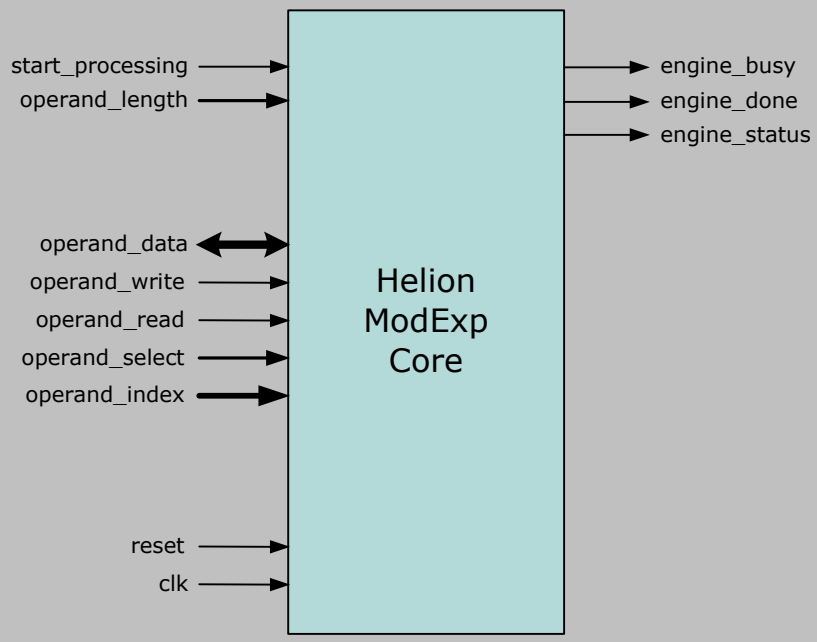
Helion Technology

PRODUCT BRIEF | **Modular Exponentiation Core Family for ASIC**



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, ElGamal or DSA
- Supports 192, 256, 384, 512, 768, 1024, 1536, 2048, 3072, 4096, 6144 and 8192-bit operands (configurable)
- Short exponents efficiently computed e.g. 180-bit for Diffie-Hellman
- Optional constant time operation to help protect against timing attacks
- Simple 32-bit RAM interface
- Choice of variants providing optimal area/performance trade-off
- Optimised for use in ASIC

Deliverables

- Fully synthesisable RTL source code
- VHDL/Verilog testbench with test vectors
- 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, ElGamal, 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 when these Public-Key algorithms are implemented in software. The Helion ModExp core has been designed to be highly efficient in ASIC, 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 *engine_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 *engine_busy* and *engine_done* status outputs from the core; 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 for use with the Internet Key Exchange (IKE), removing the need for the user to set up the Modulus value. A constant execution time option is also available to help protect against timing attacks. Please contact Helion for further details if this option is of interest.

