www.cryptobg.org

International Summer School

CryptoBG*2012 [MC^{3}D]

MEET CHALLENGES IN CRYPTOGRAPHY AND CYBER-DEFENSE

28 July - 5 August 2012, Oriahovitza, Bulgaria

Programme

[MC^{3}D]	9:30-11:00	11:30 - 13:00	14:30 - 16:00	16:30-18:00
S 29-Jul	09:30 Registration **10:00 Opening**	**Malika** Cryptography Basics [Introduction]	**Jetchev-1** Intro to Elliptic Curves	**Sharkov-1** Intro to Security and Resilience Management
M 30-Jul	**Nicolas-1** Intro to lattice based cryptography	**Seacord-1** Secure Coding Principles	**Valerie-1** Intro to code based cryptography	**Gabriel** Pairing based cryptography
			Seacord's Lab	**Seacord** [discussion] Dangerous Optimizations and the loss of causality
T 31-Jul	**Nicolas-2** Intro to lattice based cryptography	**Seacord-2** Secure Coding Principles	**Valerie-2** Intro to code based cryptography	**Antonio** Impact of Privacy-by-design on ICT
				[discussion]
			Seacord's Lab	
W 1-Aug	**Ben-1** Intro to Elliptic Curve Cryptography	**Birov-1** Software Architecture-Based Security	[surprise ;-]	
T 2-Aug	**Sharkov-2** Intro to Security and Resilience Management	**Tselkov-1** Models for Cryptographic Keys Distribution	**Tselkov-2** Formal Model of Multilayer Cryptographic System	**Security, Smart Defense & NATO** [discussion]
F 3-Aug	**Ben-2** Intro to Elliptic Curve Cryptography	**Manev-1** Hardness of algorithmic tasks	**Birov-2** Software Architecture-Based Security	[discussion]
S 4-Aug	**Jetchev-2** Intro to proxy re-encryption	**Manev-2** Hardness of algorithmic tasks	[surprise :-]	[musical surprise]
S 5-Aug	**Jetchev-3** Secure Storage in the Cloud and Methods for Key Management	**What's next** [discussion]		

Organized by: Balkanski-Panitza Institute for Advanced Studies (BPIAS), European Software Institute – Center EasternEurope (ESI CEE), and Minu Balkanski Foundation

Organizing Committee: Prof. Minko Balkanski, IHE, France, Dr. George Sharkov, ESI CEE, Bulgaria
Dr. Dimitar Jetchev, EPFL, Switzerland Mariya Georgieva, Université de Caen, France

Dr. Dimitar Jetchev

EPFL, Switzerland
jetchev@gmail.com, dimitar.jetchev@epfl.ch

"Introduction to Elliptic Curve Cryptography"
"Introduction to Secure Coding in the Cloud"
"Cloud Security and Proxy Re-encryption"

Dr. Dimitar Jetchev currently holds a research position at the Laboratory for Cryptologic Algorithms at EPFL supervised by Professor Arjen K. Lenstra. He specializes in the area of number theory and computational number theory with applications to cryptology. He completed his B.A. in mathematics from Harvard University in 2004 and a M.A. and Ph.D. in mathematics at UC Berkeley under the supervision of Professor Kenneth A. Ribet. He specializes in elliptic curves, Selmer groups and Euler systems. On the side of mathematical cryptology, Dimitar Jetchev works on different questions related to fundamental hardness assumptions from elliptic curve cryptography and bit security. In 2006/7, he won a Microsoft Research graduate fellowship award and has been subsequently collaborating with various groups. He is currently involved in projects on cloud security for both Microsoft SQL Azure and AlephCloud, a startup based in the Silicon Valley.

Introduction to Elliptic Curve Cryptography

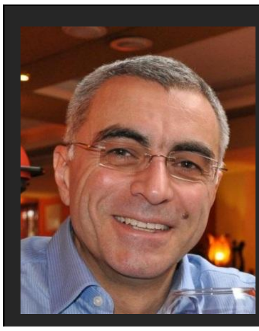
The talk will start by introducing the discrete logarithm problem - one of the fundamental problems in cryptography whose hardness is essential for the security of various basic cryptographic protocols and scheme such as ElGamal encryption, Diffie--Hellman key exchange and the digital signature algorithm among others. We will then discuss the index calculus method and the advantage of using elliptic curve groups as opposed to multiplicative groups of finite fields. We will give a brief historical overview of elliptic curves and will then introduce Weierstrass models of elliptic curves, group structures over finite fields, morphisms, isomorphisms and j-invariants of elliptic curves, endomoprhism rings and isogenies.

