Machine Learning on Encrypted Data: Hardware to the Rescue

Farinaz Koushanfar,
UC San Diego,
fkoushanfar@eng.ucsd.edu

ABSTRACT

Machine Learning on encrypted data is a yet-to-be-addressed challenge. Several recent key advances across different layers of the system, from cryptography and mathematics to logic synthesis and hardware are paving the way for practical realization of privacy preserving computing for certain target applications. This talk highlights the crucial role of hardware and advances in computing architecture in supporting the recent progresses in the field. I outline the main technologies and mixed computing models. I particularly center my talk on the recent progress in synthesis of Garbled Circuits that provide a leap in scalable realization of machine learning on encrypted data. I explore how hardware could pave the way for navigating the complex space of privacy-preserving computing in general, and enabling scalable future mixed protocol solutions. I conclude by briefly discussing the challenges and opportunities moving forward.

BIOGRAPHY

Farinaz Koushanfar is a professor and Henry Booker Faculty Scholar in the Electrical and Computer Engineering (ECE) department at University of California San Diego (UCSD), where she is the founding co-director of the UCSD Center for Machine Intelligence, Computing & Security (MICS). Prof. Koushanfar received her Ph.D. in Electrical Engineering and Computer Science as well as her M.A. in Statistics from UC Berkeley. Her research addresses several aspects of efficient computing and embedded systems, with a focus on system and device security, safe AI, privacy preserving computing, as well as real-time/energy-efficient AI under resource constraints, design automation and reconfigurable computing. Professor Koushanfar has received a number of awards and honors for her research, mentorship, teaching, and outreach activities including the Presidential Early Career Award for Scientists and Engineers (PECASE) from President Obama, the ACM SIGDA Outstanding New Faculty Award, Cisco IoT Security Grand Challenge Award, Qualcomm Innovation Award(s), MIT Technology Review TR-35, Young Faculty/CAREER Awards from NSF, DARPA, ONR and ARO, as well as a number of Best Paper Awards. Dr. Koushanfar is a fellow of the IEEE, and a fellow of the Kavli Foundation Frontiers of the National Academy of Sciences.

ASHES '21, November 19, 2021, Virtual Event, Republic of Korea

ACM ISBN 978-1-4503-8662-3/21/11.
https://doi.org/10.1145/3474376.3487276