Helger Lipmaa
Moti Yung
Dongdai Lin (Eds.)

LNCS 4318

Information Security and Cryptology

Second SKLOIS Conference, Inscrypt 2006
Beijing, China, November/December 2006
Proceedings

Springer

Helger Lipmaa Moti Yung
Dongdai Lin (Eds.)

Information Security and Cryptology

Second SKLOIS Conference, Inscrypt 2006
Beijing, China, November 29 - December 1, 2006
Proceedings

Springer

Volume Editors

Helger Lipmaa
Adastral Postgraduate Campus
University College
London, UK
E-mail: h.lipmaa@cs.ucl.ac.uk

Moti Yung
Computer Science Department
Columbia University
New York, USA
E-mail: moti@cs.columbia.edu

Dongdai Lin
SKLOIS, Institute of Software
Chinese Academy of Sciences
Beijing 100080, China
E-mail: ddlin@is.iscas.ac.cn

Library of Congress Control Number: 2006936729

CR Subject Classification (1998): E.3, D.4.6, F.2.1, C.2, J.1, C.3, K.4.4, K.6.5

LNCS Sublibrary: SL 4 – Security and Cryptology

ISSN 0302-9743
ISBN-10 3-540-49608-4 Springer Berlin Heidelberg New York
ISBN-13 978-3-540-49608-3 Springer Berlin Heidelberg New York

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 11937807 06/3142 5 4 3 2 1 0

Lecture Notes in Computer Science 4318

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

Editorial Board

Preface

The second SKLOIS Conference on Information Security and Cryptology 2006 (Inscrypt, formerly CISC) was organized by the State Key Laboratory of Information Security of the Chinese Academy of Sciences. This international conference was held in Beijing, China and was sponsored by the Institute of Software, the Chinese Academy of Sciences, the Graduate University of Chinese Academy of Sciences and the National Natural Science Foundations of China. The conference proceedings, with contributed papers, are published by Springer in this volume of *Lecture Notes in Computer Science* (LNCS).

The research areas covered by Inscrypt have been gaining increased visibility recently since modern computing and communication infrastructures and applications require increased security, trust and safety. Indeed important fundamental, experimental and applied work has been done in wide areas of cryptography and information security research in recent years. Accordingly, the program of Inscrypt 2006 covered numerous fields of research within these areas.

The International Program Committee of the conference received a total of 225 submissions, from which only 23 submissions were selected for presentation at the regular papers track and are part of this volume. In addition to this track, the conference also hosted a short paper track of 13 presentations that were carefully selected as well. All anonymous submissions were reviewed by experts in the relevant areas and based on their ranking, technical remarks and strict selection criteria the papers were selected to the various tracks.

Many people and organizations helped in making the conference a reality. We would like to take this opportunity to thank the Program Committee members and the external experts for their invaluable help in producing the conference program. We would like to further thank the conference Organizing Committee. Special thanks are due to Dongdai Lin for his excellent help in organizing the conference and the proceedings. We wish to thank the various sponsors and, last but not least, we also express our thanks to all the authors who submitted papers to the conference, the invited speakers, the session chairs and all the conference attendees.

November 2006 Helger Lipmaa and Moti Yung

Inscrypt (formerly CISC) 2006

2nd SKLOIS Conference on Information Security and Cryptology

Beijing, China November 29 - December 1, 2006

Sponsored and organized by

State Key Laboratory of Information Security
(Chinese Academy of Sciences)

General Chair

Dengguo Feng	SKLOIS, Chinese Academy of Sciences, China

Program Co-chairs

Helger Lipmaa	University College London, UK
Moti Yung	RSA Labs and Columbia University, USA

Program Committee

N. Asokan	Nokia, Finland
Catharina Candolin	SET-Security Oy, Finland
Kefei Chen	Shanhai Jiaotong University, China
Ee Chien Chang	NUS, Singapore
Debra Cook	Bell Labs, USA
Claudia Diaz	K.U. Leuven, Belgium
Orr Dunkelman	Technion, Israel
Nelly Fazio	IBM Almaden, USA
Kris Gaj	George Mason University, USA
Juan Garay	Bell Labs, USA
Minaxi Gupta	Indiana University, USA
Florian Hess	TU Berlin, Germany
Yupu Hu	Xidian University, China
Tetsu Iwata	Nagoya University, Japan
Aggelos Kiayias	University of Connecticut, USA
Kaoru Kurosawa	Ibaraki University, Japan
Peeter Laud	University of Tartu, Estonia
Benoit Libert	UCL, Belgium