Introduction to Secure Storage in the Cloud

Cloud security has become an incredibly popular area in the last couple of years due to the economic insentives of using the cloud for storage and data sharing as well as for trusted computing. In this talk, I will discuss some practical open questions related to data encryption and key management in the context of the cloud and will use as an example Microsoft SQL Azure Trusted Services. We will discuss a model for key management that relies on secret sharing and threshold cryptography. Finally, we will discuss potential cross-platform implementation of the scheme built on the top of the recently developed Stanford Javascript Crypto Library (SJCL). The latter is to be used for building the MS SQL Azure trusted services. We will introduce the library and discuss some of the efficiency issues with cryptography in Javascript (both in symmetric and in public key cryptography).

Cloud Security and Proxy Re-encryption

Proxy re-encryption is a method allowing a semi-trusted proxy to modify a ciphertext encrypted with Alice's public key in such a way that Bob can decrypt the modification with its private key without the proxy being able to decrypt the plaintext. Proxy re-encryption has numerous applications in forwarding encrypted email, law enforcement monitoring, content distribution and more generally in cloud security. The talk will start by introducing the basic re-encryption scheme of Blaise--Blumer--Strauss from 1998 used for modifying ElGamal encryption. We will explain the drawbacks of the scheme and will discuss some subsequent modifications that address some of the issues. Finally, we will discuss a key management scheme based on proxy re-encryption that effectively utilizes the cloud for cryptographic computation while supporting a frequently-changing mobile users that do not need to trust the cloud provider.



Dr. George Sharkov

European Software Institute - Center Eastern Europe (ESI CEE), Bulgaria
gesha@esicenter.bg

“Intro to Security and Resilience Management (From Cyber-Defense to resilient business)”
[Resilience Management Model-RMM, CERT, Carnegie Mellon]

Dr. George Sharkov graduated Mathematics and Computer Science at Sofia University, has PhD in Artificial Intelligence, research in applied informatics, biophysics, thermography and genetics (Gent, Belgium), enterprise information systems architectures. After 1994 leading international projects and multi-national teams for financial and banking systems, e-business, online markets (France, USA, Israel, global markets).

Since 2003 he is managing the Eastern European regional excellence center (ESI CEE, www.esicenter.eu) of the European Software Institute (www.esi.es), covering 12 countries in Eastern Europe and Caucasus region. He is instructor in SPI (Software Process Improvement), software engineering quality and management, implementation of CMMI (SEI, Carnegie Mellon), IT Mark appraiser (ESI method for SMEs). George is leading a research network in Cyber Defense and business resilience, member of the appraiser apprentice program on RMM (Resilience Management Model, CERT at SEI).

Dr. Sharkov is lecturing Software Quality (CMMI) at Sofia University and a new Digitized Ecosystems. He is leading a Program for modernization of Software Engineering Management education (SEMP) in partnership with Carnegie Mellon University and 6 Bulgarian universities. Steering Committee member of the EC CEN Workshop in ICT-skills and expert on e-competences.

George is among the founders and the first Chairman of BASSCOM (Bulgarian Association of Software Companies, PIN-SME founder), initiator and promoter of the regional ICT brand initiative (SEE-IT), a founder and board member of the Bulgarian ICT Cluster. He is Program Committee member of 5 international conferences, jury member of national and international ICT contests, Grand Jury and Board member of the WSA contest under UN WSIS.

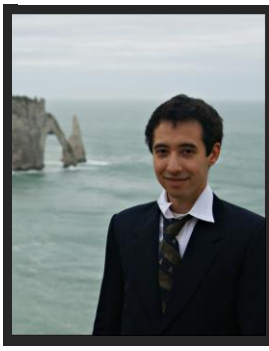
This mini-tutorial training introduces the new “Resilience Management Model - RMM” of CERT at Software Engineering Institute (SEI, Carnegie Mellon), with a particular focus on:

How well is your organization prepared to handle operational risk?
Is it about Cyber-security only and what are the current threats and vulnerabilities to our business?
When faced with disruption and stress, will your organization's most important assets - people, information, technology, and facilities - stay productive?
If and how quickly your organization could recover to normal operations after disruptions?
How to assess and continuously improve our readiness to “handle the unknown”?

