2016 ASIACRYPT

4-8 December, 2016, Hanoi, Vietnam

22ND ANNUAL INTERNATIONAL CONFERENCE ON THE THEORY AND APPLICATIONS OF CRYPTOLOGY AND INFORMATION SECURITY

HANDBOOK

Organizer

VIASM

Co-organizer

Xlim

Institut de recherche

Sponsors

INTERNATIONAL ASSOCIATION FOR CRYPTOLOGIC RESEARCH

i a c r

Microsoft

VIETTEL

Hãy nói theo cách của bạn

ECPay

HỘI TỤ CỦA SỨC MẠNH

BIDV

NGÂN HÀNG TMCP ĐẦU TƯ VÀ PHÁT TRIỂN VIỆT NAM

CISCO

intel

FPT

Google

EHN

HA NOI ELECTRICAL
EQUIPMENT & TECHNOLOGY JSC

VP9 VIET NAM

HANOI CITY

TIME ZONE: UTC/GMT +7

TELEPHONE COUNTRY CODE: The Vietnam phone code is +84 and the area code for Hanoi is 4.

CLIMATE: The average temperature is between 19 and 24 degrees Celsius (between 66 and 75 degrees Fahrenheit) during the day. Please keep in mind that rain can come suddenly in Hanoi. Be aware that the weather can become very cold during rainy days due to the effect of the monsoon. So, having a thin coat would be useful.

EMERGENCIES: Police: 113

Fire: 114

Ambulance – First Aid: 115

CURRENCY AND BANKING FACILITIES:

Vietnamese currency is Vietnamese Dong (VND). There are nine denominations of bills from VND 1,000 to VND 500,000.

Approximate exchange rate: 1US$»22,500VND and 1EUR»24,300VND. You can sometimes pay by US dollars or Euros in Vietnam (but it is not recommended). The widely accepted credit cards in Vietnam are Visa, MasterCard and American Express.

Foreign currency can be exchanged into VND at the airport or at any bank in the city. However, in general, by our rule, you can hardly exchange from VND back to foreign currency, even at banks. Thus, please only exchange an amount enough for the duration of your stay.

For a small fee obtaining cash by credit or debit cards is very easy from ATM cash machines that can be found at almost each bank office, hotel or on the street. Please be sure to follow the usual safety precautions and plan your withdrawals ahead of time.

ELECTRICITY: The voltage and frequency are 220V, 50Hz. Plug types: A, C, G

CROSSING THE STREETS: Never run, go backward, or make any sudden movement. Walk slowly and stop if you feel unsafe.

TAXIS

Taxi fare ranges from 12,000 to 18,000 VND per km (depending on car quality). Most of taxies are safe. Very rarely, but sometimes you could get a fake taxi or a bad driver who might ask you to overpay. We recommend the following taxi brands:

* Mai Linh Taxi: (84 - 4) 38 616 161 – (84 - 4) 38 333 333

* Taxi Group: (84 - 4) 38 535 353 – (84 - 4) 38 262 626

* Thanh Nga Taxi: (84 - 4) 38 215 215

UBER

Uber is available in Hanoi and most major cities in Vietnam, and is usually cheaper than taxis.

AIRPORT TRANSFER

Noi Bai International Airport in Hanoi is 35 km from the city centre, and the travel time to or from the city centre is approximately 45 minutes (1 hour in peak time). Various transportation services, including public taxis, Uber, minibus and public buses, are available at Hanoi Noi Bai Airport arrivals level.

The best way to go from Noi Bai Airport to hotels in the centre of Hanoi is to take a taxi. Taxi ranks are located immediately outside Noi Bai airport arrival areas of Both T1 (Domestic) and T2 (International) Terminal. Taxi service is provided for all flights of the days, including weekends and holidays. You should choose one of these taxi firms (other taxis could be cheaper and also safe):

* Airport Taxi: (844) 38 866 666

* Noi Bai Airport Taxi: (844) 38 868 888

* Mai Linh Airport Taxi: (84 – 4) 38 222 666

One way taxi fare between Noi Bai airport and the conference venue is approximately US$ 16 – 18 (350,000 - 400,000 VND). Taxi from the city center to the airport costs approximately US$11 – 14 (230,000 - 300,000 VND).

CONFERENCE INFORMATION

CONFERENCE VENUE

The conference will be held at the InterContinental Hanoi Westlake Hotel (address: 5 Từ Hoa, Tây Hồ, Hà Nội).

