D5.3 Final Report for the use and dissemination of foreground

Project number:	238811
Project acronym:	**UNIQUE**
Project title:	Foundations for Forgery-Resistant Security Hardware
Start date of the project:	01.09.2009
Duration:	33 months

Deliverable type:	Report
Deliverable reference number:	238811/ D5.3 / FINAL | 1.0
Deliverable title:	Final Report for the use and dissemination of foreground
WP contributing to the deliverable:	WP5
Due date:	2012-02-29 (M30)
Actual submission date:	2012-02-29

Responsible organisation:	TEC
Authors:	TEC (Franziska Andratsch, Martina Truskaller) with contributions from all UNIQUE partners
Abstract:	The aim of this deliverable is to give an overview of all dissemination and exploitation activities of all project partners already done during the Unique project. The report also includes a section detailing how the consortium intends to exploit the project in the future with regard to new products and services.
Keywords:	Dissemination, Exploitation, Results, Foreground

Dissemination level:	Public
Revision:	FINAL | 1.0

Instrument:	STREP
Thematic Priority:	ICT

Table of Contents

1 Executive Summary

On the one hand the purpose of this deliverable D5.3 "final report for the use and dissemination of foreground" is to give an overview of the dissemination and exploitation activities done during the whole project by all project partners.

These activities have been very important to raise the awareness and publicity of the UNIQUE project as well as its outcome in order to make UNIQUE a successful and sustainable project. So in its first part this report shortly describes all dissemination activities (dissemination measures, list of scientific publications and other dissemination activities).

On the other hand this deliverable presents which exploitation activities were done by each of the partners until now and what are their results and which activities are planned for the future in particular with regard to new products and services. The main focus is the use and dissemination of foreground and the approach by the partners to intend to exploit the project to enable a maximum impact on the European security market.

Finally this deliverable presents a short overview of the cooperation with external cooperations or other projects/programmes.

2 Use and dissemination of foreground

Exploitation and dissemination activities are essential to implement and transfer the technology developed within the project as well as to maximize the benefits for the project partners. Carefully planned dissemination and exploitation strategies are an imperative for a successful project lifecycle. While dissemination activities already started right from the beginning of the UNIQUE project, exploitation activities more or less centre on the project`s results gained during the last project phase and beyond, to reach sustainability after the project has closed. Sustainability related to the UNIQUE project means that the developed products will be used as the basis for further research activities and additionally, that the products will be used in real corporate creativity contexts. Exploitation describes all activities which are done to promote, exploit and commercialize the research results gained during the project`s lifetime. Scientists need to always keep in mind the usability of research results, the possibility for their application in different areas, and their relevance for the community.

To ensure that adequate exploitation activities are performed, it is important that any project consortium starts to elaborate on potential exploitation possibilities already before the project starts and should develop an exploitation concept or plan. Market analyses help to ascertain what the customer preferences are, thereby assisting in finding out if the customers need, want and will accept the new technology.

For inventions/innovations with high exploitation potential it is common practice to create a business plan pointing out the advantages of the new technology, possible areas of application, its market potential as well as possibilities for commercial exploitation. Project results that can be transferred into marketable products in a very short period of time, offer the possibility to generate huge competitive advantages and thereby helping to generate considerable profits. Here, it is important to establish respective management structures which ensure that IPRs and project achievements are adequately protected and exploited.

2.1 Dissemination Measures

Dissemination represents a key part within any research project since the awareness and publicity of a project is important to ensure the project success. For this reason dissemination activities have been provided to ensure the visibility and awareness of the UNIQUE project and to support the widest adoption of its results in industry and research. The goal of dissemination activities within the UNIQUE project was to spread the technological and scientific achievements to the widest possible audience. The target groups for external dissemination activities in the UNIQUE project were on the one hand the general public and on the other hand potential business partners as well as specific scientific experts. A further target audience were public institutions like governmental and European audiences. It has to be considered that not every dissemination activity could target all of these groups simultaneously; hence to appeal a specific audience the differences between the groups need to be recognised and addressed when preparing a dissemination activity.

To ensure efficient and effective work in the field of dissemination the UNIQUE partners developed at the beginning of the project a dissemination plan based on a form collected from each partner, with the purpose to gather information on all the dissemination activities. This dissemination plan contained both the strategies and activities of the consortium in general as well as the individual dissemination approaches of the partner organisations. The preparation of this dissemination plan was part of Work Package 5 (D5.2), "Project dissemination plan". It described the dissemination channels to be used and the dissemination material to be produced and indicated their schedule. So the dissemination plan gave an overview via the various activities and enabled their coordination. At this point it is important to note, that the focus of the mentioned dissemination activities of the UNIQUE partners was in the first half of the project. The reason for this was in the impreciseness of planning of activities that are lying ahead. So this dissemination plan can be regarded as a guideline and was supplemented in the course of the project duration. The purpose was to coordinate and plan the dissemination activities on consortium and partner level because one of the goals of the UNIQUE project was to widely disseminate the results at different levels. The dissemination activities ensured that the public is aware of the project, interested parties are able to learn about the project and have access to up-to-date information.

In addition to the UNIQUE project the partners do or did participate also in many other EC or national research projects. These relationships created and will create opportunities to disseminate the UNIQUE results and help to make sure that the partners are always aware of the latest results and developments in related areas.

Hereafter, a list of all scientific (peer reviewed) publications relating to the foreground of the project as well as a list of all dissemination activities (publications, conferences, workshops, web sites/applications, press releases, flyers, articles published in the popular press, videos, media briefings, presentations, exhibitions, thesis, interviews, films, TV clips, posters) will be given. These tables are cumulative, which means that they show all publications and activities from the beginning until after the end of the project.

2.1.1 List of scientific (peer reviewed) publications, starting with the most important ones

This table is cumulative, which means that it shows all publications from the beginning until after the end of the project!

Title	Main author	Title of the periodical or the series	Number, date or frequency	Publisher	Place of publication	Year of publication	Relevant pages	Permanent identifiers (if available)[1]	Is/Will open access [2]provided to this publication?
Anonymizer-Enabled Security and Privacy for RFID	A.-R. Sadeghi, I. Visconti, C. Wachsmann; (RUB)	In 8th International Conference on Cryptology And Network Security (CANS)	Volume 5888 of LNCS	Springer	Kanazawa, Ishikawa, Japan	2009	134-153	http://dx.doi.org/10.1007/978-3-642-10433-6_10	No
Future of assurance: Ensuring that a System is Trustworthy	A.-R. Sadeghi, I. Verbauwhede, C. Vishik; (RUB, KULEUVEN, INTEL)	ISSE 2009 Securing Electronic Business Processes	---	Vieweg + Teubner	The Hague, Netherlands	2009	339-349	http://dx.doi.org/10.1007/978-3-8348-9363-5_34	No
Random Number Generators for Integrated Circuits and FPGAs	B. Sunar, and D. Schellekens; Editor: I. Verbauwhede; (KULEUVEN)	In Secure Integrated Circuits and Systems, Integrated Circuits and Systems	---	Springer	USA	2010	107-124	http://dx.doi.org/10.1007/978-0-387-71829-3_6	Yes

[1] A permanent identifier should be a persistent link to the published version full text if open access or abstract if article is pay per view or to the final manuscript accepted for publication (link to article in repository).

[2] Open Access is defined as free of charge access for anyone via Internet. Please answer "yes" if the open access to the publication is already established and also if the embargo period for open access is not yet over but you intend to establish open access afterwards.

