– – Call for Participation –

- The 22nd Workshop on Elliptic Curve Cryptography (ECC 2018)

– November 17–21 2018, Osaka, Japan

Contact: ecc2018-organizer@crypto-cybersec.comm.eng.osaka-u.ac.jp

Workshop Web Site: https://cy2sec.comm.eng.osaka-u.ac.jp/ecc2018/

The 22nd Workshop on Elliptic Curve Cryptography (ECC 2018) will be held in Osaka, Japan in November 2018. It will be co-organized by Osaka University, Japan Advanced Institute of Science and Technology (JAIST), Information-technology Promotion Agency, Japan (IPA), and CREST (JPMJCR1404) at Japan Science and Technology Agency (JST).

ECC is an annual workshop dedicated to the study of elliptic curve cryptography and related areas. Since the first ECC workshop, held 1997 in Waterloo, the ECC conference series has broadened its scope beyond elliptic curve cryptography and now covers a wide range of areas within modern cryptography. This is the first time for ECC to be held in East Asia.

Program - Autumn school:

Saturday, November 17, 2018

10:00-10:30	Registration
10:30-10:40	Opening Remarks
10:40-12:10	ECC Autumn School I (Coordinator: Akinori Kawachi)
10:40-12:10	**Classical attacks on elliptic curve cryptosystems: an overview** Mehdi Tibouchi(NTT Corporation)
12:10-13:10	Lunch Break
13:10-16:20	ECC Autumn School II (Coordinator: Naoto Yanai)
13:10-14:40	**Introduction to Hardware Implementation of ECC** Kazuo Sakiyama(The University of Electro-Communications)
14:40-14:50	Short Break
14:50-16:20	**CSIDH: a post-quantum drop-in replacement for ECDH** Chloe Martindale(Technical University of Eindhoven)
16:20-16:30	Coffee Break
16:30-18:00	ECC Autumn School III (Coordinator: Seiko Arita)
16:30-18:00	**Software implementations of ECC: security and efficiency** Tung Chou(Osaka University)
18:30-20:30	Dinner

Sunday, November 18, 2018

09:00-12:20	ECC Autumn School IV

	(Coordinator: Yuji Suga)
09:00-10:30	**Blockchain: Fundamental and Advanced Topics** Roger Wattenhofer(ETH Zurich)
10:30-10:50	Coffee Break
10:50-12:20	**An introduction to SIDH** David Jao(University of Waterloo/evolutionQ, Inc.,Waterloo)

Program - Main conference:

Monday, November 19, 2018 (8 talks)

08:30-09:00	Registration
09:00-09:20	Opening Remarks
09:20-11:00	Isogeny-based cryptography (1) (Chair: Tsuyoshi Takagi)
09:20-10:10	**Implementing supersingular isogeny cryptography** David Jao(University of Waterloo/evolutionQ, Inc., Waterloo)
10:10-11:00	**Computing isogenies and endomorphism rings of supersingular elliptic curves** Travis Morrison(The Pennsylvania State University)
11:00-11:20	Coffee Break
11:20-12:40	Block chain (Chair: Kazumasa Omote)
11:20-12:10	**Ring signatures for blockchain** Eiichiro Fujisaki(JAIST)
12:10-12:40	**The Role of Cryptography in Distributed Systems** Roger Wattenhofer(ETH Zurich)
12:40-13:40	Lunch Break
13:40-15:20	Beyond ECC (Chair: Tanja Lange)
13:40-14:30	**Point counting on hyperelliptic curves of genus 3 and higher in large characteristic** Pierrick Gaudry(LORIA)
14:30-15:20	**A new public key cryptosystem based on Mersenne numbers** Divesh Aggarwal(National University of Singapore)
15:20-15:40	Coffee Break
15:40-17:20	Fundamental (Computer algebra to Quantum Computer) (Chair: Akira Otsuka)
15:40-16:30	**Quantum Information Processing — Similarities and Differences with Classical Information Processing** Nobuyuki Imoto(Osaka University)
16:30-17:20	**Computing the number of points of quasi-diagonal hypersurfaces** Henri Cohen(Université de Bordeau)
19:00-21:00	Banquet

Tuesday, November 20, 2018 (3 talks)

09:00-09:50	ECC implementation (Chair: Ryuichi Sakai)
09:00-09:50	**Lower-level Verifications for Cryptographic Software involving Elliptic Curves and others** Bo-Yin Yang(Institute of Information Science, Academia

