

Department of Applied Mathematics and Statistics  
The Johns Hopkins University

SEMINAR

Christian Scheideler  
Department of Computer Science  
The Johns Hopkins University

March 3, 2005  
304 Whitehead Hall  
Refreshments: 3:30 p.m.  
Seminar: 4:00 p.m.

**ADVERSARIAL MIXING THEORY**  
**Or: How to Keep a System Mixed Under Adversarial Behavior**

ABSTRACT

Consider the following simple game. There are  $n$  white pebbles and  $\epsilon n$  black pebbles, for some fixed constant  $\epsilon < 1$ . Initially, all of the white pebbles are laid down in a ring, and the adversary has all of the black pebbles in its bag. In each round, the adversary can look at the entire ring and can choose to add a black pebble to the ring (if its bag is not empty) or to take any black pebble from the ring and put it back into its bag (i.e., we allow adaptive adversaries). However, the adversary cannot place a black pebble into any position it likes. This is handled by a join strategy to be specified by the system. The goal is to find an oblivious join strategy, i.e., a strategy that cannot distinguish between the white and black pebbles in the ring, that integrates the black pebbles into this ring and may do some further rearrangements so that for a polynomial number of rounds the adversary will not manage to include its black pebbles into the ring so that there is a sequence of  $s = \Theta(\log n)$  consecutive pebbles in which at least half of the pebbles are black. If this is achieved by the join strategy, it wins. Otherwise, the adversary wins.

This game is very important for the area of proactive security and systems of mutually untrusting nodes such as peer-to-peer systems, as its solution allows for the design of systems that are scalable and robust against adversarial behavior.

We will discuss efficient mixing strategies for this and related games and show how to prove that they can indeed keep the system in a sufficiently mixed state even under adversarial behavior.