Title	Main author	Title of the periodical or the series	Number, date or frequency	Publisher	Place of publication	Year of publication	Relevant pages	Permanent identifiers (if available)[1]	Is/Will open access [2]provided to this publication?
Process Variations for Security: PUFs	R. Maes, and P. Tuyls; Editor: I. Verbauwhede; (KULEUVEN, IID)	In Secure Integrated Circuits and Systems, Integrated Circuits and Systems	---	Springer	Leuven, Belgium	2010	125-143	http://dx.doi.org/10.1007/978-0-387-71829-3_7	No
Physically Unclonable Functions: a Study on the State of the Art and Future Research Directions	R. Maes, and I. Verbauwhede; Editor: D. Naccache, and A. Sadeghi; (KULEUVEN)	In Towards Hardware-Intrinsic Security, Security and Cryptology	Information Security and Cryptography	Springer	---	2010	3-37	http://dx.doi.org/10.1007/978-3-642-14452-3_1	No
Enhancing RFID Security and Privacy by Physically Unclonable Functions	Ahmad-Reza Sadeghi, Ivan Visconti, and Christian Wachsmann; Editor: D. Naccache, and A. Sadeghi; (RUB / TUD)	In Towards Hardware-Intrinsic Security, Security and Cryptology	Information Security and Cryptography	Springer	---	2010	281-305	http://dx.doi.org/10.1007/978-3-642-14452-3_13	No
Efficient Secure Two-Party Computation with Untrusted Hardware Tokens (Full Version)	K. Järvinen, V. Kolesnikov, A.-R. Sadeghi, T. Schneider; Editor: D. Naccache, and A. Sadeghi; (RUB)	In Towards Hardware-Intrinsic Security, Security and Cryptology	Information Security and Cryptography	Springer	---	2010	367-386	http://dx.doi.org/10.1007/978-3-642-14452-3_17	No

Title	Main author	Title of the periodical or the series	Number, date or frequency	Publisher	Place of publication	Year of publication	Relevant pages	Permanent identifiers (if available)[1]	Is/Will open access [2]provided to this publication?
Memory Leakage-Resilient Encryption based on Physically Unclonable Functions	F. Armknecht, R.Maes, A-R. Sadeghi, B. Sunar, P. Tuyls; Editor: D. Naccache, and A. Sadeghi; (RUB, KULEUVEN, IID)	In Towards Hardware-Intrinsic Security, Security and Cryptology	Information Security and Cryptography	Springer	---	2010	685-702	http://dx.doi.org/10.1007/978-3-642-10366-7_40	No
Strong PUFs: Models, Constructions and Security Proofs	U. Rührmair, H. Busch, S. Katzenbeisser; Editor: D. Naccache, and A. Sadeghi; (TUD)	In Towards Hardware-Intrinsic Security, Security and Cryptology	Information Security and Cryptography	Springer	---	2010	79-96	http://dx.doi.org/10.1007/978-3-642-14452-3_4	No
Recyclable PUFs: Logically Reconfigurable PUFs	Stefan Katzenbeisser, Ünal Kocabas, Vincent van der Leest, Ahmad-Reza Sadeghi, Geert-Jan Schrijen, Christian Wachsmann (TUD, IID)	International Workshop on Cryptographic Hardware and Embedded Systems (CHES) 2011	LNCS 6917	Springer	Nara, Japan	2011	374-389	http://dx.doi.org/10.1007/978-3-642-23951-9_25	No
Lightweight Remote Attestation using Physical Functions	Steffen Schulz, Ahmad-Reza Sadeghi, Christian Wachsmann (TUD)	ACM Conference on Wireless Network Security (WiSec) 2011	WiSec	ACM Press	Hamburg, Germany	2011	109-114	http://dx.doi.org/10.1145/1998412.1998432	No

Title	Main author	Title of the periodical or the series	Number, date or frequency	Publisher	Place of publication	Year of publication	Relevant pages	Permanent identifiers (if available)[1]	Is/Will open access [2]provided to this publication?
A Formal Foundation for the Security Features of Physical Functions	Frederik Armknecht, Roel Maes, Ahmad-Reza Sadeghi, Christian Wachsmann, Francois-Xavier Standaert (TUD, KULEUVEN)	IEEE Symposium on Security and Privacy (SSP) 2011	SSP	IEEE Computer Society	Oakland, CA, USA	2011	397-412	http://perso.uclouvain.be/fstandae/PUBLIS/95.pdf	Yes
Lightweight Anonymous Authentication with TLS and DAA for Embedded Mobile Devices	Liqun Chen, Kurt Dietrich, Hans Löhr, Ahmad-Reza Sadeghi, Christian Wachsmann, Johannes Winter (TUD)	Information Security Conference (ISC) 2010	LNCS 6531	Springer	Boca Raton, FL, USA	2011	84-98	http://dx.doi.org/10.1007/978-3-642-18178-8_8	No
Anonymous Authentication for RFID Systems	Frederik Armknecht, Liqun Chen, Ahmad-Reza Sadeghi, Christian Wachsmann (TUD)	Workshop on RFID Security (RFIDSec) 2010	LNCS 66370	Springer	Istanbul, Turkey	2010	158-175	http://dx.doi.org/10.1007/978-3-642-16822-2_14	No

Title	Main author	Title of the periodical or the series	Number, date or frequency	Publisher	Place of publication	Year of publication	Relevant pages	Permanent identifiers (if available)[1]	Is/Will open access [2]provided to this publication?
On RFID Privacy with Mutual Authentication and Tag Corruption	Frederik Armknecht, Ahmad-Reza Sadeghi, Ivan Visconti, Christian Wachsmann (TUD)	International Conference on Applied Cryptography and Network Security (ACNS) 2010	LNCS 6123	Springer	Beijing, China	2010	493-510	http://dx.doi.org/10.1007/978-3-642-13708-2_29	No
Impossibility Results for RFID Privacy Notions	Frederik Armknecht, Ahmad-Reza Sadeghi, Alessandra Scafuro, Ivan Visconti, Christian Wachsmann (TUD)	Transactions on Computational Science IX	LNCS 6480	Springer	---	2010	39-63	http://dx.doi.org/10.1007/978-3-642-17697-5_3	No
Location Privacy in RFID Applications	Ahmad-Reza Sadeghi, Ivan Visconti, Christian Wachsmann (TUD)	Research Issues and Emerging Trends	LNCS 5599	Springer	---	2009	127-150	http://dx.doi.org/10.1007/978-3-642-03511-1_6	No
Logically Reconfigurable PUFs: Memory-Based Secure Key Storage	Ilze Eichhorn, Patrick Koeberl, Vincent van der Leest (Intel, IID)	Publication accepted for STC workshop during ACM 2011	---	ACM Press	New York, USA	2011	---	http://dx.doi.org/10.1145/2046582.2046594	No

Title	Main author	Title of the periodical or the series	Number, date or frequency	Publisher	Place of publication	Year of publication	Relevant pages	Permanent identifiers (if available)[1]	Is/Will open access [2]provided to this publication?
Comparison of SRAM and FF PUF in 65nm technology	Mathias Claes, Vincent van der Leest, An Braeken (IID)	Publication accepted for NordSec 2011 proceedings	LNCS 7161	LNCS	---	---	---	---	No
Efficient Implementation of True Random Number Generator based on SRAM PUFs	Vincent van der Leest, Erik van der Sluis, Geert-Jan Schrijen, Pim Tuyls, and Helena Handschuh (IID)	To appear in LNCS 6805	LNCS 6805	LNCS	---	2012	---	---	No
Recyclable PUFs: Logically Reconfigurable PUFs	Stefan Katzenbeisser, Ünal Kocabas, Vincent van der Leest, Ahmad-Reza Sadeghi, Geert-Jan Schrijen, Christian Wachsmann (TUD,IID)	To appear in Journal of Cryptographic Engineering	Journal of Cryptographic Engineering	Springer	---	2011	177-186	http://dx.doi.org/10.1007/s13389-011-0016-9	No
Comparative analysis of SRAM memories used as PUF primitives	Geert-Jan Schrijen, Vincent van der Leest (IID)	Publication accepted at DATE 2012 conference	---	IEEE	---	---	---	---	No

