Huaxiong Wang
Josef Pieprzyk
Vijay Varadharajan (Eds.)

LNCS 3108

Information Security and Privacy

9th Australasian Conference, ACISP 2004
Sydney, Australia, July 2004
Proceedings

Springer

TP309-53
A181
2004

Huaxiong Wang Josef Pieprzyk
Vijay Varadharajan (Eds.)

Information Security and Privacy

9th Australasian Conference, ACISP 2004
Sydney, Australia, July 13-15, 2004
Proceedings

Springer

Volume Editors

Huaxiong Wang
Josef Pieprzyk
Vijay Varadharajan
Macquarie University
Department of Computing
Sydney, NSW 2109, Australia
E-mail: {hwang,josef,vijay}@ics.mq.edu.au

Library of Congress Control Number: 2004108445

CR Subject Classification (1998): E.3, K.6.5, D.4.6, C.2, E.4, F.2.1, K.4.1

ISSN 0302-9743
ISBN 3-540-22379-7 Springer-Verlag Berlin Heidelberg New York

This work is subject to copyright. All rights are reserved, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, re-use of illustrations, recitation, broadcasting, reproduction on microfilms or in any other way, and storage in data banks. Duplication of this publication or parts thereof is permitted only under the provisions of the German Copyright Law of September 9, 1965, in its current version, and permission for use must always be obtained from Springer-Verlag. Violations are liable to prosecution under the German Copyright Law.

Springer-Verlag is a part of Springer Science+Business Media

springeronline.com

© Springer-Verlag Berlin Heidelberg 2004
Printed in Germany

Typesetting: Camera-ready by author, data conversion by PTP-Berlin, Protago-TeX-Production GmbH
Printed on acid-free paper SPIN: 11019282 06/3142 5 4 3 2 1 0

Lecture Notes in Computer Science 3108

Commenced Publication in 1973
Founding and Former Series Editors:
Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Editorial Board

Takeo Kanade
Carnegie Mellon University, Pittsburgh, PA, USA
Josef Kittler
University of Surrey, Guildford, UK
Jon M. Kleinberg
Cornell University, Ithaca, NY, USA
Friedemann Mattern
ETH Zurich, Switzerland
John C. Mitchell
Stanford University, CA, USA
Moni Naor
Weizmann Institute of Science, Rehovot, Israel
Oscar Nierstrasz
University of Bern, Switzerland
C. Pandu Rangan
Indian Institute of Technology, Madras, India
Bernhard Steffen
University of Dortmund, Germany
Madhu Sudan
Massachusetts Institute of Technology, MA, USA
Demetri Terzopoulos
New York University, NY, USA
Doug Tygar
University of California, Berkeley, CA, USA
Moshe Y. Vardi
Rice University, Houston, TX, USA
Gerhard Weikum
Max-Planck Institute of Computer Science, Saarbruecken, Germany

Preface

The 9th Australasian Conference on Information Security and Privacy (ACISP 2004) was held in Sydney, 13–15 July, 2004. The conference was sponsored by the Centre for Advanced Computing – Algorithms and Cryptography (ACAC), Information and Networked Security Systems Research (INSS), Macquarie University and the Australian Computer Society.

The aims of the conference are to bring together researchers and practitioners working in areas of information security and privacy from universities, industry and government sectors. The conference program covered a range of aspects including cryptography, cryptanalysis, systems and network security.

The program committee accepted 41 papers from 195 submissions. The reviewing process took six weeks and each paper was carefully evaluated by at least three members of the program committee. We appreciate the hard work of the members of the program committee and external referees who gave many hours of their valuable time.

Of the accepted papers, there were nine from Korea, six from Australia, five each from Japan and the USA, three each from China and Singapore, two each from Canada and Switzerland, and one each from Belgium, France, Germany, Taiwan, The Netherlands and the UK. All the authors, whether or not their papers were accepted, made valued contributions to the conference.

In addition to the contributed papers, Dr Arjen Lenstra gave an invited talk, entitled *Likely and Unlikely Progress in Factoring.*

This year the program committee introduced the Best Student Paper Award. The winner of the prize for the Best Student Paper was Yan-Cheng Chang from Harvard University for his paper *Single Database Private Information Retrieval with Logarithmic Communication.*

We would like to thank all the people involved in organizing this conference. In particular we would like to thank members of the organizing committee for their time and efforts, Andrina Brennan, Vijayakrishnan Pasupathinathan, Hartono Kurnio, Cecily Lenton, and members from ACAC and INSS.