Dongdai Lin	SKLOIS, China
Javier Lopez	University of Malaga, Spain
Masahiro Mambo	Tsukuba University, Japan
Wenbo Mao	HP Shanghai, China
Steven Myers	Indiana University, USA
Lan Nguyen	WinMagic Inc., Canada
Hieu Phan	UCL, UK
Raphael Phan	Swinburne University of Technology, Malaysia
Markku-Juhani O. Saarinen	Royal Holloway, UK
Palash Sarkar	ISI, India
Nitesh Saxena	Polytechnic University, USA
Katja Schmidt-Samoa	TU Darmstadt, Germany
Berry Schoenmakers	Eindhoven University of Technology, Netherlands
Yiannis Stamatiou	CTI, Greece
Rainer Steinwandt	FAU, USA
Ivan Visconti	University of Salerno, Italy
Guilin Wang	I2R, Singapore
Huaxiong Wang	Macquarie University, Australia
Xiaoyun Wang	Tsinghua University, China
Yunlei Zhao	Fudan University, China

Proceedings Co-editors

Helger Lipmaa	University College London, UK
Moti Yung	RSA Labs and Columbia University, USA
Dongdai Lin	Chinese Academy of Sciences, China

Organizing Committee

Dongdai Lin	SKLOIS, Chinese Academy of Sciences, China
Jiwu Jing	SKLOIS, Chinese Academy of Sciences, China
Chuankun Wu	SKLOIS, Chinese Academy of Sciences, China
Wenling Wu	SKLOIS, Chinese Academy of Sciences, China
Zhenfeng Zhang	SKLOIS, Chinese Academy of Sciences, China

Secretary and Treasurer

Yi Qin	Chinese Academy of Sciences, China

Lecture Notes in Computer Science

For information about Vols. 1–4216

please contact your bookseller or Springer

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

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.

Vol. 4306: Y. Avrithis, Y. Kompatsiaris, S. Staab, N.E. O'Connor (Eds.), Semantic Multimedia. XII, 241 pages. 2006.

Vol. 4302: J. Domingo-Ferrer, L. Franconi (Eds.), Privacy in Statistical Databases. XI, 383 pages. 2006.

Vol. 4300: Y.Q. Shi (Ed.), Transactions on Data Hiding and Multimedia Security I. IX, 139 pages. 2006.

Vol. 4296: M.S. Rhee, B. Lee (Eds.), Information Security and Cryptology – ICISC. XIII, 358 pages. 2006.

Vol. 4295: J.D. Carswell, T. Tezuka (Eds.), Web and Wireless Geographical Information Systems. XI, 269 pages. 2006.

Vol. 4293: A. Gelbukh, C.A. Reyes-Garcia (Eds.), MICAI 2006: Advances in Artificial Intelligence. XXVIII, 1232 pages. 2006. (Sublibrary LNAI).

Vol. 4292: G. Bebis, R. Boyle, B. Parvin, D. Koracin, P. Remagnino, A. Nefian, G. Meenakshisundaram, V. Pascucci, J. Zara, J. Molineros, H. Theisel, T. Malzbender (Eds.), Advances in Visual Computing, Part II. XXXII, 906 pages. 2006.

Vol. 4291: G. Bebis, R. Boyle, B. Parvin, D. Koracin, P. Remagnino, A. Nefian, G. Meenakshisundaram, V. Pascucci, J. Zara, J. Molineros, H. Theisel, T. Malzbender (Eds.), Advances in Visual Computing, Part I. XXXI, 916 pages. 2006.

Vol. 4290: M. van Steen, M. Henning (Eds.), Middleware 2006. XIII, 425 pages. 2006.