Core versions

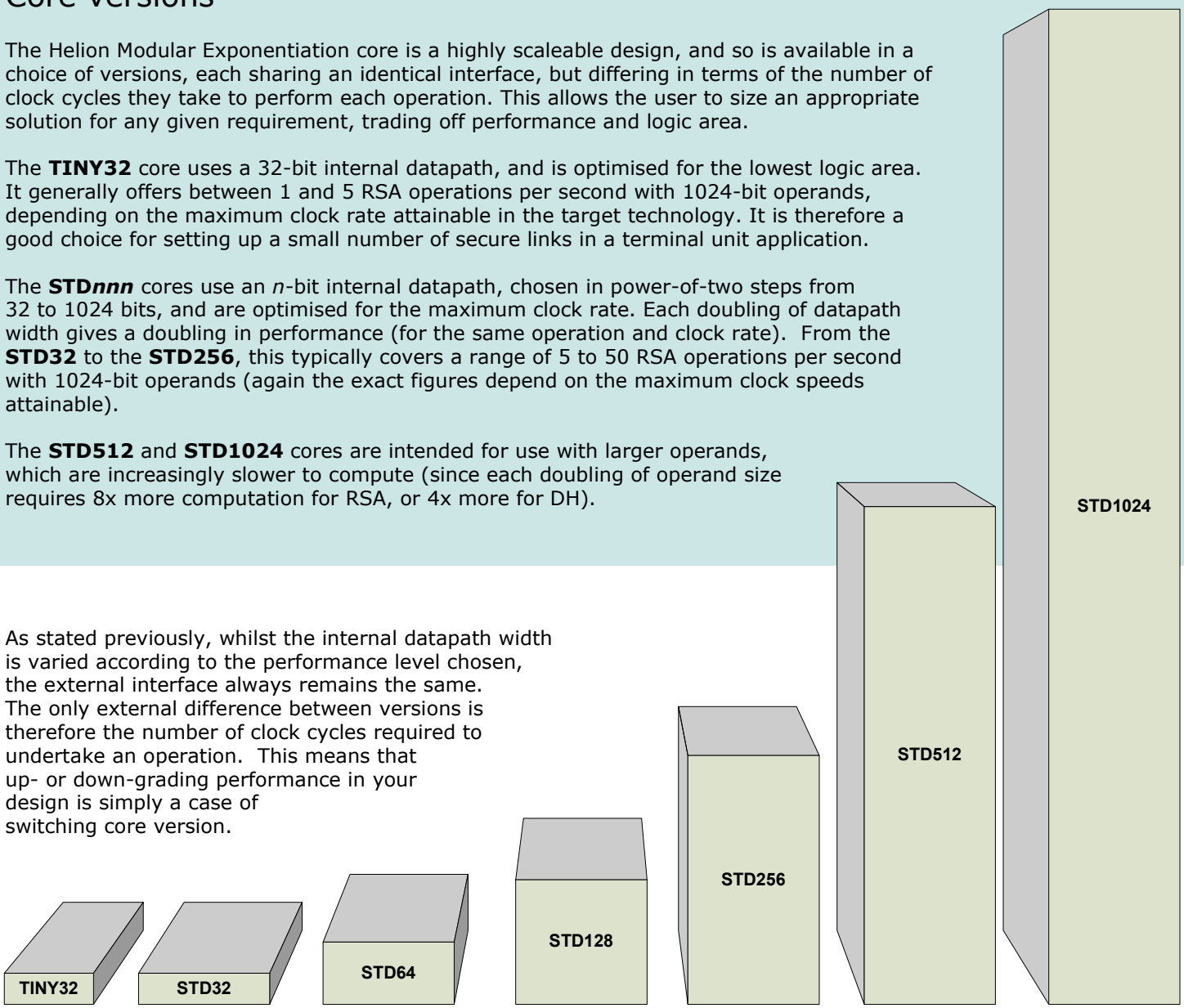
The Helion Modular Exponentiation core is a highly scaleable design, and so is available in a choice of versions, each sharing an identical interface, but differing in terms of the number of clock cycles they take to perform each operation. This allows the user to size an appropriate solution for any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

The **TINY32** core uses a 32-bit internal datapath, and is optimised for the lowest logic area. It generally offers between 1 and 5 RSA operations per second with 1024-bit operands, depending on the maximum clock rate attainable in the target technology. It is therefore a good choice for setting up a small number of secure links in a terminal unit application.

The **STD*nnn*** cores use an *n*-bit internal datapath, chosen in power-of-two steps from 32 to 1024 bits, and are optimised for the maximum clock rate. Each doubling of datapath width gives a doubling in performance (for the same operation and clock rate). From the **STD32** to the **STD256**, this typically covers a range of 5 to 50 RSA operations per second with 1024-bit operands (again the exact figures depend on the maximum clock speeds attainable).

The **STD512** and **STD1024** cores are intended for use with larger operands, which are increasingly slower to compute (since each doubling of operand size requires 8x more computation for RSA, or 4x more for DH).

As stated previously, whilst the internal datapath width is varied according to the performance level chosen, the external interface always remains the same. The only external difference between versions is therefore the number of clock cycles required to undertake an operation. This means that up- or down-grading performance in your design is simply a case of switching core version.



Core Performance

	Core Clock = 200MHz	
	RSA ops/second |E|=1024, |M|=1024	DH ops/second |E|=180, |M|=1024
TINY32	3.9	22.6
STD32	3.9	22.6
STD64	7.8	45.0
STD128	15.6	89.2
STD256	31.0	178.5
STD512	7.7 (2K Operands)	89.2
STD1024	1.9 (4K Operands)	44.4

This table shows the numbers of operations per second that each of the core versions will support at a nominal clock frequency of 200MHz. Achievable core performance can be easily determined for any other clock frequency by simple up or down scaling.

For a particular application, a core version should be chosen that will support the required performance, with an appropriate and practical core clock frequency.

Remember that usable clock frequencies will depend on the exact ASIC process being used. Please see below for guidance on this.