**For more information on the RMM please visit*: http://www.sei.cmu.edu/training/P66.cfm or http://www.cert.org/resilience/rmm.html

CERT-RMM serves as a foundation from which an organization can measure its current competency, set improvement targets, and establish plans and actions to close any identified gaps. As a result, the organization repositions and repurposes its security and business continuity activities and adopts a process improvement mindset that helps to keep services and assets productive in the long term.

CERT-RMM comes from the creators of the set of “maturity models” – Software Engineering Institute (SEI, Carnegie Mellon), which evolved for 20 years from defense industry standards to de-facto global quality models. These are CMMI for Development, CMMI for Services and CMMI for Acquisition, as well as People CMM and the famous PSP/TSP of Watts Humphrey, and since 2010 - RMM. With similar structure, appraisal method and process improvement orientation, the RMM serves as a meta-framework based on the best practices and strong areas of multiple complementary established models and standards (like the various ISOs on Information Security, Services; CoBIT; business and IT - ITIL, SPICE; CMMI-SVC, etc.). The 26 process areas structured in the 4 categories of the model cover and bridge the usually separated governance of corporate security, information security and business continuity. Thus, RMM is not “yet another model”, but a comprehensive and complete reference model or framework to help the organizations in maintaining the multi-standard compliances and certifications through unified enterprise policy and optimized resources and investments, without creating additional bureaucratic burden. The examples provided for sectors like banking & finances, public services, as well as international collaboration and international policies based on it will enable the participants to identify the real benefits and the suitable approach for their organizations.



Dr. Nicolas Gama

Université de Versailles, France
nicolas.gama@prism.uvsq.fr

"Introduction of lattice based cryptography"
[GGH, NTRU, LWE, Worst-Case to Average-Case reduction]

Nicolas Gama is Assistant Professor at the PRiSM laboratory of University of Versailles.

He studied Foundations of Computer Sciences at the Ecole Normale Supérieure, and specialized himself in the domains of Algorithmic and Cryptology.

He made his PhD under the supervision of Phong Nguyen on Geometry of numbers and its applications to Cryptology, and graduated in 2008. He made two post-docs at the university of Caen and at EPFL in Lausanne, and joined the Crypto team of Versailles in 2010.

After defining what is a lattice, we review the main algorithms to solve the famous shortest vector problem (SVP) and the closest vector problems (CVP). Some of these algorithms, like sieving and Voronoi cell Computation, have a simply exponential complexity even on sparse lattices. Other algorithms, like LLL and its blockwise extensions run in polynomial time, but should only achieve an exponential approximation factor. In practice, these algorithm behave better than expected, allowing to approximate the optimal solutions to a factor lower than 3 in dimensions as high as 200.

At first, lattices were used in Cryptanalysis in order to solve not only linear problems, but also more generic problems of number theory: factorization of rational polynomials, factorization of specific integers.

Lattice reduction algorithms were so powerful in practice that the first cryptosystems based on subset sum or euclidean spaces were all broken (Merkle Hellmann, first attempts of GGH and NTRUSign).

However, an unexpected turn of events occurred with Ajtai's discovery of a worst-case to average case proof for lattice problems. By increasing the parameter size and preserving a polynomial density, average instances of lattice problems in specific classes are harder than approximating the worst case lattice problems. We explain in this course a variant of his reduction, which proves that the dense modular subset sum in average is harder than approximate lattice reduction in the worst case, and explain a few new-generation lattice-based cryptosystems based on worst-case security.

Robert C. Seacord

CERT, SEI, Carnegie Mellon University, Pittsburgh, USA
rcs@cert.org

"Secure Coding Principles" + 4 Secure Coding Workshops [on 30 & 31 July]

Robert C. Seacord leads the Secure Coding Initiative at CERT, located in Carnegie Mellon University's Software Engineering Institute (SEI) in Pittsburgh, PA. The CERT, among other security related activities, regularly analyzes software vulnerability reports and assesses the risk to the Internet and other critical infrastructure. Seacord is an adjunct professor in the Carnegie Mellon University School of Computer Science and in the Information Networking Institute and part-time Faculty at the University of Pittsburgh.