Vol. 4284: X. Lai, K. Chen (Eds.), Advances in Cryptology – ASIACRYPT 2006. XIV, 468 pages. 2006.

Vol. 4283: Y.Q. Shi, B. Jeon (Eds.), Digital Watermarking. XII, 474 pages. 2006.

Vol. 4281: K. Barkaoui, A. Cavalcanti, A. Cerone (Eds.), Theoretical Aspects of Computing - ICTAC 2006. XV, 371 pages. 2006.

Vol. 4280: A.K. Datta, M. Gradinariu (Eds.), Stabilization, Safety, and Security of Distributed Systems. XVII, 590 pages. 2006.

Vol. 4279: N. Kobayashi (Ed.), Programming Languages and Systems. XI, 423 pages. 2006.

Vol. 4278: R. Meersman, Z. Tari, P. Herrero (Eds.), On the Move to Meaningful Internet Systems 2006: OTM 2006 Workshops, Part II. XLV, 1004 pages. 2006.

Vol. 4277: R. Meersman, Z. Tari, P. Herrero (Eds.), On the Move to Meaningful Internet Systems 2006: OTM 2006 Workshops, Part I. XLV, 1009 pages. 2006.

Vol. 4276: R. Meersman, Z. Tari (Eds.), On the Move to Meaningful Internet Systems 2006: CoopIS, DOA, GADA, and ODBASE, Part II. XXXII, 752 pages. 2006.

Vol. 4275: R. Meersman, Z. Tari (Eds.), On the Move to Meaningful Internet Systems 2006: CoopIS, DOA, GADA, and ODBASE, Part I. XXXI, 1115 pages. 2006.

Vol. 4273: I. Cruz, S. Decker, D. Allemang, C. Preist, D. Schwabe, P. Mika, M. Uschold, L. Aroyo (Eds.), The Semantic Web - ISWC 2006. XXIV, 1001 pages. 2006.

Vol. 4272: P. Havinga, M. Lijding, N. Meratnia, M. Wegdam (Eds.), Smart Sensing and Context. XI, 267 pages. 2006.

Vol. 4271: F.V. Fomin (Ed.), Graph-Theoretic Concepts in Computer Science. XIII, 358 pages. 2006.

Vol. 4270: H. Zha, Z. Pan, H. Thwaites, A.C. Addison, M. Forte (Eds.), Interactive Technologies and Sociotechnical Systems. XVI, 547 pages. 2006.

Vol. 4269: R. State, S. van der Meer, D. O'Sullivan, T. Pfeifer (Eds.), Large Scale Management of Distributed Systems. XIII, 282 pages. 2006.

Vol. 4268: G. Parr, D. Malone, M. Ó Foghlú (Eds.), Autonomic Principles of IP Operations and Management. XIII, 237 pages. 2006.

Vol. 4267: A. Helmy, B. Jennings, L. Murphy, T. Pfeifer (Eds.), Autonomic Management of Mobile Multimedia Services. XIII, 257 pages. 2006.

Vol. 4266: H. Yoshiura, K. Sakurai, K. Rannenberg, Y. Murayama, S. Kawamura (Eds.), Advances in Information and Computer Security. XIII, 438 pages. 2006.

Vol. 4265: L. Todorovski, N. Lavrač, K.P. Jantke (Eds.), Discovery Science. XIV, 384 pages. 2006. (Sublibrary LNAI).

Vol. 4264: J.L. Balcázar, P.M. Long, F. Stephan (Eds.), Algorithmic Learning Theory. XIII, 393 pages. 2006. (Sublibrary LNAI).

Vol. 4263: A. Levi, E. Savas, H. Yenigün, S. Balcisoy, Y. Saygin (Eds.), Computer and Information Sciences – ISCIS 2006. XXIII, 1084 pages. 2006.

Vol. 4261: Y. Zhuang, S. Yang, Y. Rui, Q. He (Eds.), Advances in Multimedia Information Processing - PCM 2006. XXII, 1040 pages. 2006.

Vol. 4260: Z. Liu, J. He (Eds.), Formal Methods and Software Engineering. XII, 778 pages. 2006.

