Jae-Kwang Lee
Okyeon Yi
Moti Yung (Eds.)

LNCS 4298

Information Security Applications

7th International Workshop, WISA 2006
Jeju Island, Korea, August 2006
Revised Selected Papers

Springer

Jae-Kwang Lee Okyeon Yi Moti Yung (Eds.)

Information Security Applications

7th International Workshop, WISA 2006
Jeju Island, Korea, August 28-30, 2006
Revised Selected Papers

Springer

Volume Editors

Jae-Kwang Lee
Hannam University, School of Computer Engineering
133 Ojeong Dong, Daedeuk Gu, Daejeon, 306-791, Korea
E-mail: jklee@netwk.hannam.ac.kr

Okyeon Yi
Kookmin University, Department of Mathematics
861-1 Jeongneung-Dong, Songbuk-Gu, Seoul, 136-702, Korea
E-mail: oyyi@kookmin.ac.kr

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

Library of Congress Control Number: 2007922329

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 3-540-71092-2 Springer Berlin Heidelberg New York
ISBN-13 978-3-540-71092-9 Springer Berlin Heidelberg New York

Springer is a part of Springer Science+Business Media

springer.com

Printed in Germany

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 12025299 06/3142 5 4 3 2 1 0

Preface

The 7th International Workshop on Information Security Applications (WISA 2006) was held on Jeju Island, Korea during August 28-30, 2006. 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).

WISA aims at providing a forum for professionals from academia and industry to present their work and to exchange ideas. The workshop covers all technical aspects of security applications, including cryptographic and non-cryptographic techniques.

We were very pleased and honored to serve as the Program Committee Co-chairs of WISA 2006. The Program Committee received 146 papers from 11 countries, and accepted 31 papers for the full presentation track and 18 papers for a short presentation track. The papers were selected after an extensive and careful refereeing process in which each paper was reviewed by at least three members of the Program Committee.

In addition to the contributed papers, the workshop had three special talks. Moti Yung gave a tutorial talk, entitled "Phishing and Authentication in Banks." Sushil Jajodia and Seong G. Kong gave invited talks in the full presentation track, entitled "Topological Analysis of Network Attack Vulnerability" and "Imaging Beyond the Visible Spectrum for Personal Identification and Threat Detection," respectively.

Many people deserve our gratitude for their generous contributions to the success of the workshop. We would like to thank all the people 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 their hard work in organizing the workshop.

Last but not least, on behalf of all those involved in organizing the workshop, we would like to thank all the authors who submitted papers to this workshop. Without their submissions and support, WISA could not have been a success.

December 2006

Jae-Kwang Lee
Okyeon Yi
Moti Yung

Organization

Advisory Committee

Man-Young Rhee	Kyung Hee University, Korea
Hideki Imai	Tokyo University, Japan
Chu-Hwan Yim	ETRI, Korea
Bart Preneel	Katholieke Universiteit Leuven, Belgium
Kil-Hyun Nam	Korea National Defense University, Korea
Sang-Jae Moon	Kyungpook National University, Korea
Dong-Ho Won	Sungkyunkwan University, Korea
Sehun Kim	KAIST, Korea
Pil-Joong Lee	POSTECH, Korea
Dae-Ho Kim	NSRI, Korea

General Co-chairs

Sung-Won Sohn	ETRI, Korea
Joo-Seok Song	Yonsei University, Korea

Steering Committee

Heung-Youl Youm	Soonchunhyang University, Korea
Suk-Woo Kim	Hansei University, Korea
Ki-Joon Chae	Ewha University, Korea
Chae-Hun Lim	Sejong University, Korea
Kyo-Il Chung	ETRI, Korea
TaeKyoung Kwon	Sejong University, Korea
Im-Yeong Lee	Soonchunhyang University, Korea