Seacord started programming professionally for IBM in 1982, working in communications and operating system software, processor development, and software engineering. Robert also has worked at the X Consortium, where he developed and maintained code for the Common Desktop Environment and the X Window System.

Seacord is a technical expert for the ISO/IEC JTC1/SC22/WG14 international standardization working group for the C programming language.

Secure Coding in C and C++

This course provides a detailed explanation of common programming errors in C and C++ and describes how these errors can lead to code that is vulnerable to exploitation. The course concentrates on security issues intrinsic to the C and C++ programming languages and associated libraries. The intent is for this course to be useful to anyone involved in developing secure C and C++ programs regardless of the specific application.

The course assumes basic C and C++ programming skills but does not assume an in-depth knowledge of software security. The ideas presented apply to various development environments, but the examples are specific to Microsoft Visual Studio and Linux/GCC and the 32-bit Intel Architecture (IA-32). Material in this presentation was derived from the Addison-Wesley books *Secure Coding in C and C++* and *The CERT C Secure Coding Standard*.

Who should attend?

This course is designed for C and C++ developers.

The focus of this short course will be the use of strings in C and C++ programs. We will examine basic concepts, common coding errors and how these may be exploited, and mitigation strategies. Examples are taken from both the Microsoft Visual Studio and GCC compilers on Windows and Linux platforms.

An online demonstration version of the strings and integer modules from this course can be accessed at http://oli.web.cmu.edu. Enter the course key: scodedemo.

Objectives

Participants should come away from this course with a working knowledge of common programming errors that lead to software vulnerabilities, how these errors can be exploited, and effective mitigation strategies for preventing the introduction of these errors. In particular, participants will learn how to

- improve the overall security of any C or C++ application
- thwart buffer overflows and stack-smashing attacks that exploit insecure string manipulation logic

Moreover, this course encourages programmers to adopt security best practices and develop a security mindset that can help protect software from tomorrow's attacks, not just today's.

Prerequisites and Required Equipment

It is recommended that participants have a basic to intermediate understanding of the C and C++ programming languages. Software security knowledge or experience is not required.

Students must bring a personal computer equipped with:

- 3GB or greater of free hard disk space
- C and C++ programming language development environments (compiler, editor, etc.)
- CD-ROM or memory stick
- the latest version of Adobe Reader (this can be downloaded from http://www.adobe.com/products/acrobat/readstep2.html)

Dr. Valérie Gautier

Université de Caen, France
valerie.gauthier01@unicaen.fr

"Introduction of code based cryptography"

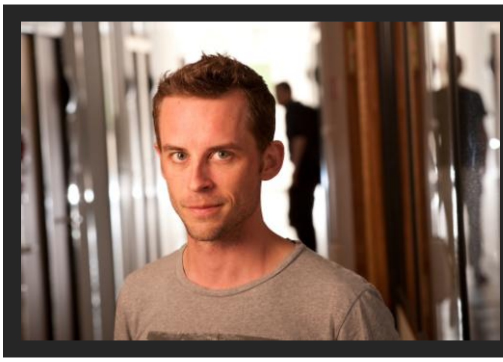
I studied mathematics at the University of Los Andes in Bogotá (Colombia). I did the master Erasmus-mundus ALGANT (Algebra, Geometry and Number Theory), the first year at the Université de Bordeaux 1 in France and the second at the Università degli Studi di Padova in Italy. I did my PhD studies at the Department of Mathematics of the Technical University of Denmark (DTU) under the supervision of Lars R. Knudsen and Gregor Leander. At the moment I am a post-doct at the Université de Caen, France.

The main goal of this course is to give an introduction to code-based cryptography. The course will be divided in two parts: In the first part, we will introduce coding theory, give the main definitions, explain how to encode and decode a message using linear codes and give some examples. In the second part we will see an overview of code-based cryptography. We will introduce McEliece's cryptosystem that is the first public-key encryption scheme based on the hardness of decoding random (looking) linear codes. And we will do an overview of the main attacks, the security proof, some of its variants and one signature scheme based in this cryptosystem.

