Alfred Menezes (Ed.)

LNCS 4622

Advances in Cryptology – CRYPTO 2007

27th Annual International Cryptology Conference
Santa Barbara, CA, USA, August 2007
Proceedings

International Association for Cryptologic Research

Springer

Alfred Menezes (Ed.)

Advances in Cryptology – CRYPTO 2007

27th Annual International Cryptology Conference
Santa Barbara, CA, USA, August 19-23, 2007
Proceedings

Springer

Volume Editor

Alfred Menezes
University of Waterloo
Department of Combinatorics & Optimization
Waterloo, Ontario N2L 3G1, Canada
E-mail: ajmeneze@uwaterloo.ca

Library of Congress Control Number: 2007932207

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

LNCS Sublibrary: SL 4 – Security and Cryptology

ISSN 0302-9743
ISBN-10 3-540-74142-9 Springer Berlin Heidelberg New York
ISBN-13 978-3-540-74142-8 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: 12104802 06/3180 5 4 3 2 1 0

Lecture Notes in Computer Science 4622

Preface

CRYPTO 2007, the 27th Annual International Cryptology Conference, was sponsored by the International Association for Cryptologic Research (IACR) in cooperation with the IEEE Computer Society Technical Committee on Security and Privacy, and the Computer Science Department of the University of California at Santa Barbara. The conference was held in Santa Barbara, California, August 19-23 2007. CRYPTO 2007 was chaired by Markus Jakobsson, and I had the privilege of serving as the Program Chair.

The conference received 186 submissions. Each paper was assigned at least three reviewers, while submissions co-authored by Program Committee members were reviewed by at least five people. After 11 weeks of discussion and deliberation, the Program Committee, aided by reports from over 148 external reviewers, selected 33 papers for presentation. The authors of accepted papers had four weeks to prepare final versions for these proceedings. These revised papers were not subject to editorial review and the authors bear full responsibility for their contents.

The Committee identified the following three papers as the best papers: "Cryptography with Constant Input Locality" by Benny Applebaum, Yuval Ishai and Eyal Kushilevitz; "Practical Cryptanalysis of SFLASH" by Vivien Dubois, Pierre-Alain Fouque, Adi Shamir and Jacques Stern; and "Finding Small Roots of Bivariate Integer Polynomial Equations: A Direct Approach" by Jean-Sébastien Coron. The authors of these papers received invitations to submit full versions to the *Journal of Cryptology*. After a close vote, the Committee selected Benny Applebaum, Yuval Ishai and Eyal Kushilevitz, the authors of the first paper, as recipients of the Best Paper Award.

The conference featured invited lectures by Ross Anderson and Paul Kocher. Ross Anderson's paper "Information Security Economics – And Beyond" has been included in these proceedings.

There are many people who contributed to the success of CRYPTO 2007. I would like the thank the many authors from around the world for submitting their papers. I am deeply grateful to the Program Committee for their hard work, enthusiasm, and conscientious efforts to ensure that each paper received a thorough and fair review. Thanks also to the external reviewers, listed on the following pages, for contributing their time and expertise. It was a pleasure working with Markus Jakobsson and the staff at Springer. I am grateful to Andy Clark, Cynthia Dwork, Arjen Lenstra and Bart Preneel for their advice. Finally, I would like to thank Dan Bernstein for organizing a lively Rump Session, and Shai Halevi for developing and maintaining his most useful Web Submission and Review Software.

June 2007 Alfred Menezes

CRYPTO 2007

August 19-23, 2007, Santa Barbara, California, USA

Sponsored by the
International Association for Cryptologic Research (IACR)

in cooperation with
IEEE Computer Society Technical Committee on Security and Privacy,
Computer Science Department, University of California, Santa Barbara

