

信息安全国家重点实验室

第五届安全协议研讨会日程

2010年6月10日 地点：北京，中关村，中科院软件所5号楼3层报告厅

时 间	报 告 题 目	报 告 人
9:00—10:00	Leakage-Resilient Cryptography	Jonathan Katz
10:00—10:30	休息	
10:30—11:00	Cryptanalysis and Improvement of an Anonymous Password-based Authenticated Key Exchange Protocol	Wang Fengjiao
11:00—11:30	具有更低轮复杂度的可验证秘密分享	张斌
11:30—12:00	Pseudo-randomness Extraction for Generalized Diffie-Hellman Problem over Composite Modulus under Factoring Assumption	Xianhui Lu
12:00—13:00	午饭	
13:00—14:30	Privacy Notions for Privacy Preserving Microdata Publishing	Ninghui Li
14:30—15:00	Provably Secure Identity-Based Authenticated Key Agreement Protocols under Simple Assumption	Zhao Xiufeng
15:00—15:30	Gateway-oriented password-authenticated key exchange based on RSA	Fushan Wei
15:30—16:00	Fully Secure Anonymous Hierarchical Identity-Based Encryption with Constant-Size Ciphertext	Hao Wang
16:00—16:30	Rational Secret Sharing As Extensive Games	Zhifang Zhang
16:30—17:00	Provably Secure Three-party Password-based Authenticated Key Exchange Protocol	



时间： 6月10日上午 9:00-10:30

Talk 1

Title: Leakage-Resilient Cryptography

Abstract: Real-world implementations of cryptosystems are often attacked by using various forms of side-channel cryptanalysis to obtain information about the secret key. In one attempt to address these attacks, cryptographers have recently considered the notion of leakage-resilient cryptosystems that remain secure even if some information about the secret key is leaked.

In this talk I will describe constructions of signature schemes with *bounded* leakage resilience, and then discuss some recent work aimed at achieving security against *continual* (unbounded) leakage in a model where the secret key is periodically refreshed.

Based on joint work with Zvika Brakerski, Yael Tauman Kalai, and Vinod Vaikuntanathan

Talk 2:

时间： 6月11日上午 9:00-10:00

Title: Rational Secret Sharing

Abstract: One goal at the intersection of game theory and cryptography is to model participants in a distributed (cryptographic) protocol as rational entities, in the hopes of both circumventing known impossibility results (by relying on self-interested, rather than byzantine, behavior) as well as offering a more realistic picture of real-world behavior (in which altruism may not be present). This line of work has so far reached its greatest success in the study of *rational secret sharing*, where all players wish to reconstruct a secret while preventing other players from doing so. This talk will offer a survey of this area, focusing on both the protocols themselves as well as the development of appropriate definitions of rationality for this setting.

Based on joint work with Dov Gordon, Georg Fuchsbauer, and David Naccache

Jonathan Katz is an associate professor of computer science at the University of Maryland whose research focuses on security, cryptography, and theoretical computer science. He received undergraduate degrees in mathematics and chemistry from MIT in 1996, and a PhD in computer science from Columbia University in 2002. His textbook "Introduction to Modern Cryptography" was published in 2007, and his monograph "Digital Signatures" is due out later this year.



Title: Privacy Notions for Privacy Preserving Microdata Publishing

时间: 6月10日下午 13:00—14:30

Abstract:

In this information age, data and knowledge extracted by data mining techniques represent a key asset driving research, innovation, and policy-making activities. Many organizations have recognized the need of accelerating such trends and are therefore willing to release the microdata they collected. In microdata, each piece of data is about one individual entity, such as an individual, a household, or an organization. However microdata publishing may result in privacy breaches, and must be executed in a way that protects the privacy of the respondents.

To counter the privacy threats, privacy preserving microdata publishing has been intensively studied recently over the last decade or so. Many privacy notions have been introduced, including k -anonymity, l -diversity, t -closeness, and several others. These privacy notions are defined based on syntactic properties of the anonymized data. In recent years, it has been increasingly recognized that they do not provide rigorous privacy guarantees. They are often based on (explicit or implicit) assumptions of a particular kind of adversary, with specific prior knowledge and inference procedures. And they often break down when facing adversaries with other kinds of prior knowledge or different inference procedures (such as those exploit the knowledge of the algorithm). In recent years, differential privacy has gradually been accepted as the privacy notion of choice for answering statistical queries. However, applying differential privacy to microdata appears difficult, and there exist few practical methods on publishing microdata that satisfies differential privacy. Challenges remain to find privacy notions that both offer strong privacy protections and are practically satisfiable.

In this talk, we will survey the privacy notions for microdata publishing and discuss potential candidate privacy notions.

Brief Bio:

Ninghui Li is an Associate Professor of Computer Science at Purdue University. He received a Bachelor's degree from the University of Science and Technology of China in 1993 and a Ph.D. in Computer Science

from New York University in 2000. Before joining the faculty of Purdue in 2003, he was a Research Associate at Stanford University Computer Science Department for 3 years.

Prof. Li's research interests are in computer and information security and privacy, with focuses on access control and data privacy. He has published over 90 referred papers, and has served on the Program Committees of more than 50 international conferences and workshops, including serving as the Program Chair of the 2008 ACM Symposium on Access Control Models and Technologies and the 2009 IFIP WG 11.11 International Conference on Trust Management (IFIPTM). He is on the editorial board of the VLDB Journal. His research is funded by the US National Science Foundation, the US Air Force Office of Scientific Research (AFOSR), the US Office of Naval Research (ONR), and by IBM and Google. In 2005, he was awarded a NSF CAREER award.