July 2004

Huaxiong Wang
Josef Pieprzyk
Vijay Varadharajan

此为试读,需要完整PDF请访问: www.ertongbook.com

Australasian Conference on Information Security and Privacy
ACISP 2004

Sponsored by
Centre for Advanced Computing – Algorithms and Cryptography (ACAC)
Information and Networked Security Systems Research (INSS)
Macquarie University
Australian Computer Society

General Chair:

Vijay Varadharajan	*Macquarie University, Australia*

Program Chairs:

Josef Pieprzyk	*Macquarie University, Australia*
Huaxiong Wang	*Macquarie University, Australia*

Program Committee

Feng Bao	*Institute for Infocomm Research, Singapore*
Lynn Batten	*Deakin University, Australia*
Colin Boyd	*QUT, Australia*
Nicolas Courtois	*Axalto Smart Cards, France*
Ed Dawson	*QUT, Australia*
Yvo Desmedt	*Florida State University, USA*
Cunsheng Ding	*Hong Kong University of Sci. & Tech., China*
Dieter Gollmann	*Technical University of Hamburg, Germany*
Goichiro Hanaoka	*University of Tokyo, Japan*
Thomas Johansson	*Lund University, Sweden*
Kwangjo Kim	*ICU, Korea*
Kaoru Kurosawa	*Ibaraki Univ., Japan*
Kwok-Yan Lam	*Tsinghua University, China*
Keith Martin	*Royal Holloway, UK*
Yi Mu	*University of Wollongong, Australia*
Christine O'Keefe	*CSIRO, Australia*
David Pointcheval	*CNRS, France*
Leonid Reyzin	*Boston University, USA*
Greg Rose	*Qualcomm, Australia*
Rei Safavi-Naini	*University of Wollongong, Australia*
Palash Sarkar	*Indian Statistical Institute, India*
Jennifer Seberry	*University of Wollongong, Australia*

Igor Shparlinski	*Macquarie University, Australia*
Doug Stinson	*University of Waterloo, Canada*
Hung-Min Sun	*National Tsinghua University, Taiwan*
Serge Vaudenay	*EPFL, Switzerland*
Chaoping Xing	*National University of Singapore, Singapore*

External Referees

Mehdi-Laurent Akkar
Kazumaro Aoki
Tomoyuki Asano
Paul Ashley
Nuttapong Attrapadung
Roberto Avanzi
Gildas Avoine
Thomas Baigneres
Emmanuel Bresson
Dario Catalano
Sanjit Chatterjee
Chien-Ning Chen
Ling-Hwei Chen
Xiaofeng Chen
Bo-Chao Cheng
Chi-Hung Chi
Joo Yeon Cho
Siu-Leung Chung
Andrew Clark
Scott Contini
Don Coppersmith
Yang Cui
Tanmoy Kanti Das
Alex Dent
Christophe Doche
Ratna Dutta
Chun-I Fan
Serge Fehr
Ernest Foo
Pierre-Alain Fouque
Jun Furukawa
Rosario Gennaro
Juanma Gonzalez-Nieto
Louis Goubin
Zhi Guo
Philip Hawkes
Martin Hell
Matt Henricksen
Shoichi Hirose
Yvonne Hitchcock
Chiou-Ting Hsu
Min-Shiang Hwang
Gene Itkis
Toshiya Itoh
Tetsu Iwata
Marc Joye
Pascal Junod
Byoungcheon Lee
Yan-Xia Lin
Der-Chyuan Lou
Chi-Jen Lu
Stefan Lucks
Phil MacKenzie
Subhamoy Maitra
Cecile Malinaud
Tal Malkin
Wenbo Mao
Thomas Martin
Tatsuyuki Matsushita
Toshihiro Matsuo
Luke Mcaven
Robert McNerney
Tom Messerges
Pradeep Kumar Mishra
Chris Mitchell
Jean Monnerat
Joern Mueller-Quade
James Muir
Seiji Munetoh
Sean Murphy
Anderson Nascimento
Lan Ngyuen
Phong Nguyen
Philippe Oechslin
Miyako Ohkubo
Yasuhiro Ohtaki
Wakaha Ogata
Michael Paddon
Doug Palmer
Jacques Patarin
Kenny Paterson
Kun Peng
Krzysztof Pietrzak
Angela Piper
Jason Reid
Ryuichi Sakai
Renate Scheidler
Nichoas Sheppard
SeongHan Shin
Leonie Simpson
Hong-Wei Sun
Willy Susilo
Isamu Teranishi
Dong To
Woei-Jiunn Tsaur
Din-Chang Tseng
Takeyuki Uehara
David Wagner
Chih-Hung Wang
William Whyte
Hongjun Wu
Tzong-Chen Wu
Sung-Ming Yen
Lu Yi
Takuya Yoshida
Ming Yung
Moti Yung
Fangguo Zhang
Rui Zhang
Xi-Bin Zhao