It is placed over the serene waters of West Lake while only minutes from Hanoi's famous Old Quarter (4 km and less than 5 USD by taxi). The hotel is also approximately 25 km away from Noi Bai International airport.

REGISTRATION DESK OPENING TIME

Sunday 4th December: 18.00 – 20.00

Monday 5th December to Wednesday 7th : 8.00 – 17.00

CONFERENCE OPENING

The opening ceremony starts at 9.00 and the first invited lecture commences at 9.30 on Monday, 5th December at the Grand Ballroom.

FUNCTIONAL ROOMS

Functional rooms Westlake 2 or Westlake 3&4 are located on the Ground Floor (under the Grand Ballrooms). There is a direct video transmission from the conference sessions in the Grand Ballrooms to the functional rooms.

CONFERENCE CLOSING

The technical program of the conference finishes at 12:50 on Thursday 8th December and all the participants are invited for lunch after the last session.

REFRESHMENTS

All catering is served on the Ground Floor. International buffet lunch is served at Café du Lac restaurant.

NAME BADGES

All participants shall receive a name badge, which must be worn at all times within the conference venue.

SATCHELS

All participants shall receive a conference satchel. Your satchel includes the conference handbook, a notebook, a pen and a souvenir from the organizers.

INTERNET ACCESS

Free WiFi is available at the conference venue. The WIFI network does not require any password.

INSTRUCTION FOR PRESENTING AUTHORS

Presentations are generally scheduled for 25 minutes including questions and speaker change-over. If you are giving a presentation, please ensure your lecture slides are uploaded on the computer in the schedule room well in advance of your presentation. You can send your slides by email to the session chairs and the general chair.

