



Oberste Priorität: Sicherheit



Grafik: Atmel

Neues aus der Welt der Chipkarten sowie der Sicherheits-ICs für Embedded-Systeme

Alfred Vollmer, Redaktion *elektronik industrie*

Es gibt zwei generelle Trends im Bereich der Chipkarten- und Sicherheits-ICs: Zum einen sind ständig stärkere Verschlüsselungen und damit mehr Rechenleistung gefragt, um den Hackern stets mit angemessenem Zeitpuffer voraus zu eilen. Zum anderen soll aus Komfort-Gründen sowie auf Grund von technischen Rahmenbedingungen der auf dem Chip integrierte nichtflüchtige Speicher immer größer werden.

Das Geschäft mit der Sicherheit läuft immer besser, denn das Schutzbedürfnis der Anwender nimmt ständig zu. „Sicherheitslösungen machen mittlerweile mehr als 10 % unseres Umsatzes aus und außerdem ist Security unser am schnellsten wachsendes Geschäftsgebiet“, betont B. Jeffrey Katz, Vice President Marketing bei Atmel. So hat Atmel jetzt einen neuen sicheren Smartcard-Controller für High-End-Anwendungen auf den Markt gebracht, der nach Angaben von Katz den Anforderungen gemäß ITSEC 4+ genügt und so entwickelt wurde, dass er den Zertifizierungen von EAL5+ standhält.

Das neue IC basiert auf dem SecureCore SC100 von ARM und enthält auf seiner Gesamtfläche von unter 20 Quadratmillimetern unter anderem auch 256 KByte ROM und 10 KByte RAM sowie ein 72 KByte großes EEPROM für Daten. Der neue 32-bit-RISC-Baustein mit der Bezeichnung AT91SC25672RC verfügt über einen speziellen Hardware-Beschleuniger zum Einsatz in JavaCard-Implementierungen, der von der aktuellen JavaCard-Version unabhängig ist und somit auch mit weiterentwickeltem Byte-Code arbeiten kann.

Der integrierte Hardware-Verschlüsselungsprozessor mit MAC-Architektur arbeitet mit bis zu 50 MHz und ermöglicht beispielsweise eine RSA-Verschlüsselung mit 1024-bit-Exponent ohne CRT binnen 60 ms, ist aber in der Lage, Schlüssellängen von bis zu 2048 zu handhaben.

B. Jeffrey Katz sieht sich mit diesem IC als „Marktführer beim Verhältnis MIPS/Watt und bei der Coddichte“. Die Argumente allerer, die zumindest für SIM-Anwendungen lieber auf einen 16-bit-Controller setzen, entkräftet Katz: „Wenn ein Sicherheits-

Controller erst einmal in einer 0,18-µm-Technologie oder mit noch kleineren Strukturen gefertigt wird, dann ist es beim Einsatz großer Speicher für die Chipgröße unerheblich, ob es sich um einen 8-, 16- oder 32-bit-Controller handelt.“

Auch die ersten Früchte des MEDEA-Projekts EsP@ss-is A302 sind jetzt reif, denn STMicroelectronics bemustert bereits seinen im Rahmen dieses paneuropäischen Smartcard-Projekts entwickelten 32-bit-Smartcard-Prozessor ST22FJ1M mit integriertem 1 MByte großem Flash-Speicher.

Mit dem ST22FJ1M erweitert ST seine bereits auf dem Markt eingeführte 32-bit-Plattform SmartJ um Page-Flash- und Standard-Flash-Speicher. Neben 128 KByte Anwender-ROM und einem großen Anwender-Flash-Bereich von 768 KByte zum Speichern von Programmcode ist ein Page-Flash-Speicher mit einer Kapazität von 256 KByte vorhanden. Page Flash bietet vereinfacht gesagt EEPROM-Funktionalität zum Flash-Preis. „Mit dem ST22FJ1M haben Entwickler die Chance, multitasking- und multithreading-fähige Lösungen auf der Basis offener Plattformen für den Internet-Zugang zu realisieren – und zwar unter Verwendung mehrerer Netzwerkprotokoll-Schichten, mehrerer Applikationsprotokoll-Schichten und mehrerer Sicherheits-Ebenen“, erläutert Reza Kazerounian, Group Vice President und General Manager der

Smartcard ICs Division von STMicroelectronics.

Auch Philips Semiconductors setzt eine seiner Prioritäten auf großen Speicher, denn das Unternehmen hat speziell für den Einsatz in mobilen Anwendungen (2.5G/3G) einen 32-bit-Smartcard-Controller auf SmartMIPS-Basis auf den Markt gebracht, der mehr als 650 KByte nichtflüchtigen Speicher enthält. Das HiPerSmart P9SC648 genannte IC verfügt über 512 KByte Flash-Speicher, 142 KByte EEPROM und 16 KByte RAM.

