專 題 演 講

演 講 者：Professor Ten H. Lai

(The Ohio State University)

演講題目：A Brief Story of Computing on Private Data

演講摘要：

This talk consists of two parts. The first part is an introduction to a recent breakthrough in cryptography --- Craig Gentry's fully homomorphic encryption (FHE) --- which is interesting, inspiring, and considered by many as a holy grail of cryptography. FHE enables clouds to process users private data in an encrypted form (under a single key). The second part of this talk is a result of ours. We show that it is possible to convert any single-key FHE scheme into a multi-key (or even multi-scheme) FHE scheme. Such schemes allow clouds to process data that are encrypted under different keys or even different encryption schemes. For example, consider the well-known Yao's millionaires problem. Suppose two numbers x and y are encrypted as cx and cy by different schemes (and/or under different keys). We can decide if x < y by directly processing the ciphertexts cx and cy without decrypting them. This talk is accessible (I hope) to those without much background in cryptography.

講者簡歷：

Ten H. Lai is a Professor of Computer Science and Engineering at the Ohio State University. He is interested in applying Zen to teaching and research. He served as program chair of ICPP 1998, general chair of ICPP 2000, program co-chair of ICDCS 2004, general chair of ICDCS 2005, and recently, general co-chair of ICPP 2007. He is/was an editor of IEEE Transactions on Parallel and Distributed Systems, ACM/Springer Wireless Networks, Academia Sinica's Journal of Information Science and Engineering, International Journal of Sensor Networks, and International Journal of Ad Hoc and Ubiquitous Computing.