Jong In Lim
Dong Hoon Lee (Eds.)

Information Security and Cryptology – ICISC 2003

LNCS 2971

6th International Conference
Seoul, Korea, November 2003
Revised Papers

Springer

Jong In Lim Dong Hoon Lee (Eds.)

Information Security and Cryptology – ICISC 2003

6th International Conference
Seoul, Korea, November 27-28, 2003
Revised Papers

Springer

Series Editors

Gerhard Goos, Karlsruhe University, Germany
Juris Hartmanis, Cornell University, NY, USA
Jan van Leeuwen, Utrecht University, The Netherlands

Volume Editors

Jong In Lim
Dong Hoon Lee
Korea University
1,5-Ka, Anam-dong Sungbuk-ku, Seoul, 136-701,Korea
E-mail:{jilim/donghlee}@korea.ac.kr

Library of Congress Control Number: 2004102811

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 3-540-21376-7 Springer-Verlag Berlin Heidelberg New York

Typesetting: Camera-ready by author, data conversion by DA-TeX Gerd Blumenstein
Printed on acid-free paper SPIN: 10992845 06/3142 5 4 3 2 1 0

Lecture Notes in Computer Science 2971

Edited by G. Goos, J. Hartmanis, and J. van Leeuwen

Springer
Berlin
Heidelberg
New York
Hong Kong
London
Milan
Paris
Tokyo

Preface

We would like to express a hearty welcome to all the participants of the 6th International Conference on Information Security and Cryptology (ICISC 2003). It was organized by the Korea Institute of Information Security and Cryptology (KIISC) and sponsored by the Korean Ministry of Information and Communication, and was held at the Seoul Olympic Parktel, Korea from November 27 to 28, 2003. As in the five previous years, it served as a forum to bring together researchers from academia and commercial developers from industry to discuss the current state of the art in information security and cryptology.

The Program Committee received 163 submissions from 25 countries and regions (Australia, Austria, Belgium, Canada, China, Finland, France, Germany, Hong Kong, India, Indonesia, Iran, Italy, Japan, Korea, Netherlands, Malaysia, Poland, Russia, Switzerland, Singapore, Taiwan, Turkey, UK, and USA), of which 32 papers were selected for presentation. All submissions were anonymously reviewed by at least 3 experts in the relevant areas. There were two invited talks, by Jonathan Katz and Jean-Jacques Quisquater.

We are very grateful to all the Program Committee members who devoted much effort and valuable time to reading and selecting the papers. We also thank the external experts who assisted the Program Committee in evaluating various papers. We owe special thanks to Jung Yeon Hwang and Judy Kang for always being available when their helping hand was needed.

Finally, we would like to thank all the authors who submitted papers to ICISC 2003, including those whose submissions were not successful, and the participants who together made this conference an intellectually stimulating event through their active contribution.

December 2003

Jong In Lim, Dong Hoon Lee

ICISC 2003

2003 International Conference on Information Security and Cryptology

Seoul Olympic Parktel, Seoul, Korea
November 27–28, 2003

Organized by

Korea Institute of Information Security and Cryptology (KIISC)
(http://www.kiisc.or.kr)

Sponsored by

MIC (Ministry of Information and Communication), Korea
(http://www.mic.go.kr)