Vol. 4259: S. Greco, Y. Hata, S. Hirano, M. Inuiguchi, S. Miyamoto, H.S. Nguyen, R. Słowiński (Eds.), Rough Sets and Current Trends in Computing. XXII, 951 pages. 2006. (Sublibrary LNAI).

Vol. 4257: I. Richardson, P. Runeson, R. Messnarz (Eds.), Software Process Improvement. XI, 219 pages. 2006.

Vol. 4256: L. Feng, G. Wang, C. Zeng, R. Huang (Eds.), Web Information Systems – WISE 2006 Workshops. XIV, 320 pages. 2006.

Vol. 4255: K. Aberer, Z. Peng, E.A. Rundensteiner, Y. Zhang, X. Li (Eds.), Web Information Systems – WISE 2006. XIV, 563 pages. 2006.

Vol. 4254: T. Grust, H. Höpfner, A. Illarramendi, S. Jablonski, M. Mesiti, S. Müller, P.-L. Patranjan, K.-U. Sattler, M. Spiliopoulou, J. Wijsen (Eds.), Current Trends in Database Technology – EDBT 2006. XXXI, 932 pages. 2006.

Vol. 4253: B. Gabrys, R.J. Howlett, L.C. Jain (Eds.), Knowledge-Based Intelligent Information and Engineering Systems, Part III. XXXII, 1301 pages. 2006. (Sublibrary LNAI).

Vol. 4252: B. Gabrys, R.J. Howlett, L.C. Jain (Eds.), Knowledge-Based Intelligent Information and Engineering Systems, Part II. XXXIII, 1335 pages. 2006. (Sublibrary LNAI).

Vol. 4251: B. Gabrys, R.J. Howlett, L.C. Jain (Eds.), Knowledge-Based Intelligent Information and Engineering Systems, Part I. LXVI, 1297 pages. 2006. (Sublibrary LNAI).

Vol. 4249: L. Goubin, M. Matsui (Eds.), Cryptographic Hardware and Embedded Systems - CHES 2006. XII, 462 pages. 2006.

Vol. 4248: S. Staab, V. Svátek (Eds.), Managing Knowledge in a World of Networks. XIV, 400 pages. 2006. (Sublibrary LNAI).

Vol. 4247: T.-D. Wang, X. Li, S.-H. Chen, X. Wang, H. Abbass, H. Iba, G. Chen, X. Yao (Eds.), Simulated Evolution and Learning. XXI, 940 pages. 2006.

Vol. 4246: M. Hermann, A. Voronkov (Eds.), Logic for Programming, Artificial Intelligence, and Reasoning. XIII, 588 pages. 2006. (Sublibrary LNAI).

Vol. 4245: A. Kuba, L.G. Nyúl, K. Palágyi (Eds.), Discrete Geometry for Computer Imagery. XIII, 688 pages. 2006.

Vol. 4244: S. Spaccapietra (Ed.), Journal on Data Semantics VII. XI, 267 pages. 2006.

Vol. 4243: T. Yakhno, E.J. Neuhold (Eds.), Advances in Information Systems. XIII, 420 pages. 2006.

Vol. 4242: A. Rashid, M. Aksit (Eds.), Transactions on Aspect-Oriented Software Development II. IX, 289 pages. 2006.

Vol. 4241: R.R. Beichel, M. Sonka (Eds.), Computer Vision Approaches to Medical Image Analysis. XI, 262 pages. 2006.

Vol. 4239: H.Y. Youn, M. Kim, H. Morikawa (Eds.), Ubiquitous Computing Systems. XVI, 548 pages. 2006.

Vol. 4238: Y.-T. Kim, M. Takano (Eds.), Management of Convergence Networks and Services. XVIII, 605 pages. 2006.

Vol. 4237: H. Leitold, E. Markatos (Eds.), Communications and Multimedia Security. XII, 253 pages. 2006.

Vol. 4236: L. Breveglieri, I. Koren, D. Naccache, J.-P. Seifert (Eds.), Fault Diagnosis and Tolerance in Cryptography. XIII, 253 pages. 2006.

