

RSA Offload Processor

The CS1024-MI is an RSA processor designed to support the use of Chinese Remainder Theorem (CRT). It implements the modular inversion operations required in the RSA algorithm and is usually paired with one or more CS1024-RSA cores. Together these two cores accelerate the operations which are very cumbersome when done in software.

The CS1024-MI is designed for optimal performance in ASIC and FPGA applications. FPGA designers can take advantage of the core for use in designs hosted in cost-effective Xilinx Spartan-3 and Altera Cyclone devices or high-performance Virtex and Stratix devices where outstanding performance can be achieved.

Core Pin-out

The core offers the same pin-out as the CS1024-MI to simplify integration into the target SoC or FPGA.

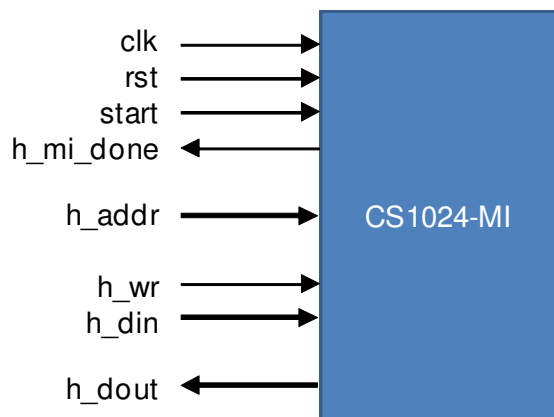


Figure 1 Core Pin-out

Chinese Remainder Theorem:

Chinese Remainder Theorem is used to

accelerate RSA operations – particularly those involving the private key which has a very high one's density and therefore consumes many CPU cycles or offload engine activity.

Details of the RSA algorithm are beyond this scope of this datasheet, but it is worthwhile to provide a brief synopsis in order to explain the use of CRT, the impact it can have on system performance and the choice of the companion modular exponentiation core.

In RSA private key operations specified by (n,d) such as decrypting a message (m) or generating a cryptographic signature, the modular exponentiation $m = c^d \text{ mod } n$ must be calculated. The private exponent d is not as convenient as the public exponent, for which a value with as few '1' bits as possible is chosen. For a modulus n of k bits in length, the private exponent d will be of similar length, with approximately half being '1'. The effort to compute the exponent is proportional to the number bits in the modulus, so there is either much more computing to do or a larger offload engine will be required. CRT is therefore commonly used to compute $m = cd \text{ mod } n$ more efficiently.

In CRT the following values must be calculated given p, q with $p > q$ where p and q are prime factors of n :

$$dP = (1/e) \text{ mod } (p-1)$$

$$dQ = (1/e) \text{ mod } (q-1)$$

$$qInv = (1/q) \text{ mod } p$$

where the $(1/e)$ and $(1/q)$ notation indicates the modular inverse. Therefore CRT requires the completion of three modular

CS1024-MI Data Sheet

inversion operations which can be offloaded by the CS1024-MI core.

To compute the plaintext message m from the ciphertext c the following calculations are required when using CRT:

$$m1 = c^{dP} \text{ mod } p$$

$$m2 = c^{dQ} \text{ mod } q$$

$$h = q\text{Inv}*(m1 - m2) \text{ mod } p$$

$$m = m2 + h*q$$

It is important to note that the calculation of $m1$ and $m2$ involve the exponents dP and dQ which are roughly half the size of p and q . This is why there is such an improvement in execution speed when the CRT algorithm is used. Equally important to note that given the size of dP and dQ , it is possible to use a smaller modular exponentiation engine for hardware offload. If 2048-bit RSA operations are required for example, it is possible to implement a 1024-bit offload engine such as the CS1024-RSA and support these RSA operations.

There is an excellent tutorial on the web that was used as a source for this material. It explains the algorithms in detail and offers examples using small numbers (not secure) and real life large number calculations. It can be found at the following URL:

http://www.di-mgt.com.au/rsa_alg.html#crt

General Operation

The Host processor invokes a particular operation by initially writing specific operands and system constants into core

memory then writing the control register to initiate the operation. The CS1024-MI then takes control of the SRAM memory until the operation completes.

Licensing and Availability

The CS1024-MI is available for immediate licensing. Export permits may be required for customers outside of North America and the EU. Please contact us for more information.

The core is available either under Crack Semiconductor's license agreement or the Xilinx SignOnce license.

Resources

In ASIC form, the CS1024-MI required 10K ASIC gates and a total of six DPRAM memory instances occupying 6144 bits. FPGA resource requirements can be generated – upon request. Please let us know your target FPGA choice.

Deliverables

The IP is available for license as Verilog RTL or EDIF Netlist. The deliverables include:

- User Manual
- Test bench