



The  
University  
Of  
Sheffield.

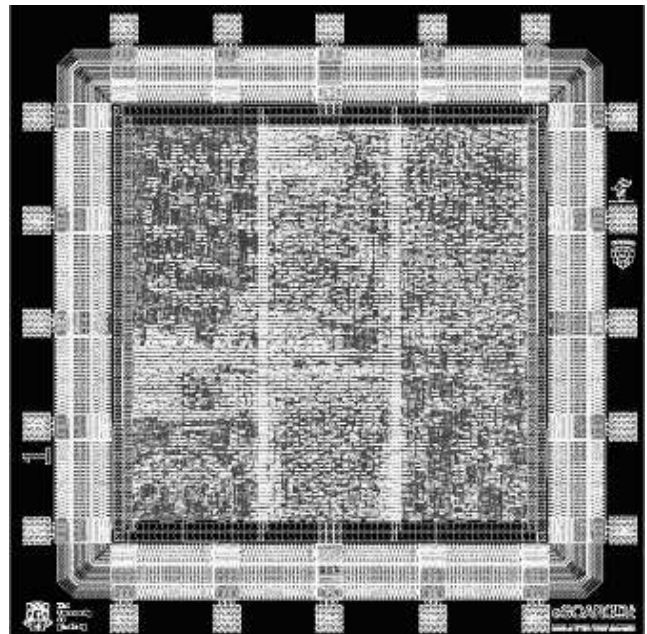
Department of  
Electrical and  
Electronic  
Engineering

# eSCARGO<sup>II</sup>

**European Stream Ciphers Are Ready (to) GO**

**0.18 $\mu$ m ASIC Datasheet (Short-form)**

- Technology: UMC 0.18 $\mu$ m CMOS  
overall chip size 1521x1521 $\mu$ m
- Package: SOIC20
- Voltage: 3.3V I/O, 1.8V core
- Synchronous Serial Interface  
with handshaking
- Four bit number to select cipher
- Phase-III hardware profile designs:  
*Moustique, Edon80, Trivium,  
Decim80/128, F-fcsr-h/16,  
Grain80/128, Mickey80/128 &  
Pomaranich80/128*
- Internally  $\times 8$  accelerated designs for  
*Trivium & Grain80.*



———— PRELIMINARY ————  
**SAMPLES EXPECTED 31 MARCH 2008**

## Pin Assignments

|                          |    |   |    |                        |
|--------------------------|----|---|----|------------------------|
| ready_for_iv ←           | 1  | o | 20 | — V <sub>IO</sub> 3.3V |
| ready_for_key ←          | 2  |   | 19 | ← keyiv                |
| cipher[0] →              | 3  |   | 18 | ← decrypt              |
| cipher [1] →             | 4  |   | 17 | ← rst                  |
| V <sub>CORE</sub> 1.8V — | 5  |   | 16 | ← clk [Schmitt]        |
| cipher [2] →             | 6  |   | 15 | — GND <sub>CORE</sub>  |
| cipher[3] →              | 7  |   | 14 | ← slew_control         |
| load →                   | 8  |   | 13 | ← drive_strength       |
| din →                    | 9  |   | 12 | → output_valid         |
| GND <sub>IO</sub> —      | 10 |   | 11 | → dout                 |

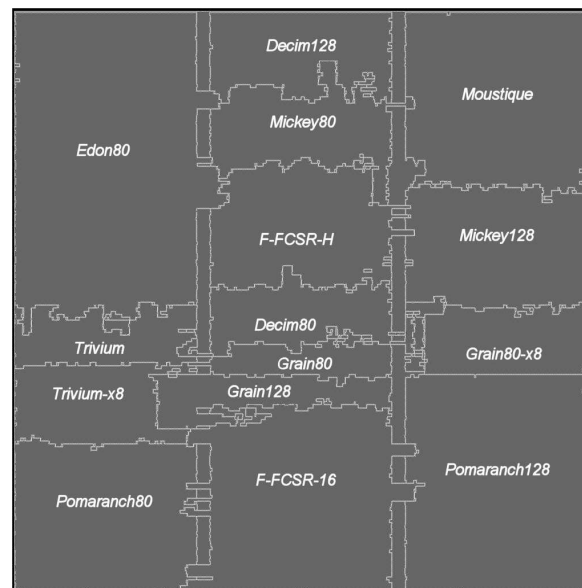
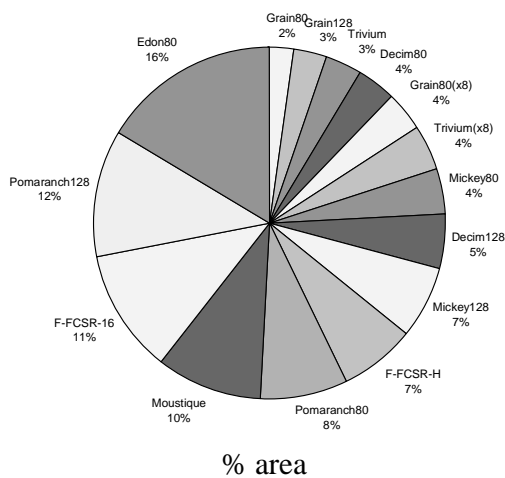
## Interface

