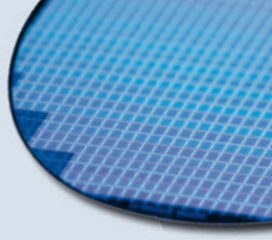
INTEGRITY GUARD

Integrity Guard –

The newest generation of digital security technology

www.infineon.com



Infineon's innovative answer to the highest security requirements

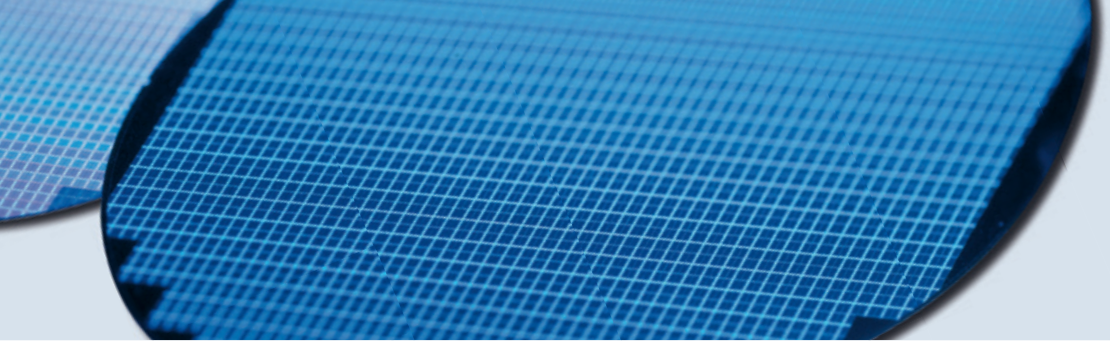
Attacks on security chips have
existed for many years already and they are continuously being refined. For example, attackers use probes to find out what is going on inside the chip or interfere with specific computing functions to illegally access information stored on the chip. Over time, chip manufacturers have continuously integrated more security functions in order to impede attacks. For a long time, chip manufacturers reacted to specific attacks with individual protective measures, such as special sensors. This thinking method no longer meets today's requirements.

Infineon has thus focused on developing a comprehensive, truly scalable security technology. A completely new approach was adopted, which is based on a digital security concept for chip cards and IT applications. The Integrity Guard from Infineon represents the newest generation of security technology and is currently the only one of its kind in the world. The inspiration for the concept was the double helix of a human cell. The idea behind it: every biological cell is comparable to a "secure computer" that must safely store and process genetic information.

Thanks to the totally new scope of their digital security features,
controllers with Integrity Guard meet very high security requirements. Their robust design overcomes the disadvantages of analog security technologies. Full on-chip encryption, including encrypted calculation in the CPU itself and full error-detection capabilities over the complete core architecture provides the basis for the efficient protection of sensitive data against external attacks.

For the challenges on the path toward high security,
a professional approach is necessary in order to evaluate the future of attacks and suitable countermeasures. When developing new product families, the planned and anticipated lifetime needs to be kept in mind. As is the case for electronic passport chips, there is often a span of ten to fifteen years between the design and end of the product's lifetime in the field.

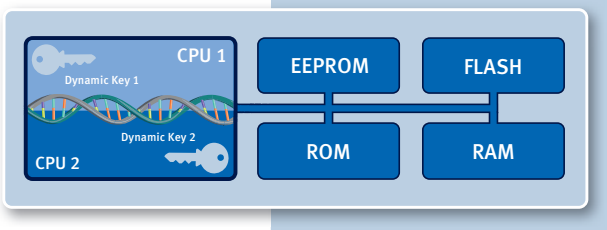
Infineon's own security laboratories therefore focus on researching what will appear next in terms of known or even completely new attack scenarios. Localized attack methods aim at finding secret keys in the very heart of a chip – the CPU. Unencrypted CPUs make access to sensitive data easier; they can be analyzed by an attacker using today's state-of-the-art methods, such as optical emission analysis or electromagnetic emanation attacks. It has been shown that conventional, scenario-specific countermeasures not only drive the cost spiral upwards, and lead to tedious security updates, but no longer serve the requirements of applications with a high security demand.



