In Favour of Posting

THE CHINESE UNIVERSITY OF HONG KONG

Department of Information Engineering

Seminar

Registration-Based Encryption: How to build it without garbling

By

Mr. Dimitris Kolonelos

IMDEA Software Institute & Universidad Politécnica de Madrid, Spain

Date : 11 December 2023 (Monday)
Time : 11:00am – 12:00pm
Venue : Rm 801, Ho Sin Hang Engineering Building, CUHK

Abstract

Registration-based encryption (RBE) was recently introduced as an alternative to identity-based encryption (IBE), to resolve the key-escrow problem: In RBE, the trusted authority is substituted with a weaker entity, called the key curator, who has no knowledge of any secret key. Users generate keys on their own and then publicly register their identities and their corresponding public keys to the key curator. RBE is a promising alternative to IBE, retaining many of its advantages while removing the key-escrow problem, the major drawback of IBE. Unfortunately, all prior constructions of RBE use cryptographic schemes in a non black-box way, which makes them prohibitively expensive.

In this talk we see ways of constructing RBE that is concretely highly efficient, avoiding the use of heavy (non black-box)cryptographic machinery, such as general-purpose indistinguishability obfuscation or garbled circuits.

The talk is based on two recent works [GKMR, CCS 2023] (https://eprint.iacr.org/2022/1505.pdf) and [FKdP23, ASIACRYPT 2023] (https://eprint.iacr.org/2023/1389.pdf).

Biography

Dimitris Kolonelos is a final year PhD student at IMDEA Software Institute advised by Dario Fiore. His research interests lie broadly in the theoretical and practical aspects of Cryptography with a focus on Succinct Cryptographic Primitives and Advanced Encryption Schemes.

**** ALL ARE WELCOME ****

Host: Prof. Sherman S. M. Chow (Tel: 3943-8376, Email: sherman@ie.cuhk.edu.hk)
Enquiries: Information Engineering Dept., CUHK (Tel.: 3943-8474)