

Eurocrypt PARIS

IEEE EuroS&P

April 29th - 30th, 2017



Affiliated events
Brochure



IEEE



IEEE
FRANCE SECTION

IEEE  computer society



Summary

----- x

Venue and where to eat ----- 2

Overview of Affiliated Events ----- 7

Abstracts ----- 8

Program for Saturday, April 29th ----- 14

CataCrypt ----- 14

CrossFyre ----- 15

EuroUSEC ----- 15

FOQUS ----- 17

IMPS ----- 17

MTP ----- 18

S4CIP ----- 18

S&B ----- 19

TPT ----- 20

Program for Sunday, April 30th ----- 21

CFRG ----- 21

CrossFyre ----- 21

FewMul ----- 22

FOCUS ----- 22

QsCI ----- 23

SEMS ----- 23



TLS:DIV ----- 24

WCS ----- 25

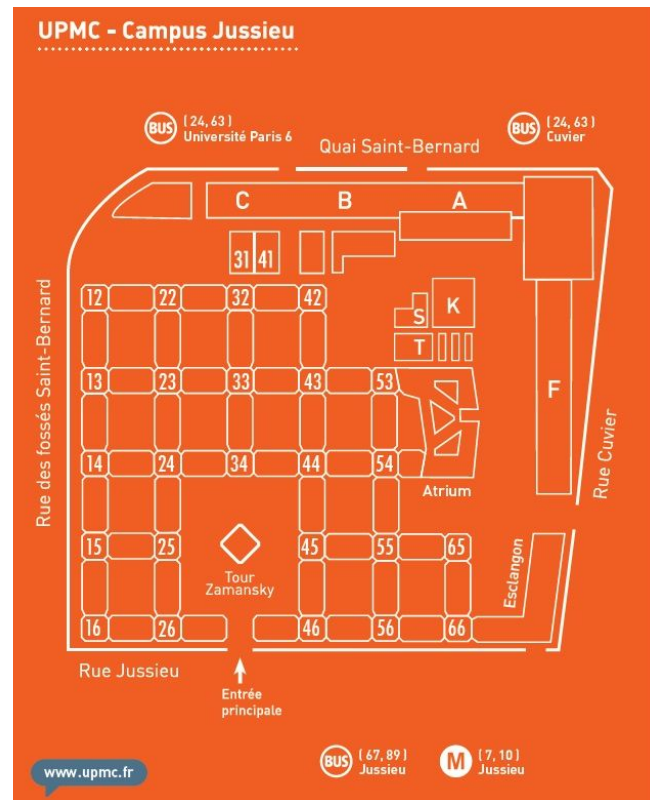
wr0ng ----- 26

Venue and where to eat

Venue:

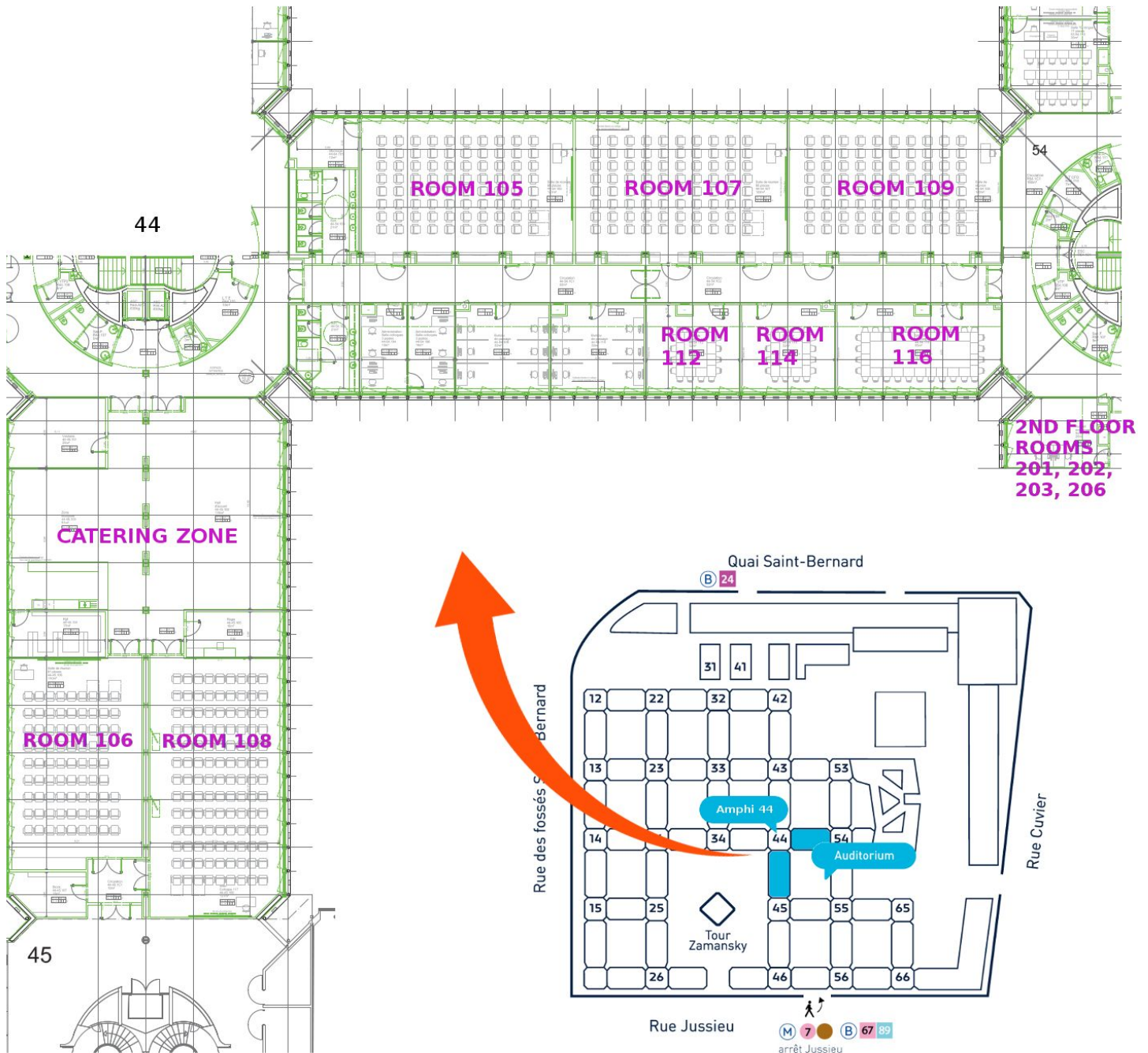
Université Pierre et Marie Curie - - - - - Place Jussieu  

Workshops' rooms - - - - - Corridor 44-54



The Workshops' rooms are on the campus of the University Pierre et Marie Curie. The university is in the Jussieu area in Paris (Jussieu subway stop).

