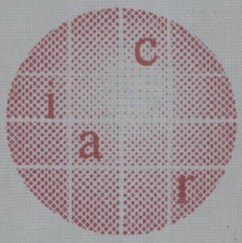
Lecture Notes in Computer Science 1592

Jacques Stern (Ed.)

Advances in Cryptology – EUROCRYPT '99

International Conference on the Theory and Application of Cryptographic Techniques
Prague, Czech Republic, May 1999
Proceedings



Springer

Jacques Stern (Ed.)

Advances in Cryptology – EUROCRYPT '99

International Conference on the Theory
and Application of Cryptographic Techniques
Prague, Czech Republic, May 2-6, 1999
Proceedings

Springer

Series Editors

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

Volume Editor

Jacques Stern
Ecole Normale Supérieure
45, rue d'Ulm, F-75230 Paris 05, France
E-mail: Jacques.Stern@ens.fr

Cataloging-in-Publication data applied for

Die Deutsche Bibliothek – CIP-Einheitsaufnahme

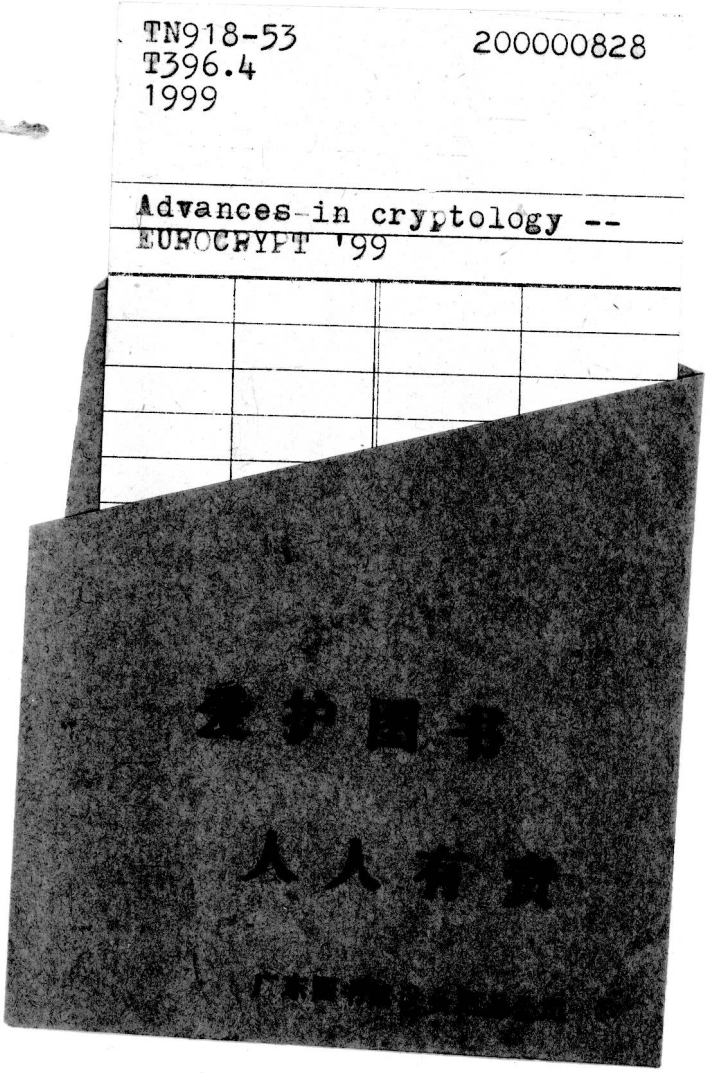
Advances in cryptology : proceedings / EUROCRYPT '99, International Conference on the Theory and Application of Cryptographic Techniques, Prague, Czech Republic, May 2 - 6, 1999. Jacques Stern (ed.). - Berlin ; Heidelberg ; New York ; Barcelona ; Hong Kong ; London ; Milan ; Paris ; Singapore ; Tokyo : Springer, 1999
(Lecture notes in computer science ; Vol. 1592)
ISBN 3-540-65889-0

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

ISSN 0302-9743
ISBN 3-540-65889-0 Springer-Verlag Berlin Heidelberg New York

Typesetting: Camera-ready by author
SPIN 10704664 06/3142 – 5 4 3 2 1 0 Printed on acid-free paper

