Reed Electronics Group

MICROPROCESSOR REPORT

www.MPRonline.com

THE INSIDER'S GUIDE TO MICROPROCESSOR HARDWARE

ALCHEMY ADDS SECURITY ENGINE

AMD Network Processor Adopts SafeNet Encryption Technology

By Tom R. Halfhill {4/5/04-01}

AMD's Alchemy family of MIPS32-based embedded processors has a new member that integrates a security engine for encrypted communications. The new Au1550 supports Internet Protocol security (IPsec) and the Secure Sockets Layer (SSL) protocol for virtual private networks (VPN).

The Au1550 is the fourth, and most advanced, member of the embedded-processor family that AMD gained by acquiring Alchemy Semiconductor in 2002. (See *MPR 3/4/02-01*, "AMD Acquires Alchemy to Make Gold in Embedded Markets.") It's the first Alchemy chip to incorporate a security engine for accelerating data encryption and decryption. Instead of developing a security engine of its own, AMD licensed the SafeXcel IP engine from SafeNet, whose intellectual property, chips, boards, and software are widely used throughout the industry.

By using the SafeXcel IP engine to process the VPN packet protocol in hardware, the Au1550 frees its MIPS32 processor core for other tasks. AMD says the engine can sustain multiple VPN tunnels using IPsec at a maximum theoretical throughput of 140Mb/s (assuming 100-byte packets). It implements the DES, Triple-DES (3DES), AES, ARC-4, SHA-1, and MD5 encryption standards, and it has a hardware random-number generator for creating secure encryption keys.

AMD designed the Au1550 for network-gateway products and network-attached storage (NAS) subsystems. Its relatively low power consumption—less than 500mW at 400MHz—makes it suitable for some mobile wireless applications as well as for power-over-Ethernet systems on wired networks. The chip is sampling now and is scheduled for production in 2Q04.

A Plethora of Peripherals

In addition to the security engine, the Au1550 is stuffed with on-chip peripherals and I/O interfaces, some of which are new to the Alchemy line. It's the first Alchemy processor to support DDR-400 DRAM as well as SDRAM, and the

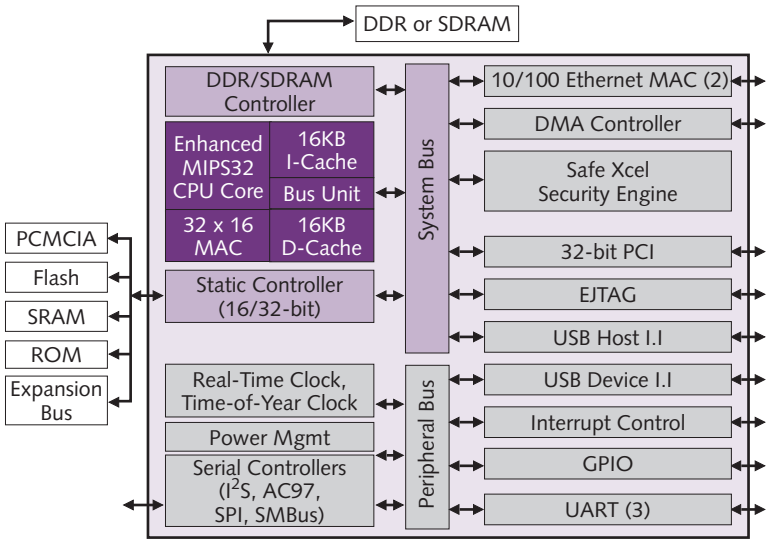

Figure 1. AMD's Alchemy Au1550 is a well-integrated processor for network-gateway systems that need the security of encrypted communications. SafeNet's SafeXcel IP security engine offloads the IPsec and SSL protocol processing from the MIPS32 general-purpose CPU core.

first to have a System Management Bus (SMBus) and a time-of-year clock that can work with a backup battery. SMBus is a low-speed two-wire bus that uses the I²C protocol to exchange system-management messages among various chips in a system. The time-of-year clock is similar to a real-time clock (also included in the Au1550), but it continues ticking while the processor saves power in its sleep or hibernation mode, allowing the chip to wake up at a certain time.

Another new feature of the Au1500 is a descriptor-based direct memory access (DDMA) controller. Although other chips in the Alchemy family have DMA, the Au1550's DDMA uses descriptors in memory to define attributes that can be specific to any of the 16 DMA channels. For instance, it can autonomously manage multiple sequential data transfers between different regions of memory, between on-chip and off-chip peripherals, and between memory and the FIFO buffer for flash memory and off-chip peripherals.

Other notable features of the Au1550 include two 10–100Mb/s Ethernet media-access controllers, a 32-bit 33/66MHz PCI controller, USB 1.1 host/device controllers, and a 16/32-bit interface for ROM, SRAM, flash memory, and nonmemory-mapped external devices. Like all Alchemy processors, the Au1550 has a MIPS32 core with a 16 × 32-bit multiply-accumulate (MAC) unit, 16K instruction/data caches, and an MMU. The MMU allows the Au1550 to run some higher-end embedded operating systems, such as Linux, Microsoft Windows CE.NET, and Wind River's VxWorks. Figure 1 is a block diagram of the Au1550.