Once at Jussieu you can make your way to Tour 44 or Tour 54 in order to reach Corridor 44-54. The following maps should help you finding your way around.



The affiliated events are hosted in the seminar rooms on the 1st floor between towers 44-45 (room 106, 108, and the catering zone) and 44--54 (rooms 105, 107, 109, and 116), as well as in some of the seminar rooms on the 2nd floor between towers 54--55 (rooms 201, 202, 203, 206). The registration desk for the affiliated events is in the Catering Zone on the 1st floor between towers 44 and 45. Some of these seminar rooms are displayed in the larger diagram above (courtesy of EuroS&P).

Restaurants open on Saturday, April 29th:

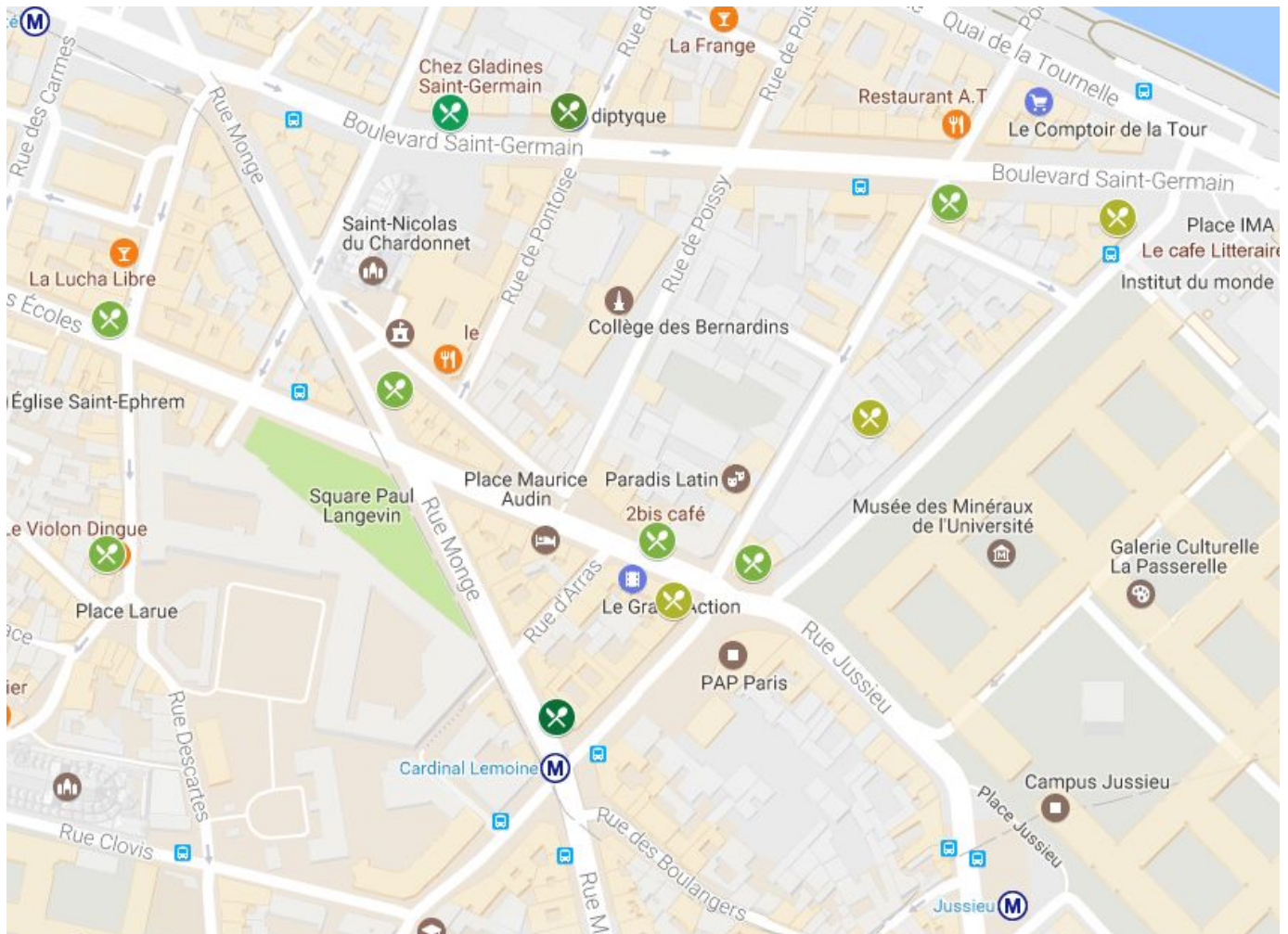
- Cueva del Diablo - - - - - 13 rue Cardinal Lemoine
- Itinéraires - - - - - 15 Rue de Pontoise
- Chez Gladines - - - - - 44 Boulevard Saint-Germain,
- Bar à lodes - - - - - 34 Boulevard Saint-Germain,
- Bocca Rossa - - - - - 8 Rue de Poissy
- Cardinal Saint Germain - - - - - 11 Boulevard Saint-Germain
- Le Nouvel Institut - - - - - 1 Boulevard Saint-Germain,
- L'Authre Bistro - - - - - 22 Rue des Écoles
- Le Restaurant - - - - - -20 Rue Saint-Victor
- Café Saint Victor - - - - - 1 Rue Monge
- Le puits de Légumes - - - - - 18 Rue du Cardinal Lemoine
- L'AOC - - - - - 14 Rue des Fossés Saint-Bernard
- FalaFelo - - - - - 30 Rue des Fossés Saint-Bernard
- Moissonnier - - - - - 28 Rue des Fossés Saint-Bernard
- I Lazzari - - - - - 44 Rue de la Montagne Sainte Geneviève
- Bonvivant - - - - - 7 Rue des Écoles
- Zbis Café - - - - - 2 B Rue des Écoles
- Royal Jussieu - - - - - royal jussieu 1 Rue des Écoles
- Le Passage - - - - - 46 Rue des Fossés Saint-Bernard
- Cardinal Sushi - - - - - 55 Rue du Cardinal Lemoine
- La Voix Lactée - - - - - 34 Rue du Cardinal Lemoine
- 58 Quality Street - - - - - 58 Rue de la Montagne Sainte Geneviève
- La Table De Geneviève- - - - - 8 Rue Descartes
- Le Petit Cardinal - - - - - 29 Rue Monge,
- Comptoir Méditerranée - - - - - -42 Rue du Cardinal Lemoine
- Chez Odille - - - - - 42 Rue des Boulangers
- Saigon Panthéon - - - - - 27 Rue Descartes
- Kokoro - - - - - 36 Rue des Boulangers
- Mobster Diner - - - - - 20 Rue des Boulangers
- Mezzo Di Pasta - - - - - 3 Rue des Boulangers
- Terronia - - - - - 11 Rue des Boulangers,