Lecture Notes in Computer Science 1592
Edited by G. Goos, J. Hartmanis and J. van Leeuwen



Springer
Berlin
Heidelberg
New York
Barcelona
Hong Kong
London
Milan
Paris
Singapore
Tokyo

Preface

EUROCRYPT '99, the seventeenth annual Eurocrypt Conference, was sponsored by the International Association for Cryptologic Research (IACR), in cooperation with the Group of Cryptology within the Union of Czech Mathematicians and Physicists. The General Chair, Jaroslav Hruby, was responsible for the overall organization of the conference in the beautiful city of Prague. Let me mention that it was a pleasure to work together: although we were in different locations, we managed to stay in close contact and maintain a smooth organization of the conference.

The Program Committee, consisting of 21 members, considered 120 papers and selected 32 for presentation. In addition, Ross Anderson kindly agreed to chair the traditional rump session for informal short presentations of new results. These proceedings include the revised versions of the 32 papers accepted by the Program Committee. These papers were selected on the basis of originality, quality, and relevance to cryptography. As a result, they should give a proper picture of how the field is evolving. Revisions were not checked and the authors bear full responsibility for the contents of their papers.

The selection of papers was a difficult and challenging task. Each submission was refereed by at least three reviewers and most had four reports or more. I wish to thank the program committee members, who did an excellent job. In addition, I gratefully acknowledge the help of a large number of colleagues who reviewed submissions in their areas of expertise. They are: Michel Abdalla, Josh Benaloh, Charles Bennett, Simon Blackburn, Matt Blaze, Christian Cachin, Jan Camenisch, Ran Canetti, Benny Chor, Galdi Clemente, Jean-Sébastien Coron, Paolo D'Arco, Anand Desai, Uri Feige, Marc Fischlin, Roger Fischlin, Matt Franklin, Steven Galbraith, Rosario Gennaro, Pierre Girard, Dieter Gollmann, Shai Halevi, Helena Handschuh, Yuval Ishai, Markus Jakobsson, Mike Just, Ted Krovetz, Kaoru Kurosawa, Eyal Kushilevitz, Keith Martin, Barbara Masucci, Johannes Merkle, Daniele Micciancio, Victor S. Miller, Fauzan Mirza, Serge Mister, Peter L. Montgomery, Tal Mor, David M'Raïhi, Luke O'Connor, Andrew Odlyzko, Wakaha Ogata, Koji Okada, Pascal Paillier, Pino Persiano, David Pointcheval, Bart Preneel, Tal Rabin, Omer Reingold, Phil Rogaway, Ludovic Rousseau, Berry Schoenmakers, Peter Shor, Jean-Pierre Seifert, Othmar Staffelbach, Ugo Vaccaro, Serge Vaudenay, Ruizhong Wei, Mike Wiener, Rebecca Wright, Xian-Mo Zhang, and Robert Zuccherato. I apologize for any inadvertent omission.

I also wish to thank my PhD students Phong Nguyen, Thomas Pornin, and Guillaume Poupard, who helped me a great deal at various steps of the whole process. Their computer skills and the time and effort they invested were a crucial ingredient of my ability to run the program committee. Thomas ran the electronic submission phase and was able to print all postscript files, including those produced by non-standard word processors. Guillaume opened a private

FTP server and Web site for PC members, and Phong did the editing work, both in paper and in electronic form. I hope I did not distract them too much from their research, but they were kind enough to tell me they had learnt a lot. Thanks also to Joelle Isnard and Nadine Riou, who organized the PC meeting in Paris.

Following the example of CRYPTO '98, EUROCRYPT '99 was the first of the Eurocrypt series with electronic submissions. The electronic submission option was a clear choice for almost all authors, with only 5% of the papers submitted by regular mail. I believe that the time has come to make e-submission mandatory, but it will be the choice of future Crypto and Eurocrypt PC chairs. I wish to thank Joe Kilian, who forwarded us the electronic submission software used for CRYPTO '98 and helped us run it. This software was originally developed by ACM's SIGACT group and I thank the ACM for allowing us to use their system.

Finally, I wish to thank the all authors who submitted papers for making this conference possible by creating the scientific material, and especially the authors of accepted papers. I would also like to thank the publisher, Springer-Verlag, for working within a tight schedule in order to produce these proceedings in due time.