Title	Main author	Title of the periodical or the series	Number, date or frequency	Publisher	Place of publication	Year of publication	Relevant pages	Permanent identifiers (if available)[1]	Is/Will open access [2]provided to this publication?
Evaluation of a PUF Device Authentication Scheme on a Discrete 0.13um SRAM	Patrick Koeberl, Jiangtao Li, Roel Maes, Anand Rajan, Claire Vishik and Marcin Wojcik	To appear in LNCS	---	Springer	---	2011	---	---	No
Reverse Fuzzy Extractors: Enabling Lightweight Mutual Authentication for PUF-enabled RFIDs	Anthony Van Herrewege, Stefan Katzenbeisser, Roel Maes, Roel Peeters, Ahmad-Reza Sadeghi, Ingrid Verbauwhede and Christian Wachsmann	To appear in LNCS	FC	Springer	Bonaire	2012	---	http://fc12.ifca.ai/pre-proceedings/paper_89.pdf	Yes
Signal Processing for Cryptography and Security Applications,	M. Knezevic, L. Batina, E. De Mulder, J. Fan, B. Gierlichs, Y. K. Lee, R. Maes, and I. Verbauwhede	Handbook of Signal Processing Systems	(2nd edition)	Springer	US	2010	19	http://dx.doi.org/10.1007/978-1-4419-6345-1_7	No
A Pay-per-Use Licensing Scheme for Hardware IP Cores in Recent SRAM based FPGAs	R. Maes, D. Schellekens, and I. Verbauwhede	IEEE Transactions on Information Forensics and Security	7(1)	IEEE	US	2012	98-108	http://dx.doi.org/10.1109/TIFS.2011.2169667	Yes

Title	Main author	Title of the periodical or the series	Number, date or frequency	Publisher	Place of publication	Year of publication	Relevant pages	Permanent identifiers (if available)[1]	Is/Will open access [2]provided to this publication?
PUF-based Secure Test Wrapper Design for Cryptographic SoC Testing	A. Das, U. Kocabas, A. Sadeghi, and I. Verbauwhede	Design, Automation and Test in Europe (DATE 2012)	---	IEEE	---	2012	6	---	No
Low-Cost Implementations of On-the-fly Tests for Random Number Generators	F. Veljkovic, V. Rozic, and I. Verbauwhede	Design, Automation and Test in Europe (DATE 2012)	---	IEEE	---	2012	6	---	No
A Practical Device Authentication Scheme Using SRAM PUFs	Patrick Koeberl, Jiangtao Li, Anand Rajan, Claire Vishik and Wei Wu	Published in: Proceeding TRUST'11 Proceedings of the 4th international conference on Trust and trustworthy computing	ISBN: 978-3-642-21598-8	Springer	Berlin	2011	---	---	No

2.1.2 List of dissemination activities

This table is cumulative, which means that it always shows all activities from the beginning until after the end of the project.

Type of activities[3]	Main leader	Title	Date	Place	Type of audience[4]	Size of audience	Type and goal of the event	Countries addressed
Workshop	Ammar Alkassar (SIRRIX), Denis Royer (SIRRIX)	Project-Internal Introduction Workshop	29.09.2009	Lyon, France	Industry, Scientific Community	5	Evaluation of potential inter-project cooperation in the field of TPMs and HW tamper protection with members of the TCG board of directors	International
Workshop	Pim Tuyls (IID)	Workshop on Cryptographic Hardware and Embedded Systems - CHES 2009 *http://www.iacr.org/workshops/ches/ches2009/start.html*	September 2009	Lausanne, Switzerland	Scientific Community	---	Dissemination of PUF results	International
Workshop	INTEL	ISSE 2009 (Information Security Solutions Europe) *http://www.enisa.europa.eu/events/ee/isse09*	06.-09.10.2009	The Hague, The Netherlands	Scientific Community	---	Hardware assurance / RFID Security	International
Workshop	Ammar Alkassar	Project-Internal	01.-	Amman,	Govern-	27	Possible research	International

[3] e.g.: publications, conferences, workshops, web, press releases, flyers, article published in the popular press, videos, media briefings, presentations, exhibitions, thesis, interviews, films, TV clips, posters, Other.

[4] e.g.: Scientific Community (higher education, Research), Industry, Civil Society, Policy makers, Medias (multiple choices is possible.

Type of activities[3]	Main leader	Title	Date	Place	Type of audience[4]	Size of audience	Type and goal of the event	Countries addressed
	(SIRRIX)	Introduction Workshop	05.11.2009	Jordan	ment, Scientific Community		collaboration and exploitation of UNIQUE results with gov. & research institutions	
Workshop	Timm Korte (SIRRIX)	Project-Internal Introduction Workshop	14.-17.12. 2009	Amman, Jordan	Govern-ment, Scientific Community	15	Follow-up meeting research collaboration	International
Workshop	Jérôme Quévremont (TCS)	Security Seminar	15.12.2009	Rennes, France	Govern-ment	Approx. 30	Present UNIQUE project.	National (France)
Conference	Ahmad-Reza Sadeghi and Thomas Schneider (RUB)	Financial Cryptography and Data Security '10 - FC 2010 *http://fc10.ifca.ai/*	25.-28.01.2010	Tenerife, Spain	Academia, Industry	--	Attendance and presentation of the paper "Embedded SFE: Offloading server and network using hardware tokens" by Kimmo Järvinen, Vladimir Kolesnikov, Ahmad-Reza Sadeghi, and Thomas Schneider	International
Workshop	KULEUVEN	First International Workshop on Constructive Side-Channel Analysis and Secure Design - COSADE *http://cosade2010.cased.de/index.html*	04.-05.02.2010	Darmstadt, Germany	Industry, Scientific Community	--	Constructive side-channel analysis and secure design	International
Workshop	Ingrid Verbauwhede	International workshop,	15.-	Leiden, The	Industry, Scientific	--	Attendance and	International

Type of activities[3]	Main leader	Title	Date	Place	Type of audience[4]	Size of audience	Type and goal of the event	Countries addressed
	(KULEUVEN)	"Provable security against physical attacks" *http://www.lorentzcenter.nl/lc/web/2010/383/info.php3?wsid=383*	19.02.2010	Netherlands	Community		invited presenter	
Workshop	Patrick Koeberl (Intel), Ahmad-Reza Sadeghi, Thomas Schneider, and Christian Wachsmann (RUB), Geert-Jan Schrijen and Vincent van der Leest (IID)	Project-Internal Introduction Workshop	18.02.2010	Bochum, Germany	Project partners	15	UNIQUE Introduction Workshop about PUFs in general, Reconfigurable PUFs and the FIPS140-2 Standard	International
Workshop	Ammar Alkassar (SIRRIX)	Project-Internal Introduction Workshop	18.-19.04.2010	Munich, Germany	Industry	5	Exploitation of UNIQUE results with RF Industry for protecting radios	National (Germany), International
Workshop	Claire Vishik (INTEL)	6th Annual Cyber Security and Information Intelligence Research Workshop – CSIIRW *http://www.ioc.ornl.gov/csiirw/10/*	21.-23.04.2010	Oak Ridge, USA	Scientific Community	---	Attend workshop on Cyber Security Issues, present paper 'Threat Agents - A Neccessary Component of Threat Analysis'	International
Workshop	Roel Maes, (KULEUVEN), Erik	Secure Component and System	26.-27.04.2010	Cologne, Germany	Academia, Industry	50	Attendance at the workshop: Details	International

Type of activities[3]	Main leader	Title	Date	Place	Type of audience[4]	Size of audience	Type and goal of the event	Countries addressed
	van der Sluis, Geert-Jan Schrijen and Pim Tuyls (IID), and Christian Wachsmann (RUB)	Identification - SECSI 2010 *http://www.secsi-workshop.org/*					can be found on http://sharcs.crypto.rub.de/program.html	
Presentation	Intel representatives, academics, industry, EU POs and press	Research@Intel	04.05.2010	Brussels, Belgium	Industry	---	Showcase UNIQUE	International
Conference/Forum	Ammar Alkassar (SIRRIX)	GPEC 2010 *http://www.jkdefence.de/id316of5.html*	05.-06.05.2010	Leipzig, Germany	Industry, Scientific Community	700	Presenting UNIQUE @ GPEC Police Forum 2010	International
Other (Seminar)	Ahmad-Reza Sadeghi and Christian Wachsmann (RUB)	IFIP WG 11.2 Seminar on Pervasive Systems Security	07.05.2010	Istanbul, Turkey	Scientific Community	---	Attendance, talk and discussion on "RFID Privacy Models and Practice" by Ahmad-Reza Sadeghi	International
Workshop	Ahmad-Reza Sadeghi and Christian Wachsmann (RUB), Pim Tuyls (IID)	Radio Frequency Identification Security - RFIDSec 2010 *http://www.wikicfp.com/cfp/servlet/event.showcfp?eventid=7784&copyownerid=8337*	07.-09.05.2010	Istanbul, Turkey	Academia, Industry	60	Attendance at the workshop, presentation of the paper "Anonymous Authentication for RFID Systems" by Frederik Armknecht, Liqun Chen, Ahmad-Reza Sadeghi, and Christian Wachsmann. Invited talk by Pim Tuyls.	International
Workshop	Organizer (IID and RUB)	Workshop on Security Hardware	21.-23.06.2010	Berlin, Germany	Academia, Industry	---	Security Hardware, co-located with	International

