

2023-06-19 (Monday)



9:00-9:30

Registration



9:30-9:40

Opening remarks

Kazumasa Omote & Chunhua Su

9:40-11:10

Web security

Session chair TBD

Tiny WFP : Lightweight and Effective Website Fingerprinting Via Wavelet Multi-Resolution Analysis

Cong Tian, Dengpan Ye, Chuanxi Chen

Those Aren't Your Memories and They're Somebody Else's: Seeding Misinformation in Chat Bot Memories

Conor Atkins, Benjamin Zi Hao Zhao, Hassan Jameel Asghar, Ian Wood, Mohamed Ali Kaafar

Social Honeypot for Humans: Luring People through Self-managed Instagram Pages

Sara Bardi, Mauro Conti, Luca Pajola, Pier Paolo Tricomi

Capturing Antique Browsers in Modern Devices: A Security Analysis of Captive Portal Mini-Browsers

Ping-Lun Wang, Kai-Hsiang Chou, Shou-Ching Hsiao, Ann Tene Low, Tiffany Hyun-Jin Kim, Hsu-Chun Hsiao

11:10-11:30

Coffee break

11:30-12:30

Invited talk I

Mehdi Tibouchi

Challenges and Solutions to Post-Quantum Secure Messaging

Shuichi Katsumata

12:30-14:00

Lunch

14:00-15:55

Lattices and codes

Session chair TBD

**Forward Security of Fiat-Shamir Lattice Signatures**

Yang Tao, Rui Zhang, Yunfeng Ji

**Shorter and Faster Identity-Based Signatures with Tight Security in the (Q)ROM from Lattices**

Eric Sageloli, Pierre Pébereau, Pierrick Méaux, Céline Chevalier

**A Gapless Post-Quantum Hash Proof System in the Hamming Metric**

Bénédict Tran, Serge Vaudenay

**Spherical Gaussian Leftover Hash Lemma via the Rényi Divergence**

Hiroki Okada, Kazuhide Fukushima, Shinsaku Kiyomoto, Tsuyoshi Takagi

**BIKE Key-Recovery: Combining Power Consumption Analysis and Information-Set Decoding**

Agathe Cheriére, Nicolas Aragon, Tania Richmond, Benoît Gérard

15:55-16:15

Coffee break

16:15-17:45

Symmetric cryptanalysis

Session chair TBD

**A Novel Automatic Technique Based on MILP to Search for Impossible Differentials**

Yong Liu, Zejun Xiang, Siwei Chen, Shasha Zhang, Xiangyong Zeng

**Meet-in-the-Filter and Dynamic Counting with Applications to Speck**

Alex Biryukov, Luan Cardoso dos Santos, Je Sen Teh, Aleksei Udoenko, Vesselin Velichkov

**Near Collision Attack against Grain v1**

Subhadeep Banik, Daniel Collins, Willi Meier

**TIDAL: Practical Collisions on State-Reduced Keccak Variants**

Sahiba Suryawanshi, Dhiman Saha, Shashwat Jaiswal

18:00-21:00

Poster session & Welcome reception

2023-06-20 (Tuesday)



9:00-10:30

**Machine learning**

Session chair TBD

**Fast and Efficient Malware Detection with Joint Static and Dynamic Features Through Transfer Learning**

Mao V. Ngo, Tram Truong-Huu, Dima Rabadi, Jia Yi Loo, Sin G. Teo

**Efficient Network Representation for GNN-based Intrusion Detection**

Hamdi Friji, Alexis Olivereau, Mireille Sarkiss

**EVADE: Efficient Moving Target Defense for Autonomous Network Topology Shuffling Using Deep Reinforcement Learning**

Qisheng Zhang, Jin-Hee Cho, Terrence J. Moore, Dan Dongseong Kim, Hyuk Lim, Frederica Nelson

**Steal from Collaboration: Spy Attack by a Dishonest Party in Vertical Federated Learning**

Hongbin Chen, Chaohao Fu, Na Ruan

10:30-10:50

Coffee break

10:50-12:20

## Side-channel and fault attacks

Session chair TBD

### Formal Verification of Arithmetic Masking in Hardware and Software

Barbara Gigerl, Robert Primas, Stefan Mangard

### Layered Binary Templating

Martin Schwarzl, Erik Kraft, Daniel Gruss

### HS-based error correction algorithm for noisy binary GCD side-channel sequences

Kenta Tani, Noboru Kunihiro

### Divide and Rule: DiFA - Division Property Based Fault Attacks on PRESENT and GIFT

Anup Kumar Kundu, Shibam Ghosh, Dhiman Saha, Mostafizar Rahman

12:20-13:50

Lunch

13:50-15:20

## Embedded security

Session chair TBD

### A Forkcipher-based Pseudo-Random Number Generator

Elena Andreeva, Andreas Wenzinger

### DMA'n'Play: Practical Remote Attestation Based on Direct Memory Access

Sebastian Surminski, Christian Niesler, Lucas Davi, Ahmad-Reza Sadeghi

### Recommendation for a holistic secure embedded ISA extension

Florian Stolz, Marc Fyrbiak, Pascal Sasdrich, Tim Güneysu

### QuantumCharge: Post-Quantum Cryptography for Electric Vehicle Charging

Dustin Kern, Christoph Krauß, Timm Lauser, Nouri Alnahawi, Alexander Wiesmaier, Ruben Niederhagen