February 1999

Jacques Stern
Program Chair
EUROCRYPT '99

EUROCRYPT '99

May 2 – 6, 1999, Prague, Czech Republic

Sponsored by the

International Association for Cryptologic Research (IACR)

in cooperation with the

Group of Cryptology within the Union of Czech Mathematicians and Physicists

General Chair

Jaroslav Hruby, UCMP, Czech Republic

Program Chair

Jacques Stern, École Normale Supérieure, France

Program Committee

Eli Biham ..... Technion, Israel
Mihir Bellare ..... University of California, San Diego, USA
Carlo Blundo ..... Università di Salerno, Italy
Dan Boneh ..... Stanford University, USA
Stefan Brands ..... Brands Technologies, Netherlands
Mike Burmester ..... Royal Holloway, London, UK
Don Coppersmith ..... IBM Research, USA
Claude Crépeau ..... McGill University, Canada
Cynthia Dwork ..... IBM Almaden Research Center, USA
Joan Feigenbaum ..... AT&T Labs - Research, USA
Lars Knudsen ..... University of Bergen, Norway
Tsutomu Matsumoto ..... Yokohama National University, Japan
Willi Meier ..... Fachhochschule Aargau, Switzerland
David Naccache ..... Gemplus, France
Jean-Jacques Quisquater ..... Université de Louvain, Belgium
Bruce Schneier ..... Counterpane Systems, USA
Claus Schnorr ..... Universität Frankfurt, Germany
Victor Shoup ..... IBM Zurich Research Lab, Switzerland
Paul Van Oorschot ..... Entrust Technologies, Canada
Yuliang Zheng ..... Monash University, Australia

Lecture Notes in Computer Science

For information about Vols. 1–1505
please contact your bookseller or Springer-Verlag

Vol. 1506: R. Koch, L. Van Gool (Eds.), 3D Structure from Multiple Images of Large-Scale Environments. Proceedings, 1998. VIII, 347 pages. 1998.

Vol. 1507: T.W. Ling, S. Ram, M.L. Lee (Eds.), Conceptual Modeling – ER '98. Proceedings, 1998. XVI, 482 pages. 1998.

Vol. 1508: S. Jajodia, M.T. Özsu, A. Dogac (Eds.), Advances in Multimedia Information Systems. Proceedings, 1998. VIII, 207 pages. 1998.

Vol. 1510: J.M. Zytkow, M. Quafafou (Eds.), Principles of Data Mining and Knowledge Discovery. Proceedings, 1998. XI, 482 pages. 1998. (Subseries LNAI).

Vol. 1511: D. O'Hallaron (Ed.), Languages, Compilers, and Run-Time Systems for Scalable Computers. Proceedings, 1998. IX, 412 pages. 1998.

Vol. 1512: E. Giménez, C. Paulin-Mohring (Eds.), Types for Proofs and Programs. Proceedings, 1996. VIII, 373 pages. 1998.

Vol. 1513: C. Nikolaou, C. Stephanidis (Eds.), Research and Advanced Technology for Digital Libraries. Proceedings, 1998. XV, 912 pages. 1998.

Vol. 1514: K. Ohta, D. Pei (Eds.), Advances in Cryptology – ASIACRYPT'98. Proceedings, 1998. XII, 436 pages. 1998.

Vol. 1515: F. Moreira de Oliveira (Ed.), Advances in Artificial Intelligence. Proceedings, 1998. X, 259 pages. 1998. (Subseries LNAI).

Vol. 1516: W. Ehrenberger (Ed.), Computer Safety, Reliability and Security. Proceedings, 1998. XVI, 392 pages. 1998.

Vol. 1517: J. Hromkovič, O. Sýkora (Eds.), Graph-Theoretic Concepts in Computer Science. Proceedings, 1998. X, 385 pages. 1998.

Vol. 1518: M. Luby, J. Rolim, M. Serna (Eds.), Randomization and Approximation Techniques in Computer Science. Proceedings, 1998. IX, 385 pages. 1998.

1519: T. Ishida (Ed.), Community Computing and Support Systems. VIII, 393 pages. 1998.