	SinicaTaipeiTaiwan)
09:50-10:10	Coffee Break
10:10-11:30	Post-Quantum and Privacy-Enhancing Cryptography (Chair: Kwangjo Kim)
10:10-10:40	**Recent Developments in Post-Quantum Cryptography** Tsuyoshi Takagi(University of Tokyo)
10:40-10:30	**Privacy-Enhancing Signatures** Sherman S. M. Chow(Chinese University of Hong Kong)
11:45-20:00	Excursion and dinner at Nara Park

Wednesday, November 21, 2018 (4 talks)

08:50-10:30	Homomorphic encryptions (Chair: Serge Vaudenay)
08:50-09:40	**Design and application of approximate homomorphic encryption** Yongsoo Song(Microsoft Research, Redmond)
09:40-10:30	**Practical Two-level Homomorphic Encryption in Prime-order Bilinear Groups** Goichiro Hanaoka(AIST)
10:30-10:50	Coffee Break
10:50-12:30	Isogeny-based cryptography (Chair: Shinya Okumura)
10:50-11:40	**CSIDH: An Efficient Post-Quantum Commutative Group Action** Chloe Martindale(Technical University of Eindhoven)
11:40-12:30	**One-Round Authenticated Group Key Exchange from Isogenies** Katsuyuki Takashima(Mitsubishi Electric Corp)

Registration Fees

Category		[Early] Until 2018/10/9	[Late] Until 2018/11/5
Regular	Autumn School Only	JPY 30,000	JPY 40,000
	Workshop Only	JPY 50,000	JPY 65,000
	Both Autumn School & Workshop	JPY 75,000	JPY 95,000
Student	Autumn School Only	JPY 25,000	JPY 35,000
	Workshop Only	JPY 35,000	JPY 50,000
	Both Autumn School & Workshop	JPY 55,000	JPY 75,000

Workshop Organization:

General Chair*:* Akira Otsuka (Institute of Information Security, Japan)
Program Co-Chairs: Atsuko Miyaji (Osaka University/JAIST, Japan) and Chen-Mou Cheng (Osaka University, Japan)

Workshop Venue: Osaka is the second largest area in Japan. Osaka is known as historical merchant city and used to be called “the nation's kitchen." Moreover, Osaka is close to Kyoto and Nara (Japanese old capitals) and Kobe (popular port town). The workshop venue is Osaka University Suita Campus (http://www.osaka-u.ac.jp/en/access/#suita)

Travel Information: The workshop venue is located approximately 17 kilometers north of Osaka Station. The nearest station is Handai-Byoin-Mae station of Osaka Monorail, from which it will take about 5–15 minutes on foot.
From Overseas:

- **Kansai International Airport (IATA Code: KIX)**: There are some international flights from overseas to Kansai Airport. There are several ways to get to the conference venue via public transportation, and here we give a rather simple example: 1) take JR line to Osaka[*1] Station; 2) take subway Midosuji Line to Senri-Chuo Stations; and 3) take Osaka Monorail and exit at Handai-Byoin-Mae Station.

From Tokyo Area:

- **By train (Shinkansen)**: You can get to Shin-Osaka Station from Tokyo Station by Tokaido Shinkansen operated by JR (Japan Railway). The cost will be about 14,000 JPY, which may vary depending on travel conditions. 'Nozomi' is the fastest type and takes about 2.5 hours. 'Hikari' stops at more stations than 'Nozomi' does and takes about 3 hours. From Shin-Osaka Station, you can take subway Midosuji Line to Senri-Chuo, and then take Osaka Monorail to exit at Handai-Byoin-Mae Station.
- **By airplain**: You can get to Osaka International Airport (Itami Airport) from Haneda Airport. From Osaka International Airport, you can take Osaka Monorail and exit at Handai-Byoin-Mae Station.

Supported by:
Special Interest Group on Computer Security (CSEC), IPSJ, Japan, Technical Committee on Hardware Security (HWS), IEICE, Japan, Technical Committee on Information and Communication System Security (ICSS), IEICE, Japan, Technical Group on Information Security (ISEC), IEICE, Japan

Sponsored by:
Mercari, Inc., Accenture Japan Ltd., BC Technology Laboratories Inc., Eltes Co., Ltd., LINE Corporation, Cybozu, Inc, Hokuriku Telecommunication Network Co.,Inc., and Mitsubishi Electric Corporation