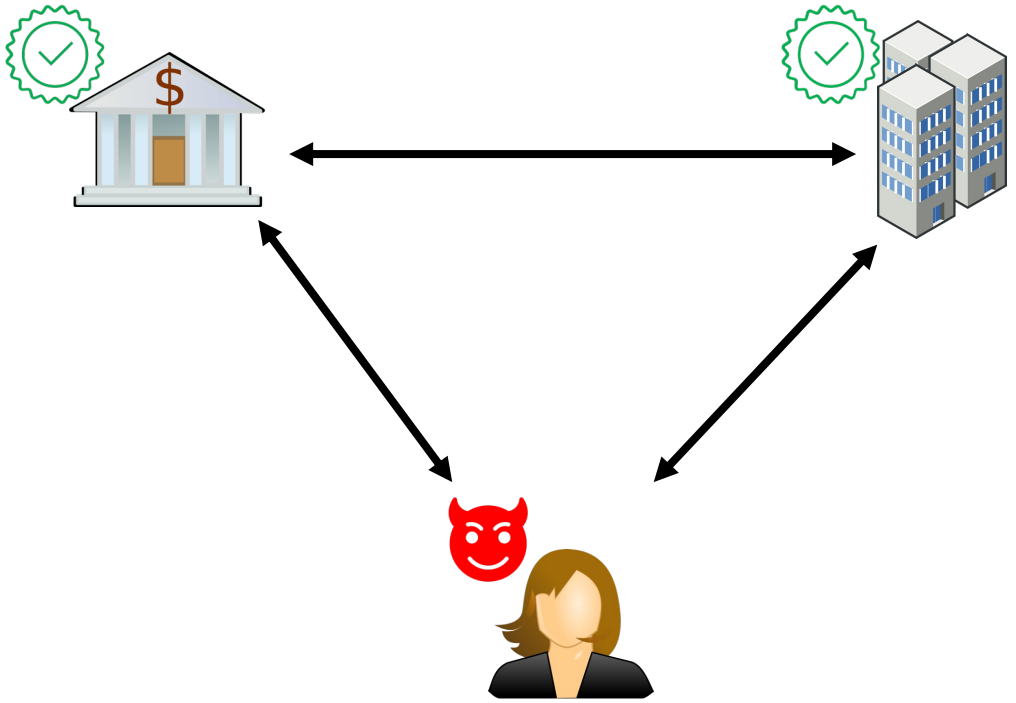
Is Everyone Equally Trustworthy in Practice?

