Abstract: Two-party Private Function Evaluation (PFE) enables the participants to jointly execute a computation for which one of them provides the function while the other one the input to it. A PFE protocol should not leak more information, neither about the function nor the input, then that is revealed by the output of the computation. We observe that the function privacy requirement, in fact, makes input privacy meaningless as it allows for the unnoticeable evaluation of the identity function, entirely disclosing the input. In this work, we ask the question, whether it is possible to compute a function on the confidential data of someone else without revealing the function, but still enabling some control over the executable computations. We propose the notion of Controlled Private Function Evaluation (CPFE) and answer the question affirmatively by showing a simple, generic realization of CPFE based on functional encryption. To demonstrate the applicability of our approach, we show a concrete instantiation of our protocol for inner product computation that enables secure statistical analysis (and more) under the standard Decisional Diffie-Hellman assumption in the random oracle model.

Bio: Máté obtained his MSc diploma in computer science in the Security and Privacy program of EIT ICT Labs at the University of Trento (Italy) and Eötvös Loránd University (Hungary). His bachelor degree is in mathematics from the Budapest University of Technology and Economics. He has been doing research in the CrySyS Lab since 2014.