A Third Generation Many-Core Processor for Secure Embedded Computing Systems

John Irza
Coherent Logix, Inc.
Andover, MA
irza@coherentlogix.com

Michael Doerr, Michael Solka
Coherent Logix, Inc.
Austin, TX
doerr|solka@coherentlogix.com

***Abstract* — As compute-intensive products proliferate, there is an ever growing need to provide security features to detect tampering, identify cloned or counterfeit hardware, and deter cybersecurity threats. This paper describes the security features of the third generation 100-core HyperX™ processor which addresses these needs. Programmable security barriers allow the processor to implement a red-black System on Chip solution. The implementation of Physically Unclonable Functions (PUFs), encryption/decryption engines, a secure boot controller, and anti-tamper features enable the engineer to realize a secure embedded computing solution in an ultra-low power, many-core, C programmable processor-memory network.**

Keywords - HyperX; ultra-low power, C-programmable; many-core; anti-tamper; red-black; encryption; AES; GCM; PUF

I. Introduction

As compute-intensive products proliferate, there is an ever growing need to provide security features to detect tampering, identify cloned or counterfeit hardware, protect embedded IP, and deter cybersecurity threats.

The HyperX hx3100 processor is a third generation programmable processor-memory network which enables compute-intensive applications to be implemented in a low power embedded system. It has been recently enhanced with numerous security features.

II. The Programmable Processor-Memory Network Processor

Before elaborating on the security concepts and features of the latest processor, it is useful to establish a context by reviewing the general architecture of the hx3100 series.

The HyperX hx3100 processor is comprised of an array of 100 processing elements (PEs), each of which is a fully capable 500MHz DSP/GPP processor core. The PEs support 8-bit, 16-bit, extended precision integer, and 32-bit single-precision floating-point. The hx3100 processor is capable of 50,000 MIPS (50 GMACs) performance or 25 GFLOPS, with total device core power consumption ranging from 25mW to 2.5 W (typical, algorithm dependent).

Interconnected within the PE matrix is a memory and communication network of 121 data memory routers (DMRs), which facilitate autonomous data movement across the chip.

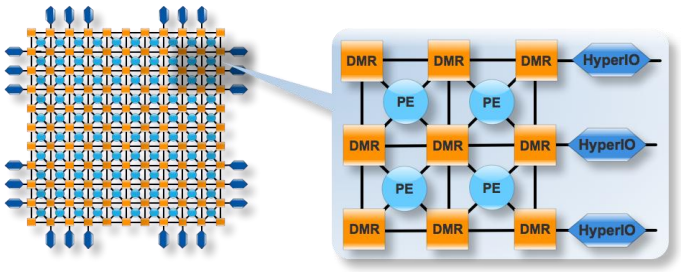

Figure 1. The HyperX processor consists of a 10 x 10 matrix of floating-point DSPs, interconnected by Data-Memory Routers.

Programmable I/O routers surround the PE-DMR fabric, supporting greater than 104 Gbps of data throughput via high-speed memory interfaces (DDR2) and general purpose LVDS/CMOS I/O channels. Custom packaging is also available to support up to 168 Gbps of I/O bandwidth.

The software controlled 'processor-memory network fabric' enables real-time mapping of computational tasks according to natural algorithm topology. The extensive on-chip communication network streams data between computing resources without interrupting any computations in progress and prevents processor stalls due to data starvation. By balancing distributed processing, memory, and high on-chip/off-chip data bandwidth, the fabric creates a power efficient platform.

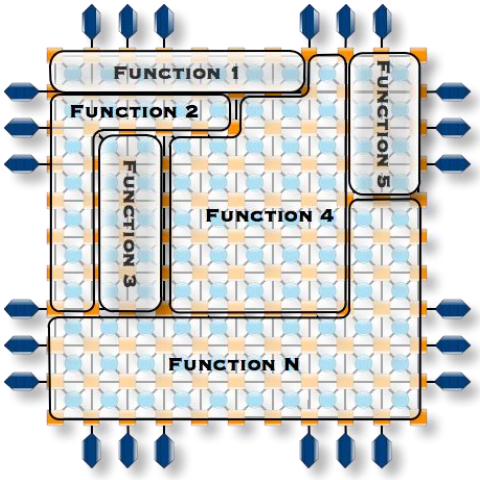

Figure 2. Mapping a system design onto the HyperX processor-memory network fabric.

III. Security Usage Scenarios and Concepts

A. Security Scenarios

A variety of usage scenarios compels the introduction of security features into a many-core processor such as the HyperX processor. These include:

- Secure processing (combined red/black system)
- Device tracking and counterfeit detection
- Third party IP protection
- Digital Rights Management (DRM)

B. Security Concepts

To meet the requirements of these usage scenarios, the following security concepts must be addressed:

- Physical and logical isolation of data & processes
- Key generation and management
- Encryption and decryption
- Authentication
- Secure boot
- Tamper detection

Essential to implementing these concepts is the need to maintain a flexible, programmable realization of the hardware, supported by software development tools.