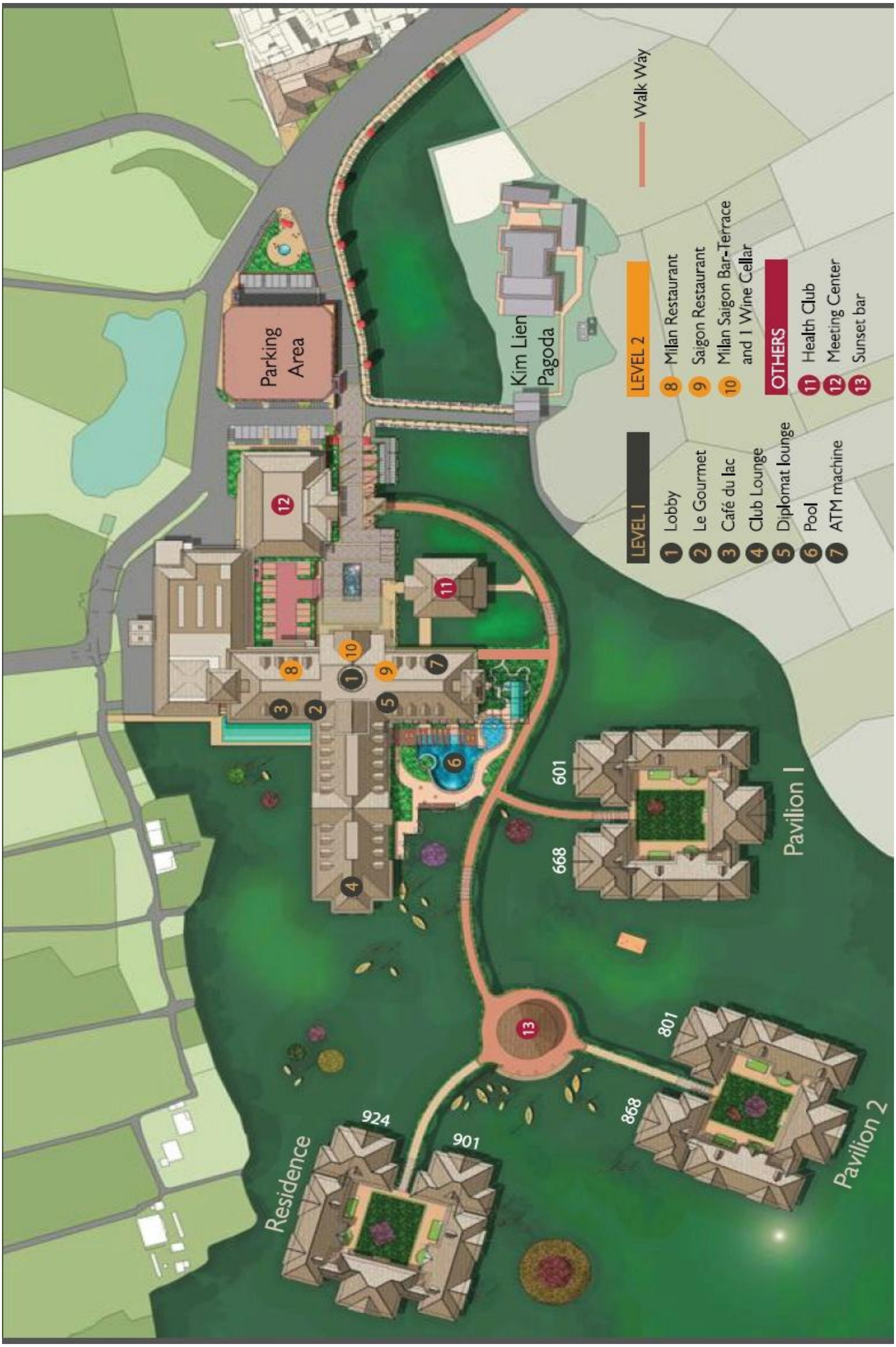
PROGRAM AND SCHEDULE

Updates of the program and schedule shall be posted on the monitors at the conference venue and http://www.asiacrypt2016.org/.

USEFUL CONTACT NUMBERS

Prof. Phan Duong Hieu (General co-Chair): (+84) 971 613 427, duong-hieu.phan@unilim.fr

Ms. Le Thi Lan Anh (Secretary): (+84) 979 074 911, ltlanh@viasm.edu.vn


Parking Area
Kim Lien Pagoda
Walk Way
LEVEL 1
1 Lobby
2 Le Gourmet
3 Café du lac
4 Club Lounge
5 Diplomat lounge
6 Pool
7 ATM machine
LEVEL 2
8 Milan Restaurant
9 Saigon Restaurant
10 Milan Saigon Bar-Terrace and I Wine Cellar
OTHERS
11 Health Club
12 Meeting Center
13 Sunset bar
601
668
Pavilion 1
801
868
Pavilion 2
924
901
Residence

SOCIAL FUNCTIONS

WELCOME RECEPTION

Welcome Reception is held at Sunset Bar on Sunday 4th December from 18.00 to 20.00.

PHOTO SESSION

The Photo Session is held on Monday 5th December from 10.50 to 11.00.

RUMP SESSION

The Rump Session takes place from 19.00 to 21.00 on Tuesday 6th December at the Grand Ballroom.

CONFERENCE BANQUET

The Gala Dinner commences at 19.30 on Wednesday 7th December at the Grand Ballroom.

HANOI EXCURSION

Hanoi Excursion includes a visit of the Vietnam Museum of Ethnology (14.15 - 16.15) and a show at the Thang Long Water Puppet Theatre (17.20 - 18.10). Departing by car from the InterContinental Hanoi Westlake at 14.00 on Tuesday 6th December.

PROGRAM

Sunday, December 4	
18:00-20:00	**Welcome Reception (Cocktails at Sunset Bar)**

Monday, December 5		
8:00-9:00	**Registration (Grand Ballroom)**	
9:00-9:30	**Welcome**	
9:30-10:20	**Invited Lecture I** **Nadia Heninger**, "The Reality of Cryptographic Deployments on the Internet" **(Jung Hee Cheon)**	
10:25-10:50	**Best Paper** Faster Fully Homomorphic Encryption: Bootstrapping in less than 0.1 Seconds; **Ilaria Chillotti; Nicolas Gama; Mariya Georgieva; Malika Izabachène (Tsuyoshi Takagi)**	
10:50-11:00	**Conference Photo**	
11:00-11:30	**Coffee Break**	
	R - track	**I - track**
	Mathematical Analysis I (Mehdi Tibouch)	**Zero Knowledge (Georg Fuchsbauer)**
11:30-11:55	▪ A General Polynomial Selection Method and New Asymptotic Complexities for the Tower Number Field Sieve Algorithm; **Palash Sarkar; Shashank Singh**	▪ Zero-Knowledge Accumulators and Set Algebra; **Esha Ghosh; Olga Ohrimenko; Dimitrios Papadopoulos; Roberto Tamassia; Nikos Triandopoulos**
11:55-12:20	▪ On the Security of Supersingular Isogeny Cryptosystems; **Steven D. Galbraith; Christophe Petit; Barak Shani; Yan Bo Ti**	▪ Zero-Knowledge Arguments for Matrix-Vector Relations and Lattice-Based Group Encryption; **Benoît Libert; San Ling; Fabrice Mouhartem; Khoa Nguyen; Huaxiong Wang**
12:20-14:20	**Lunch**	

