Cahners
MICROPROCESSOR REPORT
www.MPRonline.com
THE INSIDER'S GUIDE TO MICROPROCESSOR HARDWARE

SMARTMIPS FOR SMART CARDS

The MIPS Technologies Low-Power Challenge

By Cary D. Snyder {10/1/01-02}

There are processor architectures that are known for their low-power attributes, but the MIPS ISA is not one of them. This situation may change if MIPS Technologies can successfully introduce its SmartMIPS architecture; it has been working on creating this architecture with Gemplus SA, the leading smart-card OEM, for more than a year. MIPS Technologies has released its first product and is shipping its MIPS32 4KSc smart-card core, based on its SmartMIPS architecture.

SmartMIPS isn't without competitors, ARM has its own processor-core architecture for smart cards, which it calls SecurCore. The currently shipping SecurCore is ARM's SC100, a new version of which is being announced for the end of October 2001. Analysis of the SecurCore architecture and its core derivatives will appear in a future article.

The billion-dollar question remains: Is the smart-card market big enough for processor-core vendors to turn a profit where OEMs must meet a total cost target of $4 per unit? Smart cards are currently more popular abroad than in the United States. Smart-card development was pushed in European countries, owing to their higher telecommunications cost, which created difficulties in implementing a cost-efficient centralized security and management scheme. A centralized system depends on access to a low-cost telephone or communications infrastructure—something that has been slow to develop or, in some cases, unavailable outside the United States.

Smart-card technology not only dominates credit- and bankcard transactions in Europe but has become essential for everyday activities: smart cards are used in transportation systems, health services, public telephones, employee identification, and, in many countries, for network or computer security access in many companies. Average consumers in Europe carry five to six different smart cards on their persons as credit cards, employee passes, and telephone cards, and as access cards for medical, dental, and other services. Companies in the United States are starting to run advertisements for new "smarter" credit cards with a similar seven-contact oval smart-card interface and the traditional magnetic stripe.

Compelling Business Reason

Smart-card makers have been boasting about the merits of open systems for several years, but they have traditionally had limited processing power and memory space to meet the low-cost requirements of smart cards themselves, eight-bit processors and microcontrollers being the predominant silicon shipping today. Infineon Technologies provides more than 60% of the world's smart-card processor chips. There is a strong desire to expand features and capabilities in next-generation smart cards to increase the value and security in higher-end applications.

The smart-card evolutionary process will incorporate more features and faster processing capability with higher standalone security while maintaining the ultralow power budget. Smart-card manufacturers, or rather the issuers of smart cards, require an adaptable cryptographic processing platform while they control the features and options of their smart-card users. High-end applications having the greatest antitampering, antifraud capabilities would be able to match smart card and user to an international database with virtually 100% reliability, eliminating forged documents, such as

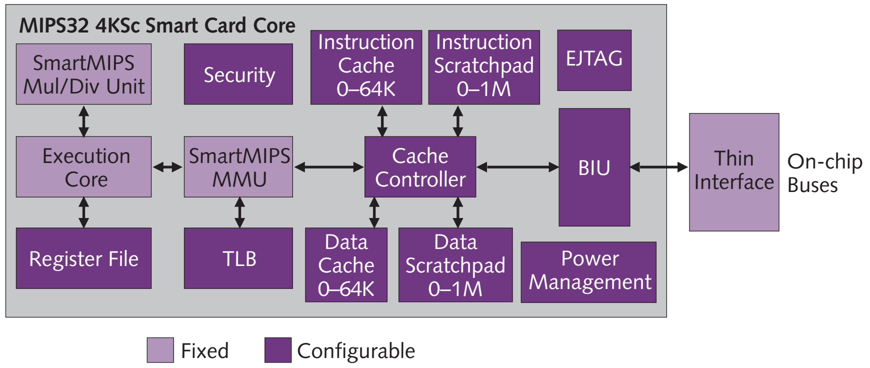

Figure 1. The SmartMIPS architecture includes fixed and configurable logic.

passports. The expanding smart-card market is creating an excellent opportunity for providers of synthesizable cores.