Organizing Committee

Chair:	Dong-Il Seo	ETRI, Korea
Finance:	Hyung-Woo Lee	Hanshin University, Korea
Publication:	Ji-Young Lim	Korean Bible University, Korea
Publicity:	Yoo-Jae Won	KISA, Korea
	Sang-Choon Kim	Kangwon National University, Korea
Registration:	Heuisu Ryu	Gyeongin National University of Education, Korea
Treasurer:	Do-Won Hong	ETRI, Korea
Local Arrangements:	Ki-Wook Sohn	NSRI, Korea
	Khi Jung Ahn	Cheju National University, Korea

Program Committee

Co-chairs :	Jae-Kwang Lee	Hannam University, Korea
	Moti Yung	Columbia University, USA
	Okyeon Yi	Kookmin University, Korea
Members :	Choong Seon Hong	KyungHee University, Korea
	Jae-Cheol Ryou	Chungnam University, Korea
	Dong Hoon Lee	CIST, Korea University, Korea
	Seungjoo Kim	Sungkyunkwan University, Korea
	Taekyoung Kwon	Sejong University, Korea
	Joongchan Na	ETRI, Korea
	Janghee You	ETRI, Korea
	Jung-Cheol Ahn	NSRI, Korea
	Myungsoo Rhee	KT, Korea
	Youngtae Cha	Secui.com, Korea
	Heesun Yang	KOMSCO, Korea
	Gildas Avoine	MIT, CSAIL, USA
	Sven Dietrich	CERT, CMU, USA
	Marc Joye	Gemplus, France
	Jaeyeon Jung	MIT, CSAIL
	Stefan Katzenbeisser	Philips Research, The Netherlands
	Brian King	Indiana University Purdue University, USA
	Dongdai Lin	SKLIS, Chinese Academy of Sciences, China
	Helger Lipmaa	University of Tartu, Estonia
	Havier Lopez	University of Malaga, Spain
	Lan Nguyen	CSIRO ICT Centre, Canbarra, Australia
	Yoram Ofek	University of Trento, Italy
	Susan Pancho-Festin	University of the Philippines, Phillipines
	C.Pandu Rangan	IIT Madras, India
	Duong Hieu Phan	University College London, UK
	Raphael C.-W. Phan	Swinburne University of Tech., Malaysia
	Vassilis Prevelakis	Drexel University, USA
	Pankaj Rohatgi	IBM Resaerch, USA
	Ahmad-Reza Sadeghi	Ruhr University, Bochum, Germany
	Kouichi Sakurai	Kyushu University, Japan
	Stuart Schechter	MIT, Lincoln Lab, USA
	Tom Shrimpton	Portland State University, USA
	Radu Sion, SUNY	Stony Brook, USA
	Stamatiou Iwannis	CTI, Greece
	Koutarou Suzuki	NTT Labs, Japan

Huaxiong Wang	Macquarie University, Australia
Duncan Wong	City University, Hong Kong
Rui Zhang	AIST, Japan
Jianying Zhou	Inst. for Infocomm Research, Singapore
Shozo Naito	Kyoto College of Graduate Studies for Informatics, Japan
Ko, Hong Seung	Kyoto College of Graduate Studies for Informatics, Japan

Lecture Notes in Computer Science 4298

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

Lecture Notes in Computer Science

For information about Vols. 1–4310

please contact your bookseller or Springer

Vol. 4429: R. Lu, J.H. Siekmann, C. Ullrich (Eds.), Cognitive Systems. X, 161 pages. 2007. (Sublibrary LNAI).

Vol. 4424: O. Grumberg, M. Huth (Eds.), Tools and Algorithms for the Construction and Analysis of Systems. XX, 738 pages. 2007.

Vol. 4420: S. Krishnamurthi, M. Odersky (Eds.), Compiler Construction. XIV, 233 pages. 2007.

Vol. 4415: P. Lukowicz, L. Thiele, G. Tröster (Eds.), Architecture of Computing Systems - ARCS 2007. X, 297 pages. 2007.

Vol. 4414: S. Hochreiter, R. Wagner (Eds.), Bioinformatics Research and Development. XVI, 482 pages. 2007. (Sublibrary LNBI).