Type of activities[3]	Main leader	Title	Date	Place	Type of audience[4]	Size of audience	Type and goal of the event	Countries addressed
		http://www.trust2010.org/workshop-hw.html					TRUST 2010	
Conference	All UNIQUE partners	3rd International Conference on Trust and Trustworthy Computing TRUST 2010 *http://www.trust2010.org/*	21.-23.06.2010	Berlin, Germany	Academia, Industry	100-200	Trust and Trustworthy Computing, A detailed overview of the single presentations can be found on	International
Conference	Christian Wachsmann (RUB)	8th International Conference on Applied Cryptography and Network Security ACNS 2010 *http://icsd.i2r.a-star.edu.sg/staff/jianying/acns_home/*	22.-25.06.2010	Beijing, China	Academia, Industry	100	Attendance and presentation of the paper "On RFID Privacy with Mutual Authentication and Tag Corruption" by Frederik Armknecht, Ahmad-Reza Sadeghi, Ivan Visconti, and Christian Wachsmann.	International
Conference	Pim Tuyls (IID)	12th Information Hiding Conference 2010 *https://ih2010.cpsc.ucalgary.ca/*	28.-30.06.2010	Calgary, Canada	Scientific Community	---	Invited talk by Pim Tuyls on PUF based security.	International
Workshop	Geert-Jan Schrijen (IID)	Paca Security Trends in	June 2010	Gardanne, France	Scientific Community	---	Invited talk by Geert-Jan Schrijen	International

Type of activities[3]	Main leader	Title	Date	Place	Type of audience[4]	Size of audience	Type and goal of the event	Countries addressed
		embedded Systems - PASTIS 2010 *http://www.emse.fr/spip/IMG/pdf/Pastis2010_comm.pdf*					on PUF based security	
Workshop	Ahmad-Reza Sadeghi and Thomas Schneider (RUB), Jean-Christophe Courrege (TCS)	Workshop on Cryptographic Hardware and Embedded Systems - CHES 2010 *http://www.iacr.org/workshops/ches/ches2010/start.html*	17.-20.08.2010	Santa Barbara, USA	Academia, Industry	---	Attendance and presentation of the paper "Garbled circuits for leakage-resilience: Hardware implementation and evaluation of one-time programs" by Kimmo Järvinen, Vladimir Kolesnikov, Ahmad-Reza Sadeghi, and Thomas Schneider.	International
Workshop	Geert-Jan Schrijen (IID)	CAST 2010 *http://www.associationforsoftwaretesting.org/conference/cast-2010/*	August 2010	Darmstadt, Germany	Scientific Community	---	Invited talk by Geert-Jan Schrijen on PUF based security	International
Other (Seminar)	IID: Pim Tuyls, Geert-Jan Schrijen INTEL: Patrick Koeberl, Claire Vishik, Anand Rajan, Timothy Casey	International Spring Seminar on Electronics Technology - ISSE 2010 *http://www.revolution1.plus.com/isse/downloads/ISSE%202010%20Programme_21.pdf*	05.-07.10.2010	Berlin, Germany	Scientific Community	---	Papers accepted: 'Silicon PUFs in Practice'', 'Threat Agents - A Neccessary Component of Threat Analysis' IID: Invited talks, UNIQUE promotion INTEL: Presented paper 'Silicon PUFs in Practice', raise	International

Type of activities[3]	Main leader	Title	Date	Place	Type of audience[4]	Size of audience	Type and goal of the event	Countries addressed
							awareness of the Unique Project, PUF and related technology; presented paper on threat analysis in the area of unique	
Conference	Ahmad-Reza Sadeghi (RUB), Christian Wachsmann (RUB)	Conference ISC 2010 Information Security - 13th International Conference *http://math.fau.edu/~isc2010/index.html*	26.-28.10.2010	Boca Raton, Florida, USA	Academia, Industry	100	Participation in the conference, presentation of the paper "Lightweight Anonymous Authentication with TLS and DAA for Embedded Mobile Devices" by Liqun Chen, Kurt Dietrich, Hans Löhr, Ahmad-Reza Sadeghi, Christian Wachsmann, and Johannes Winter, and promotion of the UNIQUE project	International
Workshop	Vincent van der Leest (IID)	5th Benelux Workshop on Information and System Security - WISSec 2010 *http://es.ewi.utwente.nl/wissec2010/*	29.-30.11.2010	Nijmegen, The Netherlands	Scientific Community	---	Presented two papers on PUFs, including promotion for the UNIQUE project	International
Conference	Ahmad-Reza Sadeghi (TUD)	International Conference on Trusted Systems	13.-15.12.2010	Beijing, China	Academia, Industry	---	Invited talk on "Trusted and Secure Computing in Practice: Where are	International

Type of activities[3]	Main leader	Title	Date	Place	Type of audience[4]	Size of audience	Type and goal of the event	Countries addressed
		(INTRUST) 2010 *http://www.mysmu.edu/faculty/xhding/intrust-cfp.pdf*					We Now!"	
Other (Symposium)	Geert-Jan Schrijen (IID) speaker	"Security with noisy data", symposium at Eindhoven Technical University	21.01.2011	Eindhoven, The Netherlands	Industry, Scientific community	---	IEEE symposium organized to celebrate the fact that JP Linnartz was elevated to the grade of IEEE Fellow	International
Workshop	Anand Rajan (Intel), Claire Vishik (Intel)	Security Workshop *http://www.securityconference.de/Home.4.0.html*	27.01.2011	Munich, Germany	Industry, Scientific community	---	Gave talk	International
Other (Symposium)	Vincent van der Leest (IID) speaker	"Embedded Systems & Security"	27.01.2011	Diepenbeek, Belgium	Scientific community	---	Symposium to conclude TETRA project STRES	International
Presentation	Ahmad-Reza Sadeghi and Thomas Schneider (TUD)	Cryptographers' Track at the RSA Conference (CT-RSA) 2011 *http://ct-rsa2011.di.uoa.gr/*	14.-18.02.2011	San Francisco, CA, USA	Industry, Academia	---	Presented paper "Secure Set Intersection with Entrusted Hardware Tokens"	International
Other (Discussion)	Ahmad-Reza Sadeghi (TUD)	Financial Cryptography and Data Security (FC) 2011 *http://ifca.ai/fc11/*	28.02.-04.03.2011	St. Lucia	Academia, Industry	---	Panel discussion on "The Future of Banking Security and Financial Transactions for the 21st Century"	International
Presentation	Heike Schröder and Christian Wachsmann	CeBIT 2011 *http://www.cebit.de/en/about-the-*	01.-05.03.2011	Hannover, Germany	Industry, Public, Academia	---	Presented UNIQUE project	International