	AES and White-Box (Amir Moradi)	**Post Quantum Cryptography (Steven Galbraith)**
14:20-14:45	▪ Simpira v2: A Family of Efficient Permutations Using the AES Round Function; **Shay Gueron; Nicky Mouha**	▪ From 5-pass MQ-based identification to MQ-based signatures; **Ming-Shing Chen; Andreas Hülsing; Joost Rijneveld; Simona Samardjiska; Peter Schwabe**
14:45-15:10	▪ Towards Practical Whitebox cryptography: Optimizing Efficiency and Space Hardness; **Andrey Bogdanov; Takanori Isobe; Elmar Tischhauser**	▪ Collapse-binding quantum commitments without random oracles; **Dominique Unruh**
15:10-15:35	▪ Efficient and Provable White-Box Primitives; **Pierre-Alain Fouque; Pierre Karpman; Paul Kirchner; Brice Minaud**	▪ Digital Signatures Based on the Hardness of Ideal Lattice Problems in all Rings; **Vadim Lyubashevsky**
15:35-16:05	**Coffee Break**	
	Hash Function (Lai Xuejia)	**Provable Security I (Takahiro Matsuda)**
16:05-16:30	▪ MiMC : Efficient Encryption and Cryptographic Hashing with Minimal Multiplicative Complexity; **Martin Albrecht; Lorenzo Grassi; Christian Rechberger; Arnab Roy; Tyge Tiessen**	▪ Adaptive Oblivious Transfer and Generalization; **Olivier Blazy; Céline Chevalier; Paul Germouty**
16:30-16:55	▪ Balloon Hashing: A Memory-Hard Function Providing Provable Protection Against Sequential Attacks; **Dan Boneh; Henry Corrigan-Gibbs; Stuart Schechter**	▪ Selective Opening Security from Simulatable Data Encapsulation; **Felix Heuer; Bertram Poettering**
16:55-17:20	▪ Linear Structures: Applications to Cryptanalysis of Round-Reduced Keccak; **Jian Guo; Meicheng Liu; Ling Song**	▪ Selective-Opening Security in the Presence of Randomness Failures; **Viet Tung Hoang; Jonathan Katz; Adam O'Neill; Mohammad Zaheri**
17:20-17:30	**Switch Time**	

	Randomness (Dominique Unruh)	**Provable Security II (Huaxiong Wang)**
17:30-17:55	▪ When are Fuzzy Extractors Possible?; **Benjamin Fuller; Leonid Reyzin; Adam Smith**	▪ Efficient KDM-CCA Secure Public-Key Encryption for Polynomial Functions; **Shuai Han; Shengli Liu; Lin Lyu**
17:55-18:20	▪ More Powerful and Reliable Second-level Statistical Randomness Tests for NIST SP800-22; **Shuangyi Zhu; Yuan Ma; Jingqiang Lin; Jia Zhuang; Jiwu Jing**	▪ Structure-Preserving Smooth Projective Hashing; **Olivier Blazy; Céline Chevalier**

Tuesday, December 6		
9:00-9:50	**Invited Lecture II** **Hoeteck Wee**, "Advances in Functional Encryption" **(Tatsuaki Okamoto)**	
9:55-10:20	**Invited to JoC** Nonlinear Invariant Attack --Practical Attack on Full SCREAM, iSCREAM, and Midori64; **Yosuke Todo; Gregor Leander; Yu Sasaki (Mitsuru Matsui)**	
10:20-10:50	**Coffee Break**	
	R - track	**I - track**
	Authenticated Encryption (Yosuke Todo)	**Digital Signature (Willy Susilo)**
10:50-11:15	▪ Trick or Tweak: On the (In)security of OTR's Tweaks; **Raphael Bost; Oliver Sanders**	▪ Signature Schemes with Efficient Protocols and Dynamic Group Signatures from Lattice Assumptions; **Benoît Libert; San Ling; Fabrice Mouhartem; Khoa Nguyen; Huaxiong Wang**
11:15-11:40	▪ Universal Forgery and Key Recovery Attacks on ELmD Authenticated Encryption Algorithm; **Aslı Bay; Oğuzhan Ersoy; Ferhat Karakoç**	▪ Towards Tightly Secure Lattice Short Signature and Id-Based Encryption; **Xavier Boyen; Qinyi Li**
11:40-12:05	▪ Statistical Fault Attacks on Nonce-Based Authenticated Encryption Schemes; **Christoph Dobraunig; Maria Eichlseder; Thomas Korak; Victor Lomné; Florian Mendel**	▪ From Identification to Signatures, Tightly: A Framework and Generic Transforms; **Mihir Bellare; Bertram Poettering; Douglas Stebila**

