We present a practical digital signature scheme to be used in conjunction with network coding. Our scheme simultaneously provides authentication and detects malicious nodes that intentionally corrupt content on the network.

Following the important work of Ahlswede *et al* and Li *et al*, network coding has been established as a viable alternative to the store and forward mechanisms used in peer-to-peer networks. However, network coding is inherently vulnerable to pollution attacks by malicious nodes in the network. The pollution of packets spreads quickly since the output of (even an) honest node is corrupted if at least one of the incoming packets is corrupted. The question of how to prevent pollution attacks in the network coding scheme remained open and was the subject of the paper by Krohn *et al* in the generalized setting of rateless erasure codes. They show that a construction based on homomorphic hashing works to detect the polluted packets. This scheme, however, assumes that there is a separate secure channel which is used to transmit the hash values of the packets to all the nodes.

In this paper we propose a different solution to the problem of detecting pollution attacks. We design a new *homomorphic* signature scheme for use with network coding. The homomorphic property of the signatures allows nodes to sign any linear comination of the incoming packets without contacting the signing authority. At first glance one might think that this is a weakness of the signature scheme. This is not so, in our scheme it is computationally infeasible for a node to sign a linear combination of the packets without disclosing what linear combination was used in the generation of the packet. Furthermore, we can prove that the signature scheme is secure under well known cryptographic assumptions of the hardness of the Discrete-Log problem and the computational co-Diffie-Hellman problem on elliptic curves. Our scheme has a three-fold advantage over the scheme based on homomorphic hashing: Firstly, we do not need to securely transmit hash values of the packets that the source transmits; secondly, since our scheme is based on elliptic curves smaller security parameters suffice and this translates to improved efficiency since the bit lengths involved are smaller; finally, our scheme provides authentication of the data in addition to detecting pollution of packets.