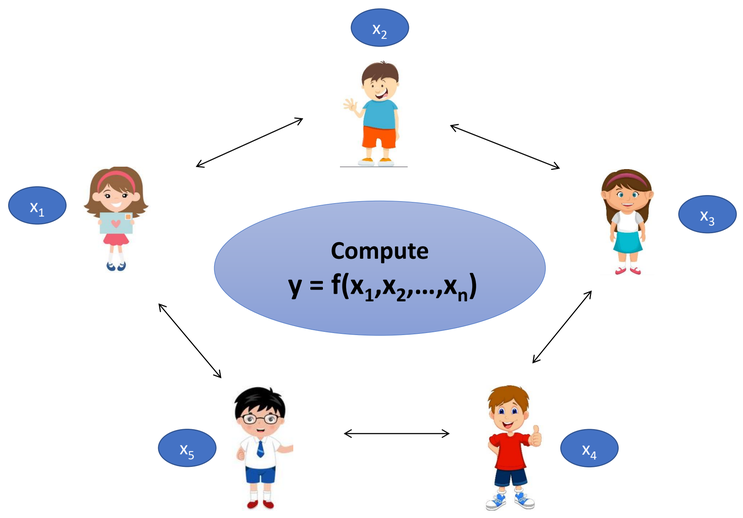
Fast Actively Secure Five Party Computation with Security Beyond Abort

***Megha Byali**, Carmit Hazay, Arpita Patra, Swati Singla*
Indian Institute Of Science, Bangalore

Secure Multi Party Computation



Goals:

✓ **Correctness:** $y = f(x_1,x_2,\ldots,x_n)$.

✓ **Privacy:** Nothing beyond the function output must be revealed.

Setup:

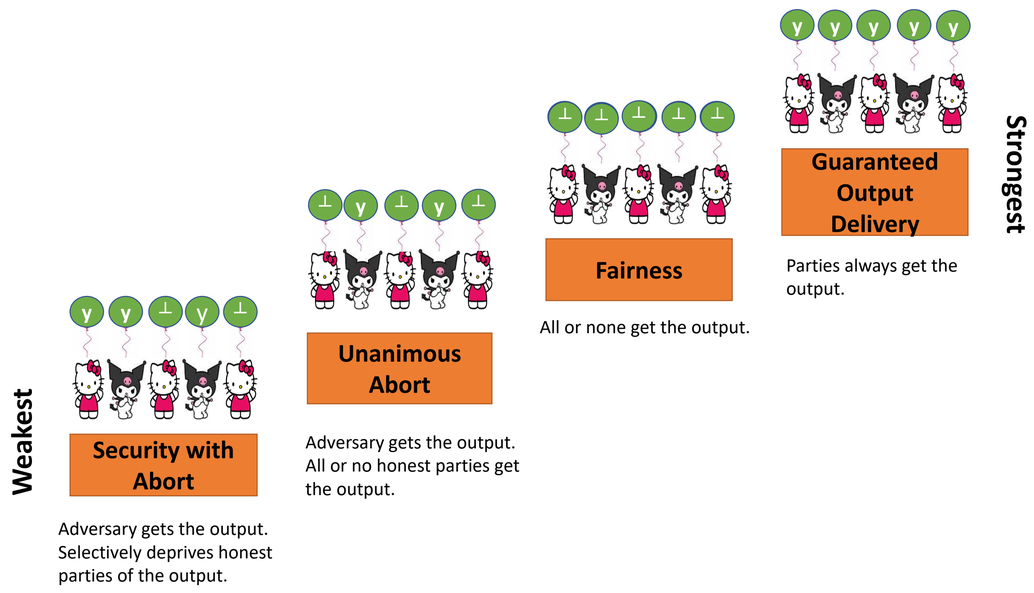
- *n* parties $P_1,P_2,\ldots,P_n$ *t* of which are controlled by a centralized adversary.
- Each P_i has private input x_i.

Our Setting

Malicious Adversary: Arbitrarily deviates from the protocol.

Corruption Threshold: *t<n/2* (*Honest Majority*)

Security Notions



Why Small Population?

