Jooseok Song
Taekyoung Kwon
Moti Yung (Eds.)

LNCS 3786

Information Security Applications

6th International Workshop, WISA 2005
Jeju Island, Korea, August 2005
Revised Selected Papers

Springer

Jooseok Song Taekyoung Kwon
Moti Yung (Eds.)

Information Security Applications

6th International Workshop, WISA 2005
Jeju Island, Korea, August 22-24, 2005
Revised Selected Papers

Springer

Volume Editors

Jooseok Song
Yonsei University
Department of Computer Science
134 Shinchon-Dong, Seodaemun-Gu, Seoul, 120-749, Korea
E-mail: jssong@emerald.yonsei.ac.kr

Taekyoung Kwon
Sejong University
Department of Computer Engineering
98 Gunja-Dong, Kwangjin-Gu, Seoul, 143-747, Korea
E-mail: tkwon@sejong.ac.kr

Moti Yung
RSA Laboratories
and
Computer Science Department, Columbia University
Room 464, S.W. Mudd Building, New York, NY 10027, USA
E-mail: moti@cs.columbia.edu

Library of Congress Control Number: 2006920030

CR Subject Classification (1998): E.3, D.4.6, F.2.1, C.2, J.1, C.3, K.6.5

LNCS Sublibrary: SL 4 – Security and Cryptology

ISSN 0302-9743
ISBN-10 3-540-31012-6 Springer Berlin Heidelberg New York
ISBN-13 978-3-540-31012-9 Springer Berlin Heidelberg New York

Springer is a part of Springer Science+Business Media

springeronline.com

Printed in Germany

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 11604938 06/3142 5 4 3 2 1 0

Lecture Notes in Computer Science 3786

Lecture Notes in Computer Science

For information about Vols. 1–3773

please contact your bookseller or Springer

Vol. 3872: H. Bunke, A. L. Spitz (Eds.), Document Analysis Systems VII. XIII, 630 pages. 2006.

Vol. 3870: S. Spaccapietra, P. Atzeni, W.W. Chu, T. Catarci, K.P. Sycara (Eds.), Journal on Data Semantics V. XIII, 237 pages. 2006.

Vol. 3868: K. Römer, H. Karl, F. Mattern (Eds.), Wireless Sensor Networks. XI, 342 pages. 2006.

Vol. 3863: M. Kohlhase (Ed.), Mathematical Knowledge Management. XI, 405 pages. 2006. (Sublibrary LNAI).

Vol. 3861: J. Dix, S.J. Hegner (Eds.), Foundations of Information and Knowledge Systems. X, 331 pages. 2006.

Vol. 3860: D. Pointcheval (Ed.), Topics in Cryptology – CT-RSA 2006. XI, 365 pages. 2006.

Vol. 3858: A. Valdes, D. Zamboni (Eds.), Recent Advances in Intrusion Detection. X, 351 pages. 2006.

Vol. 3857: M. Fossorier, H. Imai, S. Lin, A. Poli (Eds.), Applied Algebra, Algebraic Algorithms and Error-Correcting Codes. XI, 350 pages. 2006.

Vol. 3855: E. A. Emerson, K.S. Namjoshi (Eds.), Verification, Model Checking, and Abstract Interpretation. XI, 443 pages. 2005.

Vol. 3853: A.J. Ijspeert, T. Masuzawa, S. Kusumoto (Eds.), Biologically Inspired Approaches to Advanced Information Technology. XIV, 388 pages. 2006.

Vol. 3852: P.J. Narayanan, S.K. Nayar, H.-Y. Shum (Eds.), Computer Vision - ACCV 2006, Part II. XXXI, 977 pages. 2005.

Vol. 3851: P.J. Narayanan, S.K. Nayar, H.-Y. Shum (Eds.), Computer Vision - ACCV 2006, Part I. XXXI, 973 pages. 2006.

Vol. 3850: R. Freund, G. Păun, G. Rozenberg, A. Salomaa (Eds.), Membrane Computing. IX, 371 pages. 2006.

Vol. 3848: J.-F. Boulicaut, L. De Raedt, H. Mannila (Eds.), Constraint-Based Mining and Inductive Databases. X, 401 pages. 2006. (Sublibrary LNAI).

Vol. 3847: K.P. Jantke, A. Lunzer, N. Spyratos, Y. Tanaka (Eds.), Federation over the Web. X, 215 pages. 2006. (Sublibrary LNAI).

Vol. 3844: J.-M. Bruel (Ed.), Satellite Events at the MoDELS 2005 Conference. XIII, 360 pages. 2006.

Vol. 3843: P. Healy, N.S. Nikolov (Eds.), Graph Drawing. XVII, 536 pages. 2006.

Vol. 3842: H.T. Shen, J. Li, M. Li, J. Ni, W. Wang (Eds.), Advanced Web and Network Technologies, and Applications. XXVII, 1057 pages. 2006.