[Recommended articles]

[1] J. Justesen and T. Hoholdt A Course in Error-Correcting Codes. European Mathematical Society, 2004
[2] F. MacWilliams and N. Sloane. The theory of error-correcting codes. North Holland, Amsterdam, 1977
[3] D. Bernstein, J. Buchmann, and E. Dahmen, editors. Post-Quantum Cryptography. Springer, 2009

Two good references for coding theory are [1] and [2] and a good reference for post-quantum and code-based cryptography is [3].



Dr. Benjamin Smith

INRIA, Ecole Polychechnique, France
smith@lix.polytechnique.fr

"Introduction to Elliptic Curve Cryptography"

Ben Smith is an Australian researcher in asymmetric cryptography, working in France, where he is a permanent researcher at INRIA (a French public research institute for computing and applied maths) and a teacher at the École polytechnique. His research applies algorithmic arithmetic geometry, and computational number theory to asymmetric cryptographic primitives. He is particularly interested in algorithms for the construction of efficient curve-based cryptosystems, as well as their cryptanalysis.

After studying in the computational algebra and number theory research groups at the university of Sydney, Ben moved to London as a postdoctoral research assistant in the Information Security Group at Royal Holloway, University of London. He has been a member of the Cryptography and Coding Theory group (INRIA project-team GRACE, formerly known as TANC) at LIX, the computing laboratory of the École polytechnique, since November 2007.

Elliptic Curve Cryptography represents the state of the art in modern asymmetric (public-key) cryptography. It offers better per-bit security efficiency than the famous RSA suite of tools, and also makes new cryptographic constructions possible through the theory of pairings.

In these lectures we will introduce at the cryptographic applications of elliptic curves, and consider some of the opportunities and challenges that they present to cryptographers (and everyday users).

[Recommended articles]

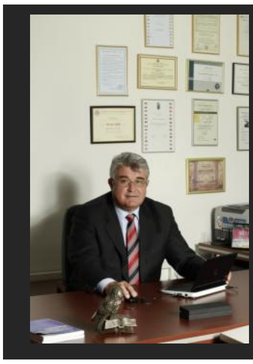
- R. Crandall and C. Pomerance, "Prime Numbers: a Computational Perspective"
- N. P. Smart, "Cryptography, an Introduction". Available free from http://www.cs.bris.ac.uk/~nigel/Crypto_Book/
- F. Blake, G. Seroussi, and N. P. Smart (eds.): "Elliptic Curves in Cryptography"
- S. D. Galbraith, "Mathematics of Public-Key Cryptography"

Assoc. Prof. Dimitar Birov

FMI, Sofia University, Bulgaria (visiting at School of Computer Science, Carnegie Mellon University)
birov@fmi.uni-sofia.bg

"Software Architecture-Based Security"

Dimitar Birov is Associate Professor at the Faculty of Mathematics and Informatics of Sofia University. He has professional experience as research fellow, lecturer, and project manager at Sofia University, University College of Dublin, Ireland, University of Orleans, France, Microsoft Corporation, Redmond, USA, Carnegie Mellon University, and Pittsburgh, USA. He has industrial experience like software developer, software architect, consultant, and CEO. He is patent inventor-Microsoft US Patent. His primary research interests are in software engineering and software architecture, programming languages and knowledge management.



Prof. Veselin Tzelkov

Commission for Personal Data Protection,
University for Library Studies and Information Technologies, Bulgaria
vtselkov@cpdp.bg

"Models for Cryptographic Keys Distribution"
"Formal Model of Multilayer Cryptographic System"

Veselin Tsenov Tselkov was born in 1955 in the town of Vratsa.

He has graduated from the Faculty of Mathematics and Mechanics at St. Kliment Ohridski Sofia University, department - Mathematical Logic.

He has defended a doctorate entitled Management of Information in Computer Networks. Senior Research Associate II rank in Informatics (Information Security). In November 2008 he has defended a dissertation for the science rank "doctor of technical sciences". In August 2010 he was awarded the academic title "professor".

He has specialized in George Marshal European Centre for Security Studies and Communication and Information Technologies (Cisco Academy) at Technical University, Bucharest, Romania.

Veselin Tselkov is a lecturer in Information Security at St. Kliment Ohridski Sofia University, New Bulgarian University and Specialized Higher School of Library Science and Information Technologies. He is a director of studies of undergraduate and post-graduate students in the field of information security. He is the head and a certified instructor of the regional Cisco Academy at G. S. Rakovski Military Academy.

