

“Be weird. Be random. Be who you are. Because you never know who would love the person you hide.”

## Scientific Publications


### THESIS

1. Ajith Suresh. *MPCLeague: Robust MPC Platform for Privacy-Preserving Machine Learning*. PhD Thesis, 2021. Under the supervision of Prof. Arpita Patra. Indian Institute of Science (IISc), Bangalore. [PDF]
2. Ajith Suresh. *Fast Actively Secure OT Extension for Short Secrets*. Master Thesis, 2017. Under the supervision of Prof. Arpita Patra. Indian Institute of Science (IISc), Bangalore. [PDF]
3. Ajith Suresh. *Proximity-based Sentiment Analysis with Contextual Phrase Polarity*. Bachelor Thesis, 2014. College of Engineering (CET), Trivandrum.

### CONFERENCES & JOURNALS

Publications in cryptography usually order authors alphabetically (using surnames) and conferences ([C]) are more common than journals ([J]). Workshops and affiliated events with proceedings ([W]) are marked with ‡.



1. [J] Najwa Aaraj, Abdelrahman Aly, Tim Güneysu, Chiara Marcolla, Johannes Mono, Rogerio Paludo, Iván Santos-González, Mireia Scholz, Eduardo Soria-Vazquez, Victor Sucasas and Ajith Suresh.  
*FANNG-MPC: Framework for Artificial Neural Networks and Generic MPC*.  
In *IACR Transactions on Cryptographic Hardware and Embedded Systems (CHES'25)* (CORE rank- A) [📄]
2. [J] Christopher Harth-Kitserow, Ajith Suresh, Yonqing Wang, Hossein Yalame, Georg Carle and Murali Annavaram.  
*High-Throughput Secure Multiparty Computation with an Honest Majority in Various Network Settings*.  
In *25th Privacy Enhancing Technologies Symposium (PETS'25)* (CORE rank- A) [📄]
3. [C] Yaniv Ben-Itzhak, Helen Möllering, Benny Pinkas, Thomas Schneider, Ajith Suresh, Oleksandr Tkachenko, Shay Vargatik, Christian Weinert, Hossein Yalame and Avishay Yanai.  
*ScionFL: Efficient and Robust Secure Quantized Aggregation*. (Runner-Up Distinguished Paper Award)  
In *2nd IEEE Conference on Secure and Trustworthy Machine Learning (IEEE SaTML'24)* [📄] [📄]
4. [J] Vinod Ganapathy, Eikansh Gupta, Arpita Patra, Gokulnath Pillai and Ajith Suresh.  
*Privadome: Delivery Drones and Citizen Privacy*.  
In *24th Privacy Enhancing Technologies Symposium (PETS'24)* (CORE rank- A) [📄]
5. [C] Andreas Brüggemann, Oliver Schick, Thomas Schneider, Ajith Suresh and Hossein Yalame.  
*Don't Eject the Impostor: Fast Three-Party Computation With a Known Cheater*.  
In *45th IEEE Symposium on Security and Privacy (IEEE S&P'24)* (CORE rank- A\*) [📄] [📄]
6. [C] Gowri R Chandran, Raine Nieminen, Thomas Schneider and Ajith Suresh.  
*PrivMail: A Privacy-Preserving Framework for Secure Emails*.  
In *28th European Symposium on Research in Computer Security (ESORICS'23)* (CORE rank- A) [📄]
7. [J] Nishat Koti, Shravani Patil, Arpita Patra and Ajith Suresh.  
*MPClan: Protocol Suite for Privacy-Conscious Computations*.  
In *Journal of Cryptology (JoC'23)* (CORE rank- A\*) [📄]
8. [C] Andreas Brüggemann, Robin Hundt, Thomas Schneider, Ajith Suresh and Hossein Yalame.  
*FLUTE: Fast and Secure Lookup Table Evaluations*.  
In *44th IEEE Symposium on Security and Privacy (IEEE S&P'23)* (CORE rank- A\*) [📄] [📄]
9. [W] Till Gehlhar, Felix Marx, Thomas Schneider, Ajith Suresh, Tobias Wehrle and Hossein Yalame.  
*SafeFL: MPC-friendly framework for Private and Robust Federated Learning*‡.  
In *6th Deep Learning Security and Privacy Workshop (DLSP'23)* [📄]

10. [J] Thomas Schneider, Ajith Suresh and Hossein Yalame.  
*Comments on “Privacy-Enhanced Federated Learning Against Poisoning Adversaries”.*  
In IEEE Transactions on Information Forensics & Security (IEEE TIFS’23) (CORE rank- A),  
In IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP’23) 

Research work(s) published during PhD. I am the primary author for publications marked with †.














