Reed Electronics Group

MICROPROCESSOR REPORT

www.MPRonline.com

THE INSIDER'S GUIDE TO MICROPROCESSOR HARDWARE

CAVIUM: SECURITY OPTIONAL

New Octeon EXP Processors Omit Internal Cryptography Engine

By Tom R. Halfhill {9/6/05-01}

Cavium Networks is as closely connected with network security as Linus in *Peanuts* is associated with his security blanket. Cavium gained fame with its award-winning Nitrox security coprocessors in 2002 and soon will begin shipping its Octeon NSP multicore network processors with integrated security engines.

Now, Cavium is tossing aside part of its security blanket—for some chips, at least. Cavium's new Octeon EXP family is virtually identical to the Octeon NSP family, except that it discards the integrated cryptography engine and related features. Octeon EXP is for customers that don't need network security at this time or prefer using a separate security coprocessor. In addition, Cavium can freely export Octeon EXP chips to countries subject to U.S. government trade controls.

As a bonus, discarding the internal security engine will reduce power consumption and prices. The most powerful device in the Octeon EXP family—the CN3860, which integrates 16 processor cores—consumes about 25W (worst case) and costs $650 in 10,000-unit volumes. In comparison, the 16-core Octeon NSP CN3860 with cryptography engine consumes about 30W and costs $750. Cavium will offer similar savings for other members of the Octeon EXP family, which includes chips with 4, 8, 12, or 16 processor cores. A dual-core Octeon EXP will be announced later. All the announced chips are sampling now, with production scheduled for 4Q05.

Tiny Elves With X-Acto Knives?

Security is a key feature of Cavium's Octeon NSP family. (See *MPR 10/5/04-01*, "Cavium Branches Out.") The cryptography engine built into Octeon NSP chips is essentially an integrated version of the Nitrox Plus coprocessor that won our *MPR* Analysts' Choice Award for Best Security Processor of 2002. (See *MPR 2/18/03-09*, "Security By Design.") It accelerates both Internet Protocol Security (IPsec) and the Secure Sockets Layer (SSL) protocol. SSL is particularly important for online commerce, and the Nitrox engine excels at speeding up the RSA cryptographic operations that are a critical component of SSL.

Internally, the Nitrox security engine has several hardwired function blocks targeting an alphabet soup of security standards, protocols, and algorithms: the Data Encryption Standard (DES); Triple DES (3DES); the Advanced Encryption Standard (AES); Message Digest 5 (MD5); the Secure Hash Algorithm (SHA-1); the Diffie-Hellman (DH) algorithm; the Rivest-Shamir-Adleman (RSA) public-key algorithm; and RSA's Rivest Cipher 4 (RC4) symmetric stream cipher, which is part of SSL. To support these security accelerators, Nitrox also implements a true random-number generator in hardware.

Octeon EXP discards all the cryptography blocks and the random-number generator. Cavium says those functions are removed, not merely disabled. *Microprocessor Report* would be surprised if Cavium actually created entirely new circuit layouts and mask sets for all the complex multicore chips in the Octeon EXP line. At this time, when sales volumes for the new devices are uncertain, it would be much more economical to disable the cryptography blocks by altering the metallization layers or blowing some fuses thoughtfully built into the designs for that purpose. A third

method would be a bond-out option at the packaging stage, although that could be reversed by repackaging the die. The other methods are virtually permanent.

Altering the existing masks would allow Cavium to leverage the basic Octeon design for Octeon EXP until sales volumes justify a complete re-layout. In addition, Cavium could salvage some rejected Octeon die by packaging them as Octeon EXP chips, if the defects were limited to the cryptography blocks. However, Cavium insists it has removed those blocks, perhaps out of concern that anything less definitive wouldn't satisfy the requirements of U.S. export regulations.