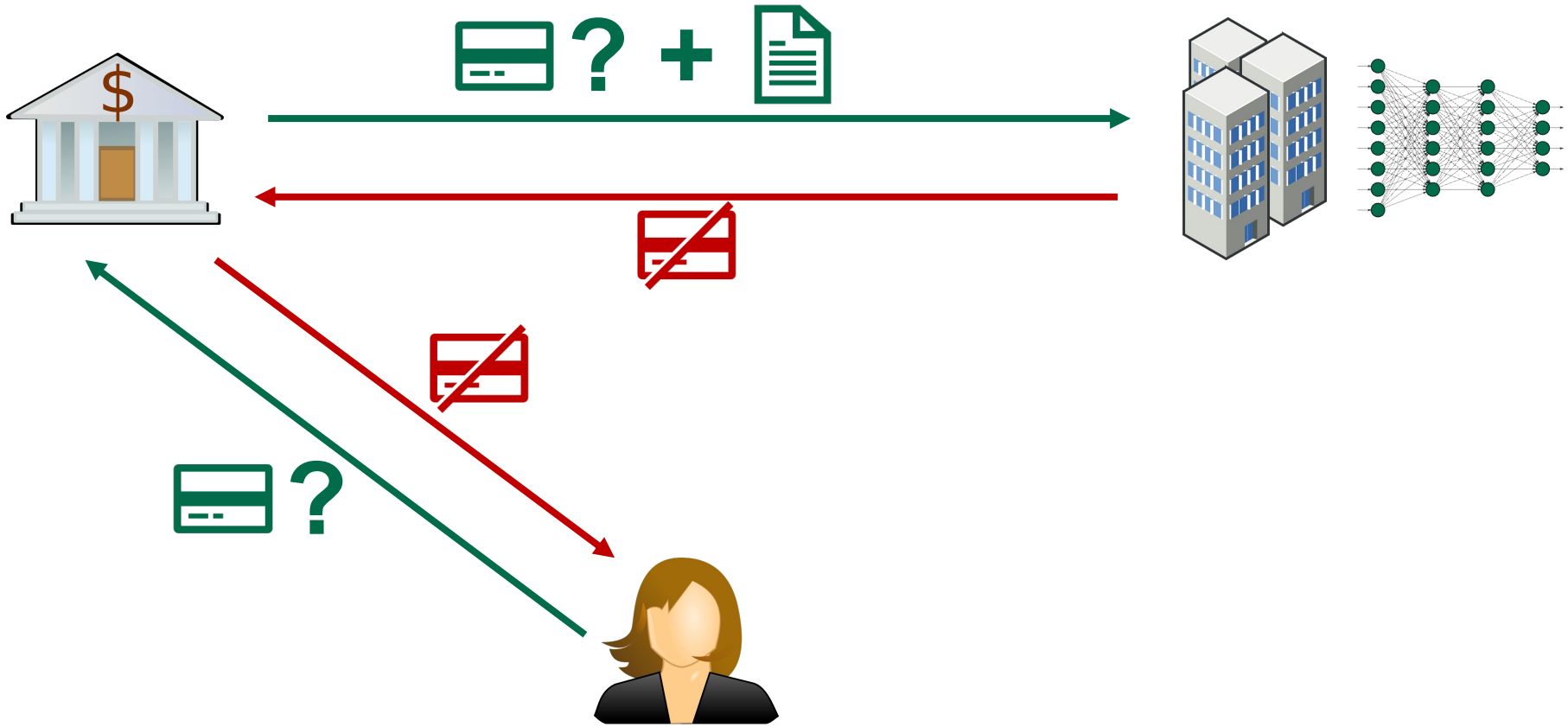
Andreas Brüggemann, Thomas Schneider, Ajith Suresh, Hossein Yalame

