



Private property

Rapid advancements in lithography continue to enable more functionality to be diffused on to single wafers, fuelling the system on a chip (SoC) era. In reality, of course, there have been examples of SoCs have been around for much longer, in the form of microcontrollers.

The massive appeal of the microcontroller is due largely to the range of peripherals available, even if this does necessitate a wider family selection. But, arguably, the most sought after feature of any microcontroller today is integrated flash memory.

Whilst perfecting the process, the capacity and performance of integrated flash memory rapidly become a key differentiating factor within families, even amongst devices with the same peripheral sets. In the same timeframe, its use also developed; from eeprom replacement for data storage, to eeprom replacement for program memory. Now, flash memory is effectively unified, providing the capacity and performance needed to meet most of the micro's storage needs.

With the novelty wearing off, attention turned to the security of the flash memory

IP protection goes beyond hardware design. By **Philip Ling**.

– both in terms of the program and the data stored. Poaching IP from flash storage is a serious threat in some applications and even for low risk applications, protecting the memory's contents from unintentional alteration or unwanted investigation has always been an issue. So how secure are microcontrollers?

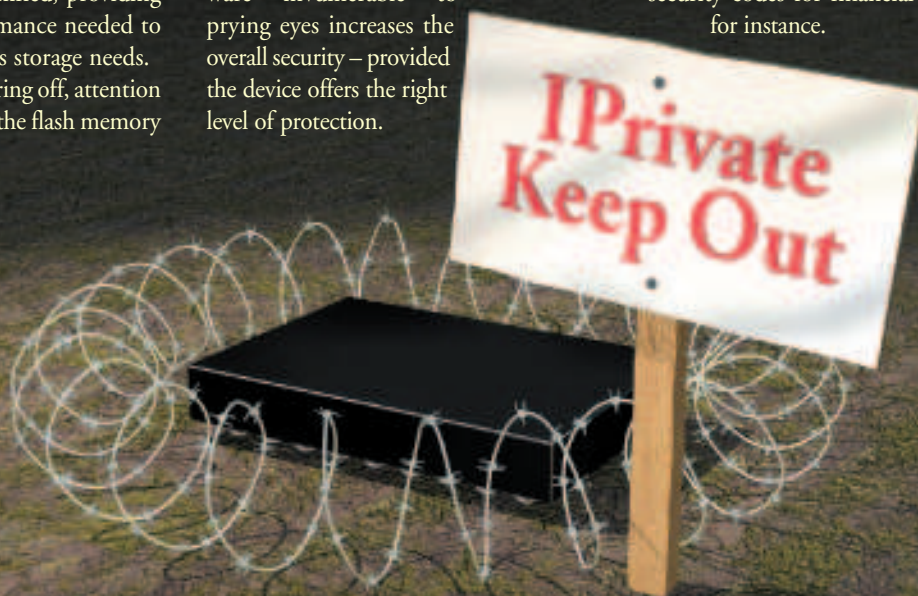
Keep out!

Having the memory diffused in the same silicon as the core obviously offers greater security than specifying a separate memory, but does it necessarily meet the requirements of the very secure conscious?

It's an important consideration; protecting the IP of a hardware design is hard enough, particularly where discrete standard products are used. Making the software invulnerable to prying eyes increases the overall security – provided the device offers the right level of protection.

Securing data/program memory is a serious challenge for microcontroller suppliers; if they offer a built in level of security, it has to work, rather than be an option that users may choose to implement. The challenge is tackled in a number of ways, with both software and hardware approaches apparent.

One issue with a floating gate memory, such as flash, is its complex erase cycle compared to, say, sram. Flash requires a voltage supply to erase its contents and will retain its contents indefinitely when power is removed. To avoid this potential security threat, Maxim offers a range of 8051 compatible microcontrollers that employ non volatile sram instead of flash, along with cryptography techniques to render the secure information 'impervious to hackers'. Added to that, the device also employs measures to erase sram contents upon violation, even if power is removed. That may be extreme, but it could be necessary in some applications, such as those that access security codes for financial transactions, for instance.





In this example, the sram is external to the microcontroller but it employs dedicated program and data memory interfaces with hardwired encryption/decryption engines, with some onchip sram supplied for the most sensitive data. Because its use of external sram with a dedicated battery for data retention may be an issue to some customers, it also offers modular elements.

One of the reasons cited by Maxim for not using floating gate memory is that it can be examined using equipment and techniques that are reasonably easy to source.

removed. Protecting the contents during these 'quiet' periods is a potential security risk and the technique used in many microcontrollers is to use a security bit, which once set inhibits access to the flash memory. Resetting the security bit requires a full flash erase, protecting its contents by removal. Making those security bits less susceptible to hackers is a challenge that silicon vendors will continue to address.

Keeping unwanted visitors in the pc world at bay is aided by firewall technology, which may be a hardware or soft-


attacks; fault injection attacks, and invasive attacks including reverse engineering and microprobing.

Trust me

Another of ARM's technologies targeting secure applications is TrustZone. A relatively new addition to the security world, TrustZone extends beyond smart card applications to offer security for other consumer devices that require memory protection, particularly those using commercial operating systems that aren't necessarily targeted at secure applications, such as Symbian, Linux and Windows CE.

TrustZone technology comprises both hardware and software elements and at the recent 3GSM conference ARM made a number of announcements involving licensees of its TrustZone Software API, notably around digital rights management (DRM) applications. Specifically, ARM announced the release of an Open Media Alliance (OMA) V2 compliant DRM solution based on the TrustZone software framework and API. It's an important issue, as the distribution of digital media increases, suppliers and consumers want to know that what they're supplying isn't falling into the wrong hands – or ears.

"Strong content protection technology enables high quality content rights to be secured and ensures that digital content can be shared freely and securely across mobile phones, pcs and other consumer electronics," said Markku Mehtala, vice president of business development at Beep Science. "By enhancing our mobile DRM solution with ARM TrustZone technology, we enable device manufacturers and operators to deliver rich mobile media content in all forms of devices that consumers expect."

"The OMA DRM standard is paving the way for a seamless DRM enabled digital content ecosystem across consumer devices," said Lance Howarth, general manager, Embedded Software, ARM. "The ARM TrustZone Software greatly increases the robustness of DRM solutions and, together with Beep Science, we can enable the delivery of highly secure and advanced digital products based on TrustZone technology enabled processors." 



The OMA DRM standard is paving the way for a seamless ... digital content ecosystem across consumer devices."

Lance Howarth, **Arm**

Part of the fear here is the use of so called 'lock bits', which may be unlocked by tenacious hackers. For instance, using simple masking techniques and exposure to uv light, Maxim claims that lock bits in eeprom devices can be reset without erasing the entire device, rendering them open to investigation.

It cuts both ways

Necessarily, the double edged sword of non volatile memory is that its contents tend to be sustained when power is

ware solution. In the embedded domain, these solutions aren't quite as abundant. But one example is ARM's SecurCore technology. Atmel's AT91SC range, which implements ARM's SC100 core, is one example of where this feature has been used – and the target is secure smart card applications.

It builds on Atmel's SecureAVR 8/16bit devices, providing a migration path to the more powerful 32bit architecture – at least in terms of security features. Like the Maxim solutions, they offer hardware DES/Triple DES (data encryption standard), as well as a host of other features designed specifically to protect against data raids, including: high/low voltage/frequency detection; illegal op code and access code detection; non invasive attacks; side channel