Omitting Crypto Saves Power

In all other respects, Octeon EXP is identical to Octeon NSP. The chips have superscalar MIPS64-compatible processor cores clocked at 400MHz, 500MHz, or 600MHz; 512KB or 1MB of L2 cache; a 64- or 128-bit DDR2 memory interface

Feature	Cavium Octeon EXP CN3630	Cavium Octeon EXP CN3830	Cavium Octeon EXP CN3840	Cavium Octeon EXP CN3850	Cavium Octeon EXP CN3860	Cavium Octeon NSP CN3xxx
CPU Architecture	MIPS64-R2	MIPS64-R2	MIPS64-R2	MIPS64-R2	MIPS64-R2	MIPS64-R2
Architecture Width	64 bits	64 bits	64 bits	64 bits	64 bits	64 bits
CPU Cores	4	4	8	12	16	2, 4, 8, or 16
Core Frequency	400–600MHz	400–600MHz	400–600MHz	400–600MHz	400–600MHz	400–600MHz
Superscalar Issue	2-way	2-way	2-way	2-way	2-way	2-way
ALU Pipeline Depth	5 stages	5 stages	5 stages	5 stages	5 stages	5 stages
Max ALU Instr Per Sec	4.8 billion	4.8 billion	9.6 billion	14.4 billion	19.2 billion	2.4–19.2 billion
Instruction Cache	32K, 64 ways	32K, 64 ways	32K, 64 ways	32K, 64 ways	32K, 64 ways	32K, 64 ways
Data Cache	8K, 64 ways	8K, 64 ways	8K, 64 ways	8K, 64 ways	8K, 64 ways	8K, 64 ways
L2 Cache	512K, 16 ways	1MB, 16 ways	1MB, 16 ways	1MB, 16 ways	1MB, 16 ways	1MB, 16 ways
TLB	32 entries	32 entries	32 entries	32 entries	32 entries	32 entries
Hardware FPU	—	—	—	—	—	—
DRAM Controller	DDR2 800MHz 72b ECC Single channel	DDR2 800MHz 72b or 144b ECC Single channel	DDR2 800MHz 72b or 144b ECC Single channel	DDR2 800MHz 72b or 144b ECC Single channel	DDR2 800MHz 72b or 144b ECC Single channel	DDR1/DDR2 800MHz 72b or 144b ECC Single channel
Max DRAM Bandwidth	6.4GB/s	12.8GB/s	12.8GB/s	12.8GB/s	12.8GB/s	6.4–12.8GB/s
Max DRAM Memory	16GB	16GB	16GB	16GB	16GB	16GB
RLDRAM/FCRAM	1 x 16-bit I/O	2 x 16-bit I/O	2 x 16-bit I/O	2 x 16-bit I/O	2 x 16-bit I/O	1 or 2 x 16-bit I/O
Max RLDRAM/FCRAM	1GB	1GB	1GB	1GB	1GB	1GB
Packet I/O Interfaces	4 x RGMII (4 x GbE MACs or 1 x SPI-4.2)	8 x RGMII (8 x GbE MACs or 2 x SPI-4.2)	8 x RGMII (8 x GbE MACs or 2 x SPI-4.2)	8 x RGMII (8 x GbE MACs or 2 x SPI-4.2)	8 x RGMII (8 x GbE MACs or 2 x SPI-4.2)	4 or 8 x RGMII (4 or 8 x GbE MACs) (0 or 2 x SPI-4.2)
PCI/PCI-X Controller	PCI-X 64-bit 133MHz Host/slave	PCI-X 64-bit 133MHz Host/slave	PCI-X 64-bit 133MHz Host/slave	PCI-X 64-bit 133MHz Host/slave	PCI-X 64-bit 133MHz Host/slave	PCI-X 64-bit 133MHz Host/slave
PCI Express	—	—	—	—	—	—
HyperTransport	—	—	—	—	—	—
Other I/O	Flash, UARTs, MDIO, GPIO, TCAM, FPGA	Flash, UARTs, MDIO, GPIO, TCAM, FPGA	Flash, UARTs, MDIO, GPIO, TCAM, FPGA	Flash, UARTs, MDIO, GPIO, TCAM, FPGA	Flash, UARTs, MDIO, GPIO, TCAM, FPGA	Flash, UARTs, MDIO, GPIO, TCAM, FPGA
TCP Offload Engine	Yes	Yes	Yes	Yes	Yes	Yes
ZIP Compress Engine	Yes	Yes	Yes	Yes	Yes	Yes
Reg-Expression Engine	8	16	16	16	16	8 or 16
Crypto Engines	—	—	—	—	—	DES, 3DES, AES, RSA, DH, MD5, SHA-1, RC4
True RND Generator	—	—	—	—	—	Yes
Memory-Alloc Engine	Yes	Yes	Yes	Yes	Yes	Yes
Fabrication Process	TSMC 0.13µm	TSMC 0.13µm	TSMC 0.13µm	TSMC 0.13µm	TSMC 0.13µm	TSMC 0.13µm
Packaging	FCBGA-1521	FCBGA-1521	FCBGA-1521	FCBGA-1521	FCBGA-1521	FCBGA-1521
Power (Worst Case)	<10W	n/a	n/a	n/a	<25W	5W–30W
Price (10K Units)	$350	n/a	n/a	n/a	$650	$125–$750
Availability	Samples now; production 4Q05	Samples now; production 4Q05	Samples now; production 4Q05	Samples now; production 4Q05	Samples now; production 2H05	Samples now; production 2H05