TECHNISCHE UNIVERSITÄT DARMSTADT

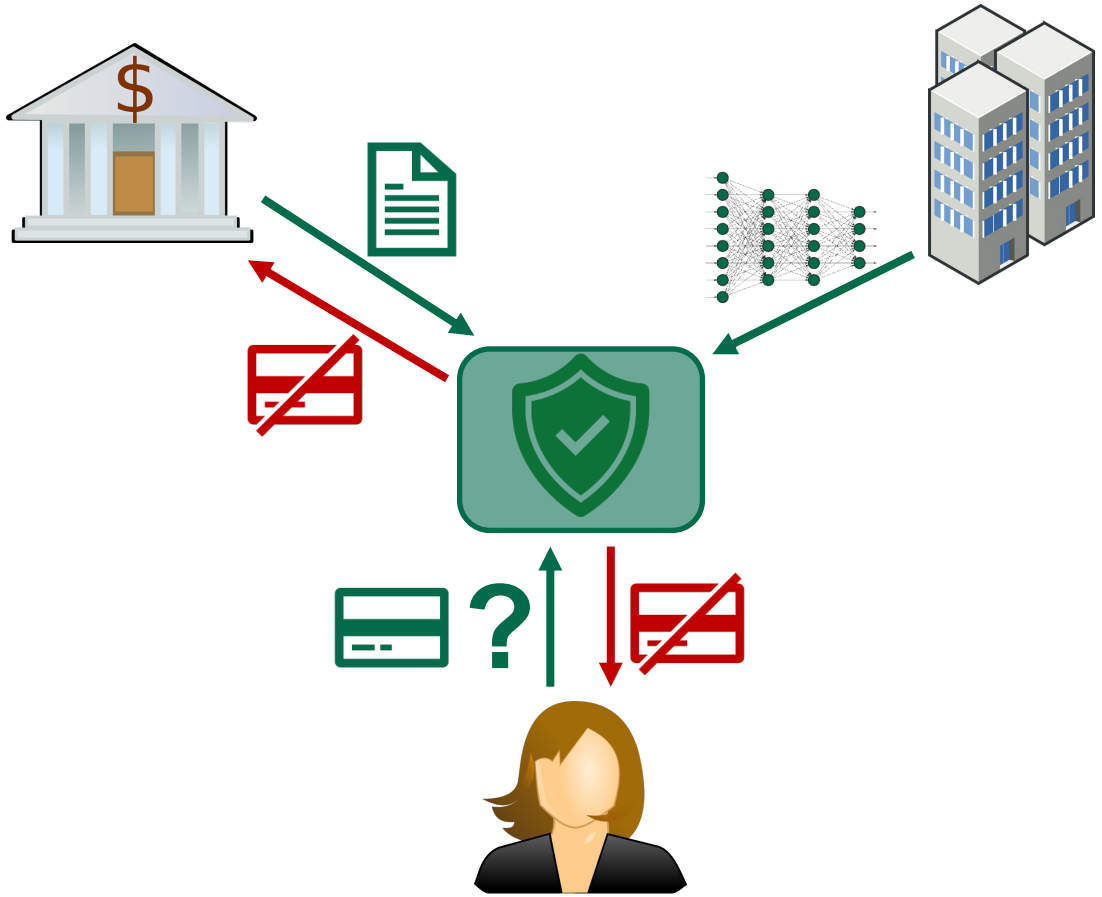
ENCRYPTO CRYPTOGRAPHY AND PRIVACY ENGINEERING



Example: Credit Scoring



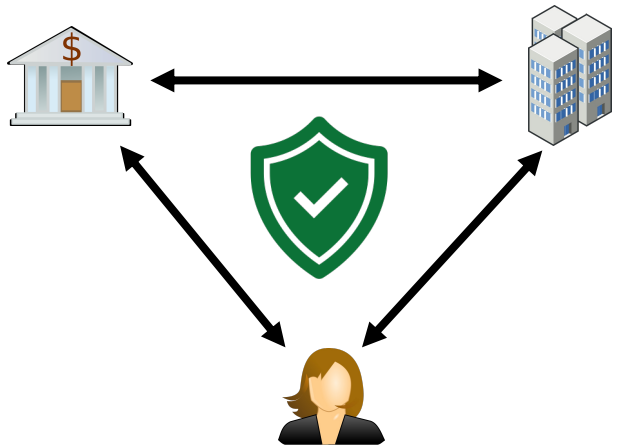
Example: Private Credit Scoring



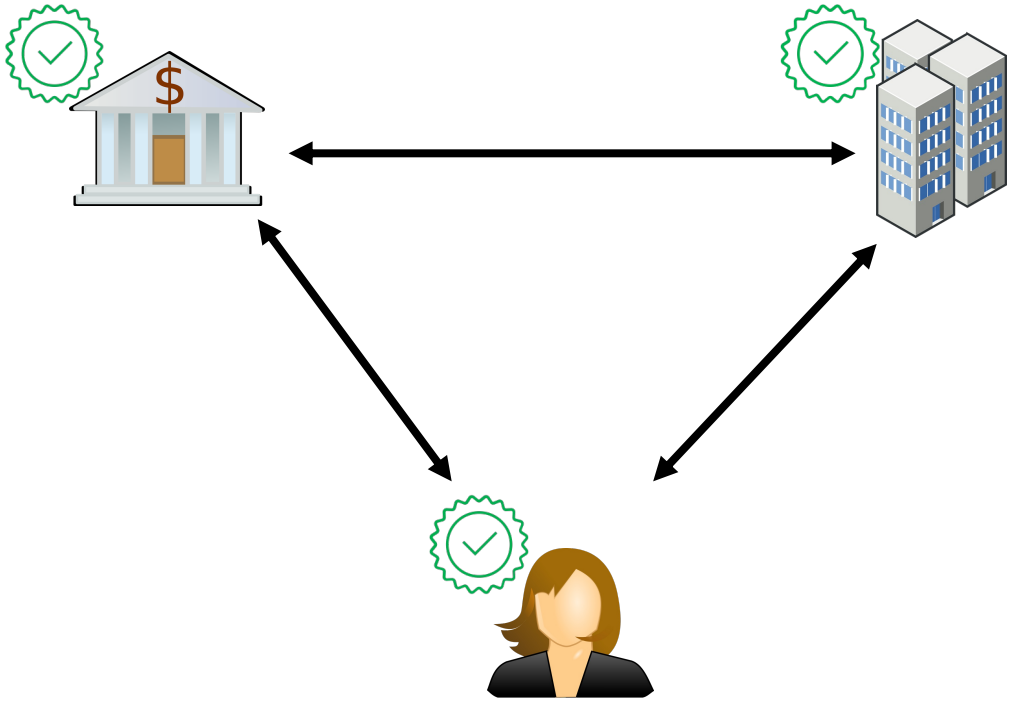
- Customer worried about sensitive data
- Bank must protect customer's privacy
- Model owner wants to protect ML model