12:05-12:30	▪ Authenticated Encryption with Variable Stretch; **Reza Reyhanitabar; Serge Vaudenay; Damian Vizár**	▪ How to Obtain Fully Structure-Preserving (Automorphic) Signatures from Structure-Preserving Ones; **Yuyu Wang; Zongyang Zhang; Takahiro Matsuda; Goichiro Hanaoka; Keisuke Tanaka**
12:30-14:00	**Lunch**	
14:00-19:00	**Hanoi Excursion**	
19:30-22:00	**Rump Session (Steven Galbraith)**	

Wednesday, December 7		
9:00-9:50	**Invited Lecture III** **Neal Koblitz**, "Cryptography in Vietnam in the French and American Wars" **(Ngo Bao Chau)**	
9:55-10:20	**Invited to JoC** Cliptography: Clipping the Power of Kleptographic Attacks; **Alexander Russell; Qiang Tang; Moti Yung; Hong-Sheng Zhou (Serge Vaudenay)**	
10:20-10:50	**Coffee Break**	
	R - track	**I - track**
	Block Cipher I (Palash Sarkar)	**Functional and Homomorphic Cryptography (Sarah Meiklejohn)**
10:50-11:15	▪ Salvaging Weak Security Bounds for Blockcipher-Based Constructions; **Thomas Shrimpton; R. Seth Terashima**	▪ Multi-Key Homomorphic Authenticators; **Dario Fiore; Aikaterini Mitrokotsa; Luca Nizzardo; Elena Pagnin**
11:15-11:40	▪ How to Build Fully Secure Tweakable Blockciphers from Classical Blockciphers; **Lei Wang; Jian Guo; Guoyan Zhang; Jingyuan Zhao; Dawu Gu**	▪ Multi-Input Functional Encryption with Unbounded-Message Security; **Vipul Goyal; Aayush Jain; Adam O'Neill**
11:40-12:05	▪ Design Strategies for ARX with Provable Bounds: SPARX and LAX; **Daniel Dinu; Léo Perrin; Aleksei Udovenko; Vesselin Velichkov; Johann Großschädl; Alex Biryukov**	▪ Verifiable Function Encryption; **Saikrishna Badrinarayanan; Vipul Goyal; Aayush Jain; Amit Sahai**

12:05-14:05	**Lunch**	
	SCA and Leakage Resilience I (Kris Gaj)	**ABE and IBE (Duncan Wong)**
14:05-14:30	▪ Side-Channel Analysis Protection and Low-Latency in Action - case study of PRINCE and Midori; **Amir Moradi; Tobias Schneider**	▪ Dual System Encryption Framework in Prime-Order Groups via Computational Pair Encodings; **Nuttapong Attrapadung**
14:30-14:55	▪ Characterisation and Estimation of the Key Rank Distribution in the Context of Side Channel Evaluations; **Daniel P. Martin; Luke Mather; Elisabeth Osward; Martijin Stam**	▪ Efficient IBE with Tight Reduction to Standard Assumption in the Multi-challenge Setting; **Junqing Gong; Xiaolei Dong; Jie Chen; Zhenfu Cao**
14:55-15:20	▪ Taylor Expansion of Maximum Likelihood Attacks for Masked and Shuffled Implementations; **Nicolas Bruneau; Sylvain Guilley; Annelie Heuser; Olivier Rioul; François-Xavier Standaert; Yannic Teglia**	▪ Déjà Q All Over Again: Tighter and Broader Reductions of q-Type Assumptions; **Melissa Chase; Mary Maller; Sarah Meiklejohn**
15:20-15:45	▪ Unknown-Input Attacks in the Parallel Setting: Improving the Security of the CHES 2012 Leakage-Resilient PRF; **Marcel Medwed; François-Xavier Standaert; Ventzislav Nikov; Martin Feldhofer**	▪ Partitioning via Non-Linear Polynomial Functions: More Compact IBEs from Ideal Lattices and Bilinear Maps; **Shuichi Katsumata; Shota Yamada**
15:45-16:15	**Coffee Break**	
	Block Cipher II (Takanori Isobe)	**Foundation (Eiichiro Fujisaki)**
16:15-16:40	▪ A New Algorithm for the Unbalanced Meet-in-the-Middle Problem; **Ivica Nikolić; Yu Sasaki**	▪ How to Generate and use Universal Samplers; **Dennis Hofheinz; Tibor Jager; Dakshita Khurana; Amit Sahai; Brent Waters; Mark Zhandry**

