

Programme Committee

Ronald Cramer
CWI, the Netherlands

Touradj Ebrahimi
EPFL, Switzerland

Franck Leprévost
Université Du Luxembourg

Co-ordinators

Enric Nart
Universitat Autònoma de Barcelona

Jorge Luis Villar
Universitat Politècnica de Catalunya

Acknowledgements. The Conference on Cryptology and Digital Content Security is supported by the “Ministerio de Educación y Ciencia” (ref. MTM2006-26624-E), by the project “Ingenio Mathematica”, and is also an activity of MATH-FSS (Shaping new Directions in Mathematics for Science and Society), a NEST co-ordination action of the EC.

Contents

1	General Information	5
2	Programme	7
4	Abstracts	11
5	List of participants	23

1 General Information

Lecture Room: The course will take place in the CRM “Auditori” located in the Sciences Building (Edifici de Ciències), Universitat Autònoma de Barcelona in Bellaterra.

Secretariat: The Secretariat of the CRM will be available to the participants Monday through Friday from 9:00 am to 5:00 pm.

Computer facilities / working space: The computer space of the CRM will be available for the participants of the conference with the following login information:

username: crmactivities

password: participant

The CRM premises as well as most of the UAB campus have wireless connection.

Library: The library of the Science Building of the UAB will be open from 8:30 am to 7:30 pm on working days.

Breaks: Coffee and cookies will be served during the morning breaks.

Lunch: The CRM provides all participants with free lunch tickets to be used at the Restaurant located in the Science Building of the UAB for the days of the conference in which they are registered. Information on nearby restaurants open for lunch on weekends is given with the documentation package.

Dinner*: A dinner party will take place in Barcelona, on Wednesday, May 16 at a Restaurant in Barcelona (to be announced upon arrival). Please, make sure to sign for the event before Tuesday, May 15 at 1 pm at the Secretariat. Participants can bring a companion by paying the dinner fee at the Secretariat at the time of registration (40 euro).

Cocktail party: A cocktail party for all participants will be organised for Friday, May 18 at 17:30.

Picture: A group picture will be taken one of the days of the conference (to be announced). We will inform you of the day, time and place to meet. The picture will be posted on the conference’s web page.

Questionnaire: Following the directions of the CRM Governing Board, we give a questionnaire to all the people participating in activities at the CRM in order to assess their level of satisfaction. The questionnaire is anonymous and not mandatory, but we would greatly appreciate it if you could answer the questions and return it to us. Thank you for your cooperation.

** Note about the signing up procedure: to sign up for the dinner and the cultural activity you will be asked to pay a 5 euro non refundable fee to confirm your reservation*

Local emergency numbers:

Medical emergency campus number	1800 / 1900 during office hour 2525 at other times
UAB's Science Faculty reception office	1055
General emergency (police, firefighters, ambulances)	112

2 Programme

Monday, May 14 Background and Training

8:30 - 9:00	REGISTRATION
9:00 - 10:00	<i>Reductionist security in cryptography</i> Ronald Cramer, CWI
10:00 - 10:30	Coffee break
10:30 - 11:30	<i>Secret sharing schemes</i> Carles Padró, Universitat Politècnica de Catalunya
12:00 - 13:00	<i>Provable security</i> Serge Fehr, CWI
13:00 - 15:00	LUNCH BREAK
15:00 - 16:00	<i>Post-Quantum Signatures</i> Johannes Buchmann, Technische Universität Darmstadt
16:30 - 17:30	<i>Elliptic curves and discrete logarithm problem</i> Franck Leprévost, Université du Luxembourg

Tuesday, May 15 Background and Training

9:00 - 10:00	<i>Network security</i> Pascal Bouvry, Université du Luxembourg
10:00 - 10:30	Coffee break
10:30 - 11:30	<i>Cryptography and Digital Rights Management</i> Louis Goubin, Université de Versailles
12:00 - 13:00	<i>Information hiding and steganography</i> Jordi Herrera, Universitat Oberta de Catalunya
13:00 - 15:00	LUNCH BREAK
15:00 - 16:00	<i>Watermarking</i> Jean-Luc Dugelay, EURECOM
16:30 - 17:30	<i>Biometrics for the purpose of identity verification</i> Andrzej Drygajlo, EPFL

Wednesday, May 16
**Special activity: Privacy and Security for Citizens,
 Corporations and Governments***

