Sihan Qing
Wenbo Mao
Javier Lopez
Guilin Wang (Eds.)

LNCS 3783

Information and Communications Security

7th International Conference, ICICS 2005
Beijing, China, December 2005
Proceedings

Springer

Sihan Qing Wenbo Mao Javier Lopez
Guilin Wang (Eds.)

Information and Communications Security

7th International Conference, ICICS 2005
Beijing, China, December 10-13, 2005
Proceedings

Springer

Volume Editors

Sihan Qing
Chinese Academy of Sciences, Institute of Software
Beijing 100080, P.R. China
E-mail: qsihan@ercist.iscas.ac.cn

Wenbo Mao
HP Labs. China
112 Jian Guo Road, Beijing 100022, P.R. China

Javier Lopez
University of Malaga, Computer Science Department
29071 Malaga, Spain
E-mail: jlm@lcc.uma.es

Guilin Wang
Institute for Infocomm Research
21 Heng Mui Keng Terrace, Singapore 119613
E-mail: glwang@i2r.a-star.edu.sg

Library of Congress Control Number: 2005937067

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

ISSN	0302-9743
ISBN-10	3-540-30934-9 Springer Berlin Heidelberg New York
ISBN-13	978-3-540-30934-5 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: 11602897 06/3142 5 4 3 2 1 0

Lecture Notes in Computer Science 3783

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

Preface

The Seventh International Conference on Information and Communications Security, ICICS 2005, was held in Beijing, China, 10-13 December 2005. The ICICS conference series is an established forum for exchanging new research ideas and development results in the areas of information security and applied cryptography. The first event began here in Beijing in 1997. Since then the conference series has been interleaving its venues in China and the rest of the world: ICICS 1997 in Beijing, China; ICICS 1999 in Sydney, Australia; ICICS 2001 in Xi'an, China; ICICS 2002 in Singapore; ICICS 2003 in Hohhot City, China; and ICICS 2004 in Malaga, Spain. The conference proceedings of the past events have always been published by Springer in the Lecture Notes in Computer Science series, with volume numbers, respectively: LNCS 1334, LNCS 1726, LNCS 2229, LNCS 2513, LNCS 2836, and LNCS 3269.

ICICS 2005 was sponsored by the Chinese Academy of Sciences (CAS); the Beijing Natural Science Foundation of China under Grant No. 4052016; the National Natural Science Foundation of China under Grants No. 60083007 and No. 60573042; the National Grand Fundamental Research 973 Program of China under Grant No. G1999035802, and Hewlett-Packard Laboratories, China. The conference was organized and hosted by the Engineering Research Center for Information Security Technology of the Chinese Academy of Sciences (ERCIST, CAS) in co-operation with the International Communications and Information Security Association (ICISA).

The aim of the ICICS conference series has been to offer the attendees the opportunity to discuss the latest developments in theoretical and practical aspects of information and communications security. The Technical Program for this year had three parts: (1) paper presentations, which consisted of 40 papers selected from 235 submissions, (2) two invited speeches, one from academia by Prof. Jean-Jacques Quisquater of the University of Louvain and one from industry by Mr. Graeme Proudler of Hewlett-Packard Laboratories, Bristol and Chairman of the Technical Committee of the Trusted Computing Group, and (3) Trusted Computing Technical Presentations (TCTP@ICICS 2005), which consisted of Trusted Computing solutions and demo showcases presented by Trusted Computing technology providers from industry. TC, which is defined, specified and promoted by the industry standard body Trusted Computing Group (TCG), is an important and pervasively progressing topic in platform security. However, it has so far mainly been researched and developed in industry. We believe that a closer involvement in TC from academia will help to advance this important area. TCTP@ICICS 2005 aimed to enhance interactions between academia and industry on the topic of TC.

We are grateful to the program committee members and external referees for their precious time and valued contribution to the tough and time-consuming review process. We are also pleased to thank Dr. Guilin Wang for his great help in publishing affairs, Dr. Jianbo He for his great contribution to website related affairs, and Mr. Yinghe Jia, Prof. Yeping He, Prof. Xizhen Ni, and other members of the Organizing Committee for helping with many local details.

Finally we wish to thank the authors of every paper, whether accepted or not, the attendees of the conference and all the other people who contributed to the conference in various ways.

