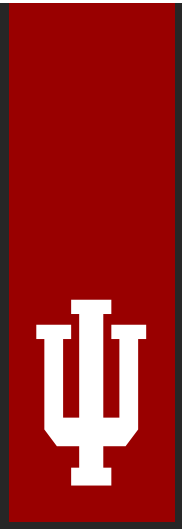
Efficient Secure Multiparty Computation of Large-Scale, Complex Protocols

RUIYU ZHU, INDIANA UNIVERSITY

Cybersecurity Research Acceleration Workshop and Showcase, Indianapolis, IN
October 11, 2017



School of Informatics, Computing and Engineering

Pool: Scalable On-Demand Secure Computation Service Against Malicious Adversaries

Ruiyu Zhu

October 12, 2017

INDIANA UNIVERSITY BLOOMINGTON

Cybersecurity Research Acceleration Workshop and Showcase

October 11, 2017 | Indianapolis, IN

POOL: Scalable On-Demand Active-Secure Computation Service

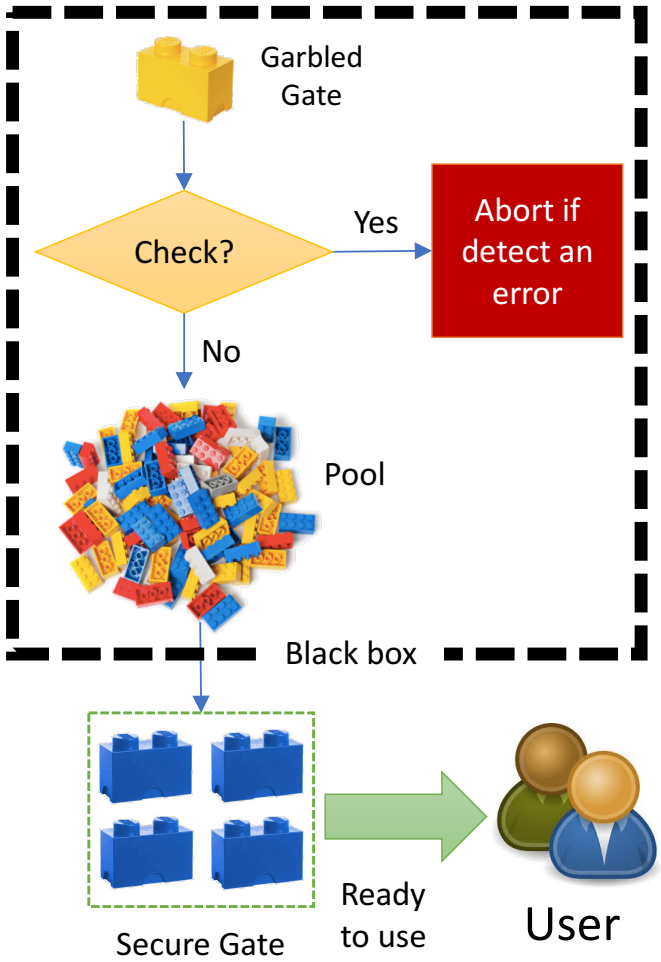
Challenge:

- 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

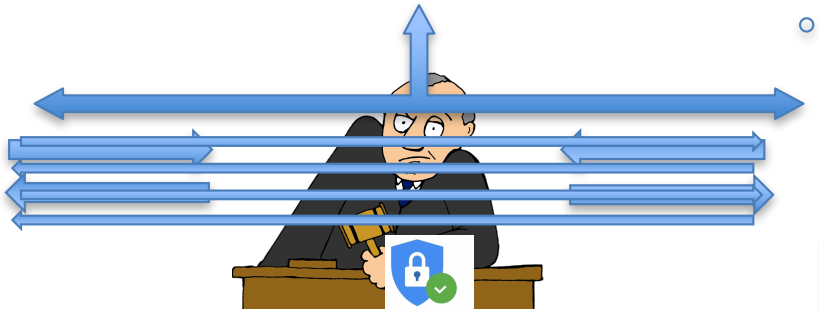
- yh33@iu.edu
- zhu52@iu.edu

Motivation

Is this a *fraudulent* transaction?

