Freescale C29x Family of Crypto Coprocessors

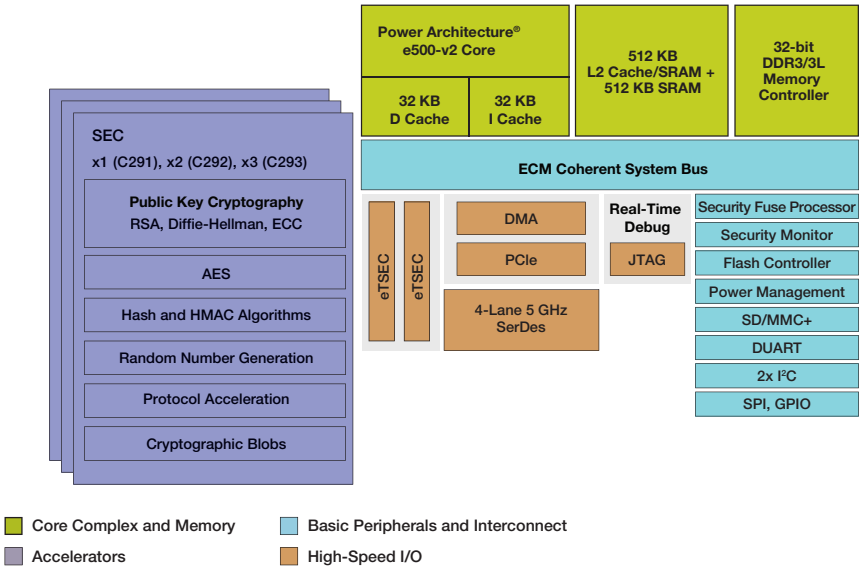
C291/C292/C293

Overview

Freescale introduces the C29x family of crypto coprocessors as a public key offload solution for data center and network security appliances. Initially consisting of three high-performance devices, the C291, C292 and C293 are optimized for public key operations. Public key algorithms such as RSA, Diffie-Hellman and elliptic curve cryptography (ECC) are the basis of digital signature and key exchange protocols that make electronic commerce possible.

With the United States National Institute of Standards and Technology's 2010 deprecation of 1024-bit keys, 2048-bit and larger keys are becoming the norm. However, the computational effort to perform 2048-bit operations is up to five times higher than 1024-bit. Performing public key in software on general-purpose processors is impractical in systems requiring thousands of operations per second. Even where public key acceleration is already in place, that hardware may be unable to keep up with larger key sizes and increasing public keys rates. Although modern multicore SoCs offer cryptographic acceleration, the performance of the crypto hardware is biased toward bulk encryption. The performance level of the integrated public key acceleration is generally only sufficient for applications with modest session establishment requirements. Applications such as remote access gateways, network admission control appliances and application delivery controllers require more public key performance than a networking-oriented multicore SoC can afford to embed. This disconnect creates a market need for an optimized public key coprocessor, for which the C29x devices are ideally suited.

C291/C292/C293 Crypto Coprocessors



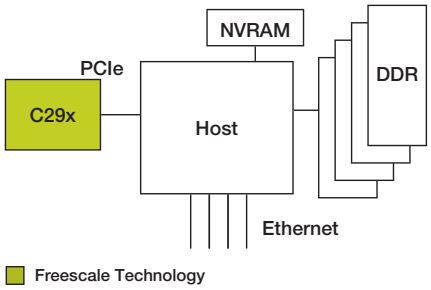
Target Applications

The C29x devices are designed to operate as simple coprocessors at maximum performance (public key calculator mode) or as hardware security modules/secure key management modules.

When operating as a public key calculator, the device connects to a host processor via PCIe, with the coprocesor requiring no external memory (neither NVRAM nor DDR and generally no peripheral ICs). The host handles packet Rx and Tx functions, classification, protocol termination and defines the operations it wants the coprocessor to perform via descriptors.