Use As a Cell-phone Coprocessor

Smart-card technology is essential to wireless and cell phone applications. Using smart cards offloads security-processing and service validation applications from the cell phone's handset processors, making it easier for a carrier to manage its customers. However, smart cards have created a political debate over whether the handset manufacturer or the carrier will own or provide value-added services, and over which services will be controlled. Smart cards used in cell phones are called SIM (subscriber identity module) cards and are currently completely independent of the cell phone.

SIM cards and their stamp-size packages are at the core of the GSM wireless communications—standards like DECT, PDC, CDMA, Inmarsat, and Globalstar. Carriers and handset manufacturers see where SIM cards would be the key component in value-added services involving financial transactions, loyalty programs, electronic cash, and so on. As GSM cell phone standards evolve, smart cards will be expected to support additional services like over-the-air management of worldwide services.

Security, Less Code, Low Power, and More

It is hard to imagine that the long list of key features and functions could be implemented with a 32-bit processor and meet the less-than-$4 cost requirement for smart cards. With the average smart card selling in the $1–$4 price range, IP providers like ARM and MIPS Technologies can expect pennies of royalty revenue per chip. The high-volume possibility of smart cards, measured in the billions, justifies the investment involved in pursuing this market.

The need for 32-bit processing in smart cards is being driven by the need to address larger memory maps to obtain increased security and enhanced cryptographic processing to protect system resources. Confidential data include medical and biographical records plus private keys, account numbers, passwords, and other forms of personal information that could enhance the security of the overall system. Emerging smart-card software is becoming feature rich and therefore too complex to be efficiently run on 8- and 16-bit processors. Complex methods to overcome memory-address limitation by bank switching and creating memory overlays is reminiscent of techniques first employed with address-space-limited minicomputers in the 1970s.

Small die size is an absolute requirement for smart-card silicon: the size must be less than 24mm^2 for use in a higher-cost universal smart card (several applications and/or services provided on one card) and 10–12mm^2 for single-use cards like bank smart cards. The small die must contain processor, peripherals, and all memory.

Ultralow-power silicon is a critical operating requirement for contactless smart cards, as their primary power source comes from weak radio-frequency (RF) fields in a contactless DC-power mechanism. Low power is also important for contact smart cards, the largest number in use today. Smart-card cores typically operate at less than 1V, demanding a low-voltage semiconductor process. Power consumption must be in the 0.4–0.7mW/MHz range in a cost-effective 0.18-micron or 0.25-micron process.

As expected, smart-card security is essential, but the level of security isn't what one might expect for a computing system that is carried in a wallet. Smart cards must include cryptographic processing, physical antitampering/-counterfeiting measures, and a host of other security features like memory-scrambling/-protection and databus encryption. One area of concern is the theoretical vulnerability of smart-card security by those using techniques like Simple Power Analysis (SPA) and Differential Power Analysis (DPA). Using SPA/DPA countermeasures can ameliorate these concerns, but such countermeasures can eliminate much of the benefit derived from common power-management techniques like clock gating.

A smart card's embedded-memory resources are a precious commodity, given the small die size and code-footprint requirements. The types of software applications that target smart cards result in the need to run an assortment of Java-type programs at the lowest possible power consumption. The ability to run a variety of programs thus becomes a major product-differentiation issue.

SmartMIPS Designed for Smart Cards Only

The SmartMIPS architecture is based on its proven MIPS32 RISC architecture, with a number of application-specific extensions that are optimized to meet smart-card requirements. The MIPS 4KSc core supports an assortment of cryptography and code-compression algorithms and operating systems, such as Sun Microsystems' Java Card and Microsoft Windows for Smart Cards, under low-power, low-voltage conditions. Achieving the smallest possible die size led the MIPS Technologies/Gemplus design team to incorporate software cryptographic functionality as part of the MIPS 4KSc core to eliminate the additional gates of a dedicated security coprocessor.

