DATE	TIME SLOT		EVENT	TITLE	SPEAKER/AUTHORS	SESSION CHAIR
	UTC + 0	JST (UTC + 9)				
						ACNS
June 21	8:00-8:15	17:00-17:15	Opening and welcome			
	8:15-9:15	17:15-18:15	Keynote speech 1	Privacy-Preserving Authentication: Concepts, Applications, and New Advances	Anja Lehmann	Nils Ole Tippenhauer
	9:15-10:00	18:15-19:00	Session 1: Cryptographic Protocols	Adaptive-ID Secure Hierarchical ID-Based Authenticated Key Exchange under Standard Assumptions without Random Oracles	Ren Ishibashi and Kazuki Yoneyama	Joaquin Garcia-Alfaro
				Analysis of Client-side Security for Long-term Time-stamping Services	Long Meng and Liqun Chen	
				Towards Efficient and Strong Backward Private Searchable Encryption with Secure Enclaves	Viet Vo, Shangqi Lai, Xingliang Yuan, Joseph Liu and Surya Nepal	
	10:00-10:30	19:00-19:30	break			
	10:30-11:15	19:30-20:15	Session 2: Secure and Fair Protocols	CECMLP: New Cipher-Based Evaluating Collaborative Multi-Layer Perceptron Scheme in Federated Learning	Yuqi Chen, Xiaoyu Zhang, Yi Xie, Meixia Miao and Xu Ma	Qiang Tang
				Blind Polynomial Evaluation and Data Trading	Yi Liu, Qi Wang and Siu Ming Yiu	
				Coin-Based Multi-Party Fair Exchange	Handan Kilinc Alper and Alptekin Kupcu	
	11:30-12:15	20:30-21:15	Session 3: Cryptocurrency and Smart Contracts	P2DEX: Privacy-Preserving Decentralized Cryptocurrency Exchange	Carsten Baum, Bernardo David and Tore Frederiksen	Ghassan Karame
				WOTS+ up my Sleeve! A Hidden Secure Fallback for Cryptocurrency Wallets	David Chaum, Mario Larangeira, Mario Yaksetig and William Carter	
				Terrorist Attacks for Fake Exposure Notifications in Contact Tracing Systems	Gennaro Avitabile, Daniele Friolo and Ivan Visconti	
	12:15-13:00	21:15-22:00	Virtual social event (virtual tour of Kamakura ect.)			

DATE	TIME SLOT		EVENT	TITLE	SPEAKER/AUTHORS	SESSION CHAIR
	UTC + 0	JST (UTC + 9)				
June 22	8:00-9:00	17:00-18:00	Keynote speech 2	Digital Being	Nat Sakimura	Kazue SAKO
	9:10-10:00	18:10-19:00	Session 4: Digital Signatures	Unlinkable and Invisible γ-Sanitizable Signatures	Angèle Bossuat and Xavier Bultel	Zekeriya Erkin
				Partially Structure-Preserving Signatures: Lower Bounds, Constructions and More	Essam Ghadafi	
				An Efficient Certificate-Based Signature Scheme in the Standard Model	Guoqiang Wang and Yanmei Cao	
	10:00-10:30	19:00-19:30	break			
	10:30-11:15	19:30-20:15	Session 5: Embedded System Security	SnakeGX: a sneaky attack against SGX Enclaves	Flavio Toffalini, Mariano Graziano, Mauro Conti and Jianying Zhou	Sooel Son
				Telepathic Headache: Mitigating Cache Side-Channel Attacks on Convolutional Neural Networks	Hervé Chabanne, Jean-Luc Danger, Linda Guiga and Ulrich Kühne	
				Efficient FPGA Design of Exception-Free Generic Elliptic Curve Cryptosystems	Kiyofumi Tanaka, Atsuko Miyaji and Yaoan Jin	
	11:30-12:15	20:30-21:15	Session 6: Lattice Cryptography	Access Control Encryption from Group Encryption	Xiuhua Wang, Harry W.H. Wong and Sherman S. M. Chow	Nico Döttling
				Password Protected Secret Sharing from Lattices	Partha Sarathi Roy, Sabyasachi Dutta, Willy Susilo and Reihaneh Safavi-Naini	
				Efficient Homomorphic Conversion Between (Ring) LWE Ciphertexts	Hao Chen, Wei Dai, Miran Kim and Yongsoo Song	

