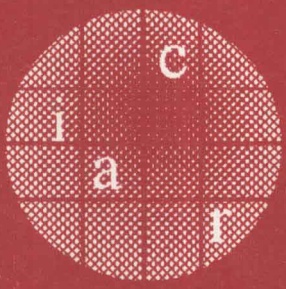
Serge Vaudenay (Ed.)

LNCS 3386

Public Key Cryptography – PKC 2005

8th International Workshop
on Theory and Practice in Public Key Cryptography
Les Diablerets, Switzerland, January 2005, Proceedings



Springer

Serge Vaudenay (Ed.)

Public Key Cryptography – PKC 2005

8th International Workshop
on Theory and Practice in Public Key Cryptography
Les Diablerets, Switzerland, January 23-26, 2005
Proceedings

Springer

Volume Editor

Serge Vaudenay
Ecole Polytechnique Fédérale de Lausanne
School of Computer and Communication Sciences
Security and Cryptography Laboratory
1015 Lausanne, Switzerland
E-mail: serge.vaudenay@epfl.ch

Library of Congress Control Number: 2004117654

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

ISSN 0302-9743
ISBN 3-540-24454-9 Springer Berlin Heidelberg New York

Typesetting: Camera-ready by author, data conversion by Olgun Computergrafik
Printed on acid-free paper SPIN: 11376477 06/3142 5 4 3 2 1 0

Preface

The 2005 issue of the International Workshop on Practice and Theory in Public Key Cryptography (PKC 2005) was held in Les Diablerets, Switzerland during January 23–26, 2005. It followed a series of successful PKC workshops which started in 1998 in Pacifico Yokohama, Japan. Previous workshops were successively held in Kamakura (Japan), Melbourne (Australia), Cheju Island (South Korea), Paris (France), Miami (USA), and Singapore. Since 2003, PKC has been sponsored by the International Association for Cryptologic Research (IACR). As in previous years, PKC 2005 was one of the major meeting points of worldwide research experts in public-key cryptography. I had the honor to co-chair the workshop together with Jean Monnerat and to head the program committee. Inspired by the fact that the RSA cryptosystem was invented on ski lifts, we decided that the best place for PKC was at a ski resort. Jean Monnerat and I hope that this workshop in a relaxed atmosphere will lead us to 25 more years of research fun.

PKC 2005 collected 126 submissions on August 26, 2004. This is a record number. The program committee carried out a thorough review process. In total, 413 review reports were written by renowned experts, program committee members as well as external referees. Online discussions led to 313 additional discussion messages and 238 emails. The review process was run using email and the Webreview software by Wim Moreau and Joris Claessens. Every submitted paper received at least 3 review reports. We selected 28 papers for publication on October 28, 2004. Authors were then given a chance to revise their submission over the following two weeks. This proceedings includes all the revised papers. Due to time constraints the revised versions could not be reviewed again.

Double submissions, where authors send the same or almost the same paper to multiple conferences that explicitly prohibit such practices, is an increasing problem for the research community worldwide. I do regret that we had to reject 6 such submissions without consideration of their scientific merits. I would like to thank the program chairs of other events who collaborated in this effort, in particular Anne Canteaut, Joe Kilian, Choonsik Park, and Seongtaek Chee.

With the approval of the IACR Board of Directors, PKC 2005 delivered the *PKC Best Paper Award* for the first time. The purpose of the award is to formally acknowledge authors of outstanding papers and to recognize excellence in the cryptographic research fields. Committee members were invited to nominate papers for this award. A poll then yielded a clear majority. This year, we were pleased to deliver the PKC Best Paper Award to Yevgeniy Dodis and Aleksandr Yampolskiy for their brilliant paper "A Verifiable Random Function with Short Proofs and Keys." This paper concluded the workshop.

