds
- Flow-through architecture
 - Ingress and egress FIFO depth configurable at build time
- Supports ECB, CBC, OFB, CFB modes of operation
- 20K ASIC gates

Applications:

- Set-top boxes
- Digital television sets
- Mobile handsets

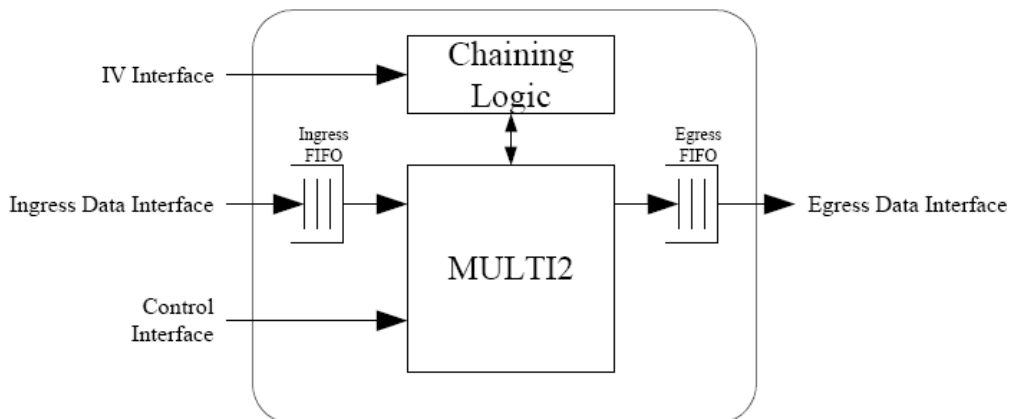


Figure 1 CLP-43 MULTI2 Flow-through core block diagram

General Description

MULTI2 is a symmetric key algorithm with variable number of rounds. It has a block size of 64 bits, and a key size of 64 bits. MULTI2 is used as the standard cipher for Communications Satellite (CS) Digital broadcasting in Japan. CS-Digital broadcasting has become very popular in Japan with a vast assortment of music and television content being offered to consumers on a pay-per-use basis. As such, the MULTI2 cipher has become a requirement for set-top boxes, mobile phones and media players targeted at the Japanese market.

The CLP-43 core implements the MULTI2 algorithm as specified in the ISO 9979/0009 Algorithm Register Entry. The algorithm can support a variable number of rounds ranging from 4 to 256 rounds in multiples of 4 rounds.

Ellipsys Middleware Toolkit

Elliptic offers a complete toolkit of symmetric and asymmetric software algorithms in Ellipsys™. Ellipsys Release 2.1 includes the Multi2 cipher and offers customers either a software alternative to the hardware core or a quick methodology to verify the hardware core. Ellipsys is available in source code formats so it can be ported to different operating systems and is rigorously verified through the NIST Cryptographic Algorithm Verification Program (CAVP). Ellipsys supports most popular ciphers and hashes including AES, DES, KASUMI and SHA as well as asymmetric operations such as RSA algorithms for sign and verify and Elliptic Curve Cryptography (ECC).

Deliverables

The CLP-43 is available in soft IP form in Verilog HDL or as a Netlist. The deliverables include:

HDL Source Licenses:

- Verilog HDL
- Testbench
- Sample synthesis script
- Documentation

Netlist Licenses:

- Post synthesis netlist
- Testbench
- Sample simulation script
- Documentation

An FPGA load can be made available under license for evaluation purposes or the core can be made available on either of the Elliptic evaluation system – the EVAL-01 or EVAL-02. For more information on pricing and a full data sheet, please contact:

© Elliptic Semiconductor, Inc.
62 Steacie Drive, Suite 201
Ottawa, ON, K2K 2A9

Phone: +1 613 254-5456
Fax: +1 613 254-7260
info@ellipticsemi.com