DATE	TIME SLOT		EVENT	TITLE	SPEAKER/AUTHORS	SESSION CHAIR
	UTC + 0	JST (UTC + 9)				
June 23	8:00-9:00	17:00-18:00	Keynote speech 3	Cryptography and the Changing Landscape of Payment Fraud	Ross Anderson	Zhou Jianying
	9:15-10:00	18:15-19:00	Session 7: Analysis of Applied Systems	Breaking and Fixing Third-Party Payment Service for Mobile Apps	Shangcheng Shi, Xianbo Wang and Wing Cheong Lau	Cristina Alcaraz
				DSS: Discrepancy-Aware Seed Selection Method for ICS Protocol Fuzzing	Shuangpeng Bai, Dongliang Fang, Yue Sun, Puzhuo Liu, Hui Wen and Limin Sun	
				Threat for the Secure Remote Password Protocol and a leak in Apple's Cryptographic Library	Andy Russon	
	10:00-10:30	19:00-19:30	break			
	10:30-11:15	19:30-20:15	Session 8: Secure Computations	Privacy-Preserving Data Aggregation with Probabilistic Range Validation	F. W. Dekker and Zekeriya Erkin	F. Betül Durak
				LLVM-based Circuit Compilation for Practical Secure Computation	Tim Heldmann, Thomas Schneider, Oleksandr Tkachenko, Christian Weinert and Hossein Yalame	
				An Efficient Passive-to-Active Compiler for Honest-Majority MPC over Rings	Mark Abspoel, Anders Dalskov, Daniel Escudero and Ariel Nof	
	11:30-12:15	20:30-21:15	Session 9: Cryptanalysis	Experimental Review of the IKK Query Recovery Attack: Assumptions, Recovery Rate and Improvements	Ruben Groot Roessink, Andreas Peter and Florian Hahn	Kazuhiko Minematsu
				Efficient Methods to Search for Best Differential Characteristics on SKINNY	Stephanie Delaune, Patrick Derbez, Paul Huynh, Marine Minier, Victor Mollimard and Charles Prud'Homme	
				Towards Efficient LPN-Based Symmetric Encryption	Thomas Locher, Sonia Bogos, Dario Korolija and Serge Vaudenay	

DATE	TIME SLOT		EVENT	TITLE	SPEAKER/AUTHORS	SESSION CHAIR
	UTC + 0	JST (UTC + 9)				
June 24	24:00-1:15	9:00-10:15	Session 10: System Security	A Differentially Private Hybrid Approach to Traffic Monitoring	Rogério Rocha, Pedro Libório, Harsh Kupwade Patil and Diego Aranha	Martin Ochoa
				Proactive Detection of Phishing Kit Traffic	Qian Cui, Guy-Vincent Jourdan and Iosif Viorel Onut	
				Vestige: Identifying Binary Code Provenance for Vulnerability Detection	Yuede Ji, Lei Cui and H. Howie Huang	
				SoK: Auditability and Accountability in Distributed Payment Systems	Panagiotis Chatzigiannis, Foteini Baldimtsi and Konstantinos Chalkias	
				Defending Web Servers Against Flash Crowd Attacks	Rajat Tandon, Abhinav Palia, Jaydeep Ramani, Brandon Paulsen, Genevieve Bartlett and Jelena Mirkovic	
	1:15-1:45	10:15-10:45	Poster Session	POSTER: Resistance analysis of two AES-like against the boomerang attack	Laetitia Debesse, Sihem Mesnager , and Mounira Msahli	Masaki Shimaoka
				POSTER: LHSA: Lightweight Hardware Security Arbitrato	Yongjin Kim	
				POSTER: Another Look At Boyar-Peralta's Algorithm	Anubhab Baksi, Banashri Karmakar, and Vishnu Asutosh Dasu	
				POSTER: Optimizing Device Implementation Of Linear Layers With Automated Tools	Anubhab Baksi, Banashri Karmakar, and Vishnu Asutosh Dasu	
	1:45-3:00	10:45-12:00	Session 11: Cryptography and its Applications	TurboIKOS: Improved Non-interactive Zero Knowledge with Sublinear Memory	Yaron Gvili, Julie Ha, Sarah Scheffler, Mayank Varia, Ziling Yang and Xinyuan Zhang	Man Ho Au
				Cryptanalysis of the Binary Permuted Kernel Problem	Thales Paiva and Routo Terada	
				Security Comparisons and Performance Analyses of Post-Quantum Signature Algorithms	Manohar Raavi, Simeon Wuthier, Pranav Chandramouli, Yaroslav Balytskyi, Xiaobo Zhou and Sang-Yoon Chang	
				Tighter Proofs for the SIGMA and TLS 1.3 Key Exchange Protocols	Hannah Davis and Felix Günther	
				Improved Structured Encryption for SQL Databases via Hybrid Indexing	David Cash, Ruth Ng and Adam Rivkin	
	3:00-3:15	12:00-12:15	Closing Session			