Vol. 4405: L. Padgham, F. Zambonelli (Eds.), Agent-Oriented Software Engineering VII. XII, 225 pages. 2007.

Vol. 4403: S. Obayashi, K. Deb, C. Poloni, T. Hiroyasu, T. Murata (Eds.), Evolutionary Multi-Criterion Optimization. XIX, 954 pages. 2007.

Vol. 4397: C. Stephanidis, M. Pieper (Eds.), Universal Access in Ambient Intelligence Environments. XV, 467 pages. 2007.

Vol. 4396: J. García-Vidal, L. Cerdà-Alabern (Eds.), Wireless Systems and Mobility in Next Generation Internet. IX, 271 pages. 2007.

Vol. 4394: A. Gelbukh (Ed.), Computational Linguistics and Intelligent Text Processing. XVI, 648 pages. 2007.

Vol. 4393: W. Thomas, P. Weil (Eds.), STACS 2007. XVIII, 708 pages. 2007.

Vol. 4392: S.P. Vadhan (Ed.), Theory of Cryptography. XI, 595 pages. 2007.

Vol. 4390: S.O. Kuznetsov, S. Schmidt (Eds.), Formal Concept Analysis. X, 329 pages. 2007. (Sublibrary LNAI).

Vol. 4389: D. Weyns, H.V.D. Parunak, F. Michel (Eds.), Environments for Multi-Agent Systems III. X, 273 pages. 2007. (Sublibrary LNAI).

Vol. 4385: K. Coninx, K. Luyten, K.A. Schneider (Eds.), Task Models and Diagrams for Users Interface Design. XI, 355 pages. 2007.

Vol. 4384: T. Washio, K. Satoh, H. Takeda, A. Inokuchi (Eds.), New Frontiers in Artificial Intelligence. IX, 401 pages. 2007. (Sublibrary LNAI).

Vol. 4383: E. Bin, A. Ziv, S. Ur (Eds.), Hardware and Software, Verification and Testing. XII, 235 pages. 2007.

Vol. 4381: J. Akiyama, W.Y.C. Chen, M. Kano, X. Li, Q. Yu (Eds.), Discrete Geometry, Combinatorics and Graph Theory. XI, 289 pages. 2007.

Vol. 4380: S. Spaccapietra, P. Atzeni, F. Fages, M.-S. Hacid, M. Kifer, J. Mylopoulos, B. Pernici, P. Shvaiko, J. Trujillo, I. Zaihrayeu (Eds.), Journal on Data Semantics VIII. XV, 219 pages. 2007.

Vol. 4378: I. Virbitskaite, A. Voronkov (Eds.), Perspectives of Systems Informatics. XIV, 496 pages. 2007.

Vol. 4377: M. Abe (Ed.), Topics in Cryptology – CT-RSA 2007. XI, 403 pages. 2006.

Vol. 4376: E. Frachtenberg, U. Schwiegelshohn (Eds.), Job Scheduling Strategies for Parallel Processing. VII, 257 pages. 2007.

Vol. 4374: J.F. Peters, A. Skowron, I. Düntsch, J. Grzymała-Busse, E. Orłowska, L. Polkowski (Eds.), Transactions on Rough Sets VI, Part I. XII, 499 pages. 2007.

Vol. 4373: K. Langendoen, T. Voigt (Eds.), Wireless Sensor Networks. XIII, 358 pages. 2007.

Vol. 4372: M. Kaufmann, D. Wagner (Eds.), Graph Drawing. XIV, 454 pages. 2007.

Vol. 4371: K. Inoue, K. Satoh, F. Toni (Eds.), Computational Logic in Multi-Agent Systems. X, 315 pages. 2007. (Sublibrary LNAI).

Vol. 4370: P.P Lévy, B. Le Grand, F. Poulet, M. Soto, L. Darago, L. Toubiana, J.-F. Vibert (Eds.), Pixelization Paradigm. XV, 279 pages. 2007.

