CRYPTO-PPML 2019 Program

Sunday, August 18, 2019	
9:00–9:30	**A Survey** **A Survey on Deep Learning Techniques for Privacy-Preserving** Harry Chandra Tanuwidjaja, Rakyong Choi, Kwangjo Kim (speaker) *KAIST*
9:30–10:30	**Invited Talk** **Fairness in Automated Classification: A Foundational Perspective** Guy Rothblum (Weizmann Institute of Science)
10:30–11:00	**Coffee Break**
11:00–12:00	**Invited Talk** **Unwanted Machine Learning** Vitaly Shmatlikov (Cornell Tech)
12:00–12:45	**Contributed Talks** **CrptFllow: Secure Tensorflow Inference** Nishanth Chandran (speaker), Nishant Kumar, Mayank Rathee, Divya Gupta, Aseem Rastogi, Rahul Sharma *Microsoft Research, India* **CHET: An Optimizing Compiler for Fully-Homomorphic Neural-Network Inferencing** Roshan Dathathri (speaker), Olli Saarikivi, Hao Chen, Kim Laine, Kristin Lauter, Saeed Maleki, Madanlal Musuvathi, Todd Mytkowicz *University of Texas at Austin, Microsoft Research* **Foundations of Differentially Oblivious Algorithms** T-H. Hubert Chan, Kai-Min Chung, Bruce Maggs, Elaine Shi (speaker) *HKU, Academia Sinica, Duke, Cornell*
12:45–14:00	**Lunch**
14:00–15:00	**Invited Talk** **Private AI** Kristin Lauter (Microsoft Research)
15:00–15:30	**Contributed Talks** **Garbled Neural Networks are Practical** Marshall Ball (speaker), Brent Carmer, Tal Malkin, Mike Rosulek, Nichole Schimanski *Columbia University, Galois, Inc, Oregon State University* **Helen: Maliciously Secure Coopetitive Learning for Linear Models** Wenting Zheng (speaker), Raluca Ada Popa, Joseph E. Gonzalez, Ion Stoica *UC Berkeley*
15:30–16:00	**Coffee Break**
16:00–17:00	**Contributed Talks** **How to trade Efficiency and Accuracy using Fault-Tolerant Computations over the Reals** Ran Cohen (speaker), Jonathan Frankle, Shafi Goldwasser, Hayim Shaul, Vinod Vaikuntanathan *Boston University and Northeastern University, MIT, UC Berkeley, IDC Herzliya* **Secure Evaluation of Quantized Neural Networks** Anders Dalskov (speaker), Daniel Escudero, Marcel Keller *Aarhus University, Data61* **Partially Encrypted Machine Learning using Functional Encryption** Théo Ryffel, Edouard Dufour-Sans (speaker), Romain Gay, Francis Bach, David Pointcheval *ENS, INRIA, ENS, ENS, UC Berkeley, INRIA, ENS* **Improving the Adaptability of Differential Privacy** Mugunthan Vaikkunth (speaker), Wanyi Xiao, Lalana Kagal *MIT*