Speaker: Juan A. Garay, AT&T Labs - Research

Title: Secure Computation and the Combinatorics of Hidden Diversity

In the setting of cryptographic protocols, the corruption of a party has been viewed as a simple, uniform and atomic operation, where the adversary decides to get control over a party and this party immediately gets corrupted. In this paper, motivated by the fact that different players may require different resources to get corrupted, we put forth the notion of *resource-based corruptions*, where the adversary must invest some resources in order to do so.

If the adversary has full information about the system configuration then resource-based corruptions would provide no fundamental difference from the standard corruption model. However, in a resource "anonymous" setting, in the sense that such configuration is hidden from the adversary, much is to be gained in terms of efficiency and security.

We showcase the power of such *hidden diversity* in the context of secure multiparty computation (MPC) with resource-based corruptions and prove that it can effectively be used to circumvent known impossibility results.
Specifically, if OPT is the corruption budget that violates the completeness of MPC (the case when half or more of the players are corrupted), we show that if hidden diversity is available, the completeness of MPC can be made to hold against an adversary with as much as a B*OPT budget, for any constant B > 1. This result requires a suitable choice of parameters (in terms of number of players and their hardness to corrupt), which we provide and further prove other tight variants of the result when the said choice is not available. Regarding efficiency gains, we show that hidden diversity can be used to force the corruption threshold to drop from 1/2 to 1/3, in turn allowing the use of much more efficient (information-theoretic) MPC protocols.

We achieve the above through a series of technical contributions:

(1) The formulation of the notion of {\em inversion effort preserving} (IEP) functions which is a type of direct-sum property, and the property of *hardness indistinguishability*. While hardness indistinguishability enables the dissociation of parties' identities and the resources needed to corrupt them, IEP enables the discretization of adversarial work into corruption tokens;

(2) the modeling of the corruption process in the setting of MPC through *corruption oracles* as well as the introduction of a notion of reduction to relate such oracles;

(3) the abstraction of the corruption game as a combinatorial problem and its analysis,

all of which may be of independent interest.

This is joint work with Aggelos Kiayias, David Johnson and Moti Yung.