In Favour of Posting

香港中文大學
The Chinese University of Hong Kong

Institute of Theoretical Computer Science and Communications

Joint ITCSC-CSE Seminar

Adaptive Garbled Circuits with Near-Optimal Online Complexity

By

Akshayaram Srinivasan

UC Berkeley

10 January 2019, Thursday

11:00 am – 12:00 nn

Room 121, 1/F,* Ho Sin Hang Engineering Building, *CUHK

Abstract:

Garbled circuits are fundamental cryptographic primitives. They have diverse applications such as designing secure multiparty computation protocols, in parallel cryptography, in constructing program obfuscation and more recently in constructing IBE schemes without pairings. The security of garbling schemes have been analyzed in two settings: the selective setting and the adaptive setting. In the selective setting, an adversary is forced to declare the input on which he wishes to evaluate the circuit before seeing the garbled circuit and in the adaptive setting, he is allowed to choose the input adaptively depending on the garbled circuit. Constructing adaptive garbled circuits where the size of the garbled input is small has been a major open problem in cryptography. In this talk, I will give a construction of adaptive garbled circuits where the size of the garbled input is (nearly) optimal.

Joint work with Sanjam Garg.

Biography:

Akshayaram Srinivasan is a fourth-year Ph.D. student in the theory group at UC Berkeley. His advisor is Prof. Sanjam Garg. He received his B.Tech in Computer Science and Engineering from IIT-Madras in 2015.

He is broadly interested in theoretical computer science and in particular, in the theory and applications of cryptography. He has published research papers in top conferences in cryptography such as Foundations of Computer Science (FOCS), Crypto, Eurocrypt, and TCC. His research has been recognized with the best paper award at Eurocrypt 2018.

******* ALL ARE WELCOME *******

Hosted & Enquiries : Prof Andrej Bogdanov/ Institute of Theoretical Computer Science and Communications Tel: 3943 4261 / 3943 3452