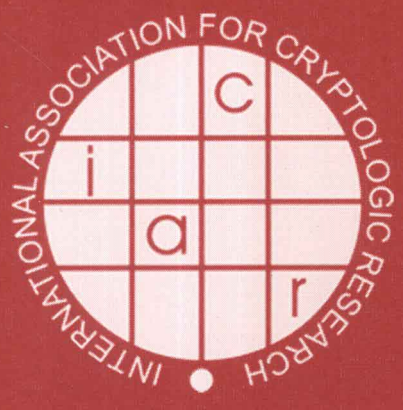
Moti Yung Yevgeniy Dodis
Aggelos Kiayias Tal Malkin (Eds.)

Public Key Cryptography – PKC 2006

LNCS 3958

9th International Conference
on Theory and Practice of Public-Key Cryptography
New York, NY, USA, April 2006, Proceedings



Springer

Moti Yung Yevgeniy Dodis
Aggelos Kiayias Tal Malkin (Eds.)

Public Key Cryptography – PKC 2006

9th International Conference
on Theory and Practice of Public-Key Cryptography
New York, NY, USA, April 24-26, 2006
Proceedings

Springer

Volume Editors

Moti Yung
RSA Laboratories
and
Columbia University
Computer Science Department
1214 Amsterdam Avenue, New York, NY 10027, USA
E-mail: moti@cs.columbia.edu

Yevgeniy Dodis
New York University
Department of Computer Science
251 Mercer Street, New York, NY 10012, USA
E-mail: dodis@cs.nyu.edu

Aggelos Kiayias
University of Connecticut
Department of Computer Science and Engineering Storrs
CT 06269-2155, USA
E-mail: aggelos@cse.uconn.edu

Tal Malkin
Columbia University
Department of Computer Science
1214 Amsterdam Avenue, New York, NY 10027, USA
E-mail: tal@cs.columbia.edu

Library of Congress Control Number: 2006924182

CR Subject Classification (1998): E.3, F.2.1-2, C.2.0, K.4.4, K.6.5

LNCS Sublibrary: SL 4 – Security and Cryptology

ISSN 0302-9743
ISBN-10 3-540-33851-9 Springer Berlin Heidelberg New York
ISBN-13 978-3-540-33851-2 Springer Berlin Heidelberg New York

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 11745853 06/3142 5 4 3 2 1 0

Preface

The 9th International Conference on Theory and Practice of Public-Key Cryptography (PKC 2006) took place in New York City. PKC is the premier international conference dedicated to cryptology focusing on all aspects of public-key cryptography. The event is sponsored by the International Association of Cryptologic Research (IACR), and this year it was also sponsored by the Columbia University Computer Science Department as well as a number of sponsors from industry, among them: EADS and Morgan Stanley, which were golden sponsors, as well as Gemplus, NTT DoCoMo, Google, Microsoft and RSA Security, which were silver sponsors. We acknowledge the generous support of our industrial sponsors; their support was a major contributing factor to the success of this year's PKC.

PKC 2006 followed a series of very successful conferences that started in 1998 in Yokohama, Japan. Further meetings were held successively in Kamakura (Japan), Melbourne (Australia), Jeju Island (Korea), Paris (France), Miami (USA), Singapore and Les Diablerets (Switzerland). The conference became an IACR sponsored event (officially designated as an IACR workshop) in 2003 and has been sponsored by IACR continuously since then. The year 2006 found us all in New York City where the undertone of the conference was hummed in the relentless rhythm of the city that never sleeps.

This year's conference was the result of a collaborative effort by four of us: Moti Yung served as the conference and program chair. Moti orchestrated the whole project and led the Program Committee's efforts in the careful selection of the 34 papers that you will find in this volume. Yevgeniy Dodis served as the general and sponsorship chair, coordinating the sponsorship efforts. Aggelos Kiayias served as the publicity and publication chair, tending to the conference's publicity aspects, Web-site, submission and reviewing site as well as the editorial preparation of the present volume. Tal Malkin served as the general and local arrangements chair and was responsible for the very critical job of hosting PKC 2006 at Columbia University.

