technische universität dortmund

control and cyberphysical systems

Secure MPC via Multi-Party Computation

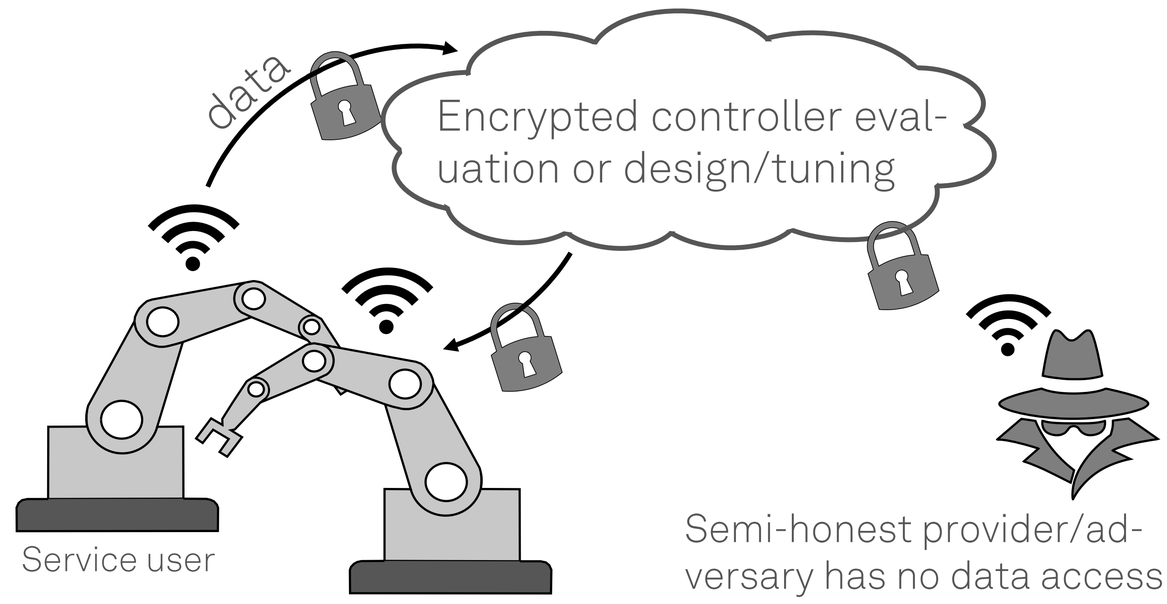
Nils Schlüter, Philipp Binfet, and Moritz Schulze Darup

Motivation

- Control services and distributed systems require computations on external platforms

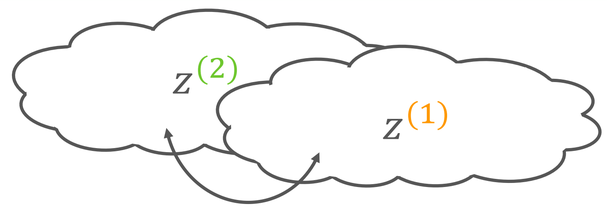
↓

- Privacy during data transmission and computations is required



Cryptosystems with Homomorphisms for Secure Computations

- Multiple parties are enabled to perform computations jointly
- Parties must be non-colluding



Additive (2,2) Secret Sharing

- Secrets $z \in \mathbb{Z}_q := \left[-\frac{q}{2}, \frac{q}{2}\right) \cap \mathbb{Z}$ with large q can be used in secret sharing
- Choose $z^{(1)} \leftarrow \mathbb{Z}_q$ and set $z^{(2)}$ such that $z = z^{(1)} + z^{(2)} \bmod q$
- Efficient protocols for add and mult exist
- Boolean functions are inefficient due to high communication effort

Garbled Circuits

- Enable Boolean functions
- Require (relatively) heavy cryptography and communication
- Cannot be reused

v	w	$y = \mathbf{AND}(v, w)$
0	0	0
1	0	0
0	1	0
1	1	1

Random labels →

v	w	y
ℓ_0^v	ℓ_0^w	ℓ_0^y
ℓ_1^v	ℓ_0^w	ℓ_0^y
ℓ_0^v	ℓ_1^w	ℓ_0^y
ℓ_1^v	ℓ_1^w	ℓ_1^y

Encryption Permutation →

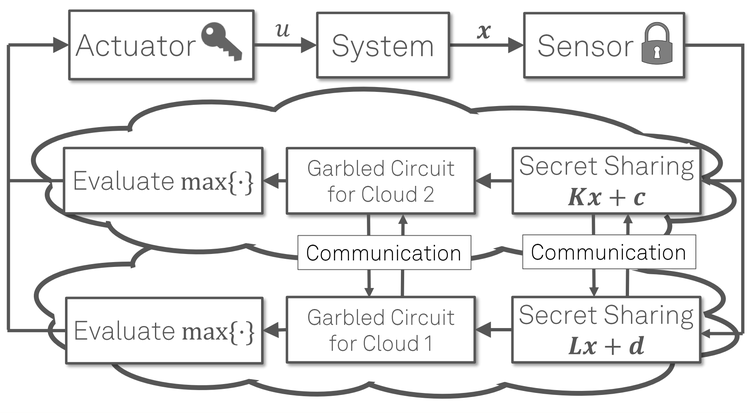
Garbled Circuit
$\mathrm{Enc}_{\{\ell_1^v, \ell_0^w\}}(\ell_1^y)$
$\mathrm{Enc}_{\{\ell_0^v, \ell_0^w\}}(\ell_0^y)$
$\mathrm{Enc}_{\{\ell_1^v, \ell_0^w\}}(\ell_0^y)$
$\mathrm{Enc}_{\{\ell_1^v, \ell_0^w\}}(\ell_0^y)$

Convex Decomposition

- Smooth control laws, e.g., explicit MPC can be decomposed into

$$u(\boldsymbol{x}) := \max\{\boldsymbol{K}\boldsymbol{x} + \boldsymbol{c}\} - \max\{\boldsymbol{L}\boldsymbol{x} + \boldsymbol{d}\}$$

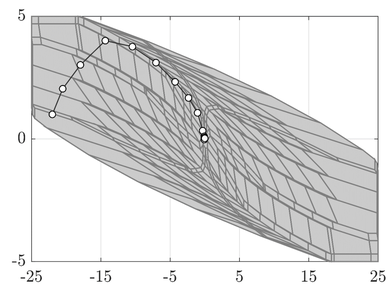
Architecture



Confidential Implementation

- In the convex decomposition we use
  - Secret sharing for (+,×)
  - Garbled circuits for $\max\{\cdot\}$
- Advantages:
  - Each technique used where most efficient
  - No rebuilding of garbled circuits necessary during evaluation of control action

p	MSE	l	t_{avg}
8	$18.57 \cdot 10^{-6}$	16	79 ms
		32	167 ms
16	$1.99 \cdot 10^{-6}$	16	170 ms
		32	348 ms



DISC Summer School 2022 (based on a contribution to the 60th IEEE Conference on Decision and Control 2021)