Table 1. Cavium has announced five Octeon EXP chips, with a dual-core chip anticipated in the future. All are derived from Octeon NSP–family designs, which integrate up to 16 MIPS64-compatible processor cores. Core clock frequencies across both families are 400MHz, 500MHz, or 600MHz; otherwise, performance varies mainly with the number of cores on a chip. Cavium has removed the cryptography engine in the Octeon EXP family, which is the sole feature distinguishing it from the Octeon NSP family. Another distinguishing factor of these chips, in addition to the number of processor cores, is their I/O interfaces. For instance, some parts have four software-configurable RGMIIs for packet I/O, whereas others have eight.

clocked at 400MHz (effectively 800MHz); a PCI-X controller; a TCP offload engine (TOE); a ZIP compression engine; 8 or 16 regular-expression engines; a memory-allocation engine; and various I/O interfaces.

For packet I/O, the quad-core Octeon EXP CN3630 has four reduced-gigabit media-independent interfaces (RGMII), which are software-configurable as four Gigabit Ethernet media-access controllers (MAC). The 8-, 12-, and 16-core Octeon EXP chips have eight RGMIIs, software-configurable as eight Gigabit Ethernet MACs or two SPI-4.2 interfaces. There's also a quad-core chip (the Octeon EXP CN3830) with the same I/O interfaces as the 8-, 12-, and 16-core chips.

Octeon NSP and Octeon EXP chips have compatible footprints, allowing system vendors to make one board for both families. Table 1 compares all the announced Octeon EXP devices with each other and with their Octeon NSP counterparts.

Although the Octeon NSP and Octeon EXP die are almost identical—all are fabricated by TSMC in the same 0.13-micron process—omitting the cryptography acceleration and related logic saves some power. Cavium estimates that the 16-core Octeon EXP will require less than 25W (worst case), about 17% less power than the 16-core Octeon NSP requires. We expect a slightly greater percentage reduction with parts integrating fewer processor cores, because the discarded logic occupies a relatively larger portion of the smaller die.

Offering a line of processors without the latest cryptography acceleration makes sense. Some applications can dispense with the level of cryptography the Nitrox engine provides, although we believe the number of those applications is declining. In an increasingly security-conscious world, the trend is toward more encryption and authentication, not less. In other cases, a customer might prefer to mate a Cavium processor with a cryptographic coprocessor from another vendor, probably to avoid rewriting some legacy software.

The third reason for disabling cryptography—U.S. government export regulations—is likely the most compelling. Octeon EXP is marketable to rapidly developing nations like China that remain subject to restrictions on exported technology.