The selection of papers for this year's program was a delicate and laborious task. PKC 2006 had received a total of 124 submissions by the day of the submission deadline, November 15, 2005. Each paper was refereed by at least four committee members who were frequently assisted by external reviewers. The online discussions together with the reviews that were posted on the online reviewing site, if printed, would require more than 450 pages of densely printed text. The present proceedings volume contains the revised versions of the accepted extended abstracts as submitted by the authors after an alloted three week revision period based on the Program Committee's comments. The PKC 2006 Program Committee had the pleasure of according this year's *PKC Best Paper Award* to Daniel Bleichenbacher and Alexander May for their advancement

of RSA cryptanalysis in their paper entitled "New Attacks on RSA with Small Secret CRT-Exponents."

We would like to thank the Program Committee members as well as the external reviewers for their volunteered hard work invested in selecting the program. We thank the PKC Steering Committee for their support. We also wish to thank the following individuals: Shai Halevi for providing his Web-review and submission system to be used for the conference and for providing technical support; the submission and reviewing-site administrator David Walluck as well as the other students of the CryptoDRM Lab at the University of Connecticut for providing technical support; and Michael Locasto for Web-site administration support at Columbia University. Finally big thanks are due to all authors of submitted papers whose quality contributions make this research area a pleasure to work in, and made this conference a possibility.

March 2006

Moti Yung
Yevgeniy Dodos
Aggelos Kiayias
Tal Malkin

Organization

PKC Steering Committee

Ronald Cramer	CWI and Leiden University, The Netherlands
Yvo Desmedt	University College London, UK
Hideki Imai (Chair)	University of Tokyo, Japan
Kwangjo Kim	Information and Communications University, Korea
David Naccache	École Normale Supérieure, France
Tatsuaki Okamoto	NTT Labs, Japan
Jacques Stern	École Normale Supérieure, France
Moti Yung	RSA Laboratories and Columbia University, USA
Yuliang Zheng (Secretary)	University of North Carolina at Charlotte, USA

Organizing Committee

Conference and Program Chair	Moti Yung
General and Sponsorship Chair	Yevgeniy Dodis
Publicity and Publication Chair	Aggelos Kiayias
General and Local Arrangements Chair	Tal Malkin

Industrial Sponsors

EADS
Morgan Stanley
Gemplus
NTT DoCoMo
Google
Microsoft
RSA Security

Program Committee

Masayuki Abe	NTT Japan
Feng Bao	I2R, Singapore
Paulo S.L.M. Barreto	University of São Paulo, Brazil
Amos Beimel	Ben Gurion University, Israel
Xavier Boyen	Voltage Technology, USA
Serge Fehr	CWI, The Netherlands
Pierre-Alain Fouque	ENS Paris, France
Juan Garay	Bell Labs, USA
Rosario Gennaro	IBM Research, USA
Nick Howgrave-Graham	NTRU Cryptosystems, USA
Dong Hoon Lee	Korea University, Korea
Wenbo Mao	HP Labs, China
Alexander May	Paderborn University, Germany
David Naccache	ENS, France
Rafail Ostrovsky	UCLA, USA
Kenny Paterson	Royal Holloway, U. of London, UK
Giuseppe Persiano	University of Salerno, Italy
Benny Pinkas	Haifa University, Israel
Leonid Reyzin	Boston University, USA
Kazue Sako	NEC Japan
Jean-Sébastien Coron	University of Luxembourg
Alice Silverberg	U. C. Irvine, USA
Jessica Staddon	PARC, USA
Ron Steinfeld	Macquarie University, Australia
Edlyn Teske	University of Waterloo, Canada
Wen-Guey Tzeng	NCTU, Taiwan
Susanne Wetzel	Stevens Institute, USA
Yiqun Lisa Yin	Independent Consultant, USA
Adam Young	MITRE, USA
Moti Yung	RSA Labs and Columbia U., USA

External Reviewers

Michel Abdalla	Melissa Chase	Paolo D'Arco
Ben Adida	Lily Chen	Michael De Mare
Luis von Ahn	Liqun Chen	Breno de Medeiros
Giuseppe Ateniese	Benoît Chevallier-Mames	Nenad Dedić
Joonsang Baek	Chen-Kang Chu	Alex Dent
Paulo Barreto	Mathieu Ciet	Glenn Durfee
Daniel Brown	Scott Contini	Pooya Farshim
Jan Camenisch	Yang Cui	Marc Fischlin
Ran Canetti	Martin Döring	Jun Furukawa

