Secure Multiparty Computation (MPC)

Arpita Patra
Department of Computer Science & Automation, Indian Institute of Science

Performance Record

Research Conducted: Multiparty Computation (MPC), Byzantine Agreement (BA), Public Key Encryption (PKC).

Publications: **3** International Journals and **5** International conferences

New Areas Undertaken: Circuit Garbling Schemes, Oblivious Transfer Extensions, Hybrid Secure Computation, Non-interactive Secure Computation, Efficient Zero-knowledge protocols.

Students Guided: 1 PhD (ongoing), 4 M. Tech Research (ongoing), 4 M. Tech

Grant Proposals:

- Grant application with title "Secure Multi-party Computation: Feasibility and Efficiency" is made for SERB Women Excellence Award.

- Grant application titled "Information Security Research and Development" funded by Department of Electronics & Information Technology (DeitY) for a period of five years starting from 2015. Jointly with four colleagues.

Teaching and Talks: Courses on Cryptography and Secure Computation offered at IISc. Several talks delivered at Workshops on Introductory Cryptography and Advanced Cryptography organized at IISc.

Research Facilities: Cryptography and Information Security (CrIS) Lab at CSA, IISc.

Publications (2015-2016)

1. Carmit Hazay and **Arpita Patra**. Efficient One-Sided Adaptively Secure Computation. **Journal of Cryptology**, vol. 30, no. 1, pp. 321–371, 2017.
2. Ashish Choudhury and **Arpita Patra**. An Efficient Framework for Unconditionally Secure Multiparty Computation. **IEEE Transactions on Information Theory**, vol. 63, no. 1, pp. 428–468, 2017.
3. **Arpita Patra**, Ashish Choudhury and C. Pandu Rangan. Efficient Asynchronous Verifiable Secret Sharing and Multiparty Computation. **Journal of Cryptology**, vol. 28, no. 1, pp. 49–109, 2015.
4. Chaya Ganesh and **Arpita Patra**. Broadcast Extensions with Optimal Communication and Round Complexity. **PODC 2016**, pp. 371–380, ACM Press, 2016.
5. Ashish Choudhury, Emmanuela Orsini, **Arpita Patra** and Nigel P. Smart. Linear Overhead Optimally-Resilient Robust MPC Using Preprocessing. **SCN 2016**, LNCS 9841, pp 147–168, Springer, 2016.
6. Carmit Hazay, **Arpita Patra** and Bogdan Warinschi. Selective Opening Security Revisited. **ASIACRYPT 2015**, LNCS 9452, pp. 443–469, 2015.
7. Carmit Hazay, Yehuda Lindell and **Arpita Patra**. Adaptively Secure Computation with Partial Erasures. **PODC 2015**, pp. 291–300, ACM Press, 2015.
8. Ashish Choudhury and **Arpita Patra**. Optimally Resilient Asynchronous MPC with Linear Communication Complexity. **ICDCN 2015**, ACM, 2015.

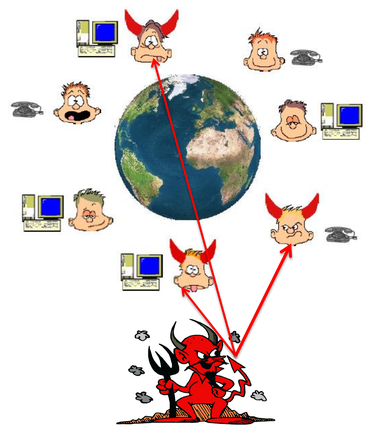
Future Research Plan

Asynchronous Networks. More effort towards closing the feasibility and efficiency gaps. Explore the role of partial synchrony.

Non-Interactive Secure Computation. For an asynchronous network or a network with high latency, non-interactiveness is a great feature. Study MPC and Private Function Evaluation (where the function is a private input of one of the parties) in non-interactive setting.

Two-party to Multi-party Computation. Tremendous efforts have gone in to make 2PC practical in the last few years. Relatively we find few attempts for multi-party case. It is unclear whether the techniques for practical 2PC protocols can be adapted to the multi-party setting. We would like to explore such possibilities.

