LNCS 4752

Atsuko Miyaji
Hiroaki Kikuchi
Kai Rannenberg (Eds.)

Advances in Information and Computer Security

Second International Workshop on Security, IWSEC 2007
Nara, Japan, October 2007
Proceedings

Springer

Atsuko Miyaji Hiroaki Kikuchi
Kai Rannenberg (Eds.)

Advances in Information and Computer Security

Second International Workshop on Security, IWSEC 2007
Nara, Japan, October 29-31, 2007
Proceedings

Springer

Volume Editors

Atsuko Miyaji
Japan Advanced Institute of Science and Technology
School of Information Science
Ishikawa, Japan
E-mail: miyaji@jaist.ac.jp

Hiroaki Kikuchi
Tokai University
School of Information Technology and Electronics
Kanagawa, Japan
E-mail: kikn@tokai.ac.jp

Kai Rannenberg
Goethe University Frankfurt
Institute of Business Informatics
Frankfurt/Main, Germany
E-mail: kai.rannenberg@m-lehrstuhl.de

Library of Congress Control Number: Applied for

CR Subject Classification (1998): E.3, G.2.1, D.4.6, K.6.5, K.4.1, C.2, J.1

LNCS Sublibrary: SL 4 – Security and Cryptology

ISSN 0302-9743
ISBN-10 3-540-75650-7 Springer Berlin Heidelberg New York
ISBN-13 978-3-540-75650-7 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: 12041589 06/3180 5 4 3 2 1 0

Lecture Notes in Computer Science 4752

Preface

The International Workshop on Security (IWSEC 2007) was the second in the annual series that started in 2006. IWSEC 2007 was held at the New Public Hall in Nara, Japan, during October 29–31, 2007.

This year there were 112 paper submissions, and from these 30 papers were accepted. Accepted papers came from 27 different countries, with the largest proportion coming from Japan (12). Estonia, China, Korea, Spain, Taiwan and the USA contributed 2 papers each and Canada, Germany, Greece, Poland, Turkey and Vietnam contributed 1 paper each. We would like to thank all of the authors who submitted papers to IWSEC 2007.

The contributed papers were supplemented by one invited talk from the eminent researcher Prof. Doug Tygar (UC Berkeley) in information security.

We were fortunate to have an energetic team of experts who formed the Program Committee. Their names may be found overleaf, and we are sincerely grateful for all their great efforts. This team was supported by an even larger number of individuals who reviewed papers in their particular areas of expertise. A list of these names is also provided; we hope it is complete.

We are delighted to acknowledge the generous financial sponsorship of IWSEC 2007 by Carnegie Mellon CyLab Japan, the International Communication Foundation (ICF), and the National Institute of Information and Communications Technology (NICT). The workshop was co-sponsored jointly by ISEC, a technical group on information security of IEICE (The Institute of Electronics, Information and Communication Engineers) and CSEC, a special interest group on computer security of IPSJ (Information Processing Society of Japan). The excellent Local Organizing Committee was led by the IWSEC 2007 General Chairs, Prof. Masakatu Morii and Dr. Masato Terada.

October 2007

Atsuko Miyaji
Hiroaki Kikuchi
Kai Rannenberg

IWSEC 2007
Second International Workshop on Security

Co-sponsored by

ISEC (Technical Group on Information Security, Engineering Sciences Society, of the Institute of Electronics, Information and Communication Engineers, Japan)
CSEC (Special Interest Group on Computer Security of Information Processing Society of Japan)

Financially Sponsored by

Carnegie Mellon CyLab Japan
International Communication Foundation (ICF)
National Institute of Information and Communications Technology (NICT)

General Co-chairs

Masakatu Morii (Kobe University, Japan)
Masato Terada (Hitachi Ltd., Japan)

Program Committee Co-chairs

Atsuko Miyaji (Japan Advanced Institute of Science and Technology, Japan)
Hiroaki Kikuchi (Tokai University, Japan)
Kai Rannenberg (Goethe University Frankfurt, Germany)

Advisory Committee

Norihisa Doi (Chuo University, Japan)
Akira Hayashi (Kanazawa Institute of Technology, Japan)
Hideki Imai (Chuo University, Japan)
Guenter Mueller (University of Freiburg, Germany)
Yuko Murayama (Iwate Prefectural University, Japan)
Eiji Okamoto (University of Tsukuba, Japan)
Ryoichi Sasaki (Tokyo Denki University, Japan)
Shigeo Tsujii (Institute of Information Security, Japan)