Vol. 4234: I. King, J. Wang, L. Chan, D. Wang (Eds.), Neural Information Processing, Part III. XXII, 1227 pages. 2006.

Vol. 4233: I. King, J. Wang, L. Chan, D. Wang (Eds.), Neural Information Processing, Part II. XXII, 1203 pages. 2006.

Vol. 4232: I. King, J. Wang, L. Chan, D. Wang (Eds.), Neural Information Processing, Part I. XLVI, 1153 pages. 2006.

Vol. 4231: J. F. Roddick, R. Benjamins, S. Si-Saïd Cherfi, R. Chiang, C. Claramunt, R. Elmasri, F. Grandi, H. Han, M. Hepp, M. Hepp, M. Lytras, V.B. Mišić, G. Poels, I.-Y. Song, J.D. Trujillo, C. Vangenot (Eds.), Advances in Conceptual Modeling - Theory and Practice. XXII, 456 pages. 2006.

Vol. 4230: C. Priami, A. Ingólfsdóttir, B. Mishra, H.R. Nielson (Eds.), Transactions on Computational Systems Biology VII. VII, 185 pages. 2006. (Sublibrary LNBI).

Vol. 4229: E. Najm, J.F. Pradat-Peyre, V.V. Donzeau-Gouge (Eds.), Formal Techniques for Networked and Distributed Systems - FORTE 2006. X, 486 pages. 2006.

Vol. 4228: D.E. Lightfoot, C.A. Szyperski (Eds.), Modular Programming Languages. X, 415 pages. 2006.

Vol. 4227: W. Nejdl, K. Tochtermann (Eds.), Innovative Approaches for Learning and Knowledge Sharing. XVII, 721 pages. 2006.

Vol. 4226: R.T. Mittermeir (Ed.), Informatics Education – The Bridge between Using and Understanding Computers. XVII, 319 pages. 2006.

Vol. 4225: J.F. Martínez-Trinidad, J.A. Carrasco Ochoa, J. Kittler (Eds.), Progress in Pattern Recognition, Image Analysis and Applications. XIX, 995 pages. 2006.

Vol. 4224: E. Corchado, H. Yin, V. Botti, C. Fyfe (Eds.), Intelligent Data Engineering and Automated Learning – IDEAL 2006. XXVII, 1447 pages. 2006.

Vol. 4223: L. Wang, L. Jiao, G. Shi, X. Li, J. Liu (Eds.), Fuzzy Systems and Knowledge Discovery. XXVIII, 1335 pages. 2006. (Sublibrary LNAI).

Vol. 4222: L. Jiao, L. Wang, X. Gao, J. Liu, F. Wu (Eds.), Advances in Natural Computation, Part II. XLII, 998 pages. 2006.

Vol. 4221: L. Jiao, L. Wang, X. Gao, J. Liu, F. Wu (Eds.), Advances in Natural Computation, Part I. XLI, 992 pages. 2006.

Vol. 4220: C. Priami, G. Plotkin (Eds.), Transactions on Computational Systems Biology VI. VII, 247 pages. 2006. (Sublibrary LNBI).

Vol. 4219: D. Zamboni, C. Kruegel (Eds.), Recent Advances in Intrusion Detection. XII, 331 pages. 2006.

Vol. 4218: S. Graf, W. Zhang (Eds.), Automated Technology for Verification and Analysis. XIV, 540 pages. 2006.

Vol. 4217: P. Cuenca, L. Orozco-Barbosa (Eds.), Personal Wireless Communications. XV, 532 pages. 2006.

Table of Contents

Digital Signature Schemes

Sequences and Stream Ciphers

Symmetric-Key Cryptography

Cryptographic Schemes

Network Security

Access Control

Computer and Applications Security

Web and Media Security

Cryptanalysis of Two Signature Schemes Based on Bilinear Pairings in CISC '05

Haeryong Park[1,*], Zhengjun Cao[2], Lihua Liu[3], Seongan Lim[4,**], Ikkwon Yie[4], and Kilsoo Chun[1]