MPC- The Holy Grail



Settings:
- n parties $P_1,....,P_n$.
- t corrupted by centralized adversary A
- P_i has private input x_i
- A common n-input function f

Goals:
- **Correctness:** Compute $y=f(x_1,x_2,..x_n)$
- **Privacy:** Nothing more than y is leaked to A

Applications:
- E-voting, E-auction, Privacy-preserving Data mining, preventing collision of satellites etc.

Results on MPC

MPC in Asynchronous Networks [2,3,8].

Synchronous
Global Clock
Channels have fixed delay

Asynchronous
No global Clock
Channels have arbitrary yet finite delay

Security	Network	Resilience	Communication Complexity
Perfect	Synchronous Asynchronous	t < n/3 t < n/4	$\mathcal{O}(\|C\|n\|\mathbb{F}\|)$ $\mathcal{O}(\|C\|n^2\|\mathbb{F}\|)$ [3]
Statistical	Synchronous Asynchronous	t < n/2 t < n/3 t < n/4 (non-optimal)	$\mathcal{O}(\|C\|n\|\mu)$ $\mathcal{O}(\|C\|n^5\mu)$ $\mathcal{O}(\|C\|n\|\mu)$ [2]
Cryptographic	Synchronous Asynchronous	t < n/2 t < n/3	$\mathcal{O}(\|C\|n\kappa)$ $\mathcal{O}(\|C\|n\kappa)$ [8]

MPC with Adaptive Security [1,7].

Static
Corrupted parties decided at the outset
Weak model

Adaptive
Corrupted parties decided on the fly
Strong model
captures real life scenarios

- Intermediate models to close efficiency gaps are proposed in [1,7]
- [1] suggests adaptive corruption of `some' of the involved parties and exploits the fact that all the parties are not adaptively corrupt
- [7] suggests to exploit erasure in almost minimal sense. As long as one of the parties can erase intermediate randomness, security is guaranteed

MPC with Fast Online Phase [5]. Takes advantage of offline-online paradigm where input-independent raw material is generated in the offline phase and the function computation takes place in fast speed in the online phase using the raw material.
- Online phase with linear (in n) communication complexity
- Works for both synchronous and asynchronous network

Results on BA and PKE

BA in Dishonest Majority Setting [4]. BA allows a set of mutually distrusting parties to jointly reach agreement on their private inputs even in the face of a coalition of cheating parties. In the dishonest-majority setting, our work presents a Byzantine Agreement that is simultaneously communication and round optimal while previous works achieved optimality for communication only.

Public Key Encryption (PKE) [6]. Our work on public key encryption in a practical attack model (known as selective opening attack) deepens the understanding of relations between various available definitions and presents several efficient constructions.

Contact

Arpita Patra
Department of Computer Science & Automation
Indian Institute of Science
Email: arpita@csa.iisc.ernet.in
Phone: 08022933566

Website:

http://drona.csa.iisc.ernet.in/~arpita/

Preprints and Papers Accepted for Publication

1. **Arpita Patra**, Pratik Sarkar and Ajith Suresh. Fast Actively Secure OT Extension for Short Secrets. NDSS 2017.
2. **Arpita Patra** and Divya Ravi. Bridging the Theoretical Gap between Synchronous and Asynchronous Verifiable Secret Sharing. In Submission.
3. Ashish Choudhury, **Arpita Patra** and Divya Ravi. VSS with Quadratic Communication Complexity. In Submission.
4. Yashvanth Kondi and **Arpita Patra**. Privacy-Free Garbled Circuits for Formulas: Size Zero and Information-Theoretic. In Submission.
5. **Arpita Patra** and Pratik Sarkar. Fast Non-interactive Secure Computation. In Submission.
6. Ashish Choudhury, Gayathri Garimella, **Arpita Patra**, Divya Ravi and Pratik Sarkar. Crash-tolerant Consensus in Directed Graph Revisited. Under Preparation.
7. Chaya Ganesh and **Arpita Patra**. Communication Optimal Broadcast Extension Protocols. Under Preparation.