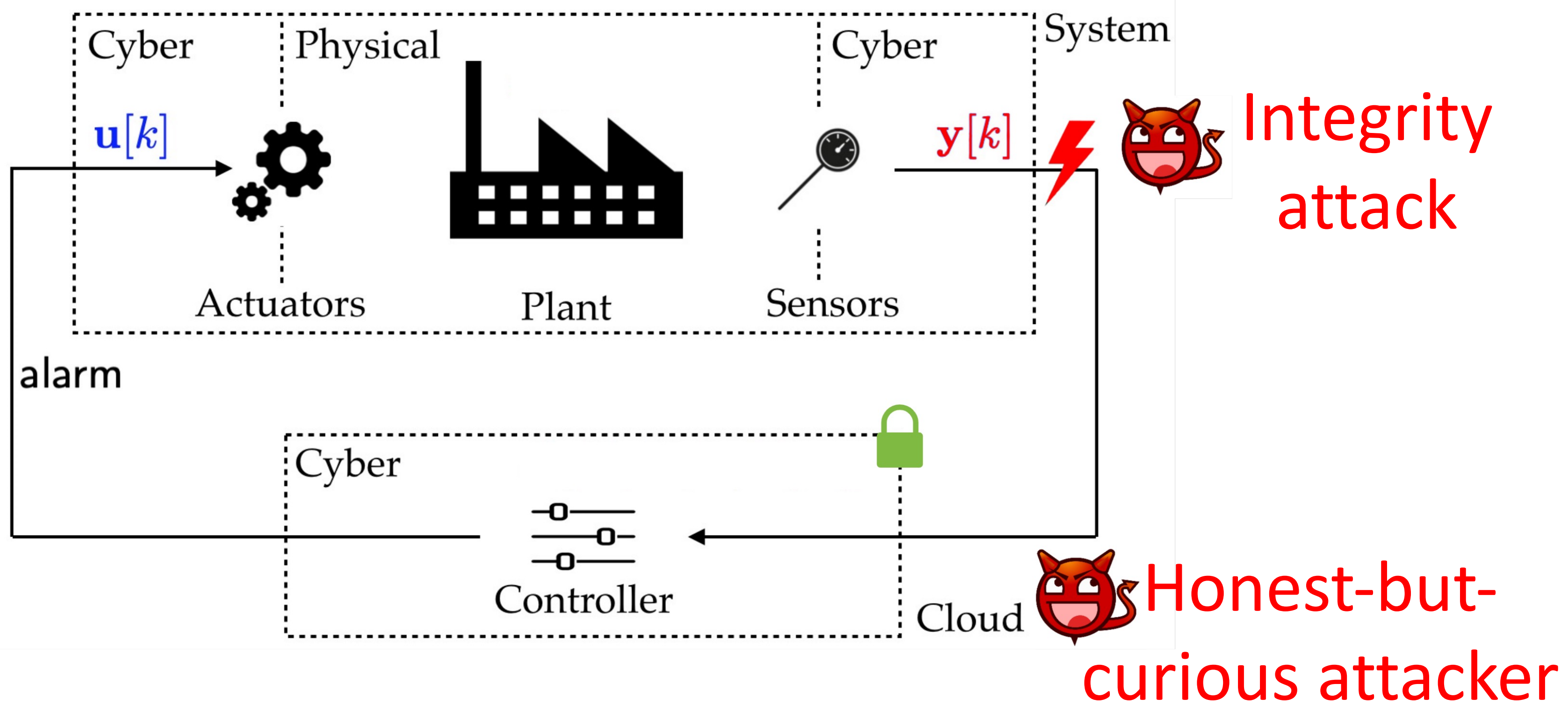
CPS: MEDIUM: COLLABORATIVE RESEARCH: SECURITY VS. PRIVACY IN CYBER-PHYSICAL SYSTEMS

PIs: Alvaro Cardenas, University of California at Santa Cruz
Murat Kantarcioglu, University of Texas at Dallas
Jonathan Katz, University of Maryland

Motivation: With time, control systems have become more interconnected, creating the possibility of outsourcing the control computation to another entity. This creates several security concerns regarding the **confidentiality** and **integrity** of the data. While previous works have dealt with confidentiality or integrity separately, we deal with both at the same time.