[1] Korea Information Security Agency (KISA), Seoul, Korea 138-803
{hrpark, kschun}@kisa.or.kr
[2] Department of Mathematics, Shanghai University, Shanghai, China 200444
zjcamss@163.com
[3] Department of Information and Computation Sciences, Shanghai Maritime University, Shanghai, China 200135
[4] Department of Mathematics, Inha University, Incheon, Korea 402-751
{seongannym, ikyie}@inha.ac.kr

Abstract. The bilinearity of pairings allows efficient signature verification for signature schemes based on discrete logarithm type problem and often provides useful additional functionalities to signature schemes. In recent years, bilinear pairings have been widely used to create signature schemes. But the bilinearity can also be an attack point in uncarefully designed protocols. We cryptanalyze two signature schemes presented at CISC '05, Cheng et al.'s group signature scheme and Gu et al.'s ID-based verifiably encrypted signature scheme, both based on bilinear pairings. We show that their improper uses of a bilinear pairing lead to untraceable group signatures for Cheng et al.'s group signature scheme and universally forgeable signatures for Gu et al.'s ID-based verifiably encrypted signature scheme.

Keywords: bilinear pairing, group signature, ID-based cryptography, verifiably encrypted signature.

1 Introduction

Recently, bilinear pairings have been widely used to create many signature schemes with additional functionality or better efficiency. For example, there have been papers on short signatures, group signatures, verifiably encrypted signatures, and many more. The linearity of bilinear pairings is very effective in terms of both "efficiency" and "functionality". But one should be careful so that the linearity should not be manipulated in a malicious way by an attacker.

In this paper, we shall show that two signature schemes proposed at CISC '05 based on bilinear pairings can be attacked by using the taking advantage of the bilinearity property.

* This work was supported by MIC.
** This work was supported by the KRF Grant (KRF-2004- R03-10023) funded by the Korean Government(MOEHRD).

H. Lipmaa, M. Yung, and D. Lin (Eds.): Inscrypt 2006, LNCS 4318, pp. 1–12, 2006.

Group signature. Basic security requirements of group signature schemes can be understood as *correctness*, *unforgeability*, *anonymity*, *unlinkability*, *traceability*, *exculpability*, and *coalition-resistance*. Bellare et al. formalized this large set of security requirements in terms of *correctness*, *Full-Anonymity Full-traceability* [5]. The traceability is one of the core security requirements of group signature. For group signature schemes, a signer (group member) might act as an adversary against the traceability property. Short group signature schemes using bilinear pairing have been developed by Boneh et al.[6]. For a secure group signature schemes based on bilinear pairings, it should be designed so the signer cannot treat the linearity in the group signature verification formula to generate an untraceable group signature.

In [11], Cheng et al. proposed group signature schemes using bilinear pairing by introducing SEM (SEcurity Mediator), an on-line third party. Their group signature schemes can be considered as a modification of regular signature scheme based on bilinear pairing [9]. They claimed that their schemes have traceability because no valid group signature can be generated without help from SEM. In this paper, we point out that the group signature schemes constructed by Cheng et al. allow to generate a untraceable group signature due to their improper use of bilinear pairing in the verification formula.

Verifiably encrypted signature. It's well known that Shamir [15] first proposed the idea of ID-based public key cryptography to simplify the key management procedure of traditional certificate-based PKI. Using bilinear maps defined on some elliptic curves, researchers have proposed many ID-based signature schemes [16,21,22] ever since the paper of Boneh and Franklin [7] was published.

Generally, Signer wants to show Verifier that he has signed a message, but dose not want Verifier to possess the signature. A verifiably encrypted signature is a special extension of common signature that gives such functionality. A verifiably encrypted signature enables the Signer to give Verifier a signature that is encrypted using Adjudicator's public key. The Verifier can check the validity of the signature, but the verifier cannot obtain any information on the signer's signature since the signature has been encrypted by Adjudicator's public key. The Adjudicator is a trusted third party, who can reveal the signature if needed. At a later stage when it is needed, the verifier can either obtain the signature from the signer or resort to the adjudicator who can reveal the signer's signature. The property, namely, Verifier cannot know the original signature corresponding to a verifiably encrypted signature, is very useful in some cases, such as online contract signing.