Vol. 3841: X. Zhou, J. Li, H.T. Shen, M. Kitsuregawa, Y. Zhang (Eds.), Frontiers of WWW Research and Development - APWeb 2006. XXIV, 1223 pages. 2006.

Vol. 3840: M. Li, B. Boehm, L.J. Osterweil (Eds.), Unifying the Software Process Spectrum. XVI, 522 pages. 2006.

Vol. 3839: J.-C. Filliâtre, C. Paulin-Mohring, B. Werner (Eds.), Types for Proofs and Programs. VIII, 275 pages. 2006.

Vol. 3838: A. Middeldorp, V. van Oostrom, F. van Raamsdonk, R. de Vrijer (Eds.), Processes, Terms and Cycles: Steps on the Road to Infinity. XVIII, 639 pages. 2005.

Vol. 3837: K. Cho, P. Jacquet (Eds.), Technologies for Advanced Heterogeneous Networks. IX, 307 pages. 2005.

Vol. 3836: J.-M. Pierson (Ed.), Data Management in Grids. X, 143 pages. 2006.

Vol. 3835: G. Sutcliffe, A. Voronkov (Eds.), Logic for Programming, Artificial Intelligence, and Reasoning. XIV, 744 pages. 2005. (Sublibrary LNAI).

Vol. 3834: D.G. Feitelson, E. Frachtenberg, L. Rudolph, U. Schwiegelshohn (Eds.), Job Scheduling Strategies for Parallel Processing. VIII, 283 pages. 2005.

Vol. 3833: K.-J. Li, C. Vangenot (Eds.), Web and Wireless Geographical Information Systems. XI, 309 pages. 2005.

Vol. 3832: D. Zhang, A.K. Jain (Eds.), Advances in Biometrics. XX, 796 pages. 2005.

Vol. 3831: J. Wiedermann, G. Tel, J. Pokorný, M. Bieliková, J. Štuller (Eds.), SOFSEM 2006: Theory and Practice of Computer Science. XV, 576 pages. 2006.

Vol. 3829: P. Pettersson, W. Yi (Eds.), Formal Modeling and Analysis of Timed Systems. IX, 305 pages. 2005.

Vol. 3828: X. Deng, Y. Ye (Eds.), Internet and Network Economics. XVII, 1106 pages. 2005.

Vol. 3827: X. Deng, D.-Z. Du (Eds.), Algorithms and Computation. XX, 1190 pages. 2005.

Vol. 3826: B. Benatallah, F. Casati, P. Traverso (Eds.), Service-Oriented Computing - ICSOC 2005. XVIII, 597 pages. 2005.

Vol. 3824: L.T. Yang, M. Amamiya, Z. Liu, M. Guo, F.J. Rammig (Eds.), Embedded and Ubiquitous Computing – EUC 2005. XXIII, 1204 pages. 2005.

Vol. 3823: T. Enokido, L. Yan, B. Xiao, D. Kim, Y. Dai, L.T. Yang (Eds.), Embedded and Ubiquitous Computing – EUC 2005 Workshops. XXXII, 1317 pages. 2005.

Vol. 3822: D. Feng, D. Lin, M. Yung (Eds.), Information Security and Cryptology. XII, 420 pages. 2005.

Vol. 3821: R. Ramanujam, S. Sen (Eds.), FSTTCS 2005: Foundations of Software Technology and Theoretical Computer Science. XIV, 566 pages. 2005.

Vol. 3820: L.T. Yang, X.-s. Zhou, W. Zhao, Z. Wu, Y. Zhu, M. Lin (Eds.), Embedded Software and Systems. XXVIII, 779 pages. 2005.

Vol. 3819: P. Van Hentenryck (Ed.), Practical Aspects of Declarative Languages. X, 231 pages. 2005.

Vol. 3818: S. Grumbach, L. Sui, V. Vianu (Eds.), Advances in Computer Science – ASIAN 2005. XIII, 294 pages. 2005.

Vol. 3817: M. Faundez-Zanuy, L. Janer, A. Esposito, A. Satue-Villar, J. Roure, V. Espinosa-Duro (Eds.), Nonlinear Analyses and Algorithms for Speech Processing. XII, 380 pages. 2006. (Sublibrary LNAI).

Vol. 3816: G. Chakraborty (Ed.), Distributed Computing and Internet Technology. XXI, 606 pages. 2005.

Vol. 3815: E.A. Fox, E.J. Neuhold, P. Premsmit, V. Wuwongse (Eds.), Digital Libraries: Implementing Strategies and Sharing Experiences. XVII, 529 pages. 2005.

Vol. 3814: M. Maybury, O. Stock, W. Wahlster (Eds.), Intelligent Technologies for Interactive Entertainment. XV, 342 pages. 2005. (Sublibrary LNAI).

