VirginiaTech

VIRGINIA POLYTECHNIC INSTITUTE AND STATE UNIVERSITY

Computer Science Seminar Series

National Capital Region

Multi-client Verifiable Computation with Stronger Security Guarantees

Speaker: Feng-Hao Liu

University of Maryland

Friday, March 6, 2015

1:00PM- 2:00PM, NVC 325

Abstract

Choi et al. (TCC 2013) introduced the notion of *multi-client verifiable computation* (MVC) in which a set of *computationally weaker* clients outsource to a *powerful yet perhaps untrusted* server the computation of a function f over their collective inputs in a sequence of time periods. The task is to design a procedure for the clients to efficiently check the correctness of the answers (without redoing the computation and further interactions).

In this talk, I will review the problem of MVC, previous approaches, and their limitations. Then I will discuss our new approaches to overcome the limitations and achieve stronger security guarantees. We developed a new technique – a distributed version of *attribute-based encryption* (ABE) that plays the central role of our construction. I will elaborate on this method, and then discuss several generalizations, such as how to achieve input privacy, how to handle collusions among parties (server-client, client-client collusions). I will point out both possibilities and impossibilities in various settings.

This is a joint work with S. Dov Gordon (ACS), Jonathan Katz (UMD), Elaine Shi (UMD), and Hong-Sheng Zhou (VCU).

Biography

Feng-Hao Liu is a postdoctoral researcher at the Maryland Cybersecurity Center, University of Maryland. He obtained his Ph.D. at Brown University 2013, under supervision of Anna Lysyanskaya. His research interests include foundations of cryptography and their applications to scenarios in cloud computing and physical attacks. Additionally, Feng-Hao is also interested in other topics such as mathematical aspects of cryptographic hardness assumptions and security amplifications.