Lecture Notes in Computer Science

For information about Vols. 1–3027

please contact your bookseller or Springer-Verlag

Vol. 3133: A.D. Pimentel, S. Vassiliadis (Eds.), Computer Systems, Architectures, Modeling, and Simulation. XIV, 562 pages. 2004.

Vol. 3125: D. Kozen (Ed.), Mathematics of Program Construction. X, 401 pages. 2004.

Vol. 3123: A. Belz, R. Evans, P. Piwek (Eds.), Natural Language Generation. X, 219 pages. 2004. (Subseries LNAI).

Vol. 3120: J. Shawe-Taylor, Y. Singer (Eds.), Learning Theory. X, 648 pages. 2004. (Subseries LNAI).

Vol. 3118: K. Miesenberger, J. Klaus, W. Zagler, D. Burger (Eds.), Computer Helping People with Special Needs. XXIII, 1191 pages. 2004.

Vol. 3116: C. Rattray, S. Maharaj, C. Shankland (Eds.), Algebraic Methodology and Software Technology. XI, 569 pages. 2004.

Vol. 3114: R. Alur, D.A. Peled (Eds.), Computer Aided Verification. XII, 536 pages. 2004.

Vol. 3113: J. Karhumäki, H. Maurer, G. Paun, G. Rozenberg (Eds.), Theory Is Forever. X, 283 pages. 2004.

Vol. 3112: H. Williams, L. MacKinnon (Eds.), New Horizons in Information Management. XII, 265 pages. 2004.

Vol. 3111: T. Hagerup, J. Katajainen (Eds.), Algorithm Theory - SWAT 2004. XI, 506 pages. 2004.

Vol. 3110: A. Juels (Ed.), Financial Cryptography. XI, 281 pages. 2004.

Vol. 3109: S.C. Sahinalp, S. Muthukrishnan, U. Dogrusoz (Eds.), Combinatorial Pattern Matching. XII, 486 pages. 2004.

Vol. 3108: H. Wang, J. Pieprzyk, V. Varadharajan (Eds.), Information Security and Privacy. XII, 494 pages. 2004.

Vol. 3107: J. Bosch, C. Krueger (Eds.), Software Reuse: Methods, Techniques and Tools. XI, 339 pages. 2004.

Vol. 3105: S. Göbel, U. Spierling, A. Hoffmann, I. Iurgel, O. Schneider, J. Dechau, A. Feix (Eds.), Technologies for Interactive Digital Storytelling and Entertainment. XVI, 304 pages. 2004.

Vol. 3104: R. Kralovic, O. Sykora (Eds.), Structural Information and Communication Complexity. X, 303 pages. 2004.

Vol. 3103: K. Deb (Ed.), Genetic and Evolutionary Computation - GECCO 2004. XLIX, 1439 pages. 2004.

Vol. 3102: K. Deb (Ed.), Genetic and Evolutionary Computation - GECCO 2004. L, 1445 pages. 2004.

Vol. 3101: M. Masoodian, S. Jones, B. Rogers (Eds.), Computer Human Interaction. XIV, 694 pages. 2004.

Vol. 3100: J.F. Peters, A. Skowron, J.W. Grzymała-Busse, B. Kostek, R.W. Świniarski, M.S. Szczuka (Eds.), Transactions on Rough Sets I. X, 405 pages. 2004.

Vol. 3099: J. Cortadella, W. Reisig (Eds.), Applications and Theory of Petri Nets 2004. XI, 505 pages. 2004.

Vol. 3098: J. Desel, W. Reisig, G. Rozenberg (Eds.), Lectures on Concurrency and Petri Nets. VIII, 849 pages. 2004.