Vol. 1520: M. Maher, J.-F. Puget (Eds.), Principles and Practice of Constraint Programming - CP98. Proceedings, 1998. XI, 482 pages. 1998.

Vol. 1521: B. Rovan (Ed.), SOFSEM'98: Theory and Practice of Informatics. Proceedings, 1998. XI, 453 pages. 1998.

Vol. 1522: G. Gopalakrishnan, P. Windley (Eds.), Formal Methods in Computer-Aided Design. Proceedings, 1998. IX, 529 pages. 1998.

Vol. 1524: G.B. Orr, K.-R. Müller (Eds.), Neural Networks: Tricks of the Trade. VI, 432 pages. 1998.

Vol. 1525: D. Aucsmith (Ed.), Information Hiding. Proceedings, 1998. IX, 369 pages. 1998.

Vol. 1526: M. Broy, B. Rumpe (Eds.), Requirements Targeting Software and Systems Engineering. Proceedings, 1997. VIII, 357 pages. 1998.

Vol. 1527: P. Baumgartner, Theory Reasoning in Connection Calculi. IX, 283. 1999. (Subseries LNAI).

Vol. 1528: B. Preneel, V. Rijmen (Eds.), State of the Art in Applied Cryptography. Revised Lectures, 1997. VIII, 395 pages. 1998.

Vol. 1529: D. Farwell, L. Gerber, E. Hovy (Eds.), Machine Translation and the Information Soup. Proceedings, 1998. XIX, 532 pages. 1998. (Subseries LNAI).

Vol. 1530: V. Arvind, R. Ramanujam (Eds.), Foundations of Software Technology and Theoretical Computer Science. XII, 369 pages. 1998.

Vol. 1531: H.-Y. Lee, H. Motoda (Eds.), PRICAI'98: Topics in Artificial Intelligence. XIX, 646 pages. 1998. (Subseries LNAI).

Vol. 1096: T. Schael, Workflow Management Systems for Process Organisations. Second Edition. XII, 229 pages. 1998.

Vol. 1532: S. Arikawa, H. Motoda (Eds.), Discovery Science. Proceedings, 1998. XI, 456 pages. 1998. (Subseries LNAI).

Vol. 1533: K.-Y. Chwa, O.H. Ibarra (Eds.), Algorithms and Computation. Proceedings, 1998. XIII, 478 pages. 1998.

Vol. 1534: J.S. Sichman, R. Conte, N. Gilbert (Eds.), Multi-Agent Systems and Agent-Based Simulation. Proceedings, 1998. VIII, 237 pages. 1998. (Subseries LNAI).

Vol. 1535: S. Ossowski, Co-ordination in Artificial Agent Societies. XV; 221 pages. 1999. (Subseries LNAI).

Vol. 1536: W.-P. de Roever, H. Langmaack, A. Pnueli (Eds.), Compositionality: The Significant Difference. Proceedings, 1997. VIII, 647 pages. 1998.

Vol. 1537: N. Magnenat-Thalmann, D. Thalmann (Eds.), Modelling and Motion Capture Techniques for Virtual Environments. Proceedings, 1998. IX, 273 pages. 1998. (Subseries LNAI).

Vol. 1538: J. Hsiang, A. Ohori (Eds.), Advances in Computing Science – ASIAN'98. Proceedings, 1998. X, 305 pages. 1998.

Vol. 1539: O. Rüthing, Interacting Code Motion Transformations: Their Impact and Their Complexity. XXI,225 pages. 1998.

Vol. 1540: C. Beeri, P. Buneman (Eds.), Database Theory – ICDT'99. Proceedings, 1999. XI, 489 pages. 1999.

Vol. 1541: B. Kågström, J. Dongarra, E. Elmroth, J. Waśniewski (Eds.), Applied Parallel Computing. Proceedings, 1998. XIV, 586 pages. 1998.

Vol. 1542: H.I. Christensen (Ed.), Computer Vision Systems. Proceedings, 1999. XI, 554 pages. 1999.

Vol. 1543: S. Demeyer, J. Bosch (Eds.), Object-Oriented Technology ECOOP'98 Workshop Reader. 1998. XXII, 573 pages. 1998.

Vol. 1544: C. Zhang, D. Lukose (Eds.), Multi-Agent Systems. Proceedings, 1998. VII, 195 pages. 1998. (Subseries LNAI).