Steven Galbraith
Clemente Galdi
David Galindo
Decio Gazzoni
Kristian Gjøsteen
Dorian Goldfeld
Philippe Golle
Vanessa Gratzer
Shai Halevi
Wei Han
Darrel Hankerson
Anwar Hasan
Javier Herranz
Jason Hinek
Dennis Hofheinz
Nicholas Hopper
Toshiyuki Isshiki
Stanislaw Jarecki
Markus Kaiser
Jonathan Katz
Tim Kerins
Eike Kiltz
Hugo Krawczyk
Sebastien Kunz-Jacques
Kaoru Kurosawa
Eonkyung Lee
Xiangxue Li
Benoît Libert
Shia-Yin Lin
Yehuda Lindell
Pierre Loidreau
Anna Lysyanskaya
John Malone-Lee
Gwenaëlle Martinet
Barbara Masucci
Bernd Meyer
Ulrike Meyer
Peter Montgomery
Kengo Mori
Volker Müller
James Muir
Chanathip Namprempre
Phong Nguyen
Jesper Buus Nielsen
Satoshi Obana
Daniel Page
Adriana Palacio
Josef Pieprzyk
David Pointcheval
Geraint Price
Karl Rubin
Tomas Sander
Oliver Schirokauer
Katja Schmidt-Samoa
Michael Scott
Hovav Shacham
Junji Shikata
Nigel Smart
Diana Smetters
Jerry Solinas
Rainer Steinwandt
Willy Susilo
Koutaro Suzuki
Isamu Teranishi
Nicholas Theriault
Richard M. Thomas
Xiaojian Tian
Ivan Visconti
Guilin Wang
Huaxiong Wang
Brent Waters
Ralf-Philipp Weinmann
Enav Weinreb
Kai Wirt
Duncan Wong
David Woodruff
Rui Zhang
Yunlei Zhao
Sheng Zhong
Huafei Zhu
Sebastien Zimmer

Table of Contents

Cryptanalysis and Protocol Weaknesses

Distributed Crypto-computing

Encryption Methods

Cryptographic Hash and Applications

Number Theory Algorithms

Pairing-Based Cryptography

Cryptosystems Design and Analysis

Signature and Identification

Authentication and Key Establishment

Multi-party Computation

PKI Techniques

New Attacks on RSA with Small Secret CRT-Exponents

Daniel Bleichenbacher[1] and Alexander May[2]

[1] daniel_bleichenbacher@yahoo.com
[2] Department of Computer Science,
TU Darmstadt,
64289 Darmstadt, Germany
may@informatik.tu-darmstadt.de

Abstract. It is well-known that there is an efficient method for decrypting/signing with RSA when the secret exponent d is small modulo $p-1$ and $q-1$. We call such an exponent d a small CRT-exponent. It is one of the major open problems in attacking RSA whether there exists a polynomial time attack for small CRT-exponents, i.e. a result that can be considered as an equivalent to the Wiener and Boneh-Durfee bound for small d. At Crypto 2002, May presented a partial solution in the case of an RSA modulus $N = pq$ with unbalanced prime factors p and q. Based on Coppersmith's method, he showed that there is a polynomial time attack provided that $q < N^{0.382}$. We will improve this bound to $q < N^{0.468}$. Thus, our result comes close to the desired normal RSA case with balanced prime factors. We also present a second result for balanced RSA primes in the case that the public exponent e is significantly smaller than N. More precisely, we show that there is a polynomial time attack if $d_p, d_q \leq \min\{(N/e)^{\frac{2}{5}}, N^{\frac{1}{4}}\}$. The method can be used to attack two fast RSA variants recently proposed by Galbraith, Heneghan, McKee, and by Sun, Wu.

Keywords: RSA, small exponents, lattices, Coppersmith's method.

1 Introduction

Let $N = pq$ be an RSA modulus. The public exponent e and the secret exponent d satisfy the equation $ed = 1 \bmod \phi(N)$, where $\phi(N) = (p-1)(q-1)$ is Euler's totient function. The main drawback of RSA is its efficiency. A normal RSA decryption/signature generation requires time $\Theta(\log d \log^2 N)$.