Vol. 3813: R. Molva, G. Tsudik, D. Westhoff (Eds.), Security and Privacy in Ad-hoc and Sensor Networks. VIII, 219 pages. 2005.

Vol. 3811: C. Bussler, M.-C. Shan (Eds.), Technologies for E-Services. VIII, 127 pages. 2006.

Vol. 3810: Y.G. Desmedt, H. Wang, Y. Mu, Y. Li (Eds.), Cryptology and Network Security. XI, 349 pages. 2005.

Vol. 3809: S. Zhang, R. Jarvis (Eds.), AI 2005: Advances in Artificial Intelligence. XXVII, 1344 pages. 2005. (Sublibrary LNAI).

Vol. 3808: C. Bento, A. Cardoso, G. Dias (Eds.), Progress in Artificial Intelligence. XVIII, 704 pages. 2005. (Sublibrary LNAI).

Vol. 3807: M. Dean, Y. Guo, W. Jun, R. Kaschek, S. Krishnaswamy, Z. Pan, Q.Z. Sheng (Eds.), Web Information Systems Engineering – WISE 2005 Workshops. XV, 275 pages. 2005.

Vol. 3806: A.H. H. Ngu, M. Kitsuregawa, E.J. Neuhold, J.-Y. Chung, Q.Z. Sheng (Eds.), Web Information Systems Engineering – WISE 2005. XXI, 771 pages. 2005.

Vol. 3805: G. Subsol (Ed.), Virtual Storytelling. XII, 289 pages. 2005.

Vol. 3804: G. Bebis, R. Boyle, D. Koracin, B. Parvin (Eds.), Advances in Visual Computing. XX, 755 pages. 2005.

Vol. 3803: S. Jajodia, C. Mazumdar (Eds.), Information Systems Security. XI, 342 pages. 2005.

Vol. 3802: Y. Hao, J. Liu, Y.-P. Wang, Y.-m. Cheung, H. Yin, L. Jiao, J. Ma, Y.-C. Jiao (Eds.), Computational Intelligence and Security, Part II. XLII, 1166 pages. 2005. (Sublibrary LNAI).

Vol. 3801: Y. Hao, J. Liu, Y.-P. Wang, Y.-m. Cheung, H. Yin, L. Jiao, J. Ma, Y.-C. Jiao (Eds.), Computational Intelligence and Security, Part I. XLI, 1122 pages. 2005. (Sublibrary LNAI).

Vol. 3799: M. A. Rodríguez, I.F. Cruz, S. Levashkin, M.J. Egenhofer (Eds.), GeoSpatial Semantics. X, 259 pages. 2005.

Vol. 3798: A. Dearle, S. Eisenbach (Eds.), Component Deployment. X, 197 pages. 2005.

Vol. 3797: S. Maitra, C. E. V. Madhavan, R. Venkatesan (Eds.), Progress in Cryptology - INDOCRYPT 2005. XIV, 417 pages. 2005.

Vol. 3796: N.P. Smart (Ed.), Cryptography and Coding. XI, 461 pages. 2005.

Vol. 3795: H. Zhuge, G.C. Fox (Eds.), Grid and Cooperative Computing - GCC 2005. XXI, 1203 pages. 2005.

Vol. 3794: X. Jia, J. Wu, Y. He (Eds.), Mobile Ad-hoc and Sensor Networks. XX, 1136 pages. 2005.

Vol. 3793: T. Conte, N. Navarro, W.-m.W. Hwu, M. Valero, T. Ungerer (Eds.), High Performance Embedded Architectures and Compilers. XIII, 317 pages. 2005.

Vol. 3792: I. Richardson, P. Abrahamsson, R. Messnarz (Eds.), Software Process Improvement. VIII, 215 pages. 2005.

Vol. 3791: A. Adi, S. Stoutenburg, S. Tabet (Eds.), Rules and Rule Markup Languages for the Semantic Web. X, 225 pages. 2005.

Vol. 3790: G. Alonso (Ed.), Middleware 2005. XIII, 443 pages. 2005.

Vol. 3789: A. Gelbukh, Á. de Albornoz, H. Terashima-Marín (Eds.), MICAI 2005: Advances in Artificial Intelligence. XXVI, 1198 pages. 2005. (Sublibrary LNAI).

Vol. 3788: B. Roy (Ed.), Advances in Cryptology - ASIACRYPT 2005. XIV, 703 pages. 2005.

Vol. 3787: D. Kratsch (Ed.), Graph-Theoretic Concepts in Computer Science. XIV, 470 pages. 2005.

Vol. 3786: J. Song, T. Kwon, M. Yung (Eds.), Information Security Applications. XI, 378 pages. 2006.

