unique

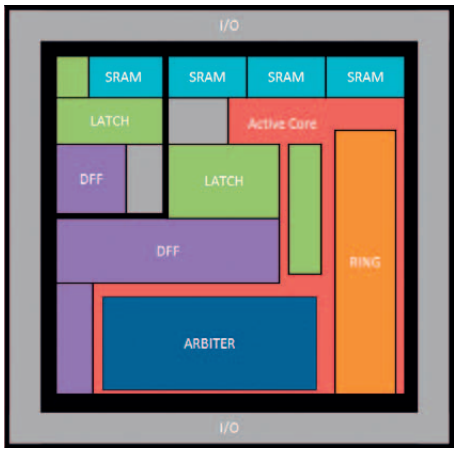
Newsletter
March 2011

Project number: **238811** Project web-site: **www.unique-security.eu** Project start: **September 1, 2009** Project duration: **2,5 years**

UNIQUE ASIC development

The UNIQUE project is in the process of investigating and developing integrated solutions to protect hardware systems against counterfeiting, cloning, reverse engineering, tampering, and insertion of malicious components. This is accomplished through a combination of innovative hardware based security primitives with cryptographic protocols and algorithms and by applying secure design and evaluation principles.

An important aspect in the UNIQUE project is the development of an ASIC, which has been specifically designed by the involved project partners. This ASIC will be manufactured by the Europractice IC Service under their mini@sic program. For this program Europractice has selected several MPW runs in different technologies on which universities and research labs can prototype small designs. The UNIQUE ASIC is manufactured in TSMC's 65nm CMOS technology.



Floorplan of the UNIQUE ASIC design

The purpose of this ASIC development is to investigate and demonstrate how Physically Unclonable Functions (PUFs) can be used to protect hardware systems. Several types of hardware intrinsic PUFs are implemented on the device. Furthermore, an "active core" is included which produces different amounts of switching activity and allows to simulate realistic operating conditions.
Besides the active core and a test interface, the ASIC contains several blocks which implement different types of PUF constructions, as shown in Figure 1. The implemented PUF types can be divided into two categories based on their operating principles. The chip contains three variants of memory based PUFs which make use of the unpredictable start-up behavior of uninitialized memory cells: the SRAM PUF, the flip-flop PUF and the latch PUF. These are mainly applied for secure key generation and storage solutions. The second category consists of two delay based PUF implementations that derive their unique challenge-response behavior from the randomness present in the delay of logic circuits: the ring oscillator PUF and the arbiter PUF.

A major research focus of the UNIQUE project is to evaluate different practical and security properties of PUFs. With this ASIC development, different types of PUFs are implemented together in the same technology and on the same platform for the first time. This allows to make a truly objective and realistic comparison of their performance, efficiency and security. Furthermore, several PUF based application scenarios will be implemented for demonstration and research purposes by the UNIQUE consortium. The cryptographic and security primitives required for these prototypes will not be part of this IC but are implemented separately. Finally, the physical security of the implementations will be thoroughly evaluated by assessing the outcome of several non-invasive and invasive attacks.

**Article source: Vincent van der Leest, Intrinsic-ID;
Roel Maes, KU Leuven;
Erik van der Sluis, Intrinsic-ID**

PHOTO: Technikon

Niina Uusitalo, editor

Editorial

Dear reader,

The UNIQUE newsletter is intended to offer you information on the interesting activities and results of the project. In this first issue the focus is on the first-hand report about UNIQUE ASIC design, provided by Vincent van der Leest, Roel Maes and Erik van der Sluis.

Further, you can read the short report on how UNIQUE was represented at the CeBIT 2011 by TU Darmstadt. The upcoming events are also listed for you to have a clear view of the future conferences and fairs, where some of the UNIQUE results will be presented.

I hope the content of this issue is of interest to you. Any feedback is warmly welcome.

UNIQUE at CeBIT 2011, Heart of the digital World

TU Darmstadt represented the UNIQUE project at the world's largest international exhibition for information and communication technology, CeBIT 2011, which took place in Hannover, Germany, 1.-5. of March. The UNIQUE promotion video was shown to the public and it inspired many interesting discussions with industry representatives and other visitors, who were all very interested in the research and the results of the UNIQUE project.

The UNIQUE promotion video is available at YouTube:

www.youtube.com/watch?v=UG42aBGN2bg

PHOTO: TU Darmstadt

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 30 months from September 2009 until February 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 major electronics companies from six European countries.

UPCOMING EVENTS

IEEE GLSVLSI 2011
Lausanne, Switzerland
May 2-4, 2011

KU Leuven is invited to keep a presentation on intrinsic PUFs at the IEEE GLSVLSI 2011 conference in Lausanne.

IEEE Symposium on Security and Privacy 2011
California, USA
May 22-25, 2011

TU Darmstadt and KU Leuven will present a paper on formal security modeling of PUFs at a flagship security conference, IEEE Symposium on Security and Privacy 2011.

WISTP 2011
Heraklion, Greece
June 1-3, 2011

Intrinsic-ID gives a keynote presentation on "New Developments in Hardware Intrinsic Security " at the WISTP 2011 conference.

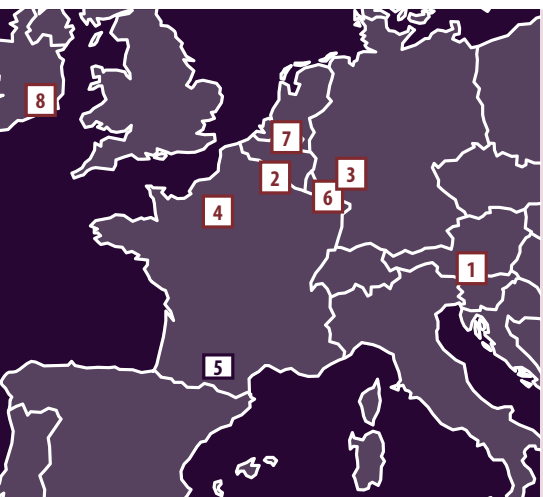
WiSec 2011
Hamburg, Germany
June 15-17, 2011

TU Darmstadt will publish a paper on PUF-based remote attestation, i.e., a PUF-based protocol that allows verifying the integrity and authenticity of a remote embedded device, at a renowned conference on wireless network security, WiSec 2011. Moreover, KU Leuven will give an invited talk at this conference.

„UNIQUE offered me a great opportunity to work with the experts in PUF technology and inspired me to write a Master Thesis on Cryptographic Applications with Physically Unclonable Functions."

Martin Deutschmann, Technikon

http://www.unique-security.eu/downloads/UNIQUE-238811-Master-Thesis-MD.pdf



Consortium:

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

Contact:

UNIQUE Project Coordination Team
Niina Uusitalo
Technikon Forschungsgesellschaft mbH
Burgplatz 3a, A-9500 Villach
Tel.: +43 4242 23355 – 0
Fax: + 43 4242 23355 - 77
E-Mail: coordination@unique-security.eu
Web: **www.unique-security.eu**