General Chair

Markus Jakobsson, Indiana University, USA

Program Chair

Alfred Menezes, University of Waterloo, Canada

Program Committee

Amos Beimel .... Ben-Gurion University, Israel
Alex Biryukov .... University of Luxembourg, Luxembourg
Xavier Boyen .... Voltage Security, USA
Yevgeniy Dodis ....New York University, USA
Orr Dunkelman ....Katholieke Universiteit Leuven, Belgium
Matt Franklin ....UC Davis, USA
Steven Galbraith .... Royal Holloway, University of London, UK
Rosario Gennaro ....IBM Research, USA
Martin Hirt ....ETH Zurich, Switzerland
Nick Howgrave-Graham ....NTRU, USA
Antoine Joux ....DGA and Université de Versailles, France
John Kelsey ....NIST, USA
Neal Koblitz ....University of Washington, USA
Kaoru Kurosawa ....Ibaraki University, Japan
Tanja Lange ....Technische Universiteit Eindhoven, Netherlands
Kristin Lauter .... Microsoft Research, USA
Kenny Paterson .... Royal Holloway, University of London, UK
David Pointcheval ....École Normale Supérieure, France
Bart Preneel ....Katholieke Universiteit Leuven, Belgium
Zulfikar Ramzan .... Symantec, USA
Omer Reingold ....Weizmann Institute of Science, Israel
Rei Safavi-Naini .... University of Calgary, Canada
Amit Sahai ....UCLA, USA
Palash Sarkar ....Indian Statistical Institute, India
Nigel Smart ....University of Bristol, UK
Adam Smith ....UCLA and Penn State University, USA
Rainer Steinwandt .... Florida Atlantic University, USA
Yiqun Lisa Yin .... Independent Consultant, USA

Advisory Members

Cynthia Dwork (CRYPTO 2006 Program Chair) .... Microsoft, USA
David Wagner (CRYPTO 2008 Program Chair) .... UC Berkeley, USA

External Reviewers

Michel Abdalla
Masayuki Abe
Joel Alwen
Elena Andreeva
Tomoyuki Asano
Nuttapong Attrapadung
Georges Baatz
Lejla Batina
Aurélie Bauer
Zuzana Beerliová
Josh Benaloh
Waldyr Benits Jr.
Daniel J. Bernstein
Jens-Matthias Bohli
Alexandra Boldyreva
Carl Bosley
Colin Boyd
Daniel R.L. Brown
Ran Canetti
David Cash
Dario Catalano
Denis Charles
Lily Chen
Benoît Chevallier-Mames
Sherman Chow
Carlos Cid
Henry Cohn
Scott Contini
Jason Crampton
Joan Daemen
Quynh Dang
Cécile Delerablée
Alex Dent
Zeev Dvir
Morris Dworkin
Phil Eagle
Pooya Farshim
Marc Fischlin
Matthias Fitzi
Georg Fuschbauer
Nicolas Gama
Joachim von zur Gathen
Willi Geiselmann
Craig Gentry
Marc Girault
Mark Gondree
Jens Groth
Manabu Hagiwara
Iftach Haitner
Shai Halevi
Goichiro Hanaoka
Kristiyan Haralambiev
Danny Harnik
Swee-Huay Heng
Shoichi Hirose
Katrin Hoepper
Susan Hohenberger
Thomas Holenstein
Emeline Hufschmitt
Russell Impagliazzo
Yuval Ishai
Tetsu Iwata
Malika Izabachène
Shaoquan Jiang
Charanjit Jutla
Jonathan Katz
Aggelos Kiayias
Eike Kiltz
Darko Kirovski
Lars Knudsen
Yuichi Komano
Hugo Krawczyk
Sébastien Kunz-Jacques
Brian LaMacchia
Gaëtan Leurent
Yehuda Lindell
Joseph Liu
Stefan Lucks
Norbert Lütkenhaus
Philip MacKenzie
Tal Malkin
Keith Martin
Alexander Maximov
David Mireles
Ilya Mironov
Anton Mityagin
Payman Mohassel
David Molnar
Tal Moran
Moni Naor
Ashwin Nayak
Adam O'Neill
Gregory Neven
Phong Nguyen
Jesper Buus Nielsen
Kobbi Nissim
Wakaha Ogata
Rafail Ostrovsky
Elisabeth Oswald
Rafael Pass
Maura Paterson
Olivier Pereira
Giuseppe Persiano
Duong Hieu Phan
Benny Pinkas
Angela Piper
Alf van der Poorten
Manoj Prabhakaran
Bartosz Przydatek
Prashant Puniya
Tal Rabin
Dominik Raub
Oded Regev
Jean-René Reinhard