Type of activities[3]	Main leader	Title	Date	Place	Type of audience[4]	Size of audience	Type and goal of the event	Countries addressed
	(TUD)	*trade-show/facts-figures/profile/cebit-2011-review*						
Workshop	Christian Wachsmann (TUD)	CAST Workshop on Product Piracy *http://www.cast-forum.de/workshops/infos/150*	14.04.2011	Darmstadt, Germany	Industry, Academia	32	Gave talk	National (Germany)
Other (Symposium)	Ahmad-Reza Sadeghi, Christian Wachsmann (TUD)	IEEE Symposium on Security and Privacy *http://www.ieee-security.org/TC/SP2011/*	22.05.-25.05.2011	Berkeley, CA, USA	Academia, Industry	450	Presented research paper on "A Formal Foundation for the Security Features of Physical Functions", gave short talk on "Lightweight Remote Attestation based on Physical Functions"	International
Conference	Anand Rajan (Intel)	TRUST 2011 4th International Conference on Trust & Trustworthy Computing *http://www.trust2011.org/*	22.06 – 25.06.2011	Pittsburgh, PA, USA	Academia, Industry	100-200	Presented paper: "A Practical Device Authentication Scheme Using SRAM PUFs"	International
Workshop	Ammar Alkassar (SIRRIX)	Forensic Workshop	21.-27.07.2011	Riad, Saudi Arabia	Scientific Community, Industry	45	Presentation of UNIQUE results at Forensic workshop with Industry and Government	International
Workshop	Ammar Alkassar (SIRRIX)	Project-Internal Introduction Workshop	4.08.2011	Bremen, Germany	Industry	9	Exploitation of UNIQUE results with Defense Industry for protecting IP	International

Type of activities[3]	Main leader	Title	Date	Place	Type of audience[4]	Size of audience	Type and goal of the event	Countries addressed
Workshop	Ammar Alkassar (SIRRIX)	Project-Internal Introduction Workshop	20.09.2011	München, Germany	Govern-ment	15	Exploitation of UNIQUE results with German Government	Germany
Workshop	Ammar Alkassar (SIRRIX)	Project-Internal Introduction Workshop	18-19.08.2011	Berlin, Germany	Industry, Scientific Community	7	Exploitation of UNIQUE results with Crypto Industry for protecting IP	International
Conference	Steffen Schulz (TUD), Ahmad-Reza Sadeghi (TUD)	ACM Conference on Computer and Communications Security (ACM CCS) *http://www.sigsac.org/ccs/CCS2011/*	17.-21.10.2011	Chicago, IL, USA	Academia, Industry	---	Present poster on "Practical Embedded Remote Attestation Using Physically Unclonable Functions"	International
Workshop	Ünal Kocabas (TUD)	Workshop on Cryptographic Hardware and Embedded Systems (CHES) 2011 *http://www.iacr.org/workshops/ches/ches2011/start.html*	25.09-01.10.2011	Nara, Japan	Academia, Industry	---	Present paper on "Recyclable PUFs: Logically reconfigurable PUFs"	International
Presentation	Jérôme Quévremont (TCS)	TOISE (ENIAC) project meeting *http://www.tst-sistemas.es/en/rd/toise-2/*	13.10.2011	Milano, Italy	Academia, Industry	30-35	Overview of PUF and UNIQUE.	International
Presentation	Patrick Koeberl (INTEL)	ACM STC 2011 *http://www.sigsac.org/ccs/CCS2011/preworkshops.shtml*	17.10.2011	Chicago, USA	Academia	30-40	Present paper: 'Logically Reconfigurable PUFs: Memory-Based Secure Key Storage'	International

Type of activities[3]	Main leader	Title	Date	Place	Type of audience[4]	Size of audience	Type and goal of the event	Countries addressed
Presentation	Patrick Koeberl (INTEL)	ISEE2010 *http://www.isee2010.org/*	22.11.2011	Prague, Czech Republic	Academia, Industry	100-200	Present paper: 'Conumerization: Consequences of Fuzzy Home-Work Boundaries'	International
Conference	Vincent van der Leest (IID)	NordSec 2011 Conference *http://nordsec2011.cyber.ee/*	26-28.10.2011	Tallinn, Estonia	Academia, Industry	30-40	Present paper: "Comparison of SRAM and FF PUF in 65nm technology"	International
Presentation	Shaobin Wang (INTEL)	INTRUST 2011 *http://www.onets.com.cn/intrust11/*	27.11.2011	Beijing, China	Academia	---	Present paper: 'Evaluation of a PUF Device Authentication Scheme on a Discrete Shaobinum SRAM'	International
Other (Talk)	INTEL	Aspects of Hardware Trust	21.01.2010	UCL UK	Scientific community	---	Aspects of Hardware Trust	National
Other (Seminar)	KULEUVEN	COSIC seminar - Leakage-Resilient Storage (D. Venturi) *http://www.esat.kuleuven.be/scd/event.php?view=0&id=1081*	01.02.2010	3000 Leuven, Belgien	Scientific community	---	Addressing theoretical aspects of hardware security in a leakage model	National
Other (Seminar)	KULEUVEN	COSIC seminar – Leakage-Resilient Signatures (S. Faust) *http://www.esat.kuleuven.be/scd/event.php?view=2&id=1082*	04.02.2010	3000 Leuven, Belgien	Scientific community	---	Addressing theoretical aspects of hardware security in a leakage model	National

Type of activities[3]	Main leader	Title	Date	Place	Type of audience[4]	Size of audience	Type and goal of the event	Countries addressed
Workshop	TUD	Workshop on Trustworthy Embedded Devices (TrustED) 2011 *http://www.trust.informatik.tu-darmstadt.de/events/trusted-2011/*	15.-16.09.2011	Leuven, Belgium	Academia and Industry	Approx. 30	Bringing together experts from academia, research institutes, industry and government for discussing and investigating problems, challenges and recent scientific and technological developments in the field of cyber-physical systems.	International
Presentation (Paper)	IID Authors: Vincent van der Leest, Geert-Jan Schrijen, Pim Tuyls, Helena Handschuh,	Hardware Intrinsic Security from D Flip-flops	October 4th 2010	Publication accepted for STC workshop during ACM 2010	Industry, Scientific community	---	IID (Dissemination of research results on D Flip-flop PUFs)	International
Other (Paper)	IID Authors: Vincent van der Leest, Geert-Jan Schrijen, Pim Tuyls, Helena Handschuh	Hardware Intrinsic Security from D Flip-flops	June 22nd 2010	Paper presented at hardware security workshop during TRUST2010	Industry, Scientific community	---	IID (Dissemination of research results on D Flip-flop PUFs)	International
Other (Paper)	IID Authors: Vincent van der Leest, Geert-Jan Schrijen, Pim Tuyls, Helena Handschuh	Hardware Intrinsic Security from D Flip-flops	November 30th 2010	Paper presented at WISSEC2010	Industry, Scientific community	---	IID (Dissemination of research results on D Flip-flop PUFs)	International

Type of activities[3]	Main leader	Title	Date	Place	Type of audience[4]	Size of audience	Type and goal of the event	Countries addressed
Other (Paper)	IID Authors: Georgios Selimis, Mario Konijnenburg, Maryam Ashouei, Jos Huisken, Harmke de Groot, Vincent van der Leest, Geert-Jan Schrijen, Marten van Hulst, Pim Tuyls	Evaluation of use of 90nm 6T-SRAM as a PUF for secure key generation in a wireless communication system	November 30th 2010	Paper presented at WISSEC2010	Industry, Scientific community	---	IID (Dissemination of research results on D Flip-flop PUFs)	International
Other (Paper)	IID Authors: Georgios Selimis, Mario Konijnenburg, Maryam Ashouei, Jos Huisken, Harmke de Groot, Vincent van der Leest, Geert-Jan Schrijen, Marten van Hulst, Pim Tuyls	Evaluation of use of 90nm 6T-SRAM as a PUF for secure key generation in a wireless communication system	May 16th 2011	Publication accepted for ISCAS2011	Industry, Scientific community	---	IID (Dissemination of research results on D Flip-flop PUFs)	International
Web	TEC	http://www.unique-security.eu/	Online since September 2009	Internet	Scientific Community, Industry, Civil Society, Policy makers, Medias	---	The official web-site of the UNIQUE project.	International

Type of activities[3]	Main leader	Title	Date	Place	Type of audience[4]	Size of audience	Type and goal of the event	Countries addressed
Web	KULEUVEN	http://www.esat.kuleuven.be/scd/project.php?prid=480	Online since 01/2010	Internet	Scientific Community, Industry, Civil Society, Policy makers, Medias	---	Internal project description of KULEUVEN.	International
Web	IID	http://www.intrinsic-id.com/subsidy_projects.htm	Online since 01/2010	Internet	Scientific Community, Industry, Civil Society, Policy makers, Medias	---	Internal project description of Intrinsic-ID	International
Web	TUD	http://www.trust.informatik.tu-darmstadt.de/research/projects/current-projects/unique-foundations-for-forgery-resistant-security-hardware/	---	Internet	Scientific Community, Industry, Civil Society, Policy makers, Medias	---	Internal project description of TUD	International
Press releases	TEC	Novel Security Technologies PUFs-will tackle the Problem of Counterfeiting and Tampering UNIQUE develops high innovative Hardware components which can be uniquely identified	November 2009	Internet	Scientific Community, Industry, Civil Society, Policy makers, Medias	---	http://www.unique-security.eu/downloads/Public/UNIQUE_Press_Relaese.doc	International