Legend: from forest green to red, average price of a menu

- | | | |
|---|----------------------|--------|
|  | Take Away - - - - - | <10€ |
|  | Restaurant - - - - - | <10€ |
|  | Restaurant - - - - - | 5-15€ |
|  | Restaurant - - - - - | 10-20€ |
|  | Restaurant - - - - - | 20-30€ |
|  | Restaurant - - - - - | 30-40€ |
|  | Restaurant - - - - - | 40-50€ |
|  | Restaurant - - - - - | >50€ |

Restaurants open on Sunday, April 30th:

- Chez Gladines - - - - - 44 boulevard Saint-Germain
- Le nouvel Institut - - - - - 1 Boulevard Saint-Germain
- Le Cardinal Saint-Germain - - - - - 11 Boulevard Saint-Germain
- Le Passage - - - - - 46 Rue des Fossés Saint-Bernard
- Royal-Jussieu - - - - - 1 Rue des Écoles
- Zbis café - - - - - 2 B Rue des Écoles
- Café Saint-Victor - - - - - 11 Rue Monge
- L'Authre Bistro - - - - - 22 Rue des Écoles
- I LAZZARI - - - - - 44 Rue de la Montagne Sainte Geneviève



Overview of Affiliated Events

Saturday, April 29th (8:00-18:00):

cataCrypt Catastrophic events related to Cryptography Room 206	FOQUS Frontiers Of Quantum Safe Cryptography Room 106	MTP Models and Tools for Security Analysis and Proofs Room 109
S&B Security on Blockchains Room 105	TPT Tamarin-Prover Tutorial Room 203	CrossFyre Cryptography for Female Young Researchers Room 201
EuroUSEC European Workshop on Usable Security Room 107	IMPS Innovations in Mobile Privacy and Security Room 202	S4CIP Safety & Security aSSurance for Critical Infrastructures Protection Room 116

Sunday, April 30th (8:00-18:00):

CFRG Crypto Forum Research Group Room 203	FewMul Fewer Multiplications in Cryptography Room 116	FOQUS Frontiers Of Quantum Safe Cryptography Room 106
QsCI Quantum-safe Crypto for Industry (RISQ) Room 106	SEMS Security for Embedded and Mobile Systems Room 109	TLS:DIV TLS 1.3: Design, Implementation, Verification Room 107
WCS 2nd workshop on Communication Security Room 202	wrOng Random Number Generation Done Right Room 105	CrossFyre Cryptography for Female Young Researchers Room 201

Abstracts

CataCrypt — catastrophic events related to Cryptography and possible solutions

Many cryptographic protocols are only based on the security of one cryptographic algorithm (e.g. RSA) and we don't know the exact RSA security. What if somebody finds a clever and fast factoring algorithm? Well, it is indeed a hypothesis but we know several instances of possible progress. A new fast algorithm is a possible catastrophe if not handled properly. And there are other problems with hash functions, elliptic curves, also. Think also about the Heartbleed bug (April 2014): the discovery was very late and we were close to a catastrophic situation. This workshop deals with these possible problems and their solutions.

CFRG — Crypto Forum Research Group

The Crypto Forum Research Group (CFRG) is a general forum for discussing and reviewing uses of cryptographic mechanisms, both for network security in general and for the IETF in particular. It serves as a bridge between theory and practice, bringing new cryptographic techniques to the Internet community and promoting an understanding of the use and applicability of these mechanisms via Informational RFCs (in the tradition of, e.g., RFC 1321 (MD5) and RFC 2104 (HMAC)). Our goal is to provide a forum for discussing and analyzing general cryptographic aspects of security protocols, and to offer guidance on the use of emerging mechanisms and new uses of existing mechanisms. IETF working groups developing protocols that include cryptographic elements are welcome to bring questions concerning the protocols to the CFRG for advice.

CrossFyre — Cryptography, Robustness, and Provably Secure Schemes for Female Young Researchers

The CrossFyre Workshop aims to bring female researchers in the field of Cryptography and Information Security together to promote their research topics and careers as women in Computer Science and Engineering. We hope to encourage a tighter cooperation across women, and to motivate joint papers. In this spirit, you are kindly invited to attend and give a short presentation of your research topic to your fellow participants.

EuroUSEC — European Workshop on Usable

The European Workshop on Usable Security (EuroUSEC) is the European sister of the established USEC workshop, and thus as a premier forum for research in the area of human factors in security and privacy. The European Workshop on Usable Security solicits previously unpublished work offering novel research contributions in any aspect of human factors in security and privacy for end-users and IT professional such as software developers and administrators of IT systems. The aim of this workshop is to bring together an interdisciplinary group of researchers and practitioners in human computer interaction, security and privacy as well as researchers and practitioners from other domains such as psychology, social science and economics.