Vol. 3785: K.-K. Lau, R. Banach (Eds.), Formal Methods and Software Engineering. XIV, 496 pages. 2005.

Vol. 3784: J. Tao, T. Tan, R.W. Picard (Eds.), Affective Computing and Intelligent Interaction. XIX, 1008 pages. 2005.

Vol. 3783: S. Qing, W. Mao, J. Lopez, G. Wang (Eds.), Information and Communications Security. XIV, 492 pages. 2005.

Vol. 3782: K.-D. Althoff, A. Dengel, R. Bergmann, M. Nick, T.R. Roth-Berghofer (Eds.), Professional Knowledge Management. XXIII, 739 pages. 2005. (Sublibrary LNAI).

Vol. 3781: S.Z. Li, Z. Sun, T. Tan, S. Pankanti, G. Chollet, D. Zhang (Eds.), Advances in Biometric Person Authentication. XI, 250 pages. 2005.

Vol. 3780: K. Yi (Ed.), Programming Languages and Systems. XI, 435 pages. 2005.

Vol. 3779: H. Jin, D. Reed, W. Jiang (Eds.), Network and Parallel Computing. XV, 513 pages. 2005.

Vol. 3778: C. Atkinson, C. Bunse, H.-G. Gross, C. Peper (Eds.), Component-Based Software Development for Embedded Systems. VIII, 345 pages. 2005.

Vol. 3777: O.B. Lupanov, O.M. Kasim-Zade, A.V. Chaskin, K. Steinhöfel (Eds.), Stochastic Algorithms: Foundations and Applications. VIII, 239 pages. 2005.

Vol. 3776: S.K. Pal, S. Bandyopadhyay, S. Biswas (Eds.), Pattern Recognition and Machine Intelligence. XXIV, 808 pages. 2005.

Vol. 3775: J. Schönwälder, J. Serrat (Eds.), Ambient Networks. XIII, 281 pages. 2005.

Vol. 3774: G. Bierman, C. Koch (Eds.), Database Programming Languages. X, 295 pages. 2005.

¥410.00元

Preface

The 6th International Workshop on Information Security Applications (WISA 2005) was held on Jeju Island, Korea, during August 22–24, 2005. The workshop was sponsored by the Korea Institute of Information Security and Cryptology (KIISC), the Electronics and Telecommunications Research Institute (ETRI) and the Ministry of Information and Communication (MIC).

The aim of the workshop is to serve as a forum for new conceptual and experimental research results in the area of information security applications, with contributions from the academic community as well as from industry. The workshop program covers a wide range of security aspects including network security, e-commerce, cryptography, cryptanalysis, applications and implementation aspects.

The Program Committee received 168 papers from 17 countries, and accepted 29 papers for a full presentation track and 16 papers for a short presentation track. Each paper was carefully evaluated through a peer-review process by at least three members of the Program Committee. This volume contains revised versions of 29 papers accepted and presented in the full presentation track. Short papers only appeared in the WISA 2005 pre-proceedings as preliminary versions, and their extended versions may be published elsewhere.

In addition to the contributed papers, the workshop had five special talks. Moti Yung gave a tutorial talk, entitled "Malware Meets Cryptography." Virgil Gligor and Michel Abdalla gave invited talks in the full presentation track, entitled "On the Evolution of Adversary Models in Security Protocols" and "Public-Key Encryption with Keyword Search," respectively. Finally, Shozo Naito and Jonguk Choi gave invited talks in the short presentation track, entitled "New RSA-Type Public-Key Cryptosystem and Its Performance Evaluation" and "A New Booming Era of DRM: Applications and Extending Business," respectively.

Many people helped and worked hard to make WISA 2005 successful. We would like to thank all the individuals involved in the Technical Program and in organizing the workshop. We are very grateful to the Program Committee members and the external referees for their time and efforts in reviewing the submissions and selecting the accepted papers. We also express our special thanks to the Organizing Committee members for making the workshop possible. Finally, we would like to thank all the authors of the submitted papers and the invited speakers for their contributions to the workshop.

December 2005

Jooseok Song
Taekyoung Kwon
Moti Yung

Organization

Advisory Committee

Man Young Rhee	Kyung Hee Univ., Korea
Hideki Imai	Tokyo Univ., Japan
Chu-Hwan Yim	ETRI, Korea
Bart Preneel	Katholieke Universiteit Leuven, Belgium

General Co-chairs

Dae Ho Kim	KIISC, Korea
Sung Won Sohn	ETRI, Korea

Steering Committee

Kil-Hyun Nam	Korea National Defense Univ., Korea
Sang Jae Moon	Kyungpook National Univ., Korea
Dong Ho Won	Sungkyunkwan Univ., Korea
Sehun Kim	KAIST, Korea
Pil-Joong Lee	POSTECH, Korea
Kyo-Il Chung	ETRI, Korea