11. [C] Nishat Koti, Arpita Patra, Rahul Rachuri and Ajith Suresh.  
*Tetrad: Actively Secure 4PC for Secure Training and Inference.*†  
In 29th Network and Distributed System Security Symposium (NDSS’22) (CORE rank- A\*)  
12. [C] Arpita Patra, Thomas Schneider, Ajith Suresh and Hossein Yalame.  
*SynCirc: Efficient Synthesis of Depth-Optimized Circuits for Secure Computation.*  
In IEEE International Symposium on Hardware Oriented Security and Trust (HOST’21) 
13. [C] Nishat Koti, Mahak Pancholi, Arpita Patra and Ajith Suresh.  
*SWIFT: Super-fast and Robust Privacy-Preserving Machine Learning.*†  
In 30th USENIX Security Symposium (USENIX’21) (CORE rank- A\*)  
14. [C] Patra, Thomas Schneider, Ajith Suresh and Hossein Yalame.  
*ABY2.0: Improved Mixed-Protocol Secure Two-Party Computation.*†  
In 30th USENIX Security Symposium (USENIX’21) (CORE rank- A\*)  
15. [C] Arpita Patra and Ajith Suresh.  
*BLAZE: Blazing Fast Privacy-Preserving Machine Learning.*†  
In 27th Network and Distributed System Security Symposium (NDSS’20) (CORE rank- A\*)  
16. [C] Harsh Chaudhari, Rahul Rachuri and Ajith Suresh.  
*Trident: Efficient 4PC Framework for Privacy Preserving Machine Learning.*†  
In 27th Network and Distributed System Security Symposium (NDSS’20) (CORE rank- A\*) 
17. [J] Megha Byali, Harsh Chaudhari, Arpita Patra and Ajith Suresh.  
*FLASH: Fast and Robust Framework for Privacy-preserving Machine Learning.*  
In 20th Privacy Enhancing Technologies Symposium (PETS’20) (CORE rank- A)  
18. [C] Harsh Chaudhari, Ashish Choudhury, Arpita Patra and Ajith Suresh.  
*ASTRA: High Throughput 3PC over Rings with Application to Secure Prediction.*††  
In ACM Conference on Cloud Computing Security Workshop (ACM CCSW’19) 

Research work(s) published during M.Tech. (Research). I am the primary author for publications marked with †.



19. [C] Arpita Patra, Pratik Sarkar and Ajith Suresh.  
*Fast Actively Secure OT Extension for Short Secrets.*†  
In 24th Network and Distributed System Security Symposium (NDSS’17) (CORE rank- A\*)  

## WORKSHOPS, SYMPOSIUMS & POSTERS

1. Christopher Harth-Kitzerow, Ajith Suresh, Yonqing Wang, Hossein Yalame, Georg Carle and Murali Annavaram.  
*High-Throughput Secure Multiparty Computation with an Honest Majority in Various Network Settings.*  
In TPMPC’25 (Contributed Talk) 
2. Soumyadyuti Ghosh, Boyapally Harishma, Ajith Suresh, Arpita Patra, Soumyajit Dey, and Debdeep Mukhopadhyay.  
*Stable and Accurate Real-Time Pricing in Smart Grids.*  
In TPMPC’25 (Contributed Talk)
3. Andreas Brüggemann, Oliver Schick, Thomas Schneider, Ajith Suresh and Hossein Yalame.  
*Don’t Eject the Impostor - Honest-Majority MPC With Fixed Malicious Parties.*  
In TPMPC’25 (Contributed Talk) 
4. Najwa Aaraj, Abdelrahman Aly, Tim Güneysu, Chiara Marcolla, Johannes Mono, Rogerio Paludo, Iván Santos-González, Mireia Scholz, Eduardo Soria-Vazquez, Victor Sucasas and Ajith Suresh.  
*FANNG-MPC: Framework for Artificial Neural Networks and Generic MPC.*  
In TPMPC’24 (Contributed Talk)   
5. Andreas Brüggemann, Thomas Schneider, Ajith Suresh and Hossein Yalame.  
*Is Everyone Equally Trustworthy in Practice? (Short Talk).*  
In IEEE S&P’23 (Short Talk) 