Organization

General Chair

Se Hun Kim	KAIST, Korea

Program Co-chairs

Jong In Lim	Korea University, Korea
Dong Hoon Lee	Korea University, Korea

Program Committee

Ronald Cramer	Aarhus, Denmark
Zongduo Dai	Academia Sinica, China
Ed Dawson	Queensland University of Technology, Australia
Robert H. Deng	Institute for Infocomm Research, Singapore
Jovan Golic	Tilab, Telecom Italia, Italy
Gene Itkis	Boston University, USA
Markus Jakobsson	RSA Laboratories, USA
Kwangjo Kim	ICU, Korea
Pil Joong Lee	POSTECH, Korea
Seongan Lim	Korea Information Security Agency, Korea
Masahiro Mambo	Tohoku University, Japan
Sang Jae Moon	Kyungpook National University, Korea
Chanathip Namprempre	Thammasat University, Thailand
David Naccache	Gemplus Card International, France
Tatsuaki Okamoto	NTT, Japan
Choonsik Park	ETRI, Korea
Dingyi Pei	Chinese Academy of Science, China
David Pointcheval	CNRS/ENS, France
Bart Preneel	Katholieke Universiteit Leuven, Belgium
Jean-Jacques Quisquater	UCL, Belgium
Kouichi Sakurai	Kyushu University, Japan
Palash Sarkar	Indian Statistical Institute, India
Nigel Smart	University of Bristol, UK
Serge Vaudenay	EPFL, Switzerland
Sung-Ming Yen	National Central University, Taiwan
Moti Yung	Columbia University, USA

Organizing Committee Chair

Heung Youl Youm	Soonchunhyang University, Korea

Organizing Committee

HaGwang Soo Rhee	Sookmyung Women's University, Korea
Ji Hong Kim	Semyung University, Korea
Kyo Il Chung	ETRI, Korea
Jae Cheol Ha	Korea Nazarene University, Korea
Hong Geun Kim	KISA, Korea
Su Kyung Chae	MIC, Korea
Kyung Sim Kim	KIISC, Korea

External Reviewers

Alex Biryukov
Alex Dent
Andrew Clark
Beatrice Peirani
Bo-Ching Wu
Chang Seop Park
Chao-Chih Hsu
Chi-Dian Wu
Chien-ning Chen
Chong Hee KIM
Christophe De Canniere
Claude Barral
Dae Hyun Yum
Dan Page
Dario Catalano
Dingyi Pei
Dong Jin PARK
Emmanuel Bresson
Eric Brier
E-Transaction Protection Tech team
Eul Gyu Im
Frederik Vercauteren
G. Hanaoka
Geriant Price
Gildas Avoine
Gregory Neven
Guohua Xiong
Helena Handschuh
Helger Lipmaa
Henry Lee
Hisashi Inoue
Hsi-Chung Lin
Huafei Zhu
Hyeong Joon Kim
Hyeong Joong Kim
In Kook Park
Jacques Fournier
Jae Hwan Park
Javier Herranz Sotoca
Javier Herranz Sotoca
Jean Monnerat
Jean Sebastien Coron
Jean-Francois Dhem
Ji Hyun Jeong
John Malone-Lee
Jonghoon Shin
Joon-Hah Park
Joseph Lano
Juanma Gonzalez-Nieto
Julien Brouchier
JuSung Kang
Katsu Okeya
Kazu Fukushima
Kazuto Matsuo
Kenji Imamoto
Ki Sik Chang
Kishan Chand Gupta
Kun Peng

Lauren May
Lejla Batina
Lionel Victor
Louis Granboulan
Marc Joye
Mark Looi
Martijn Stam
Masanobu Koike
Matt Henricksen
Matthew Dailey
Mike Szydlo
Moriai Shiho
Mridul Nandi
Naouel Ben Salem
Nora Dabbous
Olivier Benoit
Olivier Chevassut
Pascal Guterma
Pascal Junod
Pascal Paillier
Philippe Oechslin
Pierre-Alain Fouque
Pierrick Gaudry
Pinakpani Pal
Pradeep Kumar Mishra
Qingjun Cai
R. Sakai
Renato Menicocci
Sang Gyoo SIM
Sang Yun Han
Sebastien Canard
Selwyn Russell
Seok Won Jeong
SeongTaek Chee
SeungJoo Kim
Shouhuai Xu
Shunsuke Araki
Simon Blackburn
Sourav Mukhopadhyay
Steven Galbraith
Subhamoy Maitra
Sugata Gangopadhyay
Sung Ho Yoo
Taweesak Kitkarnjanarat
Tieyan Li
Tomo Asano
Tony Rhodes
Toshihiro Tabata
Tsuyoshi Takagi
Vittorio Bagini
Vo Duc Liem
Xiaofeng Chen
Yaron Sella
Yasuyuki Sakai
Yasuyuki Sakai
Yeon Hyeong Yang
Yi Lu
Yong Ho Hwang
Yong Li
Yong Man Ro
Yongdong Wu
Yongyuth Permpoontanalarp
Young Tae Youn
YS Her
Yvonne hitchcock