Local Organizing Committee

Finance Chairs	Yoshiaki Shiraishi (Nagoya Institute of Technology, Japan)
	Masayuki Terada (NTT DoCoMo, Inc., Japan)
	Keisuke Takemori (KDDI R&D Laboratories Inc., Japan)
Publicity Chairs	Naoto Sone (Naruto University of Education, Japan)
	Tsuyoshi Takagi (Future University Hakodate, Japan)
	Koji Chida (NTT Co., Japan)
Local Arrangement Chairs	Hidenori Kuwakado (Kobe University, Japan)
	Masakatsu Nishigaki (Shizuoka University, Japan)
	Yuji Suga (Canon Inc., Japan)
Publication Chairs	Toshihiro Tabata (Okayama University, Japan)
	Masahiro Mambo (University of Tsukuba, Japan)
	Isao Echizen (National Institute of Informatics, Japan)
Registration Chairs	Mitsuru Matsui (Mitsubishi Electric Co., Japan)
	Masayuki Terada (NTT DoCoMo, Inc., Japan)
	Keisuke Takemori (KDDI R&D Laboratories Inc., Japan)
Award Chairs	Hiroshi Doi (Institute of Information Security, Japan)
	Hiroshi Yoshiura (University of Electro-Communications, Japan)
	Tetsuya Izu (Fujitsu Laboratories Ltd., Japan)
Liaison Chairs	Katsunari Yoshioka (National Institute of Information and Communications Technology, Japan)
	Takehisa Kato (Toshiba Solutions Corporation, Japan)
	Ryuya Uda (Tokyo University of Technology, Japan)

Program Committee

Koichiro Akiyama (Toshiba Corporation, Japan)
Tomoyuki Asano (Sony Corporation, Japan)
Feng Bao (Institute for Infocomm Research, Singapore)
Kevin Butler (Pennsylvania State University, USA)
George Robert Blakley, Jr. (Texas A&M University, USA)
Liqun Chen (HP Laboratories, UK)
Soon Ae Chun (City University of New York, USA)

George Danezis (Katholieke Universiteit Leuven, Belgium)
Ed Dawson (Queensland University of Technology, Australia)
Bart De Decker (Katholieke Universiteit Leuven, Belgium)
Hiroshi Doi (Institute of Information Security, Japan)
Ee-Chien Chang (National University of Singapore, Singapore)
Steven Furnell (University of Plymouth, UK)
Soichi Furuya (Hitachi, Ltd., Japan)
Dimitris Gritzalis (Athens University of Economics & Business, Greece)
Shoichi Hirose (University of Fukui, Japan)
Keiichi Iwamura (Tokyo University of Science, Japan)
Tetsu Iwata (Nagoya University, Japan)
Marc Joye (Thomson R&D, France)
Angelos D. Keromytis (Columbia University, USA)
Kwangjo Kim (Information and Communications University, Korea)
Michiharu Kudo (IBM Japan, Japan)
Noboru Kunihiro (The University of Electro-Communications, Japan)
Xuejia Lai (Shanghai Jiao Tong University, China)
Kwok-Yan Lam (Tsinghua University, China)
Byoungcheon Lee (Joongbu University, Korea)
Dong Hoon Lee (Korea University, Korea)
Pil Joong Lee (Pohang University of Science and Technology, Korea)
William List (Firm Wm. List & Co, UK)
Javier Lopez (University of Malaga, Spain)
Masahiro Mambo (University of Tsukuba, Japan)
Mark Manulis (Ruhr-University of Bochum, Germany)
Wenbo Mao (HP Labs, China)
Keith Martin (Royal Holloway, University of London, UK)
Mitsuru Matsui (Mitsubishi Electric, Japan)
Kanta Matsuura (University of Tokyo, Japan)
Toru Nakanishi (Okayama University, Japan)
Masakatsu Nishigaki (Shizuoka University, Japan)
Takeshi Okamoto (University of Tsukuba, Japan)
Kazumasa Omote (Fujitsu Laboratories, Ltd., Japan)
Kenneth G. Paterson (Royal Holloway, University of London, UK)
Adrian Perrig (Carnegie Mellon University, USA)
Raphael Phan (EPFL, Switzerland)
Rei Safavi-Naini (University of Wollongong, Australia)
Kouichi Sakurai (Kyushu University, Japan)
Masakazu Soshi (Japan Advanced Institute of Science and Technology, Japan)
Willy Susilo (University of Wollongong, Australia)
Mitsuru Tada (Chiba University, Japan)
Tsuyoshi Takagi (Future University Hakodate, Japan)
Toshiaki Tanaka (KDDI R&D Laboratories Inc., Japan)
Ryuya Uda (Tokyo University of Technology, Japan)
Serge Vaudenay (EPFL, Switzerland)