Vol. 4369: M. Umeda, A. Wolf, O. Bartenstein, U. Geske, D. Seipel, O. Takata (Eds.), Declarative Programming for Knowledge Management. X, 229 pages. 2006. (Sublibrary LNAI).

Vol. 4368: T. Erlebach, C. Kaklamanis (Eds.), Approximation and Online Algorithms. X, 345 pages. 2007.

Vol. 4367: K. De Bosschere, D. Kaeli, P. Stenström, D. Whalley, T. Ungerer (Eds.), High Performance Embedded Architectures and Compilers. XI, 307 pages. 2007.

Vol. 4366: K. Tuyls, R. Westra, Y. Saeys, A. Nowé (Eds.), Knowledge Discovery and Emergent Complexity in Bioinformatics. IX, 183 pages. 2007. (Sublibrary LNBI).

Vol. 4364: T. Kühne (Ed.), Models in Software Engineering. XI, 332 pages. 2007.

Vol. 4362: J. van Leeuwen, G.F. Italiano, W. van der Hoek, C. Meinel, H. Sack, F. Plášil (Eds.), SOFSEM 2007: Theory and Practice of Computer Science. XXI, 937 pages. 2007.

Vol. 4361: H.J. Hoogeboom, G. Păun, G. Rozenberg, A. Salomaa (Eds.), Membrane Computing. IX, 555 pages. 2006.

Vol. 4360: W. Dubitzky, A. Schuster, P.M.A. Sloot, M. Schroeder, M. Romberg (Eds.), Distributed, High-Performance and Grid Computing in Computational Biology. X, 192 pages. 2007. (Sublibrary LNBI).

Vol. 4358: R. Vidal, A. Heyden, Y. Ma (Eds.), Dynamical Vision. IX, 329 pages. 2007.

Vol. 4357: L. Buttyán, V. Gligor, D. Westhoff (Eds.), Security and Privacy in Ad-Hoc and Sensor Networks. X, 193 pages. 2006.

Vol. 4355: J. Julliand, O. Kouchnarenko (Eds.), B 2007: Formal Specification and Development in B. XIII, 293 pages. 2006.

Vol. 4354: M. Hanus (Ed.), Practical Aspects of Declarative Languages. X, 335 pages. 2006.

Vol. 4353: T. Schwentick, D. Suciu (Eds.), Database Theory – ICDT 2007. XI, 419 pages. 2006.

Vol. 4352: T.-J. Cham, J. Cai, C. Dorai, D. Rajan, T.-S. Chua, L.-T. Chia (Eds.), Advances in Multimedia Modeling, Part II. XVIII, 743 pages. 2006.

Vol. 4351: T.-J. Cham, J. Cai, C. Dorai, D. Rajan, T.-S. Chua, L.-T. Chia (Eds.), Advances in Multimedia Modeling, Part I. XIX, 797 pages. 2006.

Vol. 4349: B. Cook, A. Podelski (Eds.), Verification, Model Checking, and Abstract Interpretation. XI, 395 pages. 2007.

Vol. 4348: S.T. Taft, R.A. Duff, R.L. Brukardt, E. Ploedereder, P. Leroy (Eds.), Ada 2005 Reference Manual. XXII, 765 pages. 2006.

Vol. 4347: J. Lopez (Ed.), Critical Information Infrastructures Security. X, 286 pages. 2006.

Vol. 4346: L. Brim, B. Haverkort, M. Leucker, J. van de Pol (Eds.), Formal Methods: Applications and Technology. X, 363 pages. 2007.

Vol. 4345: N. Maglaveras, I. Chouvarda, V. Koutkias, R. Brause (Eds.), Biological and Medical Data Analysis. XIII, 496 pages. 2006. (Sublibrary LNBI).

Vol. 4344: V. Gruhn, F. Oquendo (Eds.), Software Architecture. X, 245 pages. 2006.

Vol. 4342: H. de Swart, E. Orłowska, G. Schmidt, M. Roubens (Eds.), Theory and Applications of Relational Structures as Knowledge Instruments II. X, 373 pages. 2006. (Sublibrary LNAI).

