

Integrity Guard

The smartest digital security technology in the industry

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 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 approach no longer meets today's requirements.

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

Thanks to digital security features, controllers with Integrity Guard meet very high security requirements. Their robust design overcomes the disadvantages of analog security technologies. A fully encrypted data path, including encrypted calculation in the CPU itself and full error-detection capabilities throughout the complete core architecture, including memories, buses, caches and the dual CPU, provides the basis for the efficient protection of sensitive data against attacks.

Future-proof security requires the professional evaluation of future attacks and the development of 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 phase and the end of the product's lifetime in the field.

At Infineon's own security laboratories, the focus is on localized attack methods aimed at exposing secret keys stored at 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 also no longer serve the requirements of applications with a high security demand.

The innovative solution

Full error detection

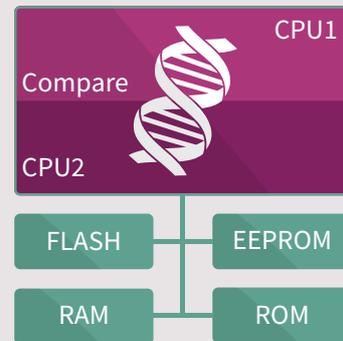
Integrity Guard security chips were the first of their kind to be equipped with a full error detection capability for the complete data path. A dual CPU approach allows error detection even while processing – the CPUs constantly check each other to establish whether the other unit is functioning correctly. 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. This approach includes error detection and correction throughout the entire system.

Total encryption

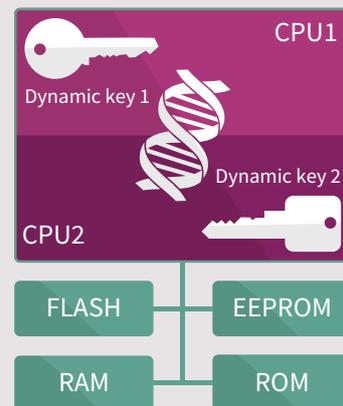
Security controllers with Infineon's Integrity Guard are equipped with full encryption throughout the entire CPU core and the memories – meaning no more plain data is left on the chip. It is the first time ever in commercial security controllers that the two CPUs utilize fully hardware-encrypted calculation, and have 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.

Signal protection

In signal protection, the main objective is to minimize the attractiveness of the signals for the attacker. This is done by means of full encryption. Attackers are hindered from manipulating or eavesdropping on encrypted signals. Nevertheless, in every chip there are signals that are more important than others, so Infineon developed a specific shielding with secure wiring. 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 underneath less valuable lines. Subsequently, an intelligent shielding algorithm finishes the upper layers, completing the so-called I²-shield.



The dual-CPU processor core allows comprehensive error detection



CPU-internal encryption using different dynamic keys

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 at a high financial cost – 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 create 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

Robust digital security

Thanks to their robust design, security chips with Integrity Guard technology can also be used in more difficult and demanding environments. Their digital features require neither adjustment nor calibration, 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 throughout the complete core architecture, including memories, buses, caches and the dual CPU.

Attack-repellent

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



Integrity Guard

Integrity Guard is a digital security technology developed by Infineon. Infineon is a leader in chip-based security technologies with 30 years of experience and in-depth system competence. Integrity Guard was developed especially for applications that require exceptionally 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.

Infineon Technologies AG

81726 Munich
Germany

Published by
Infineon Technologies AG

© 2018 Infineon Technologies AG.
All rights reserved.

Order number: B181-I0677-V1-7600-EU-EC
Date: 06 / 2018

www.infineon.com

