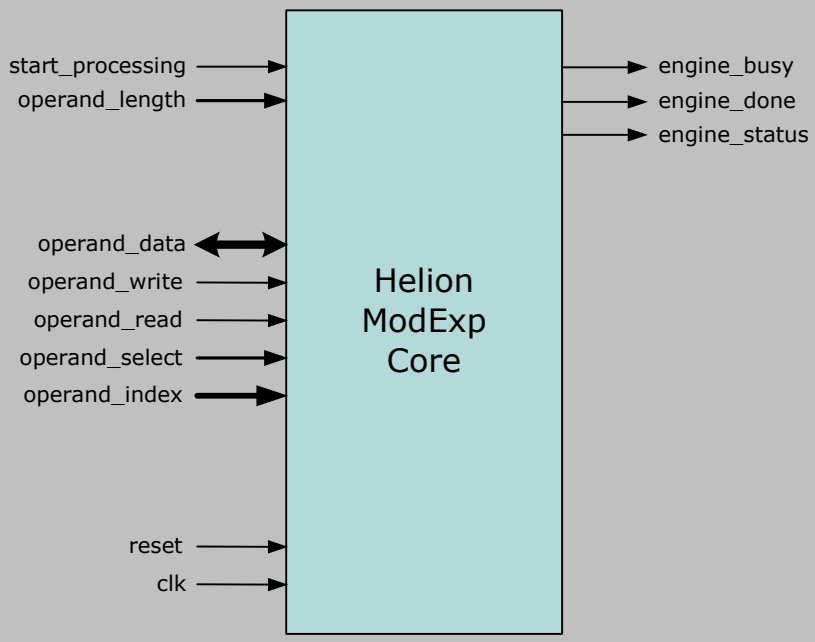
Helion Technology

FULL DATASHEET – Modular Exponentiation Core Family for Altera FPGA



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 Altera FPGA

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 encryption 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 Altera FPGA, 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. Please contact Helion for further details if this option is of interest.

Core versions

The Helion Modular Exponentiation core is a highly scaleable design, and so is available in a choice of versions, each sharing an identical interface, but differing in terms of the number of clock cycles they take to perform each operation. This allows the user to size an appropriate solution for any given requirement, trading off performance and logic area.

The tables below show the logic utilisation and maximum clock rates for four of our most popular variants. The smallest core is called **TINY32**, and typically offers between 1 and 5 1024-bit RSA operations per second (when both E and M are 1024-bits in length) depending on your choice of Altera target technology. It is therefore a good choice for setting up a small number of secure links in a typical terminal unit application.

For higher performance requirements, the **STD64** version covers the range 5 to 15 operations per second, the **STD128** version covers the range 10 to 25 operations per second, and the **STD256** version covers the range 15 to 50 operations per second; again the exact figure depending on the maximum attainable clock speed in your choice of Altera technology.

Important Note: all these quoted operation rates are for full-size 1024-bit RSA (|E|=1024, |M|=1024). Operations with shorter exponents like those typically used for Diffie-Hellman or for public key encryptions will be much faster in any given implementation, and if evaluating different solutions it is important to ensure that comparisons are made under identical conditions. For accurate performance figures for any of these solutions in any target technology, please contact Helion and we will be very happy to discuss all the options in detail.

Logic Utilisation and Performance

	ModExp TINY32			
technology	Cyclone III C6	Cyclone IV C6	Arria II GX C4	Stratix IV C2
logic resource	689 LEs 4 M9K	688 LEs 4 M9K	411 ALMs 2 M9K	417 ALMs 2 M9K
max clock	98 MHz	101 MHz	212 MHz	250 MHz
RSA ops/second |E|=1024, |M|=1024	1.9	1.9	4.1	4.9
DH ops/second |E|=180, |M|=1024	11.0	11.4	23.9	28.2

The figures above cover the smallest solution in the Helion ModExp core range, with the three faster versions featured on the next page. Please note that full support is available for all versions of the ModExp core in all Altera device families – full details are available from Helion on request.

Logic Utilisation and Performance (continued)

	—ModExp STD64—		—ModExp STD128—		—ModExp STD256—	
technology	Arria II GX C4	Stratix IV C2	Arria II GX C4	Stratix IV C2	Arria II GX C4	Stratix IV C2
logic resource	782 ALMs 2 M9K	767 ALMs 2 M9K	1282 ALMs 2 M9K	1314 ALMs 2 M9K	2228 ALMs 2 M9K	2254 ALMs 2 M9K
max clock	289 MHz	366 MHz	285 MHz	352 MHz	275 MHz	335 MHz
RSA ops/second |E|=1024, |M|=1024	11.3	14.4	22.3	27.6	42.6	51.9
DH ops/second |E|=180, |M|=1024	65.1	82.4	127.7	157.8	243.9	297.1

About Helion

Founded in 1992, Helion is a well established British company based in Cambridge, England, offering a range of product-proven Data Security IP cores backed up by 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.

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.

In addition, our Design Services team have an impressive track record in the development of real security products for our customers; we are proud to have been involved in the design of numerous highly acclaimed security products. This knowledge and experience is fed back into our IP cores, to ensure that they are easy to integrate into real systems, and perform appropriately for real engineering applications.

Helion has a very long history in working with high performance FPGAs, so we take our Altera implementations very seriously indeed. Our cores have been designed from the ground up to be highly optimal in Altera FPGA; they are not simply based on a generic ASIC design like much of the competition.

Most Helion IP cores make use of Altera-specific architectural features; in fact in many cases we build-up custom internal logic structures by hand, in order to achieve the very highest performance and most efficient logic resource utilisation. The benefits of this dedicated approach can be clearly demonstrated by direct comparison between Helion Data Security IP cores and the equivalents from other 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