I would like to thank Jean Monnerat who accepted the responsibility to co-chair the PKC 2005 workshop. I would like to thank the PKC steering committee for their support and trust. The program committee and external reviewers

worked extremely hard under a tight schedule. I heartily thank them for this volunteer work. Acknowledgments also go to the authors of submitted papers and the speakers who made the real meat of PKC 2005. I am grateful to Antoine Junod and Julien Brouchier for their support with the Webreview software. I also thank my assistants Pascal Junod, Thomas Baignères, Yi Lu, Gildas Avoine, and Matthieu Finiasz for their help in the PKC 2005 organization. Special thanks to Martine Corval who orchestrated the PKC 2005 logistics. We appreciate the kind help of Christian Cachin in the advertising and registration process. We also owe our gratitude to Kevin McCurley for spending a substantial amount of his valuable time to set up the online registration website. We thank our generous sponsors Gemplus and personally David Naccache, and HP Labs and personally Wenbo Mao, for supporting PKC 2005. We also thank EPFL and IACR for sponsoring this event. It was a very pleasant experience. Crypto is fun!

Lausanne, November 19, 2004 Serge Vaudenay

PKC Steering Committee (as of November 2004)

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

Organizing Committee

General Co-chairs	Jean Monnerat
	Serge Vaudenay
Local Organization	Martine Corval
Assistants	Gildas Avoine
	Thomas Baignères
	Matthieu Finiasz
	Pascal Junod
	Yi Lu

Program Committee

Carlisle Adams	University of Ottawa, Canada
Feng Bao	Institute for Infocomm Research, Singapore
Yvo Desmedt	University College London, UK
Juan Garay	Bell Labs – Lucent Technologies, USA
Martin Hirt	ETH Zurich, Switzerland
Kwangjo Kim	Information and Communications University, South Korea
Kaoru Kurosawa	Ibaraki University, Japan
Anna Lysyanskaya	Brown University, USA
Wenbo Mao	HP Labs Bristol, UK
David Naccache	Gemplus, France and Royal Holloway, University of London, UK
Kaisa Nyberg	Nokia, Finland
Tatsuaki Okamoto	NTT Labs, Japan
Josef Pieprzyk	Macquarie University, Australia
David Pointcheval	CNRS-ENS, France
Reihaneh Safavi-Naini	University of Wollongong, Australia
Kazue Sako	NEC, Japan
Claus-Peter Schnorr	University of Frankfurt am Main, Germany
Berry Schoenmakers	Technische Universiteit Eindhoven, The Netherlands
Nigel Smart	University of Bristol, UK
Edlyn Teske	University of Waterloo, Canada
Serge Vaudenay	EPFL, Switzerland
Moti Yung	University of Columbia, USA
Yuliang Zheng	University of North Carolina at Charlotte, USA

External Reviewers

Masayuki Abe
Ben Adida
Gildas Avoine
Joonsang Baek
Thomas Baignères
Mihir Bellare
Daniel Bleichenbacher
Colin Boyd
Emmanuel Bresson
Eric Brier
Duncan Buell
Srdjan Capkun
Dario Catalano
Liqun Chen
Benoît Chevallier-Mames
Jean-Sébastien Coron
Ronald Cramer
Jean-François Dhem
Christophe Doche
Atsushi Fujioka
Eiichiro Fujisaki
Jun Furukawa
Steven Galbraith
Pierrick Gaudry
Louis Granboulan
Rob Granger
Jaime Gutierrez
Darrel Hankerson
Anwar Hasan
Alex Healy
Jason Hinek
Susan Hohenberger
Thomas Holenstein
Heng Swee Huay
Toshiyuki Isshiki
Kouichi Itoh
Michael Jacobson
Marc Joye
Pascal Junod
Charanjit Jutla
Jonathan Katz
Tetsutaro Kobayashi
Robert König
Byoungcheon Lee
Arjen Lenstra
Moses Liskov
Javier Lopez
Yi Lu
John Malone-Lee
Toshihiko Matsuo
Noel McCullagh
Anton Mityagin
Atsuko Miyaji
Jean Monnerat
Waka Nagao
Phong Q. Nguyễn
Satoshi Obana
Takeshi Okamoto
Katsuyuki Okeya
Dan Page
Pascal Paillier
Jacques Patarin
Kenneth Paterson
Chris Peikert
Krzysztof Pietrzak
Bartosz Przydatek
Tal Rabin
Peter Roelse
Hans-Georg Rueck
Ryuichi Sakai
Takakazu Satoh
Katja Schmidt-Samoa
Michael Scott
Hovav Shacham
Andrey Sidorenko
Johan Sjödin
Martijn Stam
Andreas Stein
Ron Steinfeld
Makoto Sugita
Willy Susilo
Koutarou Suzuki
Tsuyoshi Takagi
Keisuke Tanaka
Isamu Teranishi
Jacques Traoré
Shigenori Uchiyama
Frederik Vercauteren
Duong Quang Viet
Jorge L. Villar
Guilin Wang
Huaxiong Wang
Stephen Weis
Claire Whelan
Christopher Wolf
Go Yamamoto
Chung-Huang Yang
Danfeng Yao
Sung-Ming Yen
Huafei Zhu

