In Favour of Posting

THE CHINESE UNIVERSITY OF HONG KONG
Department of Information Engineering

Seminar

Distributed Cryptographic Security using Advanced Algebra

by

Professor Yvo Desmedt
Jonsson Distinguished Professor
University of Texas at Dallas
U.S.A.

Date	**:**	**5 June, 2015 (Friday)**
Time	**:**	**4:15 – 5:15pm**
Venue	**:**	**Room 833, Ho Sin Hang Engineering Building** **The Chinese University of Hong Kong**

Abstract

Trust is often distributed and so, such operations, as digital signatures, need to be performed jointly by mutually untrusted parties. Such a distributed cryptographic operation is called Threshold Signing. Jointly, with Secure Multiparty Computation (which allows maximal privacy when performing distributed computation), these are considered today the main building blocks of practical distributed security.

We first survey the role of algebra, (such as tensor products of tensors, Chinese Remainder Theorem, content of polynomials) in making some of these distributed cryptographic security more practical.

Many non-Abelian group operations occur in secure multiparty computation. We survey some of the approaches using planar graphs that have been used to address this problem.

We also explain the importance of above work in the context of Snowden's leaks, that have undermined the trust one used to have in hardware and in cryptographic algorithms.

Finally, we announce a new Verifiable Secret Sharing approach, which relies on some special case of Tensor Codes. We also talk about some open problems in the area of secret sharing intersecting with the area of algebra.

The talk does not assume the audience to be familiar with advanced algebra.

Biography

Yvo Desmedt is the Jonsson Distinguished Professor at the University of Texas at Dallas, chair at the University College London and a Fellow of the International Association of Cryptologic Research (IACR). He received his Ph.D. (1984, Summa cum Laude) from the University of Leuven, Belgium. He held positions at: Universite de Montreal, University of Wisconsin - Milwaukee (founding director of the Center for Cryptography, Computer and Network Security), and Florida State University (Director of the Laboratory of Security and Assurance in Information Technology, an NSA Center of Excellence since 2000). He has held numerous visiting appointments. He is the Editor-in-Chief of IET Information Security and Chair of the Steering Committees of CANS and ICITS. He was Program Chair of e.g., Crypto 1994, the ACM Workshop on Scientific Aspects of Cyber Terrorism 2002, and ISC 2013. He has authored over 200 refereed papers, primarily on cryptography, computer security, and network security. He has made important predictions, such as his 1983 technical description how cyber could be used to attack control systems (realized by Stuxnet), and his 1996 prediction hackers will target Certifying Authorities (DigiNotar was targeted in 2011).

**** ALL ARE WELCOME ****

Host: Professor Sherman S.M. Chow (Tel: 3943-8376, Email: smchow@ie.cuhk.edu.hk)
Enquiries: Information Engineering Dept., CUHK (Tel.: 3943-8385)