9:00 - 9:30	<i>Digital Rights Management - The enabler of information society</i> Leonardo Chiariglione, CEDEO, Italy
9:30 - 10:00	<i>CASES - a Luxembourg initiative to reduce the digital divide in information security</i> François Thill, Ministère de l'Economie et du Commerce Extérieur, Luxembourg
10:00 - 10:30	<i>Information Warfare - the operational need for national cryptology solutions</i> Bernd Weber, BACO SARL, France
10:30 - 11:00	Coffee break
11:00 - 11:30	<i>Payment Card Industry - Data Security Standards - A real cryptographic application domain</i> Charles Delbrassine, IT Works SA, Luxembourg
11:30 - 12:00	<i>Legal aspects of information security in Europe</i> Bertrand Warusfel, Université de Lille 2, France
12:00 - 12:30	<i>Practical experiences of PKI-enabled applications and implications for mass deployments of e-IDs</i> Victor Canivell, WISeKey, Spain
12:30 - 15:00	LUNCH BREAK
15:00 - 15:30	<i>The new spanish electronic identity card: DNI-e</i> Javier Espinosa, SAFELAYER SA, Spain
15:30 - 16:00	<i>PKI: Social-Economic Impact and cryptographic research expectations</i> Pierre Zimmer, LuxTrust, Luxembourg
16:00 - 16:30	Break
16:30 - 18:00	Round Table

Thursday, May 17
Workshop: Cryptology and Digital Content Security

9:30 - 10:15	<i>Recent Advances in Public-Key Cryptography</i> Eike Kiltz, CWI, The Netherlands
10:15 - 10:45	Coffee Break
10:45 - 11:30	<i>Security of Global Computing Platforms: Authentication and Computed Results Integrity</i> Sébastien Varrette, Univesité du Luxembourg
11:30 - 12:15	<i>State of the Art in Design and Analysis of Stream Ciphers</i> Alexander Maximov
12:30 - 13:00	<i>Privacy technologies in the information society</i> Josep Domingo-Ferrer, Universitat Rovira i Virgili
13:00 - 15:00	LUNCH BREAK
15:00 - 15:30	<i>Fingerprinting-based detection of (modified) image duplicates</i> Yannick Maret, EPFL
15:45 - 16:30	<i>Video surveillance preserving privacy</i> Touradj Ebrahimi, EPFL

Friday, May 18
Workshop: Mathematics of Cryptology. Recent Trends in Secure Computation

9:00 - 10:00	<i>Randomization techniques for secure computation and parallel cryptography</i> Yuval Ishai, Technion
10:00 - 10:30	Coffee break
10:30 - 11:30	<i>Interplays between secure computation, algebra, geometry and coding theory</i> Ronald Cramer, CWI
12:00 - 13:00	<i>Linear Secret Sharing Schemes from High Degree Rational Points on Algebraic Curves</i> Hao Chen, Fudan University
13:00 - 15:00	LUNCH BREAK
15:00 - 16:00	<i>Geometry of multi-variable secret sharing schemes</i> Iwan Duursma, University of Illinois at Urbana-Champaign
16:30 - 17:30	<i>Ideal Multiplicative Linear Secret Sharing Schemes</i> Carles Padró, UPC
17:30 - 18:30	Cocktail party

4 Abstracts

Network Security.

Pascal Bouvry, Université du Luxembourg, Luxembourg

We will present the notion of intrusion detection systems for wired TCP-IP networks. Signature based approaches and anomaly detection will be developed and illustrated on existing systems like Snort. New techniques, including artificial immune systems and evolutionary computing will then be introduced. After that we will overview emerging challenges brought by new generation of wireless networks and in particular trust management for delay-tolerant mobile ad-hoc networks. A game-theoretical approach will eventually be described.

Email address: pascal.bouvry@uni.lu

Post-Quantum Signatures.

Johannes Buchmann, Technische Universität Darmstadt, Germany

All digital signature schemes that are used today in practice will become insecure if sufficiently large quantum computers can be built. In this talk we report about candidates for post-quantum signature schemes that remain secure even in the presence of quantum computers. In particular we explain the Merkle hash tree signature scheme and recent improvements that make this scheme practical.

Email address: buchmann@cdc.informatik.tu-darmstadt.de

Practical experiences of PKI-enabled applications and implications for mass deployments of e-ID's.