Type of activities[3]	Main leader	Title	Date	Place	Type of audience[4]	Size of audience	Type and goal of the event	Countries addressed
Other (Newsletter)	TEC	UNIQUE Newsletter March 2011	March 2011	Internet	Scientific Community, Industry, Civil Society, Policy makers, Medias	---	http://www.unique-security.eu/downloads/UNIQUE-238811-Newsletter-March-2011.pdf	International
Other (Leaflet/Logo)	TEC, all	http://www.unique-security.eu/images/stories/UNIQUE_No238811_Leaflet_20091217.pdf	2009	Internet	Scientific Community, Industry, Civil Society, Policy makers, Medias	---	---	International
Other (Master thesis)	Martin Deutschmann (TEC)	Cryptographic Applications with Physically Unclonable Functions http://www.unique-security.eu/downloads/UNIQUE-238811-Master-Thesis-MD.pdf	2010	University, Klagenfurt	Scientific Community, Industry, Civil Society, Policy makers, Medias	---	---	International
Other (Promotion video)	TEC	UNIQUE promotion video on YouTube http://www.youtube.com/watch?v=UG42aBGN2bg	November 2010	Internet	Scientific Community, Industry, Civil Society, Policy makers, Medias	---	---	International

Type of activities[3]	Main leader	Title	Date	Place	Type of audience[4]	Size of audience	Type and goal of the event	Countries addressed
Workshop Tutorials	KULEUVEN: Ingrid Verbauwhede, Roel Maes, Benedikt Gierlichs	CHEW 2012: http://cse.iitkgp.ac.in/conf/CHEW12/	March 2012	IIT Kharagpur, India	Students, Academic and Industry	---	In-depth tutorial sessions on numerous hardware security topics, including PUFs and the proceedings of the UNIQUE project	India, International
Round-table discussion	KULEUVEN: Ingrid Verbauwhede	HOST-2012 - "Can we trust the chips of the future?," (published in IEEE Design & Test of Computers 28(5), pp. 96-103, 2011)	2011	HOST-2012	Scientific and Industry	---	Round-table discussion	International
Talk	KULEUVEN: Ingrid Verbauwhede	"Design and design methods for embedded security (invited),"	2011	Tetra closing event - STRES project	Academic	---	Invited talk	Belgium
Other (Newsletter)	TEC, IID	UNIQUE Newsletter October 2011	October 2011	Internet	Scientific Community, Industry, Civil Society, Policy makers, Medias	---	http://www.unique-security.eu/downloads/UNIQUE-238811-Newsletter-October-2011.pdf	International

2.2 Exploitable Foreground and Exploitation Plans

Exploitation is recognised as the key enabler for the success of the UNIQUE project. It describes all activities which are done to promote, exploit and commercialise the research results gained during the project's lifetime. Scientists need to always keep in mind the usability of research results, the possibility for their application in different areas, and their relevance for the community.

Exploitation activities are essential to implement and transfer the technology developed within the project as well as to maximise the benefits for the project partners. Carefully planned dissemination and exploitation strategies are an imperative for a successful project lifecycle.

Hence all partners of UNIQUE were aware of and committed to the exploitation of the project results. It is the principle of all exploitation activities to use research results to create value within all participating organisations and thus to improve their competitive advantage. Only by scaling up the results into commercial offerings, can all European constituents be reached while ensuring profitability through economies of scale.

Wherever possible, research results will be used for the creation and support of new products and services. These products and services will lead to a competitive advantage of the participating organisations and will substantially contribute to the benefit of the targeted constituents. In order for the exploitation to be effective, an integrated approach will be necessary, combining experience and expertise from the development department and solution management, and the involvement of a user base represented by the consortium partners and the user council.

Project results that can be transferred into marketable products in a very short period of time offer the possibility to generate huge competitive advantages and thereby helping to generate considerable profits. It is important to establish respective management structures which ensure that IPRs and project achievements are adequately protected and exploited.

2.2.1 Initially planned Exploitation Activities

The exploitation of the project results is clearly defined in the objectives of UNIQUE. As the project consortium consists of major European players in both science and industry the usage of the results will be exploited in both the science and commercial sector. The main exploitation will be through each partner's own organisation.

2.2.2 List of applications for patents, trademarks, registered designs

In the beginning of the project, the UNIQUE consortium has established an efficient IPR framework to maximise project exploitation. The contractual basis for this IPR framework has been laid down in the UNIQUE Consortium Agreement where explicit rules for use of Foreground, Sideground and Background and its distribution within the project as well as rules for handling sensitive or confidential information were established.

Background is understood to be information, knowledge and any IPR relevant to the project already held by the project partners before the accession to the EC Grant Agreement.

Foreground instead is understood to consist of tangible and intangible results in terms of information, materials and knowledge generated inside the project. The new knowledge produced during the UNIQUE project belongs to the partner who generated it; when the generation of foreground is a joint process, it is, unless the partners don't agree on another solution, jointly owned by the participants. The owner of the foreground is able to decide to apply for a patent on its own and the other partners must not interfere in this process. The UNIQUE partners designed the management structure, workflows and tools always with the protection of knowledge in mind. Hence any business exploitation or public disclose of new knowledge can only be done after the owner has given his or her consent.

The monitoring of IPR issues has been the responsibility of WP5. However, in terms of patents, trademarks and registered designs, nothing has been reported within the framework of the UNIQUE project.

2.2.3 Exploitable Foreground

The consortium was active in several exploitation areas:

Type of exploitable foreground	Description of exploitable fore-ground	Con-fidential (Yes/No)	Foreseen embargo date (dd.mm.yyyy)	Exploitable product(s) or measure(s)	Sector(s) of application	Timetable, commercial or any other use	Patents or other IPR exploitation (licences)	Owner and other beneficiaries involved
Engineering competence for PUF security architectures	Usage of different PUF types for the implementation of security use cases and application scenarios.	No	Not applicable	Engineering Security Services for PUF technology	(a) general ICT, (b) Smart Meter, (c) Secure Embedded systems	Engineering Services since 2012	Not yet; Patents on cryptographic functions foreseen beyond 2013	TEC
Experience on ASIC design, reliability testing and PUF use cases.	ASIC design flow, reliability tests on 65nm TSMC process, security use case studies for PUF primitives.	No	Not applicable	Can be used to show experience towards new customers and to give direction to future developments within Intrinsic-ID.	We see potential apps in secure chip solutions	2012 and beyond	No	IID
General advancement of knowledge in PUF security architectures	Usage and verification of different PUF types in upcoming security architectures	No	Not applicable	Development of PUF-based security architectures and verification of such systems	(a) Smartcards (b) secure embedded systems	Starting 2012	Not yet	SIRRIX
Engineering competence for PUF security architectures	Usage of various PUF types for secure ICs; typical application scenarios	Yes	Not applicable	Development of security architectures using PUFs	High assurance professional electronics	Confidential	Confidential	TCS

