SysteMPC'25: 1st Workshop on Systems for Secure Multi-Party Computation

https://www.bu.edu/riscs/events/systempc/

John Liagouris
Boston University
liagos@bu.edu

Vasiliki Kalavri
Boston University
vkalavri@bu.edu

Mayank Varia
Boston University
varia@bu.edu

Abstract

The SysteMPC workshop brings together cryptographers and systems researchers to discuss advances in overcoming practical challenges of using MPC in the wild. Topics of interest include cryptography and systems co-design, programming abstractions, modularity of cryptographic software, hardware acceleration, experimentation, and integration with the existing ecosystem. In this short report, we summarize the inaugural edition of the workshop, which was held on July 10, 2025 at Boston University.

1 Introduction

Cryptographically secure multi-party computation (MPC) enables mutually distrusting parties to perform computations on their collective data while keeping their own private data siloed from each other (and from external adversaries) with provable security guarantees [3]. MPC has been deployed to protect healthcare data like disease surveillance, educational data like student GPAs, financial data like credit modeling, advertising data like conversion rates, public interest data like the gender wage gap, and more [1, 2, 4, 5]. Nevertheless, MPC adoption is still at its infancy due to several challenges, including performance issues caused by the high computational and communication cost of MPC protocols, deployment complexity, and the requirement for cryptographic expertise.

We believe that the field of MPC has reached a turning point, where advancements in cryptographic techniques necessitate the development of efficient system implementations to achieve practical and widespread adoption. At the same time, performing systems research in MPC requires a deep understanding of cryptographic protocols. This interplay between cryptography and systems is a critical juncture, at which innovations in one area are closely intertwined with the development of meaningful solutions in the other. To this end, the SysteMPC workshop aims to catalyze fruitful collaborations between cryptographers and system experts and to foster more understanding of each side's ideas and methodologies.

The inaugural SysteMPC workshop, held on July 10, 2025 at the Duan Family Center for Computing and Data Sciences at Boston University, brought together researchers, developers, and practitioners from both the cryptography and systems communities for the first time. The workshop featured keynote speeches, invited talks, and lightning talks, covering topics, such as compilers for MPC, scalability and performance of MPC protocols, secure data analytics systems, secure aggregation, applications of private set intersection, correlated randomness generation, and secure machine learning. The workshop also provided a platform for participants to share their experiences, showcase their research, and discuss future directions.

2 Topics of interest and audience

The focus of the SysteMPC workshop is to share experiences in developing, operating, and deploying MPC systems, to discuss recent advances in cryptographic techniques for MPC and related technologies in the context of the systems that implement them, and to highlight open challenges.

Topics of interest include but are not limited to the following:

- Cryptography and systems co-design
- Programming abstractions for MPC
- Performance optimization for secure computations
- Secure query optimization
- Domain-specific systems for MPC, e.g., secure machine learning, graph analytics, time series analytics
- Integration of MPC with other PETs
- Modularity of cryptographic software
- Hardware acceleration
- Operating systems optimizations for MPC
- Experimentation, benchmarks, and evaluation studies
- Deployment and orchestration of MPC systems
- Integration of MPC tools with the existing ecosystem

The intended audience are, but not limited to, academic and industrial computer scientists interested in cryptography and secure computation, distributed systems, database systems, operating systems, cloud computing, and algorithms. Along with novel research work, SysteMPC welcomes contributions of experience reports, demonstrations, case studies, and real-world deployments of MPC.

In its first edition, SysteMPC attracted a total of 54 participants from over 20 institutions and organizations, representing a diverse range of backgrounds and expertise in cryptography, systems, and applications. Out of those, approximately 50% were PhD students, highlighting the workshop's success in attracting a new generation of researchers who are eager to explore the intersection of cryptography and systems.

3 Workshop program

SysteMPC'25 offered a full-day program, consisting of two keynote talks, six invited talks, and two sessions with 5-minute lightning talks.