Less Integrated but Still Specialized

Last year, Cavium trumpeted Octeon as the first in a new class of processors: the network services processor (NSP). On a single chip, Octeon NSP handles packet processing, content filtering, and security. Octeon has relatively little competition in that class, especially with its multiple processor cores and specialized logic. But when shorn of its cryptography features, Octeon EXP is no longer an NSP, by Cavium's definition. It joins the proletarian ranks of less integrated (but still well integrated) network and communications processors.

That's why Cavium is pitching Octeon EXP as a less-specialized, more-general-purpose processor for networking. With multiple MIPS64-compatible processor cores, Octeon EXP can simultaneously run control-plane and data-plane tasks. In the control plane, Octeon EXP can run popular operating systems, such as MontaVista's Linux SMP and Wind River's VxWorks. The operating system can distribute workloads symmetrically or asymmetrically among the processor cores, because each core has its own memory-management resources, including an MMU and translation lookaside buffer (TLB). Integrated memory controllers and I/O interfaces eliminate the need for external I/O chips, keeping the system's chip count low. And for the data plane, Octeon EXP has all the same features as Octeon NSP, except for cryptography.

Despite Octeon EXP's impressive control-plane resources, it still looks more optimized for data-plane tasks. Features like the TCP offload engine, ZIP compression engine, and regular-expression engines are rare in the general-purpose processors commonly assigned to control-plane duties. In addition, the RISC chips most often found in the control plane—MIPS-compatible and PowerPC processors from the likes of Broadcom, Freescale, IBM, and PMC-Sierra—typically run at much higher clock frequencies than Cavium's processors, which top out at 600MHz. Freescale's new PowerPC MPC7448, clocked at 1.7GHz, recently set records in EEMBC's networking and telecommunications suites. (See *MPR 7/5/05-01*, "PowerPC Ain't Dead Yet.")

True, the Octeon EXP family includes chips with as many as 16 processor cores, whereas the chips from the aforementioned competitors have only one, two, or four cores. But large numbers of cores more readily lend themselves to parallel packet processing in the data plane than to control-code processing in the control plane. Not that Octeon EXP can't be an effective control-plane processor—it's simply better equipped to compete in the data plane, or in systems that don't need extremely high control-plane performance.

Surveying the Competitors

Octeon EXP will face stiff competition from Freescale's well-established PowerQUICC chips, which have only one or two processor cores but lots of networking features. (See *MPR 3/21/05-01*, "Freescale Quickens PowerQUICC.") There are PowerQUICC chips for almost every application. Freescale's first multicore chip in this family is the PowerQUICC III MPC8641D, due in 1H06. It's a dual-core chip based on the same PowerPC e600 core as the MPC7448, but with much more network integration. Thanks to 90nm fabrication, clock speeds will exceed 1.5GHz. (See *MPR 10/25/04-01*, "Embedded CPUs Zoom at FPF.")

Broadcom is another tough competitor, especially with its SiByte family. Interestingly, the MIPS64-compatible SB-1 processor core in SiByte chips was custom designed by former DEC engineers—just as another group of DEC veterans

designed Octeon's custom cnMIPS64 core. The SiByte BCM12xx series has two MIPS64 processor cores, and the BCM14xx series has four. Broadcom finally began sampling the quad-core BCM1480 late last year, just in time to win our *MPR* Analysts' Choice Award for Best High-Performance Embedded Processor. Clock speeds range from 800MHz to 1.2GHz, and their integration is impressive: 1MB L2 cache, DDR1/DDR2 DRAM controller, 64-bit 133MHz PCI-X, four