Organization Committee

Chair:	Im-Yeong Lee	Soonchunhyang Univ., Korea
Finance:	Dong-Il Seo	ETRI, Korea
Publication:	Ji Young Lim	Korean Bible Univ., Korea
Publicity:	Yoo-Jae Won	KISA, Korea
Registration:	Hyun-Gon Kim	Mokpo National Univ., Korea
Treasurer:	Hyung Woo Lee	Hanshin Univ., Korea
Local Arrangements:	Ki-Wook Sohn	NSRI, Korea
	Khi Jung Ahn	Cheju National Univ., Korea

Program Committee

Co-chairs:	Taekyoung Kwon	Sejong Univ., Korea
	Jooseok Song	Yonsei Univ., Korea
	Moti Yung	Columbia Univ., USA
Members:	Michel Abdalla	École Normale Superieure, France
	Dan Bailey	RSA Laboratories, USA

Feng Bao	Institute for Infocomm Research, Singapore
Colin Boyd	Queen's Univ. of Technology, Australia
Emmanuel Bresson	CELAR Technology Center, France
Liqun Chen	Hewlett-Packard, UK
Jung-Hee Cheon	Seoul National Univ., Korea
Kyo-Il Chung	ETRI, Korea
Mathieu Ciet	Gemplus, France
Bruno Crispo	Vrije Universiteit, Netherlands
Paulo D'Arco	Univ. of Salerno, Italy
Shlomi Dolev	Ben-Gurion University, Israel
Seungjoo Kim	Sungkyunkwan Univ., Korea
Yongdae Kim	Univ. of Minnesota at Twin Cities, USA
Chi Sung Laih	National Cheng Kung Univ., Taiwan
Moses Liskov	The College of William and Mary, USA
Kwok-Yan Lam	Tsinghua Univ., China
Dong Hoon Lee	CIST, Korea
Chae Hoon Lim	Sejong Univ., Korea
Javier Lopez	Malaga, Spain
Kanta Matsuura	Tokyo Univ., Japan
Atsuko Miyaji	JAIST, Japan
Fabian Monrose	Johns Hopkins University, USA
Gregory Neven	K.U. Leuven, Belgium
Daehun Nyang	Inha Univ., Korea
Sang-Woo Park	NSRI, Korea
Atul Prakash	Univ. of Michigan, USA
Jaechul Ryu	Chungnam National Univ., Korea
Kouichi Sakurai	Kyushu Univ., Japan
Stuart Schechter	Havard Univ., USA
Hovav Shacham	Stanford University, USA
Yannis C. Stamatiou	University of Ioannina, Greece
Willy Susilo	Univ. of Wollongong, Australia
William Whyte	NTRU System, USA
Yoo-Jae Won	KISA, Korea
Shouhuai Xu	Univ. of Texas, USA
Bulent Yener	Rensselaer Polytechnic Institute, USA
Kee Young Yoo	Kyungpook National University, Korea
Adam Young	MITRE, USA
Jianying Zhou	Institute for Infocomm Research, Singapore

Table of Contents

Security Analysis and Attacks

System Security

Network Security

DRM/Software Security

Efficient HW Implementation

Side-Channel Attacks

Privacy/Anonymity

Efficient Implementation

Security Weakness in Ren et al.'s Group Key Agreement Scheme Built on Secure Two-Party Protocols*

Junghyun Nam, Seungjoo Kim, and Dongho Won

School of Information and Communication Engineering,
Sungkyunkwan University, Republic of Korea
jhnam@dosan.skku.ac.kr, skim@ece.skku.ac.kr, dhwon@dosan.skku.ac.kr

Abstract. A group key agreement protocol is designed to allow a group of parties communicating over an insecure, public network to agree on a common secret key. Recently, in WISA'04, Ren et al. proposed an efficient group key agreement scheme for dynamic groups, which can be built on any of secure two-party key establishment protocols. In the present work we study the main EGAKA-KE protocol of the scheme and point out a critical security flaw in the protocol. We show that the security flaw leads to a vulnerability to an active attack mounted by two colluding adversaries.

Keywords: Group key agreement, key authentication, collusion attack.

1 Introduction

Key establishment protocols are a critical building block for securing electronic communications over an untrusted, open network like the Internet. Even if it is computationally infeasible to break the cryptographic algorithm used, the whole system becomes vulnerable to all manner of attacks if the keys are not securely established. However, the experience has shown that the design of key establishment protocols that are secure against an active adversary is not an easy task to do, especially in a multi-party setting. Indeed, there is a long history of protocols for this domain being proposed and subsequently broken by some active attacks (e.g., [11, 15, 4, 18, 14]). Therefore, key establishment protocols must be subjected to the strictest scrutiny possible before they can be deployed into today's hostile networking environment.