Renato Renner
Reza Reyhanitabar
Alon Rosen
Guy Rothblum
Jacob Schuldt
Gil Segev
Siamak Shahandashti
Jamshid Shokrollahi
Igor Shparlinski
Tom Shrimpton
Andrey Sidorenko
Johan Sjödin
Till Stegers
Christine Swart
Mike Szydlo
Stefano Tessaro
Jacques Traoré
José Villegas
Ivan Visconti
Shabsi Walfish
Huaxiong Wang
Bogdan Warinschi
Brent Waters
Enav Weinreb
Daniel Wichs
Douglas Wikström
Christopher Wolf
Stefan Wolf
Ronald de Wolf
David Woodruff
Hongjun Wu
Qianhong Wu
Jürg Wullschleger
Vassilis Zikas

Lecture Notes in Computer Science

For information about Vols. 1–4543

please contact your bookseller or Springer

Vol. 4671: V. Malyshkin (Ed.), Parallel Computing Technologies. XIV, 635 pages. 2007.

Vol. 4660: S. Džeroski, J. Todorovski (Eds.), Computational Discovery of Scientific Knowledge. X, 327 pages. 2007. (Sublibrary LNAI).

Vol. 4651: F. Azevedo, P. Barahona, F. Fages, F. Rossi (Eds.), Recent Advances in Constraints. VIII, 185 pages. 2007. (Sublibrary LNAI).

Vol. 4647: R. Martin, M. Sabin, J. Winkler (Eds.), Mathematics of Surfaces XII. IX, 509 pages. 2007.

Vol. 4643: M.-F. Sagot, M.E.M.T. Walter (Eds.), Advances in Bioinformatics and Computational Biology. IX, 177 pages. 2007. (Sublibrary LNBI).

Vol. 4634: H.R. Nielson, G. Filé (Eds.), Static Analysis. XI, 469 pages. 2007.

Vol. 4632: R. Alhajj, H. Gao, X. Li, J. Li, O.R. Zaïane (Eds.), Advanced Data Mining and Applications. XV, 634 pages. 2007. (Sublibrary LNAI).

Vol. 4628: L.N. de Castro, F.J. Von Zuben, H. Knidel (Eds.), Artificial Immune Systems. XII, 438 pages. 2007.

Vol. 4626: R.O. Weber, M.M. Richter (Eds.), Case-Based Reasoning Research and Development. XIII, 534 pages. 2007. (Sublibrary LNAI).

Vol. 4624: T. Mossakoski, U. Mantanari, M. Haveraaen (Eds.), Algebra and Coalgebra in Computer Science. XI, 463 pages. 2007.

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

Vol. 4619: F. Dehne, J.-R. Sack, N. Zeh (Eds.), Algorithms and Data Structures. XVI, 662 pages. 2007.

Vol. 4618: S.G. Akl, C.S. Calude, M.J. Dinneen, G. Rozenberg, H.T. Wareham (Eds.), Unconventional Computation. X, 243 pages. 2007.

Vol. 4617: V. Torra, Y. Narukawa, Y. Yoshida (Eds.), Modeling Decisions for Artificial Intelligence. XII, 502 pages. 2007. (Sublibrary LNAI).

Vol. 4616: A. Dress, Y. Xu, B. Zhu (Eds.), Combinatorial Optimization and Applications. XI, 390 pages. 2007.

Vol. 4615: R. de Lemos, C. Gacek, A. Romanovsky (Eds.), Architecting Dependable Systems IV. XIV, 435 pages. 2007.

Vol. 4613: F.P. Preparata, Q. Fang (Eds.), Frontiers in Algorithmics. XI, 348 pages. 2007.

Vol. 4612: I. Miguel, W. Ruml (Eds.), Abstraction, Reformulation, and Approximation. XI, 418 pages. 2007. (Sublibrary LNAI).

Vol. 4611: J. Indulska, J. Ma, L.T. Yang, T. Ungerer, J. Cao (Eds.), Ubiquitous Intelligence and Computing. XXIII, 1257 pages. 2007.

Vol. 4610: B. Xiao, L.T. Yang, J. Ma, C. Muller-Schloer, Y. Hua (Eds.), Autonomic and Trusted Computing. XVIII, 571 pages. 2007.

Vol. 4609: E. Ernst (Ed.), ECOOP 2007 – Object-Oriented Programming. XIII, 625 pages. 2007.

Vol. 4608: H.W. Schmidt, I. Crnkovic, G.T. Heineman, J.A. Stafford (Eds.), Component-Based Software Engineering. XII, 283 pages. 2007.