Table of Contents

Cryptanalysis

Key Establishment

Optimization

Building Blocks

RSA Cryptography

Multivariate Asymmetric Cryptography

Signature Schemes

Identity-Based Cryptography

Best Paper Award

A New Related Message Attack on RSA

Oded Yacobi[1] and Yacov Yacobi[2]

[1] Department of Mathematics, University of California San Diego, 9500 Gilman Drive, La Jolla, CA 92093, USA
oyacobi@math.ucsd.edu
[2] Microsoft Research, One Microsoft Way, Redmond, WA 98052, USA
yacov@microsoft.com

Abstract. Coppersmith, Franklin, Patarin, and Reiter show that given two RSA cryptograms $x^e \bmod N$ and $(ax+b)^e \bmod N$ for known constants $a, b \in \mathbb{Z}_N$, one can compute x in $O(e \log^2 e)$ $\mathbb{Z}_N$-operations with some positive error probability. We show that given e cryptograms $c_i \equiv (a_i x + b_i)^e \bmod N$, $i = 0, 1, ...e-1$, for any known constants $a_i, b_i \in \mathbb{Z}_N$, one can deterministically compute x in $O(e)$ $\mathbb{Z}_N$-operations that depend on the cryptograms, after a pre-processing that depends only on the constants. The complexity of the pre-processing is $O(e \log^2 e)$ $\mathbb{Z}_N$-operations, and can be amortized over many instances. We also consider a special case where the overall cost of the attack is $O(e)$ $\mathbb{Z}_N$-operations. Our tools are borrowed from numerical-analysis and adapted to handle formal polynomials over finite-rings. To the best of our knowledge their use in cryptanalysis is novel.

1 Introduction

Messages with known relations may occur for example if an attacker pretends to be the recipient in a protocol that doesn't authenticate the recipient, and in addition the message is composed of the content concatenated with a serial number. In that case the attacker can claim that she didn't receive the transmission properly and ask that it be sent again. The next transmission will have the same content as the original but an incremented serial number. If the increment is known we have a known relation. Other examples appear in [4].

Related message attacks can be avoided all together if before RSA-encryption the message M is transformed using e.g. the OAEP function ([3]; There are other methods and some issues are not settled yet, see [5]). This transformation destroys the relations between messages and increases the message length.

Nevertheless it is useful to know the ramifications in case for some reason one chooses not to use OAEP or similar methods (even though it is highly recommended). For example RFID tags may pose tough engineering challenges of creating very compact cryptosystems, and the trade-off must be known precisely.

In [4] it was shown that given two RSA cryptograms $x^e \bmod N$, and $(ax+b)^e \bmod N$ for any known constants $a, b \in \mathbb{Z}_N$ one can compute x in $O(e \log^2 e)$ $\mathbb{Z}_N$-operations with some small error probability.

S. Vaudenay (Ed.): PKC 2005, LNCS 3386, pp. 1–8, 2005.

We show that given e cryptograms $c_i \equiv (a_i x + b_i)^e \bmod N$, $i = 0, 1, ...e-1$, for any known constants $a_i, b_i \in \mathbb{Z}_N$, one can deterministically compute x in $O(e)$ $\mathbb{Z}_N$-operations, after doing $O(e \log^2 e)$ pre-computations that depend only on the known constants. The descriptions of the protocol and the attack determine the values of these constants. For example the attack described at the beginning of this section has for all i $a_i = b_i = 1$. The cost of the pre-computations can be amortized over many instances of the problem.