The original idea of extending the two-party Diffie-Hellman scheme [8] to the multi-party setting dates back to the classical paper of Ingemarsson et al. [10], and is followed by many works [6, 2, 17, 12] offering various levels of complexity. Recently, in WISA 2004, Ren et al. [16] proposed an efficient group key agreement scheme for dynamic groups. Instead of building the scheme from the scratch, they

* This work was supported by the University IT Research Center Project funded by the Korean Ministry of Information and Communication.

J. Song, T. Kwon, and M. Yung (Eds.): WISA 2005, LNCS 3786, pp. 1–9, 2006.

construct it by utilizing an existing two-party key establishment protocol that is secure against an active adversary. The scheme consists of two sub-protocols: the key establishment protocol EGAKA-KE and the key update protocol EGAKA-KU. The main EGAKA-KE protocol allows a set of group members to establish a common secret key (called either *group key* or *session key*). The EGAKA-KU protocol aims to efficiently handle dynamic membership changes in the group. In this paper, we uncover a security flaw in the EGAKA-KE protocol and show that the security flaw leads to a vulnerability to an active attack mounted by two colluding adversaries.

2 Preliminaries

The EGAKA-KE protocol is based on a binary key tree structure [13], where every node is either a leaf or a parent of two nodes. The root is located at level 0 and all leaves are at level d or $d-1$, with d being the height of the key tree. Let $\mathcal{G} = \{M_1, \ldots, M_n\}$ be a set of group members wishing to agree on a group key. Group members are arranged at leaves of the tree; all interior nodes are logical nodes hosting no group members. We denote by $N_{l,r}$ the rth node from the left at level l and by $\hat{N}_{l,r}$ the sibling node of $N_{l,r}$. An illustrative example of the considered key tree is given in Fig. 1.

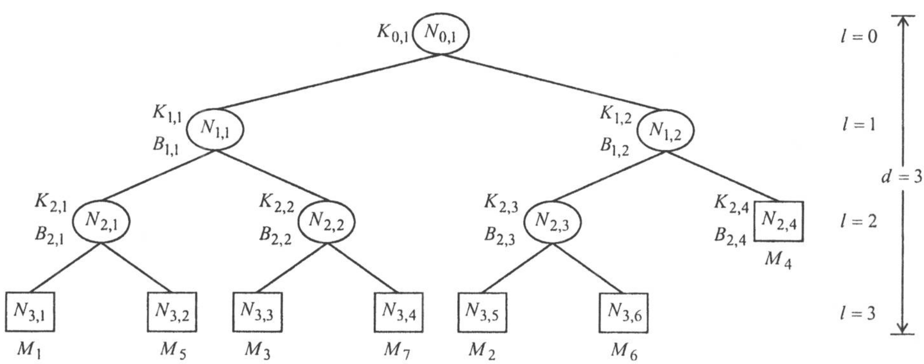

Fig. 1. An illustration of the key tree structure for $\mathcal{G} = \{M_1, \ldots, M_7\}$

Each node $N_{l,r}$, where $l \neq d$, in the key tree is associated with a key pair, the secret key $K_{l,r}$ and its corresponding blinded key $B_{l,r}$. Let $\mathcal{G}_{l,r}$ denote the subgroup consisting of the members in the subtree $T_{l,r}$ rooted at node $N_{l,r}$. Then, the secret key $K_{l,r}$ is shared only by the members in the subgroup $\mathcal{G}_{l,r}$, meaning that the root key $K_{0,1}$ serves as the group key shared by all the members in $\mathcal{G}$. To simplify the protocol description, we introduce some new notations through the following definitions.

Definition 1. *For each proper subtree of the key tree, there is a* designated negotiator (DN) *that is a group member at the leftmost leaf node of the subtree.*

By definition of DN, a group member can be a DN for multiple subtrees (up to d). For example, in Fig. 1, M_2 is the DN for the three subtrees $T_{3,5}$, $T_{2,3}$ and $T_{1,2}$, while M_4 is the DN only for the single-node subtree $T_{2,4}$.

Definition 2. *Let $\hat{T}_{l,r}$ denote the sibling subtree of $T_{l,r}$, i.e., the subtree rooted at $\hat{N}_{l,r}$. Let $M_{l,r}$ and $\hat{M}_{l,r}$ denote the DNs respectively for $T_{l,r}$ and $\hat{T}_{l,r}$. Then, we say that two DNs $M_{l,r}$ and $\hat{M}_{l,r}$ are* partnered *together, or equivalently, are* partners *of each other.*

As already mentioned, the EGAKA-KE protocol is built on an existing two-party protocol which is used to establish pairwise keys between group members. Each DN $M_{l,r}$ is designated as the representative of the subgroup $\mathcal{G}_{l,r}$, and is responsible for negotiating a pairwise key $k_{l,r}$ with his partner $\hat{M}_{l,r}$, hence the name of it.