September 2005

Sihan Qing
Wenbo Mao
Javier Lopez

ICICS 2005

Seventh International Conference on Information and Communications Security

Beijing, China
December 10-13, 2005

Organized by

Engineering Research Center for Information Security Technology (ERCIST)
(Chinese Academy of Sciences)

In co-operation with

International Communications and Information Security Association (ICISA)

Sponsored by

Chinese Academy of Sciences (CAS)
Beijing Natural Science Foundation of China
National Natural Science Foundation of China
National Grand Fundamental Research 973 Program of China *and*
Hewlett-Packard Laboratories, China

General Chair

Sihan Qing	Chinese Academy of Sciences, China

Program Chairs

Sihan Qing	Chinese Academy of Sciences, China
Wenbo Mao	HP Labs, Beijing & Bristol
Javier Lopez	University of Malaga, Spain

Program Committee

Tuomas Aura	Microsoft, UK
Feng Bao	Institute for Infocomm Research, Singapore
Alex Biryukov	Katholieke Univ. Leuven, Belgium
Mike Burmester	Florida State University, USA
Chin-Chen Chang	National Chung Cheng University, Taiwan
Lily Chen	Motorola, USA
Welland Chu	Thales, Hong Kong, China

Bruno Crispo	Vrije University, Holland
Ed Dawson	Queensland University of Technology, Australia
Robert H. Deng	Singapore Management University, Singapore
Yvo Desmedt	University College London, UK
Josep Domingo-Ferrer	Univ. Rovira-Virgili, Spain
Dengguo Feng	Chinese Academy of Sciences, China
Antonio Gomez-Skarmeta	Univ. of Murcia, Spain
Stefanos Gritzalis	University of Aegean, Greece
Yongfei Han	Onets, China
Hai Jin	Huazhong Univ. of Sci. & Tech., China
Marc Joye	Gemplus & CIM-PACA, France
Kwangjo Kim	Information and Communications University, Korea
Chi-Sung Laih	National Cheng Kung University, Taiwan
Antonio Maña	University of Malaga, Spain
Catherine Meadows	Naval Research Laboratory, USA
Eiji Okamoto	University of Tsukuba, Japan
Giuseppe Persiano	Università di Salerno, Italy
David Pointcheval	ENS, France
Jean-Jacques Quisquater	UCL, Belgium
Bimal Roy	Indian Statistical Institute, India
Rei Safavi-Naini	University of Wollongong, Australia
Kouichi Sakurai	Kyushu University, Japan
Tomas Sander	HP Labs, Princeton, USA
Nigel Smart	Bristol University, UK
Miguel Soriano	UPC, Spain
Vijay Varadharajan	Macquarie University, Australia
Guozhen Xiao	Xidian University, China
Yiqun Lisa Yin	Independent security consultant, USA
Moti Yung	Columbia University & RSA Labs, USA
Yuliang Zheng	University of North Carolina at Charlotte, USA
Jianying Zhou	Institute for Infocomm Research, Singapore

Publication Chair

Guilin Wang	Institute for Infocomm Research, Singapore

Organizing Committee Chairs

Yinghe Jia	China Information Security Technology Committee, China
Yeping He	ERCIST, Chinese Academy of Sciences, China
Xizhen Ni	ERCIST, Chinese Academy of Sciences, China

External Reviewers

Joonsang Baek
Venkat Balakrishnan
T. Balopoulos
Paulo Barreto
Kemal Bicakci
Colin Boyd
Xavier Boyen
Hongxu Cai
Oscar Canovas
Alvaro Cardenas
Jordi Castellà-Roca
Dario Catalano
Julien Cathalo
Debrup Chakraborty
Sanjit Chatterjee
Yongxi Cheng
Zhian Cheng
Andrew Clark
Félix J. García Clemente
Scott Contini
Paolo D'Arco
Xuhua Ding
Yevgeniy Dodis
Qingkuan Dong
Boris Dragovic
Jiang Du
Dang Nguyen Duc
Ratna Dutta
Oscar Esparza
Marcel Fernandez
Jordi Forne
Xiaotong Fu
Clemente Galdi
Chandana Gamage
Jie Guo
Lifeng Guo
L. Gymnopoulos
Shai Halevi
Yong-Sork Her
Juan Hernández-Serrano
Yoshiaki Hori
John Iliadis
Kenji Imamoto
Sarath Indrakanti
C. Kalloniatis
Georgios Kambourakis
HyunChan Kim
Costas Lambrinoudakis
Tri V. Le
Eonkyung Lee
Hyunrok Lee
Dimitrios Lekkas
Manuel Leone
Jung-Shian Li
Minming Li
Ninghui Li
Shengqiang Li
Benoît Libert
Vo Duc Liem
Chi-Jen Lu
Wenming Lu
Miao Ma
Antoni Martínez-Ballesté
Barbara Masucci
Gabriel López Millán
José L. Muñoz-Tapia
Aarthi Nagarajan
Gregory Neven
Svetla Nikova
Peng Ning
Ryuzo Nishi
Elisabeth Oswald
Dan Page
Pascal Paillier
Jae Min Park
Josep Pegueroles
Kun Peng
Olivier Pereira
Gregorio Martinez Perez
Angela Piper
Bogdan Popescu
Chun Ruan
Palash Sarkar
Jasper Scholten
Francesc Sebé
Wook Shin
Agusti Solanas
Martijn Stam
François-Xavier Standaert
Gelareh Taban
Dongvu Tonien
Udaya Kiran Tupakula
Yoshifumi Ueshige
Frederik Vercauteren
Ivan Visconti
Zhiguo Wan
Chen Wang
Shuhong Wang
Yongdong Wu
Jing Xiao
JonPhil Yang
Yanjiang Yang
Janson Zhang
Jing Zhang
Ning Zhang
Weiliang Zhao
Yingchao Zhao
Yunlei Zhao
Huafei Zhu