3.1 Keynotes and invited talks

SysteMPC'25 hosted two keynote presentations from leading experts in the field. Attendees were fortunate to hear from Marcel Keller, senior research scientist with CSIRO's Data61, a research unit of Australia's national science agency, and from Peter Rindal, a cryptographic researcher specializing in secure multi-party computation (MPC) and privacy-preserving cryptographic protocols at Visa Research.

The full list of invited speakers, in the order they appeared in the program, is given below.

- Marcel Keller (CSIRO's Data61)
- Kert Tali (Cybernetica)
- Mariana Raykova (Google)
- Antigoni Polychroniadou (JP Morgan Chase)
- Marina Blanton (University at Buffalo)
- John Liagouris (Boston University)
- Peihan Miao (Brown University)
- Peter Rindal (Visa Research)

3.2 Lightning talks

SysteMPC also featured two Lightning Talks sessions, providing a platform for researchers to share early-stage work, experiences, and use cases. In response to a call for submissions, we received a total of 13 proposals from speakers representing 6 different institutions. The talks covered real-world deployments of MPC systems, experience reports on using MPC tools, innovative approaches to optimizing MPC operations for machine learning and oblivious relational joins, hardware acceleration for MPC, MPC-based authentication, and others.

The full list of lightning talk speakers, in the order they appeared in the program, is given below.

- Christopher Smith (Stony Brook University)
- Sam Buxbaum (Boston University)
- Andrea Lin (MIT Lincoln Laboratory)
- Qi Pang (Carnegie Mellon University)
- Seyda Nur Guzelhan (Boston University)
- Komal Kumari (New Jersey Institute of Technology)
- Eli Baum (Boston University)
- Muhammad Faisal (Boston University)
- Noah Luther (MIT Lincoln Laboratory)
- Ryan Little (Boston University)
- Xiangrui Xu (Old Dominion University)
- Xiteng Yao (Boston University)
- Tarakaram Gollamudi

4 Future of SysteMPC

The feedback from attendees was overwhelmingly positive, with many expressing their appreciation for the opportunity to engage with leading researchers and practitioners in the field. The success of the workshop has led us to plan for its annual recurrence, with the aim of creating a permanent platform for the cryptographic and systems communities to come together and advance the state-of-the-art in multi-party computation systems. We are committed to building on the momentum generated by this inaugural event and to ensuring that the SysteMPC workshop remains a premier forum for researchers and practitioners to share knowledge, exchange ideas, and collaborate on the development of innovative MPC systems.

5 Acknowledgement

We thank the U.S. National Science Foundation (Award No. #2209194), the Boston University Computer Science department, and the Boston University Center for Reliable Information Systems & Cyber Security (RISCS) for their generous support. We are also grateful to Kristen Dionne and Stephen Thomas Brown for their support with speaker travel and local arrangements. The workshop would not have been possible without the invaluable help of our student volunteers, Sakshi Sharma, Yuhang Song, Sam Buxbaum, Eli Baum, and Muhammad Faisal.

References

[1] David W. Archer, Dan Bogdanov, Yehuda Lindell, Liina Kamm, Kurt Nielsen, Jakob Illeborg Pagter, Nigel P. Smart, and Rebecca N. Wright. 2018. From Keys to Databases - Real-World Applications of Secure Multi-Party Computation. *Comput. J.* 61, 12 (2018), 1749–1771.

[2] Boston Women's Workforce Council. 2025. Gender and Racial Wage Gaps in Boston by the Numbers. https://thebwwc.org/wage-gap-studies. [Online; accessed September 2025].

[3] Yehuda Lindell. 2020. Secure multiparty computation. *Commun. ACM* 64, 1 (dec 2020), 86–96. https://doi.org/10.1145/3387108

[4] MPC Deployments. 2025. MPC Deployments: A hub for real-world MPC deployments. https://mpc.cs.berkeley.edu. [Online; accessed September 2025].

[5] United Nations Global Working Group (GWG) Task Team on Privacy Preserving Techniques. 2023. Case study repository. https://unstats.un.org/wiki/display/UGTTOPPT/Case+study+repository. [Online; accessed September 2025].