Vol. 4341: P.Q. Nguyen (Ed.), Progress in Cryptology - VIETCRYPT 2006. XI, 385 pages. 2006.

Vol. 4340: R. Prodan, T. Fahringer, Grid Computing. XXIII, 317 pages. 2007.

Vol. 4339: E. Ayguadé, G. Baumgartner, J. Ramanujam, P. Sadayappan (Eds.), Languages and Compilers for Parallel Computing. XI, 476 pages. 2006.

Vol. 4338: P. Kalra, S. Peleg (Eds.), Computer Vision, Graphics and Image Processing. XV, 965 pages. 2006.

Vol. 4337: S. Arun-Kumar, N. Garg (Eds.), FSTTCS 2006: Foundations of Software Technology and Theoretical Computer Science. XIII, 430 pages. 2006.

Vol. 4336: V.R. Basili, H.D. Rombach, K. Schneider, B. Kitchenham, D. Pfahl, R.W. Selby (Eds.), Empirical Software Engineering Issues. XVII, 194 pages. 2007.

Vol. 4335: S.A. Brueckner, S. Hassas, M. Jelasity, D. Yamins (Eds.), Engineering Self-Organising Systems. XII, 212 pages. 2007. (Sublibrary LNAI).

Vol. 4334: B. Beckert, R. Hähnle, P.H. Schmitt (Eds.), Verification of Object-Oriented Software. XXIX, 658 pages. 2007. (Sublibrary LNAI).

Vol. 4333: U. Reimer, D. Karagiannis (Eds.), Practical Aspects of Knowledge Management. XII, 338 pages. 2006. (Sublibrary LNAI).

Vol. 4332: A. Bagchi, V. Atluri (Eds.), Information Systems Security. XV, 382 pages. 2006.

Vol. 4331: G. Min, B. Di Martino, L.T. Yang, M. Guo, G. Ruenger (Eds.), Frontiers of High Performance Computing and Networking – ISPA 2006 Workshops. XXXVII, 1141 pages. 2006.

Vol. 4330: M. Guo, L.T. Yang, B. Di Martino, H.P. Zima, J. Dongarra, F. Tang (Eds.), Parallel and Distributed Processing and Applications. XVIII, 953 pages. 2006.

Vol. 4329: R. Barua, T. Lange (Eds.), Progress in Cryptology - INDOCRYPT 2006. X, 454 pages. 2006.

Vol. 4328: D. Penkler, M. Reitenspiess, F. Tam (Eds.), Service Availability. X, 289 pages. 2006.

Vol. 4327: M. Baldoni, U. Endriss (Eds.), Declarative Agent Languages and Technologies IV. VIII, 257 pages. 2006. (Sublibrary LNAI).

Vol. 4326: S. Göbel, R. Malkewitz, I. Iurgel (Eds.), Technologies for Interactive Digital Storytelling and Entertainment. X, 384 pages. 2006.

Vol. 4325: J. Cao, I. Stojmenovic, X. Jia, S.K. Das (Eds.), Mobile Ad-hoc and Sensor Networks. XIX, 887 pages. 2006.

Vol. 4323: G. Doherty, A. Blandford (Eds.), Interactive Systems. XI, 269 pages. 2007.

Vol. 4322: F. Kordon, J. Sztipanovits (Eds.), Reliable Systems on Unreliable Networked Platforms. XIV, 317 pages. 2007.

Vol. 4320: R. Gotzhein, R. Reed (Eds.), System Analysis and Modeling: Language Profiles. X, 229 pages. 2006.

Vol. 4319: L.-W. Chang, W.-N. Lie (Eds.), Advances in Image and Video Technology. XXVI, 1347 pages. 2006.

Vol. 4318: H. Lipmaa, M. Yung, D. Lin (Eds.), Information Security and Cryptology. XI, 305 pages. 2006.

Vol. 4317: S.K. Madria, K.T. Claypool, R. Kannan, P. Uppuluri, M.M. Gore (Eds.), Distributed Computing and Internet Technology. XIX, 466 pages. 2006.