Type of exploitable foreground	Description of exploitable fore-ground	Con-fidential (Yes/No)	Foreseen embargo date (dd.mm.yyyy)	Exploitable product(s) or measure(s)	Sector(s) of application	Timetable, commercial or any other use	Patents or other IPR exploitation (licences)	Owner and other beneficiaries involved
Engineering competence for PUF security evaluation	Knowledge of various PUF types and applicable evaluation methods	Yes	Not applicable	Security evaluation of ICs containing PUFs (incl. Common Criteria evaluation).	Security market	Confidential	Confidential	TCS
General advancement of knowledge	Design of PUF-based authentication and attestation protocols	No	Not applicable	Development, design and implementation of PUF-based security mechanisms	Not applicable	Not applicable	Not applicable	TUD
General advancement of knowledge	Evaluation methodologies for PUFs	No	Not applicable	Development of a (security) evaluation framework for PUFs	Not applicable	Not applicable	Not applicable	TUD
Technical and engineering knowledge of aspects of PUF functionality	Use cases, threat models, and security features	No	Not applicable	Use cases including types of PUFs studied by Unique	Not applicable	Not applicable	Not applicable	INTEL
General advancement of knowledge	Experience and insight in development and implementation flows for the hardware aspects of PUFs	No	Not applicable	Increased potential for building better PUFs in a more efficient manner	Research and development	Not applicable	Not applicable	KULEUVEN

Type of exploitable foreground	Description of exploitable fore-ground	Con-fidential (Yes/No)	Foreseen embargo date (dd.mm.yyyy)	Exploitable product(s) or measure(s)	Sector(s) of application	Timetable, commercial or any other use	Patents or other IPR exploitation (licences)	Owner and other beneficiaries involved
General advancement of knowledge	Development of useful metrics for reliability, security and usability of PUFs + Assessment of these metrics on large quantities of measurement data	No	Not applicable	Capability of quickly assessing the quality of a PUF and comparing different PUF implementations in a fair manner. + Insight into relation between PUF quality and hardware design decisions	Research and development	Not applicable	Not applicable	KULEUVEN
General advancement of knowledge	Deployment of PUFs in security-related use cases	No	Not applicable	Better understanding of the strengths and weaknesses of different PUF structures w.r.t. each other and other primitives + Innovative approaches to applying PUFs in 'atypical' ways	Research and development	Not applicable	Not applicable	KULEUVEN

2.2.4 IPR issues identified in the UNIQUE project

In the environment of international applied research projects with industrial partners such as UNIQUE, the careful handling of IPR issues is of strategic importance. Within the UNIQUE project, many individuals of numerous organisations cooperate across national borders. In order to develop novel technologies, concepts or processes, exchanging information with other parties is a necessity. Furthermore, jointly creating new intellectual properties is common. Therefore confidentiality is a very important issue for participants in UNIQUE, from the project start-up phase of joint activities to the implementation phase and further to the exploitation of results.

All efforts related to IPR issues aim to create a favourable environment for respecting intellectual property rights (IPR) because of moral and economic reasons. Without IPR protection the joint creativity of natural persons or legal bodies as well as the dissemination and exploitation of results would be highly restricted not to risk a substantial drain of knowledge. Intellectual property (IP) is an intangible asset and created as a result of intellectual creative effort of the human mind in relation to works of authorship and/or inventions. With the ownership of intangible assets certain legal exclusive property rights which are established by law or by contractual obligation are connected and maintain the control in relation to the protection of the interests of the creators by excluding these creations from public property. This means the right to permit or deny the use and exploitation of the creative work. So IPR provides a protection of the creations and inventions to the owners by preventing users from using or copying them without reservation or payment for a certain period of time.

Intellectual property can be classified into

- industrial property items like inventions which can be a product or a process providing new solutions for solving (technical) problems and which can be protected by registering a patent and
- copyright items which provide exclusive rights to the creator to prohibit the unauthorized copying, adaptation and reproduction of its intellectual work.

In the last few month of the project all partners formed a common sense on the further usage of the UNIQUE ASICs and UNIQUE ASIC boards as following below:

UNIQUE ASIC/board common understanding

The purpose of this agreement is to clarify in which way and under which conditions the UNIQUE consortium and each individual partner is allowed to use and disseminate the developed foreground connected to the UNIQUE ASICs and test boards after project ending. It includes both specific and general rules for the use of UNIQUE ASICs and boards outside of the UNIQUE consortium.

This document adds all to the Consortium Agreement, which was signed by each of the project partners prior to project start and officially, came into force as from the Effective Date. Effective Date means the date of entering into force of the Grant Agreement, which was the 10.08.2009. The names of the project partners (TEC, IID, TUD, KULEUVEN, SIRRIX, INTEL, TCS) coincide with the partners mentioned in the Consortium Agreement, apart from the Ruhr-University-Bochum, which left the project in the first year and handed over all project rights and obligations to our project partner University Darmstadt (TUD). Any rule set herewith will have to obey the Consortium Agreement and will be based on the will of all partners.

The Consortium came to the following agreement:

- Commercial activities with the UNIQUE ASICs are prohibited as also defined by the production rules for Europractice[5] hardware.
- The ASIC-Interface Board should be handled under the same terms as the ASIC.
- With respect to point 1, UNIQUE partners are allowed to use the ASICs and measured data of the ASICs for other research, education and demonstration purposes as well as in other research projects outside the UNIQUE consortium, as long as the ASICs are always under the physical possession and responsibility of the corresponding UNIQUE partners.
- Reverse engineering should not be allowed to parties outside the UNIQUE consortium.
- If part of the chip or the chip itself (modified) is refabricated all rules as defined by the Consortium Agreement are sustained.
- ASICs measurements can be shared with partners in public funded research projects outside of UNIQUE, as long as the source of data and the UNIQUE project is mentioned as reference.
- Any information from work done with the UNIQUE ASICs or chips data has to reference as source the UNIQUE project.

The following UNIQUE partners declared to have own IP within the ASICs: KU Leuven developed and integrated full custom arbiter PUF (layout has been provided), ring oscillator PUF and latch PUF (VHDL has been provided). IID has integrated IP on certain PUF constructions and developed and integrated their buskeeper PUF solution. SIRRIX declared to own the layout of the Interface Board. TSMC, the producer of the chips, has IP in libraries/technologies used to produce the chip. UNIQUE Partners not listed before haven't declared any ownership of IP within the ASIC.

This agreement may become law after the termination of the UNIQUE project and would request joint signature of all partners.

As of February 2012 the legal advisors of all partners are creating, under the lead of Ms Tara MacMahon from INTEL, a legal binding formulation for the upper statements.

[5] *www.**europractice**.com*

2.2.5 IPR issues after the project conclusion / future plans

In addition to the table above, the UNIQUE partners provided an explanation of the exploitable foreground:

1. Foreground developed: Its purpose or its nature, how the foreground will be exploited, when and by whom, further research necessary?

TEC: TECHNIKON established during the last phase of the project a new industrial service line called "Security Engineering Services with programmable physically unclonable functions". Our new service initiative was granted the price for research and innovation in Austria in November 2011 and Technikon was nominated for the Austrian econovius 2012.

IID: While working in the UNIQUE project, Intrinsic-ID has increased its knowledge on ASIC design flows by managing the implementation of the test chip in TSMC 65nm technology. Furthermore, reliability tests on this technology node have shown the stability of memory based PUFs that are being used in Intrinsic-IDs products. Measurement results therefore form a proof point towards customers and the comparison (in terms of reliability and entropy) towards alternative PUF technologies can be used to promote Intrinsic-ID's PUF approach. Also, the ASIC developed in the UNIQUE project contains a first ever implementation of a buskeeper PUF developed by Intrinsic-ID. The successful implementation and promising measurement results in the UNIQUE project form a first proof of concept for this new kind of Physical Unclonable Function.

SIRRIX: We developed a practical knowledge about the development and integration of PUFs and related security protocols. We intent to use this knowledge in upcoming projects and are looking at options to extend the functionality of secure systems based on the results of UNIQUE.

TCS: We have developed a practical knowledge of PUF, through their validation or verification. We intend to turn them into industrial use cases through the PREMISE project, before being able to include them into products.

On the evaluation side, we have developed our knowledge to evaluate such functions.

TUD: We extended our expertise on integrating PUFs in security protocols and higher level architectures, such as PUF-based authentication and attestation schemes. We will use this expertise in scientific publications and upcoming national and international research projects.

INTEL: The Intel UNIQUE team consists of multiple stakeholders who will take the knowledge developed during the project and incorporate it into their R&D and technology development activities as appropriate.