The innovative solution

Full error detection

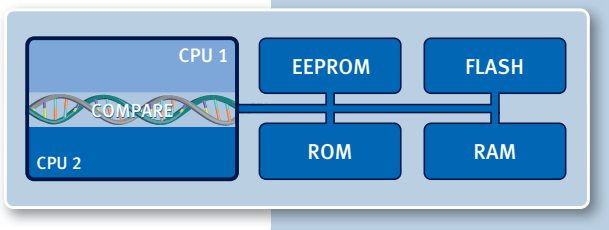
Integrity Guard security chips are the first of their kind to be equipped with a full error detection capability for the complete data path. A dual CPU approach allows error detection even while processing – the CPUs constantly check each other to establish whether the other unit is functioning correctly. Relevant attack scenarios can be detected, whereas things that would not lead to an error are more or less ignored. Thus the risk of false alarms – a significant disadvantage in conventional solution concepts – is significantly reduced. The approach includes error detection and correction throughout the entire system.



CPU-internal encryption using different dynamic keys

Total encryption

The security controllers with Infineon's Integrity Guard will be equipped with full encryption over the complete CPU core and the memories – meaning no more plain data is left on the chip. It is the first time ever in commercial security controllers that the two CPUs have utilized fully hardware-encrypted calculation, and with different dynamic secret keys. This process is only possible because the CPUs have been implemented from scratch by Infineon, which allows the integration of real encrypted operations.



The Dual-CPU processor core allows comprehensive error detection

Signal protection

In signal protection, the main objective is to reduce to the minimum the attractiveness of the signals for the attacker. This is done by means of full encryption. Attackers can neither manipulate nor eavesdrop on encrypted signals. Nevertheless, in every chip there are signals that are more important than others, so an Infineon-specific shielding, combined with secure wiring, has been developed. With this method, first all the signals are classified according to their value for the attacker. In a second step, during the design of the chip, the more interesting signals are automatically routed under less valuable lines. Subsequently, an intelligent shielding algorithm finishes the upper layers, completing the so-called I^2-shield.

Integrity Guard

The advantages

Integrity Guard offers a multitude of important advantages, which fully pay off in the development of secure products.

Customer-friendly security
Today, providing top-level security often means investing great effort and high costs – not only for the chip manufacturer, but also for the application developers. Adding security often decreases flexibility in conventional applications. In Infineon's security controllers with Integrity Guard technology, almost all security features are automated. "Customer-friendly security" means that security features are easy to use and engender confidence along the entire value chain – from chip manufacturer and chip card manufacturer to system integrators and the customer. This customer-friendly security results in significantly lower overall costs over the product life cycle

Digital robust security
Thanks to their robust design, security chips with Integrity Guard technology can also be used in difficult and demanding environments. Their digital features neither have to be adjusted nor calibrated, which makes the chips even more resistant. Conditions that do not directly harm the chip itself will therefore not affect its correct functioning.

Mathematically modeled security
Error-detection codes and digital security features can be mathematically modeled. This facilitates the security evaluation and certification both internally and when performed by third parties.

Self-checking security
Security chips with Integrity Guard have self-controlling security mechanisms. The most important element is the comprehensive digital error detection over the complete core architecture, including memories, buses, caches, and the dual CPU.

Attack-repellent
The design of the security chips alone impedes attacks. Full encryption is used for CPU, memories, and buses, covering all stored, processed, and transferred data. These mechanisms are automated and facilitate the software implementation and use.

INTEGRITY GUARD

Integrity Guard is a digital security technology developed by Infineon. Infineon has been developing innovative solutions in the area of chip-based security for over 25 years and has been a global market leader for the last 15 years. Integrity Guard was developed especially for applications that require particularly high-level data security and resilience for a particularly long term of life. Important fields of application for Integrity Guard include governmental identity cards as well as bank and credit cards, in which Integrity Guard sets the technological standard for chip-based security. Security controllers are also used increasingly in numerous networked systems, such as computers, IT infrastructures, industrial control systems, and critical infrastructure systems. In these applications, Integrity Guard plays a decisive role in securing the entire system.

Order Number: B181-H9754-X-X-7600
Date: September 2012