Cryptography
(Org: **Bruce Kapron** (University of Victoria))

BRUCE KAPRON, University of Victoria
Co-induction and Computational Semantics for Public-key Encryption with Key Cycles

Micciancio recently has shown that with a co-inductive definition of indistinguishability it is possible to obtain computational soundness for private-key cryptography in the presence of key cycles. We explore co-inductive definitions of security in public-key cryptography, and extend a soundness result of Herzog to key-cyclic expressions. We also show that a completeness result is achievable in the absence of key cycles with respect to any length-revealing encryption system. (Joint work with M. Hajiabadi)

YASSINE LAKHNECH, University of Grenoble, CNRS - VERIMAG
Computational Indistinguishability Logic

Computational Indistinguishability Logic is a logic for reasoning about cryptographic primitives in computational models. It captures reasoning patterns that are common in provable security, such as simulations and reductions. CIL is sound for the standard model, but also supports reasoning in the random oracle and other idealized models. We illustrate the benefits of CIL by discussing several case studies.

REI SAFAVI-NAINI, University of Calgary
cryptographic keys from noisy channels

In Secure Key Establishment (SKE) problem, Alice and Bob want to share a secure key by communicating over a pair of noisy channels that leak information to Eve. We assume parties do not have any other sources of randomness. We derive lower and upper bounds on the secret key capacity of this setup and show that SKE is possible even if in both channels, Eve has a less noisy reception than Alice and Bob's.

ANDRE SCEDROV, University of Pennsylvania
Bounded memory Dolev-Yao adversaries

We investigate how much damage can be done by insiders alone, without collusion with an outside adversary. All the players inside our system, including potential adversaries, have similar capabilities. They have bounded storage capacity. We investigate the complexity of the decision problem of whether or not an adversary is able to discover secret data. We show that this problem is PSPACE-complete. Joint work with M. Kanovich, T. Ban Kirigin, and V. Nigam.