FewMul — Fewer Multiplications in Cryptography

Cryptographic primitives realized with few multiplications can significantly improve (or even enable!) applications in areas as diverse as homomorphic encryption, side-channel attack countermeasures, secure multiparty computation, or zero-knowledge proofs. This one-time workshop aims to provide an overview of results, applications and current research in this area. This covers theory, design and analysis, as well as implementations. Major goals are to bring together researchers from the unusual set of relevant disciplines within cryptography/security and outside (e.g. circuit complexity), and to identify open problems and more applications. This is a one-day event consisting of invited talks only.

FOQUS — Frontiers Of Quantum Safe Cryptography

The objective of the workshop is to promote research at the frontiers of Quantum-safe cryptography, i.e. to design and analyze cryptographic tasks secure against quantum-capable adversaries, using concepts and techniques from modern cryptography and/or quantum information. The program will be composed of invited talks. Target audience is composed of modern cryptographers interested in the implications of quantum information to cryptography as well as quantum information researchers interested in cryptography. The goal of the workshop will be to strengthen the collaboration between the two communities on some important topics in quantum-safe cryptography and to identify new ones.

Frontier research topics in Quantum-Safe Cryptography are:

- Security models for quantum-safe cryptography and their relation to "classical" models
- Power of quantum adversaries for lattice and code-based cryptography
- Design of quantum-safe cryptographic primitives
- Hardware security, attacks and implementation security certification
- Practical applications and deployment of quantum-safe cryptographic systems

IMPS — Innovations in Mobile Privacy and Security

IMPS aims to bring together researchers working on challenges in security and privacy for mobile platforms, broadly considered. We are interested in investigations into existing security platforms, their users, applications and app store ecosystems, and research into novel security or privacy mechanisms, tools and analysis techniques. Besides established mobile platforms such as iOS and Android, the workshop will consider new and emerging platforms including those for small and embedded devices for example, in the Internet-of-Things setting.

MTP — Models and Tools for Security Analysis and Proofs

It has become clear that computer aided tools and their associated abstract models are indispensable to scalable and rigorous analysis of cryptographic systems. The aim of the workshop is two-fold: to survey the state of the art in the area and to chart future research directions. The workshop is addressed to both researchers in the area of formal models and tools but also to cryptographers interested in the limits and support provided by existing tools. There will be plenty of scope for discussion.

QsCI — Quantum-safe Crypto for Industry (RISQ)

Quantum-Safe Safe cryptography aims at constructing systems that are secure against quantum and conventional computers. The status of quantum-safe cryptography is currently completely changing. It is quickly moving from a purely academic theme to a topic of major industrial interest, driven by the fact that quantum-safe cryptography has recently received much attention from the standardization and policy spectra such as NIST, ETSI, and CSA. The goal of the QsCI workshop is to regroup speakers from the industry and the academia to discuss of the construction and development of quantum-safe systems. The event will include a selection of speakers in the area of quantum-safe cryptography, standardization and industrial challenges for quantum-safe cryptography.

S4CIP — 2nd Workshop on Safety & Security aSSurance for Critical Infrastructures Protection

Modern society heavily relies on large, heterogeneous and complex software-intensive systems to support all kinds of daily activities. Services such as urban transportation, logistics, health-care, data communication, railway, aerospace, and power distribution, to name a few, are becoming more and more dependent on the availability of such infrastructures. Any discontinuity of service may lead to serious problems, from severe financial losses to fatalities or injuries; the causes have different natures, either human errors, unexpected acts of nature, or intentional attacks like sabotage. Safety and security (S&S) assessments in critical infrastructures measure how these disruptions are handled and what is the impact suffered by the critical infrastructure under stress. These assessments are normally performed using analytical or simulation-based techniques often addressing one single specific aspect at a time rather than studying these infrastructures in a holistic manner. This workshop aims at providing a forum for people from academia and industry to communicate their latest results on theoretical advances, industrial case studies, practical scenarios, and lessons learned in the assurance of S&S for critical infrastructures. Since the special interest on S&S assurance, a special focus will be put on model-based approaches; to the joint modelling and analysis of both cyber and physical aspects of critical infrastructures; and to the definition of unifying modelling and analysis methodologies. Research papers focused on safety or security assurance only are also welcome.

S&B — Security on Blockchains

Today, the security and privacy properties of blockchain technologies are still an emerging field that is need of further research. The Bitcoin electronic cash system introduced the new field of blockchain technology as a practical mechanism for a permissionless and censorship-resistant e-cash over the Internet. However, the decentralized network and public verifiability of Bitcoin often do not provide the security and privacy properties assumed by its users. For example, despite a common assumption that Bitcoin is anonymous, transactions can be de-anonymized, limiting the commercial utility of the network and also harms individual privacy. Generalizations of Bitcoin's underlying blockchain technology as a platform for smart contracts by Ethereum are still immature. For example, security issues in the underlying programming language for smart contracts in Ethereum led to the massive DAO hack. More than ever, proper security and privacy properties need to be designed into the underlying framework for blockchain technologies.

SEMS — Security for Embedded and Mobile Systems

Embedded and mobile devices that provide security and crypto functionalities and manage private and confidential data are omnipresent in our daily lives. Examples of such devices range from smart cards and RFID tags, to mobile phones, tablets, and IoT devices. Ensuring the security and privacy of these devices is a challenging problem, as witnessed by recent breaking of crypto and security systems used in mobile phones, car keys, and RFID-enabled cards. Typical threats to extract the keys include side-channel and fault analysis. Additionally, the vulnerabilities of the devices also imply privacy concerns. The operating systems supporting some of those devices, particularly mobile phones and tablets, but also IoT ones, have become very complex. Various sorts of malware present a constant threat for users. Although measures like application sandboxing take place, they also open the court for new attacks by constantly collecting and organizing sensitive information about the user.

TLS:DIV — TLS 1.3: Design, Implementation, Verification

The goals of the TLS:DIV workshop are threefold: first, to explain and justify the latest changes to the TLS 1.3 design (from draft 13 to draft 19); second, to give an overview of some ongoing efforts to prove the cryptographic security of the TLS 1.3 protocol, and third, to showcase recent tools and methods to evaluate and improve the safety and security of TLS implementations, up to the level of cryptographic primitives.