Therefore, one might be tempted to use small secret exponents to speed up the decryption/signing process. Unfortunately, Wiener[14] showed in 1991 that if $d < N^{\frac{1}{4}}$ then the factorization of N can be found in polynomial time using only the public information (N, e). In 1999, Boneh and Durfee[1] improved the bound to $d < N^{0.292}$. One can view these bounds as a benchmark for attacking RSA (see also the comments in the STORK-roadmap [11]). Thus, improving these bounds is a major research issue in public key cryptanalysis.

M. Yung et al. (Eds.): PKC 2006, LNCS 3958, pp. 1–13, 2006.

It remains an important open problem whether there is an analogue of these attacks in the case of small secret CRT-exponents d, i.e. exponents d such that $d_p = d \bmod p-1$ and $d_q = d \bmod q-1$ both are small. For the construction of such small CRT-exponents with a given bit-size, we refer to Boneh, Shacham [2]. Notice that small CRT-exponents enable to efficiently raise to the d^{th} power modulo p and modulo q, respectively. The results are then combined using the Chinese Remainder Theorem (CRT), yielding a solution modulo N. For the normal RSA case with balanced prime factors p, q and full-size e, the best algorithm that is currently known has time and space complexity $\mathcal{O}(\sqrt{\min\{d_p, d_q\}})$.

At Crypto 2002, May[9] presented two polynomial time attacks for the case of imbalanced prime factors p and q. His attacks are based on Coppersmith's method for finding small roots of modular equations. His first attack is rigorous and solves a polynomial equation modulo p. This attack works whenever $q < N^{0.382}$. May's second attack is a heuristic method that is based on a resultant heuristic for Coppersmith's method in the multivariate modular case. This attack works whenever $q < N^{\frac{3}{8}}$.

Let us have a look at the size of d_p that can be attacked by May's approaches as a function of the size of q. In Fig. 1 we present both of these sizes as a fraction of the bits of N.

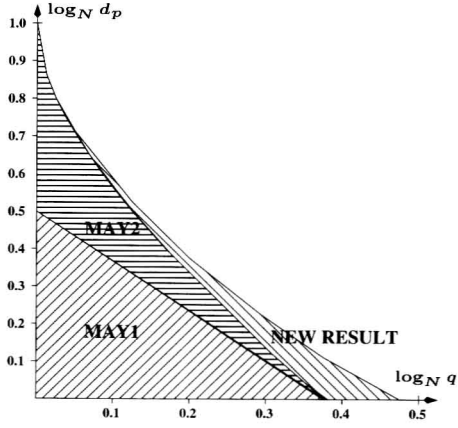


Fig. 1. The attacks of [9] in comparison with the new approach

A close look at the functions presented in Fig. 1 reveals that there is a tiny region where May's first method is better than his second one. Hence, it is a natural question to ask whether there is a unifying method that covers both regions of the key space.

In this work, we present a new attack that solves this question. In Fig. 1, we give the improved sizes of d_p that can be attacked by our new approach as a function of q. One can see that the new attack works up to $q < N^{0.468}$ and covers the key spaces of the previously known attacks. Thus, we are able to improve the benchmark for attacking CRT-RSA up to almost balanced prime factors.

Interestingly, we get the improvement by making just a small twist to May's second method. He solved a polynomial equation $f(x,y) = x(N-y)+N$ with a small root (x_0, q) modulo e. In this work, we make additional use of the fact that the desired small solution contains the prime factor q. Namely, we introduce a new variable z for the prime factor p and further use the equation $yz = N$.

Our new approach immediately raises an interesting open problem: The polynomial $f(x,y) = x(N-y)+N$ used here is very similar to the polynomial $g(x,y) = x(N+1-y)+1$ that is used in the Boneh-Durfee approach to show the currently best bound of $d < N^{0.292}$ for attacking small secret exponent RSA. Notice that both polynomials $f(x,y)$ and $g(x,y)$ have the same set of monomials, i.e. the same Newton polytope. In contrast to $f(x,y)$, the polynomial $g(x,y)$ has a small root $(x_0', p+q)$. It is a natural question to ask whether one can improve the Boneh-Durfee bound by using the fact that this root contains the sum of the prime factors p and q.

