In Favour of Posting

香港中文大學
The Chinese University of Hong Kong

Institute of Theoretical Computer Science and Communications

ITCSC-CSE Seminar

Equivocating Yao: Constant-Round Adaptively Secure Multiparty Computation in the Plain Model

By

Oxana Poburinnaya

PhD student, Boston University

4 December 2017, Monday

5:30 pm – 6:30 pm

Room 401, 4/F, William MW Mong Engineering Building, CUHK

Abstract:

Yao's garbling scheme is one of the basic building blocks of cryptographic protocol design. Originally designed to enable two-message, two-party secure computation, the scheme has been extended in many ways and has innumerable applications. Still, a basic question has remained open throughout the years: how many rounds of interaction are required for adaptively secure computation? In particular, can Yao's scheme be extended to guarantee security in the face of an adversary that corrupts both parties, adaptively, as the computation proceeds?

We answer this question in the affirmative. We define a new type of encryption, called functionally equivocal encryption (FEE), and show that when Yao's scheme is implemented with an FEE as the underlying encryption mechanism, it becomes secure against such adaptive adversaries. We then show how to implement FEE from any one way function.

Combining our scheme with non-committing encryption, we obtain the first two-message, two-party computation protocol, and the first constant-round multiparty computation protocol, in the plain model, that are secure against semi-honest adversaries who can adaptively corrupt all parties.

Joint work with Ran Canetti and Muthuramakrishnan Venkitasubramaniam

Biography:

Oxana is a PhD student at Boston University. She graduated from Lomonosov Moscow State University, math department, in 2013. Her research interests are secure multiparty computation and deniable computation.

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

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