Jozef Vyskoc (VaF, Slovak Republic)
Hajime Watanabe (National Institute of Advanced Science and Technology, Japan)
Duncan Wong (City University of Hong Kong, China)
Sung-Ming Yen (National Central University, Taiwan)
Hiroshi Yoshiura (University of Electro-Communications, Japan)
Yuliang Zheng (University of North Carolina, USA)
Jianying Zhou (Institute for Infocomm Research, Singapore)
Alf Zugenmaier (DoCoMo Euro-Labs, Germany)

External Reviewers

Toru Akishita, Elli Androulaki, Michael Arnold, Man Ho Au, Jean-Philippe Aumasson, Thomas Baignères, Tor E. Bjorstad, Jeffrey Bloom, Emmanuel Bresson, Matt Burnside, Haibo Chen, Kuo-Zhe Chiou, Kim-Kwang Raymond Choo, Siu-Leung Chung, Carlos Cid, Lizzie Coles-Kemp, Debra L. Cook, Jason Crampton, Gabriela Cretu, Jintai Ding, Ling Dong, Stelios Dritsas, Dang Nguyen Duc, William Enck, Koichi Fujisaki, Kazuhide Fukushima, Soichi Furuya, Steven Galbraith, Meng Ge, Willi Geiselmann, Chris Grier, Tim Güneysu, Satoshi Hada, Yu Haifeng, Goichiro Hanaoka, Yoshikazu Hanatani, Yoshiki Higashikado, Jin Ho Kim, Katrin Hoeper, Dennis Hofheinz, Yoshiaki Hori, Chao-Chih Hsu, Qiong Huang, Taichi Isogai, Yukio Izumi, Ik Rae Jeong, Shaoquan Jiang, Mohamed Karroumi, Yasuharu Katsuno, Young Mok Kim, Samuel T. King, Wataru Kitada, Divyan M. Konidala, Masafumi Kusakawa, Eun Jeong Kwon, Frédéric Lefèbfre, Arjen K. Lenstra, Wanqing Li, Vo Duc Liem, Wei-Chih Lien, Hoon Wei Lim, Hsi-Chung Lin, Yu Long, Antoine Monsifrot, Shiho Moriai, Cedric Ng, Steven Noel, Satoshi Obana, Yutaka Oiwa, Hiroyuki Okazaki, Haruki Ota, Toru Owada, Je Hong Park, Sylvain Pasini, Francesco De Pellegrini, Ludovic Perret, Rodrigo Roman, Eun-Kyung Ryu, Jae Woo Seo, Joshua Schiffman, Jörg Schwenk, Mike Scott, Abhi Shelat, Nicholas Sheppard, Jong Hoon Shin, Masaaki Shirase, Stelios Sidiroglou, Leonie Simpson, Yingbo Song, Rainer Steinwandt, Chunhua Su, Hongwei Sun, Daisuke Suzuki, Koutarou Suzuki, Amril Syalim, Gelareh Taban, Kenichi Takahashi, Takeaki Terada, Marianthi Theoharidou, Xiaojian Tian, Patrick Traynor, Eran Tromer, Bill Tsoumas, Jheng-Hong Tu, Yoshifumi Ueshige, Kentaro Umesawa, Kristof Verslype, Jose L. Vivas, Yuji Watanabe, Nicholas Weaver, Yongdong Wu, Shinji Yamanaka, Guomin Yang, Yeon-Hyeong Yang, Tomoko Yonemura, Maki Yoshida, Rui Zhang, Huafei Zhu

Lecture Notes in Computer Science

Sublibrary 4: Security and Cryptology

Vol. 4779: J.A. Garay, A.K. Lenstra, M. Mambo, R. Peralta (Eds.), Information Security . XIII, 437 pages. 2007.