We should point out that our new attack works for small d_p and arbitrary sizes of d_q. It is an open problem how to make use of a small parameter d_q in this attack. Maybe a clever use of d_q could already help to push the bound from $q < N^{0.468}$ to the desired normal RSA-case of balanced prime factors.

As a second result, we are able to give a different lattice-based attack on RSA with small CRT-exponents that works in the case of balanced prime factors, but with the restriction that the parameter e is significantly smaller than N. This second attack makes use of small d_p and small d_q. The result is achieved by multiplying the equations $ed_p = 1 \bmod p-1$ and $ed_q = 1 \bmod q-1$ and then using a linearization technique. Our attack works whenever $d_p, d_q < \min\{\frac{1}{4}(N/e)^{\frac{2}{5}}, \frac{1}{3}N^{\frac{1}{4}}\}$, i.e., up to roughly half of the bit-size of p, q for sufficiently small e. The attack requires to find a shortest vector in a 3-dimensional lattice and is extremely fast. As an application of our second result, we show that recently proposed RSA variants by Galbraith, Heneghan and McKee [5] and Sun, Wu [12] are vulnerable to the new attack.

We would like to point out that both new attacks are heuristic methods. We implemented both methods and provide several experiments that show that the heuristics work well in practice.

The organization of the paper is as follows. In Section 2, we state some lattice basis theory and in Section 3 we review May's result. In Section 4, we show how to achieve the improved bound of $q < N^{0.468}$. In Section 5, we present our second attack for $d_p, d_q < \min\{\frac{1}{4}(N/e)^{\frac{2}{5}}, \frac{1}{3}N^{\frac{1}{4}}\}$ and show how this attack breaks recently proposed fast RSA variants. We conclude our work by providing some experimental results for our attacks in Section 6.

2 Lattice Theory and Definitions

Let $b_1, \ldots, b_n \in \mathbb{Z}_n$ be linearly independent. Then these vectors span a lattice of dimension n defined by

$$L := \Big\{ x \in \mathbb{Z}_n \mid x = \sum_{i=1}^{n} a_i b_i, \text{ where } a_i \in \mathbb{Z} \Big\}.$$

We call the set $B = \{b_1, \ldots, b_n\}$ a basis of L. There are infinitely many bases. A basis can be transformed into another basis by a unimodular transformation, i.e. a multiplication by a matrix with determinant ± 1. Therefore, the absolute value of the determinant of a basis matrix is an invariant of the lattice L. We call this invariant the determinant of L, which is denoted by $\det(L) = |\det(B)|$.

A famous theorem of Minkowski gives an upper bound for the length of a shortest vector v in a lattice in terms of a function of the determinant and the dimension n:

$$\|v\| \leq \sqrt{n} \dim(L)^n.$$

In lattices with fixed dimension, a shortest vector can be found in polynomial time. In arbitrary dimension, approximations of a shortest vector can be obtained in polynomial time by applying the well-known L^3 basis reduction algorithm of Lenstra, Lenstra and Lovász [8].

Theorem 1 (Lenstra, Lenstra, Lovász). *Let $B = \{b_1, \ldots, b_n\}$ be a basis. On input B, the L^3-algorithm outputs another basis $\{v_1, \ldots, v_n\}$ with*

$$\|v_1\| \leq \|v_2\| \leq 2^{\frac{n}{4}} \det(L)^{\frac{1}{n-1}},$$

in time polynomial in n and in the bit-size of the entries in B.

Let $f(x, y) = \sum_{i,j} a_{i,j} x^i y^j \in \mathbb{Z}[x, y]$. We define the norm of f by the Euclidean norm of its coefficient vector: $\|f\|^2 = \sum_{i,j} a_{i,j}^2$.

Based on the L^3-algorithm, Coppersmith [4] presented in 1996 a method that finds small solutions to modular polynomial equations. The idea behind Coppersmith's method is to construct a polynomial which has the desired small root over the integers. Howgrave-Graham [7] in turn formulated a useful condition how to find such a polynomial in terms of the norm of a polynomial.