Lecture Notes in Computer Science

For information about Vols. 1–3726

please contact your bookseller or Springer

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

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

Vol. 3833: K.-J. Li, C. Vangenot (Eds.), Web and Wireless Geographical Information Systems. XI, 309 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. XXIII, 1204 pages. 2005.

Vol. 3823: T. Enokido, L. Yan, B. Xiao, D. Kim, Y. Dai, L.T. Yang (Eds.), Embedded and Ubiquitous Computing. 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. Zhou, W. Zhao, Z. Wu, Y. Zhu, M. Lin (Eds.), Embedded Software and Systems. XXVIII, 779 pages. 2005.

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

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

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. (Subseries LNAI).

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

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

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

Vol. 3773: A. Sanfeliu, M.L. Cortés (Eds.), Progress in Pattern Recognition, Image Analysis and Applications. XX, 1094 pages. 2005.

Vol. 3772: M. Consens, G. Navarro (Eds.), String Processing and Information Retrieval. XIV, 406 pages. 2005.

Vol. 3771: J.M.T. Romijn, G.P. Smith, J. van de Pol (Eds.), Integrated Formal Methods. XI, 407 pages. 2005.

Vol. 3770: J. Akoka, S.W. Liddle, I.-Y. Song, M. Bertolotto, I. Comyn-Wattiau, W.-J. van den Heuvel, M. Kolp, J. Trujillo, C. Kop, H.C. Mayr (Eds.), Perspectives in Conceptual Modeling. XXII, 476 pages. 2005.

Vol. 3768: Y.-S. Ho, H.J. Kim (Eds.), Advances in Multimedia Information Processing - PCM 2005, Part II. XXVIII, 1088 pages. 2005.

Vol. 3767: Y.-S. Ho, H.J. Kim (Eds.), Advances in Multimedia Information Processing - PCM 2005, Part I. XXVIII, 1022 pages. 2005.

Vol. 3766: N. Sebe, M.S. Lew, T.S. Huang (Eds.), Computer Vision in Human-Computer Interaction. X, 231 pages. 2005.

Vol. 3765: Y. Liu, T. Jiang, C. Zhang (Eds.), Computer Vision for Biomedical Image Applications. X, 563 pages. 2005.

Vol. 3764: S. Tixeuil, T. Herman (Eds.), Self-Stabilizing Systems. VIII, 229 pages. 2005.

Vol. 3762: R. Meersman, Z. Tari, P. Herrero (Eds.), On the Move to Meaningful Internet Systems 2005: OTM 2005 Workshops. XXXI, 1228 pages. 2005.

Vol. 3761: R. Meersman, Z. Tari (Eds.), On the Move to Meaningful Internet Systems 2005: CoopIS, DOA, and ODBASE, Part II. XXVII, 653 pages. 2005.

Vol. 3760: R. Meersman, Z. Tari (Eds.), On the Move to Meaningful Internet Systems 2005: CoopIS, DOA, and ODBASE, Part I. XXVII, 921 pages. 2005.

Vol. 3759: G. Chen, Y. Pan, M. Guo, J. Lu (Eds.), Parallel and Distributed Processing and Applications - ISPA 2005 Workshops. XIII, 669 pages. 2005.

Vol. 3758: Y. Pan, D.-x. Chen, M. Guo, J. Cao, J.J. Dongarra (Eds.), Parallel and Distributed Processing and Applications. XXIII, 1162 pages. 2005.

Vol. 3757: A. Rangarajan, B. Vemuri, A.L. Yuille (Eds.), Energy Minimization Methods in Computer Vision and Pattern Recognition. XII, 666 pages. 2005.