Vol. 4752: A. Miyaji, H. Kikuchi, K. Rannenberg (Eds.), Advances in Information and Computer Security. XIII, 460 pages. 2007.

Vol. 4734: J. Biskup, J. López (Eds.), Computer Security - ESORICS 2007. XIV, 628 pages. 2007.

Vol. 4727: P. Paillier, I. Verbauwhede (Eds.), Cryptographic Hardware and Embedded Systems - CHES 2007. XIV, 468 pages. 2007.

Vol. 4691: T. Dimitrakos, F. Martinelli, P.Y.A. Ryan, S. Schneider (Eds.), Formal Aspects in Security and Trust. VIII, 285 pages. 2007.

Vol. 4677: A. Aldini, R. Gorrieri (Eds.), Foundations of Security Analysis and Design IV. VII, 325 pages. 2007.

Vol. 4657: C. Lambrinoudakis, G. Pernul, A M. Tjoa (Eds.), Trust and Privacy in Digital Business. XIII, 291 pages. 2007.

Vol. 4637: C. Kruegel, R. Lippmann, A. Clark (Eds.), Recent Advances in Intrusion Detection. XII, 337 pages. 2007.

Vol. 4622: A. Menezes (Ed.), Advances in Cryptology - CRYPTO 2007. XIV, 631 pages. 2007.

Vol. 4593: A. Biryukov (Ed.), Fast Software Encryption. XI, 467 pages. 2007.

Vol. 4586: J. Pieprzyk, H. Ghodosi, E. Dawson (Eds.), Information Security and Privacy. XIV, 476 pages. 2007.

Vol. 4582: J. López, P. Samarati, J.L. Ferrer (Eds.), Public Key Infrastructure. XI, 375 pages. 2007.

Vol. 4579: B. M. Hämmerli, R. Sommer (Eds.), Detection of Intrusions and Malware, and Vulnerability Assessment. X, 251 pages. 2007.

Vol. 4575: T. Takagi, T. Okamoto, E. Okamoto, T. Okamoto (Eds.), Pairing-Based Cryptography – Pairing 2007. XI, 408 pages. 2007.

Vol. 4521: J. Katz, M. Yung (Eds.), Applied Cryptography and Network Security. XIII, 498 pages. 2007.

Vol. 4515: M. Naor (Ed.), Advances in Cryptology - EUROCRYPT 2007. XIII, 591 pages. 2007.

Vol. 4499: Y.Q. Shi (Ed.), Transactions on Data Hiding and Multimedia Security II. IX, 117 pages. 2007.

Vol. 4464: E. Dawson, D.S. Wong (Eds.), Information Security Practice and Experience. XIII, 361 pages. 2007.

Vol. 4462: D. Sauveron, K. Markantonakis, A. Bilas, J.-J. Quisquater (Eds.), Information Security Theory and Practices. XII, 255 pages. 2007.

Vol. 4450: T. Okamoto, X. Wang (Eds.), Public Key Cryptography – PKC 2007. XIII, 491 pages. 2007.

Vol. 4437: J.L. Camenisch, C.S. Collberg, N.F. Johnson, P. Sallee (Eds.), Information Hiding. VIII, 389 pages. 2007.

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

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

Vol. 4356: E. Biham, A.M. Youssef (Eds.), Selected Areas in Cryptography. XI, 395 pages. 2007.

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

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

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

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

Vol. 4307: P. Ning, S. Qing, N. Li (Eds.), Information and Communications Security. XIV, 558 pages. 2006.

Vol. 4301: D. Pointcheval, Y. Mu, K. Chen (Eds.), Cryptology and Network Security. XIII, 381 pages. 2006.

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

Vol. 4298: J.K. Lee, O. Yi, M. Yung (Eds.), Information Security Applications. XIV, 406 pages. 2007.

Vol. 4296: M.S. Rhee, B. Lee (Eds.), Information Security and Cryptology – ICISC 2006. XIII, 358 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. 4266: H. Yoshiura, K. Sakurai, K. Rannenberg, Y. Murayama, S.-i. Kawamura (Eds.), Advances in Information and Computer Security. XIII, 438 pages. 2006.