Feature	Broadcom SiByte	Cavium Octeon EXP	Freescale PowerPC 8641/D	PMC-Sierra RM11200	Raza Micro XLR
Chip Family	BCM1255 (2 CPU) BCM1280 (2 CPU) BCM1455 (4 CPU) BCM1480 (4 CPU)	CN3630 (4 CPU) CN3830 (4 CPU) CN3840 (8 CPU) CN3850 (12 CPU) CN3860 (16 CPU)	PowerQUICC III 8641 (1 CPU) 8641D (2 CPU)	RM11200 (2 CPU)	XLR308 (2 CPU) XLR508 (2 CPU) XLR516 (4 CPU) XLR716 (4 CPU) XLR532 (8 CPU) XLR732 (8 CPU)
Applications	Storage, control plane, high-density computing	L3–L7 routing, telecom, storage, control plane, load balancing, content filtering, general embedded	L2–L4 routing, telecom, storage, general embedded	Routing, telecom, storage, general embedded	Routing, telecom, storage, general embedded
Architecture	MIPS64	MIPS64-R2	PowerPC	MIPS64	MIPS64
Arch Width	64 bits	64 bits	32 bits	64 bits	64 bits
CPU Core	SiByte SB-1	cnMIPS64	e600 (G4+)	E11K	MIPS64
CPUs	2 or 4	4, 8, 12, or 16	1 or 2	2	2–8
Core Frequency	800MHz–1.2GHz	400–600MHz	>1.5GHz	1.8GHz	Up to 1.5GHz
Superscalar	4-way	2-way	4-way	2-way	Uniscalar
ALU Pipeline	9 stages	5 stages	7 stages	7 stages	10 stages
ALU Instr / Sec	6.4–19.2 billion	2.4–19.2 billion	>6–12 billion	7.2 billion	3.0–12 billion
L1 Cache I/D	32K / 32K	32K / 8K	32K / 32K	64K / 32K	32K / 32K
L2 Cache (Total)	512K or 1MB	Up to 1MB	1MB or 2MB	1024K	512K–2MB
FPU	4 or 8	—	1 or 2	2	—
DRAM Controller (MHz)	DDR1 400 DDR2 800	DDR2 800	DDR2 667MHz	DDR2 800	DDR2 800
DRAM I/O Width	2x64 bits or 4x32 bits	1x64 bits or 1x128 bits	2x64 bits	2x64 bits	2x64 bits
Max DRAM B/W	12.8GB/s	12.8GB/s	10.6GB/s	12.8GB/s	12.8GB/s
Max DRAM	16GB	16GB	16GB or 32GB	1TB	n/a
Other Memory Interfaces	Boot ROM	RLDRAM, FCRAM, TCAM, flash, boot ROM	Local bus for boot ROM, flash	Boot ROM	800MHz SRAM, PCMCIA, flash, I^2C, UART, GPIO
Ethernet MAC	4xGbE,TOE, FIFO	4 or 8xGbE	4xGbE	4xGbE	3 or 4 GbE 0 or 2 10GbE
PCI/PCI-X (MHz)	64b PCI-X (133) 64b PCI (66)	64b PCI-X (133)	—	—	64b PCI-X (133)
PCI Express	—	—	2 x8-lane	2 x4-lane or 1 x8-lane	—
HyperTransport	0 or 3x16 bits	—	—	1x8 bits	1x8 bits
SPI-4.2	0 or 3	1 or 2	—	—	2
Other I/O	GMII, SMbus, UART, PCMCIA, GPIO	4 or 8 RGMII, flash, I ^{2}C, UART, MDIO, GPIO, 2-Wire	Serial RapidIO, UARTs, I2C	UARTs, GPI-16	—
Hardware Acceleration	Packet DMA, hash, route, checksum	TOE, ZIP compress, reg-exp, malloc	TCP/IP checksum, IPv6, TOE, QoS	Direct I/O to L2 cache	Packet distrib, TCP checksum
Crypto Hardware	—	—	—	—	AES, ARC4, DES, 3DES, SHA, RSA
True RND	—	—	—	—	Yes
Fab Process	90nm	0.13µm	90nm SOI	90nm	90nm
Packaging	BGA-1936	FCBGA-1521	HiTCE-960	FCBGA-1152	BGA-786/1605
Power (Typical)	13–23W (1GHz)	<10W–25W (worst case)	10–25W	~15W	10W–50W
Price (Units)	$599–$1,199 (10K)	$350–$650 (10K)	n/a	~$450	$150–$850 (10K)
Production	1H05–2H05	4Q05	1H06	4Q05–1Q06	4Q05