15:20-15:40

Coffee break

15:40-16:50

Elliptic curves and pairings

Session chair TBD

Pairings in Rank-1 Constraint System

Youssef El Housni

Binary Kummer Line

Sabyasachi Karati

Generalised Asynchronous Remote Key Generation for Pairing-based Cryptosystems

Nick Frymann, Daniel Gardham, Mark Manulis, Hugo Nartz

16:50-18:00

Isogeny-based cryptography

Session chair TBD

Low Memory Attacks on Small Key CSIDH

Jesús-Javier Chi-Domínguez, Andre Esser, Sabrina Kunzweiler, Alexander May

Practical Robust DKG Protocols for CSIDH

Shahla Atapoor, Karim Baghery, Daniele Cozzo, Robi Pedersen

Efficient Isogeny Proofs Using Generic Techniques

Kelong Cong, Yi-Fu Lai, Shai Levin

2023-06-21 (Wednesday)



9:00-10:30

## Privacy-preserving protocols

Session chair TBD

### Constant-Round Multiparty Private Function Evaluation With (Quasi-)Linear Complexities

Yongfeng Xu, Hanyu Jia, Xiangxue Li, Qiang Li, Yue Bao, Xintian Hou

### Predicate Private Set Intersection With Linear Complexity

Yaxi Yang, Jian Weng, Yufeng Yi, Changyu Dong, Leo Yu Zhang, Jianying Zhou

### A Framework for UC Secure Privacy Preserving Biometric Authentication using Efficient Functional Encryption

Johannes Ernst, Katerina Mitrokotsa

### Private Information Retrieval with Result Verification for More Servers

Pengzhen Ke, Liang Feng Zhang

10:30-10:50

Coffee break

10:50-12:00

## Homomorphic cryptography

Session chair TBD

### PIE: p-adic Encoding for High-Precision Arithmetic in Homomorphic Encryption

Luke Harmon, Gaetan Delavignette, Arnab Roy, David Silva

### Analysis and Prevention of Averaging Attacks against Obfuscation Protocols

Kilian Becher, J. A. Gregor Lagodzinski, Javier Parra Arnau, Thorsten Strufe

### FLSwitch: Towards Secure and Fast Model Aggregation for Federated Deep Learning with a Learning State-Aware Switch

Yunlong Mao, Ziqin Dang, Yu Lin, Tianling Zhang, Yuan Zhang, Jingyu Hua, Sheng Zhong

12:00-13:30

Lunch

13:30-14:30

Invited talk II

XiaoFeng Wang

Language-enforced Data Confidentiality against Memory Disclosure and Transient Execution Attacks

Michalis Polychronakis

14:30-22:00

Tour & Conference dinner

University Center Lagoon Plaza

2023-06-22 (Thursday)



9:00-10:30

Encryption

Session chair TBD

On the Complete Non-Malleability of the Fujisaki-Okamoto Transform

Daniele Friolo, Matteo Salvino, Daniele Venturi

Optimal Security Notion for Decentralized Multi-Client Functional Encryption

Ky Nguyen, Duong Hieu Phan, David Pointcheval

Anonymous (Hierarchical) Identity-Based Encryption from Broader Assumptions

Huangting Wu, Sherman S. M. Chow

Publicly Auditable Functional Encryption

Vlasis Koutsos, Dimitrios Papadopoulos

10:30-10:50

Coffee break

10:50-12:20

Advanced primitives

Session chair TBD

Robustly Reusable Fuzzy Extractors in a Post-Quantum World

Amit Deo, Charles Grover

Subversion-Resilient Authenticated Encryption without Random Oracles

Pascal Bemmman, Sebastian Berndt, Denis Diemert, Tibor Jager, Thomas Eisenbarth

Scored Anonymous Credentials

Sherman S. M. Chow, Jack P. K. Ma, Tsz Hon Yuen

GeT a CAKE: Generic Transformations from Key Encapsulation Mechanisms to Password Authenticated Key Exchanges

Hugo Beguinet, Céline Chevalier, David Pointcheval, Thomas Ricosset, Mélissa Rossi

12:20-13:50

Lunch

13:50-15:20

Multiparty computation

Session chair TBD

Explicit and Nearly Tight Lower Bound for 2-party Perfectly Secure FSS

Keitaro Hiwatashi, Koji Nuida

Multi-Theorem Fiat-Shamir Transform from Correlation-Intractable Hash Functions

Michele Ciampi, Yu Xia

Game-Theoretically Secure Protocols for the Ordinal Random Assignment Problem

T-H. Hubert Chan, Ting Wen, Hao Xie, Quan Xue

**A New Approach to Garbled Circuits**

Anasuya Acharya, Tomer Ashur, Efrat Cohen, Carmit Hazay, Avishay Yanai

15:20-15:40

Coffee break

15:40-16:50

Blockchain

**Mt. Random: Multi-Tiered Randomness Beacons**

Ignacio Cascudo, Bernardo David, Omer Shlomovits, Denis Varlakov

**Revisiting Transaction Ledger Robustness in the Miner Extractable Value Era**

Fredrik Kamphuis, Bernardo Magri, Ricky Lamberty, Sebastian Faust

**An Empirical Analysis of Security and Privacy Risks in Android Cryptocurrency Wallet Apps**

I Wayan Budi Sentana, Muhammad Ikram, Mohamed Ali Kaafar

16:50-17:00

Closing remarks

Mehdi Tibouchi & XiaoFeng Wang