Vol. 3097: D. Basin, M. Rusinowitch (Eds.), Automated Reasoning. XII, 493 pages. 2004. (Subseries LNAI).

Vol. 3096: G. Melnik, H. Holz (Eds.), Advances in Learning Software Organizations. X, 173 pages. 2004.

Vol. 3094: A. Nürnberger, M. Detyniecki (Eds.), Adaptive Multimedia Retrieval. VIII, 229 pages. 2004.

Vol. 3093: S.K. Katsikas, S. Gritzalis, J. Lopez (Eds.), Public Key Infrastructure. XIII, 380 pages. 2004.

Vol. 3092: J. Eckstein, H. Baumeister (Eds.), Extreme Programming and Agile Processes in Software Engineering. XVI, 358 pages. 2004.

Vol. 3091: V. van Oostrom (Ed.), Rewriting Techniques and Applications. X, 313 pages. 2004.

Vol. 3089: M. Jakobsson, M. Yung, J. Zhou (Eds.), Applied Cryptography and Network Security. XIV, 510 pages. 2004.

Vol. 3086: M. Odersky (Ed.), ECOOP 2004 – Object-Oriented Programming. XIII, 611 pages. 2004.

Vol. 3085: S. Berardi, M. Coppo, F. Damiani (Eds.), Types for Proofs and Programs. X, 409 pages. 2004.

Vol. 3084: A. Persson, J. Stirna (Eds.), Advanced Information Systems Engineering. XIV, 596 pages. 2004.

Vol. 3083: W. Emmerich, A.L. Wolf (Eds.), Component Deployment. X, 249 pages. 2004.

Vol. 3080: J. Desel, B. Pernici, M. Weske (Eds.), Business Process Management. X, 307 pages. 2004.

Vol. 3079: Z. Mammeri, P. Lorenz (Eds.), High Speed Networks and Multimedia Communications. XVIII, 1103 pages. 2004.

Vol. 3078: S. Cotin, D.N. Metaxas (Eds.), Medical Simulation. XVI, 296 pages. 2004.

Vol. 3077: F. Roli, J. Kittler, T. Windeatt (Eds.), Multiple Classifier Systems. XII, 386 pages. 2004.

Vol. 3076: D. Buell (Ed.), Algorithmic Number Theory. XI, 451 pages. 2004.

Vol. 3074: B. Kuijpers, P. Revesz (Eds.), Constraint Databases and Applications. XII, 181 pages. 2004.

Vol. 3073: H. Chen, R. Moore, D.D. Zeng, J. Leavitt (Eds.), Intelligence and Security Informatics. XV, 536 pages. 2004.

Vol. 3072: D. Zhang, A.K. Jain (Eds.), Biometric Authentication. XVII, 800 pages. 2004.

Vol. 3071: A. Omicini, P. Petta, J. Pitt (Eds.), Engineering Societies in the Agents World. XIII, 409 pages. 2004. (Subseries LNAI).

Vol. 3070: L. Rutkowski, J. Siekmann, R. Tadeusiewicz, L.A. Zadeh (Eds.), Artificial Intelligence and Soft Computing - ICAISC 2004. XXV, 1208 pages. 2004. (Subseries LNAI).

Vol. 3068: E. André, L. Dybkj{\}ae r, W. Minker, P. Heisterkamp (Eds.), Affective Dialogue Systems. XII, 324 pages. 2004. (Subseries LNAI).

Vol. 3067: M. Dastani, J. Dix, A. El Fallah-Seghrouchni (Eds.), Programming Multi-Agent Systems. X, 221 pages. 2004. (Subseries LNAI).

Vol. 3066: S. Tsumoto, R. Słowiński, J. Komorowski, J.W. Grzymała-Busse (Eds.), Rough Sets and Current Trends in Computing. XX, 853 pages. 2004. (Subseries LNAI).

Vol. 3065: A. Lomuscio, D. Nute (Eds.), Deontic Logic in Computer Science. X, 275 pages. 2004. (Subseries LNAI).

Vol. 3064: D. Bienstock, G. Nemhauser (Eds.), Integer Programming and Combinatorial Optimization. XI, 445 pages. 2004.

Vol. 3063: A. Llamosí, A. Strohmeier (Eds.), Reliable Software Technologies - Ada-Europe 2004. XIII, 333 pages. 2004.