IV. Features for Secure Embedded Computing

To support the aforementioned security concepts, a variety of physical features must be implemented in hardware and support by the software development tools.

A. Security Barriers

Security barriers provide for logically and physically "walling off" areas of the hx3100 processor. These barriers are made up of a set of locks on individual data transfer ports on the Data Memory Routers.

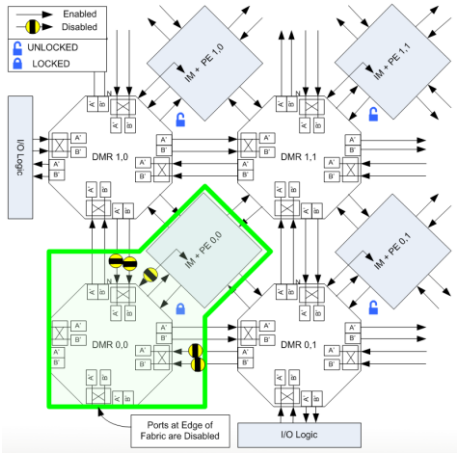

Figure 3. Locked data paths implement security barriers.

Once the security barriers are constructed they may be locked from further changes until the chip is reset. Based on the programming chosen, a chip reset can simply rebuild the barriers before any external access is allowed. The boot controller can program the access limitations for each access type.

B. Tamper Detection and Response

Various methods of tamper detection are implemented on-chip. For example, package and die related tamper detection can be triggered from lid removal, de-processing, and pin tampering.

The response to tamper detection is configurable and established during the boot process. Potential tamper responses include:

- Zero DMR (data) memory
- Zero PE (processor) memory
- Zero battery-backed RAM
- PE-specific program execution
- Disable chip operation

Each PE can be programmed to select which response(s) to implement or alternatively, choose to ignore tamper command.

C. Hardware AES Engine

Implemented in hardware are multiple Advanced Encryption Standard (AES) encryption/decryption engines which supports both 128 bit and 256 bit symmetric keys. Multiple encryption modes are supported including Cipher Block Chaining (CBC) encryption and Electronic Codebook (ECB) encryption as well as Galois/Counter Mode (GCM) for authenticated encryption. Each AES engine provides a 1 Gbps processing rate.

In addition to the hardware implementations, users can also choose to implement AES purely in software.

D. Physically Unclonable Function

The chip provides hardware support for Physically Unclonable Functions (PUFs) by utilizing the power-up state of SRAM bits as a source of a unique identifier. This bit pattern is then used to produce unique function for each die, based on proprietary algorithms. Enrollment process used to obtain a unique and public Activation Code (AC) for each part that is stored in non-secure memory during system manufacture. Enrollment can be done on-chip or by separate program off-chip.

This AC is used during runtime to reproduce a secret Root Key at boot that is used for decryption and authentication. Optionally, additional ACs can also be used to support key management for mission mode operation. Lastly, the AC and algorithm contain sufficient information to correct for SRAM bit differences between power-up cycles.

E. Secure Boot

The secure boot controller is a fully programmable and extendable mechanism for configuring and controlling processor initialization. It enables:

- Automatic boot from external SPI FLASH using PUF and AES-GCM for decryption and authentication of the encrypted boot stream
- Reading from an external encrypted boot stream image using secured PEs for programmable support of decryption and authentication with hardware acceleration

During the software development process, the operation of the secure boot controller is emulated in the development tools environment.

F. Control of Off-Chip Access

By programming the boot controller, off-chip access can be precisely controlled. The processor can be configured for:

- Normal I/O access
- JTAG access
- Full scan access
- DAP access
- SPI access

It is also possible to lock the configuration from further change or to only allow authenticated users to change the access privileges.

G. Secure Serial Bus

The on-chip control and configuration of these security features is conducted across a Secure Serial Control and Configuration Bus.

This serial bus can be accessed by any PE and supports a Validated Command Mode which allows an independent task to generate serial bus commands which are then validated by the hardware.

Each DMR has a Security Configuration Register which may be written until a ‘security enable’ bit is set, after which point the register can only be read.

When the security enable bit is set, only a limited number of serial bus commands can be supported; for the purposes of reading and validating the proper configuration.

H. Other Features

In addition to the features previously described, the hx3100 processor also supports specific hardware random number generation for the generation of random 16 bit sequences which can be concatenated in software to create any arbitrary length.

Also available on-chip is a battery backed SRAM with dedicated power pins. This memory can be used for storage of keys, a boot image, or to maintain static provisioning information. This memory can be configured to be zeroized on the detection of a tamper event.

Lastly, on-chip eFuses can be used for management of PUF enrollment and backup keys.

V. SUMMARY

The security features of the new HyperX hx3100 processor have been presented. These features enable this 100 core processor to be used in secure embedded computing applications.

For military applications the security features enable the processor to implement combined red/black processing on a single chip, while also providing anti-tamper, secure boot, encryption, and key management functions.

For commercial applications the security features enable the processor to protect third party IP and implement Digital Rights Management functions.

For all applications the security features can implement device tracking to facilitate detection of counterfeit products.