Our problem could be solved by using the Newton expansion of $c_i \equiv (a_i x + b_i)^e \bmod N$, renaming $z_j = x^j$ and using linear algebra to find z_1. However, our method is more efficient.

We also show that in the special case where $c_i \equiv (ax + b \cdot i)^e \bmod N$, $i = 0, 1, ...e-1$, for any known constants $a, b \in \mathbb{Z}_N$, where $\gcd(a, N) = \gcd(b, N) = \gcd(e!, N) = 1$, one can deterministically compute x in overall $O(e)$ $\mathbb{Z}_N$-operations using

$$x \equiv a^{-1} b [(b^e e!)^{-1} \sum_{i=0}^{e-1} \binom{e-1}{i} \cdot c_i \cdot (-1)^{e-1+i} - \frac{e-1}{2}] \bmod N$$

If any of the above gcd conditions do not hold then the system is already broken.

It remains an open problem whether the new approach can improve the general case of implicit linear dependence, i.e., suppose for known constants a_i, $i = 0, 1, 2, ...k$, there is a known relation $\sum_{i=1}^{k} a_i x_i = a_0$ among messages $x_1, x_2, ...x_k$. The current complexity of attacking this problem is $O(e^{k/2} k^2)$ [4].

Our major attack-tools are divided-differences and finite-differences. These tools are borrowed from numerical-analysis, and adapted to handle formal polynomials over finite-rings. To the best of our knowledge their use in cryptanalysis is novel.

For a survey of the work on breaking RSA see [2].

2 Main Result

2.1 Divided Differences

We borrow the concept of *divided-differences* from numerical analysis and adapt it to handle formal polynomials over finite rings. This will allow us to extract the message from a string of e cryptograms whose underlying messages are linearly related. We specialize our definitions to the ring of integers modulo N, a product of two primes (the "RSA ring"). All the congruences in this paper are taken mudulo N.

Definition 1. *Let h be a polynomial defined over the ring of integers modulo N, and let $x_0, x_1, ...x_n$ be distinct elements of the ring such that $(x_0 - x_i)^{-1} \bmod N$ exist for $i = 0, 1, ...n$. The n^{th} divided-difference of h relative to these elements is defined as follows:*

$$[x_i] \equiv h(x_i),$$
$$[x_0, x_1] \equiv \frac{[x_0] - [x_1]}{x_0 - x_1},$$
$$[x_0, x_1, ...x_n] \equiv \frac{[x_0, x_1, ...x_{n-1}] - [x_1, x_2, ...x_n]}{x_0 - x_n}.$$

Let x be an indeterminate variable, and for $i = 0, 1, ...n$, let $x_i \equiv x + b_i$ for some known constants b_i (these are the general explicit linear relations that we assume later). We can now view the above divided differences as univariate polynomials in x defined over $\mathbb{Z}_N$.

The following lemma is true for the divided difference of any polynomial $\bmod N$, but for our purposes it is enough to prove it for the RSA polynomial $x^e \bmod N$. Related results are stated in [8]. Before beginning the proof we introduce some notation borrowed from [7]. Let $\pi_k(y) \equiv \prod_{i=0}^{k}(y - x_i)$. Then taking the derivative of π_k with respect to y we have for $i \leq k$

$$\pi'_k(x_i) \equiv \prod_{\substack{0 \leq j \leq k \\ j \neq i}} (x_i - x_j)$$

By induction on k the following equality easily follows

$$[x_0, ..., x_k] \equiv \sum_{i=0}^{k} \frac{h(x_i)}{\pi'_k(x_i)} \tag{1}$$

Let $C_t(p)$ denote the t_{th} coefficient of the polynomial p, starting from the leading coefficients (the coefficients of the highest powers). We use $C_t[x_0, ..x_k]$ as a shorthand for $C_t([x_0, ..x_k])$.

