Workshop
8th International ISC Conference of Information Security and Cryptology
http://iscisc2011.um.ac.ir

1. **Workshop Code: W01**
2. **Title: Provably Secure Shared-Key Encryption**
3. **Abstract:** Once a tool only for making quite theoretical claims in cryptography, reductions have become the central tool for the design and analysis of practical cryptographic schemes for intermediate-level primitives. This tutorial will explore the reduction-based treatment for blockcipher modes of operation, especially schemes for symmetric (that is, shared-key) encryption. We will explore a variety of formalizations for symmetric encryption, as well as means for provably achieving them, always starting from the assumed existence of a secure blockcipher. While much of what I describe will be fairly classical, I will also include some newer topics, like the FFX scheme for format-preserving encryption and the authenticated-encryption mode OCB3.

4. **Provider:**

Name	Last Degree	Field	Job Title	Affiliation	Email
Phillip Rogaway	PhD	Electrical Engineering and Computer Science	Academic Staff	University of California, Davis, USA	rogaway@cs.ucdavis.edu

5. **Biography:** Professor Phillip Rogaway is a cryptographer at the University of California, Davis. He did his undergraduate at UC Berkeley and his Ph.D. at MIT. He next worked at IBM as a Security Architect, where he became interested in the problem of developing a theory for cryptography that would be useful, and used, for actual cryptographic practice. In a body of work done in large part with Mihir Bellare, Rogaway developed what has been called "practice-oriented provable security." For this body of work Rogaway is the recipient an ACM Kanellakis Theory and Practice Award. More than 14,000 papers reference Rogaway's academic work, and standardized cryptographic schemes that he co-invented include CMAC, DHIES, EME, OAEP, OCB, PSS, UMAC, and XTS. Interested in social and ethical issues surrounding technology, Rogaway regularly teaches a class on this subject. Prof. Rogaway recently completed his work as Program Chair for CRYPTO 2011..

6. **Time: Tuesday – September 13, 2011 – 8 – 12 AM**