Veselin Tselkov is a colonel retired of the Bulgarian Army. He worked as a research associate in the field of protection of information at Military Research Institute of the Army General Staff and a senior research associate- II rank at the Institute of Perspective Studies for the Defense, G. S. Rakovski Military Academy.

From 2002 to 2007 Veselin Tselkov was a member of the State Commission on Information Security. He participated in Bulgarian and international working parties information security issues. He was a national representative in a number of forums and working parties of NATO and the EU in the field of protection of information. He is a member of the Atlantic Club.

On 19.12.2007 he was elected a member of the Commission for Personal Data Protection.

Veselin Tselkov is fluent in English and Russian.

Prof. Veselin Tzelkov (cont.)

Models for Cryptographic Keys Distribution

There are three sections:

- Introduction to cryptographic keys management;
- Models for keys distribution by levels and groups;
- Models for keys distribution by time.

Introduction to cryptographic keys management

The main topics are: Security Services; Classes of Cryptographic Algorithms; Key Types and Other Information; Other Cryptographic or Related Information; Key States and Key Management Phases.

Models for keys distribution by groups and levels

The models realized the main principles: “Need to know” and “Sensitive labels (level of security)”

Models for keys distribution by time

Here are given three models for cryptographic keys distribution - statical, dynamical and hybrid.

The models, the methods and the modus operandi are being explained. In every model are given user's possibilities, primitives and E-net model of functioning (The model's places and transitions are defined in the sense of generalized places and generalized transitions).

Formal Model of Multilayer CryptographicSystem

This paper presents a model of multilayer cryptography system for data protection in Distribution Information Systems. The architecture, functional features and components of the system are explained. The solutions for files, e-mail and web protection are presented.

Assoc. Prof. Krassimir Manev

Sofia University "St Kliment Ohridski", Bulgaria
manev@fmi.uni-sofia.bg

"Hardness of algorithmic tasks – a fundamental for cryptography"

Krassimir Manev graduated from the National Mathematical Secondary School at 1969. Then he obtained M.Sc. in Computer Science, 1974, and Ph.D., 1988, from Sofia University (Ph.D. thesis "Computer Aided Combinatorial Research"). From 1976 to 1991 he is a Research Fellow in the Institute of Mathematics and Informatics of the Bulgarian Academy of Sciences. Since 1991 he is Assoc. Professor in Faculty of Mathematics and Computer Science of Sofia University, teaching Discrete mathematics and Algorithms. He was also guest professor in New Bulgarian University, University of Veliko Tarnovo, American University in Bulgaria and Free University of Varna. Author of more than 50 scientific publications, 1 textbook for universities and 11 textbooks for secondary schools.

Kr. Manev is a member of the editorial boards of the journals "Serdica Journal of Computing", "Olympiads in Informatics" and "Informatics in Education". From 1981 to 2008 he was a member and from 1998 to 2001 – a leader of the National commission for Olympiads in Informatics. From 2001 to 2003 and from 2006 till now he is a member of the International Committee of International Olympiad in Informatics.

Essence of the cryptography is the existence of a set C of algorithmically computable functions such that for each *f* inC there is a ***quick*** algorithm calculating *f* (*encryption*), but there is no such algorithm for calculating f^{-1} (*decryption*) or at least no such algorithm that is able to calculate quickly f^{-1} without knowledge of some additional information for encryption algorithm (*key*).
Everybody has an intuitive understanding of notions *quick* and *slow* algorithm. But for the purposes of research and development of algorithms with the required quality, a formal theory is necessary. Our 4 lectures course is a brief introduction in the Theory of (time) complexity of algorithms and algorithmic tasks.

The content of the lectures will be:

Lecture 1: Formal models of the notions *task* and *algorithm; time complexity* of an algorithm – in the *worst* and in the *average case*; examples.

Exercise 1: Practical estimation of the time complexity of algorithms.

Lecture 2: Time complexity of a task; polynomial reduction of a task; classes P and NP; is P = NP ?; NP-completeness; existence of NP-c tasks; algorithmic approaches to hard algorithmic tasks; approximations.

Exercise 2: Examples of algorithmic tasks used in the cryptography, estimation of the complexity of encryption and decryption algorithms; discussions.

