[Article] The ForwardDiffSig scheme for multicast authentication

Original Citation:

Availability:
This version is available at: http://porto.polito.it/2370848/ since: July 2010

Publisher:
IEEE

Published version:
DOI:10.1109/TNET.2010.2052927

Terms of use:
This article is made available under terms and conditions applicable to Open Access Policy Article ("Public - All rights reserved"), as described at http://porto.polito.it/terms_and_conditions.html

Porto, the institutional repository of the Politecnico di Torino, is provided by the University Library and the IT-Services. The aim is to enable open access to all the world. Please share with us how this access benefits you. Your story matters.

(Article begins on next page)
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.