AMD omitted a few features found in some other Alchemy chips intended for different applications. In particular, the Au1550 lacks an LCD controller, a Secure Digital interface, and an IrDA infrared interface. AMD says the Au1550 doesn't need those features, because it's more specifically targeted at networking systems than at media applications. Table 1 compares the features of all four chips

Feature	AMD-Alchemy Au1550	AMD-Alchemy Au1500	AMD-Alchemy Au1100	AMD-Alchemy Au1000	Intel IXP425	Motorola MPC8272
General Features						
Core Architecture	MIPS32	MIPS32	MIPS32	MIPS32	XScale/ARM	PowerPC 603e
Cache (I/D)	16K/16K	16K/16K	16K/16K	16K/16K	32K/32K	16K/16K
FPU	—	—	—	—	—	64-bit
MAC Unit	32x16-bit	32x16-bit	32x16-bit	32x16-bit	—	—
MMU	Yes	Yes	Yes	Yes	Yes	Yes
Core Freq	333–500MHz	333–500MHz	333–500MHz	266–500MHz	266–533MHz	266–400MHz
Bus Freq	100–200MHz	100–125MHz	100–125MHz	100–125MHz	133MHz	33–100MHz
Voltage (Core)	1.2V	1.5–1.8V	1.2V	1.5–1.8V	1.3V	1.5V
Voltage (I/O)	3.3V (2.5V DRAM)	3.3V	3.3V (2.5V DRAM)	3.3V	3.3V	3.3V
Power (400MHz)	<500mW	700mW	250mW	500mW	1.0–1.5W	1.2W
Package	PBGA-483 21x21mm	PBGA-424 19x19mm	PBGA-399 17x17mm	PBGA-324 23x23mm	PBGA-492 30x30mm	PBGA-516 27x27mm
Availability	2Q04	Now	Now	Now	Now	Now
Price (10K)	$21.26–33.75	$18+	$18+	$17+	n/a	$23.33–31.64
On-Chip Peripherals						
DRAM Controller	DDR/SDRAM	SDRAM	SDRAM	SDRAM	SDRAM	SDRAM
Bus Width	16/32 bits	32 bits	32 bits	32 bits	32 bits	64 bits
ROM-SRAM-Flash I/F	Yes	Yes	Yes	Yes	Yes	Yes
DMA Controller	DMA + DDMA	Yes	Yes	Yes	PCI only	Yes
Serial Controllers	4	1	4	4	2	3
Serial Protocols	AC'97, I²S, SPI, SMBus	AC'97	AC'97, I²S, SSI	AC'97, I²S, SSI	n/a	I²C, SPI
PCI Controller	33/66MHz	33/66MHz	—	—	33/66MHz	33/66MHz
USB 1.1 Controller	Host/device/OTG*	Host/device	Host/device	Host/device	Device	Host/device
LCD Controller	—	—	Yes	—	—	—
Ethernet MAC	2x10/100	2x10/100	1x10/100	2x10/100	2x10/100	2x10/100
Secure Digital I/F	—	—	2	—	—	—
Fast IrDA	—	—	Yes	Yes	—	—
Utopia 2 I/F	—	—	—	—	Yes	Yes
UART	3	2	3	4	2	1
GPIO (Total)	43	39	48	32	16	83
Real-Time Clock	1	2	2	2	—	1
Time-of-Year Clock	1	—	—	—	—	—
Security Engine	SafeNet SafeXcel IP	—	—	—	Intel	Motorola S1
Security Protocols	IPsec, SSL	—	—	—	IPsec, SSL	IPsec, SSL
HW Random Num	Yes	—	—	—	—	Yes

Table 1. Alchemy processors are based on a MIPS32 processor core enhanced with a MAC unit and clocked at relatively high core frequencies. All have a plethora of integrated peripherals and I/O interfaces that help reduce chip counts in embedded-system designs. The new Au1550 is competitive with similar network processors from Intel and Motorola. *OTG: USB On-the-Go support. n/a: data not available.

in the Alchemy line, as well as Intel's XScale IXP425 and Motorola's PowerQuicc II MPC8272.

Like most other Alchemy processors, the Au1550 will be available in three speed grades: 333, 400, and 500MHz. AMD estimates the typical power consumption will be less than 500mW for the 400MHz part; the other speed grades haven't yet been characterized. This figure puts the Au1550 in the middle of the power consumption range for Alchemy processors, which dissipate between 250mW and 700mW at the same clock frequency. Removing the LCD controller, IrDA interface, and Secure Digital interface helped to compensate for the extra weight of the security engine and higher-performance memory system.

Au1550 Stacks Up Well

Similarly priced network processors in Intel's XScale IXP family and Motorola's PowerQuicc lines offer similar features, but they tend to consume more power and offer less performance for secure packet processing than the Au1550 does. In addition, the Au1550 can process the IPsec headers and trailers as well as the encryption/hashing algorithms in hardware, while competing chips require another CPU to process the header/trailer overhead in software.

Late last year, Motorola added a security engine to some PowerPC-based PowerQuicc I and PowerQuicc II chips, which formerly required a coprocessor for security. The PowerQuicc I chips run at 50–133MHz, and the PowerQuicc II chips run at 200–450MHz. The Au1550 will match or exceed the secure packet-processing performance of the fastest PowerQuicc II, but the Motorola chips are fast enough for small-office/home-office (SOHO) gateways.

Intel's IXP425—another chip intended for SOHO gateways—securely processes packets at about 50% of the claimed rate of the Au1550 and lacks a true random-number generator in hardware. For higher-end networking applications, Intel offers more-powerful IXP processors. (See *MPR 3/18/02-01*, "Intel Beefs Up Networking Line.") However, the Intel and Motorola network processors do have a few features missing from the Au1550, such as Utopia 2 interfaces. In addition, Intel's IXP425 has a 16-bit DSP interface, and Motorola's MPC8272 has two CPU cores and an FPU.

Price & Availability

AMD's Alchemy Au1550 security processor is sampling now, and production is scheduled for 2Q04. Prices, in 10,000-unit quantities, range from $21.26 for the 333MHz part to $33.75 for the 500MHz part. For more information about the Au1550, see *www.amd.com/connectivitysolutions/au1550*. For more information about SafeNet, visit *www.safenet-inc.com*.