

Physics | Technology Offer

Process and Hardware Implementation for the Generation of Reproducible Secret Keys in Lithographic Production Processes

Market Opportunities

The innovative aspect of the encryption process presented here is that it does not require the storage or transmission of secret keys and thus the process achieves a new level of security.

Traditional methods of encryption generate a secret key by means of a random number generator and store this key within the encryption system, for example on the hard drive or in an EEPROM. Using analytical processes, such copies can be discovered and read. The need to transmit the secret key frequently represents a further significant risk factor.

To mitigate these risks, processes are necessary which for example continually generate new keys or generate the keys *a priori* and separate from the encryption system. Such processes are in general resource intensive, expensive and nevertheless not sufficiently secure. The technology presented below offers an excellent alternative.

About the Process

The invention consists of a method for the generation of reproducible secret keys in products which were manufactured by means of lithographic production processes, such as chips.

In the first application, a random number generator is being produced that depends on the physical characteristics of a chip which vary slightly and are thus random. The reproducibility comes from the fact that these parameters while variable from product to product remain constant during the life of the product.

By this means, a random number generator is created that has the characteristics of being reproducible and nevertheless is very difficult to read, measure, simulate or determine from the outside. The reproducibility is independent of the applied voltage, temperature, age and usage.

This innovation can preferentially be realized in the form of a microelectronic circuit on a chip. The parasitic capacitances between certain areas of the chip lay-out are transformed into a bit map from which a secret key is determined.

Advantages of the Innovation

- No local copies of the secret key is necessary
- No exchange of secret keys is necessary
- Long keys, suitable for Public Key processes, can be generated (> 1024 Bit)
- Simple principle
- Key can only be obtained using very substantial effort, even if the underlying generation process is known
- Hacker attacks cannot succeed

Broad Field of Application

- Authorization and access control (All-Chips Key)
- Smart-Card applications
- Transmission and distribution of multi media content (Single Chip Keys)
- Protection of software and trusted computing (All Chips Key and Single-Chip Keys)
- Configuration in FPGAs

The preferred circuit is designed in a way which ensures that the bit map is very sensitive to variations in capacitance. A small difference in capacitance between two otherwise identical chips thus results in different bit maps. (**Single Chip Keys**). This is the inevitable result of statistical process variations which occur during the manufacture of the product.

If one wants all chips to produce an identical key, the capacitances and the lay-out is selected in such a way as not to be susceptible to process variations. This second application represents a way to engrave a fixed, invisible key in all chips of a given series, rather than creating a random number generator (**All Chips Key**).

Applications in the Security Field

The invention can be implemented in the semi-conductor and chip industry which uses lithographic methods .

Authorization and Access Control

The invention can for example be used in the manufacture of remote control keys for cars. The random number generated by the chip together with the serial number of the car provides a unique secret key. This key produces a random bit sequence for each car and remote key combination. Authorization is effected by generating and exchanging this unique bit sequence during each locking or unlocking.

Smart Card Application

The process is suitable for all applications where an authorization or access control is required. Using an All-Chips-Key allows the authenticity of smart cards to be established.

A known example in digital television (Premiere) is the use of a smart card in digital receivers whereby the smart card provides a fixed key necessary for the decryption of the video data.

Transmission and Distribution of Multi Media Content (Single Chip Keys)

In this application, the invention secures the transmission and distribution of multi media content (for example music or video streaming on the internet) by ensuring that the content can only be played on a certain equipment, and not any third party equipment.

By checking the authenticity it is possible to ensure that all public keys sent to the content provider actually emanate from the multi media equipment and were not produced by the user himself (All Chips Key).

For Protecting Software and Trusted Computing (All Chips Key and Single Chip Keys)

In this application, the aim is to ensure that software is only executed on a system if the software was authorized. The use of a Single-Chip Key can achieve such a copy protection.

The ideal outcome, providing maximum flexibility and security, is obtained by a combination of All-Chips Keys and Single-Chip Keys. Single-Chip Keys identify each processor in a unique way, so that programs and in particular multi media content can only be played on authorized equipment.

The All-Chips Key on the other hand authenticates the processors (i.e. Single-Chip Keys) and makes it possible to keep certain parts of the software inaccessible to the user which provides protection against reverse engineering and user manipulation of the software code.

Configuration in FPGAs

The present invention allows improved protection of internally realised circuits in FPGAs from detection. The programming of an EPGA would always be in an encrypted form which would only be decrypted in the FPGA.

Patent Portfolio

German patent application DE 10 2005 024 379 A1
International applications
EP 1 897 139 and US 2009/0304181 A1

Technology Transfer

The invention was made by the Institute for Information Technology at the University of Mannheim. The TLB GmbH has been charged with the commercialization and now offers companies the opportunity to obtain a license to manufacture and sell this new and promising technology.

Laboratory Prototype

A prototype is currently being built. Collaborative work with the Institute to develop this technology further is possible.

For further information, please contact:

Thomas Schurr
tschurr@tlb.de
Technologie-Lizenz-Büro (TLB)
der Baden-Württembergischen Hochschulen GmbH
Ettlinger Straße 25, D-76137 Karlsruhe
Tel. +49 721 79004-0, Fax +49 721 79004-79
info@tlb.de, www.tlb.de