Department of Mathematics, Statistics and Computer Science
St. Francis Xavier University
Presents

Toward Fairness in Electronic Exchange

By
Hao Wang
Postdoctoral Fellow
Dept. of Math/Stats/CS
St. Francis Xavier University
Monday, March 31st, 2008 at 2:15pm in Annex 23a

Have you been using *PayPal* when paying online? It is a typical form of electronic exchange over the Internet. And there are more, you may want to reach an agreement with exchange of signatures on the electronic contract document; you may wish to get a receipt when you are sending out a certified email containing a very important message. Deceptions may occur in electronic exchanges, just as deception happens all the time in traditional face-face exchanges. Additionally, cheating in distributed network can be much more difficult to trace and prevent.

To prevent some forms of cheating behavior and protect impartial interests, fairness must be achieved in all kinds of electronic exchange. Over the past two decades, many fair exchange protocols have been proposed. In these protocols, a Trusted Third Party (TTP) is often used. For example, the PayPal company is a TTP, it is entrusted with money and it handles customers' payment with merchants. But a well known criticism of PayPal is that it may intentionally delay the payment procedure so as to earn more interests out of the customers' deposits. This is a basic principle in designing security protocols: attacks always exist!

Why not just drop these preventative methods? Let's try an incentive method. The recently proposed Mechanism Design is of particular interest (in our opinion). Based on game theory in Economics, it takes into account the gains and costs in the exchange, and tries to find a balance so that both parties can get maximum benefit only when they successfully finish their exchange, that is, there is no motive for either party to cheat!

This one-hour talk will give you some basic ideas about different approaches and various problems when moving towards fairness.

Refreshments will be served before the talk in AX24A