Challenges:

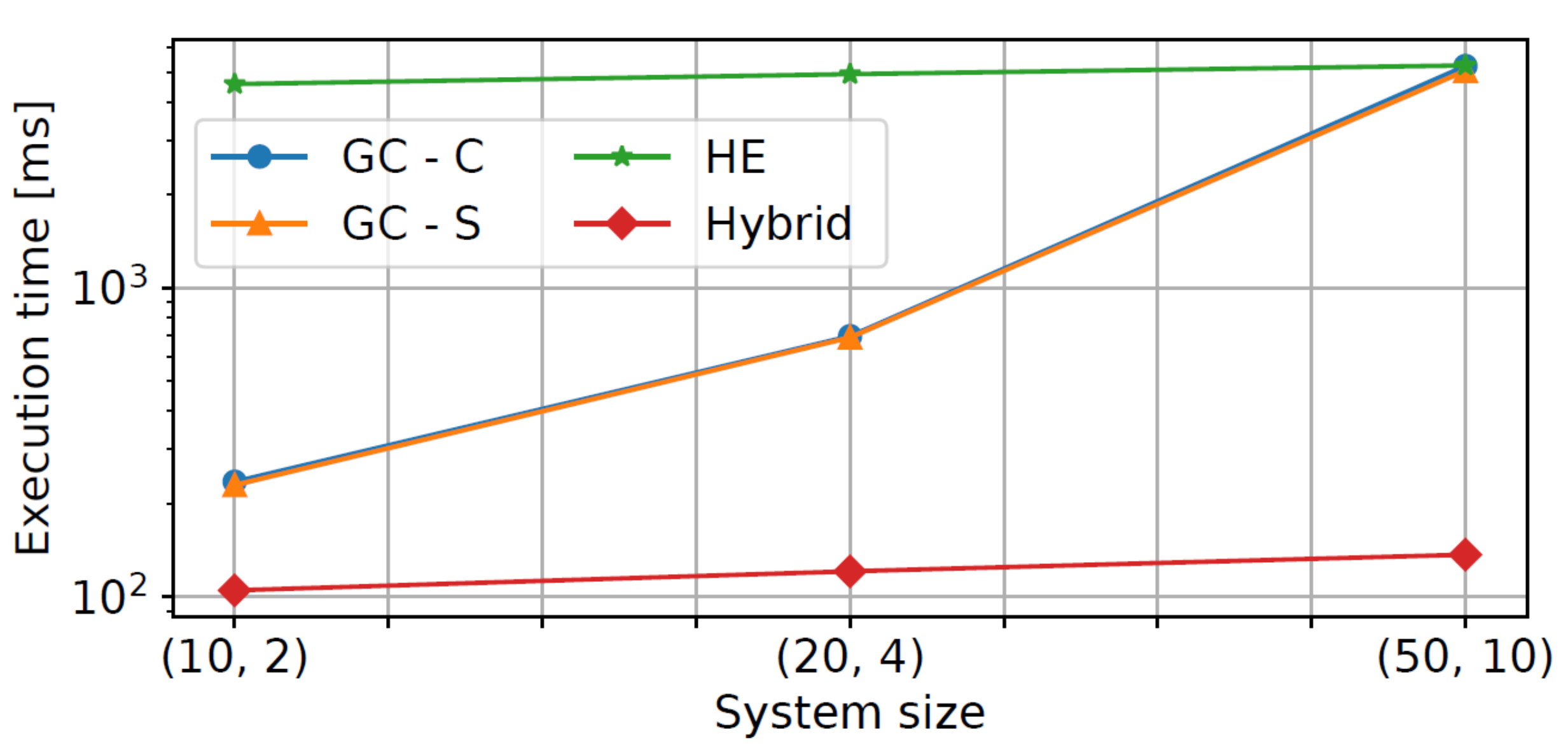
- To catch potential data injection attacks, we need anomaly detection.
- Anomaly detection requires number comparisons, which are difficult for homomorphic encryption (HE), and matrix multiplications, which are costly for garbled circuits (GC). Consequently, using only one of these approaches is inefficient.

