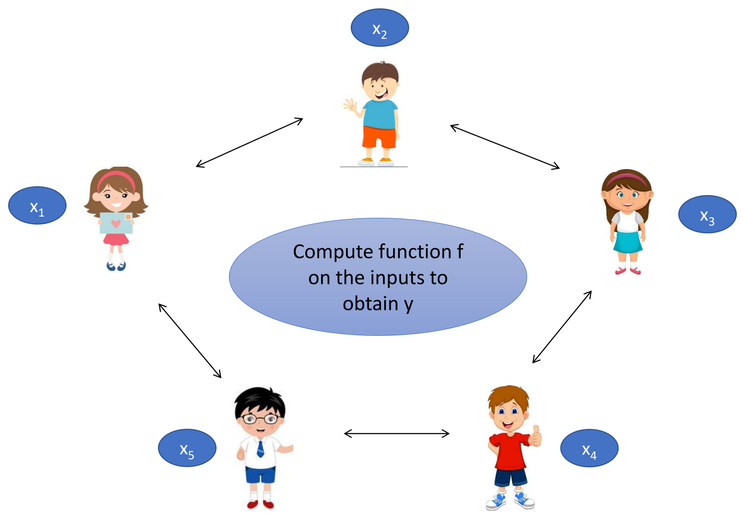
On the Exact Round Complexity of Best-of-Both-Worlds MPC

Arpita Patra, Divya Ravi, ***Swati Singla***
Indian Institute Of Science, Bangalore

Secure Multi Party Computation



Setup:
- n parties $P_1,P_2,\ldots,P_n$
- t corrupted by centralized adversary
- P_i has private input x_i
- A common n-input function $f(x_1,x_2,\ldots,x_n)$

Goals:
- ✓ Correctness $y = f(x_1,x_2,\ldots,x_n)$
- ✓ Privacy: Nothing more than the function output should be revealed.

Setting	Corruption Threshold	Bound
Honest Majority	t	t < n/2
Dishonest Majority	s	s < n

Security Notions

Guaranteed Output Delivery (GOD):
Strongest
Adversary cannot prevent honest parties from getting the output.

Fairness (fair):
Either all get the output, or no one gets the output i.e. the adversary cannot prevent the honest parties from getting the output

Unanimous Abort (UA):
Either all honest parties get the output or no one does (may be unfair).

The result of Cleve [1] proves that the stronger security notions of fairness and guaranteed output delivery can be realised only when the majority of the involved population is honest.

Existing bounds on rounds				
Bound	**Security**	**No Setup**	**Weak Setup**	**Strong Setup**
t < n/2	GOD/fair	3	3	2
s < n	UA	4	2	2

The most worrisome shortcoming of the generic protocols is: a protocol in one setting completely breaks down in the other setting i.e. the security promises are very rigid and specific to the setting. For example, a protocol for honest majority might no longer even be **private** or **correct** if half (or more) of the parties are corrupted. A protocol that guarantees security with unanimous abort for arbitrary corruptions cannot pull off the stronger security of GOD or fairness even if only a **single** party is corrupt.

Motivation

The idea of attaining the best feasible security guarantee in the respective settings of honest and dishonest majority in a single protocol is termed as **Best of Both Worlds (BoBW)** [2, 3]**.** An ideal BoBW MPC should promise the best possible security in each corruption scenario for any population of size n, as long as t < n/2 and s < n.

BoBW is impossible to achieve in expected polynomial time as long as $t + s \geq n$

This work settles the exact round complexity of two classes of Best of Both Worlds protocols in three different kinds of setups i.e. We provide lower bound proofs for the minimum number of rounds required to attain the respective security guarantees and matching upper bounds too in the form of a protocol which proves the optimality of the rounds.

GOD in Honest Majority				
Bound	**Security**	**No Setup**	**Weak Setup**	**Strong Setup**
t < n/2; t+s < n	GOD/UA	5*	3	2

*5 is sufficient, might not be necessary. Known lower bound = 4

A number of meaningful relaxations were proposed to get around the impossibility. In [4], the best possible security of guaranteed output delivery is compromised to the second-best notion of fairness in the honest-majority setting. This is one of the most elegant and meaningful relaxations that brings back the true essence of BoBW protocols with no constraint on n, apart from the natural bounds of t < n/2 and s < n.

Fair in Honest Majority				
Bound	**Security**	**No Setup**	**Weak Setup**	**Strong Setup**
t < n/2; s < n	Fair/UA	3	3	2

Contact

Swati Singla
CSA Department
Indian Institute Of Science, Bangalore
Email : swatis@iisc.ac.in
Phone : +919980580549

References

[1] R. Cleve, Limits on the security of coin ips when half the processors are faulty (extended abstract)," in ACM STOC, 1986
[2] Y. Ishai, E. Kushilevitz, Y. Lindell, and E. Petrank, On combining privacy with guaranteed output delivery in secure multiparty computation," in CRYPTO, 2006.
[3] J. Katz, On achieving the "best of both worlds" in secure multiparty computation," in STOC, 2007.
[4] C. Lucas, D. Raub, and U. M. Maurer, \Hybrid-secure MPC: trading information- theoretic robustness for computational privacy," in PODC, 2010.