Vol. 4258: G. Danezis, P. Golle (Eds.), Privacy Enhancing Technologies. VIII, 431 pages. 2006.

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

Vol. 4237: H. Leitold, E.P. 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. 4219: D. Zamboni, C. Krügel (Eds.), Recent Advances in Intrusion Detection. XII, 331 pages. 2006.

Vol. 4189: D. Gollmann, J. Meier, A. Sabelfeld (Eds.), Computer Security – ESORICS 2006. XI, 548 pages. 2006.

Vol. 4176: S.K. Katsikas, J. López, M. Backes, S. Gritzalis, B. Preneel (Eds.), Information Security. XIV, 548 pages. 2006.

Vol. 4117: C. Dwork (Ed.), Advances in Cryptology - CRYPTO 2006. XIII, 621 pages. 2006.

Vol. 4116: R. De Prisco, M. Yung (Eds.), Security and Cryptography for Networks. XI, 366 pages. 2006.

Vol. 4107: G. Di Crescenzo, A. Rubin (Eds.), Financial Cryptography and Data Security. XI, 327 pages. 2006.

Vol. 4083: S. Fischer-Hübner, S. Furnell, C. Lambrinoudakis (Eds.), Trust and Privacy in Digital Business. XIII, 243 pages. 2006.

Vol. 4064: R. Büschkes, P. Laskov (Eds.), Detection of Intrusions and Malware & Vulnerability Assessment. X, 195 pages. 2006.

Vol. 4058: L.M. Batten, R. Safavi-Naini (Eds.), Information Security and Privacy. XII, 446 pages. 2006.

Vol. 4047: M.J.B. Robshaw (Ed.), Fast Software Encryption. XI, 434 pages. 2006.

Vol. 4043: A.S. Atzeni, A. Lioy (Eds.), Public Key Infrastructure. XI, 261 pages. 2006.

Vol. 4004: S. Vaudenay (Ed.), Advances in Cryptology - EUROCRYPT 2006. XIV, 613 pages. 2006.

Vol. 3995: G. Müller (Ed.), Emerging Trends in Information and Communication Security. XX, 524 pages. 2006.

Vol. 3989: J. Zhou, M. Yung, F. Bao (Eds.), Applied Cryptography and Network Security. XIV, 488 pages. 2006.

Vol. 3969: Ø. Ytrehus (Ed.), Coding and Cryptography. XI, 443 pages. 2006.

Vol. 3958: M. Yung, Y. Dodis, A. Kiayias, T.G. Malkin (Eds.), Public Key Cryptography - PKC 2006. XIV, 543 pages. 2006.

Vol. 3957: B. Christianson, B. Crispo, J.A. Malcolm, M. Roe (Eds.), Security Protocols. IX, 325 pages. 2006.

Vol. 3956: G. Barthe, B. Grégoire, M. Huisman, J.-L. Lanet (Eds.), Construction and Analysis of Safe, Secure, and Interoperable Smart Devices. IX, 175 pages. 2006.

Vol. 3935: D.H. Won, S. Kim (Eds.), Information Security and Cryptology - ICISC 2005. XIV, 458 pages. 2006.

Vol. 3934: J.A. Clark, R.F. Paige, F.A.C. Polack, P.J. Brooke (Eds.), Security in Pervasive Computing. X, 243 pages. 2006.

Vol. 3928: J. Domingo-Ferrer, J. Posegga, D. Schreckling (Eds.), Smart Card Research and Advanced Applications. XI, 359 pages. 2006.

Vol. 3919: R. Safavi-Naini, M. Yung (Eds.), Digital Rights Management. XI, 357 pages. 2006.

Vol. 3903: K. Chen, R. Deng, X. Lai, J. Zhou (Eds.), Information Security Practice and Experience. XIV, 392 pages. 2006.

Vol. 3897: B. Preneel, S. Tavares (Eds.), Selected Areas in Cryptography. XI, 371 pages. 2006.

Vol. 3876: S. Halevi, T. Rabin (Eds.), Theory of Cryptography. XI, 617 pages. 2006.

Vol. 3866: T. Dimitrakos, F. Martinelli, P.Y.A. Ryan, S. Schneider (Eds.), Formal Aspects in Security and Trust. X, 259 pages. 2006.