Malika Izabachene

ENS Cachan
malika.izabachene@lsv.ens-cachan.fr

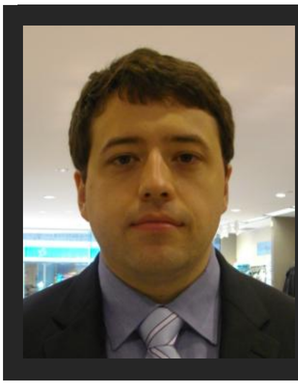
“Cryptography basics (introduction)”

Malika Izabachene is a post-doc at Ecole Normale Supérieure de Cachan.

She studied Computer Science and Mathematics at University Paris 7 and made her master thesis in Cryptography under the supervision of David Pointcheval and Michel Abdalla at Ecole Normale Supérieure de Paris.

She made her Phd under the supervision of David Pointcheval in Anonymity and Privacy. Her research interests lie in models, design and proof study of anonymous protocols.

In this talk, I will review some basic concepts of modern Cryptography. I will give security definition for basic cryptography primitives. I will discuss some issues for computational security in public key schemes and give some examples. I will finally bring some ideas on: browse confirm save as homomorphic encryption scheme constructions.



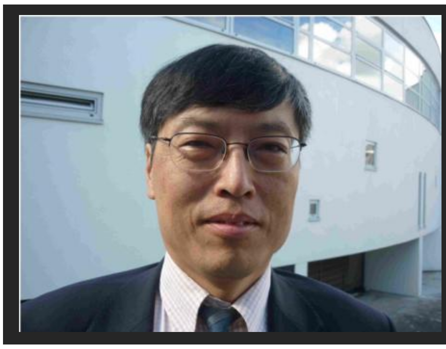
Gabriel Gauthier-Shalom

University of Waterloo
gabriel.gauthier@gmail.com

“Pairing Based Cryptography”

I am currently a PhD candidate in the Department of Combinatorics and optimization at the University of Waterloo, under the supervision of Professor David Jao. I am expecting to complete my degree in 2014 in the area of pairing-based cryptography. I did my Bachelor’s degree in Mathematics and Statistics at McGill University (2007), where I also completed my Master’s degree (2010) in number theory under the supervision of Professor Henri Darmon.

In this talk, we give an overview of Cryptographic Pairings and their applications, with emphasis on algorithms, implementation and optimization. We will present examples of cryptographic systems which have only been possible since the introduction of cryptographic pairings, such as identity-based encryption schemes. We will also present details of various recent algorithmic optimizations which have greatly improved computation times for pairings.



Antonio Kung

Trialog, France
antonio.kung@trialog.com

"Impact of Privacy-by-design on ICT"

Antonio Kung has 30-year experience in embedded systems. He was initially involved in the development of real-time kernels, before co-founding Trialog with Raffi Aslanian, where he now serves as CTO.

He heads the company product development (kernels, protocols, engineering tools) as well as research projects on embedded systems, engineering, networking and security.

Antonio is involved in R&D related to security and data protection in Intelligent Transport Systems in Europe (e.g. GST, SeVeCom, Preciosa, Evita, Oversee, Preserve). He co-chaired the eSecurity working group in the eSafety forum.

Antonio is also involved in security engineering. He coordinates the TERESA project on pattern-based security engineering and is one of the founders of the Security Engineering Forum (SEF).

The objective of the workshop will be to explain the impact of privacy on the design and architecture of ICT systems.

We will start with an analysis of the today state or play, taking examples in intelligent transport systems. Applications such as eCall, Pay-per-use, Road charging will be covered, as well as work carried out in R&D research projects on secure communication (SeVeCom, www.sevecom.org), policy enforcement (Preciosa, www.preciosa-project.org), and secure platforms (oversee, www.oversee-project.com). The various barriers for privacy preserving ICT systems at application level, at design level and at implementation level will be briefly listed.

The principles of privacy-by-design will be explained,

The workshop will then explain the concept of PEARS (Privacy Enhancing Architectures). A number of PEARS patterns will be provided and explained: physical confinement of data, hippocratic data management, isolation layer. The example of the smart meter protection profile will be taken.

Discussions

"Bulgaria in NATO Smart Defense initiative" – Bulgarian Cyber-Defense Cluster
In collaboration with NATO (Nc3A)

"Dangerous Optimizations and the loss of causality" – talk and topic, proposed by Robert Seacord