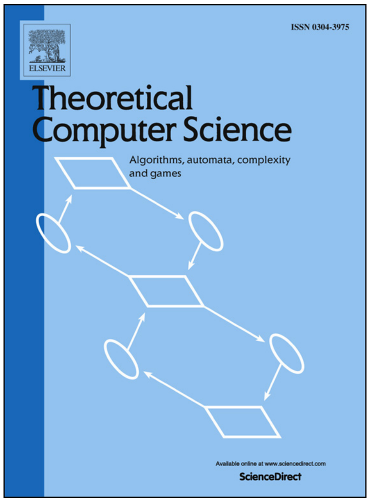
ISSN 0304-3975
ELSEVIER
Theoretical Computer Science
Algorithms, automata, complexity and games
Available online at www.sciencedirect.com
ScienceDirect

Group rekeying in the exclusive subset-cover framework

Jing Liu, Minmin Liu, Changji Wang, Shaowen Yao

PII: S0304-3975(17)30285-2
DOI: http://dx.doi.org/10.1016/j.tcs.2017.03.046
Reference: TCS 11153

To appear in: *Theoretical Computer Science*

Received date: 2 April 2015
Revised date: 11 March 2017
Accepted date: 15 March 2017

Please cite this article in press as: J. Liu et al., Group rekeying in the exclusive subset-cover framework, *Theoret. Comput. Sci.* (2017), http://dx.doi.org/10.1016/j.tcs.2017.03.046

Group Rekeying in the Exclusive Subset-Cover Framework

Jing Liu, Minmin Liu, Changji Wang, Shaowen Yao

Abstract — *Group Rekeying* deals with the problem about how to efficiently and securely distribute a new group key *GK* to remaining legitimate users when there are changes in group membership (join/leave). Given a universe *U* of *n* users, an *exclusive key* K_S for an arbitrary subset $S \subset U$ is a long-term key shared by all users in $U \setminus S$. Hence we can distribute a new group key *GK* encrypted under K_S such that all users in *U* except those in *S* can decrypt it during group rekeying. This method allows us to exclude *S* from the group with a rekey message whose length is just one single encrypted key. In this paper, we use this idea to extend the famous *Subset-Cover Framework* to obtain its exclusive version — *Exclusive Subset-Cover Framework*. We provide sufficient conditions that guarantee the security of any stateless group rekeying protocol in this framework. We propose a concrete exclusive subset-cover protocol called *exclusive complete subtree protocol*. Compared with existing 1-resilient stateless group rekeying protocols, this protocol achieves not only constant communication overhead but also better computational efficiency as well as better collusion resistance. From this protocol, it is easy to obtain a 1-resilient stateful group rekeying protocol which also outperforms the existing 1-resilient stateful protocols. Recent researches have proved some lower bounds on the communication complexity of group rekeying protocols. These bounds suggest that it is impossible to achieve a lower communication overhead without trading off some degree of collusion resistance. However, there are application scenarios which require communication overhead below these bounds. We show that any 1-resilient stateless group rekeying protocol with constant communication overhead can be used in tandem with a Subset-Cover based protocol to construct a hybrid protocol with tunable collusion-bandwidth tradeoffs.

Index Terms — multicast key distribution, group rekeying, broadcast encryption, 1-resilient, collusion resistant

1 Introduction

In this section, we first make a brief survey of research on group rekeying. Then we clarify the meaning of research on 1-resilient group rekeying protocols by showing their potential applications.

1.1 A Brief Survey on Group Rekeying

Recent years have seen the rise of a large variety of group-oriented applications, for instance, pay-per-view, Pay-TV, DVB (Digital Video Broadcast), audio/video conferences, massive multiplayer online game, collaborative applications, stock quote streaming and so on. For some group-oriented applications like stock quote streaming, providing a security guarantee of data authenticity will suffice. However, for the other applications like pay-per-view, Pay-TV, audio/video conferences, providers would like to limit content distribution to subscribers who paid for the service. Hence providing a security guarantee of confidentiality for group communication is mandatory for these applications. One of the most efficient ways to achieve private

Manuscript received 2015.

- *Jing Liu is with the School of Software, Yunnan University, Kunming 650091, China (e-mail: liujing@ynu.edu.cn).*
- *Minmin Liu is with the Institute of Astronautics & Aeronautic, University of Electronic Science and Technology of China, Chengdu 610054, China (e-mail: liumin_uestc@uestc.edu.cn)*
- *Changji Wang is with Guangdong University of Foreign Studies, Guangzhou, 510006, China (e-mail: wchangji@gmail.com).*
- *Shaowen Yao is with the School of Software, Yunnan University, Kunming 650091, China (e-mail: yaosw@ynu.edu.cn).*