Víctor Canivell, Wisekey, Spain

PKI solutions and architectures permeate an ever extending set of networking-based solutions. They allow strong security but are in most cases embedded, so invisible to the user. On the other hand, the expected mass deployments of personal e-ID's have not materialized yet. Main barriers have been the

cost, the complexity and the lack of user applications. We believe these barriers are disappearing due to both technological advances available to consumers, as well as to new paradigms that allow practical scenarios for volume usage. In Spain the National e-ID project will certainly be an enabler, and we expect a significant ripple effect on the usage of easy-to-manage and economical corporate e-ID's, integrated into the daily enterprise applications, both at the front- and back-offices.

Email address: vcanivell@es.wisekey.com

Linear Secret Sharing Schemes from High Degree Rational Points on Algebraic Curves.

Hao Chen, Fudan University, China

From the paper on R.J.McEliece and D.V.Sarwate in 1979 (the same year when Shamir and Blakley proposed the secret sharing and gave their first example of threshold secret sharing scheme) and the paper of J.L.Massey in 1995, it is well-known that ideal linear secret sharing schemes can be constructed from error correcting codes. In 2006, ideal linear secret sharing schemes (LSSS) from algebraic-geometric codes and their applications in secure multi-party computation were proposed and studied. In this talk we describe the construction of non-ideal LSSS from high degree rational points on algebraic curves. These LSSS are strongly multiplicative and thus can be applied in secure multi-party computation naturally. We give some explicit examples of weight threshold secret sharing schemes based on high degree rational points on elliptic curves. Some of our constructed weight threshold secret sharing schemes have their information rate attaining the lower bound of C.Padro and G.Saez in 2000.

This is a joint work with R.Cramer(CWI), Cunsheng Ding(Hong Kong University of Science and Technology), San Ling(Nanyang University of Technology, Singapore) and Chaoping Xing(National University of Singapore).

Email address: hchen@cs.ucdavis.edu

Digital Rights Management - The enabler of information society.

Leonardo Chiariglione, CEDEO, Italy

DRM is probably the most pervasive of digital technologies because they can potentially support the mapping to the digital space of most functions that humans have performed in the physical space. The talk will examine some of the roadblocks preventing the exploitation of the technologies and propose a path for their removal.

Email address: info@chiariglione.org

Payment Card Industry - Data Security Standards - A real cryptographic application domain.

Charles Delbrassine, IT WORKS S.A., Luxembourg

Data security, credit card fraud and identity theft are hot topics around the globe in any industry. Companies are concerned about protecting databases that contain confidential information on customers and employees. The United States Federal Trade Commission estimates that as many as 10 million Americans have their identities stolen each year and there are numerous press headlines about the topic on any give day.

In response to this threat, the Payment Card Industry (PCI) Data Security Standard (DSS) was created by major credit card companies to safeguard customer information. PCI DSS represents a common set of industry tools and measurements to help ensure the safe handling of sensitive information.

PCI compliance mandates that merchants and service providers meet minimum standards of security to protect confidential customer information. The risk of data theft is an enormous liability for any organization because the credit card associations will levy fines on the offending organization and the public will lose confidence in that company. There are 12 steps required to ensure an organization is in compliance with PCI standards. [View Compliance Standards](#)

The standard is enforced by merchant banks (on behalf of the networks) and penalties for non-compliance can be as much as \$500,000 per incident, not to mention the cost of making headline news as a result of data integrity compromises.

PCI standards, which apply to store merchants, banks, service providers and card processors, aim to reduce the risk of a security threat by mandating the proper use of various technologies and data encryption. Cryptography is becoming a day to day challenge for these companies which are not really expert in this domain.

Email address: cdelbrassine@itworks.lu

Privacy technologies in the information society.

Josep Domingo-Ferrer, Universitat Rovira i Virgili, Spain

New services for the Information Society are appearing at an ever faster rate. From location-based services for roaming users or cars to RFID, from digital rights management to intrusion detection systems, from electronic payments to data mining and warehousing, an amazing plethora of new technologies are being launched and justified with the argument of increasing the security and the satisfaction of consumers. While more efficient and secure transactions may indeed benefit the consumers, corporate profits are too often the only driving force behind the development of those new technologies. Not surprisingly then, transaction security tends to emphasize corporate security more than consumer privacy and security. Worse yet, transaction privacy, which is basically a consumer requirement, tends to be given low priority, if considered at all. The talk will give an overview of privacy problems and technical solutions in the above-mentioned areas.