Lemma 1. *Let $[x_0, ..., x_n]$ be the n^{th} divided difference relative to the RSA polynomial $h(x) \equiv x^e \bmod N$, and let $x_0, x_1, ...x_n$ be distinct elements of the ring such that $(x_0 - x_i)^{-1} \bmod N$ exist for $i = 0, 1, ...n$. Then (i) for $0 \leq n \leq e$, if $\binom{e}{e-n} \neq 0 \bmod N$ then $\deg[x_0, ..., x_n] = e - n$. (ii) $C_{e-n}[x_0, x_1, .., x_n] \equiv \binom{e}{e-n}$ (an important special case is $C_1[x_0, x_1, .., x_{e-1}] \equiv e \bmod N$).*

Comment: In practice the condition in claim (i) always holds, since $e << N$.

Proof. The claim is trivial for $n = 0$. For $n \geq 1$ we prove the equivalent proposition that $C_t\ [x_0, ..., x_n] = 0$ for $t = e, e-1, ..., e-n+1$ and $C_{e-n}[x_0, ..., x_n]$ is independent of the b_i and is not congruent to 0. We use the notations $1/b$ and b^{-1} interchangeably. We induct on n. When $n = 1$

$$[x_0, x_1] \equiv \frac{(x + b_0)^e - (x + b_1)^e}{b_0 - b_1} \equiv \frac{\sum_{i=0}^{e} \binom{e}{i} x^i [b_0^{e-i} - b_1^{e-i}]}{b_0 - b_1}$$

Note that by our assumption $(b_0 - b_1)^{-1} \bmod N$ exist. So $C_e[x_0, x_1] \equiv 0$ and $C_{e-1}[x_0, x_1] \equiv e$ and indeed our claim is true for $n = 1$. For the inductive hypothesis let $n = k - 1$ and assume that $C_t\ [x_0, ..., x_{k-1}] \equiv 0$ for $t = e, e -$

$1, ..., e-(k-1)+1$ and $C_{e-(k-1)}[x_0, ..., x_{k-1}]$ is independent of the b_i and is not congruent to 0. We want to show that when $n = k$, $C_t[x_0, ..., x_k] \equiv 0$ for $t = e, e-1, ..., e-k+1$ and $C_{e-k}[x_0, ..., x_k]$ is independent of the b_i and is not congruent to 0.

The fact that $C_t\ [x_0, ..., x_k] \equiv 0$ for $t = e, e-1, ..., e-k+1$ follows immediately from the inductive hypothesis and Definition 1. It takes a little more work to show that $C_{e-k}[x_0, ..., x_k]$ is independent of the b_i.

Using (1):

$$[x_0, x_1, ..., x_k] \equiv \sum_{i=0}^{k} \frac{(x+b_i)^e}{\pi_k'(x_i)} \equiv \sum_{j=0}^{e} \binom{e}{j} x^j [\frac{b_0^{e-j}}{\pi_k'(x_0)} + \frac{b_1^{e-j}}{\pi_k'(x_1)} + ... + \frac{b_k^{e-j}}{\pi_k'(x_k)}]$$

We want to show that $C_{e-k}[x_0, x_1, ..., x_k]$ is independent of the b_i.

$$C_{e-k}[x_0, x_1, .., x_k] \equiv \binom{e}{e-k} [\frac{b_0^k}{\pi_k'(x_0)} + \frac{b_1^k}{\pi_k'(x_1)} + ... + \frac{b_k^k}{\pi_k'(x_k)}] \tag{2}$$

So now it is sufficient to show that

$$(-1)^0 \frac{b_0^k}{(b_0-b_1)\cdots(b_0-b_k)} + ... + (-1)^k \frac{b_k^k}{(b_0-b_k)\cdots(b_{k-1}-b_k)} \tag{3}$$

is independent of the b_i.