Vol. 3756: J. Cao, W. Nejdl, M. Xu (Eds.), Advanced Parallel Processing Technologies. XIV, 526 pages. 2005.

Vol. 3754: J. Dalmau Royo, G. Hasegawa (Eds.), Management of Multimedia Networks and Services. XII, 384 pages. 2005.

Vol. 3753: O.F. Olsen, L.M.J. Florack, A. Kuijper (Eds.), Deep Structure, Singularities, and Computer Vision. X, 259 pages. 2005.

Vol. 3752: N. Paragios, O. Faugeras, T. Chan, C. Schnörr (Eds.), Variational, Geometric, and Level Set Methods in Computer Vision. XI, 369 pages. 2005.

Vol. 3751: T. Magedanz, E.R. M. Madeira, P. Dini (Eds.), Operations and Management in IP-Based Networks. X, 213 pages. 2005.

Vol. 3750: J.S. Duncan, G. Gerig (Eds.), Medical Image Computing and Computer-Assisted Intervention – MICCAI 2005, Part II. XL, 1018 pages. 2005.

Vol. 3749: J.S. Duncan, G. Gerig (Eds.), Medical Image Computing and Computer-Assisted Intervention – MICCAI 2005, Part I. XXXIX, 942 pages. 2005.

Vol. 3748: A. Hartman, D. Kreische (Eds.), Model Driven Architecture – Foundations and Applications. IX, 349 pages. 2005.

Vol. 3747: C.A. Maziero, J.G. Silva, A.M.S. Andrade, F.M.d. Assis Silva (Eds.), Dependable Computing. XV, 267 pages. 2005.

Vol. 3746: P. Bozanis, E.N. Houstis (Eds.), Advances in Informatics. XIX, 879 pages. 2005.

Vol. 3745: J.L. Oliveira, V. Maojo, F. Martín-Sánchez, A.S. Pereira (Eds.), Biological and Medical Data Analysis. XII, 422 pages. 2005. (Subseries LNBI).

Vol. 3744: T. Magedanz, A. Karmouch, S. Pierre, I. Venieris (Eds.), Mobility Aware Technologies and Applications. XIV, 418 pages. 2005.

Vol. 3742: J. Akiyama, M. Kano, X. Tan (Eds.), Discrete and Computational Geometry. VIII, 213 pages. 2005.

Vol. 3740: T. Srikanthan, J. Xue, C.-H. Chang (Eds.), Advances in Computer Systems Architecture. XVII, 833 pages. 2005.

Vol. 3739: W. Fan, Z. Wu, J. Yang (Eds.), Advances in Web-Age Information Management. XXIV, 930 pages. 2005.

Vol. 3738: V.R. Syrotiuk, E. Chávez (Eds.), Ad-Hoc, Mobile, and Wireless Networks. XI, 360 pages. 2005.

Vol. 3737: C. Priami, E. Merelli, P. Gonzalez, A. Omicini (Eds.), Transactions on Computational Systems Biology III. VII, 169 pages. 2005. (Subseries LNBI).

Vol. 3735: A. Hoffmann, H. Motoda, T. Scheffer (Eds.), Discovery Science. XVI, 400 pages. 2005. (Subseries LNAI).

Vol. 3734: S. Jain, H.U. Simon, E. Tomita (Eds.), Algorithmic Learning Theory. XII, 490 pages. 2005. (Subseries LNAI).

Vol. 3733: P. Yolum, T. Güngör, F. Gürgen, C. Özturan (Eds.), Computer and Information Sciences - ISCIS 2005. XXI, 973 pages. 2005.

Vol. 3731: F. Wang (Ed.), Formal Techniques for Networked and Distributed Systems - FORTE 2005. XII, 558 pages. 2005.

Vol. 3729: Y. Gil, E. Motta, V. R. Benjamins, M.A. Musen (Eds.), The Semantic Web – ISWC 2005. XXIII, 1073 pages. 2005.

Vol. 3728: V. Paliouras, J. Vounckx, D. Verkest (Eds.), Integrated Circuit and System Design. XV, 753 pages. 2005.

Vol. 3727: M. Barni, J. Herrera Joancomartí, S. Katzenbeisser, F. Pérez-González (Eds.), Information Hiding. XII, 414 pages. 2005.

