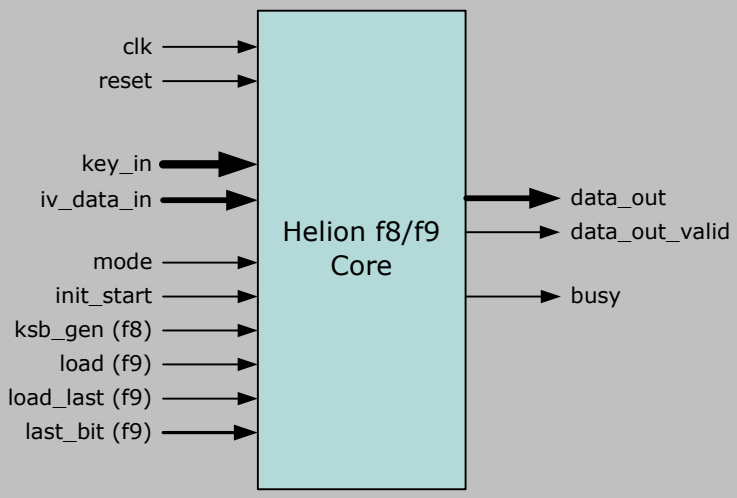
Helion Technology

DATASHEET – 3GPP KASUMI f8 and f9 cores for ASIC



Features

- Implement 3GPP f8 confidentiality and f9 integrity to 3GPP TS 35.201
- Both cores support KASUMI ECB mode encryption to 3GPP TS 35.202
- f8 core fully supports GSM A5/3 and GPRS GEA3 encryption algorithms
- f8 core generates 64-bit wide keystream output data
- f9 core performs bit padding of last block and outputs 32-bit MAC-I
- Area from only 7k ASIC gates for f8 and f9 cores
- Both cores capable of throughputs over 1 Gbps in 0.13um process
- Simple external interface

Deliverables

- Fully synthesisable Verilog RTL code
- Simulation model and testbench with 3GPP TS 35.204 test vectors
- Comprehensive user documentation

Overview

The Helion 3GPP KASUMI cores perform the f8 confidentiality and f9 integrity algorithms required to provide data security within the GSM/EDGE and UMTS mobile communication standards. Both algorithms are based on the KASUMI 64-bit block cipher which uses a 128-bit key. The KASUMI algorithm was designed by the Security Algorithms Group of Experts (SAGE) within ETSI, and is an optimised version of the MISTY1 block cipher originally developed by Mitsubushi Electric Corporation of Japan. Within ETSI, the f8 and f9 algorithms are now known as UEA1 and UIA1 respectively.

The cores are ideally suited to accelerating the f8 and f9 security algorithms within SOC based GERAN and UTRAN implementations to efficiently provide 3GPP confidentiality and integrity at very high data throughputs. The f8 confidentiality core can also be used to perform the A5/3 encryption algorithm used for GSM and the GEA3 encryption algorithm used in GPRS.

Helion Technology Limited
Ash House, Breckenwood Road,
Fulbourn, Cambridge CB21 5DQ, England

Functional Description

The Helion 3GPP f8 core performs the stream cipher that generates the keystream required to implement the f8 (UEA1) confidentiality algorithm. The core must firstly be initialised by the user readying the 64-bit initial value (Count, Bearer and Direction) on the *iv_data_in* input, and the 128-bit key on the *key_in* input, before asserting the *init_start* input. Once initialisation is complete (as indicated by the *busy* output) the core may be used to generate successive keystream blocks by asserting the *ksb_gen* input. The availability of a valid keystream block on *data_out* is indicated by the assertion of *data_out_valid*.

The Helion 3GPP f9 core performs the Message Authentication Code (MAC) calculation required to implement the f9 (UIA1) integrity algorithm. When the 128-bit key input is valid, the core may be started by asserting the *init_start* input. The user application then inputs consecutive message data blocks for authentication using the *load* and *iv_data_in* inputs. At the end of the message data, coincident with the final *load*, the user indicates the presence of the last message block by asserting the *load_last* input and indicating the position of the last message bit on the *last_bit* input. The core then applies padding to the last block and completes computation of the final 32-bit MAC value. The MAC value is available on *data_out* when *data_out_valid* is asserted by the core.

Alternatively, using the *mode* input, both cores also support KASUMI ECB mode encryption.

Logic Utilisation and Performance

The table below illustrates the relationship between the ASIC gate count and the clock frequency constraint used for synthesis using a standard foundry 0.13um library. The gate count figures will vary with synthesis tool, synthesis settings, and target technology library, so these figures are intended for illustrative purposes only.

	f8 confidentiality			**f9 integrity**		
technology	ASIC 0.13um	ASIC 0.13um	ASIC 0.13um	ASIC 0.13um	ASIC 0.13um	ASIC 0.13um
Gate count	6916	7127	9115	7127	7743	9431
constraint	50 MHz	100 MHz	250 MHz	50 MHz	100 MHz	250 MHz
throughput	188 Mbps	376 Mbps	940 Mbps	188 Mbps	376 Mbps	940 Mbps

About Helion

Helion is a well established British company based in Cambridge, England, offering a range of product-proven Data Security silicon IP cores backed up by our highly experienced and professional design service capabilities.

Unlike many IP core vendors, Helion also spends a great deal of effort designing its cores at the very lowest level. We strongly believe that if you are buying IP, it should have been designed with the ultimate in care, and crafted to achieve the desired performance; not just put together at a high level to get the job done quickly. We find that this approach pushes the results much closer to the intended performance envelope. The value of this approach can be clearly appreciated by direct comparison with solutions offered by the more broadline IP vendors.

More Information

For more detailed information on this or any of our other products and services, please contact Helion and we will be pleased to discuss how we can assist with your individual requirements.

Helion Technology Limited
Ash House, Breckenwood Road,
Fulbourn, Cambridge CB21 5DQ, England

tel: +44 (0)1223 500 924 email: info@heliontech.com
fax: +44 (0)1223 500 923 web: www.heliontech.com