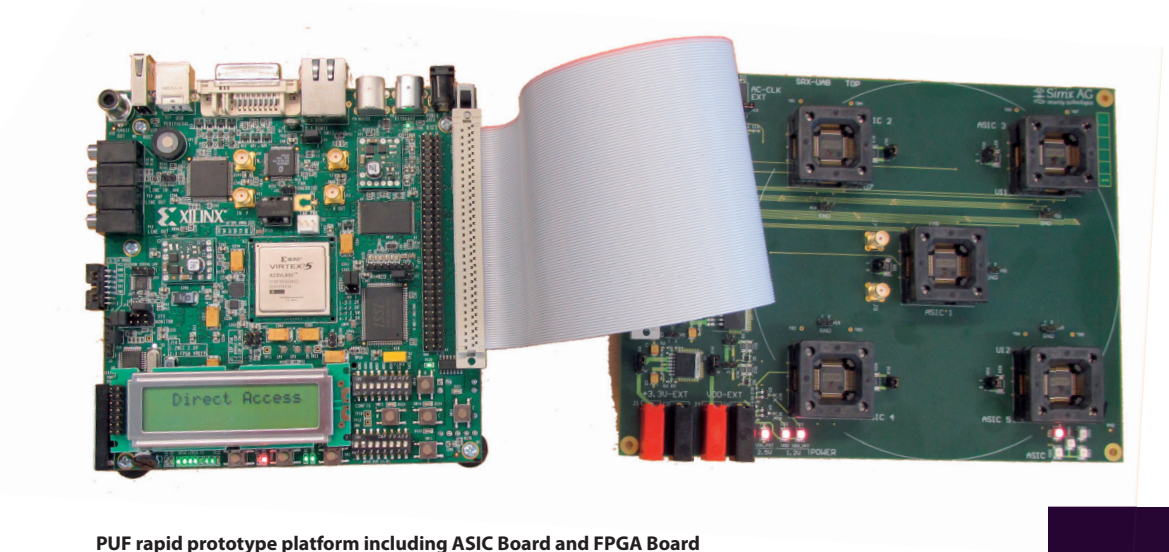
unique

Newsletter
October 2011

Project number: **238811** Project web-site: **www.unique-security.eu** Project start: **September 1, 2009** Project duration: **33 months**



PUF rapid prototype platform including ASIC Board and FPGA Board

UNIQUE project sets new standard for quality in PUF research

Security mechanisms using Physically Unclonable Functions (PUFs) are an essential part of hardware intrinsic security. Hardware intrinsic properties, which are the basis of PUFs, are very similar in nature to human biometrics and can be seen as the specific fingerprint of an electronic circuit.

Due to deep-submicron manufacturing process variations, components (like transistors, delay lines) in a chip have slightly different physical properties that lead to measurable differences. Since these process variations are uncontrollable during manufacturing it is very hard, expensive and economically not viable to create on purpose a device with a given fingerprint. PUF implementations require electronic circuits that measure the responses of hardware to certain given inputs or challenges. These responses depend on the specific physical properties of the device. Hence PUFs are physical functions which are easy to challenge and whose response is easy to measure, but very hard to reproduce by construction. Major applications of PUFs are deriving device unique cryptographic keys and device identifiers or authentication primitives for protection against cloning of data and counterfeiting of devices.

In the UNIQUE project, the research on PUFs has recently reached a new milestone. This milestone has been achieved by the production of an ASIC, specifically designed for research purposes within the project, which contains the implementations of six different PUF types. Never before has an IC been produced that contains this many different PUF implementations, which makes this chip the perfect platform to objectively evaluate the performance and requirements of the different PUFs. This objective assessment will be performed by researchers from academia and industry, gathered in the European funded UNIQUE project. The ASIC is the product of joined efforts by designers from different partners in UNIQUE and has been produced in 65nm technology at TSMC through IMEC and Europractice's mini@sic program, which is specifically intended for universities and research labs to prototype designs on MPW runs. Initial testing performed on the UNIQUE ASICs has shown that all PUF implementations are operational and can therefore be used in the forthcoming evaluations.

The PUF types implemented in the ASIC can be divided into two categories based on their operating principles. The chip contains several variants of memory-based PUFs, which make use of the unpredictable start-up behavior of uninitialized

PHOTO: Technikon

Martina Truskaller, editor

Editorial

Dear reader,

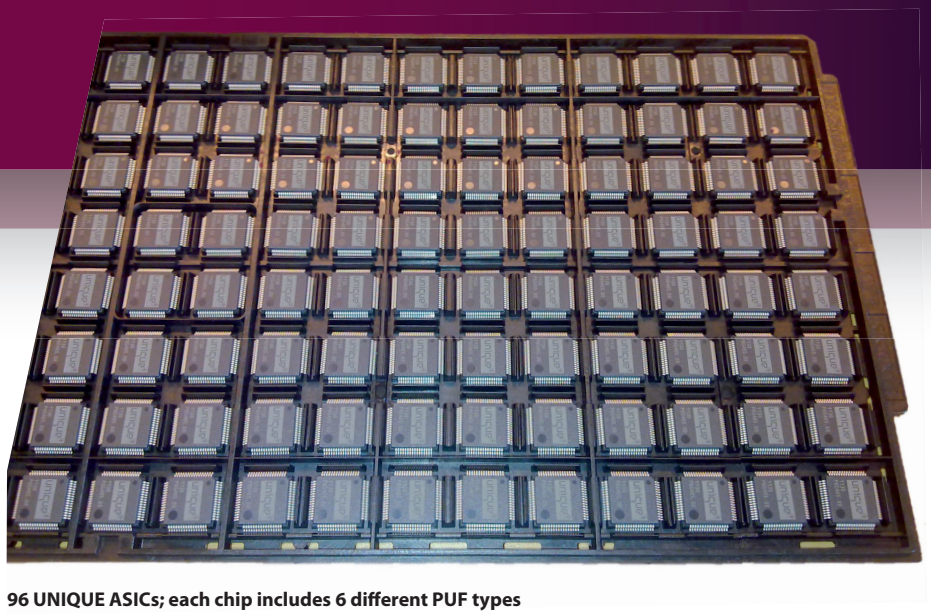
The UNIQUE newsletter is intended to offer you information on interesting activities and results of the project. This issue features an article on new standards for quality in PUF research set within UNIQUE, provided by Vincent van der Leest from Intrinsic-ID.