Vol. 4607: L. Baresi, P. Fraternali, G.-J. Houben (Eds.), Web Engineering. XVI, 576 pages. 2007.

Vol. 4606: A. Pras, M. van Sinderen (Eds.), Dependable and Adaptable Networks and Services. XIV, 149 pages. 2007.

Vol. 4605: D. Papadias, D. Zhang, G. Kollios (Eds.), Advances in Spatial and Temporal Databases. X, 479 pages. 2007.

Vol. 4604: U. Priss, S. Polovina, R. Hill (Eds.), Conceptual Structures: Knowledge Architectures for Smart Applications. XII, 514 pages. 2007. (Sublibrary LNAI).

Vol. 4603: F. Pfenning (Ed.), Automated Deduction – CADE-21. XII, 522 pages. 2007. (Sublibrary LNAI).

Vol. 4602: S. Barker, G.-J. Ahn (Eds.), Data and Applications Security XXI. X, 291 pages. 2007.

Vol. 4600: H. Comon-Lundh, C. Kirchner, H. Kirchner (Eds.), Rewriting, Computation and Proof. XVI, 273 pages. 2007.

Vol. 4599: S. Vassiliadis, M. Berekovic, T.D. Hämäläinen (Eds.), Embedded Computer Systems: Architectures, Modeling, and Simulation. XVIII, 466 pages. 2007.

Vol. 4598: G. Lin (Ed.), Computing and Combinatorics. XII, 570 pages. 2007.

Vol. 4597: P. Perner (Ed.), Advances in Data Mining. XI, 353 pages. 2007. (Sublibrary LNAI).

Vol. 4596: L. Arge, C. Cachin, T. Jurdziński, A. Tarlecki (Eds.), Automata, Languages and Programming. XVII, 953 pages. 2007.

Vol. 4595: D. Bošnački, S. Edelkamp (Eds.), Model Checking Software. X, 285 pages. 2007.

Vol. 4594: R. Bellazzi, A. Abu-Hanna, J. Hunter (Eds.), Artificial Intelligence in Medicine. XVI, 509 pages. 2007. (Sublibrary LNAI).

Vol. 4592: Z. Kedad, N. Lammari, E. Métais, F. Meziane, Y. Rezgui (Eds.), Natural Language Processing and Information Systems. XIV, 442 pages. 2007.

Vol. 4591: J. Davies, J. Gibbons (Eds.), Integrated Formal Methods. IX, 660 pages. 2007.

Vol. 4590: W. Damm, H. Hermanns (Eds.), Computer Aided Verification. XV, 562 pages. 2007.

Vol. 4589: J. Münch, P. Abrahamsson (Eds.), Product-Focused Software Process Improvement. XII, 414 pages. 2007.

Vol. 4588: T. Harju, J. Karhumäki, A. Lepistö (Eds.), Developments in Language Theory. XI, 423 pages. 2007.

Vol. 4587: R. Cooper, J. Kennedy (Eds.), Data Management. XIII, 259 pages. 2007.

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

Vol. 4585: M. Kryszkiewicz, J.F. Peters, H. Rybinski, A. Skowron (Eds.), Rough Sets and Intelligent Systems Paradigms. XIX, 836 pages. 2007. (Sublibrary LNAI).

Vol. 4584: N. Karssemeijer, B. Lelieveldt (Eds.), Information Processing in Medical Imaging. XX, 777 pages. 2007.

Vol. 4583: S.R. Della Rocca (Ed.), Typed Lambda Calculi and Applications. X, 397 pages. 2007.

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

Vol. 4581: A. Petrenko, M. Veanes, J. Tretmans, W. Grieskamp (Eds.), Testing of Software and Communicating Systems. XII, 379 pages. 2007.

Vol. 4580: B. Ma, K. Zhang (Eds.), Combinatorial Pattern Matching. XII, 366 pages. 2007.

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

Vol. 4578: F. Masulli, S. Mitra, G. Pasi (Eds.), Applications of Fuzzy Sets Theory. XVIII, 693 pages. 2007. (Sublibrary LNAI).

Vol. 4577: N. Sebe, Y. Liu, Y.-t. Zhuang (Eds.), Multimedia Content Analysis and Mining. XIII, 513 pages. 2007.

