Information-Theoretically Secure Multi-Party Computation with Minimal Interaction

Maki Yoshida[1]

1) *NICT, Japan*

Corresponding Author: Maki Yoshida, maki-yos@nict.go.jp

ABSTRACT

Achieving as strong security as possible in a minimal scenario for secure Multi-Party Computation (MPC) is not only an essential interest in theory but also a critical problem to be solved in real-world applications handling sensitive information. We proposed MPC with a minimal communication pattern and an information-theoretical security. I will overview our results on the (im)possibility of non-interactive MPC and explain our methods of achieving a best possible security.