KULEUVEN: The results of the UNIQUE project extended our expertise on PUFs on a number of levels:

- PUF implementation: improved insight into hardware development flows and in particular the peculiarities faced when designing PUF structures. Also a deeper understanding of the impact of many (early-stage) design decisions on the quality and efficiency of the eventually manufactured PUFs.
- PUF assessment: better understanding of the strengths and weaknesses of different PUF structures, both w.r.t. implementations issues as well as w.r.t. application requirements. Also, development and assessment of

usability metrics capturing the distinct security and reliability properties of PUFs as accurately and objectively as possible.

- PUF deployment: increased insight into the added value of PUFs in different security related use cases. Also, experience in the development and innovative application of PUFs, keeping in mind their implementation constraints and quality measures.

As a research institution, we aim to continuously improve our knowhow in this topic and apply it in an innovative manner through scientific publications and research collaborations.

2. IPR exploitable measures taken or intended?

TEC: Technikon's team is working on new solutions for Fuzzy extractors to create more robust PUF architectures. Several Master and PhD Thesis's were triggered. We expect to be able to protect new knowledge with IPR measures in 2013 and beyond.

IID: No, IPR exploitable measures are not foreseen in the near future.

SIRRIX: No, IPR exploitable measures are not taken or intended yet.

TCS: No, IPR exploitable measures are not foreseen in the near future.

TUD: No, IPR exploitable measures are not taken or intended yet.

INTEL: Intel does not plan any IPR activities directly related to the work carried out as part of the UNIQUE project.

KULEUVEN: No, IPR exploitable measures are not taken or intended yet.

3. Potential/expected impact (quantify where possible):

TEC: Technikon expects to increase its yearly turnover based on industrial services provided for programmable physically unclonable functions by 25% at least.

IID: The research conducted within the UNIQUE project forms a strong support case for Intrinsic-IDs products and has identified potential new PUF implementations (such as logically reconfigurable PUFs) that are considered worthwhile for Intrinsic-ID to investigate in more detail.

SIRRIX: Sirrix will promote PUF technology in research and commercial applications.

TCS: Thales could include PUF in high assurance ICs within a few years.

TUD: TU Darmstadt will promote PUFs in the scientific community and for industrial research.

INTEL: The Intel stakeholder group will bring knowledge of PUF technology through into their product development teams for future consideration.

KULEUVEN:

- Impact in the scientific community through continuous publications on the UNIQUE research results and follow-up work on PUFs.
- Impact in industry through collaborations in future projects and advisory assignments.

4. Please chart up your ideas/strategies for short-, mid-, long-term exploitation of results:

TEC:

Short-term/ Mid-term/Long-Term: Technikon will develop and expand their competences in Security Services based on PUF technology.

IID:

Short-term: IID will use the reliability results to promote and support memory based PUF technology towards customers.

Mid-term: IID will investigate further the reliability and ageing aspects of different PUFs, like buskeeper and flipflop PUFs.

Long-Term: IID will develop new solutions for use cases as have been investigated in the UNIQUE project, for example, using logically reconfigurable PUFs for preventing software downgrading.

SIRRIX:

Short-term: SIRRIX will exploit UNIQUE results in other currently active projects.

Mid-term: SIRRIX will extend PUF integration and verification knowledge.

Long-Term: SIRRIX will introduce PUFs in products to enhance their security.

TCS:

Short-term: TCS will share UNIQUE results within TCS.

Mid-term: TCS will increase the technological readiness level of PUF for our application domain (see PREMISE project below).

Long-Term: TCS could introduce PUF in products to enhance their security.

TUD:

Short-term: TUD will build upon the UNIQUE results to generate scientific publications.

Mid-term: TUD will build upon the UNIQUE results within a joint research centre with Intel.

Long-Term: TUD will use and extend the competence on PUF technology and its applications in other research projects.

INTEL:

Short-term: Progress of the UNIQUE project was/is consistently shared with the internal Intel stakeholders group to ensure bi-directional flow of information.

Mid-term: Intel will evaluate PUF technology as appropriate product strategies are developed.

Long-term: Intel will study the relevant aspects of PUFs in direct relation technology maps, to product strategies and product development.

KULEUVEN:

Short-term: KULEUVEN will directly exploit the research results of the project in scientific publications and course material.

Mid-term: KULEUVEN will apply the achieved experience and insights into other research projects and collaborations.

Long-Term: KULEUVEN will continue its effort to improve and apply PUF structures for use in embedded security.

5. Please indicate your impact on the European security market:

TEC: Technikon will have an indirect impact on the European Security Market. We are guiding our customers to introduce and use PUF technology within their products.

IID: Intrinsic-ID's leadership position is further reinforced in the European security market in general and in the card, automotive and mobile markets in particular.

SIRRIX: We strongly believe that the technology we researched and developed within the UNIQUE project will be crucial for the competitiveness of the European IT-Security industry. It will allow innovative business models as well as economically necessary workflows in the production of security-sensitive equipment and components. We expect in these areas an interesting (niche) market for us as SME that requires a high degree of expertise. At the same time the providing of these solutions will foster the competitiveness of a broad bandwidth of related industries.

In addition, we also expect an emerging market for verification of services and products in which we want to exploit our UNIQUE results.

TCS: We are a European leader on the professional security market for high assurance needs (banking, government, emergency services, defence…) and offer components, equipments and systems to our customers.

We also embed an ITSEF (information technology security evaluation facility) focused on the evaluation of hardware technologies according to Common Criteria.

TUD: We are part of the Center for Advanced Security Research Darmstadt (CASED), which is one of the largest competence centres for IT security research in Europe. We will play an advisory role for the European Security Market.

INTEL: Intel is a leader in the semiconductor industry, with significant operations in Europe in R&D, manufacturing, and other areas. Intel components enable computing and support systems operating in all technology areas, both for individual users and organizations. Security is one of the strategic areas for Intel.

KULEUVEN: We will perform advisory activities within the European Security Market.

6. Will one or more of your products be enhanced through the results of your work within the UNIQUE project? Please indicate the enhancement as well:

TEC: Technikon expanded its industrial service line by a new item called "Security Engineering Services with programmable physically unclonable Functions".

IID: The research from UNIQUE will lead to enhancement for Intrinsic-ID in several areas. First, the results for UNIQUE can be used to demonstrate the possibilities of PUFs as security primitives to our customers. Furthermore, the experience gained in UNIQUE on ASIC design, reliability testing, and PUF use cases will be used to give direction to our future research and development. Combining all of these benefits should lead to an increase in the overall quality of work at Intrinsic-ID (and therefore its products).

TCS: Some UNIQUE technical and technological achievements will be used in the PREMISE project which is more focused on industrial use cases. On the security evaluation side, Thales ITSEF has developed their knowledge on the PUF technology and its evaluation method.

SIRRIX: Some of the results gathered within UNIQUE will already be included in another study regarding the use of PUF technology for electronic-ID cards.

TUD: Not applicable. Since TUD is a university it has no products.

INTEL: As a result of UNIQUE, Intel developed actionable knowledge of PUF technology that can be used as a consideration for future products and technology development.

KULEUVEN: Not applicable.

2.3 Cooperation with external organisations or other projects / programmes

The UNIQUE partners TEC, IID and TCS started on January 1st 2012 the PREMISE No. 287192 project (FP7 managed by Galileo SA) on PRS receivers with embedded hardware intrinsic security enhancements. The UNIQUE partners IID, KUL started working together on February 1st 2012 the new FP7 FET SME project PUFFIN No. 284833 on "Physically unclonable functions found in standard PC components".

Furthermore, follow up projects building forward on the UNIQUE results are being set up both internally and externally for international research projects and collaborations.

These relationships will create opportunities to disseminate the UNIQUE results. Moreover, to achieve the ambitious goal of the UNIQUE project, cooperation with external bodies and organisations is/will be essential for the project success.

The list below shows various cooperations with external organisations or other projects/programmes that are relevant for the UNIQUE project.

Actual/ planned date (dd.mm.yyyy)	**Programme Line**	**Project**	**Cooperation partners**	**Countries addressed** (international/ national – which country)	**UNIQUE partners involved**
01.01.2012	FP7 project	PREMISE	UC Louvain	International	TEC, TCS, IID
01.02.2012	FP7 project	PUFFIN	TUE	International	IID, KULEUVEN, TUD