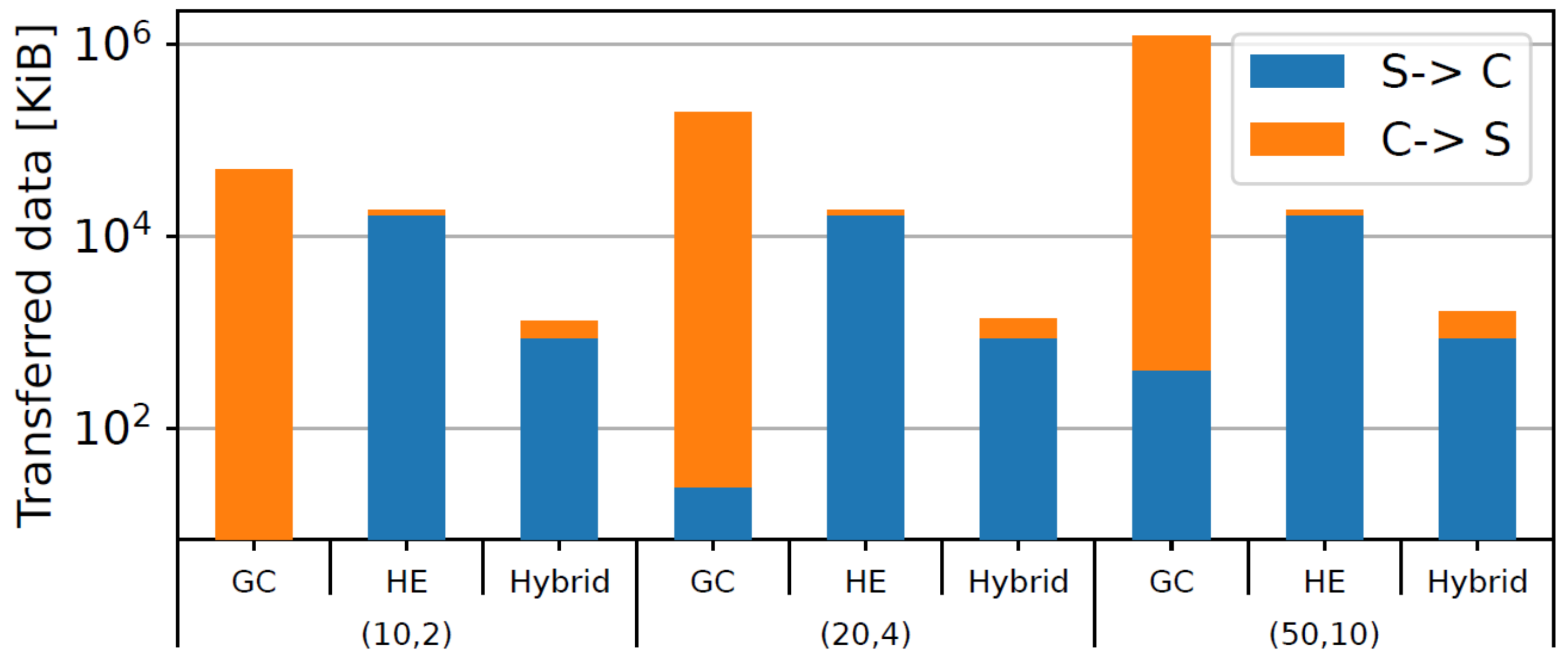
Solution:

- We propose and implement protocols for privacy-preserving anomaly detection in a linear control system using garbled circuits, homomorphic encryption, and a combination of the two.
- We show how to distribute private computations between the system and the controller to reduce the amount of computation–in particular at the low-power system.

Results:

- **Combining HE and GC for different parts of the computation is the more efficient solution.**
- The main strategies' bottleneck is the communication overhead.





(n, m) is the number of states and inputs. e.g., (10,2) is a system with 10 states and 2 inputs.

Selected Publication:

- Alexandru, Burbano, Çeliktuğ, Gomez, Cardenas**,** Kantarcioglu, Katz, *Private Anomaly Detection in Linear Controllers: Garbled Circuits vs. Homomorphic Encryption*. **CDC 2022**

Broader impacts:

- Interdisciplinary theoretical advances (security/control) to consider privacy and security in the design of cyber-physical systems.

Add Your Logo and/or project info here

Award ID#: 1929410 (UCSC)
1837517 (UMD)