Guest Lecture

Sharing Secrets on Boolean Circuits: Application to Key-policy Attribute-based Encryption

Prof. Ferucio Laurentiu Tiplea

Department of Computer Science
"Alexandru Ioan Cuza" University of Iasi
Iasi, Romania

Monday, 10.04.2017, 14:00 – 15:00, TU Dresden, Fakultät Informatik
Nöthnitzer Str. 46, Raum APB-1004

Abstract:
Attribute-based encryption (ABE) is a new paradigm in cryptography, where messages are encrypted and decryption keys are computed in accordance with a given set of attributes and an access structure on the set of attributes. There are two forms of ABE: key-policy ABE (KP-ABE) and ciphertext-policy ABE (CP-ABE). In a KP-ABE, each message is encrypted together with a set of attributes and the decryption key is computed for the entire access structure; in a CP-ABE, each message is encrypted together with an access structure while the decryption keys are given for specific sets of attributes.
In this talk two new key-policy attribute-based encryption schemes, based on secret sharing and bilinear maps, are discussed. The first scheme, based on secret sharing and just one bilinear map, is practically efficient for a subclass of Boolean circuits which includes Boolean formulas. The second scheme is based on secret sharing and chained multi-linear maps, a simpler form of leveled multi-linear maps. The scheme works for general Boolean circuits and is more efficient than the existing one based on multi-linear maps. Selective security of the two schemes in the standard model is proved.

Bio:

Ferucio Laurentiu Tiplea received the Ph.D. degree in computer science from ``Alexandru Iona Cuza'' University of Iasi, Romania, in 1993. He joined the Department of Computer Science of the aforementioned university in 1990, where he is currently Professor of Computer Science.
Dr. Tiplea's research interests lie in the area of theories and tools for high-level modeling, design, and analysis of systems (including Petri nets and formal verification), complexity of computation, and cryptography and computer security. He published more than 80 papers in professional journals and refereed conference proceedings in these areas, co-edited five conference volumes, contributed to six edited volumes, and delivered invited talks at many universities and international conferences. Dr. Tiplea was the recipient of several fellowships, such as the Fulbright Fellowship, German Academy Fellowship, DAAD Fellowship, Monbusho Fellowship. From December 2003 to May 2006 he held a Visiting Professor position at University of Central Florida, School of Computer Science, Orlando (USA).