Lecture Notes in Computer Science

For information about Vols. 1–2882

please contact your bookseller or Springer-Verlag

Vol. 3005: G.R. Raidl, S. Cagnoni, J. Branke, D.W. Corne, R. Drechsler, Y. Jin, C.G. Johnson, P. Machado, E. Marchiori, F. Rothlauf, G.D. Smith, G. Squillero (Eds.), Applications of Evolutionary Computing. XVII, 562 pages. 2004.

Vol. 3004: J. Gottlieb, G.R. Raidl (Eds.), Evolutionary Computation in Combinatorial Optimization. X, 241 pages. 2004.

Vol. 3003: M. Keijzer, U.-M. O'Reilly, S.M. Lucas, E. Costa, T. Soule (Eds.), Genetic Programming. XI, 410 pages. 2004.

Vol. 2998: Y. Kameyama, P.J. Stuckey (Eds.), Functional and Logic Programming. X, 307 pages. 2004.

Vol. 2997: S. McDonald, J. Tait (Eds.), Advances in Information Retrieval. XIII, 427 pages. 2004.

Vol. 2996: V. Diekert, M. Habib (Eds.), STACS 2004. XVI, 658 pages. 2004.

Vol. 2995: C. Jensen, S. Poslad, T. Dimitrakos (Eds.), Trust Management. XIII, 377 pages. 2004.

Vol. 2994: E. Rahm (Ed.), Data Integration in the Life Sciences. X, 221 pages. 2004. (Subseries LNBI).

Vol. 2993: R. Alur, G.J. Pappas (Eds.), Hybrid Systems: Computation and Control. XII, 674 pages. 2004.

Vol. 2992: E. Bertino, S. Christodoulakis, D. Plexousakis, V. Christophides, M. Koubarakis, K. Böhm, E. Ferrari (Eds.), Advances in Database Technology - EDBT 2004. XVIII, 877 pages. 2004.

Vol. 2991: R. Alt, A. Frommer, R.B. Kearfott, W. Luther (Eds.), Numerical Software with Result Verification. X, 315 pages. 2004.

Vol. 2989: S. Graf, L. Mounier (Eds.), Model Checking Software. X, 309 pages. 2004.

Vol. 2988: K. Jensen, A. Podelski (Eds.), Tools and Algorithms for the Construction and Analysis of Systems. XIV, 608 pages. 2004.

Vol. 2987: I. Walukiewicz (Ed.), Foundations of Software Science and Computation Structures. XIII, 529 pages. 2004.

Vol. 2986: D. Schmidt (Ed.), Programming Languages and Systems. XII, 417 pages. 2004.

Vol. 2985: E. Duesterwald (Ed.), Compiler Construction. X, 313 pages. 2004.

Vol. 2984: M. Wermelinger, T. Margaria-Steffen (Eds.), Fundamental Approaches to Software Engineering. XII, 389 pages. 2004.

Vol. 2983: S. Istrail, M.S. Waterman, A. Clark (Eds.), Computational Methods for SNPs and Haplotype Inference. IX, 153 pages. 2004. (Subseries LNBI).

Vol. 2982: N. Wakamiya, M. Solarski, J. Sterbenz (Eds.), Active Networks. XI, 308 pages. 2004.

Vol. 2981: C. Müller-Schloer, T. Ungerer, B. Bauer (Eds.), Organic and Pervasive Computing – ARCS 2004. XI, 339 pages. 2004.

Vol. 2980: A. Blackwell, K. Marriott, A. Shimojima (Eds.), Diagrammatic Representation and Inference. XV, 448 pages. 2004. (Subseries LNAI).

