Inscrypt 2014

10th China International Conference on Information Security and Cryptology

Program

December 13-15, 2014

Beijing, China

Conference Information

Conference Venue: Building No.8, Beijing Friendship Hotel
(北京友谊宾馆，嘉宾楼5号会议室)

Registration and Information:

December 12,	14:00-19:00. Lobby of Building No. 2 (Jingbin hotel)
December 13-14,	08:00-18:00. Lobby of Building No. 8 (Conference site)
December 15,	08:00-12:00. Lobby of Building No. 8 (Conference site)

Lunches and dinners

Tickets for registered participants are in the registration bags. Lunches and dinners are served inside the Friendship Palace, specific location needs to follow the instructions.

Taxi

Taxies can be found at the front door of Building NO. 1. You may ask the hotel front desk to make a booking.

Program Sketch

10th China International Conference on Information Security and Cryptology

(Inscrypt 2014)

December 13 – 15, 2014, Beijing China

Dec 12	14:00-19:00	Conference on site registration	Lobby of Building 2 (Jingbin hotel)
	18:00-21:00	Reception	Friendship Palace (follow instructions)
Dec 13	8:00-9:00	Conference on site registration	Lobby of Building No. 8 (Conference site)
	9:00-9:10	Opening Remarks	Meeting room No.5, Building No.8
	9:10-10:10	Invited Talk (I)	
	10:10-10:25	Group Photo	In front of Building No.8
	10:45-12:00	Session 1	Meeting room No.5, Building No.8
	12:00-13:30	Lunch	Friendship Palace (follow instructions)
	13:30-14:30	Invited Talk (II)	Meeting room No.5, Building No.8
	14:30-15:20	Session 2	
	15:40-17:45	Session 3	
	18:00-19:30	Dinner	Friendship Palace (follow instructions)
	19:30-21:00	Rump Session	Meeting room No.5, Building No.8
Dec 14	9:00-10:00	Invited Talk (III)	Meeting room No.5, Building No.8
	10:20-12:00	Session 4	
	12:00-13:30	Lunch	Friendship Palace (follow instructions)
	13:30-14:30	Invited Talk (IV)	Meeting room No.5, Building No.8
	14:30-15:20	Session 5	
	15:40-17:20	Session 6	
	18:00-20:30	Conference Banquet	Juxiu Restrant (聚秀园),Friendship Palace
Dec 15	9:00-10:00	Invited Talk (V)	Meeting room No.5, Building No.8
	10:20-12:00	Session 7	
	12:00-13:30	Lunch	Friendship Palace (follow instructions)
	13:30-14:30	Invited Talk (VI)	Meeting room No.5, Building No.8
	14:30-15:20	Session 8	
	15:40-18:00	Session 9	
	18:00-19:30	Dinner	Friendship Palace (follow instructions)
Dec 16	Tour guide (only travel agent assistance provided)		

All presentations are in Meeting room No.5, Building No.8 (嘉宾楼第5会议室)

Advanced Program

10th China International Conference on Information Security and Cryptology
(Inscrypt 2014)
Beijing Friendship Hotel

December 12, 2014	
14:00-19:00	**Conference on site registration**
18:00-21:00	**Reception**
December 13, 2014	
8:00-9:00	**Conference on site registration**
9:00-9:10	**Opening Remarks**
Invited Talk (I) : **Session Chair: Moti Yung**	
9:10-10:10	Efficient Inner-Product Encryption and Its Applications *Tatsuaki Okamoto*
10:10-10:25	**Group photo**
10:25-10:45	**Coffee Break**
Session 1: PRIVACY AND ANONYMITY **Session Chair: Qingqi Pei**	
10:45-11:10	An Efficient Privacy-preserving E-coupon System *Weiwei Liu, Yi Mu and Guomin Yang*
11:10-11:35	Spatial Bloom Filters: Enabling Privacy in Location-aware Applications *Paolo Palmieri, Luca Calderoni and Dario Maio*
11:35-12:00	Security of Direct Anonymous Authentication using TPM 2.0 Signature *Tao Zhang and Sherman S. M. Chow*
12:00-13:30	**Lunch**
Invited Talk (II) : **Session Chair: Tatsuaki Okamoto**	
13:30-14:30	Effect of λ_i Gaps on Security of Lattice-based Cryptosystems *Xiaoyun Wang*
Session 2: MULTYPARTY AND OUTSOURCE COMPUTATION **Session Chair: Tatsuaki Okamoto**	
14:30-14:55	Revocation in Publicly Verifiable Outsourced Computation *James Alderman, Carlos Cid, Jason Crampton and Christian Janson*
14:55-15:20	Private aggregation with Custom Collusion Tolerance *Constantinos Patsakis, Michael Clear and Paul Laird*
15:20-15:40	**Coffee Break**
Session 3: SIGNATURE AND SECURITY PROTOCOLS **Session Chair: Yu Chen**	
15:40-16:05	Ring Signatures of Constant Size without Random Oracles *Fei Tang and Hongda Li*

16:05-16:30	Universally Composable Identity Based Adaptive Oblivious Transfer with Access Control *Vandana Guleria and Ratna Dutta*
16:30-16:55	Three-Round Public-Coin Bounded-Auxiliary-Input Zero-Knowledge Arguments of Knowledge *Ning Ding*
16:55-17:20	A Model-driven Security Requirements Approach to Deduce Security Policies Based on OrBAC *Denisse Muñante, VaneaChiprianov, Laurent Gallon and Philippe Aniorté*
17:20-17:45	Optimal Proximity Proofs *Ioana Boureanu and Serge Vaudenay*
18:00-19:30	**Dinner**
19:30-21:00	**RUMP SESSION** **Session Chair: Chuankun Wu**

