

authors D. Berbecaru, L. Albertalli, A. Lioy
title The ForwardDiffSig scheme for multicast authentication
journal IEEE/ACM Transactions on Networking
ISSN 1063-6692
issue Vol. 18, No. 6, December 2010
pages 1855-1868
DOI [10.1109/TNET.2010.2052927](https://doi.org/10.1109/TNET.2010.2052927)

abstract This paper describes ForwardDiffSig, an efficient scheme for multicast authentication with forward security. This scheme provides source authentication, data integrity, and non-repudiation since it is based on the use of asymmetric cryptography. At the same time, it offers also protection against key exposure as it exploits OptiSum, our optimized implementation of the ISum forward-secure signature scheme. A tradeoff exists in the used keys: Short keys provide speed at the signer, whereas long keys are preferable for long-term non-repudiation. Performance has been evaluated with a custom packet simulator and shows that, by grouping the packets, ForwardDiffSig is efficient in terms of speed even for long keys at the price of a significant signature overhead. Therefore, ForwardDiffSig is fast, exhibits low delay, and provides non-repudiation and protection against key exposure, but has a nonnegligible impact in applications with strict energy or bandwidth constraints.