Vol. 2978: R. Groz, R.M. Hierons (Eds.), Testing of Communicating Systems. XII, 225 pages. 2004.

Vol. 2977: G. Di Marzo Serugendo, A. Karageorgos, O.F. Rana, F. Zambonelli (Eds.), Engineering Self-Organising Systems. X, 299 pages. 2004. (Subseries LNAI).

Vol. 2976: M. Farach-Colton (Ed.), LATIN 2004: Theoretical Informatics. XV, 626 pages. 2004.

Vol. 2973: Y. Lee, J. Li, K.-Y. Whang, D. Lee (Eds.), Database Systems for Advanced Applications. XXIV, 925 pages. 2004.

Vol. 2971: J.I. Lim, D.H. Lee (Eds.), Information Security and Cryptology - ICISC 2003. XI, 458 pages. 2004.

Vol. 2970: F. Fernández Rivera, M. Bubak, A. Gómez Tato, R. Doallo (Eds.), Grid Computing. XI, 328 pages. 2004.

Vol. 2964: T. Okamoto (Ed.), Topics in Cryptology – CT-RSA 2004. XI, 387 pages. 2004.

Vol. 2963: R. Sharp, Higher Level Hardware Synthesis. XVI, 195 pages. 2004.

Vol. 2962: S. Bistarelli, Semirings for Soft Constraint Solving and Programming. XII, 279 pages. 2004.

Vol. 2961: P. Eklund (Ed.), Concept Lattices. IX, 411 pages. 2004. (Subseries LNAI).

Vol. 2960: P.D. Mosses (Ed.), CASL Reference Manual. XVII, 528 pages. 2004.

Vol. 2958: L. Rauchwerger (Ed.), Languages and Compilers for Parallel Computing. XI, 556 pages. 2004.

Vol. 2957: P. Langendoerfer, M. Liu, I. Matta, V. Tsaoussidis (Eds.), Wired/Wireless Internet Communications. XI, 307 pages. 2004.

Vol. 2954: F. Crestani, M. Dunlop, S. Mizzaro (Eds.), Mobile and Ubiquitous Information Access. X, 299 pages. 2004.

Vol. 2953: K. Konrad, Model Generation for Natural Language Interpretation and Analysis. XIII, 166 pages. 2004. (Subseries LNAI).

Vol. 2952: N. Guelfi, E. Astesiano, G. Reggio (Eds.), Scientific Engineering of Distributed Java Applications. X, 157 pages. 2004.

Vol. 2951: M. Naor (Ed.), Theory of Cryptography. XI, 523 pages. 2004.

Vol. 2949: R. De Nicola, G. Ferrari, G. Meredith (Eds.), Coordination Models and Languages. X, 323 pages. 2004.

Vol. 2948: G.L. Mullen, A. Poli, H. Stichtenoth (Eds.), Finite Fields and Applications. VIII, 263 pages. 2004.

Vol. 2947: F. Bao, R. Deng, J. Zhou (Eds.), Public Key Cryptography – PKC 2004. XI, 455 pages. 2004.

Vol. 2946: R. Focardi, R. Gorrieri (Eds.), Foundations of Security Analysis and Design II. VII, 267 pages. 2004.

Vol. 2943: J. Chen, J. Reif (Eds.), DNA Computing. X, 225 pages. 2004.

Vol. 2941: M. Wirsing, A. Knapp, S. Balsamo (Eds.), Radical Innovations of Software and Systems Engineering in the Future. X, 359 pages. 2004.

Vol. 2940: C. Lucena, A. Garcia, A. Romanovsky, J. Castro, P.S. Alencar (Eds.), Software Engineering for Multi-Agent Systems II. XII, 279 pages. 2004.

Vol. 2939: T. Kalker, I.J. Cox, Y.M. Ro (Eds.), Digital Watermarking. XII, 602 pages. 2004.

Vol. 2937: B. Steffen, G. Levi (Eds.), Verification, Model Checking, and Abstract Interpretation. XI, 325 pages. 2004.