Vol. 3062: J.L. Pfaltz, M. Nagl, B. Böhlen (Eds.), Applications of Graph Transformations with Industrial Relevance. XV, 500 pages. 2004.

Vol. 3061: F.F. Ramos, H. Unger, V. Larios (Eds.), Advanced Distributed Systems. VIII, 285 pages. 2004.

Vol. 3060: A.Y. Tawfik, S.D. Goodwin (Eds.), Advances in Artificial Intelligence. XIII, 582 pages. 2004. (Subseries LNAI).

Vol. 3059: C.C. Ribeiro, S.L. Martins (Eds.), Experimental and Efficient Algorithms. X, 586 pages. 2004.

Vol. 3058: N. Sebe, M.S. Lew, T.S. Huang (Eds.), Computer Vision in Human-Computer Interaction. X, 233 pages. 2004.

Vol. 3057: B. Jayaraman (Ed.), Practical Aspects of Declarative Languages. VIII, 255 pages. 2004.

Vol. 3056: H. Dai, R. Srikant, C. Zhang (Eds.), Advances in Knowledge Discovery and Data Mining. XIX, 713 pages. 2004. (Subseries LNAI).

Vol. 3055: H. Christiansen, M.-S. Hacid, T. Andreasen, H.L. Larsen (Eds.), Flexible Query Answering Systems. X, 500 pages. 2004. (Subseries LNAI).

Vol. 3054: I. Crnkovic, J.A. Stafford, H.W. Schmidt, K. Wallnau (Eds.), Component-Based Software Engineering. XI, 311 pages. 2004.

Vol. 3053: C. Bussler, J. Davies, D. Fensel, R. Studer (Eds.), The Semantic Web: Research and Applications. XIII, 490 pages. 2004.

Vol. 3052: W. Zimmermann, B. Thalheim (Eds.), Abstract State Machines 2004. Advances in Theory and Practice. XII, 235 pages. 2004.

Vol. 3051: R. Berghammer, B. Möller, G. Struth (Eds.), Relational and Kleene-Algebraic Methods in Computer Science. X, 279 pages. 2004.

Vol. 3050: J. Domingo-Ferrer, V. Torra (Eds.), Privacy in Statistical Databases. IX, 367 pages. 2004.

Vol. 3049: M. Bruynooghe, K.-K. Lau (Eds.), Program Development in Computational Logic. VIII, 539 pages. 2004.

Vol. 3047: F. Oquendo, B. Warboys, R. Morrison (Eds.), Software Architecture. X, 279 pages. 2004.

Vol. 3046: A. Laganà, M.L. Gavrilova, V. Kumar, Y. Mun, C.K. Tan, O. Gervasi (Eds.), Computational Science and Its Applications – ICCSA 2004. LIII, 1016 pages. 2004.

Vol. 3045: A. Laganà, M.L. Gavrilova, V. Kumar, Y. Mun, C.K. Tan, O. Gervasi (Eds.), Computational Science and Its Applications – ICCSA 2004. LIII, 1040 pages. 2004.

Vol. 3044: A. Laganà, M.L. Gavrilova, V. Kumar, Y. Mun, C.K. Tan, O. Gervasi (Eds.), Computational Science and Its Applications – ICCSA 2004. LIII, 1140 pages. 2004.

Vol. 3043: A. Laganà, M.L. Gavrilova, V. Kumar, Y. Mun, C.K. Tan, O. Gervasi (Eds.), Computational Science and Its Applications – ICCSA 2004. LIII, 1180 pages. 2004.

Vol. 3042: N. Mitrou, K. Kontovasilis, G.N. Rouskas, I. Iliadis, L. Merakos (Eds.), NETWORKING 2004, Networking Technologies, Services, and Protocols; Performance of Computer and Communication Networks; Mobile and Wireless Communications. XXXIII, 1519 pages. 2004.

Vol. 3040: R. Conejo, M. Urretavizcaya, J.-L. Pérez-de-la-Cruz (Eds.), Current Topics in Artificial Intelligence. XIV, 689 pages. 2004. (Subseries LNAI).

Vol. 3039: M. Bubak, G.D.v. Albada, P.M. Sloot, J.J. Dongarra (Eds.), Computational Science - ICCS 2004. LXVI, 1271 pages. 2004.

