ICICS 2020 Program

Day1 (24 August 2020)	
08:45-09:00	Welcome
09:00-10:00	Keynote I: Aditya Mathur
10:00-10:10	Short Break
10:10-11:50	Session: Security I
11:50-13:30	Lunch Break
13:30-15:10	Session: Crypto I
15:10-15:25	Short Break
15:25-17:05	Session: Crypto II

Day2 (25 August 2020)	
09:00-10:40	Session: Security II
10:40-10:55	Short Break
10:55-11:55	Keynote II: Feng Hao
11:55-13:30	Lunch Break
13:30-15:10	Session: Crypto III
15:10-15:20	Short Break
15:20-17:00	Session: Crypto IV

Day3 (26 August 2020)	
09:00-10:15	Session: Security III
10:15-10:25	Short Break
10:25-12:05	Session: Crypto V
12:05-13:30	Lunch Break
13:30-14:20	Session: Crypto VI
14:20-14:35	Closing Remarks

Day 1 (24 August 2020)

08:45-09:00

Welcome

PC/General Chairs

09:00-10:00 (Session Chair: Dieter Gollmann, Hamburg University of Technology)

Keynote I: Protecting Your Critical Infrastructure During a Cyber War

Aditya Mathur, Singapore University of Technology and Design

10:00-10:10

Short Break

10:10-11:50

Session: Security I (Session Chair: Weizhi Meng, Technical University of Denmark)

- Machine Learning based Hardware Trojan Detection using Electromagnetic Emanation

Junko Takahashi, Keiichi Okabe, Hiroki Itoh, Xuan Thuy Ngo, Sylvain Guilley, Ritu Ranjan Shrivastwa, Mushir Ahmed and Patrick Lejoly

- A Machine Learning-Assisted Compartmentalization Scheme for Bare-Metal Systems

Dongdong Huo, Chao Liu, Xiao Wang, Mingxuan Li, Yazhe Wang, Peng Liu and Zhen Xu

- Detection of metamorphic malware packers using multilayered LSTM networks

Erik Bergenholtz, Emiliano Casalicchio, Dragos Ilie, Andrew Moss

- Profile Matching Across Online Social Networks

Anisa Halimi and Erman Ayday

11:50-13:30

Lunch Break

13:30-15:10

Session: Crypto I (Session Chair: Chunhua Su, University of Aizu)

- A Compact Digital Signature Scheme Based on the Module-LWR problem

Hiroki Okada, Atsushi Takayasu, Kazuhide Fukushima, Shinsaku Kiyomoto and Tsuyoshi Takagi

- Tree-based Ring-LWE Group Key Exchanges with Logarithmic Complexity

Hector Bjoljahn Hougaard and Atsuko Miyaji

- CoinBot: A Covert Botnet in the Cryptocurrency Network

Jie Yin, Xiang Cui, Chaoge Liu, Qixu Liu, Tao Cui and Zhi Wang

- A Symbolic Model for Systematically Analyzing TEE-based Protocols

Shiwei Xu, Yizhi Zhao, Zhengwei Ren, Lingjuan Wu, Yan Tong and Huanguo Zhang

15:10-15:25

Short Break

15:25-17:05

Session: Crypto II (Session Chair: Man Ho Au, The University of Hong Kong)

- New Practical Public-Key Deniable Encryption

Yanmei Cao, Fangguo Zhang, Chongzhi Gao and Xiaofeng Chen

- A Blockchain Traceable Scheme with Oversight Function

Tianjun Ma, Haixia Xu and Peili Li

- Blind Functional Encryption

Adel Hamdi, Sébastien Canard and Fabien Laguillaumie

- Lattice HIBE with Faster Trapdoor Delegation and Applications

Guofeng Tang and Tian Qiu

Day 2 (25 August 2020)

09:00-10:40

Session: Security II (Session Chair: Afsah Anwar, University of Central Florida)

- Attributes affecting user decision to adopt a Virtual Private Network (VPN) app

Nissy Sombatruang, Angela Sasse, Daisuke Miyamoto, Youki Kadobayashi, Michelle Baddeley and Tan Omiya