Vol. 1545: A. Birk, J. Demiris (Eds.), Learning Robots. Proceedings, 1996. IX, 188 pages. 1998. (Subseries LNAI).

Vol. 1546: B. Möller, J.V. Tucker (Eds.), Prospects for Hardware Foundations. Survey Chapters, 1998. X, 468 pages. 1998.

Vol. 1547: S.H. Whitesides (Ed.), Graph Drawing. Proceedings 1998. XII, 468 pages. 1998.

Vol. 1548: A.M. Haeberer (Ed.), Algebraic Methodology and Software Technology. Proceedings, 1999. XI, 531 pages. 1999.

Vol. 1550: B. Christianson, B. Crispo, W.S. Harbison, M. Roe (Eds.), Security Protocols. Proceedings, 1998. VIII, 241 pages. 1999.

Vol. 1551: G. Gupta (Ed.), Practical Aspects of Declarative Languages. Proceedings, 1999. VIII, 367 pgages. 1999.

Vol. 1552: Y. Kambayashi, D.L. Lee, E.-P. Lim, M.K. Mohania, Y. Masunaga (Eds.), Advances in Database Technologies. Proceedings, 1998. XIX, 592 pages. 1999.

Vol. 1553: S.F. Andler, J. Hansson (Eds.), Active, Real-Time, and Temporal Database Systems. Proceedings, 1997. VIII, 245 pages. 1998.

Vol. 1554: S. Nishio, F. Kishino (Eds.), Advanced Multimedia Content Processing. Proceedings, 1998. XIV, 454 pages. 1999.

Vol. 1555: J.P. Müller, M.P. Singh, A.S. Rao (Eds.), Intelligent Agents V. Proceedings, 1998. XXIV, 455 pages. 1999. (Subseries LNAI).

Vol. 1556: S. Tavares, H. Meijer (Eds.), Selected Areas in Cryptography. Proceedings, 1998. IX, 377 pages. 1999.

Vol. 1557: P. Zinterhof, M. Vajteršic, A. Uhl (Eds.), Parallel Computation. Proceedings, 1999. XV, 604 pages. 1999.

Vol. 1558: H. J.v.d. Herik, H. Iida (Eds.), Computers and Games. Proceedings, 1998. XVIII, 337 pages. 1999.

Vol. 1559: P. Flener (Ed.), Logic-Based Program Synthesis and Transformation. Proceedings, 1998. X, 331 pages. 1999.

Vol. 1560: K. Imai, Y. Zheng (Eds.), Public Key Cryptography. Proceedings, 1999. IX, 327 pages. 1999.

Vol. 1561: I. Damgård (Ed.), Lectures on Data Security.VII, 250 pages. 1999.

Vol. 1563: Ch. Meinel, S. Tison (Eds.), STACS 99. Proceedings, 1999. XIV, 582 pages. 1999.

Vol. 1567: P. Antsaklis, W. Kohn, M. Lemmon, A. Nerode, S. Sastry (Eds.), Hybrid Systems V. X, 445 pages. 1999.

Vol. 1568: G. Bertrand, M. Couprie, L. Perroton (Eds.), Discrete Geometry for Computer Imagery. Proceedings, 1999. XI, 459 pages. 1999.

Vol. 1569: F.W. Vaandrager, J.H. van Schuppen (Eds.), Hybrid Systems: Computation and Control. Proceedings, 1999. X, 271 pages. 1999.

Vol. 1570: F. Puppe (Ed.), XPS-99: Knowledge-Based Systems. VIII, 227 pages. 1999. (Subseries LNAI).

Vol. 1572: P. Fischer, H.U. Simon (Eds.), Computational Learning Theory. Proceedings, 1999. X, 301 pages. 1999. (Subseries LNAI).

Vol. 1574: N. Zhong, L. Zhou (Eds.), Methodologies for Knowledge Discovery and Data Mining. Proceedings, 1999. XV, 533 pages. 1999. (Subseries LNAI).

Vol. 1575: S. Jähnichen (Ed.), Compiler Construction. Proceedings, 1999. X, 301 pages. 1999.

Vol. 1576: S.D. Swierstra (Ed.), Programming Languages and Systems. Proceedings, 1999. X, 307 pages. 1999.