Email address: josep.domingo@urv.cat

Biometrics for the purpose of identity verification.

Andrzej Drygajlo, Ecole Polytechnique Fédérale de Lausanne, Switzerland

With an increase in identity fraud and the emphasis on security, there is a growing and urgent need to efficiently identify humans both locally and remotely on a routine basis. The appearance of electronic identity documents as applied to new technologies for passports, visas, national identity cards, drivers' licenses and health insurance cards, has triggered a real need for reliable, user-friendly and widely acceptable automated methods for checking the identity of an individual. Biometrics is a relatively new area of technology that uses unique and measurable biological and behavioural traits of individuals to automatically establish or verify their identity. The talk provides a valuable insight into the state-of-the-art of this technology which must strike the right balance between security, user convenience and privacy. It presents some of the salient research issues that need to be addressed for making biometrics an effective tool for providing a user-convenient component of the secure person-identity linkage.

Email address: Andrzej.Drygajlo@epfl.ch

Introduction to Digital Watermarking.

Jean-Luc Dugelay, Eurecom, CMM, France

Watermarking allows owners or providers to hide an invisible and robust message inside a digital Multimedia document, mainly for security purposes such as owner or content authentication. There exists a complex trade-off between the different parameters: capacity, visibility and robustness. This lecture will give an introduction to digital watermarking in image and video, will present basic existing algorithms (ie state-of-the-art), and possible applications of watermarking technologies. It will also cover the general problem of robustness and evaluation. **Email address:** Jean-

Luc.Dugelay@eurecom.fr

Geometry of multi-variable secret sharing schemes.

Iwan Duursma, University of Illinois at Urbana-Champaign, USA

In the Shamir secret sharing scheme, participants recover the secret from interpolating a function $f(x)$ through their shares $(a, f(a))$. For schemes that use a two variable polynomial, the participants need to interpolate through points $(a, b, f(a, b))$ to recover information about $f(x, y)$. It is in general not clear how many participants are needed for a correct interpolation and the access structure depends on the configuration of the assigned points. We describe the access structure for two special cases : (1) the points (a, b) assigned to the participants form a rectangular grid in the xy -plane, or (2) the points lie on an algebraic curve $F(x, y) = 0$.

Email address: duursma@math.uiuc.edu

The New Spanish Electronic Identity Card: Dni-E.

Javier Espinosa García, PricewaterhouseCoopers, Spain

The new Spanish Electronic Identity Card (DNI-e) provides a modern and secure identifying way for Spanish citizens as well as digital signature capabilities and confidence in Information Society. In this work the main physical

(card and chip) and logical (certificates, digital signature, and keys) properties of the DNI-e, are shown. Moreover, we put special emphasis on the public key infrastructure (PKI) that supports its development and future use.

Email address: javier.espinosa.garcia@es.pwc.com

Zero-knowledge proofs and a methodology for defining security.

Serge Fehr, CWI, Netherlands

I introduce and discuss the notion of an interactive proof, and in particular that of a zero-knowledge (interactive) proof. A zero-knowledge proof allows a prover P to convince a verifier V that he knows a proof p of some statement X , and thus in particular that X is true, without giving away any information on p . As a matter of fact, V learns no information at all beyond that X is true. In particular, V will not be able to convince a third party of the truth of X (unless it knew a proof beforehand). Zero-knowledge proofs are of fundamental importance in modern cryptography and have many applications, of which I discuss a few. The second part of my talk is dedicated to the problem of what exactly it should mean for a cryptographic scheme to be secure. I present what is currently considered to be "the right" approach for defining (and thus proving) security of a general cryptographic scheme. The idea is to require that the scheme, even when under attack, has to behave like a trusted party that honestly executes the task to be implemented.

Email address: Serge.Fehr@cwi.nl

Cryptography and DRM.

Louis Goubin, University of Versailles, France

When studying the security model for Digital Right Management (DRM), it is easy to observe that it substantially differs from classical internet security models. In particular, the difficulty for content providers consists in delivering content (music, video, software, ...) to legitimate users across a hostile network which cannot be assumed to be trusted. Moreover, the user itself cannot be trusted, and may also deploy many resources to attack

the content protection mechanisms (hardware or software) installed by the content owner.