The partnership of MIPS Technologies and Gemplus SA helped MIPS Technologies tailor special smart-card-specific processor extensions and security enhancements for the MIPS32 architecture. The Application Specific Extension (ASE) and its enhanced instructions improve the MIPS32 processor performance in processing cryptographic, security, and code-compression/-decompression algorithms. For example, a combination of cryptography performance features allows a 1,024-bit RSA signature authentication to be performed in less than 100msec. While it is possible to perform cryptographic processing in software, some algorithms, such as triple DES, become harder to execute without special hardware enhancements.

The increased performance of the SmartMIPS ASE hardware architectural enhancements are generic and can be applied to a wide range of cryptographic algorithms (current and future), unlike a hardware cryptographic coprocessor that is often optimized for specific algorithms. It will be interesting to see which benchmarks to measure cryptographic performance are incorporated into version 2.0 of the EEMBC benchmarks, due out in mid-2002.

SmartMIPS architects also needed to improve the software implementation of a Java virtual machine (JVM), so that Java-based programs can fit within limited system resources. Accelerating JVM operation was achieved by adding nine special instructions.

Initial technical specifications result in a SmartMIPS core that will run between less than 1MHz and 150MHz. High-end smart cards typically run at a maximum of 40MHz; however, the extra timing margins of a 150MHz core provide the necessary headroom to allow voltage scaling and added levels of security and tamper resistance. Power consumption is 0.5mW/MHz at 1.8V, excluding caches. The additional timing headroom allows voltage scaling to sub-1V levels. This performance is based on a 0.18-micron technology and a core size of 1.3mm^2, again excluding caches, as they could vary in size or not be used in a specific application. Power is expected to be 0.15mW/MHz at less than 0.18μ/1.0V.

Added Features Enhance Security

MIPS Technologies believes the SmartMIPS architecture will become a widely used smart-card architecture with software optimized for Java Card and Windows for Smart Cards, with its built-in cryptographic processing extensions. How widely SmartMIPS is adopted remains to be seen. The architectural enhancements to the standard MIPS32 4Kc core were created in response to the need to balance high cryptography-processing performance with preservation of the OEMs' ability to implement a wide variety of public- and secret-key algorithms. Smart cards in a security system allow for multiple factors of authentication (something you know, something you have, biometric data, etc.). Using specific proprietary (and potentially costly, in terms of die size and power consumption) security coprocessors that implement specific modular and S boxes often limits their ability to adapt to future encryption standards and improvements once a large system is deployed.

Characteristic	MIPS Technologies
Architecture	SmartMIPS
Core	MIPS32 4KSc
Frequency	0–150MHz
Memory/Caches	n/a
Gates—Core Only	95K
Power—Core Only	0.5mW/MHz 0.18μ/1.8V 0.15mW/MHz 0.18μ/1.0V
Power—Coprocessor or cryptographic logic	n/a
Coprocessor size	n/a
Size —Typical Implementation With Cryptographic capability	0.35μ = 5.0mm^2 0.25μ = 2.5mm^2 0.18μ = 1.3mm^2
Size —Typical Implementation	0.35μ = 5.0mm^2 0.25μ = 2.5mm^2 0.18μ = 1.3mm^2
Size—Core Only	0.25μ = 2.0mm^2
Availability	Now

Table 1. The list of features above shows the compact nature of the SmartMIPS design. n/a = not applicable

MIPS Technologies claims the software cryptographic acceleration features of its SmartMIPS architecture allow OEMs to implement multiple public- and secret-key algorithms with the same hardware platforms via simple software code upgrades. These cryptography acceleration features of the SmartMIPS architecture support a variety of both public- and secret-key cryptography algorithms, including RSA, single/triple DES, AES (Advanced Encryption Standard), and the newer elliptic-curve cryptography. Public-key cryptography performance can use special instructions, while elliptic-curve cryptography algorithms can employ new, nonarithmetic instructions. Secret-key cryptography algorithms like DES and AES are sped up by using these special instructions, whereas higher speed equals more headroom for various physical security enhancements or countermeasures an OEM might want to make.