Workshop topics:

- Evolution of the TLS 1.3 specification
- Cryptographic security proofs of the TLS 1.3 handshake and record
- Safe and secure implementations of cryptographic primitives
- Security evaluation of TLS implementations and deployment
- Applications built on top of new TLS 1.3 features (e.g. 0-RTT, late authentication)

TPT — Tamarin-Prover Tutorial

Tamarin is an automated verification tool that has been used to analyze group key protocols, public-key infrastructure proposals, and proposed standards, such as TLS. Using Tamarin, recently attacks were found in TLS 1.3. Tamarin works in the symbolic model of cryptographic protocols, and enables automatic analysis as well as a powerful interactive mode. It supports both falsification and unbounded verification of security protocols specified as multiset rewriting systems with respect to (temporal) first-order properties and a message theory that models Diffie-Hellman exponentiation combined with a user-defined subterm-convergent rewriting theory. In this tutorial, presentation and hands-on exercises will be combined to show attendees the basics of security protocol modeling with multiset rewriting, property specification, and analysis. Participants will model classic protocols, find attacks and perform verification, and leave with an understanding how to start modeling their own protocols of interest.

WCS — 2nd workshop on Communication Security

The workshop aims to provide a forum to discuss cutting-edge cross-disciplinary security research and to share visions for future joint advances in the fields of physical-layer security and cryptography. The one-day event will include the presentation of peer-reviewed papers and two prominent keynote talks by Jean-Claude Belfiore (Telecom ParisTech) and Stefano Tessaro (UC Santa Barbara).

wrOng — Random Number Generation Done Right

All cryptographic constructions heavily rely on the availability of random bits, for operations such as key generation, randomization of encryption or signatures and or nonces in protocols. Unfortunately, multiple incidents have demonstrated that the quality of the (pseudo-)random number generators leaves much to be desired. Even worse, in September 2013 it was revealed that the US government agency has deliberately undermined the security of cryptographic solutions by inserting a backdoor in the Dual EC random number generator included in ANSI, NIST and ISO standards. This highlights that a secure system can be fatally weakened by the insertion of just one flawed component; if the NSA can predict all randomness used by a system, it knows all secrets used during that time period and might even be able to recover long-term keys. In spite of their crucial importance, there are very few research papers on the topic and most industrial designs are proprietary. Moreover, existing designs and instances are notoriously difficult to evaluate. The goal of this workshop is to review new models, constructions, implementations, and evaluation methodologies. It will also be explored whether the area is mature enough to identify requirements and plan an open competition. The workshop will cover both truly random number generators and pseudo-random number generators.

Program for Saturday, April 29th

CataCrypt — catastrophic events related to Cryptography and possible solutions

Program (Saturday, 29th, room 206)

8:30-9:00	<i>Registration</i>
9:00-10:30	Session 1
	Introduction to cataCRYPT (opening remarks) Jean-Jacques Quisquater
	Blueprints for a real quantum computer Jean-Jacques Quisquater
	Quantum cryptanalysis — the catastrophe we know and don't know Tanja Lange
10:30-11:00	<i>Coffee break</i>
11:00-12:00	Session 2
	Are quantum computers more powerful than traditional ones? Jean-François Geneste
	Smart cards against cataCRYPT Louis Guillou
12:00-14:00	<i>Lunch</i>
14:00-15:30	Panel
	How to Promote Funding for Cryptanalysis? Yvo Desmedt, Nicolas Courtois, TBA, ...
15:30-16:00	<i>Coffee break</i>
16:00-17:30	Session 3
	A first catagorithm Jean-François Geneste
	Short talk Louis Guillou
	Open slots for short talks, announcements, and brain-storming.

CrossFyre — Cryptography, Robustness, and Provably Secure Schemes for Female Young Researchers

Program (Saturday, 29th, room 201)

9:00-10:30	Applications
	Reliability and topology-failure detection Ammara Gul
	Regulations for medical devices Romina Muka
10:30-11:00	<i>Coffee break</i>
11:00-12:00	Keynote 1: topic TBA Ioana Boureanu
12:00-13:30	<i>Lunch</i>
13:30-14:30	Keynote 2: topic TBA Nadia Heninger
14:30-15:30	Privacy
	Distributed storage and cloud computing with rational providers Giulia Traverso
	Towards blockchain transaction privacy Rebekah Mercer
15:30-16:00	<i>Coffee break</i>
16:00-	Panel Discussion
19:00-	<i>Dinner</i>

EuroUSEC — European Workshop on Usable Security

Program (Saturday, 29th, room 107)

8:00-9:00	<i>Break, Registration, Coffee & Refreshments</i>
9:00-9:10	Opening Remarks
9:10-10:30	Session 1: IT professionals
	I'd Like to Have an Argument, Please: Using Dialectic for Effective App Security, C. Weir, A. Rashid
	Finding Security Champions in Blends of Security Culture I. Becker, S. Parkin, M. Sasse
	I Do and I Understand. Not Yet True for Security APIs. So Sad Luigi Lo Iacono, Peter Leo Gorski
	Can Johnny build a protocol? Co-ordinating developer and user intentions for privacy-enhanced secure messaging protocols, Ksenia Ermoshina
10:30-11:00	<i>Coffee break + refreshments</i>