Vol. 2934: G. Lindemann, D. Moldt, M. Paolucci (Eds.), Regulated Agent-Based Social Systems. X, 301 pages. 2004. (Subseries LNAI).

Vol. 2930: F. Winkler (Ed.), Automated Deduction in Geometry. VII, 231 pages. 2004. (Subseries LNAI).

Vol. 2926: L. van Elst, V. Dignum, A. Abecker (Eds.), Agent-Mediated Knowledge Management. XI, 428 pages. 2004. (Subseries LNAI).

Vol. 2923: V. Lifschitz, I. Niemelä (Eds.), Logic Programming and Nonmonotonic Reasoning. IX, 365 pages. 2004. (Subseries LNAI).

Vol. 2919: E. Giunchiglia, A. Tacchella (Eds.), Theory and Applications of Satisfiability Testing. XI, 530 pages. 2004.

Vol. 2917: E. Quintarelli, Model-Checking Based Data Retrieval. XVI, 134 pages. 2004.

Vol. 2916: C. Palamidessi (Ed.), Logic Programming. XII, 520 pages. 2003.

Vol. 2915: A. Camurri, G. Volpe (Eds.), Gesture-Based Communication in Human-Computer Interaction. XIII, 558 pages. 2004. (Subseries LNAI).

Vol. 2914: P.K. Pandya, J. Radhakrishnan (Eds.), FST TCS 2003: Foundations of Software Technology and Theoretical Computer Science. XIII, 446 pages. 2003.

Vol. 2913: T.M. Pinkston, V.K. Prasanna (Eds.), High Performance Computing - HiPC 2003. XX, 512 pages. 2003. (Subseries LNAI).

Vol. 2911: T.M.T. Sembok, H.B. Zaman, H. Chen, S.R. Urs, S.H. Myaeng (Eds.), Digital Libraries: Technology and Management of Indigenous Knowledge for Global Access. XX, 703 pages. 2003.

Vol. 2910: M.E. Orlowska, S. Weerawarana, M.M.P. Papazoglou, J. Yang (Eds.), Service-Oriented Computing - ICSOC 2003. XIV, 576 pages. 2003.

Vol. 2909: R. Solis-Oba, K. Jansen (Eds.), Approximation and Online Algorithms. VIII, 269 pages. 2004.

Vol. 2908: K. Chae, M. Yung (Eds.), Information Security Applications. XII, 506 pages. 2004.

Vol. 2907: I. Lirkov, S. Margenov, J. Wasniewski, P. Yalamov (Eds.), Large-Scale Scientific Computing. XI, 490 pages. 2004.

Vol. 2906: T. Ibaraki, N. Katoh, H. Ono (Eds.), Algorithms and Computation. XVII, 748 pages. 2003.

Vol. 2905: A. Sanfeliu, J. Ruiz-Shulcloper (Eds.), Progress in Pattern Recognition, Speech and Image Analysis. XVII, 693 pages. 2003.

Vol. 2904: T. Johansson, S. Maitra (Eds.), Progress in Cryptology - INDOCRYPT 2003. XI, 431 pages. 2003.

Vol. 2903: T.D. Gedeon, L.C.C. Fung (Eds.), AI 2003: Advances in Artificial Intelligence. XVI, 1075 pages. 2003. (Subseries LNAI).

Vol. 2902: F.M. Pires, S.P. Abreu (Eds.), Progress in Artificial Intelligence. XV, 504 pages. 2003. (Subseries LNAI).

Vol. 2901: F. Bry, N. Henze, J. Ma luszyński (Eds.), Principles and Practice of Semantic Web Reasoning. X, 209 pages. 2003.

Vol. 2900: M. Bidoit, P.D. Mosses (Eds.), Casl User Manual. XIII, 240 pages. 2004.

Vol. 2899: G. Ventre, R. Canonico (Eds.), Interactive Multimedia on Next Generation Networks. XIV, 420 pages. 2003.