In this talk, we will try to show how cryptography can (and sometimes cannot) be used to avoid various attacks against digital content distribution. Such a cryptographic concept is embodied by traitor tracing schemes, which are encryption systems able to provide protection against key leakage. In a traitor tracing scheme, if a key is compromised by a pirate, the content owner will be able to identify the compromised key(s). A second kind of cryptographic mechanism is given by the so called broadcast encryption schemes, which are encryption systems allowing the revocation of compromised keys. In another direction, some techniques have been borrowed from the information hiding theory: watermarking and fingerprinting aim at including a digital mark into the content, thus personalizing the file to its owner or its licensee. Finally, software obfuscation methods are very interesting to make code reverse-engineering very difficult, and can be used together with tamper-resistant device.

In this talk, we will give an overview of some algorithms, including recent research results, and examples taken from real applications in the distribution of digital content.

Email address: Louis.Goubin@prism.uvsq.fr

Information hiding and steganography.

Jordi Herrera, Universitat Oberta de Catalunya, Spain

Steganography is often defined as the art of stealth communication and is also known as Information Hiding. In this talk we will present the main definitions and basic concepts of steganography. We will also review the state of the art of such technology and the more relevant achievements in the field. Finally we will point out the main applications of information hiding, mainly in the field of digital watermarking.

Email address: jherreraj@uoc.edu

Randomization techniques for secure computation and parallel cryptography.

Yuval Ishai, Technion, Israel

To what extent can we simplify computations if we settle for producing a randomized encoding of their output? This talk will survey algebraic techniques for tackling this problem and their applications to secure computation and parallel cryptography. In particular, I will show that under standard assumptions it is possible to carry out useful cryptographic operations (such as encryption) by functions in which every bit of the output depends on at most four bits of the input.

The talk is based in part on joint works with Benny Applebaum and Eyal Kushilevitz.

Email address: yuvali@cs.technion.ac.il

Recent Advances in Public-Key Cryptography Abstract.

Eike Kiltz, Centrum voor Wiskunde en Informatica, Netherlands

In this talk we will survey several recent “hot topics” in public-key cryptography including bilinear pairings and identity-based encryption

Email address: kiltz@cwi.nl

Elliptic curves and discrete logarithm problem.

Franck Leprévost, Université du Luxembourg, Luxembourg

The security of Public-key cryptosystems is based on mathematical problems, like the integer factorization problem, or the discrete logarithm problem (DLP). One can express the DLP in any finite cyclic group, and one important aspect is to find suitable groups where it seems to be difficult to solve the DLP. Such groups are provided as subgroups of the group of rational points of an elliptic curve defined over a finite field. In this tutorial, we shall explain this, and some of the methods used to tackle the DLP in this situation.

Email address: Franck.Leprevost@uni.lu

Fingerprinting-based detection of (modified) image duplicates.

**Yannick Maret, Ecole Polytechnique Fédérale de Lausanne,
Switzerland**

In this presentation, I will first describe the problem of image duplicate detection as well as existing approaches. Then, fingerprinting-system will be compared to the more classical watermarking approach. Finally, an actual fingerprinting-based duplicate detection system, developed at EPFL, is presented. By duplicate, it is referred not only to a bit exact copy of a given reference image, but also to modified versions of the image after minor manipulations, malicious or not, as long as these manipulations do not change the perceptual meaning of the image content. In particular, duplicates include all variants of the reference image obtained after common image processing manipulations such as compression, filtering, adjustments of contrast, or saturation of colours. The described image duplicate detection system can be applied to “copyright infringement detection” by identifying variations of a given copyrighted image. Another application is to “discover known illicit content” such as child pornography images known to the police.

Email address: yannick.maret@epfl.ch

State of the Art in Design and Analysis of Stream Ciphers.

Alexander Maximov, Université du Luxembourg, Luxembourg

Stream ciphers are basic primitives which are used to ensure confidentiality of information. They achieve good performance in software and hardware in terms of speed, footprint size and security, and could be a potential alternative to block ciphers. There have been many attempts to design a good candidate, including the project NESSIE. However, most of the new designs suffer from the security. In this talk we will describe various design techniques and introduce different cryptanalysis methods used in modern cryptography, we also support them by giving several examples, such as RC4, A5/1, and others.

Email address: alexander.maximov@uni.lu

Secret Sharing Schemes.