4321339 2017/10/10 Starbucks, Indianapolis IN, Apple Pay, $32.18

CHASE

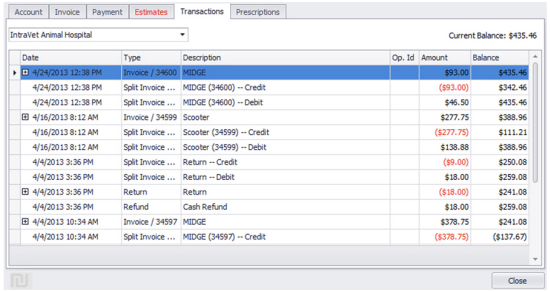


NATIONAL BANK

SPH--Transaction History

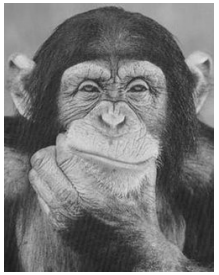
Date	Name	Activity	Shares	Price	Commission & Fee	Cost	Proceeds	Gain/Lost
10/08/10 17:24	SPH	Buy	20,000	4.060	280.20	81,480.20	-	-
30/07/10 17:49	SPH	Sell	15,000	4.130	213.77	-	61,736.23	-
22/07/10 17:50	SPH	Buy	15,000	4.000	207.04	60,207.04	-	-
21/06/10 14:15	SPH	Sell	5,000	3.890	67.12	-	19,382.88	-
18/06/10 14:12	SPH	Sell	20,000	3.880	267.78	-	77,332.22	-
11/06/10 14:11	SPH	Buy	25,000	3.730	321.78	93,571.78	-	-
Summary (Unrealized)								
			20,000	4.060	280.20	81,480.20	80,122.56	-1,357.64
Summary (Realized)								
			40,000	-	1,077.50	153,778.83	158,451.33	+4,672.50
Summary (Total)								
			60,000	-	1,357.70	235,259.03	238,573.89	+3,314.86

Secure Computation enables this!



Threat Models

Semi-honest attackers are assumed to *always follow the protocol* but try to gain extra information from observing its own execution transcripts



Full-malicious attackers are allowed to behave arbitrarily to launch an attack.

Other Applications

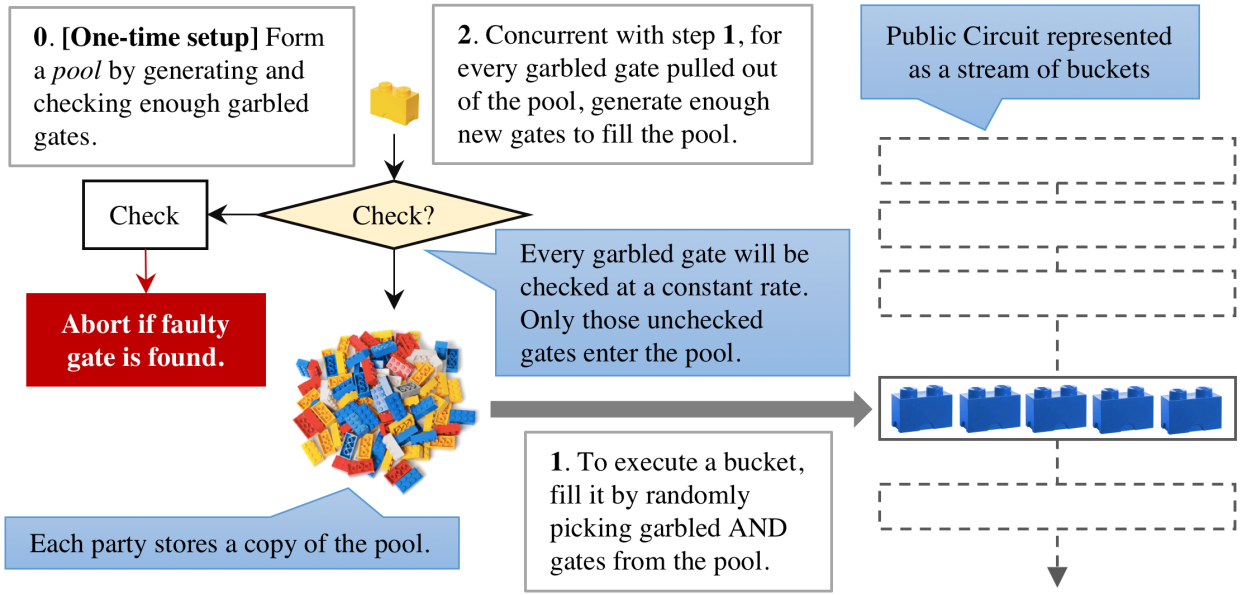
Generic Software Framework

Needed Framework Features

	KSS	WMK	JIMU NST	WRK	**POOL**
Blackbox APIs		✓			✓
Memory-efficient Scaling	✓				✓
Short Offline Delay	✓	✓			✓
Reactive Computation			✓	✓	✓
Long-term Security					✓

Full Story

[CCS'17] Pool: Scalable On-Demand Secure Computation Service Against Malicious Adversaries. Ruiyu Zhu, Yan Huang, and Darion Cassel.



Source code available at https://github.com/pool