6. Gowri R Chandran, Raine Nieminen, Thomas Schneider and Ajith Suresh.  
*PrivMail: A Privacy-Preserving Framework for Secure Emails (Short Talk).*  
In IEEE S&P'23 (Short Talk) 
7. Andreas Brüggemann, Thomas Schneider, Ajith Suresh and Hossein Yalame.  
*Efficient Three-Party Shuffling Using Precomputation.*  
In ACM CCS'22 (Poster) 
8. Daniel Günther, Marco Holz, Benjamin Judkewitz, Helen Möllering, Benny Pinkas, Thomas Schneider and Ajith Suresh.  
*Privacy-Preserving Epidemiological Modeling on Mobile Graphs.*  
In ACM CCS'22 (Poster)  
9. Nishat Koti, Shravani Patil, Arpita Patra and Ajith Suresh.  
*MPClan: Protocol Suite for Privacy-Conscious Computations.*  
In ACM CCS'22 (Poster) , In NDSS'22 (Poster) 
10. Ajith Suresh.  
*MPCLeague: Robust MPC Platform for Privacy-Preserving Machine Learning.*  
In Doctoral Symposium (AIMLSystems'22) 
11. Nishat Koti, Arpita Patra, Rahul Rachuri and Ajith Suresh.  
*Tetrad: Actively Secure 4PC for Secure Training and Inference.*  
In PPML'21 (ACM CCS'21) 
12. Arpita Patra, Thomas Schneider, Ajith Suresh and Hossein Yalame.  
*ABY2.0: Improved Mixed-Protocol Secure Two-Party Computation.*  
In PriML'21 (NeurIPS'21), In PPML'21 (ACM CCS'21), In PPML'21 (CRYPTO'21) 
13. Nishat Koti, Arpita Patra and Ajith Suresh.  
*MPCLeague: Robust and Efficient Mixed-protocol Framework for 4-party Computation.*  
In IEEE S&P'21 (Poster), In DPML'21 (ICLR'21)  
14. Nishat Koti, Mahak Pancholi, Arpita Patra and Ajith Suresh.  
*SWIFT: Super-fast and Robust Privacy-Preserving Machine Learning.*  
In ARCS'22 (Symposium), In DPML'21 (ICLR'21), In PriML/PPML'20 (NeurIPS'20) 
15. Harsh Chaudhari, Ashish Choudhury, Arpita Patra and Ajith Suresh.  
*ASTRA: High Throughput 3PC over Rings with Application to Secure Prediction.*  
In PPML'19 (ACM CCS'19) 

## PREPRINTS & MANUSCRIPTS

1. Felix Marx, Thomas Schneider, Ajith Suresh, Tobias Wehrle, Christian Weinert and Hossein Yalame.  
*WW-FL: Secure and Private Large-Scale Federated Learning.*  
Under Submission 
2. Daniel Günther, Marco Holz, Benjamin Judkewitz, Helen Möllering, Benny Pinkas, Thomas Schneider and Ajith Suresh.  
*Privacy-Preserving Epidemiological Modeling on Mobile Graphs.*  
Under Submission 
3. Arpita Patra, Joachim Schmidt, Thomas Schneider, Ajith Suresh and Hossein Yalame.  
*SynCirc: Efficient Synthesis of Depth-Optimized Circuits from High-Level Languages.*  
Under Submission
4. Soumyadyuti Ghosh, Boyapally Harishma, Ajith Suresh, Arpita Patra, Soumyajit Dey, and Debdeep Mukhopadhyay.  
*Precision and Privacy: Advancing Real-Time Pricing in Smart Grids with Secure Computation.*  
Under Submission