Carles Padró, Universitat Politècnica de Catalunya, Spain

Secret sharing schemes, which are a fundamental tool in many cryptographic protocols, were introduced by Shamir in 1979. The properties of Shamir’s

scheme are discussed in all depth and they are used as a starting point to present the main further results and open problems about this topic.

Email address: matcpl@mat.upc.es

Ideal Multiplicative Linear Secret Sharing Schemes.

Carles Padró, Universitat Politècnica de Catalunya, Spain

Multiplicative linear secret sharing schemes are a fundamental tool in the construction of secure multiparty computation protocols for general adversaries. Two different kinds of multiplicative properties have been defined for linear secret sharing schemes: the weak one and the strong one. As a consequence of the results by Cramer, Damgård, and Maurer (Eurocrypt 2000), it is possible to efficiently transform any given LSSS into a weakly multiplicative scheme by duplicating its complexity. The existence of an analogous efficient construction for strongly multiplicative LSSS is an open problem.

In this talk, we focus on the construction of ideal multiplicative LSSSs, that is, multiplicative schemes with optimal complexity. Specifically, we study the characterization of the access structures of these schemes. For weakly multiplicative schemes, this is related to an open problem about the representability of identically self-dual matroids by self-dual codes. The last results on this problem are presented and some ideas and techniques to go further in its solution are discussed. Much less is known for the strong multiplication case. Nevertheless, we present a negative result about the existence of ideal strongly multiplicative schemes. Finally, we discuss how the algebraic-geometric construction by Chen and Cramer (Crypto 2006) can be applied to this problem.

Email address: matcpl@mat.upc.es

CASES - a Luxembourg initiative to reduce the digital divide in information security.

François Thill, Ministère de l'Économie et du Commerce extérieur, Luxembourg

Education of Small and Medium-Sized Enterprises (SMEs) and citizens about information security is a prerequisite for the growth, if not survival,

of our information society. CASES focuses on helping raise awareness and providing support in IT security prevention within these two target groups. Increasing citizens' and/or SMEs' trust and confidence in an information society will help them become more engaged in the aforementioned society while, most importantly, enabling them to benefit from e-commerce and e-government services. Without increased awareness and prevention for home-users and SMEs, the frequency of attacks may continue at its current frightening speed, while severely harming economies.

Email address: francois.thill@eco.etat.lu

Security of Global Computing Platforms: Authentication and Computed Results Integrity.

Sébastien Varrette, Université du Luxembourg, Luxembourg

Nowadays, High-Performance Computing could be achieved through parallel and distributed platforms. While the former architecture consists in supercomputers which exploit a hardware parallelism, the latter gather at low cost hundreds or thousands of nodes geographically scattered through the Internet. This talk will give an overview of the different types of distributed systems – from clusters to desktop grids – before focusing on some security issues raised by those architectures. In particular, some examples of authentication systems will be expounded. Then, a large part of the talk will detail probabilistic approaches used to check the integrity of program executions in such environments, where tasks or their results could have been corrupted due to benign or malicious act. More precisely, probabilistic certification by massive attack detection is presented. The execution to certify is represented by a macro-dataflow graph which is used to randomly extract some tasks to be re-executed on safe resources in order to determine whether the execution is correct or faulty. Bounds associated with an eventually parallel certification are provided for general graphs, trees and Fork-Join graphs. Note that this latter form of graph represents Divide & Conquer algorithms which are often used in linear algebra and cryptographic computations.

Email address: Sebastien.Varrette@imag.fr

Information Warfare - the operational need for national cryptology solutions.

Bernd Weber, BACO S.ä.r.l., Luxembourg

Information Warfare is a fact of daily life. Government organizations, above all the US National Security Agency (NSA), are very actively engaged in industrial espionage in order to provide a competitive edge for their own industry. Disrespect for international law is widespread and therefore there is no legal protection against such activities. The NSA tries to gain a firm grip on crypto keys all over the world. The only protection will lie in the development of cryptographic solutions that are out of reach of the spy organizations. However, there are legal restrictions that make it particularly difficult to attain such an aim.

Email address: b.weber@baco.lu

PKI: Social-Economic Impact and cryptographic research expectations.

Pierre Zimmer, LuxTrust, Luxembourg

PKI should not be seen as a collection of technology processes. When developing PKI enabled applications we have to keep in mind how society will be impacted and that electronic identities will affect considerably our everyday life in the near future. Trust in information security is crucial to eCommerce and trust can only be obtained if certain conditions of communication, security and data privacy are fulfilled . We will see how research in cryptology can eventually contribute to reach those goals and allow companies to come up with ergonomic security solutions coping with the conflicting interests of security and data privacy.