Vol. 2898: K.G. Paterson (Ed.), Cryptography and Coding. IX, 385 pages. 2003.

Vol. 2897: O. Balet, G. Subsol, P. Torguet (Eds.), Virtual Storytelling. XI, 240 pages. 2003.

Vol. 2896: V.A. Saraswat (Ed.), Advances in Computing Science – ASIAN 2003. VIII, 305 pages. 2003.

Vol. 2895: A. Ohori (Ed.), Programming Languages and Systems. XIII, 427 pages. 2003.

Vol. 2894: C.S. Laih (Ed.), Advances in Cryptology - ASIACRYPT 2003. XIII, 543 pages. 2003.

Vol. 2893: J.-B. Stefani, I. Demeure, D. Hagimont (Eds.), Distributed Applications and Interoperable Systems. XIII, 311 pages. 2003.

Vol. 2892: F. Dau, The Logic System of Concept Graphs with Negation. XI, 213 pages. 2003. (Subseries LNAI).

Vol. 2891: J. Lee, M. Barley (Eds.), Intelligent Agents and Multi-Agent Systems. X, 215 pages. 2003. (Subseries LNAI).

Vol. 2890: M. Broy, A.V. Zamulin (Eds.), Perspectives of System Informatics. XV, 572 pages. 2003.

Vol. 2889: R. Meersman, Z. Tari (Eds.), On The Move to Meaningful Internet Systems 2003: OTM 2003 Workshops. XIX, 1071 pages. 2003.

Vol. 2888: R. Meersman, Z. Tari, D.C. Schmidt (Eds.), On The Move to Meaningful Internet Systems 2003: CoopIS, DOA, and ODBASE. XXI, 1546 pages. 2003.

Vol. 2887: T. Johansson (Ed.), Fast Software Encryption. IX, 397 pages. 2003.

Vol. 2886: I. Nyström, G. Sanniti di Baja, S. Svensson (Eds.), Discrete Geometry for Computer Imagery. XII, 556 pages. 2003.

Vol. 2885: J.S. Dong, J. Woodcock (Eds.), Formal Methods and Software Engineering. XI, 683 pages. 2003.

Vol. 2884: E. Najm, U. Nestmann, P. Stevens (Eds.), Formal Methods for Open Object-Based Distributed Systems. X, 293 pages. 2003.

Vol. 2883: J. Schaeffer, M. Müller, Y. Björnsson (Eds.), Computers and Games. XI, 431 pages. 2003.

Table of Contents

Computer Security/Mobile Security

Voting/Auction Protocols

Watermarking

Digital Signatures II

Authentication/Threshold Protocols

Block/Stream Ciphers

Binary Tree Encryption: Constructions and Applications

Jonathan Katz*

Department of Computer Science
University of Maryland
College Park, MD, USA
jkatz@cs.umd.edu

Abstract. *Binary tree encryption* (BTE), a relaxation of hierarchical identity-based encryption (HIBE), has recently emerged as a useful and intriguing primitive. On the one hand, the definition of security for BTE is sufficiently "weak" that — in contrast to HIBE — constructions of BTE *in the standard model* are known. On the other hand, BTE is sufficiently powerful that it yields a number of applications which are important from both a theoretical and a practical point of view.

This survey presents the basic definitions of BTE and also highlights some recent applications of BTE to forward-secure encryption, identity-based and hierarchical identity-based encryption, chosen-ciphertext security, and adaptively-secure encryption.

1 Introduction

The notion of identity-based cryptography has long fascinated researchers [23]. Loosely speaking, in such a scheme *any* identity (i.e., bit-string) can serve as a public key. In somewhat more detail, there is a (trusted) private-key generator PKG who generates master system parameters params along with a master secret key sk. For any identity $id \in \{0,1\}^*$ the PKG can use sk to compute a secret key SK_{id} corresponding to this identity. The pair (id, SK_{id}) then functions as a standard public-/private-key pair (with the important distinction that id can be any string!) whose functionality is determined by the underlying identity-based scheme. (The PKG would presumably authenticate the identity of the person claiming "id" before giving them the corresponding secret key SK_{id}. However, this is outside the scope of the present discussion.) An identity-based system is secure (informally) if knowledge of the secret keys corresponding to any arbitrary-size set of identities $\mathcal{I} = \{id_1, \ldots, id_n\}$ does not allow an adversary to "break" the scheme (in the appropriate sense) for any $id' \notin \mathcal{I}$.