We first multiply (3) by the necessary terms to get a common denominator. We introduce some compact notation that will simplify the process. For a given set of constants $b_0, b_1, ...b_k$ define

$$\begin{aligned} \delta(h,i) &\equiv (b_h - b_i) \\ \delta(h,i,j) &\equiv (b_h - b_i)(b_h - b_j)\delta(i,j) \\ &\vdots \\ \delta(i_0, ..., i_k) &\equiv (b_{i_0} - b_{i_1})(b_{i_0} - b_{i_2}) \cdots (b_{i_0} - b_{i_k})\delta(i_1, ..., i_k) \end{aligned}$$

Similarly we can also define $\delta_j \equiv \delta(0, 1, ..., \bar{j}, ..., k)$ where the bar denotes that the index is missing (so if $k = 4$ then $\delta_3 = \delta(0, 1, 2, 4,)$). Then (3) becomes:

$$\frac{b_0^k\delta_0 - b_1^k\delta_1 + \cdots + (-1)^k b_k^k \delta_k}{\delta(0, 1, ..., k)} \tag{4}$$

We want to show that (4) is independent of the b_i. In fact it equals 1. To see this consider the Vandermonde matrix:

$$V \equiv \begin{bmatrix} 1 & b_0 & b_0^2 & \cdots & b_0^k \\ 1 & b_1 & b_1^2 & \cdots & b_1^k \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & b_k & b_k^2 & \cdots & b_k^k \end{bmatrix}$$

We conclude from (2) that $C_{e-k}[x_0, x_1, .., x_k] \equiv \binom{e}{e-k}$, which is certainly independent of the b_i. This also implies that $C_{e-k}[x_0, x_1, .., x_k]$ is not congruent to 0 when $k \leq e$. By induction we are done.

2.2 Related-Messages Attack

Here we consider the general case where for $i = 0, 1, ...e-1$, $x_i \equiv a_i x + b_i \bmod N$. $N = pq$ is an RSA composite (p and q are large primes, with some additional restrictions which are irrelevant in the current discussion), and the constants a_i, b_i are known. Of course it is sufficient to consider just the case where $x_i \equiv x + b_i$. We now show how to deterministically compute x in $O(e)$ $\mathbb{Z}_N$-operations after some pre-computation that depends only on the known constants. If the constants b_i hold for many unknown values of cryptograms x^e then the cost of pre-computations can be amortized and discarded. We show that the cost of the additional computations that depend on the value of x is $O(e)$.

Specifically, $\pi'_n(x_k)$ is independent of y and of x, hence for all k these coefficients can be computed in advance. In that case the cost of computing $[x_0, x_1, ...x_{e-1}] \equiv ux + v \equiv w(x)$ is $O(e)$.

For each particular value x we know how to compute the value $w(x)$ without knowing x using Lemma 1 and Formula (1). More explicitly, Let $c_i \equiv (x + b_i)^e \bmod N$, $i = 0, 1, 2, ...e - 1$, be the given cryptograms, whose underlying messages are linearly related, and let $\pi'_{e-1}(x_k) \equiv \prod_{\substack{i=0 \\ i \neq k}}^{e-1} (b_k - b_i)$. We use p_k as a shorthand for $\pi'_{e-1}(x_k)$. Then

$$w(x) \equiv \sum_{k=0}^{e-1} \frac{[x_k]}{\pi'_{e-1}(x_k)} \equiv \sum_{k=0}^{e-1} \frac{c_k}{p_k}.$$

Here we assume that the inverses $(b_k - b_i)^{-1} \bmod N$ exist. Note that if for some k, i this isn't true then we can factor the RSA-modulus N, by computing $\gcd(N, (b_k - b_i))$.

From Lemma 1 (ii) we know that $u = e$. Note also that $w(0) \equiv v \equiv \sum_{k=0}^{e-1} b_k^e \cdot p_k^{-1} \bmod N$, and we can compute it in the pre-computation phase (before intercepting the cryptograms). So we can find $x \equiv (w(x) - v)e^{-1} \bmod N$.

The following algorithm summarizes the above discussion:

Algorithm 1

Given cryptograms $c_i \equiv (x+b_i)^e \bmod N$, $i = 0, 1, 2, ...e-1$, with known constants b_i, find x.