Vol. 3038: M. Bubak, G.D.v. Albada, P.M. Sloot, J.J. Dongarra (Eds.), Computational Science - ICCS 2004. LXVI, 1311 pages. 2004.

Vol. 3037: M. Bubak, G.D.v. Albada, P.M. Sloot, J.J. Dongarra (Eds.), Computational Science - ICCS 2004. LXVI, 745 pages. 2004.

Vol. 3036: M. Bubak, G.D.v. Albada, P.M. Sloot, J.J. Dongarra (Eds.), Computational Science - ICCS 2004. LXVI, 713 pages. 2004.

Vol. 3035: M.A. Wimmer (Ed.), Knowledge Management in Electronic Government. XII, 326 pages. 2004. (Subseries LNAI).

Vol. 3034: J. Favela, E. Menasalvas, E. Chávez (Eds.), Advances in Web Intelligence. XIII, 227 pages. 2004. (Subseries LNAI).

Vol. 3033: M. Li, X.-H. Sun, Q. Deng, J. Ni (Eds.), Grid and Cooperative Computing. XXXVIII, 1076 pages. 2004.

Vol. 3032: M. Li, X.-H. Sun, Q. Deng, J. Ni (Eds.), Grid and Cooperative Computing. XXXVII, 1112 pages. 2004.

Vol. 3031: A. Butz, A. Krüger, P. Olivier (Eds.), Smart Graphics. X, 165 pages. 2004.

Vol. 3030: P. Giorgini, B. Henderson-Sellers, M. Winikoff (Eds.), Agent-Oriented Information Systems. XIV, 207 pages. 2004. (Subseries LNAI).

Vol. 3029: B. Orchard, C. Yang, M. Ali (Eds.), Innovations in Applied Artificial Intelligence. XXI, 1272 pages. 2004. (Subseries LNAI).

Vol. 3028: D. Neuenschwander, Probabilistic and Statistical Methods in Cryptology. X, 158 pages. 2004.

Table of Contents

此为试读,需要完整PDF请访问: www.ertongbook.com

Fast Computation

Mobile Agents Security

Digital Signatures (II)

Protocols

Security Management

Access Control and Authorisation

Cryptosystems (II)

Cryptanalysis (III)

Multi-service Oriented Broadcast Encryption

Shaoquan Jiang and Guang Gong

Department of Electrical and Computer Engineering
University of Waterloo
Waterloo, Ontario N2L 3G1, CANADA
{jiangshq, ggong}@calliope.uwaterloo.ca

Abstract. Multi-service oriented broadcast encryption is a mechanism that allows a center to securely distribute multiple services to its authorized users. In this paper, we suggest a framework called $\mathcal{M}$ framework from the subset cover method [12] using RSA exponentiation technique. In this framework, each user's secret storage is independent of the number of services. Service subscriptions and service providing can be efficiently processed. The service unsubscriptions are dealt scalably. A small number of service unsubscriptions can be handled without key updating while the number of such users reaches a threshold, a rekeying algorithm is proposed to update the user's service memberships *explicitly*. We formalize and prove the framework is dynamically secure under the random oracle model. We realize our framework with a scheme based on complete subtree method.

1 Introduction

Broadcast encryption is a mechanism that allows one party to securely distribute his data to privileged users. This mechanism has important applications in Pay-TV, stock quotes and online database, etc. After the work by Fiat and Naor in 1993 [9], it has been extensively studied in the literature, for example, schemes for stateless receivers [1,12], public key based schemes [2,6,14] and rekeying schemes [16,15,4,10].

In this paper, we consider the multi-service oriented broadcast encryption (MOBE), which is explained as follows. Suppose that a broadcast center (BC) wants to distribute multiple services to a set of users such that each user is allowed to access a specific service if and only if he has subscribed to it. Here the security concerns are traitor tracing, service unsubscriptions, etc. A possible solution is to associate each service with a distinct system (in a single service setting). The main problem here is that a user's secret storage is proportional to the number of his subscribed services.

1.1 Related Work

MOBE problem is related to flexible access control by Chick and Tavares [5], where each user is assigned a master key using RSA exponentiation technique

H. Wang et al. (Eds.): ACISP 2004, LNCS 3108, pp. 1–11, 2004.
© Springer-Verlag Berlin Heidelberg 2004

that allows him to access his subscribed services. However, users get an identical key set if they subscribe the same services. Thus, it is impossible to distinguish such users. Consequently, traitor tracing and service unsubscriptions are not achievable.