3 A Review of the EGAKA-KE Protocol

In describing the protocol, we assume that group members have agreed on a two-party authenticated key agreement protocol that provides both perfect forward secrecy and known key security. One example of such a protocol is A-DH presented by Ateniese et al. [1]. We also assume that all members know the structure of the tree and their position within the tree. This can be done by letting one randomly chosen member generate these tree-related information and broadcast it to the other members. Despite the seemingly systematic arrangement of members in the example of Fig. 1, we note that there is no significance to the order of members' positions in the tree, but rather the members are placed in a random way as described in Section 4.1 of the original paper [16]; what really matters is that the tree should be "well-balanced" in the sense that the height of the two subtrees of a node should differ by at most one.

We now describe the details of the EGAKA-KE protocol. The operation of the protocol is broadly divided into two phases: phase one, pairwise key establishment; phase two, secret and blinded keys generation.

3.1 Phase One: Pairwise Key Establishment

During this phase, each pair of partnered DNs $M_{l,r}$ and $\hat{M}_{l,r}$ generates a pairwise key by performing the underlying two-party key agreement protocol. Note that there are $n-1$ such pairs in the key tree for the group of n members. For instance, in the tree of Fig. 1, there are 6 pairs of partnered DNs: (M_1, M_5), (M_3, M_7), (M_2, M_6), (M_1, M_3), (M_2, M_4) and (M_1, M_2). Since all the $n-1$ protocol executions can be run simultaneously, the number of communication rounds required in the first phase is the same as that needed to complete the underlying two-party protocol.

If instantiated with A-DH, this process can be made concrete as follows. Let $\mathbb{G} = \langle\alpha\rangle$ be a cyclic group of prime order q which is a subgroup of $\mathbb{Z}_p^*$ for a prime

p such that $p = kq + 1$ for some small $k \in \mathbb{N}$ (e.g., $k = 2$). Let (x_i, α^{x_i}) be the private/public key pair of M_i and let $\mathcal{P}_i$ be the set of all partners of M_i. Then, for all $M_i \in \mathcal{G}$ and for all $M_j \in \mathcal{P}_i$ such that $i < j$, M_i and M_j perform the following steps:

1. M_i chooses a random $r_i \in \mathbb{Z}_q^*$ and sends α^{r_i} to M_j.
2. M_j chooses a random $r_j \in \mathbb{Z}_q^*$ and sends $\alpha^{r_j f(\alpha^{x_i x_j})}$ to M_i. Here, f is a function mapping elements of $\mathbb{G}$ to elements of $\mathbb{Z}_q$. If p is a safe prime (i.e., $p = 2q + 1$), then a perfect mapping function would be $f(x) = x$ if $x \leq q$, and $f(x) = p - x$ if $x > q$.
3. M_i and M_j compute the same pairwise key $\alpha^{r_i r_j}$.

These pairwise keys serve as key encryption keys used for securely exchanging the blinded keys between DNs in the second phase. In the sequel, we rule out the case $n = 2$ (i.e., $d = 1$) from consideration, since the group key for this special case is the pairwise key itself established between the two members in the first phase.

3.2 Phase Two: Secret and Blinded Keys Generation

Once group members have established a pairwise key with each of their partners, the secret and blinded keys of nodes are computed in a bottom-up manner, starting with the nodes at level $d - 1$ and proceeding towards the root at level 0. The blinded key of a node is always computed by applying a one-way hash function h to the secret key of the node, i.e., $B_{l,r} = h(K_{l,r})$. Although there are some exceptions, computing the secret key of a node requires the knowledge of two blinded keys, one for each of its two child nodes. More precisely, every $K_{l,r}$ for $l > d-1$ (see below for the case $l = d-1$) is computed recursively as follows:

$$K_{l,r} = h(B_{l+1,2r-1} || B_{l+1,2r}).$$

In this manner, it requires d communication rounds for all the group members to determine the secret key of the root, i.e., the common group key; at the end of the ith round, the key pair of node $N_{l,r}$ at level $l = d - i$ becomes available to all the members of the subgroup $\mathcal{G}_{l,r}$. The details of each round are given below, where we assume $l = d - i$ for each l appearing in the description of the ith round.

Round 1: Let $l = d - 1$.

1. For each leaf node $N_{l,r}$, the secret key $K_{l,r}$ is just a random nonce chosen by the member at that node. For each internal node $N_{l,r}$, $K_{l,r}$ is the pairwise key itself shared between two members corresponding to the left and right children.
2. Each DN $M_{l,r}$ computes $B_{l,r}$ as $B_{l,r} = h(K_{l,r})$ and sends to his partner $\hat{M}_{l,r}$

$$\{B_{l,r} || M_{l,r}\}_{k_{l,r}},$$

where $\{B_{l,r} || M_{l,r}\}_{k_{l,r}}$ denotes the ciphertext of $B_{l,r} || M_{l,r}$ encrypted using some secure symmetric cryptosystem under the pairwise key $k_{l,r}$.