Email address: pierre.zimmer@mfp.etat.lu

5 List of participants

Akharraz, Ismail	i_akharraz@hotmail.com
Aranés, Maria Teresa	pmxmta@nottingham.ac.uk
Bouvry, Pascal	pascal.bouvry@uni.lu
Buchmann, Johannes	buchmann@cdc.informatik.tu-darmstadt.de
Canivell, Victor	vcanivell@es.wisekey.com
Cao, Hongjun	hongjun.cao@urjc.es
Cascudo Pueyo, Ignacio	icascudo@orion.ciencias.uniovi.es
Chen, Hao	hchen@cs.ucdavis.edu
Chiariglione, Leonardo	info@chiariglione.org
Cramer, Ronald	Ronald.Cramer@cwi.nl
de Haan, Robbert	R.de.Haan@cwi.nl
Delbrassine, Charles	cdelbrassine@itworks.lu
Demirkiran, Cevahir	cevomed@gmail.com
Domingo-Ferrer, Josep	josep.domingo@urv.cat
Drygajlo, Andrzej	Andrzej.Drygajlo@epfl.ch
Dugelay, Jean-Luc	Jean-Luc.Dugelay@eurecom.fr
Duursma, Iwan M.	duursma@math.uiuc.edu
Ebrahimi, Touradj	Touradj.Ebrahimi@epfl.ch
El Aïmani, Laila	elaimani@bit.uni-bonn.de
El Fadil, L Houssain	lhouelfadil@hotmail.com
Espinosa García, Javier	javier.espinosa.garcia@es.pwc.com
Fehm, Arno	afehm@gmx.de
Fehr, Serge	Serge.Fehr@cwi.nl
Fosson, Sophie	s.fosson@sns.it
Goubin, Louis	Louis.Goubin@prism.uvsq.fr
Heidarvand, Somayeh	heidarvand@iasbs.ac.ir
Herranz, Javier	jherranz@mat.upc.es
Herrera, Jordi	jherreraj@uoc.edu
Heymann Pignolo, Marc	mheyman@ma4.upc.edu
Ishai, Yuval	yuvali@cs.technion.ac.il
Kiltz, Eike	kiltz@cwi.nl
Kobara, Kazukuni	kobara_conf@m.aist.go.jp
Kulesza, Kamil	kamil.kulesza@ippt.gov.pl
Lavigne, Camille	camille.lavigne@info.unicaen.fr
Lee, Pil Joong	pjl@postech.ac.kr
Leprévost, Franck	Franck.Leprevost@uni.lu
Maret, Yannick	yannick.maret@epfl.ch
Martínez, Santi	santi@diei.udl.es

Maximov, Alexander	alexander.maximov@uni.lu
Morra, Anna	anna.morra@math.u-bordeaux1.fr
Murtaza, Ghulam	azarmurtaza@hotmail.com
Nart Viñals, Enric	nart@mat.uab.es
Otmani, Ayoub	ayoub.otmani@info.unicaen.fr
Padró Laimon, Carles	matcpl@mat.upc.es
Pedgaonkar, Anil	anilped@hotmail.com
Puche Coto, Pelayo	ppuche@gmail.com
Pujolàs, Jordi	jpujolas@matematica.udl.es
Radomirovic, Sasa	sasar@math.rutgers.edu
Rafols, Carla	crafols@ma4.upc.es
Rauf, Abid	abid.rauf@gmail.com
Saez, German	german@ma4.upc.edu
Sánchez Meneses, Julia	julia@ipsa.es
Thill, François	francois.thill@eco.etat.lu
Tomàs, Rosana	rosana@matematica.udl.es
Torreao Dassen, Erwin	dassen@math.leidenuniv.nl
Valdés César, José Manuel	jose.manuel.valdes.cesar@es.pwc.com
Varrette, Sébastien	Sebastien.Varrette@imag.fr
Vázquez, Leonor	leonor@ma4.upc.es
Villar Santos, Jorge Luis	jvillar@mat.upc.es
Warusfel, Bertrand	bertrand.warusfel@univ-lille2.fr
Weber, Bernd	b.weber@baco.lu
Zimmer, Pierre	pierre.zimmer@mfp.etat.lu