The basic security requirements of verifiably encrypted signature schemes are unforgeability and opacity [21]. The 'unforgeability' of verifiably encrypted signature scheme requires that it is difficult to forge a valid verifiably encrypted signature. In the signature verification of verifiably encrypted signature schemes, one needs both public keys of the Signer and the Adjudicator. Hence in pairing-based verifiably encrypted signature schemes, manipulating the linearity of the bilinear pairing in the verification formula using these two public keys should be prevented.

At CISC '05, an ID-based verifiably encrypted signature scheme has been proposed [12]. The authors claimed that its security was based on Hess's ID-based signature scheme [13], but we show that the scheme is universally forgeable in this paper. Our attack does not depend on any assumption. It is simple and direct. We only show how the linearity of the bilinear pairing can be treated using two public keys in order to get a valid verifiably encrypted signature.

Outline of this paper. Our paper is organized as follows. Section 2 describes some preliminaries. We discuss Cheng et al.'s group signature schemes [11] and explain our attacks on their schemes in Section 3. We also discuss Gu-Zhu's verifiable encrypted signature [12] and explain our attack on their scheme in Section 4. Finally we give our conclusion in Section 5.

2 Preliminaries

2.1 Bilinear Pairings and Intractable Problems

Let $(G_1, +)$ and $(G_2, \cdot)$ be two cyclic groups of prime order q and P be a cyclic generator of G_1. A map $e : G_1 \times G_1 \rightarrow G_2$ is called an *admissible bilinear pairing* if it satisfies the following properties:

1. Bilinear: $\forall A, B \in G_1, \forall \alpha, \beta \in Z_q,\ e(\alpha A, \beta B) = e(A, B)^{\alpha\beta}$;
2. Non-degenerate: $e(P, P)$ is a generator of G_2;
3. Computable: there is an efficient algorithm to compute $e(A, B)$ for any $A, B \in G_1$.

The bilinear pairing implementation of the above cases can be done using supersingular elliptic curves.

Let $a, b, c \in Z_q$. We consider the following problems on G_1.

1. The computational Diffie-Hellman problem (CDHP): Given $P, aP, bP \in G_1$, compute abP.
2. The decisional Diffie-Hellman problem (DDHP): Given $P, aP, bP, cP \in G_1$, decide if $abP = cP$.

When we discuss problems concerning an admissible bilinear pairing $e : G_1 \times G_1 \rightarrow G_2$, we usually assume that the CDHP in G_1, G_2 is intractable. We note that the existence of an admissible bilinear pairing makes the decisional Diffie-Hellman problem (DDHP) in G_1 easy. Thus, G_1 is a Gap Diffie-Hallman (GDH) Group, i.e., the CDHP is intractable while DDHP is easy.

2.2 Signature Verification Using Bilinear Pairings

Using bilinear pairings, it is possible to construct short signature schemes based on Diffie-Hellman-related problems. This is because, the bilinearity of pairings allows easy verification of the validity of a signature without solving DL type problem. A typical example of signatures scheme based on pairing is BLS short signature scheme proposed in [9] which we summarize informally below.

- Parameter: $(G, \cdot)$ and $(G_3, \cdot)$ are cyclic groups of order prime q and g is a generator of G.
- Signature generation: On input the message m and a private key x, the signature is $\sigma = H(m)^x$.
- Signature verification: For a given public key $v = g^x$, a message m, and a signature σ, the signature σ is valid if $(g, v, H(m), \sigma)$ is a valid DH-tuple.

If there is an efficiently computable bilinear pairing $\hat{e} : G \times G \rightarrow G_3$, one can easily check the validity of σ by checking $\hat{e}(g, \sigma) = \hat{e}(v, H(m))$.

3 Cheng-Zhu-Qiu-Wang's Group Signatures and Their Weakness

3.1 Group Signatures

Following the first work by Chaum and van Heyst in the year of 1991 [10], many group signature schemes were proposed and analyzed [4,3,6,17]. Additional functionality, such as providing anonymity of signers, is an important advantage of a group signature scheme over an ordinary signature schemes.

