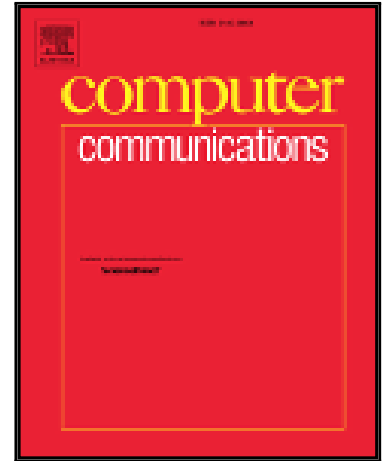


Accepted Manuscript

Group Key Management with Efficient Rekey Mechanism: A Semi-Stateful Approach for Out-of-Synchronized Members

Yi-Ruei Chen, Wen-Guey Tzeng

PII: S0140-3664(16)30289-4
DOI: [10.1016/j.comcom.2016.08.001](https://doi.org/10.1016/j.comcom.2016.08.001)
Reference: COMCOM 5365



To appear in: *Computer Communications*

Received date: 29 January 2016
Revised date: 15 June 2016
Accepted date: 3 August 2016

Please cite this article as: Yi-Ruei Chen, Wen-Guey Tzeng, Group Key Management with Efficient Rekey Mechanism: A Semi-Stateful Approach for Out-of-Synchronized Members, *Computer Communications* (2016), doi: [10.1016/j.comcom.2016.08.001](https://doi.org/10.1016/j.comcom.2016.08.001)

This is a PDF file of an unedited manuscript that has been accepted for publication. As a service to our customers we are providing this early version of the manuscript. The manuscript will undergo copyediting, typesetting, and review of the resulting proof before it is published in its final form. Please note that during the production process errors may be discovered which could affect the content, and all legal disclaimers that apply to the journal pertain.

Group Key Management with Efficient Rekey Mechanism: A Semi-Stateful Approach for Out-of-Synchronized Members

Yi-Ruei Chen, Wen-Guey Tzeng

Department of Computer Science, National Chiao Tung University, Taiwan, 30010

Abstract

This paper addresses the problem of managing a cryptographic group key among a large and highly dynamic group of members, who may miss group key update (rekey) messages frequently. We propose two provably-secure and practical schemes: *KeyDer-GKM* and *ReEnc-GKM*. The rekey process in these schemes has an $O(\log N)$ rekey message and $O(\log N)$ computation and storage cost for a member, where N is the number of group members. Moreover, our schemes have the following distinct features. (1) Each member is given only one private key and $O(\log N)$ public information. The private key remains unchanged during the membership period. For the public information, a member can hold them locally and update accordingly from each rekey message, or get them from a public bulletin if needed. (2) The size of published information is $O(N)$ no matter how many rekey processes occur. The computation cost for a member, who has missed some rekey messages, to compute the up-to-date group key is always $O(\log N)$ no matter how many rekey messages have been missed.

Our *KeyDer-GKM* scheme is very efficient since it can be implemented by using hash and XOR functions only. Our *ReEnc-GKM* scheme allows a member to reduce the cost of computing the up-to-date group key to one decryption by outsourcing $\log N$ operations. Both of our schemes are shown immune to the collusion attacks. For *KeyDer-GKM*, a set of collusive members cannot recover an unauthorized group key. For *ReEnc-GKM*, a set of collusive members cannot distinguish an unauthorized group key from a

Email addresses: yrchen.cs98g@nctu.edu.tw (Yi-Ruei Chen),
wgtzeng@cs.nctu.edu.tw (Wen-Guey Tzeng)

Download English Version:

<https://daneshyari.com/en/article/4954482>

Download Persian Version:

<https://daneshyari.com/article/4954482>

[Daneshyari.com](https://daneshyari.com)