



10<sup>TH</sup> ANNUAL  
HOT TOPICS *in the* **SCIENCE OF SECURITY**

April 3-5, 2023 | Virtually Hosted by THE NATIONAL SECURITY AGENCY

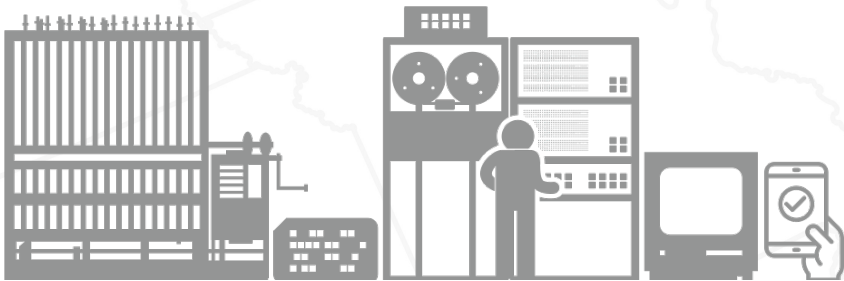
<http://hot-sos.com>

## WORKS IN PROGRESS

Certifying Safety in Reinforcement Learning  
under Adversarial Perturbation Attacks

Junlin Wu, Hussein Sibai and Yevgeniy Vorobeychik

MONDAY, APRIL 3 | 1545 - 1715



SLIDES UNAVAILABLE