11:00-12:00	Session 2: Work in Progress
	Security Narrative: Can Insecurities be Beneficial for Security Departments? Karoline Busse
	An Inquiry into Perception and Usage of Smartphone Permissions Models Sophie Russ, Lena Reinfelder
	Riddle me this! Context Sensitive CAPTCHAs Tobias Urban, René Riedel, Norbert Pohlmann
	Providing smartphone data visualizations to support Privacy Literacy Timo Jakobi
	Discussion
12:00-14:00	<i>Lunch break</i>
14:00-14:50	Keynote
	Would you like some Anti-Virus Protection with that? Adventures in Point-of-Sale Security, Angela Sasse
14:50-15:30	Session 3: What is secure?
	What is a Secure Email? Joscha Lausch, Oliver Wiese, Volker Roth
	Effects of information security risk visualization on managerial decision making, Esra Yildiz
15:30-16:00	<i>Break</i>
16:00-17:00	Session 4a: Protecting end users
	The Security Blanket of the Chat World: An Analytic Evaluation and a User Study of Telegram, Ruba Abu-Salma
	Personalized Security Messaging: Nudges for Compliance with Browser Warnings, Nathan Malkin
	Information Leakage through Mobile Motion Sensors: User Awareness and Concerns, Kirsten Crager, Anindya Maiti, Murtuza Jadliwala, Jibo He
17:00-18:00	Session 4b: People and Passwords
	Pass-Roll and Pass-Scroll : New Graphical User Interfaces for Improving Text Passwords Harshal Tupsamudre
	Pico in the Wild: Replacing Passwords, One Site at a Time Seb Aebischer, Claudio Dettoni Jr., Graeme Jenkinson, Kat Krol, David Llewellyn-Jones
	Password Logbooks and What Their Amazon Reviews Reveal About Their Users' Motivations, Beliefs, and Behaviors Ross Koppel

FOQUS — Frontiers Of Quantum Safe Cryptography

Program (Saturday, 29th, room 106)

8:30-9:30	<i>Registration and Welcome Coffee</i>
9:30-11:45	Session 1
	The urgency of quantum-safe cryptography, Michele Mosca
	Standardizing Lattice Cryptography, Vadim Lyubashevsky
	Short Stickelberger Class Relations and application to Ideal-SVP, Léo Ducas
11:45-14:00	<i>Lunch</i>
14:00-15:30	Session 2
	Quantum Cryptography Beyond Quantum Key Distribution, Christian Schaffner
	Breaking Symmetric Cryptosystems Using Quantum Algorithms, Gaëtan Leurent
15:30-16:00	<i>Coffee break</i>
16:00-17:30	Session 3
	Post-quantum security of hash functions, Dominique Unruh
	Quantum algorithms for the subset-sum problem, Stacey Jeffery

IMPS — Innovations in Mobile Privacy and Security

Program (Saturday, 29th, room 202)

8:00-9:00	<i>Registration & Breakfast</i>
9:00-9:15	Welcome to IMPS
9:15-10:30	Invited Talk 1: Industry Security Research: An Insider's View from an ex-Academic. Federico Maggi, Trend Micro
10:30-11:00	<i>Coffee break</i>
11:00-12:00	Session 1
	RandomPad: Usability of Randomized Mobile Keypads for Defeating Inference Attacks, Anindya Maiti, Kirsten Crager, Murtuza Jadliwala, Jibo He, Kevin Kwiat, and Charles Kamhoua
	Common Concerns in BYOD Policies, Joseph Hallett and David Aspinall
12:00-14:00	<i>Lunch break</i>
14:00-15:30	Panel: Research Challenges in Mobile Privacy and Security
15:30-16:00	<i>Coffee break</i>
16:00-17:00	Invited Talk 2: Challenges on Developing Secure Mobile Applications. Sascha Fahl, CISPA, Saarland University
17:00-18:00	Session 2
	The cost of push notifications for smartphones using Tor hidden services, Stephan A. Kollmann, and Alastair R. Beresford
	The Privacy API: Facilitating insights in how one's own user data is shared, Bram Bonné, Peter Quax, and Wim Lamotte

MTP — Models and Tools for Security Analysis and Proofs

Program (Saturday, 29th, room 109)

8:00-9:00	<i>Registration & Breakfast</i>
9:00-10:30	Session 1
	Programming language methods for cryptography, Gilles Barthe
	Models and Tools for Electronic Voting protocols, Veronique Cortier
10:30-11:00	<i>Coffee break</i>
11:00-12:00	Session 2
	Two approaches to verifying high-speed ECC software, Peter Schwabe
12:00-14:00	<i>Lunch</i>
14:00-15:30	Session 3
	HACL*: Writing and verifying a cryptographic library in F*, Karthik Barghavan
	Type-based cryptographic verification in F*, Cedric Fournet
15:30-16:00	<i>Coffee break</i>
16:00-17:30	Session 4
	CryptoVerif: state of the art, perspectives, and relations to other tools Bruno Blanchet
	Measuring protocol strength with security goals, Joshua Guttman

S4CIP — 2nd Workshop on Safety & Security aSSurance for Critical Infrastructures Protection

Program (Saturday, 29th, room 116)

8:00-9:00	<i>Coffee break</i>
9:00-10:30	Session 1 (Chair: Simona Bernardi)
	Towards a Unified Definition of Cyber and Physical Vulnerability in Critical Infrastructures, S. Marrone
	A Proof-theoretic Trust and Reputation Model for VANET Giuseppe Primiero, Franco Raimondi, Taolue Chen and Rajagopal Nagarajan
	Cyber-Attack Detection for Industrial Control System Monitoring with Support Vector Machine based on Communication Profile , Asuka Terai
10:30-11:00	<i>Coffee break</i>
11:00-13:00	Session 2 (Chair: Stefano Marrone)
	Formal analysis of safety and security requirements of critical systems supported by an extended STPA methodology Giles Howard, Michael Butler, John Colley and Vladimiro Sassone
	Process Mining to enhance security of Web information systems, S. Bernardi
	Security Viewpoint in a Reference Architecture Model for Cyber-Physical Production Systems Zhendong Ma, Aleksandar Hudic, Abdelkader Shaaban and Sandor Plosz
	Challenges and Approaches in Securing Safety-Relevant Railway Signalling Christian Schlehuber

S&B — Security on Blockchains

Program (Saturday, 29th, room 105)