BUILT ON Power

Public Key Calculator

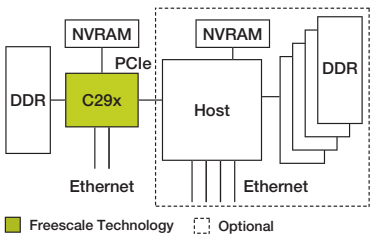


In addition to public key operations, the coprocessor can also support bulk encryption and hashing, including security header and trailer processing for IPsec and SSL.

When operating as a hardware security module/secure key management module, C29x devices can also use keys that are protected even from the host. This use case leverages trust architecture, first introduced in the Freescale QorIQ communications platform. The trust architecture platform gives the coprocessor secure boot and secure storage capability, ensuring that factory-loaded keys can only be decrypted and used by the coprocessor when it is executing trusted software. Tamper detection and secure debug round out the trust architecture feature set.

In secure key management module mode, the C29x device can be a standalone system or a PCIe-based subsystem as in the public key calculator use case. In this mode, the C29x boots with its own nonvolatile memory, DDR and optional Ethernet interfaces to either the external world or as a connection to the host.

Secure Key Management Module



C291/C292/C293 Features List

CPU and cache complex	• 32-bit e500v2 Power Architecture® core • 32 KB I and D caches • 512 KB L2 cache • Hardware cache coherency • 512 KB platform SRAM
SEC accelerator block(s)	• 15 public key hardware accelerators • AES accelerator with differential power analysis resistance • Message digest hashing accelerator • NIST-certified random number generator
One PCIe Gen 2 controller	x1, x2, x4
Main memory interface (disabled in public key calculator use case)	• 16- and 32-bit DDR3/3L controller with ECC • Supports up to 4 GB main memory in single bank • Dual-stacked and quad-stacked DDR devices also supported

Additional memory interfaces (optionally disabled in public key calculator use case)	• Integrated flash controller
	  ○ Supporting NoR and NAND (SLC and MLC) flash interfaces
	  ○ Maximum of eight banks, with a maximum of 256 MB of system memory mapped on each bank
	• Enhanced secure digital host controller (SD/MMC) which can be used for booting device using on-chip ROM

Network interfaces (disabled in public key calculator use case)	• Two enhanced three-speed Ethernet controller (eTSEC) supporting 10/100/1000 Mb/s • Supports RGMII/RMII interfaces
Trust architecture	• Security monitor • Security fuse processor • Option for battery-backed secret key • Internal boot ROM with ISBC code • Secure debug • CCSR access control • Optionally disabled in public key calculator use case, requires directly connected NVRAM
Slow-speed interfaces (optionally disabled in public key calculator use case)	• Dual I²C controllers • SPI controller used for booting with internal ROM, supporting Atmel® RapidS™ and Winbond dual read interface • Two UARTs • 64-bit GPIO
Additional logic	• Programmable interrupt controller • One four-channel DMA

Power management supporting following modes	• e500v2 modes
	  ○ Sleep: Core clock off, snooping off, cache flushed, clock to selected blocks switched off
	  ○ Nap: Core logic Idle, no snoops
	  ○ Doze: Core logic Idle
	• Software transparent clock gating of SoC logic
	• Static disable of logic blocks

Package	• 783-pin FC-PBGA • 29 x 29 mm, 1 mm pitch

C29x Family Comparison Table

	C291	C292	C293
CPU	667 MHz	1 GHz	1.2 GHz
SEC	267 MHz	333 MHz	400 MHz
DDR	800 MHz	1067 MHz	1.2 GHz
Typical power (65° C)	5 W	9 W	18 W
2048b private key	8,461	17,587	31,689
Bulk encryption (AES-HMAC-SHA-1 for SSL or Ipsec)	6 Gb/s	9 Gb/s	12 Gb/s

For more information visit, freescale.com/C29x

Document Number: C29XFAMFS REV 2