16:40-17:05	▪ Applying MILP Method to Searching Integral Distinguishers Based on Division Property for 6 Lightweight Block Ciphers; **Zejun Xiang; Wentao Zhang; Zhenzhen Bao; Dongdai Lin**	▪ Iterated Random Oracle: A Universal Approach for Finding Loss in Security Reduction; **Fuchun Guo; Willy Susilo; Yi Mu; Rongmao Chen; Jianchang Lai; Guomin Yang**
17:05-17:30	▪ Reverse Cycle Walking and Its Applications; **Sarah Miracle; Scott Yilek**	▪ NIZKs with an Untrusted CRS: Security in the Face of Parameter Subversion; **Mihir Bellare; Georg Fuchsbauer; Alessandra Scafuro**
17:45-18:30	**IACR Meeting**	
19:30	**Conference Banquet (Grand Ballroom)**	

Thursday, December 8		
	R - track	**I - track**
	Mathematical Analysis II (Peter Schwabe)	**Cryptographic Protocol (Benoit Libert)**
9:00-9:25	▪ Optimization of LPN Solving Algorithms; **Sonia Bogos; Serge Vaudenay**	▪ Universal Composition with Responsive Environments; **Jan Camenisch; Robert R. Enderlein; Stephan Krenn; Ralf Küsters; Daniel Rausch**
9:25-9:50	▪ The Kernel Matrix Diffie-Hellman Assumption; **Paz Morillo; Carla Ràfols; Jorge L. Villar**	▪ A Shuffle Argument Secure in the Generic Model; **Prastudy Fauzi; Helger Lipmaa; Michał Zając**
9:50-10:15	▪ Cryptographic applications of capacity theory: On the optimality of Coppersmith's method for univariate polynomials; **Ted Chinburg; Brett Hemenway; Nadia Heninger; Zachary Scherr**	▪ Efficient Public-Key Distance Bounding Protocol; **Handan Kılınç; Serge Vaudenay**
10:15-10:40	▪ A Key Recovery Attack on MDPC with CCA Security Using Decoding Errors; **Qian Guo; Thomas Johansson; Paul Stankovski**	▪ Indistinguishable Proofs of Work or Knowledge; **Foteini Baldimtsi; Aggelos Kiayias; Thomas Zacharias; Bingsheng Zhang**

10:40-11:10	**Coffee Break**	
	SCA and Leakage Resilience II (Olivier Rioul)	**Multi-party Computation (Nuttapong Attrapadung)**
11:10-11:35	▪ A Tale of Two Shares: Why Two-Share Threshold Implementation Seems Worthwhile-and Why it is Not; **Cong Chen; Mohammad Farmani; Thomas Eisenbarth**	▪ Size-Hiding Computation for Multiple Parties; **Kazumasa Shinagawa; Koji Nuida; Takashi Nishide; Goichiro Hanaoka; Eiji Okamoto**
11:35-12:00	▪ Cryptographic Reverse Firewall via Malleable Smooth Projective Hash Functions; **Rongmao Chen; Yi Mu; Guomin Yang; Willy Susilo; Fuchun Guo; Mingwu Zhang**	▪ How to Circumvent the Two-Ciphertext Lower Bound for Linear Garbling Schemes; **Carmen Kempka, Ryo Kikuchi, Koutarou Suzuki**
12:00-12:25	▪ Efficient Public-Key Cryptography with Bounded Leakage and Tamper Resilience; **Antonio Faonio; Daniele Venturi**	▪ Constant-Round Asynchronous Multi-Party Computation Based on One-Way Functions; **Sandro Coretti; Juan A. Garay; Martin Hirt; Vassilis Zikas**
12:25-12:50	▪ Public-Key Cryptosystems Resilient to Continuous Tampering and Leakage of Arbitrary Functions; **Eiichiro Fujisaki; Keita Xagawa**	▪ Reactive Garbling: Foundation, Instantiation, Application; **Jesper Buus Nielsen; Samuel Ranellucci**
12:50-14:50	**Lunch**	
14:50	**Adieu**	