Round i ($2 \leq i \leq d-1$, for $d \geq 3$): Let $l = d - i$.

1. For each node $N_{l,r}$, consider the two partnered DNs $M_{l+1,2r-1}$ and $M_{l+1,2r}$ respectively for its left and right subtrees. We describe this step only for $M_{l+1,2r-1}$; $M_{l+1,2r}$ acts correspondingly. $M_{l+1,2r-1}$ recovers $B_{l+1,2r}$ by decrypting the message received from $M_{l+1,2r}$, and sends
$$\{B_{l+1,2r}||M_{l+1,2r-1}\}_{K_{l+1,2r-1}}$$
to the rest of the subgroup $\mathcal{G}_{l+1,2r-1}$. Since all members in $\mathcal{G}_{l+1,2r-1}$ share the secret key $K_{l+1,2r-1}$, they can recover $B_{l+1,2r}$, and thus can compute $K_{l,r} = h(B_{l+1,2r-1}||B_{l+1,2r})$ and $B_{l,r} = h(K_{l,r})$.
2. After computing $K_{l,r}$ and $B_{l,r}$, each DN $M_{l,r}$ sends $\{B_{l,r}||M_{l,r}\}_{k_{l,r}}$ to his partner $\hat{M}_{l,r}$. Note that by definition of DN, one same member plays the role of both $M_{l+1,2r-1}$ and $M_{l,r}$.

Round d:

1. $M_{1,1}$ and $M_{1,2}$ recover respectively $B_{1,2}$ and $B_{1,1}$ by decrypting the message received from each other. $M_{1,1}$ then sends $\{B_{1,2}||M_{1,1}\}_{K_{1,1}}$ to the other members of $\mathcal{G}_{1,1}$. Similarly, $M_{1,2}$ sends $\{B_{1,1}||M_{1,2}\}_{K_{1,2}}$ to the rest of $\mathcal{G}_{1,2}$.
2. Finally, the members in $\mathcal{G}_{1,1}$ (respectively, $\mathcal{G}_{1,2}$) recover $B_{1,2}$ (respectively, $B_{1,1}$), and compute the group key as:
$$K_{0,1} = h(B_{1,1}||B_{1,2}).$$

Consider, for example, the member M_2 in Fig. 1. At the end of the first phase, M_2 holds three pairwise keys $k_{3,5}$ ($= k_{3,6}$), $k_{2,3}$ ($= k_{2,4}$) and $k_{1,2}$ ($= k_{1,1}$) shared with M_6, M_4 and M_1, respectively. In round 1 of the second phase, M_2 first computes the secret and blinded keys of node $N_{2,3}$ as $K_{2,3} = k_{3,5}$ and $B_{2,3} = h(K_{2,3})$. M_2 then, as the DN $M_{2,3}$, sends $\{B_{2,3}||M_2\}_{k_{2,3}}$ to M_4 who plays the role of the DN $M_{2,4}$. In round 2, M_2 obtains $B_{2,4}$ by decrypting $\{B_{2,4}||M_4\}_{k_{2,4}}$ received from M_4 and sends $\{B_{2,4}||M_2\}_{K_{2,3}}$ to M_6, the rest of subgroup $\mathcal{G}_{2,3}$. M_2 now computes the secret and blinded key pair of $N_{1,2}$ as $K_{1,2} = h(B_{2,3}||B_{2,4})$ and $B_{1,2} = h(K_{1,2})$, and since he serves as $M_{1,2}$, sends $\{B_{1,2}||M_2\}_{k_{1,2}}$ to M_1, the DN $M_{1,1}$. In round 3, M_2 recovers $B_{1,1}$ by decrypting $\{B_{1,1}||M_1\}_{k_{1,1}}$ received from M_1 and sends $\{B_{1,1}||M_2\}_{K_{1,2}}$ to M_4 and M_6, the other members of $\mathcal{G}_{1,2}$. Finally, M_2 computes his group key as: $K_{0,1} = h(B_{1,1}||B_{1,2})$.

4 Security Analysis

The basic security property for a key establishment protocol to achieve is *implicit key authentication*, which is defined in the following context [1, 15].

Definition 3. *Let $\mathcal{G}$ be a set of parties who wish to share a common secret key by running a key establishment protocol KEP. Let K_i be the secret key computed by $M_i \in \mathcal{G}$ as a result of protocol KEP. We say that KEP provides implicit key authentication if each $M_i \in \mathcal{G}$ is assured that no party $M_q \notin \mathcal{G}$ can learn the key K_i unless helped by a dishonest $M_j \in \mathcal{G}$.*