Narayanan, et al. [13] considered a multi-service notion called practical Pay-TV scheme. They proposed three schemes. The third one is the most interesting scheme which is secure and has traceability. However, their scheme is only suitable for application with a small number of services since the user key size is linear in the number of subscribed services. Furthermore, their service unsubscription utilizes a unicast channel. It follows that it is not suitable for applications with a large number of users or applications with frequent membership updating. The second scheme claimed the collusion can not compute the secret associated with service i. But we show that this is incorrect in the full paper [11].

1.2 Contribution

In this paper, we propose a framework called $\mathcal{M}$ framework for MOBE problem. We first achieve the multi-service functionality from the subset cover method [12] (in the single service setting) using RSA exponentiation technique. But this is not sufficient since it might become less efficient(e.g., the message overhead grows large; it increases management burdens; revoked IDs can not be reused) when unsubscription is frequent, due to lack of a rekeying mechanism. We thus propose a multi-service rekeying algorithm by extending a rekeying framework [7,10]. In the obtained full framework, user key size in $\mathcal{M}$ is independent of the number of services. Subscription and new service providing are handled without involving unintended users. Furthermore, service unsubscription is handled scalably, which makes the system flexible. To gain a better understanding of this framework, we realize it by an efficient scheme $\mathcal{M}_{cs}$, which is based on a complete subtree method [12]. Finally, in order to evaluate the security of our framework, we formalize a notion of *dynamic security*. It captures threats from an adaptive adversary that might issue queries such as subscription, rekeying, corruption and new service providing. We show that $\mathcal{M}$ framework is secure under such a *severe* attack. Our proof is in the random oracle model.

This paper is organized as follows. In Section 2, we introduce our $\mathcal{M}$ framework and show their features. In Sections 3, we present a realization of $\mathcal{M}$ framework, from complete subtree method. In Section 4, we formalize and prove the dynamic security of $\mathcal{M}$ framework.

2 A Framework for Multi-service Oriented Broadcast Encryption

In this section, we introduce our $\mathcal{M}$ framework for MOBE problem and show some advantages of this framework.

2.1 Description of $\mathcal{M}$ Framework

Let U be the set of all possible users; BC be the broadcast center; w be the number of services BC provides. BC wants to provide services $\{1, \cdots, w\}$ with a controlled access right.

Preprocessing Phase

1. BC chooses a RSA composite $N = pq$ and w primes $p_1, p_2, \cdots, p_w$, where p, q are two large primes. Then he makes $N, p_1, \cdots, p_w$ public and keeps p, q secret.
2. BC defines a collection of subsets of U: $S_1, S_2, \cdots, S_z$, where z is polynomially bounded. For security reason, we require that $\{u\}$ is contained in the collection for all $u \in U$. Then BC associates S_i with a secret number $k_i, i = 1, \cdots, z$.
3. BC defines $Q = \prod_{i=1}^{w} p_i$. Let $\{1, 2, \cdots, w\}$ be the set of services currently available, $B(u)$ be the set of services user u has subscribed, $Z(u) = \prod_{i \in B(u)} p_i$, and $K(u) = \{k_i^{Q/Z(u)} \pmod N | u \in S_i, i = 1, \cdots, z\}$.

Note that without a special mention in this paper we always assume that the exponentiation is carried out over modular N.

Join Phase. When a new person asks for join, BC first finds a free ID $u \in U$ and assigns $K(u)$ and a random subscription key c_u to this person. Here c_u is only for subscription use and remains unchanged as long as he is in the system. We denote this person simply by u when the context is clear.

Broadcast Phase. Let U_i be the set of all the users that subscribe service i. When BC wants to broadcast message M of service i to all users in $U_i \backslash R_i$, for some $R_i \subseteq U_i$, he first finds a set cover $S_{i_1}, S_{i_2}, \cdots, S_{i_m}$ for $U \backslash R_i$, i.e., $S_{i_1} \cup S_{i_2} \cup \cdots \cup S_{i_m} = U \backslash R_i$. He then forms the ciphertext as

$$\mathcal{H}_i(R_i, M) := \langle i_1, \cdots, i_m, E_{sk_{i_1,i}}(k), \cdots, E_{sk_{i_m,i}}(k), F_k(M) \rangle, \tag{1}$$

where $sk_{i_j,i} = f(k_{i_j}^{Q/p_i})$, E and F are two encryption algorithms (usually E has a higher security than F), $f : Z_N^* \to \{0,1\}^L$ is a public hash function where L is the key size of E.