- rTLS: Lightweight TLS Session Resumption for Constrained IoT devices

Koen Tange, David Howard, Travis Shanahan, Stefano Pepe, Xenofon Fafoutis and Nicola Dragoni

- PiDicators: An Efficient Artifact to Detect various VMs

Qingjia Huang, Haiming Li, Yun He, Jianwei Tai and Xiaoqi Jia

- HCC: 100 Gbps AES-GCM Encrypted Inline DMA Transfers between SGX Enclave and FPGA Accelerator

Luis Kida, Soham Desai, Alpa Trivedi, Reshma Lal, Vincent Scarlata and Santosh Ghosh

10:40-10:55

Short Break

10:55-11:55 (Session Chair: Weizhi Meng, DTU)

Keynote II: End-to-end verifiable e-voting for real-world elections

Feng Hao, University of Warwick

11:55-13:30

Lunch Break

13:30-15:10

Session: Crypto III (Session Chair: Atsuko Miyaji, Osaka University)

- Information-Theoretic Security of Cryptographic Channels

Marc Fischlin, Felix Günther and Philipp Muth

- Client-oblivious OPRAM

Gareth T. Davies, Christian Janson and Daniel P. Martin

- The Influence of LWE/RLWE Parameters on the Stochastic Dependence of Decryption Failures

Georg Maringer, Tim Fritzmann and Johanna Sepúlveda.

- One-Time, Oblivious, and Unlinkable Query Processing over Encrypted Data On Cloud

Yifei Chen, Meng Li, Shuli Zheng, Donghui Hu, Chhagan Lal and Mauro Conti

15:10-15:20

Short Break

15:20-17:00

Session: Crypto IV (Session Chair: Meng Li, Hefei University of Technology)

- A New General Method of Searching for Cubes in Cube Attacks

Lin Ding, Lei Wang, Dawu Gu, Chenhui Jin and Guan Jie

- A Love Affair Between Bias Amplifiers and Broken Noise Sources

George Teseleanu

- Towards real-time hidden speaker recognition by means of fully homomorphic encryption

Martin Zuber, Sergiu Carpov and Renaud Sirdey

- Cryptanalysis of the Post Quantum Multivariate Signature Scheme Himq-3

Jintai Ding, Zheng Zhang, Joshua Deaton and Lihchung Wang

Day3 (26 August 2020)

09:00-10:15

Session: Security III (Session Chair: Qingni Shen, Peking University)

- Statically Dissecting Internet of Things Malware: Analysis, Characterization, and Detection

Afsah Anwar, Hisham Alasmary, Jeman Park, An Wang, Songqing Chen and David Mohaisen

- Analysis of Industrial Device Architectures for Real-Time Operations under Denial of Service Attacks

Florian Fischer, Matthias Niedermaier, Thomas Hanka, Peter Knauer and Dominik Merli

- A Variational Generative Network Based Network Threat Situation Assessment

Hongyu Yang, Renyun Zeng, Fengyan Wang, Guangquan Xu and Jiyong Zhang

10:15-10:25

Short Break

10:25-12:05

Session: Crypto V (Session Chair: Jiageng Chen, Central China Normal University)

- A Hardware in the Loop Benchmark Suite to Evaluate NIST LWC Ciphers on Microcontrollers

Sebastian Renner, Enrico Pozzobon and Jürgen Mottok

- Experimental Comparisons of Verifiable Delay Function

Zihan Yang, Bo Qin, Qianhong Wu, Wenchang Shi and Bin Liang

- Attacks on Integer-RLWE

Alessandro Budroni, Benjamin Chetioui and Ermes Franch

- A Family of Subfield Hyperelliptic Curves for Use in Cryptography

Anindya Ganguly, Abhijit Das, Dipanwita Roy Chowdhury and Deval Mehta

12:05-13:30

Lunch Break

13:30-14:20

Session: Crypto VI (Session Chair: Jinguang Han, Queen's University of Belfast)

- Leakage-Resilient Inner-Product Functional Encryption in the Bounded-Retrieval Model

Linru Zhang, Xiangning Wang, Yuechen Chen and Siu Ming Yiu

- Anonymous End to End Encryption Group Messaging Protocol Based on Asynchronous Ratchet Tree

Kaiming Chen and Jiageng Chen

14:20-14:35

Closing Remarks