Cryptology ePrint Archive: Report 2011/696

Efficient Network Coding Signatures in the Standard Model

Dario Catalano and Dario Fiore and Bogdan Warinschi

Abstract: Network Coding is a routing technique where each node may actively modify the received packets before transmitting them. While this departure from passive networks improves throughput and resilience to packet loss it renders transmission susceptible to {\em pollution attacks} where nodes can misbehave and change in a malicious way the messages transmitted. Nodes cannot use standard signature schemes to authenticate the modified packets: this would require knowledge of the original sender's signing key. Network coding signature schemes offer a cryptographic solution to this problem. Very roughly, such signatures allow signing vector spaces (or rather bases of such spaces). Furthermore, these signatures are homomorphic: given signatures on a set of vectors it is possible to create signatures for any linear combination of these vectors. Designing such schemes is a difficult task, and the few existent constructions either rely on random oracles or are rather inefficient. In this paper we introduce two new network coding signature schemes. Both of our schemes are provably secure in the standard model, rely on standard assumptions, {\em and} are in the same efficiency class with previous solutions based on random oracles.

Category / Keywords: public-key cryptography / digital signatures, network coding

Publication Info: Full version of the paper appeared in the proceedings of PKC 2012

Date: received 21 Dec 2011, last revised 14 Mar 2012

Contact author: fiore at cs nyu edu