December 14, 2014

Invited Talk (III) : **Session Chair: Jianying Zhou**	
9:00-10:00	Cryptographic Applications of Algebraic Dynamics: Past, Present, Future *Vladimir Anashin*
10:00-10:20	**Coffee Break**
Session 4: LATTICE AND PUBLIC KEY CRYPTOGRAPHY **Session Chair: Constantinos Patsakis**	
10:20-10:45	Simpler CCA-Secure Public Key Encryption from Lossy Trapdoor Functions *Bei Liang, Rui Zhang and Hongda Li*
10:45-11:10	Attacking RSA with a Composed Decryption Exponent Using Unravelled Linearization *Zhangjie Huang, Lei Hu and Jun Xu*
11:10-11:35	Fully Homomorphic Encryption with Auxiliary Inputs *Fuqun Wang and Kunpeng Wang*
11:35-12:00	Trapdoors for Ideal Lattices with Application *Russell W. F. Lai, Henry K. F. Cheung and Sherman S. M. Chow*
12:00-13:30	**Lunch**
Invited Talk (IV) **Session Chair: Xiaoyun Wang**	
13:30-14:30	The Evolution of iOS Security *Jianying Zhou*
Session 5: BLOCK CIPHER AND HASH FUNCTION (I) **Session Chair: Xiaoyun Wang**	
14:30-14:55	Speeding up the Search Algorithm for the Best Differential and Best Linear Trails *Zhenzhen Bao, Wentao Zhang and Dongdai Lin*
14:55-15:20	The Boomerang Attacks on BLAKE and BLAKE2 *Yonglin Hao*
15:20-15:40	**Coffee Break**
Session 6: BLOCK CIPHER AND HASH FUNCTION (II) **Session Chair: Ning Ding**	
15:40-16:05	Second Preimage Analysis of Whirlwind *Riham Altawy and Amr Youssef*

16:05-16:30	Boomerang Attack on Step-Reduced SHA-512 *Hongbo Yu and Dongxia Bai*
16:30-16:55	Collision Attack on 4-branch, Type-2 GFN based Hash Functions using Sliced Biclique Cryptanalysis Technique *Megha Agrawal, Donghoon Chang, Mohona Ghosh and Somitra Sanadhya*
16:55-17:20	Rig: A simple, secure and flexible design for Password Hashing *Donghoon Chang, Arpan Jati, Sweta Mishra and Somitra Sanadhya*
18:00-20:30	**Banquet**

December 15, 2014

Invited Talk (V) : **Session Chair: Dongdai Lin**	
9:00-10:00	The Drunk Motorcyclist Protocol for Anonymous Communication *Moti Yung*
10:00-10:20	**Coffee Break**
Session 7: AUTHENTICATION AND ENCRYPTION **Session Chair: Jian Guo**	
10:20-10:45	Lighter, Faster, and Constant-Time: WhirlBob, the Whirlpool variant of StriBob *Markku-Juhani Olavi Saarinen and Billy Brumley*
10:45-11:10	Efficient Hardware Accelerator for AEGIS-128 Authenticated Encryption *Debjyoti Bhattacharjee and Anupam Chattopadhyay*
11:10-11:35	Fully Collusion-Resistant Traceable Key-Policy Attribute-Based Encryption with Sub-linear Size Ciphertexts *Zhen Liu, Zhenfu Cao and Duncan Wong*
11:35-12:00	Integrating Ciphertext-policy Attribute-Based Encryption with Identity-Based Ring Signature to Enhance Security and Privacy in Wireless Body Area Networks *Changji Wang, Dongyuan Shi and Yuan Li*
12:00-13:30	**Lunch**
Invited Talk (VI) **Session Chair: Miroslaw Kutylowski**	
13:30-14:30	Recent Advances in Analysis of HMAC *Jian Guo*
Session 8: ELLIPTIC CURVE **Session Chair: Miroslaw Kutylowski**	
14:30-14:55	Parallelized Software Implementation of Elliptic Curve Scalar Multiplication *Jean-Marc Robert*
14:55-15:20	A Note on Diem's Proof *Song Tian, Kunpeng Wang, Bao Li and Wei Yu*
15:20-15:40	**Coffee Break**
Session 9: CRYPTOGRAPHIC PRIMITIVE AND APPLICATION **Session Chair: Sherman S. M. Chow**	
15:40-16:05	Stand-by Attacks on E-ID Password Authentication *Lucjan Hanzlik, Przemysław Kubiak and Miroslaw Kutylowski*
16:05-16:30	Stegomalware: Playing Hide and Seek with Malicious Components in Smartphone Apps *Guillermo Suarez-Tangil, Juan Tapiador and Pedro Peris-Lopez*

16:30-16:55	A Lightweight Security Isolation Approach for Virtual Machines Deployment *Hongliang Liang and Changyao Han*
16:55-17:20	MEMS Based Random Number Generation for Wearable Computing Environments *Neel Bedekar, Chiranjit Shee and Cameron Ballingall*
17:20-18:00	Closing remarks
18:00-19:30	**Dinner**
December 16, 2014	
Tour (only travel agent assistance provided)	