→ **Possible solution:**

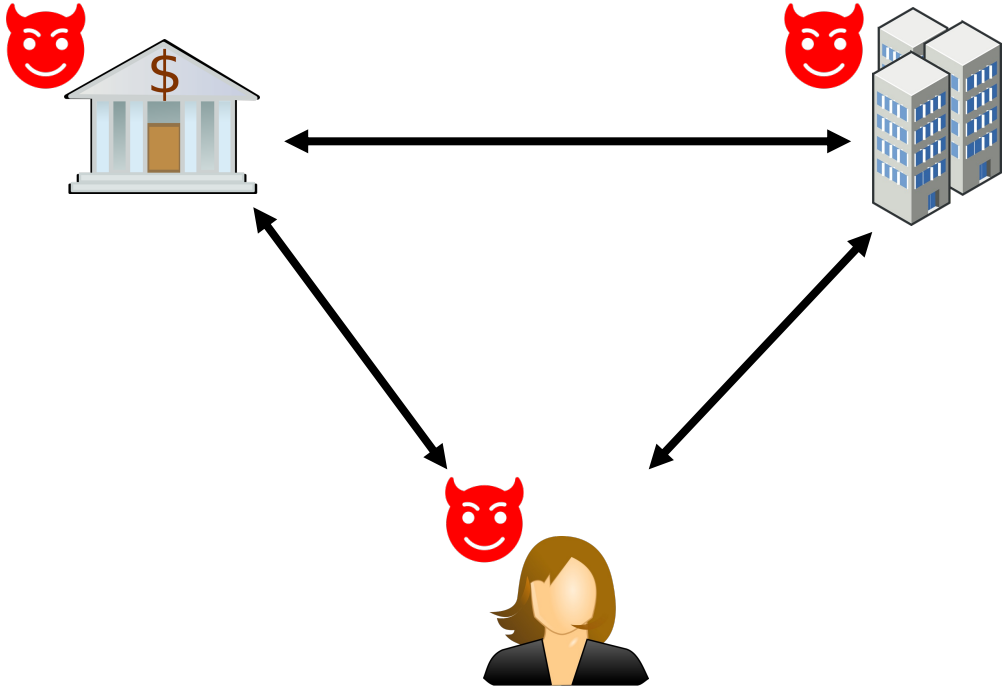
Secure multi-party computation (MPC)



