Optimally Resilient and Adaptively Secure MPC with Low Communication Locality

Nishanth Chandran, Wutichai Chongchitmate, Juan A. Garay, Shafi Goldwasser, Rafail Ostrovsky and Vassilis Zikas

August 19, 2014
CRYPTO 2014: Rump Session

https://eprint.iacr.org/2014/615


Yeah!
Yeah!
No!
Let's change the peer-review system
Let's decide by MPC
But we are too many!!!
No!
Eurocrypt 2009
hgi
Eurocrypt Cologne 2009

Overview

Starting point: [Boyle, Goldwasser, and Tessaro, TCC 2013]

MPC for n (many many many) parties with low *communication locality*

- total number of point-to-point channels each party uses polylog(n)
- round complexity polylog(n)

Assumptions

- PKI and CRS
- static adversary
- $t < (\frac{1}{3} - \epsilon)n$

Overview

Starting point: [Boyle, Goldwasser, and Tessaro, TCC 2013]

MPC for n (many many many) parties with low *communication locality*

- total number of point-to-point channels each party uses polylog(n)
- round complexity polylog(n)

Assumptions

- PKI and CRS
- static adversary
- $t < (\frac{1}{3} - \epsilon)n$

Question 1

Can we get *optimal* resiliency $t < \frac{n}{2}$?

Question 2

Can we tolerate adaptive adversary?

This work

Yes to both!

Question 1

Can we get *optimal* resiliency $t < \frac{n}{2}$?

Question 2

Can we tolerate adaptive adversary?

This work

Yes to both!

Our Results (1/2)

MPC for n parties

[BGT 2013]	Our Work
polylog(n) locality and rounds	*polylog*(n) locality and rounds
PKI & CRS	PKI & SKI*
$t < (\frac{1}{3} - \epsilon)n$	$t < \frac{1}{2}n$ **
static adversary	adaptive adversary

* SKI = Symmetric Key Infrastructure

** optimal even in a fully connected communication

The core idea

- We encode the communication patterns into the SKI:
  - Every party uses his symmetry keys to decide his set of neighbors
- Using expander-graph machinery, we show that it is infeasible *even* for an adaptive adversary to discover these patterns and disconnect two honest parties.

Full version: https://eprint.iacr.org/2014/615