

“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 are marked with †.

1. [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.
In IEEE Conference on Secure and Trustworthy Machine Learning (IEEE SaTML'24) [Full Version]
2. [J] Vinod Ganapathy, Eikansh Gupta, Arpita Patra, Gokulnath Pillai and Ajith Suresh.
Privadome: Delivery Drones and Citizen Privacy.
In Privacy Enhancing Technologies Symposium (PETS'24) (CORE rank- A) [Full Version]
3. [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 IEEE Symposium on Security and Privacy (IEEE S&P'24) (CORE rank- A*) [Full Version]
4. [C] Gowri R Chandran, Raine Nieminen, Thomas Schneider and Ajith Suresh.
PrivMail: A Privacy-Preserving Framework for Secure Emails.
In European Symposium on Research in Computer Security (ESORICS'23) (CORE rank- A) [Full Version]
5. [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*) [Full Version]
6. [C] Andreas Brüggemann, Robin Hundt, Thomas Schneider, Ajith Suresh and Hossein Yalame.
FLUTE: Fast and Secure Lookup Table Evaluations.
In IEEE Symposium on Security and Privacy (IEEE S&P'23) (CORE rank- A*) [Full Version]
7. [C] Till Gehlhar, Felix Marx, Thomas Schneider, Ajith Suresh, Tobias Wehrle and Hossein Yalame.
SafeFL: MPC-friendly framework for Private and Robust Federated Learning†.
In Deep Learning Security and Privacy Workshop (DLSP'23) [Full Version]
8. [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) [Full Version]

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

9. [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*) [Full Version]

10. [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 \(HOST'21\)](#) [\[Full Version\]](#)
11. [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*) [\[Full Version\]](#)
12. [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*) [\[Full Version\]](#)
13. [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*) [\[Full Version\]](#)
14. [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*) [\[Full Version\]](#)
15. [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) [\[Full Version\]](#)
16. [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 \(ACM CCSW'19\)](#) [\[Full Version\]](#)

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

17. [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*) [\[Full Version\]](#)

WORKSHOPS, SYMPOSIUMS & POSTERS

1. Andreas Brüggemann, Thomas Schneider, Ajith Suresh and Hossein Yalame.
Is Everyone Equally Trustworthy in Practice? (Short Talk).
In [IEEE S&P'23 \(Short Talk\)](#)
2. 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 \(Short Talk\)](#)
3. Andreas Brüggemann, Thomas Schneider, Ajith Suresh and Hossein Yalame.
Efficient Three-Party Shuffling Using Precomputation.
In [ACM CCS'22 \(Poster\)](#) [\[Poster Link\]](#)
4. 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 \(Poster\)](#) [\[Poster Link\]](#) [\[Full Version\]](#)
5. Nishat Koti, Shravani Patil, Arpita Patra and Ajith Suresh.
MPClan: Protocol Suite for Privacy-Conscious Computations.
In [ACM CCS'22 \(Poster\)](#) [\[Poster Link\]](#), In [NDSS'22 \(Poster\)](#) [\[Poster Link\]](#)
6. Ajith Suresh.
MPCLeague: Robust MPC Platform for Privacy-Preserving Machine Learning.
In [Doctoral Symposium \(AIMLSystems'22\)](#) [\[PDF\]](#)
7. Nishat Koti, Arpita Patra, Rahul Rachuri and Ajith Suresh.
Tetrad: Actively Secure 4PC for Secure Training and Inference.
In [PPML'21 \(ACM CCS'21\)](#) [\[Full Version\]](#)
8. 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 \(CRYPTO'21\)](#) [\[Full Version\]](#)
9. 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 \(ICLR'21\)](#) [\[Poster Link\]](#) [\[PDF\]](#)

10. 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) [\[Full Version\]](#)
11. 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) [\[Full Version\]](#)

PREPRINTS & MANUSCRIPTS

1. 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.
[Under Submission](#) [\[Full Version\]](#)
2. Felix Marx, Thomas Schneider, Ajith Suresh, Tobias Wehrle, Christian Weinert and Hossein Yalame.
HyFL: A Hybrid Approach For Private Federated Learning.
[Under Submission](#) [\[Full Version\]](#)
3. Daniel Günther, Marco Holz, Benjamin Judkewitz, Helen Möllering, Benny Pinkas, Thomas Schneider and Ajith Suresh.
Privacy-Preserving Epidemiological Modeling on Mobile Graphs.
[Under Submission](#) [\[Full Version\]](#)