Method:

1. Pre computation:
   For $k = 0, ...e-1$, compute $p_k^{-1} \equiv \prod_{\substack{i=0 \\ i \neq k}}^{e-1} (b_k - b_i)^{-1}$; (If for some $k, i, (b_k - b_i)^{-1}$ does not exist then factor N using $\gcd(b_k - b_i, N)$ and halt);
   $v \equiv \sum_{k=0}^{e-1} b_k^e \cdot p_k^{-1} \bmod N$;
2. Real-time computation: $x \equiv e^{-1} \cdot ((\sum_{k=0}^{e-1} c_k p_k^{-1}) - v) \bmod N$.

The complexity of the pre-computation is $O(e\log^2(e))$ (see Appendix), and the complexity of the real time computations is $O(e)$.

3 Special Case

3.1 Finite Differences

We now consider the special case where the e cryptograms are of the form $c_i \equiv (ax+b\cdot i)^e \bmod N$, $i=0,1,...e-1$, for any known constants $a,b \in \mathbb{Z}_N$, where $\gcd(a,N) = \gcd(b,N) = \gcd(e!,N) = 1$. The special linear relations among these cryptograms allows us to deterministically compute x in overall $O(e)$ $\mathbb{Z}_N$-operations. As before x denotes an indeterminate variable.

Definition 2. *For h a polynomial over any ring let $\Delta^{(0)}(x) \equiv h(x)$, and let*

$$\Delta^{(i)}(x) \equiv \Delta^{(i-1)}(x+1) - \Delta^{(i-1)}(x), i = 1,2,...$$

It is easy to see that the degree of the polynomials resulting from this simpler process keep decreasing as in the case of divided-differences. More precisely:

Lemma 2. *In the special case where $x_i \equiv x+i$, and $\gcd(n!,N)=1$, $[x_0,x_1,....x_n] \equiv \Delta^{(n)}(x)/n!$*

A similar relation can be derived when $x_i \equiv ax+ib$, for known constants a,b. The next two lemmas are stated for general polynomials $h(x)$, although eventually we use them for $h(x) \equiv x^e \bmod N$. Let $m = \deg(h)$, and $0 \le k \le m$. By induction on k:

Lemma 3. $\Delta^{(k)}(x) \equiv \sum_{i=0}^{k} \binom{k}{i} \cdot h(x+i) \cdot (-1)^{k-i} \bmod N$.

For the algorithm we will need explicit formulas for the two leading terms of $\Delta^{(k)}(x)$. Let $h(x) = \sum_{i=0}^{m} a_i x^i$ and let $T^{(k)}_{a_m,a_{m-1}}(x)$ denote the two leading terms of $\Delta^{(k)}(x)$.

Lemma 4. $T^{(k)}_{a_m,a_{m-1}}(x) \equiv \frac{(m-1)!}{(m-k)!}x^{m-k-1}(a_m m(x+k(m-k)/2)+a_{m-1}(m-k))$.

Proof. We induct on k. The basis step is trivial. We verify one more step that is needed later.

$$T^{(1)}_{a_m,a_{m-1}}(x) \equiv x^{m-2}(a_m m(x+\frac{m-1}{2})+a_{m-1}(m-1)) \tag{5}$$

$\Delta^{(1)}(x) \equiv h(x+1)-h(x)$, whose two leading terms are indeed equal to $T^{(1)}_{a_m,a_{m-1}}(x)$ above. Now assume that the two leading terms of $\Delta^{(k-1)}(x)$ are

$T^{(k-1)}_{a_m,a_{m-1}}(x) \equiv \alpha x^{m-k+1} + \beta x^{m-k}$, where $\alpha \equiv \frac{(m-1)!}{(m-k)!}a_m m$, and
$\beta \equiv \frac{(m-1)!}{(m-k)!}[a_m mk(m-k)/2 + a_{m-1}(m-k)]$.

The proof can be completed by showing that $T^{(1)}_{\alpha,\beta}(x) \equiv T^{(k)}_{a_m,a_{m-1}}(x)$. This can be done by computing the first difference of $T^{(k-1)}_{a_m,a_{m-1}}(x)$, substituting α for a_m and β for a_{m-1} in equation (5) to get the claim.