512 KByte oder 1 MByte Flash-Speicher integriert Sharp auf seiner neusten Smartcard-Lösung zur Integration eines Chips im Reisepass. Die Datenübertragung erledigt Sharp dabei kontaktlos mit einer Datenrate von 424 Kbit/s. Bedenkt man, dass zur Speicherung der Merkmale eines Gesichts beispielsweise etwa 50 KByte benötigt werden, dann erkennt man, dass dieser Chip noch genügend Reserve zur Speicherung der Iris-Daten oder der Fingerabdrücke enthält, denn das Betriebssystem benötigt nur rund 300 KByte.

Fujitsu wiederum legt sein Haupt-Augenmerk bei Smartcards auf die FRAM-Technologie. FRAM ist ähnlich schnell wie DRAM, aber dennoch nicht flüchtig – und das bei einem gegenüber Flash/EEPROM immens längeren Datenerhalt und einem niedrigeren Energiebedarf als bei EEPROMs. So sind z. B. die 32-bit-Smartcard-Controller



Bondout-Version des 32-bit Chipkartencontrollers SLE88CFX4002P.

Foto: Infineon



der Hiferron-Serie, die maximal 64 KByte FRAM enthalten, bereits in einem ID-Karten-Projekt in Japan im Einsatz. Innerhalb der nächsten zwei Jahre will Fujitsu bei FRAMs die Preise von EEPROMs erreichen. Der neue 32-bit-Smartcard-Controller AE57C von Renesas verfügt ebenfalls über einen relativ großen Speicher, der allerdings anders aufgeteilt ist als z. B. beim zuvor erwähnten ST-Chip, denn auf dem AE57C befinden sich 132 KByte EEPROM, 320 KByte ROM und 8 KByte RAM sowie ein separates, 2048 Byte großes RAM für den Coprozessor. Dieser Coprozessor unterstützt asymmetrische Algorithmen wie RSA oder Elliptische Kurven mit Schlüssel-Längen von bis zu 2112 bit. Eine separat verfügbare, ACL (Advanced Cryptographic Library) genannte Bibliothek mit sicheren RSA-Berechnungen, unterschiedlichen Hash-Funktionen und Schlüssel-Erzeugung ist ebenfalls verfügbar. Zusätzlich wurde ein neues AES-Hardware-Modul implementiert. Neben den gängigen Sicherheits-Features wie z. B. integrierte Sensoren oder verteiltes Layout hat Renesas auch eine FMU genannte Firewall-Management-Unit, einen Zufallszahlen-Generator und einen Watchdog-Timer auf dem Chip integriert. Ähnliche Wege beschreitet Samsung mit der S3CJ9QD genannten Smartcard, die zusätzlich zum 32-bit-CPU-Core

des Typs SC200 von ARM über 128 KByte EEPROM, 256 KByte ROM und 10 KByte RAM verfügt. Neben einem Krypto-Coprozessor ist auch eine Java-Hardware-Engine auf Basis von ARMs Java-Erweiterung Jazelle zur Ausführung von JavaCard-Bytecode implementiert.

Weitere Infos ...

... zu diesem Thema finden Sie in Form von über 20 Fachartikeln, indem Sie unter www.all-electronics.de nach „Chipkarte“ suchen.

... zum Thema „Sicherheit bei programmierbarer Logik“ erhalten Sie in der nächsten Ausgabe der *elektronik industrie*.

Oftmals ist die Chipkarte nur noch ein Formfaktor, während die eigentlichen Sicherheits-Chips zu über 98 % in andere monolithisch integrierte Systeme übernommen werden. So plant Atmel beispielsweise eine Variante des AT91SC25672RC, die mit einer vollwertigen USB-Schnittstelle ausgerüstet ist, während Infineon auch eine Bondout-Version des 32-bit Chipkarten-Controllers SLE88CFX4002P anbietet, der

400 KByte konfigurierbares EEPROM enthält. Derartige Sicherheits-ICs finden unter anderem in Settop-Boxen Anwendung, wobei das Silizium bei dieser Anwendung in der Regel zu 100 % mit der Chipkarten-Version identisch ist.

Im übrigen teilen sich Atmel, Infineon und National Semiconductor einen wesentlichen Teil des Marktes für TPM-ICs (TPM: Trusted Platform Module), die mehr Sicherheit in PCs bringen sollen, aber von Datenschützern noch kritischer beäugt werden als damals die Seriennummer in den Pentium-Prozessoren. Aus diesem Grund wird die TPM-Funktionalität bisher (noch) nicht genutzt, obwohl bereits einige PCs mit einem entsprechenden TPM-Modul ausgeliefert wurden.

www.atmel.com	Atmel	311
www.fme.fujitsu.com	Fujitsu	312
www.infineon.com	Infineon	313
www.national.com	National	314
www.semiconductors.philips.com	Philips Semiconductors	315
www.renesas.com	Renesas	316
www.samsung.co.kr	Samsung	317
www.sharpsme.com	Sharp	318
www.st.com	STMicroelectronics	319