微电子大楼
102讲学厅
12月11日
9:00 - 11:30

Information-theoretic Cryptography

信息论密码学

扫码报名
12月4日截止

Shun Watanabe received PhD. degree at Tokyo Institute of Technology in 2009. During Apr. 2009 to Feb. 2015, he was an assistant professor of the Department of Information Science and Intelligence Systems at the University of Tokushima. Since Feb. 2015, he has been an associate professor of the Department of Computer and Information Sciences at Tokyo University of Agriculture and Technology. He is a senior member of IEEE and a member of IEICE. During 2016 to 2020, he served as an Associate Editor for the IEEE Transactions on Information Theory. He served as a general co-chair of the 2021 IEEE Information Theory Workshop. He has been a Board of Governor of IEEE Information Theory Society. He has been elected for IEEE IT Society **Distinguished Lecturer** for 2023-2024.

Abstract The modern cryptography is roughly categorized into computational cryptography and information-theoretic cryptography. Although the computational cryptography has been widely used in practice, its security relies on certain computational assumptions. On the other hand, the information-theoretic cryptography seeks to build protocols that are secure without any assumptions on adversary's computational power, and it has been actively studied since the landmark paper by Shannon. Furthermore, some of information-theoretic concepts and tools are used in the computational cryptography as well. In this talk, we provide an overview of the field of information-theoretic cryptogprahy. Then, we present a few technical tools, such as the universal hash family and leftover hash lemma. We also present the formulation of secure computation and how to define its security against active adversary. The talk is based on the recently published textbook (Himanshu Tyagi and Shun Watanabe, "Information-theoretic Cryptography," Cambridge University Press, 2023).

IEEE INFORMATION THEORY SOCIETY Guangzhou Chapter