Table 2. This table could be much larger, because Octeon EXP competes in the fast-growing field of highly integrated network processors. Restricting the competition to multicore chips narrows the field considerably. All these chips are scheduled to enter production at approximately the same time—late this year or early next year. Note that Octeon EXP is the only one in this group not fabricated in a 90nm process, which accounts for its significantly lower clock frequencies. However, no other vendor offers as many processor cores as Cavium does. All the power-consumption numbers are vendor estimates and are remarkably similar, considering the disparities in clock speed and fabrication processes. Some vendors haven't announced pricing, but Octeon EXP looks competitively priced. (n/a = data not available)

Gigabit Ethernet MACs, four GMIIs, and three I/O ports independently software-switchable between HyperTransport and SPI-4.2. The BCM1455 is nearly identical, lacking only HyperTransport and SPI-4.2. (See *MPR 1/31/05-02*, "Multi-core Chips Rule in 2004.")

PMC-Sierra's latest contender is the RM11200, a MIPS64-compatible dual-core chip that reaches 1.8GHz, thanks to 90nm fabrication. Unlike Cavium's Octeon NSP and Octeon EXP, the RM11200 has a PCI Express controller, which can operate as a single eight-lane interface or dual four-lane interfaces. In addition, the RM11200 has four Gigabit Ethernet MACs and two 64-bit DDR2 memory controllers that match the total memory bandwidth available in Broadcom's and Cavium's chips. The RM11200 is scheduled for production at about the same time as Octeon EXP. (See *MPR 10/25/04-01*, "Embedded CPUs Zoom at FPF.")

No summary of Cavium's competition would be complete without mentioning another newcomer, Raza Microelectronics (RMI). At Spring Processor Forum, RMI unveiled its XLR family of multicore, multithreaded network processors. These chips are based on yet another custom-designed MIPS64-compatible processor core—a deeply pipelined uniscalar core supporting four-way multithreading and clock frequencies up to 1.5GHz in a 90nm process. Network integration is equally impressive. Among the six XLR devices announced so far, some have as many as four Gigabit Ethernet MACs and two 10-Gigabit Ethernet MACs, plus HyperTransport, PCI-X, SPI-4.2, multiple DDR2 memory controllers, and cryptography coprocessors. However, XLR lacks a few features of Octeon EXP, such as ZIP compression/decompression and regular-expression engines. (See *MPR 5/17/05-01*, "A New MIPS Powerhouse Arrives.") Table 2 summarizes some of the chips with enough performance and network integration to compete with Octeon EXP.

Without Cavium's superlative cryptography engine, Octeon EXP clearly isn't as compelling as Octeon NSP, but it still has much to offer. For control-plane duties in high-performance systems, developers might lean toward the higher-frequency chips from Broadcom, Freescale, IBM, PMC-Sierra, RMI, and others—if only because writing control code for a smaller number of fast processor cores seems easier than writing code for a larger number of slower cores. On the other hand, developers comfortable with multicore programming might prefer the additional cores and hardware accelerators in Octeon EXP. For applications running control-plane and data-plane code on the same chip, Octeon EXP offers a good mix of integration, and its lower clock frequencies and lower-leakage fabrication process could save power.

Price & Availability

The first five Octeon EXP chips (with 4, 8, 12, or 16 processor cores) are sampling now; production is scheduled for 4Q05. Prices will range from $350 to $650 in 10,000-unit quantities. Cavium expects to announce a dual-core Octeon EXP later. For more information, visit *www.caviumnetworks.com/Octeon_exp.html*.