These security countermeasures are designed to obscure processor activity and hide application-program signatures, thus helping to resist invasion at hardware and software levels. Invasion includes physical probing and reverse-engineering attempts through power or timing analysis or a combination thereof. Additional security measures could include disabling a card upon detection of covert attempts at hacking into restricted areas.

Synthesis and Layout Enhance Security

All smart-card cores employ extensive OEM proprietary design work to enhanced a smart card's anticounterfeiting

Price & Availability

The SmartMIPS smart-card processor core is available as licensed IP for implementation within application-specific integrated circuit (ASIC) or application-specific standard product (ASSP) designs. Pricing for SmartMIPS IP and design help is established by the needs of the semiconductor licensee and customer-specific system-level design requirements.

characteristics. Use of a synthesizable core allows a finished OEM smart-card design to be implemented in a variety of silicon processes and technologies by many semiconductor vendors. OEMs implement specific countermeasures, on top of those built into the SmartMIPS core, to help the smart card resist hardware- and software-level invasion, as well as physical tampering, be it through power or timing analysis, reverse engineering of the layout, or direct probing of the silicon's surface. The MIPS32 4KSc smart-card core implements higher-level system-encryption mechanisms and specific embedded features that disguise processor activity.

Small-Code Footprint and JVMs

Code compression is a required feature of smart cards. MIPS Technologies uses its MIPS16e code compression to reduce the application-code size, so that applications use smaller amounts of memory and a smaller die size, and also to reduce power consumption. The importance of JavaCard byte codes and similar interpretive languages used in smart-card applications has resulted in adding to the SmartMIPS architecture an instruction to accelerate JVM applications.

MIPS Technologies claims its MIPS16e code compression is equivalent in performance to ARM's 16-bit Thumb code compression. Both ISAs should have similar code densities and overall code footprints.

Memory Architecture Enhancements

A key requirement for the new generation of smart-card silicon is the ability to support multiple applications on a single card. To meet this demand, there must be separate protected data areas for each application hosted on a card. MIPS Technologies has added flexibility to its memory architecture to meet this requirement and to ensure the security of operating systems and application data.

In addition to separating and protecting data, user-application code should be restricted from accessing the operating-system code, data, and peripherals. The SmartMIPS architecture's page-protection attributes, called the Privilege Resource Architecture (PRA), allow applications to apply additional security measures by enabling assignment of separate secure memory spaces as small as 1KB. The architecture's MMU also supports read-only, execute-only, and write-only pages. This arrangement allows system implementers to easily protect sensitive consumer or financial data from rogue applications.

Largest Computing Platform

Smart-card technology is expected to be used in variety of e-commerce applications, including mobile communications, pay TV, credit card and banking systems, public transportation, workplace identification, and health care. A synthesizable core with smart-card features allows OEMs to customize core functions by adding a range of security features known only to the card issuer/developer/manufacturer. The resulting electronic-fraud countermeasures obscure processor activity and hide application-program signatures, making the smart card a secure computing platform.

The smart card, by its ubiquity in many countries and growing need in others, is likely to become the most common computing platform worldwide. The role a 32-bit processor plays in this platform is important and cannot be overlooked. Increasing security requirements and the need to run key operating systems—Sun's JavaCard and Microsoft's Windows for Smart Cards—indicate there is a healthy market for 32-bit processors.

Magnetic strips, both the key to and weakness of a highly centralized architecture, are also a security issue: plastic cards with these strips have become easy targets for illicit use. Alarming increases of credit card skimming with pocket hand-skimmers in Asia and the western United States are forcing U.S. credit card companies to take rapid action. International travel will also need a way to check a person's true identity with a secure and fraud-proof system—an electronic passport.

Smarter smart cards that support a variety of secure identity validations and credit- and bankcard transactions represent an attractive solution. The card owner—frequently, the service provider or the user's own government—must be attracted by being able to offer its customers varying levels of service in a highly secure manner at the lowest overall cost. The smart card is well on its way to becoming the world's largest single computing platform. ◇