Vol. 4316: M.M. Dalkilic, S. Kim, J. Yang (Eds.), Data Mining and Bioinformatics. VIII, 197 pages. 2006. (Sublibrary LNBI).

Vol. 4314: C. Freksa, M. Kohlhase, K. Schill (Eds.), KI 2006: Advances in Artificial Intelligence. XII, 458 pages. 2007. (Sublibrary LNAI).

Vol. 4313: T. Margaria, B. Steffen (Eds.), Leveraging Applications of Formal Methods. IX, 197 pages. 2006.

Vol. 4312: S. Sugimoto, J. Hunter, A. Rauber, A. Morishima (Eds.), Digital Libraries: Achievements, Challenges and Opportunities. XVIII, 571 pages. 2006.

Vol. 4311: K. Cho, P. Jacquet (Eds.), Technologies for Advanced Heterogeneous Networks II. XI, 253 pages. 2006.

¥603.00元

Table of Contents

Public Key Crypto Applications/Virus Protection

Cyber Indication/Intrusion Detection

Biometrics/Security Trust Management

Secure Software/Systems

Smart Cards/Secure Hardware

Mobile Security

DRM/Information Hiding/Ubiquitous Computing Security/P2P Security

Privacy/Anonymity

Internet and Wireless Security

Controllable Ring Signatures

Wei Gao[1,⋆], Guilin Wang[2], Xueli Wang[3], and Dongqing Xie[4]

[1] College of Mathematics and Econometrics, Hunan University,
Changsha 410082, China
sdgaowei@yahoo.com.cn

[2] Institute for Infocomm Research, 21 Heng Mui Keng Terrace,
Singapore 119613
glwang@i2r.a-star.edu.sg

[3] School of Mathematics Science, South China Normal University,
Guangzhou 510631, China
wangxuyuyan@yahoo.com.cn

[4] School of Computer and Communication, Hunan University,
Changsha 410082, China
dqxie@hnu.cn

Abstract. This paper introduces a new concept called controllable ring signature which is ring signature with additional properties as follow. (1) Anonymous identification: by an anonymous identification protocol, the real signer can anonymously prove his authorship of the ring signature to the verifier. And this proof is non-transferable. (2) Linkable signature: the real signer can generate an anonymous signature such that every one can verify whether both this anonymous signature and the ring signature are generated by the same anonymous signer. (3) Convertibility: the real signer can convert a ring signature into an ordinary signature by revealing the secret information about the ring signature. These additional properties can fully ensure the interests of the real signer. Especially, compared with a standard ring signature, a controllable ring signature is more suitable for the classic application of leaking secrets. We construct a controllable ring signature scheme which is provably secure according to the formal definition.

1 Introduction

The concept of ring signature was introduced by Rivest, Shamir and Tauman in [17]. It enables any individual to spontaneously conscript arbitrarily $n-1$ entities and generate a publicly verifiable 1-out-of-n signature on behalf of the whole group (called a ring), yet the actual signer remains anonymous. Many extensions of a standard ring signature, such as linkable ring signature [12], convertible ring signature [10], separable ring signature [2,11], threshold ring signature [3], ID-based ring signature [4], have been proposed in the literature. Ring signature and its variants have been used in many applications such

[⋆] This author is partially supported by CNF10271042 and CNF60373085.

J.K. Lee, O. Yi, and M. Yung (Eds.): WISA 2006, LNCS 4298, pp. 1–14, 2007.

as leaking secrets [17], designated verifier signature [17], anonymous identification/authentication for ad hoc groups [3], e-voting [12], e-cash and attestation in [18] and so on.

For the motivation of our new concept, we revisit the classic application of ring signatures in leaking secrets. Suppose that Bob (also known as "Deep Throat") is a member of the cabinet of Lower Kryptonia, and that Bob wishes to leak a juicy fact to a journalist about the escapades of the Prime Minister, in such a way that Bob remains anonymous, yet such that the journalist is convinced that the leak was indeed from a cabinet member. At a glance, it seems that a standard ring signature can help Bob to perfectly complete this task: he signs the message using a ring signature scheme on behalf of the whole cabinet. However, the following cases will show that a standard ring signature is not enough for leaking secrets in the real world.