Vol. 4576: D. Leivant, R. de Queiroz (Eds.), Logic, Language, Information and Computation. X, 363 pages. 2007.

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

Vol. 4574: J. Derrick, J. Vain (Eds.), Formal Techniques for Networked and Distributed Systems – FORTE 2007. XI, 375 pages. 2007.

Vol. 4573: M. Kauers, M. Kerber, R. Miner, W. Windsteiger (Eds.), Towards Mechanized Mathematical Assistants. XIII, 407 pages. 2007. (Sublibrary LNAI).

Vol. 4572: F. Stajano, C. Meadows, S. Capkun, T. Moore (Eds.), Security and Privacy in Ad-hoc and Sensor Networks. X, 247 pages. 2007.

Vol. 4571: P. Perner (Ed.), Machine Learning and Data Mining in Pattern Recognition. XIV, 913 pages. 2007. (Sublibrary LNAI).

Vol. 4570: H.G. Okuno, M. Ali (Eds.), New Trends in Applied Artificial Intelligence. XXI, 1194 pages. 2007. (Sublibrary LNAI).

Vol. 4569: A. Butz, B. Fisher, A. Krüger, P. Olivier, S. Owada (Eds.), Smart Graphics. IX, 237 pages. 2007.

Vol. 4568: T. Ishida, S. R. Fussell, P. T. J. M. Vossen (Eds.), Intercultural Collaboration. XIII, 395 pages. 2007.

Vol. 4566: M.J. Dainoff (Ed.), Ergonomics and Health Aspects of Work with Computers. XVIII, 390 pages. 2007.

Vol. 4565: D.D. Schmorrow, L.M. Reeves (Eds.), Foundations of Augmented Cognition. XIX, 450 pages. 2007. (Sublibrary LNAI).

Vol. 4564: D. Schuler (Ed.), Online Communities and Social Computing. XVII, 520 pages. 2007.

Vol. 4563: R. Shumaker (Ed.), Virtual Reality. XXII, 762 pages. 2007.

Vol. 4562: D. Harris (Ed.), Engineering Psychology and Cognitive Ergonomics. XXIII, 879 pages. 2007. (Sublibrary LNAI).

Vol. 4561: V.G. Duffy (Ed.), Digital Human Modeling. XXIII, 1068 pages. 2007.

Vol. 4560: N. Aykin (Ed.), Usability and Internationalization, Part II. XVIII, 576 pages. 2007.

Vol. 4559: N. Aykin (Ed.), Usability and Internationalization, Part I. XVIII, 661 pages. 2007.

Vol. 4558: M.J. Smith, G. Salvendy (Eds.), Human Interface and the Management of Information, Part II. XXIII, 1162 pages. 2007.

Vol. 4557: M.J. Smith, G. Salvendy (Eds.), Human Interface and the Management of Information, Part I. XXII, 1030 pages. 2007.

Vol. 4556: C. Stephanidis (Ed.), Universal Access in Human-Computer Interaction, Part III. XXII, 1020 pages. 2007.

Vol. 4555: C. Stephanidis (Ed.), Universal Access in Human-Computer Interaction, Part II. XXII, 1066 pages. 2007.

Vol. 4554: C. Stephanidis (Ed.), Universal Acess in Human Computer Interaction, Part I. XXII, 1054 pages. 2007.

Vol. 4553: J.A. Jacko (Ed.), Human-Computer Interaction, Part IV. XXIV, 1225 pages. 2007.

Vol. 4552: J.A. Jacko (Ed.), Human-Computer Interaction, Part III. XXI, 1038 pages. 2007.

Vol. 4551: J.A. Jacko (Ed.), Human-Computer Interaction, Part II. XXIII, 1253 pages. 2007.

Vol. 4550: J.A. Jacko (Ed.), Human-Computer Interaction, Part I. XXIII, 1240 pages. 2007.

Vol. 4549: J. Aspnes, C. Scheideler, A. Arora, S. Madden (Eds.), Distributed Computing in Sensor Systems. XIII, 417 pages. 2007.

Vol. 4548: N. Olivetti (Ed.), Automated Reasoning with Analytic Tableaux and Related Methods. X, 245 pages. 2007. (Sublibrary LNAI).

Vol. 4547: C. Carlet, B. Sunar (Eds.), Arithmetic of Finite Fields. XI, 355 pages. 2007.