8:00-9:00	<i>Registration</i>
9:00-10:30	Introductory Remarks and Keynote
	Overview of Security and Privacy on Blockchain Workshop Harry Halpin and Marta Piekarska
	Research Challenges and Directions of Development for Future Bitcoin Solutions, Adam Back
10:30-11:00	<i>Coffee break</i>
11:00-12:30	Research Papers
	BIP32-Ed25519: Hierarchical Deterministic Keys over a Non-linear Keyspace Dmitry Khovratovich, Jason Law
	Proof-of-Personhood: Redemocratizing Permissionless Cryptocurrencies Maria Borge, Eleftherios Kokoris-Kogias, Philipp Jovanovic, Linus Gasser, Nicolas Gailly, Bryan Ford
	Proofs-of-delay and randomness beacons in Ethereum Benedikt Bunz, Steven Goldfeder and Joseph Bonneau
12:30-14:00	<i>Lunch</i>
14:00-15:30	Research Papers
	Zero-Collateral Lotteries in Bitcoin and Ethereum Andrew Miller and Iddo Bentov
	Design of a Privacy-Preserving Decentralized File Storage with Financial Incentives, Henning Kopp, David Mödinger, Franz Hauck, Frank Kargl and Christoph Bösch
	Anonymous Alone? Measuring Bitcoin's Second-Generation Anonymization Techniques, Malte Möser and Rainer Boehme
15:30-16:00	<i>Coffee Break</i>
16:00-18:00	Short Research Papers
	Long-term public blockchain: Resilience against Compromise of Underlying Cryptography, Masashi Sato and Shin'ichiro Matsuo
	Auditable Zerocoin Ken Naganuma, Masayuki Yoshino, Hisayoshi Sato and Takayuki Suzuki
	Conditions of Full Disclosure: The Blockchain Remuneration Model S. Matthew English and Ehsan Nezhadian
	Towards Better Availability and Accountability for IoT Updates by means of a Blockchain, Aymen Boudguiga, Nabil Bouzerna, Louis Granboulan, Alexis Olivereau, Flavien Quesnel, Anthony Roger and Renaud Sirdey
	Oligarchic Control of Business-To-Business Blockchains Leif-Nissen Lundbaek and Michael Huth
18:00-	Open Space for "rump" talks, announcements, and brain-storming

TPT — Tamarin-Prover Tutorial

Program (Saturday, 29th, room 203)

9:00-10:30	Initial lecture
	Security protocol analysis using the Tamarin-Prover
10:30-11:00	<i>Break</i>
11:00-12:00	Hands-on session using Tamarin
12:00-14:00	<i>Lunch break</i>
14:00-15:30	Advanced lecture
	Advanced modeling, properties, and state space reduction
15:30-16:00	<i>Break</i>
16:00-18:00	Hands-on session using Tamarin

Program for Sunday, April 30th

CFRG — Crypto Forum Research Group

Program (Sunday, 30th, room 203)

16:00-16:10	CFRG status update from CFRG chairs Kenny Paterson
16:10-16:35	Argon 2 update Dmitry Khovratovich
16:35-16:50	PKEX: A Password-Authenticated Public Key Exchange Dan Harkins
16:50-17:15	Caesar's Role in the Fall of AE Security Pooya Farshim
17:15-17:40	BIP32-Ed25519 Dmitry Khovratovich
17:40-18:00	Open discussion

CrossFyre — Cryptography, Robustness, and Provably Secure Schemes for Female Young Researchers

Program (Sunday, 30th, room 201)

8:00-9:00	<i>Registration</i>
9:00-10:30	Implementations
	Obstacles to the Adoption of Secure Communication Tools, Ruba Abu-Salma
	DES S-boxes, Lauren de Meyer
	The Mifare Plus distance-bounding implementation, Rokia Lamrani Alaoui
10:30-11:00	<i>Coffee break</i>
11:00-12:00	Keynote 3: topic TBA Catuscia Palamidessi
12:00-14:00	<i>Lunch</i>

FewMul — Fewer Multiplications in Cryptography

Program (Sunday, 30th, room 116)

8:00-9:00	<i>Breakfast</i>
9:00-10:30	Session on Side-Channel Topics
	TBA, FX Standaert
	Threshold implementations against side-channel attacks, and multiplications Begul Bilgin
10:30-11:00	<i>Break</i>
11:00-12:00	Session on Foundations
	Functions with known multiplicative complexity, Rene Peralta
12:00-14:00	<i>Lunch</i>
14:00-15:30	Session on Applications
	Evaluating suitable cryptographic primitives within MPC engine Emmanuela Orsini
	Homomorphic Encryption, TBA
15:30-16:00	<i>Break</i>
16:00-17:30	Session on Theory and Concrete Constructions
	Theory, TBA
	Multiplicative complexity in block cipher design and analysis Pavol Zajac

FOQUS — Frontiers Of Quantum Safe Cryptography

Program (Sunday, 30th, room 106)

8:30-9:15	<i>Coffee break</i>
9:15-10:45	Session 4
	How secure are Quantum Key Distribution protocols and their implementations? Norbert Lütkenhaus
	Physical attacks against lattice-based schemes, Mehdi Tibouchi
10:45-11:15	<i>Coffee break</i>
11:15-12:45	Session 5
	Talk title to be announced, Stephanie Wehner
	Finding approximate short vectors in certain ideal lattices with a quantum computer Jean-François Blasse

QsCI — Quantum-safe Crypto for Industry (RISQ)

Program (Sunday, 30th, room 106)

13:30-14:00	RISQ & Quantum-Safe Crypto for Industry, Sylvain Guilley
14:00-15:00	Overview of Quantum-Safe Cryptography, Ludovic Perret, Thomas Prest
15:00-15:30	Real-life deployment of MQ, Jean-Charles Faugère
15:30-16:00	<i>Coffee break</i>
16:00-16:30	Security of Cryptographic Algorithms & Recommendations, Henri Gilbert
16:30-17:00	PQ-Crypto Standardization, Aline Gouget
17:00-18:00	Round-Table: Antoine Casanova, Louis Granboulan, Sylvain Guilley

SEMS — Security for Embedded and Mobile Systems

Program (Sunday, 30th, room 109)

