Can We Securely Outsource Big Data Analytics with Lightweight Cryptography?

Sherman S. M. Chow
sherman@ie.cuhk.edu.hk
The Chinese University of Hong Kong
Shatin, N.T., Hong Kong

ABSTRACT

Advances in cryptography such as secure multiparty computation (SMC) and fully-/somewhat-homomorphic encryption (FHE/SHE) have already provided a generic solution to the problem of processing encrypted data; however, they are still not that efficient if one directly applies them for big data analytics.

Many cryptographers have recently designed specialized privacy-preserving frameworks for neural networks. While promising, they are still not entirely satisfactory. Gazelle (Usenix Security 2018) supports inference but not training. SecureNN (PoPETS 2019), with the help of non-colluding servers, is still orders of magnitudes slower than plaintext training/inferencing.

To narrow the gap between theory and practice, we put forward a new paradigm for privacy-preserving big data analytics which leverages both trusted processor such as Intel SGX (Software Guard Extensions) and (untrusted) GPU (Graphics Processing Unit). Note that SGX is not a silver bullet in this scenario. In general, SGX is subject to a memory constraint which can be easily exceeded by a single layer of the (evergrowing) neural networks. Relying on the generic solution such as paging mechanism is, again, inefficient. GPU is an ideal platform for deep learning, yet, we do not want to assume it is trusted. We thus still need cryptographic techniques.

In this keynote, we will briefly survey the research landscape of privacy-preserving machine learning, point out the obstacles brought by seemingly slight changes of requirements (e.g., a single query from different data sources, multiple model owners, outsourcing a trained model to an untrusted cloud), and highlight a number of settings which aids in ensuring privacy without heavyweight cryptography. We will also discuss two notable recent works, Graviton (OSDI 2018) and Slalom (ICLR 2019), and our ongoing research.

CCS CONCEPTS

• **Security and privacy → Privacy-preserving protocols**; **Public key encryption**; *Management and querying of encrypted data*; • **Computing methodologies → Neural networks**;

KEYWORDS

applied cryptography; homomorphic encryption; neural networks

SCC '19, July 8, 2019, Auckland, New Zealand
© 2019 Copyright held by the owner/author(s).
ACM ISBN 978-1-4503-6788-2/19/07.
https://doi.org/10.1145/3327962.3331455

ACM Reference Format:
Sherman S. M. Chow. 2019. Can We Securely Outsource Big Data Analytics with Lightweight Cryptography?. In *The Seventh International Workshop on Security in Cloud Computing (SCC '19), July 8, 2019, Auckland, New Zealand.* ACM, New York, NY, USA, 1 page. https://doi.org/10.1145/3327962.3331455

BIO

Sherman S. M. Chow joined the Department of Information Engineering at the Chinese University of Hong Kong as an assistant professor in November 2012 and received the Early Career Award 2013/14 from the Hong Kong Research Grants Council. He was a research fellow at Department of Combinatorics and Optimization, University of Waterloo, a position he commenced after receiving his Ph.D. degree from the Courant Institute of Mathematical Sciences, New York University. During his study, he interned at NTT Research and Development (Tokyo), Microsoft Research (Redmond), and Fuji Xerox Palo Alto Laboratory.

His main interests are in Cryptography, Security, and Privacy, with publications in AsiaCrypt, CCS, EuroCrypt, ITCS, NDSS, and Usenix Security. He served on the program committee of AsiaCrypt in a consecutive of six years, and of 180+ other conferences including CCS, Crypto, ESORICS, Financial Crypt, ICDCS, Infocom, PKC, and TheWeb. He is a program co-chair of ICDM-BlockSea, CANS, AsiaCCS-SCC, ISC, and ProvSec before. He also serves on the editorial boards of IEEE Transactions on Information Forensics and Security (TIFS), IET Information Security, Intl. J. of Information Security (IJIS), J. of Information Security and Applications (JISA), SpringerBriefs on Cyber Security Systems and Networks, and EAI Endorsed Transactions on Scalable Information Systems.

He is a European Alliance for Innovation (EAI) Fellow (2019, inaugural), and named as one of the 100 Most Influential Scholars (Security and Privacy, 2018) by ArnetMiner (AMiner).

ACKNOWLEDGEMENT

S. S. M. Chow is supported in parts by the General Research Funds (CUHK 14210217 and 14209918), University Grants Committee, Hong Kong.

We would also like to thank ASM Pacific Technology Ltd, for the Bronze Award of the ASM Technology Competition 2018, given to an undergraduate final-year project under this research project.