GEORGETOWN UNIVERSITY

April 14, 2023

Subject: Nomination for Best Scientific Cybersecurity Paper

Dear Selection Committee,

I am writing to nominate “EpiGRAM: Practical Garbled RAM” by David Heath, Vladimir Kolesnikov, and Rafail Ostrovsky for the “Best Scientific Cybersecurity Paper” award. In March 2023 the White House issued its vision of advancing privacy-preserving data-sharing technology: https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Strategy-to-Advance-Privacy-Preserving-Data-Sharing-and-Analytics.pdf

The central underlying mathematics discussed in the White House report is so-called secure multiparty computation (MPC), a technology that enables privacy-preserving analytics and data sharing. Since the invention of MPC in the 80s, the approach has been almost exclusively to compile programs as circuits, and then to securely evaluate these circuits gate by gate. While circuits can encode straight-line programs efficiently, in practice compiling arbitrary programs to circuits blows up the cost. The inefficiency of compilation is unfortunate, because software engineers understand programs expressed in high-level languages which are best represented as RAM programs. In fact, significant effort has been invested in RAM MPC, however, these have primarily focused on theoretical feasibility.

Until EpiGRAM, the practically efficient approach to RAM was Oblivious RAM (ORAM). After 30 years of intense research, ORAM is still communication-inefficient, because each memory access requires many rounds of communication (e.g. 10 rounds per access). This cost becomes untenable when using ORAM in long-running programs. Another line of work, Garbled RAM (GRAM), executes all memory accesses non-interactively. However, the communication and computation costs of all prior GRAM constructions were impractical (e.g. gigabytes per access). It is therefore difficult to claim practical general MPC based on either ORAM or prior GRAM.

Efficient RAM-MPC is the holy grail of bringing MPC to practice, and RAM access is at its core. After decades of attempts, we, as a community, believed that practical constant-round RAM, enabling efficient general-purpose MPC, was unlikely. EpiGRAM is an utterly unexpected breakthrough that cleanly solves essentially all RAM access problems and lays the groundwork for practical MPC compilers for high-level languages. It is a true GRAM, running all memory accesses in one communication round while achieving communication and computation costs similar to that of the multi-round GRAM, and promises to be even more efficient. In terms of impact, I can compare designing EpiGRAM to designing a blazing-fast fully-homomorphic encryption scheme (which seems far from our reach using current technology). Besides, practical FHE operates only on circuits. EpiGRAM opens the door for practical deployment of MPC technology for large-scale applications. Quite unsurprisingly, this work was selected as the best-paper of the conference at Eurocrypt 2022, a flagship conference in cryptography.

In summary, EpiGRAM achieves noninteractive RAM access while maintaining practical communication and computation costs, making practical general-purpose MPC achievable, specifically, generic MPC compilers for high-level languages. The paper is clearly an important MPC breakthrough, and perhaps one that can revolutionize the way we compute. In my opinion, its technical innovation and practical impact warrants a prestigious recognition such as the “Best Scientific Cybersecurity Paper” award.

Brief Bio: Muthu Venkitasubramaniam is an Associate Professor at the Georgetown University and CTO of Ligero Inc. He received his B.Tech degree in computer science from the Indian Institute of Technology, Madras in 2004 and then his PhD from Cornell in 2011. He spent a year at the Courant Institute as a postdoc researcher under the CIF, and then joined the faculty at University of Rochester where he spent 10 years. In Fall 2021, he joined the faculty at Georgetown University. He is a recipient of the Google Faculty Research Award and the ICDE Influential Paper Award and part of the Steering Committee for the ZK Proof Standardization effort.

Sincerely,

Muthu

Muthuramakrishnan
Venkitasubramaniam, Ph.D