Vol. 3860: D. Pointcheval (Ed.), Topics in Cryptology – CT-RSA 2006. XI, 365 pages. 2006.

Vol. 3858: A. Valdes, D. Zamboni (Eds.), Recent Advances in Intrusion Detection. X, 351 pages. 2006.

Vol. 3856: G. Danezis, D. Martin (Eds.), Privacy Enhancing Technologies. VIII, 273 pages. 2006.

Vol. 3786: J.-S. Song, T. Kwon, M. Yung (Eds.), Information Security Applications. XI, 378 pages. 2006.

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

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

Vol. 2742: R.N. Wright (Ed.), Financial Cryptography. VIII, 321 pages. 2003.

Table of Contents

Software and Multimedia Security

Public-Key Cryptography (1)

Network Security

E-commerce and Voting

Operating Systems

Public-Key Cryptography (2)

Security and Information Management

Anonymity and Privacy

Digital Signatures, Hash Function and Protocol

A Note on the (Im)possibility of Using Obfuscators to Transform Private-Key Encryption into Public-Key Encryption

Satoshi Hada[1] and Kouichi Sakurai[2]

[1] Tokyo Research Laboratory, IBM Research, 1623-14, Shimotsuruma, Yamato, Kanagawa 242-8502, Japan
satoshih@jp.ibm.com
[2] Dept. of Computer Science and Communication Engineering, Kyushu University, 744 Motooka, Nishi-ku, Fukuoka, Fukuoka 819-0395, Japan
sakurai@csce.kyushu-u.ac.jp

Abstract. Transforming private-key encryption schemes into public-key encryption schemes is an interesting application of program obfuscation. The idea is that, given a private-key encryption scheme, an obfuscation of an encryption program with a private key embedded is used as a public key and the private key is used for decryption as it is. The security of the resulting public-key encryption scheme would be ensured because obfuscation is *unintelligible* and the public key is expected to leak no information on the private key. This paper investigates the possibility of general-purpose obfuscators for such a transformation, i.e., obfuscators that can transform an arbitrary private-key encryption scheme into a secure public-key encryption scheme. Barak et al. have shown a negative result, which says that there is a *deterministic* private-key encryption scheme that is *unobfuscatable* in the sense that, given any encryption program with a private key embedded, one can efficiently compute the private key. However, it is an open problem whether their result extends to *probabilistic* encryption schemes, where we should consider a relaxed notion of obfuscators, i.e., *sampling obfuscators*. Programs obfuscated by sampling obfuscators do not necessarily compute the same function as the original program, but produce the same distribution as the original program. In this paper, we show that there is a *probabilistic* private-key encryption scheme that can not be transformed into a secure public-key encryption scheme by sampling obfuscators which have a special property regarding input-output dependency of encryption programs. Our intention is not to claim that the required special property is reasonable. Rather, we claim that general-purpose obfuscators for the transformation, if they exist, must be a sampling obfuscator which does NOT have the special property.

1 Introduction

1.1 Obfuscation

An obfuscator is a tool to convert a program into a new program which is *unintelligible* while preserving the functionality. Several formal definitions have

A. Miyaji, H. Kikuchi, and K. Rannenberg (Eds.): IWSEC 2007, LNCS 4752, pp. 1–12, 2007.

been proposed so far [13,1,17,18,10,14]. Informally, obfuscators should satisfy the following two requirements: (1) functionality: the new program has the same functionality as the original one and (2) virtual black-box property: whatever one can efficiently compute given the new program can be computed given oracle access to the functionality. The functionality requirement is a syntactic requirement while the virtual black-box property represents the security requirement that the obfuscated program should be unintelligible.

As discussed in [1], obfuscators, if they exist, would have a wide variety of cryptographic applications including software protection, homomorphic encryption, removing random oracles, and transforming private-key encryption schemes into public-key encryption schemes. Unfortunately, the impossibility of generic obfuscation have been shown in [1,10] (even under very weak definitions based on the virtual black-box property). For example, as shown in [1], there exists a family of functions $\mathcal{F}$ that are *unobfuscatable* in the sense that there is a boolean property of functions such that, given any program that computes a function $f \in \mathcal{F}$, the property of f can be efficiently computed, yet given oracle access to a randomly selected function $f \in \mathcal{F}$, no efficient algorithm can compute the property of f much better than random guessing. However, such negative results do not rule out the possibility that there exists an obfuscator for a *specific* set of programs (a specific application). Indeed, some positive results are known for point functions [2,3,17,18,10,6,14] and re-encryption [15].