Common Settings in MPC

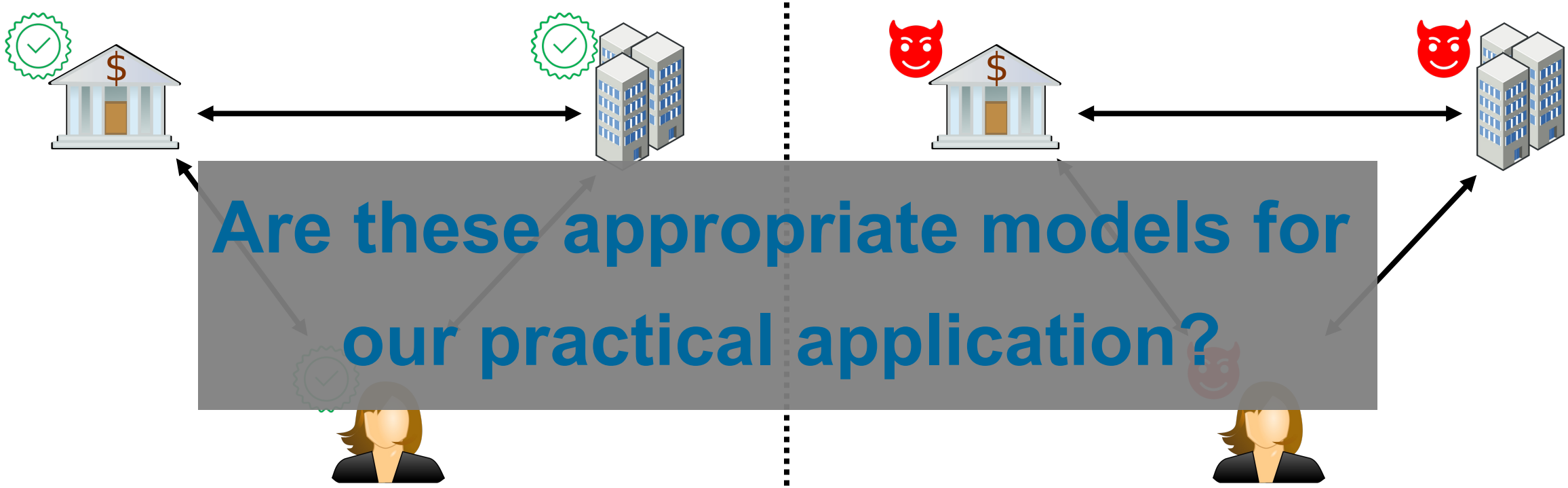


Semi-honest setting



Malicious setting

Common Settings in MPC



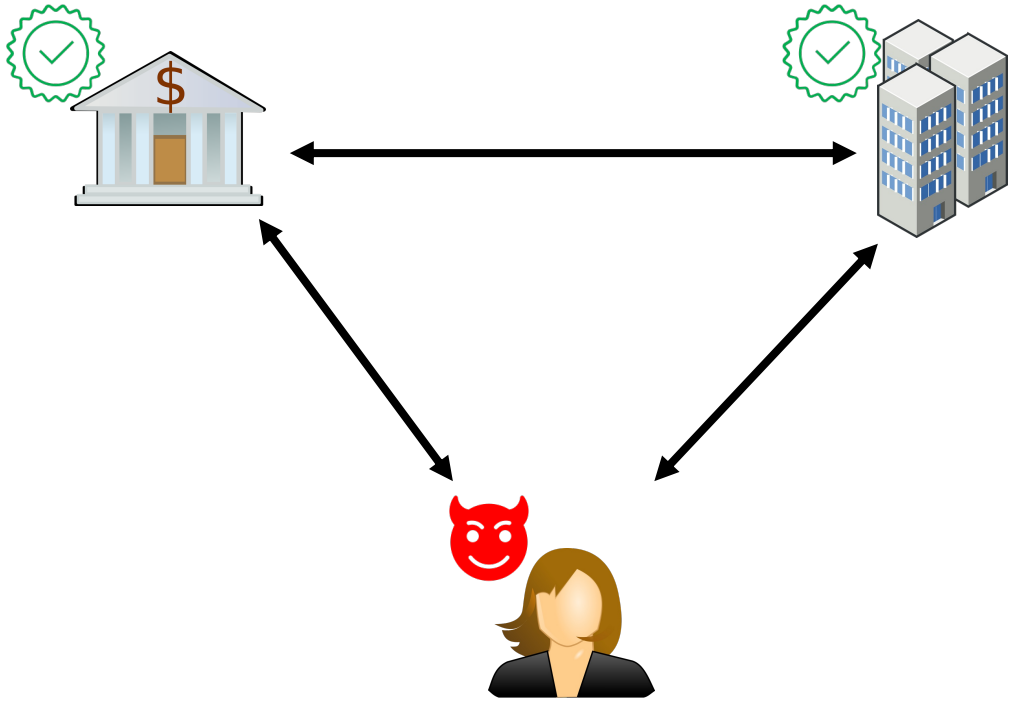
Semi-honest setting

Malicious setting

Leveraging Asymmetric Trustworthiness

- Assume: Some **fixed** parties **semi-honest**, some **fixed** parties **malicious**
- **Higher security** guarantees than **semi-honest** setting
- **Higher efficiency** than **malicious** setting

