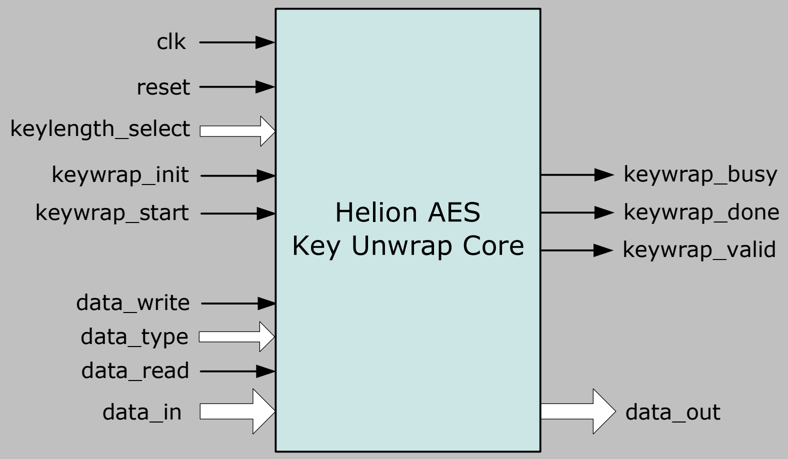
Helion Technology

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



Features

- Implements NIST AES Key Unwrap algorithm and AESKW mode of ANS X9.102
- Available in Tiny and Standard versions
- Supports 128-bit, 192-bit and 256-bit Key Encryption Key (KEK)
- Lower resource 128-bit only KEK version also available
- Supports key data lengths up to 16,064 bits (251 blocks)
- Suitable for protecting cryptographic key material within untrusted environments
- Highly optimised for use in each FPGA technology
- 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 Unwrap Core implements the AES Key Unwrap algorithm as described in the 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 if required by the Key Management scheme.

As the name suggests, the AES Key Unwrap 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 Unwrap core has a very simple interface which allows the user to write the Key, Initial Value (A0) and Key Data using the write port, start a key wrap/unwrap operation, and upon its completion, to read the unwrapped data from the read port. The ports are 8 bits wide for the Tiny version and 32 bits wide for the Standard version.

Before starting each key 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 the key unwrap operation is in progress. When the operation is complete the core de-asserts the *keywrap_busy* output and pulses high the *keywrap_done* output. 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 that the unwrapped key data is valid.

At this point the user may read the unwrapped 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 unwrap operations.

Logic Utilisation and Performance

Helion has a long history in high-end FPGA design, and we therefore take great care when implementing our IP cores. As a result they have been designed from the ground up to be highly optimal for each individual FPGA technology - they are not simply based on a synthesised generic RTL ASIC design. The Helion AES Key Unwrap core makes use of the architectural features available in each FPGA technology to achieve the highest performance combined with the most efficient logic resource utilisation.

The latest logic area, performance figures, and datasheets for the Helion AES Key Unwrap core in a range of different technologies are available at http://www.heliontech.com/aes_keywrap.htm. Please feel free to contact us should you require further details.

About Helion

Helion is a long 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. Although we specialise in providing the highest performance data encryption and authentication IP, our interest does not stop there. Unlike broadline IP vendors who try to supply a very diverse range of solutions, being specialists we can offer much more than just the IP core itself.

For instance, we are pleased to be able to supply up-front expert advice on any security applications which might take advantage of our technology. Many of our customers are adding data security into their existing systems for the first time, and are looking for a little assistance with how best to achieve this. We are pleased to help with suitable advice and support where necessary, and pride ourselves in our highly personal approach.

The quality of our IP is however the main reason our customers keep coming back for more. We passionately believe that if you are buying IP, it should have been designed with the ultimate in care, crafted to achieve the ultimate performance in each target technology, and thoroughly tested to ensure compliance with any associated standards. All this comes as standard with IP from Helion.

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