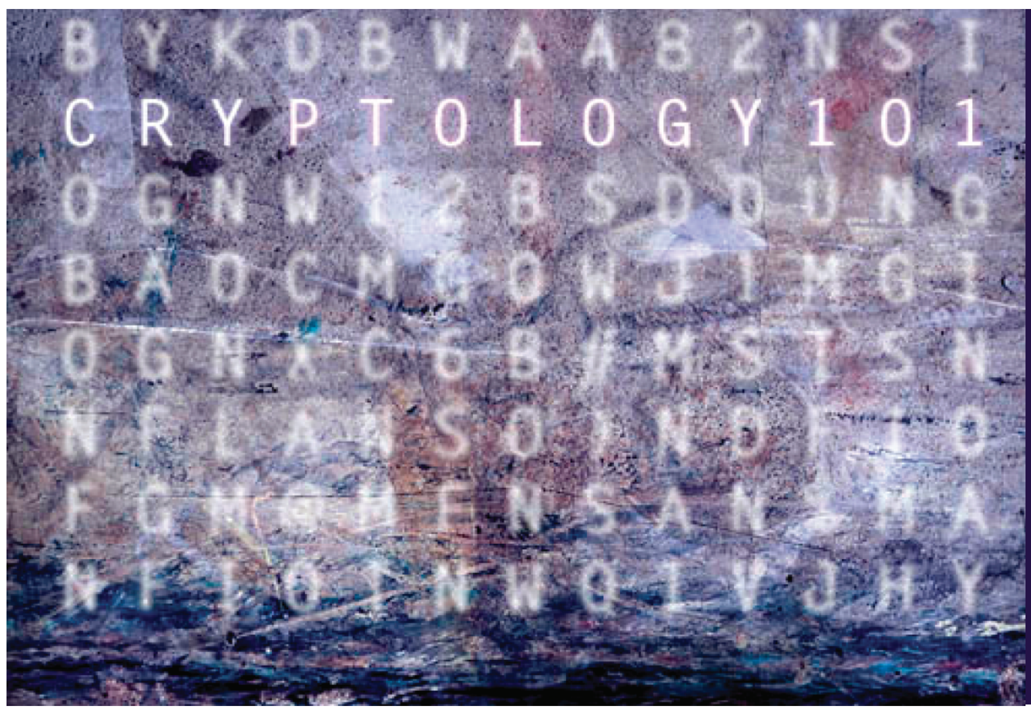

# 2009 NIMS Hot Topics Workshop on Mathematical Cryptology

## June 16-18, 2009
## Hotel Riviera, Daejeon, Korea

www.nims.re.kr/workshop/crypto2009

## • INVITED SPEAKERS

**Kristin Lauter (Microsoft), USA**
Optimizations for Elliptic Curve and Pairing-based Cryptography with the Application to Signatures for Networking Coding

**Kanta Matsuura (Tokyo University), Japan**
Economics of Provable Security and Probable Security

**Pascal Paillier (Gemalto), France**
The Provable Security of Asymmetric Privacy and Authenticity: Definitions, Design Methodologies, Proof Techniques and Related Issues

**Ik Rae Jeong (Korea University), Korea**
Privacy-Preserving Operations on Data

**Nam-Su Jho (ETRI), Korea**
Searchable Symmetric Encryption

**Seungjoo Kim (Sungkyunkwan University), Korea**
The Gap between Theory and Reality

**Daesung Kwon (ETRI), Korea**
Current Issues on Cryptographic Primitives

## • ORGANIZING COMMITTEE

Soonhak Kwon, Chair (Sungkyunkwan Univ.)
Jung Hee Cheon (Seoul National Univ.)
Sang Geun Hahn (KAIST)
Seokhie Hong (Korea Univ.)
Hyang-Sook Lee (Ewha Womans Univ.)
Hyungju Park (KIAS)
Kyung-Ah Shim (NIMS)
Hong-Yeop Song (Yonsei Univ.)
Yongjin Yeom (ETRI)

## • HOSTED BY

National Institute for Mathematical Sciences, Korea

## • SPONSORED BY

Division of Cryptography, KMS, Korea
SRC, KAIST, Korea
KIAS, Korea

**National Institute for Mathematical Sciences**