How to Synchronize Efficiently

Nathan Keller
Bar Ilan University

Joint work with Itai Dinur and Ohad Klein
Homomorphic Secret Sharing

- Introduced by Boyle, Gilboa and Ishai [BGI] (CRYPTO’16) as a (practical) alternative to FHE

- HSS allows homomorphic evaluation of a function to be distributed among two parties who do not interact with each other

- BGI constructed a group based HSS scheme
  - For functions $f$ described by a branching program
Homomorphic Secret Sharing –cont.

• Received **Best Paper Award** at CRYPTO’16

• Follow-up works: Eurocrypt’17, ACM-CCS’17, ProvSec 17, ITCS’18

• Applications:
  • Private information retrieval (PIR) construction
  • Secure MPC with minimal interaction
  • Secure data access
  • Correlated randomness generation
A main open problem in HSS

• Scheme based on share conversion procedure which may err

• Mathematical formulation of main problem (in generic group model):

We are given \( n \) random numbers arranged in a line. Two parties start in two adjacent places, but don’t know which one is the first. Each party can query at most \( T \) numbers.

The goal of the players is to synchronize: choose the same number without any communication.

• Question: What is the minimal error probability (as a function of \( T \))?
[BGI16] Solution

- Each party queries $T$ consecutive points and chooses minimum
- Assume $T=5$

A

15 77 11 104 68 39 94 53 33

B

15 77 11 104 68 39 94 53 33
Error occurs if minimum is on the edge
Error probability about $1/T$
[BGI16] Solution

- [BGI16] Error rate of $O(1/T)$
- Subsequent papers: No asymptotic improvement
Our results

• **An algorithm** which achieves $O(1/T^2)$ error rate

• **A matching lower bound** (in cryptographic groups): Result is optimal, unless DLOG in a short interval $I$ can be solved faster than in $O(\sqrt{|I|})$ operations.
  • Currently not possible for standard cryptographic groups

• **Our techniques:**
  • Random walks (complex variants of Pollard’s Kangaroo method)
  • Martingales (algorithm analysis)
  • Discrete Fourier Analysis (lower bounds)
Applications

• **Asymptotic improvement** of computational complexity of the BGI HSS scheme
  • Relevant to applications such as PIR
• Non-cryptographic applications (work in progress with Boyle, Gilboa and Ishai)
  • String algorithms
  • Boolean functions

• **Full paper**: to appear at CRYPTO’18.
Thanks for listening!