DEPARTMENT OF MATHEMATICS AND COMPUTER SCIENCE
UNIVERSITY OF SOUTHERN DENMARK, ODENSE

COMPUTER SCIENCE COLLOQUIUM

Privacy-preserving Electronic Transactions

Rene Peralta
Computer Security Division
National Institute of Standards and Technology , USA

Tuesday, 01 November, 2011 at 14:15
Auditorium U143

Abstract:

A possible component of the US National Strategy for Trusted Identities in Cyberspace (NSTIC) would encode identity as a set of encrypted attribute certificates. The user would protect his/her identity during an electronic transaction by selectively disclosing arbitrary predicates of these attributes. Additively homomorphic encryption systems can be used to selectively disclose linear predicates (over GF2). Doing the same for non-linear predicates is harder. I will discuss this problem and propose a Web service to help streamline one-prover transactions of this type.

Host: Joan Boyar