Much more relaxed atmosphere on Day 3

KUCHING: Day 3 of the International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT) 2007 here yesterday was a much more relaxed atmosphere with participants and speakers loosening up and approaching each other to exchange ideas and views.

The rump session held the previous night must have been the ice-breaker as many were spotted casually talking with their notebook computers or their laptops, discussing topics related to Cryptography and other computer-related matters.

Yesterday's session kicked off with a paper on Known-Key Distinguishers for Some Block Ciphers by Lars R Knudsen (Technical University of Denmark) and Vincent Rijmen (Graz University of Technology, Austria).

This proceeded with Generic Attacks on Unbalanced Feistel Schemes with Expanding Functions by a group of researchers from three universities in France.

Researchers from College of

William and Mary and Johns Hopkins University then presented their paper On Tweaking Luby-Rackoff Ciphers.

Next, in the multiparty computation II session, there were papers on Secure Protocols with Asymmetric Trust, Simple and Efficient Perfectly-Secure Asynchronous MPC, Efficient Byzantine Agreement with Faulty Minority and Information-theoretic Security without an Honest Majority.

After lunch break, Ueli Maurer and Dominik Raub (ETH Zürich) talked on Black-Box Extension Fields and the Inexistence of Field-Homomorphic One-Way Permutations.

They were followed by Vipul Goyal, Ryan Moriarty, Rafail Ostrovsky and Amit Sahai (UCLA) who presented Concurrent Statistical Zero-Knowledge Arguments for NP from One Way Functions.

This was ended with Anonymous Quantum Communication by researchers from Université de Montréal.

A noted cryptographer from Japan, Dr Tatsuaki Okamoto from 3G mobile phone giants NTT then presented a keynote talk on Authenticated Key Exchange and Key Encapsulation in the Standard Model.

A meeting by members of the International Association for Cryptologic Research (IACR) then ensued, before attendees took some time off to refresh themselves for the Banquet hosted by the State government last night.