Vol. 1577: J.-P. Finance (Ed.), Fundamental Approaches to Software Engineering. Proceedings, 1999. X, 245 pages. 1999.

Vol. 1578: W. Thomas (Ed.), Foundations of Software Science and Computation Structures. Proceedings, 1999. X, 323 pages. 1999.

Vol. 1579: W.R. Cleaveland (Ed.), Tools and Algorithms for the Construction and Analysis of Systems. Proceedings, 1999. XI, 445 pages. 1999.

Vol. 1580: A. Včkovski, K.E. Brassel, H.-J. Schek (Eds.), Interoperating Geographic Information Systems. Proceedings, 1999. XI, 329 pages. 1999.

Vol. 1581: J.-Y. Girard (Ed.), Typed Lambda Calculi and Applications. Proceedings, 1999. VIII, 397 pages. 1999.

Vol. 1582: A. Lecomte, F. Lamarche, G. Perrier (Eds.), Logical Aspects of Computational Linguistics. Proceedings, 1997. XI, 251 pages. 1999. (Subseries LNAI).

Vol. 1586: J. Rolim et al. (Eds.), Parallel and Distributed Processing. Proceedings, 1999. XVII, 1443 pages. 1999.

Vol. 1587: J. Pieprzyk, R. Safavi-Naini, J. Seberry (Eds.), Information Security and Privacy. Proceedings, 1999. XI, 327 pages. 1999.

Vol. 1590: P. Atzeni, A. Mendelzon, G. Mecca (Eds.), The World Wide Web and Databases. Proceedings, 1998. VIII, 213 pages. 1999.

Vol. 1592: J. Stern (Ed.), Advances in Cryptology – EUROCRYPT '99. Proceedings, 1999. XII, 475 pages. 1999.

Vol. 1593: P. Sloot, M. Bubak, A. Hoekstra, B. Hertzberger (Eds.), High-Performance Computing and Networking. Proceedings, 1999. XXIII, 1318 pages. 1999.

Vol. 1594: P. Ciancarini, A.L. Wolf (Eds.), Coordination Languages and Models. Proceedings, 1999. IX, 420 pages. 1999.

Vol. 1596: R. Poli, H.-M. Voigt, S. Cagnoni, D. Corne, G.D. Smith, T.C. Fogarty (Eds.), Evolutionary Image Analysis, Signal Processing and Telecommunications. Proceedings, 1999. X, 225 pages. 1999.

Vol. 1597: H. Zuidweg, M. Campolargo, J. Delgado, A. Mullery (Eds.), Intelligence in Services and Networks. Proceedings, 1999. XII, 552 pages. 1999.

Vol. 1605: J. Billington, M. Diaz, G. Rozenberg (Eds.), Application of Petri Nets to Communication Networks. IX, 303 pages. 1999.

Springer and the environment

At Springer we firmly believe that an international science publisher has a special obligation to the environment, and our corporate policies consistently reflect this conviction.
We also expect our business partners – paper mills, printers, packaging manufacturers, etc. – to commit themselves to using materials and production processes that do not harm the environment. The paper in this book is made from low- or no-chlorine pulp and is acid free, in conformance with international standards for paper permanency.

Springer

Table of Contents

Cryptanalysis I

Hash Functions

Foundations I

Public Key

Watermarking and Fingerprinting

Elliptic Curves

New Schemes

Block Ciphers

Distributed Cryptography

Cryptanalysis II

Tools from Related Areas

Foundations II

Broadcast and Multicast

Cryptanalysis of RSA with Private Key d Less than $N^{0.292}$

Dan Boneh* and Glenn Durfee**

Computer Science Department, Stanford University, Stanford, CA 94305-9045
{dabo,gdurf}@cs.stanford.edu

Abstract. We show that if the private exponent d used in the RSA public-key cryptosystem is less than $N^{0.292}$ then the system is insecure. This is the first improvement over an old result of Wiener showing that when $d < N^{0.25}$ the RSA system is insecure. We hope our approach can be used to eventually improve the bound to $d < N^{0.5}$.