Theorem 2 (Howgrave-Graham). *Let $f(x_1, \ldots, x_k)$ be a polynomial in k variables with n monomials. Furthermore, let m be a positive integer. Suppose that*

(1) $f(r_1, \ldots, r_k) = 0 \bmod b^m$ where $|r_i| \leq X_i$, $i = 1, \ldots, k$ and
(2) $\|f(x_1 X_1, \ldots, x_k X_k)\| < \frac{b^m}{\sqrt{n}}$.

Then $f(r_1, \ldots, r_k) = 0$ holds over the integers.

3 Revisiting May's Attack on Small CRT-Exponents

Throughout this paper, we assume that $e < \phi(N)$. Furthermore, we assume that $q \leq N^\beta$ for some $\beta \leq \frac{1}{2}$. We start by writing the RSA equation $ed_p = 1 \bmod (p-1)$ in the form

$$ed_p = 1 + k(p-1),$$

for some unknown $k \in \mathbb{N}$. Rewriting terms yields

$$ed_p = (k-1)(p-1) + p. \tag{1}$$

A multiplication with q leaves us with the equation

$$ed_pq = (k-1)(N-q) + N.$$

We assign the variables x and y to the unknown parameters on the right-hand side and obtain a bivariate polynomial

$$f(x,y) = x(N-y) + N, \tag{2}$$

with the root $(x_0, y_0) = (k-1, q)$ modulo e. In order to bound the term $k-1$, we observe that by Eq. (1)

$$k - 1 = \frac{ed_p - p}{p-1} < \frac{e}{p-1}\, d_p < (q-1)X < N^{\beta}X.$$

Let us fix a parameter m. We define the following collection of polynomials that all have the root (x_0, y_0) modulo e^m:

$$\begin{aligned} g_{i,j}(x,y) &= e^{m-i}x^j f^i(x,y) \quad \text{for } i = 0,\ldots,m;\ j = 0,\ldots,m-i \quad \text{and} \\ h_{i,j}(x,y) &= e^{m-i}y^j f^i(x,y) \quad \text{for } i = 0,\ldots,m;\ j = 1,\ldots,t. \end{aligned} \tag{3}$$

The parameter t has to be optimized as a function of m.

Since each polynomial of the collection has the small root (x_0, y_0) modulo e, every linear combination of these polynomials also has the same root modulo e.

A lower triangular lattice basis can be build from the coefficient vectors of $g_{i,j}(xX, yY)$ and $h_{i,j}(xX, yY)$. According to Howgrave-Graham's theorem (Theorem 2), linear combinations of the vectors with sufficiently small norm give raise to bivariate polynomials that have the root (x_0, y_0) not only modulo e but over the integers. Having two polynomials $f_1(x,y)$ and $f_2(x,y)$ with this root over the integers, one can take resultants in order to extract the desired root. However, the last step is a heuristic, since the resultant computation may fail due to a non-trivial gcd of f_1 and f_2.

In [9], it was shown that with the optimal choice of parameters one obtains an attack that works up to $q < N^{\frac{3}{8}}$, see also Fig. 1 in Section 1.

4 An Approach That Works for $q < N^{0.468}$

Our improvement of the algorithm presented in Section 3 is based on the observation that in Eq. (2) the polynomial $f(x,y)$ contains in its small root $(x_0, y_0) = (d_p, q)$ modulo e the prime factor q. We will use the fact that we do not deal with just an arbitrary small root but that q is already determined by N.

Let us introduce a new variable z for p. We multiply the polynomial $f(x,y)$ by a power z^s for some s that has to be optimized. Additionally, we can replace every occurence of the monomial yz by N. Let us look at the following new collection of trivariate polynomials that we obtain by multiplying the former collection from (3) with z^s:

$$\begin{aligned} g'_{i,j}(x,y,z) &= e^{m-i}x^j z^s f^i(x,y) \quad \text{for } i = 0,\ldots,m;\ j = 0,\ldots,m-i \ \text{ and} \\ h'_{i,j}(x,y,z) &= e^{m-i}y^j z^s f^i(x,y) \quad \text{for } i = 0,\ldots,m;\ j = 1,\ldots,t. \end{aligned}$$