Vol. 4546: J. Kleijn, A. Yakovlev (Eds.), Petri Nets and Other Models of Concurrency – ICATPN 2007. XI, 515 pages. 2007.

Vol. 4545: H. Anai, K. Horimoto, T. Kutsia (Eds.), Algebraic Biology. XIII, 379 pages. 2007.

Vol. 4544: S. Cohen-Boulakia, V. Tannen (Eds.), Data Integration in the Life Sciences. XI, 282 pages. 2007. (Sublibrary LNBI).

Table of Contents

I Cryptanalysis I

II Secure Searching

III Invited Talk

IV Theory I

V Lattices

VI Random Oracles

VII Hash Functions

VIII Theory II

IX Quantum Cryptography

X Cryptanalysis II

XI Encryption

XII Protocol Analysis

XIII Public-Key Encryption

XIV Multi-party Computation

Practical Cryptanalysis of SFLASH

Vivien Dubois[1], Pierre-Alain Fouque[1], Adi Shamir[1,2], and Jacques Stern[1]

[1] École normale supérieure
Département d'Informatique 45, rue d'Ulm
75230 Paris cedex 05, France
Vivien.Dubois@ens.fr,
Pierre-Alain.Fouque@ens.fr, Jacques.Stern@ens.fr
[2] Weizmann Institute of Science
Adi.Shamir@weizmann.ac.il

Abstract. In this paper, we present a practical attack on the signature scheme SFLASH proposed by Patarin, Goubin and Courtois in 2001 following a design they had introduced in 1998. The attack only needs the public key and requires about one second to forge a signature for any message, after a one-time computation of several minutes. It can be applied to both SFLASH^{v2} which was accepted by NESSIE, as well as to SFLASH^{v3} which is a higher security version.

1 Introduction

In the last twenty years, multivariate cryptography has emerged as a potential alternative to RSA or DLOG [12,2] schemes. Many schemes have been proposed whose security appears somehow related to the problem of deciding whether or not a quadratic system of equations is solvable, which is known to be NP-complete [5]. An attractive feature of such schemes is that they have efficient implementations on smart cards, although the public and secret keys are rather large. Contrary to RSA or DLOG schemes, no polynomial quantum algorithm is known to solve this problem.

The SFLASH Scheme. SFLASH is based on the Matsumoto-Imai scheme (MI) [7], also called the C^* scheme. It uses the exponentiation $x \mapsto x^{q^\theta+1}$ in a finite field $\mathbb{F}_{q^n}$ of dimension n over a binary field $\mathbb{F}_q$, and two affine maps on the input and output variables. The MI scheme was broken by Patarin in 1995 [8]. However, based on an idea of Shamir [13], Patarin *et al.* proposed at CT-RSA 2001 [10] to remove some equations from the MI public key and called the resulting scheme C^{*-}. This completely avoids the previous attack and, although not appropriate for an encryption scheme, it is well-suited for a signature scheme. The scheme was selected in 2003 by the NESSIE European Consortium as one of the three recommended public key signature schemes, and as the best known solution for low cost smart cards.

A. Menezes (Ed.): CRYPTO 2007, LNCS 4622, pp. 1–12, 2007.

Previous Attacks on SFLASH. The first version of SFLASH, called SFLASH^{v1}, is a more efficient variant of C^{*-} using a small subfield. It has been attacked by Gilbert and Minier in [6]. However, the later versions (SFLASH^{v2} and SFLASH^{v3}) were immune to this attack.

Recently, Dubois, Fouque and Stern in [1] proposed an attack on a special class of SFLASH-like signatures. They show that when the kernel of the linear map $x \mapsto x + x^{q^\theta}$ is non-trivial, the C^{*-} scheme is not secure. The attack is very efficient in this case, but relies on some specific properties which are not met by the NESSIE proposals and which make the scheme look less secure.

Our Results. In this paper, we achieve a total break of the NESSIE standard with the actual parameters suggested by the designers: given only the public key, a signature for any message can be forged in about one second after a one time computation of several minutes. The asymptotic running time of the attack is $O(\log^2(q)n^6)$ since it only needs standard linear algebra algorithms on $O(n^2)$ variables, and n is typically very small. As in [1], the basic strategy of the attack is to recover additional independent equations in order to apply Patarin's attack [8]. To this end, both attacks use the differential of the public key. However, the attacks differ in the way the invariants related to the differential are found. The differential of the public key, also called its polar form, is very important since it transforms quadratic equations into linear ones. Hence, it can be used to find some linear relations that involve the secret keys. Its cryptanalytic significance had been demonstrated in [4].

