ENCRYPTO
CRYPTOGRAPHY AND
PRIVACY ENGINEERING

Don't Eject the Impostor

Fast Three-Party Computation With a Known Cheater

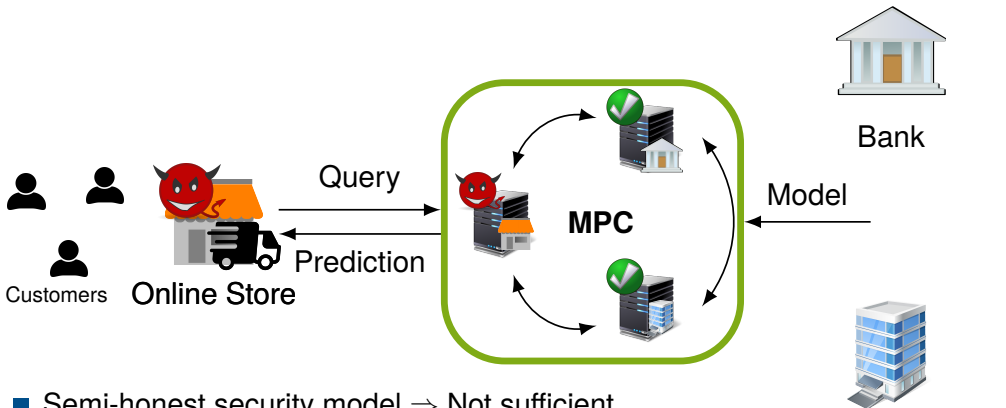
Andreas Brüggemann, Oliver Schick, Thomas Schneider, Ajith Suresh, Hossein Yalame

TECHNISCHE
UNIVERSITÄT
DARMSTADT

Contact

https://encrypto.de

Motivating Example: Credit Scoring & Fraud Detection



- Semi-honest security model ⇒ Not sufficient
- Malicious security model ⇒ Too inefficient

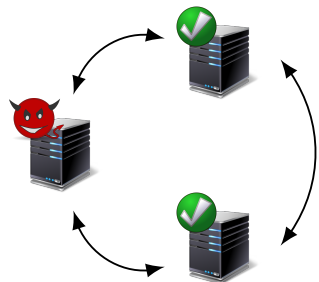
⇒ **Mixed model (this work)**

This setting is not restricted to secure inference

Trust in different people or institutions is commonly asymmetric

Contributions

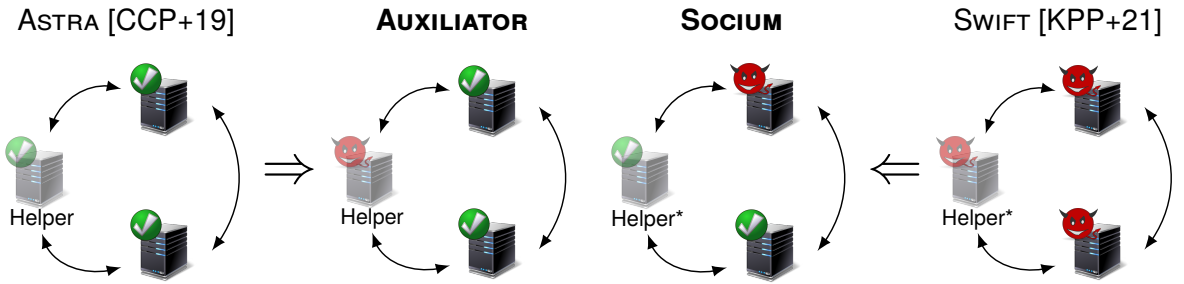
- New 3PC protocols with asymmetric trust: **Auxiliator & Socium**
- **Streamlined online** phase between two evaluators
- Multiple options for **efficient preprocessing**
- **ML-friendly**, but multi-purpose design
- **Open-source** implementation



⇒ **Bridging the gap between semi-honest and malicious model**

The World Between Astra & Swift

ENCRYPTO
CRYPTOGRAPHY AND
PRIVACY ENGINEERING



- Using *function-dependent* preprocessing, streamlined online phase
- Providing building blocks for ML (Matrix multiplication, fixed-point arithmetic, ReLU, ...)

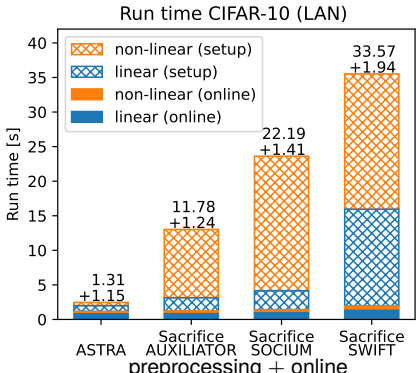
[CCP+19] H. Chaudhari, A. Choudhury, A. Patra, and A. Suresh. “ASTRA: High Throughput 3PC over Rings with Application to Secure Prediction”. *CCSW@CCS*. 2019

[KPP+21] N. Koti, M. Pancholi, A. Patra, and A. Suresh. “SWIFT: Super-fast and Robust Privacy-Preserving Machine Learning”. *USENIX Security*. 2021

Performance and Comparison

ℓ: ring size σ: statistical security parameter

Communication per Multiplication		
Verification	Sacrifice	DZKP
Preprocessing		
Astra [CCP+19]	$1 \times \mathbb{Z}_\ell$	
Auxiliator (**this work**)	$4 \times \mathbb{Z}_{\ell+\sigma}$	$1 \times \mathbb{Z}_\ell$
Socium (**this work**)	$5 \times \mathbb{Z}_{\ell+\sigma}$	$2 \times \mathbb{Z}_\ell$
Swift [KPP+21]	$9 \times \mathbb{Z}_{\ell+\sigma}$	$3 \times \mathbb{Z}_\ell$
Online		
Astra/Auxiliator	$2 \times \mathbb{Z}_\ell$	
Swift/Socium	$3 \times \mathbb{Z}_\ell$	



using the 7-layer CNN from MiniONN [LJL+17] trained on the CIFAR-10 dataset

[CCP+19] H. Chaudhari, A. Choudhury, A. Patra, and A. Suresh. "ASTRA: High Throughput 3PC over Rings with Application to Secure Prediction". *CCSW@CCS*. 2019

[KPP+21] N. Koti, M. Pancholi, A. Patra, and A. Suresh. "SWIFT: Super-fast and Robust Privacy-Preserving Machine Learning". *USENIX Security*. 2021

[LJL+17] J. Liu, M. Juuti, Y. Lu, and N. Asokan. "Oblivious Neural Network Predictions via MiniONN Transformations". *CCS*. 2017

ENCRYPTO
CRYPTOGRAPHY AND
PRIVACY ENGINEERING

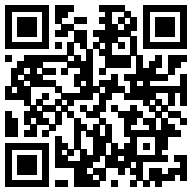
Thank You!

Questions?

Paper

https://ia.cr/2023/1744

Code



https://encrypto.de/code/MOTION-FD

Website

https://encrypto.de