Logic Utilisation and Performance

The table below shows typical gatecounts and maximum clock rates for popular configurations of the Helion ModExp core.

	Helion ModExp core			
version	**TINY32**	**STD64**	**STD128**	**STD256**
typical gatecount	<8k gates +RAM	<12k gates + RAM	<20k gates + RAM	<40k gates + RAM
typical max clock rate (65nm)	400MHz	400MHz	400MHz	400MHz

Note that exact figures will depend significantly on the target library used, as well as the synthesis method and options, so these numbers should be treated as preliminary guidance only.

All versions of the Helion ModExp core require user compiled RAMs and/or register files of varying aspect ratios in order to store the operands and for use as internal workspace. The total number of RAM storage bits required and the respective RAM aspect ratios depends on the version of the core and the operand lengths to be supported. Verilog RTL models of all synchronous RAMs are supplied with each version of the core for behavioural modelling and simulation purposes. Please contact Helion and we will be very happy to discuss all the options in detail.

Important Note on Comparing Performance

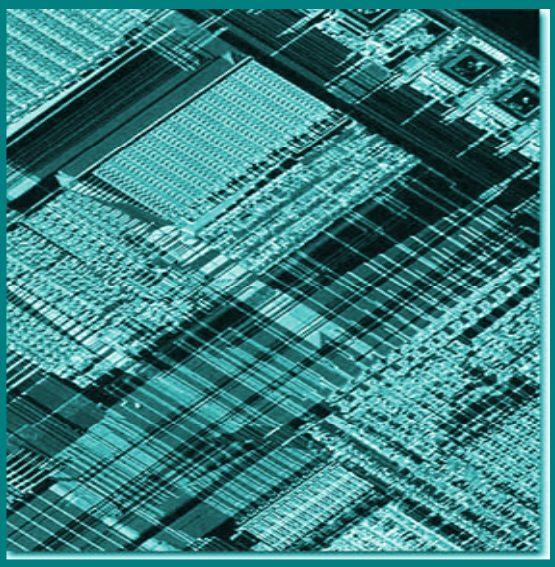
It is vital to note that the quoted RSA operation rates above are for full-size 1024-bit operands (|E|=1024, |M|=1024), except for the two largest cores where they are for 2048 and 4096-bit operands respectively. Operations with shorter exponents like those typically used for Diffie-Hellman or for public key encryptions will always be much faster, and if evaluating different solutions it is important to ensure that comparisons are made under identical conditions. For specific 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.

Ordering Information

Before ordering it is necessary to decide which of our family of Modular Exponentiation cores will best fit your application. First decide between the family members (TINY32, STD32 – STD1024) according to the number of operations per second required. Then determine what operand lengths you would like to support as well as any other special requirements your application may have.

If some of these choices are unclear, or you would just like to go over the options available, we are always happy to discuss the alternatives and help select the best solution for your application.

HELION



"I would say that the support from Helion has been outstanding from my initial contact all the way through implementation. I was very impressed when I asked questions on weekends and received answers the same day.
The core was actually so easy to use I completed my implementation almost a month early.
The product performed exactly as advertised and the price made it a very affordable option to add to our system."

Jim Cassey
Sr. Hardware Engineer
Delta Digital Video

About Helion

Founded in 1992, Helion is a long established British company based in Cambridge, England. We offer a range of product-proven Data Security and Lossless Compression IP cores, backed by a team of highly experienced engineers, proudly developing and supporting a world-class portfolio.

Our aim is to offer our customers…

Innovation
Helion works hard to anticipate, understand and then deliver great solutions for its customers. As an example, Helion offered the world's first commercial AES core back in 2001, even before the industry had fully adopted the algorithm. This process continues unabated today, with new products in development that will lead the field.

High Performance
Helion IP is specially designed and optimised for each target technology. This means lots of work for us, but this approach yields amazing results for our customers. We always aim for the best in class performance and lowest utilisation in any given ASIC or FPGA target.

High Quality
IP should be problem free, so we always go the extra mile to ensure a smooth and trouble free integration phase for our products. We realise that our customers are putting their faith in us, and want to repay that with an outstandingly easy deployment.

Ease of Use
Helion engineers have many years of real product development experience, and so our IP is designed to be used in realistic situations. It is flexible and well thought through - the result being that it is simple to drop into your system.

See how we achieve all this by visiting our Clients page at http://www.heliontech.com/clients.htm

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