FACULTAD DE CIENCIAS
FÍSICAS Y MATEMÁTICAS
UNIVERSIDAD DE CHILE

CMM
Center for
Mathematical
Modeling

cmm.uchile.cl

Beauchef 851, edificio norte, piso 7
Santiago, CHILE
CP 837 0456

tel +56 2 2978 4870

Seminario AGCO

Author: Andrew Xia, MIT.

Title: Efficient Implementation of a Practical Leakage-Resilient ID Scheme

Abstract:

Instead of viewing cryptographic algorithms as simple black-boxes, leakage-resilient cryptography accepts that certain traditionally secret parts of the algorithm will be available to the attacker through side channel attacks and aims to ensure the security of these algorithms in the presence of such leakage. We present a leakage resilient identification scheme based on the continuous memory leakage model, which assumes that the leakage of information is unrestricted in time and space. We design a three message sigma protocol, secure under the symmetric external diffie-hellman (SXDH) assumption, using pairings-based elliptic curve cryptography.

This is joint work with Chiraag Juvekar, Utsav Banerjee, Yael Kalai, and Anantha Chandrakasan.

I will present this talk such that minimal background with cryptography is necessary.

Where: Av República 701, Sala 33.

When: Wednesday, June 12, 14:30.

CONICYT
Ministerio de Educación
Gobierno de Chile

cnrs