Group signatures are signatures that provide anonymity to the signer. Any group member can sign a message using his own private key. A verifier can tell that a group member has signed without knowing the identity of the signature's originator. But, in exceptional cases such as a legal dispute, the group manager (GM) can open any group signature. Anonymity of signer, namely, impossibility of identifying the original signer for a given group signature, is very useful in the cases when signer's privacy is required. The definition of group signature is as follows:

Definition 1. *(Group Signature [5]) A group signature scheme consists of three entities: signer, verifier and group manager. There are five algorithms,* ***Setup***, ***Join***, ***Sign***, ***Verify***, *and* ***Open***.

Setup: *This is generating the system parameters, a group public-private key pair* $(GPK; GSK)$.
Join: *This is generating the group member private key* SK
Sign: *Given a group member private key* SK*, a message* m*, and the system parameters, compute a group signature* σ *on* m.
Verify: *Given a group signature* σ*, a message* m*, the group public key, and the system parameters, verify that* σ *is a valid group signature on* m.
Open: *Given a group private key* GSK*, a message* m *and a group signature* σ *on* m*, output the original signer (group member) of* σ.

A large set of security requirements for group signatures have been introduced (e.g., unlinkability, unforgeability, collusion resistance, exculpability, and framing resistance) and later have been formalized in terms of 'full anonymity' and 'full traceability' [5].

Full anonymity. The anonymity requires that an adversary not in possession of the group manager's private key find it hard to recover the identity of the signer from its signature. Here the adversary is allowed to have the private keys of all group members in his attack to distinguish the corresponding identity of the signer.

Full Traceability. In case of misuse, signer anonymity can be revoked by the group manager. The full traceability requires that no colluding set of group members can create signatures that cannot be opened, or signatures that cannot be traced back to some member of the coalition.

Due to the controlled anonymity features (guaranteed anonymity in usual situation plus traceability in cases of disputes), group signature schemes are very useful cryptographic techniques for user privacy protection. Many efficient group signature schemes based on bilinear pairing were proposed recently. As in the regular signature schemes, the bilinearity of a bilinear pairing allows an efficient signature verification. However, the bilinearity can also be an attack point with respect to the traceability for group signature schemes. The group signatures proposed by Cheng et al. [11] are examples that allow to generate untraceable signatures since they didn't use the bilinear pairing properly. We shall discuss Cheng et al.'s schemes and their security flaw in the rest of this section.

3.2 Cheng-Zhu-Qiu-Wang's Group Signatures

In this section, we describe two Cheng-Zhu-Qiu-Wang's group signatures [11]. In their schemes, they introduced a trusted on-line third party, called a SEcurity Mediator (SEM) in addition to GM and a set of users (group members). A group member must get partial information from SEM to generate a valid group signature. Let $(G_1, +)$ and $(G_2, \cdot)$ be two cyclic groups of order q, P be a generator of G_1, and $e : G_1 \times G_1 \to G_2$ be an admissible bilinear pairing. Note that $H : \{0,1\}^* \to G_1$ is a hash function.

The mini group signature. The mini group signature is proposed as a group signature without exculpability property on GM [11].

Setup: Given a security parameter κ, GM generates the system parameters $Params = \{G_1, G_2, e, q, P, H\}$. GM chooses randomly $x \in Z_q^*$ and computes $P_{pub} = xP \in G_1$. The public-private key pair of the group is (P_{pub}, x).

Join: GM chooses randomly $x_i^u \in Z_q^*$ and computes $x_i^s = (x - x_i^u) \bmod q$. GM sends x_i^u to U_i and sends (x_i^s, U_i) to SEM. Thus U_i becomes a group member and his private key is x_i^u with the following properties.

- $x_i^u \neq x_j^u$ when $i \neq j$.
- $x_{i_1}^u + x_{i_2}^u + \cdots + x_{i_j}^u \neq x \bmod q$ for any positive integers i and j.
- $x_{i_1}^u + x_{i_2}^u + \cdots + x_{i_j}^u \neq x_{i_l}^u \bmod q$ for any positive integers i, j and l.

Sign: To generate a group signature on some message m, U_i sends $H(m)$ along with his identity to SEM. SEM checks that the group membership of U_i