(1) Suppose that another cabinet member Charlie is a good friend of the Prime Minister. To help the Prime Minister, Charlie generates a ring signature on an announcement. It states that he is the leaker and the previous published story about the Prime Minister is not true but a political joke. Of course, Bob's ring signature and Charlie's ring signature use the same "ring" – the whole cabinet. Now, how can Bob prevent this impersonation?
(2) Suppose that the journalist is very interested in these leaked secrets and wants to communicate with the real signer in order to discuss more details. So the journalist publishes his telephone number and wants the real signerto contact him through an anonymous phone call. How can Bob convince the journalist that the anonymous call is from the real signer through a untransferable proof?
(3) Suppose that Bob needs to publish further proofs for the escapades of the Prime Minister. How can Bob make people believe that both the previous secrets and these further proofs are leaked by the same anonymous cabinet member?
(4) After the disgraced Prime Minister is disposed, Bob maybe wants to remove the anonymity of the ring signature. In other words, how can Bob convert the ring signature into a standard digital signature?

Roughly speaking, (2) motivate the topic of secure anonymous identification; (3) can be captured by the notion of the linkability of anonymous signatures; (4) can be formalized as the notion of convertibility of a ring signature.

1.1 Related Work

Some extensions of a standard ring signature can only partially solve the above mentioned problems. In fact, the above problems were not so comprehensively pointed out in existing literature. Now we briefly review these related work.

Linkable ring signatures proposed in [12] have some limitations for leaking secrets. First, the schemes in [12] are not unconditionally but computationally anonymous. Secondly, every one can deny a ring signature if he is not the real signer. Thirdly, the real signer can't deny the ring signature generated by himself. In fact, in [12], the linkability of a ring signature was proposed mainly for restricting the real signer. For example, a linkable ring signature can prevent a ring member from generating two ring signatures on the message in the applications such as E-cash and E-voting. On the contrary, in the application of leaking secrets, the attention should be focused on how to fully ensure the interests of the real signer.

The convertible ring signature scheme proposed in [10] is the extension of a ring signature scheme proposed in [17]. It deals with only the convertibility of the ring signature scheme. And their construction cannot be trivially extended to deal with the linkability and anonymous identification. Additionally, the authors did not formalize the security model for the convertibility of ring signatures and their analysis is too simple.

The modified ring signature in [17] can guarantee only the computational anonymity. The proposed way can be used to show that a non-signer is not the real signer. A similar way can be used to show who is the real signer. In fact, they proposed a way to convert a ring signature to an ordinary signature. However, it seems difficult to extend their way to deal with the properties of linkability and anonymous authorship of a ring signature.

1.2 Contributions

Our contributions are twofold, as listed below. On the one hand, we revisit the classic application of ring signatures in leaking secrets and point out a list of practical problems unsolved by a standard ring signature. Motivated by these problems, we formalize the new notion of controllable ring signature. It is a useful cryptographic primitive which can fully ensure the interests of the real signer and rightly restrict him as follows.

(1) The real signer remains unconditionally anonymous only if he himself exposes his identity.

(2) Despite the unconditional anonymity, the real signer has enough powers to control his signature in the sense that he can anonymously prove his authorship, generate a linkable signature, and convert the controllable ring signature.

(3) Despite the full power to control his signature, the real signer is rightly restricted since he is not able to generate a controllable ring signature and then convince a third party that it is generated by others.

(4) Despite the unconditional anonymity, any other party (non-signer) cannot abuse the anonymity. For example, there is no way for him to present the proof that the ring signature is (or not) due to him.

On the other hand, we propose an efficient construction of a controllable ring signature, which is based on the standard ring signature of Abe et al.[2]. And the underlying paradigm may also be used to transform other standard ring signatures to controllable ones.