Further, recent and upcoming events are listed, which are of interest to the UNIQUE project.
I hope the content of this issue is of interest to you. Any feedback is warmly welcome.

About UNIQUE

UNIQUE - Foundations for Forgery-Resistant Security Hardware - aims at developing novel hardware components that can be uniquely identified in order to avoid unauthorised malicious counterfeiting.

The project is running for 33 months from September 2009 until May 2012, and it is co-financed by the European Commission under EU Framework Programme FP7. The project consortium consists of two leading universities, two research SMEs and three large microelectronics companies from six European countries.



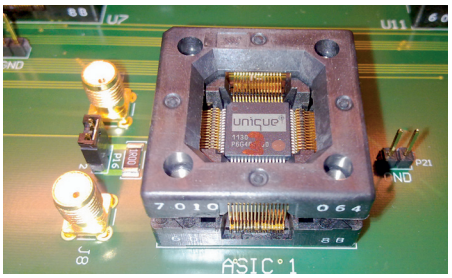
96 UNIQUE ASICs; each chip includes 6 different PUF types

memory cells. These PUFs are in practice mainly applied for secure key generation and storage solutions. The second category consists of delay-based PUFs that derive their unique challenge-response behavior from the randomness present in the delay of logic circuits.
Within UNIQUE, the research on the different PUFs from the ASIC (which will result in extensive documentation) will focus on several important practical aspects of PUF implementations:

- Reliability (how do PUFs perform under varying external conditions)
- Uniqueness (how much entropy do different PUF types contain)
- PUF requirements (area and power consumption, design constraints, etc.)
- Robustness of PUFs against several invasive and non-invasive attacks

Furthermore, the ASICs will be used to create demonstrators of cryptographic security solutions utilizing the PUFs' hardware intrinsic fingerprints.

Article source: Vincent van der Leest (Intrinsic-ID)



UNIQUE ASIC on the ASIC Board

RECENT EVENTS

September 15th to 16th
Leuven, Belgium

TU Darmstadt co-organized the Workshop on Trustworthy Embedded Devices (TrustED) that took place in Leuven from September 15th to 16th. One of the main topics of this workshop was hardware-based security, in particular PUFs. Detailed information about the workshop can be found at

http://trusted.trust.cased.de/

September 28th to October 1st
Nara, Japan

TU Darmstadt has presented a joint paper with Intrinsic-ID on "Recyclable PUFs: Logically Reconfigurable PUFs" at the top-conference on hardware security, the Workshop on Cryptographic Hardware and Embedded Systems (CHES) 2011, which has taken place in Nara, Japan from September 28th to October 1st this year.

UPCOMING EVENTS

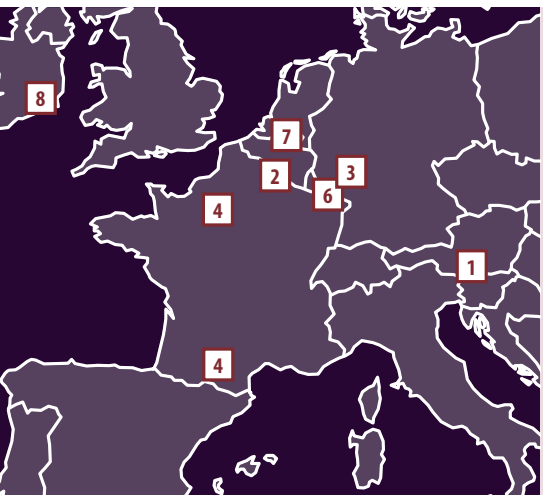
October 18th 2011
Chicago, USA

Intel will present a joint paper with Intrinsic-ID on "Logically Reconfigurable PUFs: Memory-Based Secure Key Storage" at the ACM workshop on Scalable Trusted Computing on October 18th 2011in Chicago, USA.

October 26th to 28th 2011
Tallinn, Estonia

Intrinsic-ID will present a paper on "Comparison of SRAM and FF PUF in 65nm technology" at the NordSec conference on October 26th to 28th 2011 in Tallinn, Estonia.

unique



Consortium:

1. **Technikon Forschungs- und Planungsgesellschaft mbH (Austria)**
2. **Katholieke Universiteit Leuven (Belgium)**
3. **TU Darmstadt (Germany)**
4. **Thales Communications & Security S.A. (France), two locations**
6. **Sirrix AG (Germany)**
7. **Intrinsic-ID (Netherlands)**
8. **Intel Performance Learing Solutions Limited (Ireland)**

Contact:

UNIQUE Project Coordination Team
Martina Truskaller
Technikon Forschungsgesellschaft mbH
Burgplatz 3a, A-9500 Villach
Tel.: +43 4242 233 55-0
Fax: +43 4242 233 55-77
E-Mail: coordination@unique-security.eu
Web: **www.unique-security.eu**

SEVENTH FRAMEWORK PROGRAMME

TECHNIKON