9:00-10:00	Invited talks
	Security and privacy challenges for the IoT, Bart Preneel
10:00-10:30	How to secure Over-The-Air software updates? Marc Witteman
10:30-11:00	<i>Coffee break</i>
11:00-12:00	Session 1: Side Channel Security
	Secure and Efficient RNS software implementation for Elliptic Curve Cryptography, Apostolos P. Fournaris
	Practical Power Analysis on KCipher-2 Software on Low-End Microcontrollers Wataru Kawai
	Use of simulators for side-channel analysis, Nikita Veshchikov
12:00-14:00	<i>Lunch</i>
14:00-15:00	Session 2: Mobile Security & Privacy
	The Curious Case of the Curious Case: Detecting touchscreen events using a smartphone case, Tomer Glick
	Are You Really My Friend? Efficient and Secure Friend-matching in Mobile Social Networks, Mohammad Etemad
	From Smashed Screens to Smashed Stacks: Attacking Mobile Phones using Malicious Aftermarket Parts, Omer Shwartz
15:00-15:30	Permutation-based cryptography for embedded and mobile systems Gilles Van Assche
15:30-16:00	<i>Coffee break</i>
16:00-17:00	Invited talk
	TBA, Srdjan Capkun
17:00-18:00	PANEL: "Security issues for IoT systems including standardization, malware and other attacks", Srdjan Capkun

TLS:DIV — TLS 1.3: Design, Implementation, Verification

Program (Sunday, 30th, room 107)

8:00–8:50	<i>Breakfast</i>
8:50–9:00	Opening remarks
9:00–10:30	Session 1
	Status update on the TLS 1.3 Standard Eric Rescorla
	Implementing and Proving the TLS 1.3 Record Layer Cédric Fournet
	Secure Channels Britta Hale
10:30–11:00	<i>Coffee break</i>
11:00–12:30	Session 2
	Project Wycheproof Thai Duong
	A Cryptographic Analysis of the TLS 1.3 Handshake Felix Günther
	TLS-Attacker: Future directions in testing and fuzzing Juraj Somorovsky
12:30–14:00	<i>Lunch</i>
14:00–15:30	Session 3
	Mechanized Computational Proof of the TLS 1.3 Standard Candidate Bruno Blanchet
	Mitigating cryptographic and application security attacks against TLS1.3 0-RTT data Colm MacCarthaigh
	Verified Assembly Language for Fast Cryptography Chris Hawblitzel
15:30–16:00	<i>Coffee break</i>
16:00–17:30	Session 4
	Tamarin analysis of TLS 1.3: What did we prove? Sam Scott
	Deployment and implementation of TLS 1.3 at Facebook Subodh Iyengar
	Preparing for post-quantum cryptography in TLS Douglas Stebila

WCS — 2nd workshop on Communication Security

Program (Sunday, 30th, room 202)

8:00-9:00	<i>Welcome Coffee</i>
9:00-10:30	Session 1
	A Study of Injection and Jamming Attacks in Wireless Secret Sharing Systems Arsenia Chorti
	Robust Secret Sharing for End-to-End Key Establishment with Physical Layer Keys under Active Attacks Stefan Pfennig, Sabrina Engelmann, Elke Franz and Anne Wolf
	Semantically-Secured Message-Key Trade-off over Wiretap Channels with Random Parameters Alexander Bunin, Ziv Goldfeld, Haim Permuter, Shlomo Shamai, Paul Cuff and Pablo Piantanida
	Hash-then-Encode: A Modular Semantically Secure Wiretap Code Setareh Sharifian, Fuchun Lin and Rei Safavi-Naini
10:30-11:00	<i>Coffee break</i>
11:00-12:00	Invited talk 1
	Finite-Length Lattice Coding for Gaussian Wiretap Channels: A theta series perspective Prof. Jean Claude Belfiore
12:00-14:00	<i>Lunch break</i>
14:00-15:00	Invited talk 2
	A Cryptographic Perspective on Information-theoretic Secrecy Dr. Stefano Tessaro
15:00-15:30	Session 2
	A CCA-Secure Cryptosystem Using Massive MIMO Channels Thomas Dean and Andrea Goldsmith
15:30-16:00	<i>Coffee break</i>
16:00-17:30	Session 3
	You are how you play: authenticating mobile users via game playing Marco Baesso, Pasquale Capuozzo, Mauro Conti, Luciano Gamberini, Merylin Monaro, Giuseppe Sartori and Riccardo Spolao
	Fuzzy Authentication using Rank Distance Alessandro Neri, Joachim Rosenthal and Davide Schipan
	A McEliece-based Key Exchange Protocol for Optical Communication Systems Joo Yeon Cho, Helmut Griesser and Danish Rafique
	An ICN-based Authentication Protocol for a Simplified LTE Architecture Alberto Compagno, Mauro Conti and Muhammad Hassan Khan

wr0ng — Random Number Generation Done Right

Program (Sunday, 30th, room 105)

8:50-9:00	Welcome
9:00-10:30	Session 1: Why Does Strong Randomness Matter?
	Random Number Generator Done Wrong, Nadia Heninger
	Malleability of the Blockchain's Entropy, Cécile Pierrot
10:30-11:00	Coffee break
11:00-12:30	Session 2: Backdoors in Random Number Generation
	Backdoors in PRGs and PRNGs, Kenneth Paterson
	False Backdoors in Historical Symmetric Ciphers, Nicolas Courtois
12:30-14:00	Lunch break
14:00-15:30	Session 3: True Random Number Generation and Entropy Evaluation
	Design of Secure TRNGs for Cryptography - Past, Present, and Future Viktor Fischer
	Evaluating Entropy for True Random Number Generators Maciej Skorski
15:30-16:00	Coffee break
16:00-17:30	Session 4: Constructions for Deterministic and Hybrid Random Number Generation
	Security of Pseudo-Random Number Generators With Input, Damien Vergnaud
	Provably-robust Sponge-based PRNGs, Stefano Tessaro
17:30-18:00	Concluding Discussion, Pascal Paillier

Notes

x - - - - - x

x - - - - - x

- - - - - x

x - - - - - x

- - - - - x

x - - - - - x

- - - - - x

x - - - - - x

- - - - - x

x - - - - - x

- - - - - x

x - - - - - x

- - - - - x

x - - - - - x

- - - - - x

x - - - - - x

- - - - - x

x - - - - - x

- - - - - x

x - - - - - x

- - - - - x

Conference Organizers

- - - - - x