|                       |                                       |
|-----------------------|---------------------------------------|
| <b>clk</b>            | operating clock                       |
| <b>rst</b>            | reset the current cipher              |
| <b>keyiv</b>          | synch. serial key/IV input            |
| <b>din</b>            | synch serial plain/cipher text input  |
| <b>dout</b>           | synch serial cipher/plain text output |
| <b>load</b>           | handshake input; load/ack I/O         |
| <b>ready_for_key</b>  | handshake output                      |
| <b>ready_for_iv</b>   | handshake output                      |
| <b>output_valid</b>   | handshake output                      |
| <b>decrypt</b>        | selects decrypt (Moustique only)      |
| <b>cipher[0..3]</b>   | ciphers code number (right)           |
| <b>slew_control</b>   | output driver cells (1=fast slew)     |
| <b>drive_strength</b> | output driver cells (1=max strength)  |
| <b>power</b>          | 3.3V I/O    1.8V core                 |

## Cipher code numbers

|    |                            |
|----|----------------------------|
| 0  | idle                       |
| 1  | Moustique                  |
| 2  | Edon80                     |
| 3  | Trivium                    |
| 4  | Decim80                    |
| 5  | Decim128                   |
| 6  | F-fcsr-h                   |
| 7  | F-fcsr-16                  |
| 8  | Grain80                    |
| 9  | Grain128                   |
| 10 | Mickey80 (loads IV first)  |
| 11 | Mickey128 (loads IV first) |
| 12 | Pomaranch80                |
| 13 | Pomaranch128               |
| 14 | Grain80 (×8 internally)    |
| 15 | Trivium (×8 internally)    |

## Design partitioning on chip



## Design Notes

**clk:** maximum 50MHz, input uses Schmitt triggering.

**cipher (4 bits):** internally synchronised with next clock so changes become effective on next rising edge of clock

**rst:** only affects currently selected cipher

**“idle” cipher:** a 32-bit shift register fed from key\_iv\_in and new bits loaded according to ld\_data, the output ciphertext is the result of the final bit of the SR being XORed with the plaintext. Included to permit some testing/calibration in (anyone’s) side channel test rig.

**Mickey80/128:** note that the key and IV loading process is reversed. i.e. IV is loaded before the key.

**Decim128:** uses 64-bit output buffer. Occurrence of buffer empty is improbable so the buffer refill mechanism cannot be tested. At time of this design a single tap change had been proposed and was still under consideration; accessed by setting the “decrypt” line.

**Pomaranch80/128:** Reference code to design changed 22/1/08, for designs inclusive of this change, set “decrypt” line high.

**Moustique:** dedicated decrypt input pin allows operation of self-synch decryption, if already in operation selecting this line followed by sending a ‘0’ then IV will result in decryption alternatively if decrypt selected post-reset before key loading is completed, the cipher will not ask for an IV and should proceed with ‘0’ followed by IV.

**slew\_control and drive\_strength:** set these inputs high to operate ciphers at higher I/O speeds. Frequency at which change-over required depends on capacitive loading of outputs, TBD for typical experimental setup post manufacture.

**bit ordering:** many of the test vectors for the designs are in a non-standard order. For some the bit ordering for the key, IV and keystream within the ciphers operating word has not been fully defined. The following table reflects this designers understanding and the ordering expected by this implementation.

| <i>cipher</i> | <i>key/iv</i>                 | <i>keystream</i>             |
|---------------|-------------------------------|------------------------------|
| Moustique     | normal                        | normal                       |
| Trivium       | quad byte swapped             | quadbyte swapped             |
| Pomaranch     | normal (but 18bit hex values) | normal                       |
| Mickey        | normal                        | normal                       |
| Grain         | bits in 8-bit bytes reversed  | bits in 8-bit bytes reversed |
| F-fcsr-h      | bytes reversed                | normal                       |
| F-fcsr-16     | bits in 16-bit words reversed | byte pairs swapped           |
| Edon80        | normal                        | normal                       |
| Decim         | bits reversed                 | bits reversed                |

## Further Information

T Good or M Benaissa, Department of Electronic and Electrical Engineering,  
University of Sheffield, Mappin Building, Mappin Street, Sheffield S1 3JD, U.K.  
{t.good, m.benaissa} @ sheffield.ac.uk