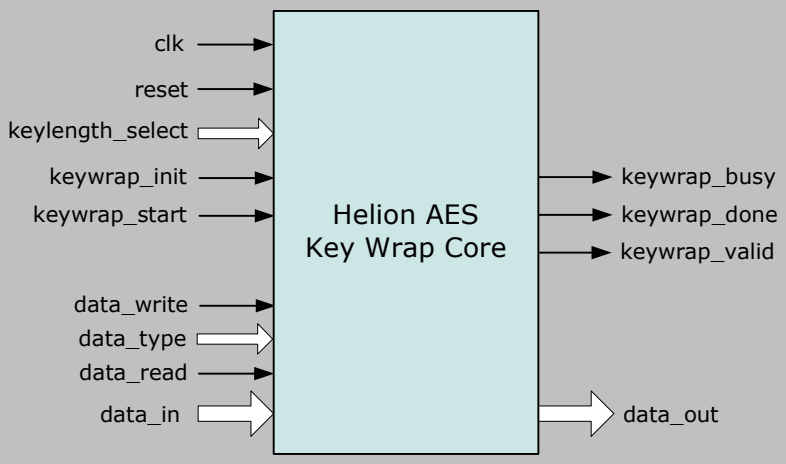
Helion Technology

FULL DATASHEET – ANS X9.102 AES Key Wrap Core for Altera FPGA



Features

- Implements NIST AES Key Wrap Specification and AESKW mode of ANS X9.102
- Supports 128-bit, 192-bit and 256-bit Key Encryption Key (KEK)
- Supports key data lengths up to 3,776 bits (59 blocks)
- Available in separate Key Wrap and Key Unwrap versions
- Available in 128-bit only KEK versions for reduced resource usage
- Suitable for protecting cryptographic key material within untrusted environments
- Optimised for use in Altera FPGA
- Simple external interface

Deliverables

- Target specific netlist or fully synthesisable RTL VHDL
- VHDL/Verilog simulation model and testbench
- User documentation

Overview

The Helion AES Key Wrap Core for Altera FPGA implements the AES Key Wrap or Unwrap algorithm as described in the original NIST AES Key Wrap Specification, and fully supports the AESKW mode proposed in ANS X9.102. It is ideally suited for protecting cryptographic keys within applications where the key material must either be transmitted over insecure communication channels, or stored within untrusted environments where required by the Key Management scheme.

As the name suggests, the AES Key Wrap algorithm uses the Advanced Encryption Standard (AES) to provide confidentiality and integrity checking for plaintext keys and other associated plaintext data (collectively known as the key data) which require protection. In the case of ANS X9.102 AESKW mode, the additional plaintext data may optionally contain a cleartext header of up to 256 bytes.

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

Functional Description

The Helion AES Key Wrap and Key Unwrap cores share a very simple interface which allows the user to write the Key, Initial Value (A0) and Key Data into them using the 8-bit write port, start a key wrap/unwrap operation, and upon its completion, to read the wrapped/unwrapped data from the 8-bit read port.

Before starting each key wrap/unwrap operation, the user must first initialise the core by pulsing *keywrap_init* high. The user may then write the Key Encryption Key (KEK), Initial Value and Key Data to the core by asserting *data_write* when *data_in* contains valid data whilst indicating the type of data (KEK, IV or Key Data) on the *data_type* input.

The user may then start the core by asserting *keywrap_start* high, at which point the core asserts the *keywrap_busy* output to indicate that operation is in progress. When the operation is complete the core de-asserts the *keywrap_busy* output and pulses high the *keywrap_done* output. In the case of an unwrap operation, the core will also show the status of the key data integrity check on the *keywrap_valid* output. A high level indicates the authentication check has passed and the key data is valid.

At this point the user may read the wrapped key data from the core by asserting the *data_read* input. The core has a pipelined read interface, and so outputs the data on the *data_out* port in the subsequent clock cycle. Once all data has been read from the core the user may initiate further key wrap or unwrap operations.

Logic Utilisation and Performance

Helion has a long history in high-end FPGA design, and we therefore take our FPGA implementations very seriously indeed. Our cores have been designed from the ground up to be highly optimal in Altera FPGA technology - they are not simply based on a synthesised generic ASIC design.

Both the Helion Key Wrap and Key Unwrap cores have been specifically designed to be highly optimal in Altera designs to yield high functionality for the logic resources used. The table below shows typical resource usage and performance for the version of each core which supports all three AES key sizes (128, 192 and 256 bits). For applications where support for the 128-bit key size only is required, a lower resource version of each core is also available. Please contact Helion for further details.

	AES Key Wrap			**AES Key Unwrap**		
technology	CycloneII C6	CycloneIII C6	StratixII C3	CycloneII C6	CycloneIII C6	StratixII C3
logic resource	675 LEs 3 M4Ks	693 LEs 3 M9Ks	383 ALMs 3 M4Ks	786 LEs 3 M4Ks	788 LEs 3 M9Ks	411 ALMs 3 M4Ks
max clock	161 MHz	170 MHz	267 MHz	158 MHz	153 MHz	250 MHz
latency (128 bit key data 128-bit KEK)	47.0 us	44.4 us	28.3 us	47.9 us	49.4 us	30.3 us

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