When we consider obfuscation of *probabilistic* algorithms (such as probabilistic encryption algorithms), we must be careful; There are two different definitions of the functionality requirement. We recall them informally in terms of obfuscation of probabilistic encryption algorithms. Let $\mathcal{E}_K(M, R)$ be a private-key encryption program, where K is an embedded private key, M is a plaintext, and R is a set of random coins. Similarly, let $\mathcal{E}'_K(M, R)$ be an obfuscation of it. The first definition is the usual one and requires that the two programs compute the same function, i.e., for every pair (M, R), we have $\mathcal{E}_K(M, R) = \mathcal{E}'_K(M, R)$. In this paper, obfuscators satisfying this functionality requirement are called *circuit obfuscators*[1]. On the other hand, the second definition requires that, for every M, the two distributions obtained by evaluating $\mathcal{E}_K(M, R)$ and $\mathcal{E}'_K(M, R)$ on independent random coins R are the same. This is a relaxed requirement, but it would be sufficient for cryptographic applications as noted in [14,15]. We call obfuscators satisfying this functionality requirement as *sampling obfuscators* as in [1, Section 6].

1.2 Transforming Private-Key Encryption into Public-Key Encryption

Transforming private-key encryption schemes into public-key encryption schemes is an interesting application of obfuscation. The idea is that, given a private-key encryption scheme, an obfuscation of an encryption program with a private key embedded is used as a public key and the private key is used for decryption as

[1] In this paper, programs are defined by boolean circuits.

it is. Let $\mathcal{E}_K(M, R)$ be a probabilistic private-key encryption program, where K is an embedded private key, M is a plaintext, and R is a set of random coins. Then we obfuscate it into a new encryption program $\mathcal{E}'_K(M, R)$, which we use as the public key. When we want to encrypt a message M by the public key, we pick a set of random coins R and execute the public key, i.e., the obfuscated program $\mathcal{E}'_K$ on (M, R). We expect that the public key reveals no information on the private key because the obfuscated program is unintelligible. In this sense, the resulting public key encryption scheme could satisfy some sort of security requirement. As mentioned above, the generic impossibility results of [1,10] does not rule out the possibility that we have a *general-purpose* obfuscator for such a transformation. By "general-purpose obfuscators", we mean obfuscators that can transform an arbitrary private-key encryption scheme into a secure public-key encryption scheme.

The transformation is very interesting for at least two reasons.

1. Impagliazzo and Rudich showed that there exists no black-box reduction from private-key encryption schemes into public-key encryption schemes [16]. The transformation by an obfuscator can bypass their impossibility result.
2. It was an original idea suggested by Diffie and Hellman in their seminal paper [5] to design a public-key encryption scheme (Recall that, when the paper was published, there was no candidate public-key encryption scheme). So we can say that it is a natural principle for the design of public-key encryption schemes. We may be able to construct a (totally) new public-key encryption scheme using this idea.

It is important to note that we should consider *probabilistic* private-key encryption schemes for this transformation to make sense. When we transform a *deterministic* private-key encryption scheme, the resulting candidate public-key encryption scheme is deterministic as well. No deterministic public-key encryption scheme is secure in the usual sense [11].

Hofheinz et al. provided a formal treatment of the transformation under their proposed definitions of the virtual black-box property [14]. They showed that a probabilistic private-key encryption scheme secure against chosen-plaintext attacks can be transformed into a probabilistic public-key encryption scheme secure against chosen-plaintext attacks if an obfuscator for the private-key scheme exists according to their definitions.

1.3 Motivating Question

Our motivating question is: Does such a general-purpose obfuscator exist? We already have at least two negative answers to this question. Both answers are based on the existence of private-key encryption schemes that are "unobfuscatable" in some sense. We need to be careful because the meaning of "unobfuscatable" is different.

The first answer is by [1, Section 4.3]. They constructed a *deterministic* private-key encryption scheme that is *unobfuscatable* in the sense that, given any encryption program with a private key embedded, one can efficiently compute