Shamir [23] was the first to suggest an implementation of an identity-based signature scheme. Following this, many provably-secure proposals for identity-based signature and identification schemes followed (e.g., [13, 16]); some of these

* Portions of this work were supported by NSF grant #ANI-0310751.

J.I. Lim and D.H. Lee (Eds.): ICISC 2003, LNCS 2971, pp. 1–11, 2004.

constructions were recently generalized and expanded upon in [11]. Although these constructions are proven secure in the random oracle model, note that it is also possible to construct identity-based signatures in the standard model based on any "regular" signature scheme (see [11]).

Recently, Boneh and Franklin [5] and Cocks [10] resolved a long-standing open problem by constructing the first identity-based public-key *encryption* schemes. Both of these constructions are proven secure in the random oracle model. Since encryption schemes are the focus of this article (and are more interesting in the sense that they are more difficult to construct), we consider only encryption from now on.

It is natural to extend the notion of identity-based encryption (IBE) to include *hierarchical* identity-based encryption (HIBE). In an HIBE scheme, the PKG (as above) issues secret keys to "first-level" identities $id \in \{0,1\}^*$; furthermore, anyone knowing the secret key SK_{id_1} corresponding to a "first-level" identity id_1 can issue a secret key $SK_{id_1||id_2}$ corresponding to any "second-level" identity $id_1||id_2$ (for arbitrary $id_2 \in \{0,1\}^*$). More generally, let $ID = (id_1||\cdots||id_t)$ and let SK_{ID} be the secret key corresponding to this identity. Then for any string $id_{t+1} \in \{0,1\}^*$ and identity $ID' \stackrel{\text{def}}{=} (ID||id_{t+1})$, knowledge of SK_{ID} enables computation of a key $SK_{ID'}$. As before, in all these cases the pair (ID, SK_{ID}) functions as a "standard" public-/private-key pair. The security requirement is modified in the obvious way: now, one requires that knowledge of the secret keys corresponding to any arbitrary-size set of identities $\mathcal{I} = \{ID_1, \ldots, ID_n\}$ should not enable an adversary to "break" the scheme (in some appropriate sense) for any ID' having no ancestors in $\mathcal{I}$, where the *ancestors* of an identity $ID = (id_1||\cdots||id_n)$ are all identities of the form $(id_1||\cdots||id_i)$ for $i \leq n$.

Horwitz and Lynn [17] were the first to suggest the notion of HIBE, and they also propose a partial solution handling identities of depth two. Gentry and Silverberg [14] were the first to give a complete solution to this problem, and they construct and prove secure a scheme supporting identities of arbitrary (constant) depth. Both of these constructions build on the IBE scheme of Boneh and Franklin [5], and both are proven secure in the random oracle model.

1.1 Binary Tree Encryption

It can be immediately noticed that the identities in a hierarchical identity-based scheme correspond in the natural way to nodes in a tree. Specifically, one may associate the PKG with the root of the tree, the "first-level" identities with the nodes of depth one (i.e., the children of the root), and the identity $ID' = (id_1||\cdots||id_{t+1})$ with a node at depth $t+1$ which is the child of a node at depth t which is in turn associated with $ID = (id_1||\cdots||id_t)$.

In a scheme as outlined above, the identity hierarchy yields a tree of *unbounded* degree. In contrast, a *binary* tree encryption (BTE) scheme [7] — as the name suggests — considers only an identity hierarchy in the form of a *binary* tree (i.e., a tree in which each node has degree two). Viewing BTE as a conceptual relaxation of HIBE, one obtains a scheme in which the PKG may