¥604.16元

Table of Contents

Fair Exchange

Digital Signatures I

Cryptographic Protocols

Cryptanalysis

Digital Signatures II

Network Security

Applied Cryptography

Key Management

Access Control

Applications

Watermarking

System Security

An Evenhanded Certified Email System for Contract Signing

Kenji Imamoto[1], Jianying Zhou[2], and Kouichi Sakurai[1]

[1] Information Science and Electrical Engineering, Kyushu University,
6-10-1 Hakozaki, Higashi-ku, Fukuoka, 812-8581, Japan
imamoto@itslab.csce.kyushu-u.ac.jp, sakurai@csce.kyushu-u.ac.jp
[2] Institute for Infocomm Research,
21 Heng Mui Keng Terrace, Singapore 119613
jyzhou@i2r.a-star.edu.sg

Abstract. Certified email is a system which enables a sender to prove a receiver's receipt of email. Such a system can be used for applications related to electronic commerce on the Internet. This paper considers a situation where a sender or a receiver wants to change his/her mind due to the change of mail content value (e.g., stock, auction, gambling) during the transaction. We point out that no traditional certified email systems have been designed for such a case, thus one of the participants can be at a disadvantage. To avoid this problem, we propose an evenhanded certified email system in which each participant can change his/her choice, either cancel or finish the transaction, at any time during the transaction.

1 Introduction

As the Internet has become more and more popular, many contracts are being signed online as well. A variant of the contract signing problem is *certified email* in which, Alice sends a mail to Bob and wants some evidence (i.e., a receipt) that Bob received her mail. *Fairness* is an important requirement for a certified email protocol that guarantees when the protocol terminates, either both parties have obtained their desired items, or neither acquired any useful information.

Many certified email systems have been proposed [1,2,3,4,5,6], and some systems are commercialized. For efficiency, most of certified email systems include a *trusted third party* (TTP) as a mediator. This mediator is involved to ensure the fairness of a transaction. Although protocols without TTP were also proposed [7], they are not practical in terms of computation and communication overheads. Hence, this paper only focuses on certified email systems that use a TTP.

Some of existing systems introduced the concept of *timeliness* (i.e., any participant can terminate a session in finite time without loss of fairness) to avoid waiting the other's response forever [1,2]. In order to provide timeliness, a system proposed in [1] has two sub-protocols: *cancel protocol* and *help protocol.* By using the cancel protocol, a sender can cancel a session if the intended receiver ignores the sender's request. On the other hand, by using the help protocol, a

S. Qing et al. (Eds.): ICICS 2005, LNCS 3783, pp. 1–13, 2005.

receiver can obtain the mail even if the sender does nothing after the receiver responded to the sender's request.

In addition to termination of a session in finite time, the cancel protocol can also be used to change a sender's decision before completing the session (i.e., she can stop transmission of the mail). However, since the receiver cannot execute the cancel protocol, he cannot change his mind after a particular point even before completing the session (i.e., he cannot deny the receipt of the mail). This difference leads to the following disadvantageous situation.

> Suppose Alice sells gold to Bob at 100 dollars. The receipt of gold means that "Alice must sell gold at 100 dollars and Bob must pay 100 dollars". Then, they execute the proposed certified email protocol to exchange gold and the receipt. After Bob's response to Alice's request (but before completing the protocol), someone who says "I want to buy gold at 120 dollars" might appear. In this case, she will cancel the protocol, and sell gold to the new buyer. On the other hand, someone who says "I want to sell gold at 80 dollars" might appear. In this case, Bob wants to cancel the protocol and buy gold from the new seller, but he cannot.

The above situation can happen frequently in the case of a contract that the item's value is changeable, for example a soccer pool where the news of a player's sudden injury may change the betters' choices. Since no traditional certified email systems have been designed for such a case, one of the participants can be at a disadvantage. In this paper, we propose an *evenhanded system* in which each participant can change his/her choice anytime before a termination without loss of fairness. We call this property "*Change of Choice*". In our proposed system, each participant has sub-processes to cope with any event in order to enjoy the best benefit. Note that each participant always plays in a way that increases his/her own benefit, and a participant who first acts will obtain the better benefit (i.e., first come, first served).

2 Model and Requirements

This paper considers contracts of changeable values, where a party owning a variable item wants to sell her item to another party. Suppose the digital item is delivered with a certified email system, and the sender can claim the payment (as indicated in the receipt) from the receiver by proving the item has been received by the receiver. To simplify our analysis, we assume the price offered at the starting point of a session is the one negotiated by both participants.

Each party communicates through a network where no message is lost or delayed, and the value of an exchanged item can change anytime. Each party decides his/her action to make own benefit as high as possible.

A standard certified email system has the following requirements.

- *Fairness*: Both participants can either obtain the result each one desires, or neither of them does.