- **Real world applications:** Secure ML, Danish Sugar Beet Auction, Fair Auctions.
- **Weaker Assumptions:** Eliminate expensive public key primitives as symmetric-key functions are sufficient.
- **Stronger Security:** The properties, fairness and guaranteed output delivery can be achieved only in the case of honest majority [Cleve86].
- **Light Weight Tools and Efficiency:**
  - Customized Secret Sharing schemes.
  - Elimination of Cut-n-Choose.
  - Customized Oblivious Transfer using symmetric key.

Our Results and Comparison

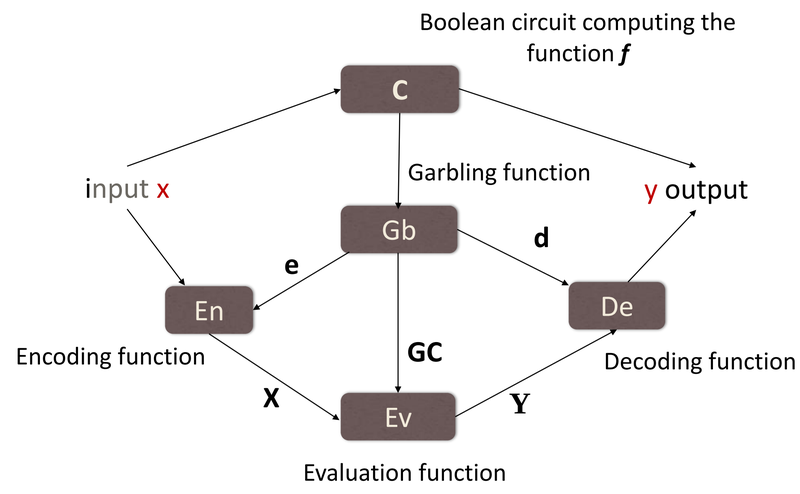
Reference	Security	Rounds	Broadcast
[ChandranGMV17]	Selective Abort	8	✗
This Paper	Unanimous Abort	8	✗
This Paper	Fairness	8	✗
This Paper	GOD	6 (Best case) 12 (Worst case)	✓ [CohenHOR16]

Assumptions

- One Way Permutations.
- Minimalistic network of point-to-point channels.
- Necessary Broadcast for guaranteed output delivery [CohenHOR16].

Our protocols guarantee stronger security notions and are highly efficient and suitable for low latency networks such as the **internet**.

Primitive: Garbled Circuit [BellareHR12]



Guarantees :

Privacy: **(GC, X, d)** leaks nothing beyond ***f*** **(x)**.
Authenticity: Given **(GC, X)** , cannot forge **Y ≠ Ev(GC,X)** that will be deemed authentic.
Obliviousness: **(GC, X)** leaks nothing about ***f*** or x.

Empirical Comparison

Protocol 5PC	LAN (ms)		WAN (s)		Communication (MB)	
	AES-128	SHA-256	AES-128	SHA-256	AES-128	SHA-256
[CGMV17]	25.01	290.38	2.54	4.78	29.55	510.26
Unanimous Abort	25.66	293.25	2.74	4.79	29.71	510.35
Fair	26.06	301.33	2.82	4.81	29.75	510.39
Guaranteed Output Delivery	26.03 (+2.62)	317.35 (+16.25)	--	--	29.67 (+0.31)	510.3 (+6.15)

Contact

Megha Byali
CSA Department
Indian Institute Of Science, Bangalore
Email : megha@iisc.ac.in
Phone : +918867036910

References

[Cleve86] R. Cleve, Limits on the security of coin ips when half the processors are faulty (extended abstract)," in ACM STOC, 1986
[ChandranGMV17] Nishanth Chandran, Juan Garay, Payman Mohassel and Satyanarayana Vusirikala. Efficient, Constant-Round and Actively Secure MPC: Beyond the Three-Party Case. In CCS 2017.
[CohenHOR16] Ran Cohen, Iftach Haitner, Eran Omri, and Lior Rotem. Characterization of Secure Multiparty Computation Without Broadcast. In TCC. 2016.
[BellareHR12] Mihir Bellare, Viet Tung Hoang, and Phillip Rogaway. Foundations of garbled circuits. In CCS, 2012.