Helion Technology

FULL DATASHEET – Modular Exponentiation Core Family for FPGA

Helion ModExp Core

Inputs: start_processing, operand_length, operand_data, operand_write, operand_read, operand_select, operand_index, reset, clk

Outputs: engine_busy, engine_done, engine_status
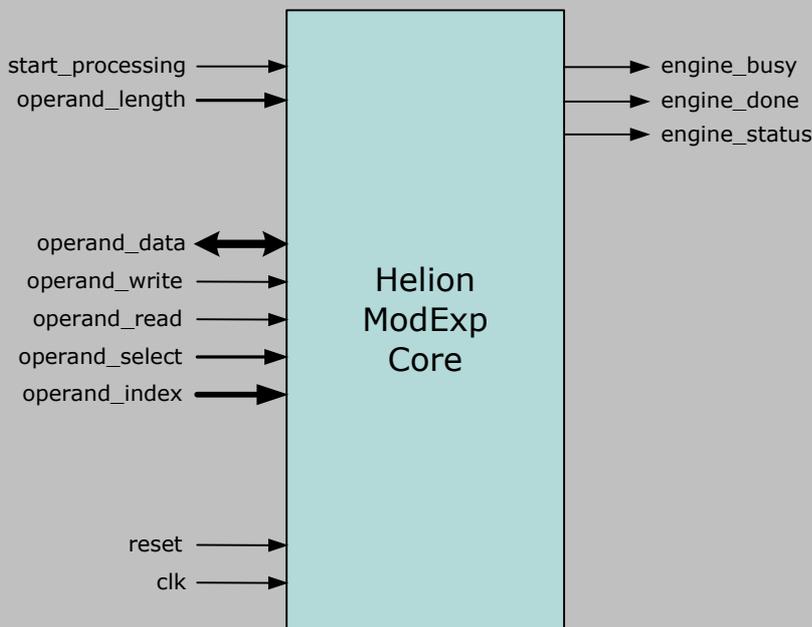
Features

- Implements the $Z = Y^E \bmod M$ Modular Exponentiation function commonly used in Public-Key Cryptography
- Ideal for hardware acceleration of RSA, Diffie-Hellman and DSA
- Supports 192, 256, 384, 512, 768, 1024, 1536 and 2048-bit operands
- Efficiently supports short exponent lengths at higher performance e.g. 180-bit for Diffie-Hellman
- Simple 32-bit RAM interface
- Available in a choice of versions allowing user to trade-off area and performance for optimal solution
- Highly optimised for use in each FPGA technology

Deliverables

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

Overview

The Helion Modular Exponentiation core performs the $Z = Y^E \bmod M$ computation which is at the heart of many commonly used Public-Key encryption schemes such as RSA, Diffie-Hellman and the Digital Signature Algorithm (DSA) described in FIPS 186-2. These algorithms provide the strong encyption to facilitate key exchange and certificate-based authentication for communication protocols such as TLS/SSL and IPsec which are widely used for securing transactions over open networks such as the Internet.

Modular Exponentiation is an extremely CPU intensive computation which can present a significant overhead for embedded systems which implement these Public-Key algorithms in software. The Helion ModExp core has been designed to be highly efficient in each different FPGA technology, and to provide an easy to use and resource efficient means to perform hardware acceleration for applications which require a cryptographic key exchange.

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

Functional Description

The Helion ModExp Core consists of a shared Operand RAM which provides the data interface and holds the computation operands (Y,E,M) and result (Z); a Modular Multiplier which provides the main datapath and performs the computation; and a Controller block which provides the control interface as well as overseeing the operation of the Multiplier, enabling it to perform the required exponentiation operations. Using a shared Operand RAM interface makes the Helion ModExp core ideal for use as a co-processor, but equally usable in other configurations.

Operation of the core is extremely simple. Whilst the core is idle (indicated by the core busy output being deasserted), full user access is available to the shared Operand RAM via ports on the core. The Y, E and M operands are first written to the Operand RAM by the user application. Note that if the M or E operand values do not change between operations, they need not be updated as they remain in the shared Operand RAM. The operand length is then selected and the computation started. Progress of the computation is indicated by the busy and done status outputs from the engine; busy will be asserted during the computation, and done will be asserted for a single clock cycle once the computation is complete. This indicates that the core is idle again, and the resulting Z value may be read from the Operand RAM.

The Helion ModExp core may optionally be supplied as a hardwired version supporting Diffie-Hellman Oakley Groups 1, 2, 14 or 15 for use with the Internet Key Exchange (IKE). This removes the need for the user to set up the Modulus value, and in some variants of the core it can reduce the required logic resources.

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 Modular Exponentiation cores make 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 Modular Exponentiation core family in a range of different technologies are available at http://www.heliontech.com/modexp.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