1 Introduction

To provide fast RSA signature generation one is tempted to use a small private exponent d. Unfortunately, Wiener [10] showed over ten years ago that if one uses $d < N^{0.25}$ then the RSA system can be broken. Since then there have been no improvements to this bound. Verheul and Tilborg [9] showed that as long as $d < N^{0.5}$ it is possible to expose d in less time than an exhaustive search; however, their algorithm requires exponential time as soon as $d > N^{0.25}$.

In this paper we give the first substantial improvement to Wiener's result. We show that as long as $d < N^{0.292}$ one can efficiently break the system. We hope our approach will eventually lead to what we believe is the correct bound, namely $d < N^{0.5}$. Our results are based on the seminal work of Coppersmith [2].

Wiener describes a number of clever techniques for avoiding his attack while still providing fast RSA signature generation. One such suggestion is to use a large value of e. Indeed, Wiener's attack provides no information as soon as $e > N^{1.5}$. In contrast, our approach is effective as long as $e < N^{1.875}$. Consequently, larger values of e must be used to defeat the attack. We discuss this variant in Section 5.

2 Overview of Our Approach

Recall that an RSA public key is a pair $\langle N, e\rangle$ where $N = pq$ is the product of two n-bit primes. For simplicity, we assume $\gcd(p-1, q-1) = 2$. The corresponding private key is a pair $\langle N, d\rangle$ where $e \cdot d \equiv 1 \bmod \frac{\phi(N)}{2}$ where $\phi(N) = N - p - q + 1$.

* Supported by DARPA.
** Supported by Certicom and an NSF Graduate Research Fellowship.

J. Stern (Ed.): EUROCRYPT'99, LNCS 1592, pp. 1–11, 1999.

Note that both e and d are less than $\phi(N)$. It follows that there exists an integer k such that

$$ed + k\left(\frac{N+1}{2} - \frac{p+q}{2}\right) = 1. \tag{1}$$

Writing $s = -\frac{p+q}{2}$ and $A = \frac{N+1}{2}$, we know:

$$k(A+s) \equiv 1 \pmod{e}.$$

Throughout the paper we write $e = N^\alpha$ for some α. Typically, e is of the same order of magnitude as N (e.g. $e > N/10$) and therefore α is very close to 1. As we shall see, when α is much smaller than 1 our results become even stronger.

Suppose the private exponent d satisfies $d < N^\delta$. Wiener's results show that when $\delta < 0.25$ the value of d can be efficiently found given e and N. Our goal is to show that the same holds for larger values of δ. By equation (1) we know that

$$|k| < \frac{2de}{\phi(N)} \leq 3de/N < 3e^{1+\frac{\delta-1}{\alpha}}.$$

Similarly, we know that

$$|s| < 2N^{0.5} = 2e^{1/2\alpha}.$$

To summarize, taking $\alpha \approx 1$ (which is the common case) and ignoring constants, we end up with the following problem: find integers k and s satisfying

$$k(A+s) \equiv 1 \pmod{e} \quad \text{where} \quad |s| < e^{0.5} \text{ and } |k| < e^\delta. \tag{2}$$

The problem can be viewed as follows: given an integer A, find an element "close" to A whose inverse modulo e is "small". We refer to this is the *small inverse problem*. Clearly, if for a given value of $\delta < 0.5$ one can efficiently list all the solutions to the small inverse problem, then RSA with private exponent smaller than N^δ is insecure (simply observe that given s modulo e one can factor N immediately, since $e > s$). Currently we can solve the small inverse problem whenever $\delta < 1 - \frac{1}{2}\sqrt{2} \approx 0.292$.

Remark 1. A simple heuristic argument shows that for any $\epsilon > 0$, if k is bounded by $e^{0.5-\epsilon}$ (i.e. $\delta < 0.5$) then the small inverse problem (equation (2)) is very likely to have a unique solution. The unique solution enables one to break RSA. Therefore, the problem encodes enough information to prove that RSA with $d < N^{0.5}$ is insecure. For $d > N^{0.5}$ we have that $k > N^{0.5}$ and the problem will no longer have a unique solution. Therefore, we believe this approach can be used to show that $d < N^{0.5}$ is insecure, but gives no results for $d > N^{0.5}$.

The next section gives a brief introduction to lattices over $\mathbb{Z}^n$. Our solution to the small inverse problem when α is close to 1 is given in Section 4. In Section 5 we give a solution for arbitrary α. Section 6 describes experimental results with the algorithm.