Organization of the Paper. In section 2, we describe the SFLASH signature scheme and the practical parameters recommended by Patarin *et al.* and approved by NESSIE. Then, in section 3 we present the multiplicative property of the differential that we need. Next, in section 4 we describe how to recover linear maps related to multiplications in the finite field from the public key. In section 5, we show how to break the NESSIE proposal given only the public key. In section 6, we extend the attack to cover the case when up to half of the equations are removed, and finally in section 7, we compare our method with the technique of [1] before we conclude.

2 Description of SFLASH

In 1988, Matsumoto and Imai [7] proposed the C^* scheme for encryption and signature. The basic idea is to hide a quadratic easily invertible mapping F in some large finite field $\mathbb{F}_{q^n}$ by two secret invertible linear (or affine) maps U and T which mix together the n coordinates of F over the small field $\mathbb{F}_q$:

$$P = T \circ F \circ U$$

where $F(x) = x^{q^\theta+1}$ in $\mathbb{F}_{q^n}$. This particular form was chosen since its representation as a multivariate mapping over the small field is quadratic, and thus the size of the public key is relatively small.

The secret key consists of the maps U and T; the public key P is formed by the n quadratic expressions, whose inputs and outputs are mixed by U and T, respectively. It can be seen that F and P are invertible whenever $\gcd(q^\theta+1, q^n-1)=1$, which implies that q has to be a power of 2 since q is a prime power.

This scheme was successfully attacked by Patarin [8] in 1996. To avoid this attack and restore security Patarin *et al.* proposed in [11] to remove from the public key the last r quadratic expressions (out of the initial n), and called this variant of C^* schemes, C^{*-}. Furthermore, if the value of r is chosen such that $q^r \geq 2^{80}$, then the variant is termed C^{*--}. If we denote by Π the projection of n variables over $\mathbb{F}_q$ onto the first $n-r$ coordinates, we can represent the public key by the composition :

$$P_\Pi = \Pi \circ T \circ F \circ U = T_\Pi \circ F \circ U.$$

In the sequel, P denotes the public key of a C^* scheme whereas P_Π denotes a C^{*-} or C^{*--} public key. In both cases the secret key consists of the two linear maps T and U.

To sign a message m, the last r coordinates are chosen at random, and the signer recovers s such that $P_\Pi(s)=m$ by inverting T, U and F. A signature (m,s) can be checked by computing $P_\Pi(s)$ with the public key, which is extremely fast since it only involves the evaluation of a small number of quadratic expressions over the small finite field $\mathbb{F}_q$.

For the NESSIE project and in [10], Patarin *et al.* proposed two particular recommended choices for the parameters of C^{*--} :

- for SFLASH^{v2} : $q=2^7$, $n=37$, $\theta=11$ and $r=11$
- for SFLASH^{v3} : $q=2^7$, $n=67$, $\theta=33$ and $r=11$

SFLASH^{v3} was actually proposed to provide an even more conservative level of security than SFLASH^{v2} [10]. However, the designers made clear that they viewed SFLASH^{v2} as providing adequate security, and no attack on these two choices of parameters had been reported so far.

The important fact to notice here is that in both cases $\gcd(n,\theta)=1$ and thus the attack described in [1] on a modified version of SFLASH in which $\gcd(n,\theta)>1$ cannot be applied. The attack described in this paper shares with [1] the basic observation about the multiplicative property of C^{*-} schemes which is described in section 3, but proceeds in a completely different way. More discussion about the relationships between the two attacks can be found in section 7.

3 The Multiplicative Property of the Differential

The attack uses a specific multiplicative property of the differential of the public key of a C^{*-} scheme.

The differential of the internal quadratic system $F(x)=x^{q^\theta+1}$ is a symmetric bilinear function in $\mathbb{F}_{q^n}$, called DF, and it is defined for all $a, x \in \mathbb{F}_{q^n}$ by the linear operator :

$$DF(a,x) = F(a+x) - F(a) - F(x) + F(0).$$