- Existing works: Most notably two-party setting, application point of view



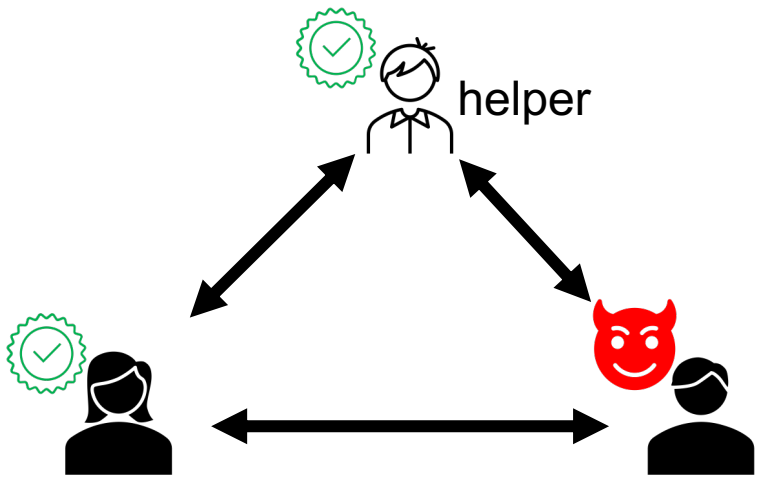
Mixed setting

R. Lehmkuhl, P. Mishra, A. Srinivasan, and R. A. Popa, “Muse: Secure Inference Resilient to Malicious Clients”, in USENIX’21.

Our Approach: Consider Three Parties

ENCRYPTO
CRYPTOGRAPHY AND PRIVACY ENGINEERING

- **3** non-colluding parties, **1 is malicious**
- Preprocessing, **fast online phase** once inputs are available
- One **helper** with low online workload, evaluators do online execution



Setting with malicious evaluator

Protocol Malicious parties	ASTRA none	SWIFT any
Offline	1	3^a
Online	2	3

Communication in globally sent ring elements / multiplication

[a] amortized

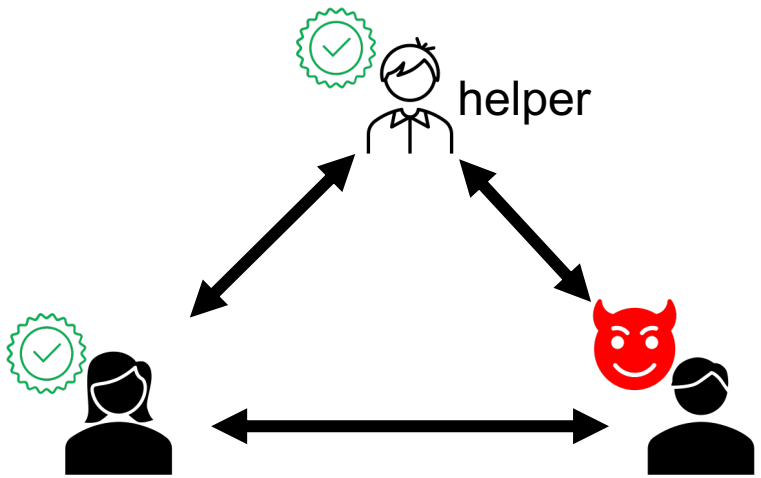
H. Chaudhari, A. Choudhury, A. Patra, and A. Suresh, “ASTRA: High Throughput 3PC over Rings with Application to Secure Prediction”, in CCSW@CCS’19.

N. Koti, M. Pancholi, A. Patra, and A. Suresh, “SWIFT: Super-fast and Robust Privacy-Preserving Machine Learning”, in USENIX’21.

Our Approach: Consider Three Parties

ENCRYPTO CRYPTOGRAPHY AND PRIVACY ENGINEERING

- **3** non-colluding parties, **1 is malicious**
- Preprocessing, **fast online phase** once inputs are available
- One **helper** with low online workload, evaluators do online execution
- We achieve **tradeoffs** between semi-honest ASTRA and malicious SWIFT!



Setting with malicious evaluator

Protocol Malicious parties	ASTRA none	Ours helper	Ours evaluator	SWIFT any
Offline	1	1^a	2^a	3^a
Online	2	2	3	3

Communication in globally sent ring elements / multiplication

^{a}amortized

H. Chaudhari, A. Choudhury, A. Patra, and A. Suresh, “ASTRA: High Throughput 3PC over Rings with Application to Secure Prediction”, in CCSW@CCS’19.

N. Koti, M. Pancholi, A. Patra, and A. Suresh, “SWIFT: Super-fast and Robust Privacy-Preserving Machine Learning”, in USENIX’21.

Thank You!

Questions?

Ideas?

brueggemann@encrypto.cs.tu-darmstadt.de