Cybersecurity Research Acceleration Workshop and Showcase

October 11, 2017 | Indianapolis, IN

POOL: Scalable On-Demand Active-Secure Computation Service

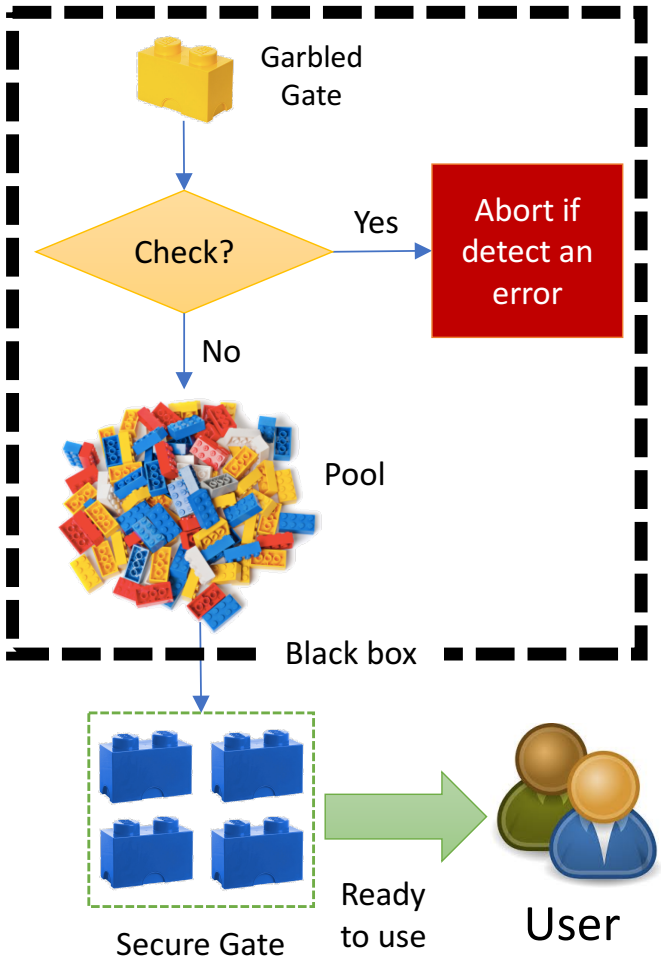
Challenge:

- Large Computation with limited memory.
- On-Demand Service with no offline cost.
- Efficient instantiation of Oblivious RAM(ORAM).
- Accessibility for non-cryptographic people.

Solution:

POOL:

- Efficient cut-and-choose scheme on unprecedented scale.
- LEGO-style protocol to handle ORAM.
- Application-independent Pool removing off-line cost.
- User-friendly API



NSF AWARD #1464113
PI: Yan Huang, Assistant Professor
Team: Ruiyu Zhu

Value proposition:

- Lifetime security guarantee after one-time setup.
- Arbitrary scale with constant memory requirement.
- Competitive efficiency close to state-of-the-art.
- ORAM compatibility.
- Accessibility with no cryptographic knowledge requirement.

Interesting Application Scenarios:

- Credit Card Companies jointly mining their sensitive data to identify fraud.
- Database owner provides private query service to the client.

Contact us

- yh33@iu.edu
- zhu52@iu.edu