

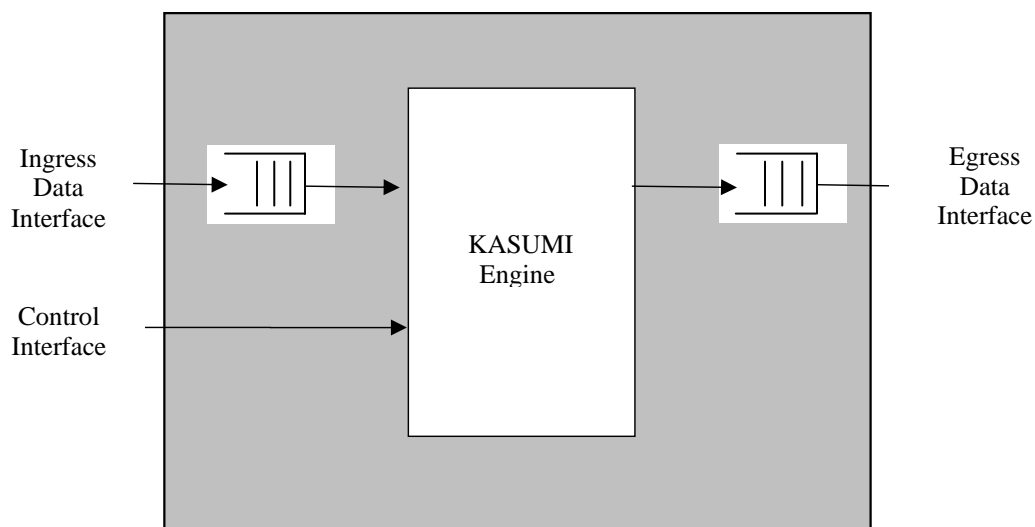
The CLP-38 core implements the KASUMI cipher. The KASUMI cipher is specified in the SAGE/ETSI document “Specification of the 3GPP TS 35.202 V7.0.0 (2007-06)”. The algorithm implements a block cipher that produces a 64-bit output from a 64-bit input using a 128-bit key. The standard requires both a confidentiality algorithm known as f8 and an integrity algorithm known as f9 - both can be implemented in the CLP-38.

### Key Features:

- KASUMI cipher for 3GPP
  - Supports both the Confidentiality (f8) and Integrity (f9) modes
- Maximum clock frequency: 226 MHz in 90nm process
  - 850 Mbps throughput
- Flow-through architecture
  - Ingress and egress FIFO depth configurable at build time
- Hardware key expansion logic
- Key size – 128 bits
- 9K ASIC gates

### Applications:

- 3GPP – GSM
- UMTS
- EDGE



**Figure 1 CLP-38 Top Level Diagram**

## Pin Description

Signal Name	Bit Width	Description
<i>Control Interface</i>		
I_key	128	Key value
I_encrypt	1	Selects between encrypt and decrypt 0 = decrypt 1 = encrypt
O_busy	1	Indicates the core is busy
I_mode	2	Selects core mode 0 = KASUMI 1 = f8 2 = f9
<i>Ingress FIFO interface</i>		
I_in_wr	1	Push the value of I_in_data into the ingress FIFO. Must not be asserted when O_in_full is asserted
I_in_data	Variable	Data to cipher
O_in_almost_empty	1	This signal is asserted one clock before O_in_empty is asserted unless I_in_wr is asserted simultaneously
O_in_empty	1	Asserted when the ingress FIFO is empty
O_in_almost_full	1	Indicates that the ingress FIFO can only accept one more write before it is full
O_in_full	1	Indicates that the ingress FIFO is full
<i>Egress FIFO interface</i>		
I_out_rd	1	Pop a value from the egress FIFO. This signal must not be asserted when O_out_empty is asserted
O_out_data	Variable	Post ciphered data output. Valid one cycle after I_out_rd is asserted
O_out_almost_empty	1	Indicates that the egress FIFO can only accept one more read before emptying
O_out_empty	1	Indicates that the egress FIFO is empty
<i>System Signals</i>		
clk	1	System clock - all signals (except rst) are synchronous to the rising edge of this signal
rst	1	Reset - assertion of this signal asynchronously resets all flip-flops to their initial state

## General Description

KASUMI is a block cipher used as the underlying crypto algorithm in the confidentiality (f8) and integrity algorithms (f9) for 3GPP mobile communications. KASUMI was designed by the Security Algorithms Group of Experts (SAGE), part of the European standards body ETSI. The designers at SAGE selected an existing algorithm, MISTY1, and changed it slightly for implementation in hardware. ETSI has also recently specified an alternative cipher for 3GPP called SNOW 3G, which Elliptic also supports.

KASUMI has a block size of 64 bits and a key size of 128 bits, and also requires support for bit-level granularity. It is a Feistel cipher with eight rounds, and it has a recursive structure, with subcomponents also having a Feistel-like form.

## Performance

The KASUMI cipher offers throughput of 3.76 bits per cycle, hence with a clock speed of 100 MHz the core can therefore encrypt or decrypt up to 376 Mbps of traffic. The core has been synthesized in 90nm processes at core clock frequencies over 200 MHz. The f8 (confidentiality) algorithm requires 1 block (64-bit) of overhead per packet while the f9 (integrity) algorithm incurs a 2 block (128-bit) overhead, which reduces the overall throughput of the core in these modes. Due to the overhead incurred, the effective throughput varies based on packet size when f8 or f9 modes are used.

The base KASUMI core has a gate count of 9K ASIC gates, while f8 and f9 add 5K additional gates. Adding a look-aside wrapper to connect to a system CPU bus adds a further 5K gates. A complete solution results in an overall gate count of 19K gates for all modes with a look-aside wrapper.

## Ellipsys Middleware

Elliptic offers a complete library of symmetric and asymmetric software algorithms in Ellipsys, including the KASUMI cipher. The next release of Ellipsys (Release 2.1) will include the SNOW 3G 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 object or source code formats, is highly portable to different operating systems and is rigorously verified through the NIST Cryptographic Algorithm Verification Program (CAVP). Ellipsys supports most popular ciphers and hashes such as AES, DES, KASUMI and SHA as well as asymmetric operations such as RSA algorithms for sign and verify as well as Elliptic Curve Cryptography (ECC).

## Deliverables

The CLP-38 is available in soft IP form, either as a Netlist or HDL Source. The deliverables available are:

### 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](mailto:info@ellipticsemi.com)