Decryption Phase. When receiving $\mathcal{H}_i(R_i, M)$, a user u in $U_i \backslash R_i (\subseteq U \backslash R_i)$ first finds j such that $u \in S_{i_j}$. Since u has $k_{i_j}^{Q/Z(u)}$, he can compute $sk_{i_j,i}$ and obtain message M.

Subscribing More Services. We now show that it is convenient for an existing user u to subscribe more services. Suppose u wants to add service j to $B(u)$. He first updates $B(u)$ to $B'(u) = B(u) \cup \{j\}$, $Z(u)$ to $Z'(u) = Z(u) \times p_j$.

BC then provides a key set $\{k_i^{Q/p_j} | u \in S_i, i = 1, \cdots, z\}$ to u encrypted under the subscription key c_u. When u gets this key set, he can update $K(u)$ to $K'(u) := \{k_i^{Q/z'(u)} | u \in S_i, i = 1, \cdots, z\}$ as follows. He finds integers a, b using the Euclidean algorithm such that $p_j a + bZ(u) = 1$ and then computes

$$(k_i^{Q/Z(u)})^a (k_i^{Q/p_j})^b = k_i^{aQ/Z(u)+bQ/p_j} = k_i^{\frac{Q}{Z'(u)}(p_j a + Z(u)b)} = k_i^{Q/Z'(u)}.$$

It is clear that $K'(u)$ is the current key set for user u. For simplicity, we still denote the updated parameters as $K(u), B(u), Z(u)$, respectively.

Service Unsubscription. Some users R_i' may quit service i at some moment. The main concern is to prevent them from access to it again after their leave. If the size of R_i' is small, this can be handled without updating other users' secret information. Specifically, in the broadcast phase, BC can use a set R_i containing R_i' as the excluding set. However, as mentioned in the introduction, when the size of R_i' grows large, this method is inefficient. In our method, we propose an extension of a rekeying algorithm [7] to *explicitly* update users' service memberships, see the rekeying phase.

Providing New Services. We show that it is convenient for BC to provide a new service $(w+1)$. To do this, BC first finds a prime number p_{w+1} and updates Q to $Q' = Q \times p_{w+1}$. Then he computes $q_{w+1} = p_{w+1}^{-1} \pmod{\phi(N)}$, where $\phi(\cdot)$ is the Euler function. For each k_i, he computes $k_i' := k_i^{q_{w+1}}$. For an existing user u, his secret key information keeps invariant since ${k_i'}^{Q'/Z(u)} = k_i^{Q/Z(u)}$. If u wants to subscribes service $(w+1)$, BC provides p_{w+1} and $\{{k_i'}^{Q'/p_{w+1}} | u \in S_i, i = 1, \cdots, z\}$ to him, encrypted under c_u. Then u updates $B(u), Z(u), K(u)$.
As a summary, providing a service does not affect an existing user's activity or even he does not need to know about this new service. On the other hand, subscribing this new service is as easy as subscribing an existing service.

Rekeying Phase. When the size of the set R_i for quitting a certain service i grows large, the system will become inefficient. Thus it is desired to permanently update users' service memberships. Let $\Delta : U \to \{1, \cdots, w\}$ be a function such that $\Delta(u)$ is the set of services that u will quit in this rekeying event. Note that revoking an illegal user is looked as quitting all the services. Now we extend a rekeying algorithm in [7] to the multi-service setting. We remark that the rekeying algorithm in [7] is an extension of that in [10]. Let R be the set of users that will quit at least one service. Then for a given pair (R, Δ), we can *simultaneously* update every user's key information (for all possible services). In order to present the algorithm in a clear way, we introduce some notations.

Definition 1. *Define $C(k_i)$ to be the minimal subset of $\{k_1, \cdots, k_z\}$ containing k_i such that generation process for elements in $C(k_i)$ shares no random bits with generation process for elements in $\{k_1, \cdots, k_z\} \backslash C(k_i)$.*

此为试读,需要完整PDF请访问: www.ertongbook.com