Signature Schemes for Network Coding

Simon R. Blackburn

Royal Holloway

The aim of a secure network coding signature scheme is to prevent malicious nodes from flooding a network with incorrect packets, by requiring each packet to be accompanied by a valid digital signature. The digital signature scheme must be specially designed so that the modified packets forwarded by intermediate nodes can be accompanied by appropriate signatures.

Boneh, Freeman, Katz and Waters provided a precise definition of a secure network coding signature scheme, providing a rigorous setting to analyse the network coding signature schemes of Krohn, Freedman and Mazires, and of Charles, Jain and Lauter. This talk will provide a brief introduction to the area, focussing on these three papers.

Department of Mathematics, Royal Holloway, University of London, Egham, Surrey TW20 0EX, United Kingdom
S.Blackburn@rhul.ac.uk