DEPARTMENT OF MATHEMATICS AND COMPUTER SCIENCE
ODENSE UNIVERSITY

COMPUTER SCIENCE COLLOQUIUM

Ripping Coins for a Fair Exchange

Markus Jakobsson
Department of Computer Science and Engineering
University of California at San Diego

Tuesday, May 30, 1995, at 2:15 PM
The Seminar Room

Abstract: A fair exchange of payments for goods and services is a barter where one of the parties cannot obtain the item desired without handing over the item he offered. We introduce the concept of ripping digital coins to solve fairness problems in payment transactions. We demonstrate how to implement coin ripping for a recently proposed payment scheme, giving a practical and transparent coin ripping scheme. We then give a general solution that can be used in any payment scheme with a challenge. We also indicate how fairness can be obtained by building a contract into the coin.

During the first part of the talk, basic digital cash issues will be presented along with the cryptographic primitives to be used; the second part will consist of the above mentioned coin ripping issues.

Joan F. Boyar