



CRYPTANALYSIS OF PUBLIC-KEY CRYPTOSYSTEMS

Presented By
Dieaa Ibrahim Nassr Abdelhai

Supervised By
Assoc. Prof. Sameh S. Daoud
Assoc. Prof. Hatem M. Bahig
Dr. Ashraf M. Bhery

SUBMITTED IN FULFILLMENT OF THE REQUIREMENTS
FOR THE **Ph.D.** DEGREE
(COMPUTER SCIENCE)
SUBMITTED TO
DEPARTMENT OF MATHEMATICS
FACULTY OF SCIENCE
AIN SHAMS UNIVERSITY
CAIRO, EGYPT

AIN SHAMS UNIVERSITY

Author: **Dieaa Ibrahim Nassr Abdelhai**
Title: **Cryptanalysis of Public-Key
Cryptosystems**
Division: **Computer Science**
Department: **Department of Mathematics**
Faculty: **Faculty of Science**
Degree: **Ph.D.** Year: **2016**

Contents

List of Tables	vi
List of Figures	vii
List of Algorithms	viii
List of Abbreviations	ix
Abstract	xi
Acknowledgements	xiii
Summary	xiv
Introduction	1
1 Mathematical Background	3
1.1 Preliminaries on RSA Modulus	3
1.2 Lattice	7
1.3 Convolution Polynomial Rings	13
2 The RSA Cryptosystem	16
2.1 RSA Algorithm	16
2.1.1 The Key Generation	16
2.1.2 Encryption and Decryption	19
2.1.3 Digital Signature and Verification	20
2.2 Efficiency	21
2.3 Security	22
2.3.1 Factorization	25

2.3.2	Private Exponent Attack	27
2.4	Some RSA Variants	29
2.4.1	Rebalanced RSA-CRT	29
2.4.2	Multi-prime RSA	31
3	New Results on Cryptanalysis of RSA Cryptosystem	33
3.1	Factoring RSA Modulus with Primes not Necessarily Shar- ing Least Significant Bits	35
3.1.1	Experiment	45
3.2	Another Look at Private Exponent Attack on RSA using Lattices	48
3.2.1	Coppersmith Interval	48
3.2.2	Previous Attacks on RSA using Coppersmith Interval	57
3.2.3	Revising Coppersmith's Result using Coppersmith Interval	62
3.2.4	Extending De Weger's Attack to Multi-Prime RSA using Coppersmith Interval	65
3.3	Cryptanalysis of RSA with Small LSB($\phi(n)$)	69
3.3.1	Constructing MSB($\phi(n)$)	70
3.3.2	Recovering d	73
3.4	Cryptanalysis of RSA with Two Small Private Exponents	78
4	The NTRU Cryptosystem	87
4.1	NTRU Algorithm	87
4.1.1	The Key Generation	87
4.1.2	Encryption and Decryption	88
4.1.3	Digital Signature and Verification	91
4.2	Efficiency	92
4.3	Security	93
4.4	Previous Lattice Attacks on NTRU	94
4.4.1	The Attack of Coppersmith and Shamir	94
4.4.2	The Attack of Nitaj	98
4.4.3	The Attack of May	100
5	A New Result on Cryptanalysis of NTRU Cryptosystem	105

6	Conclusion and Future Work	116
6.1	RSA	116
6.2	NTRU	118
6.3	Future Work	118
	Bibliography	120

List of Tables

2.1	Special purpose factoring algorithms [79][80]	26
2.2	General purpose factoring algorithms [51][59][80]	27
2.3	Lower bounds for RSA key size for commercial applications [40]	28
3.1	Experiments for which $n \pmod{8} \neq 1$	47
3.2	Experiments for which $n \pmod{8} = 1$	47
3.3	The coefficient matrix for the case $u = 3, r = 1$	52
3.4	Bounds for δ in terms of α, β	57
3.5	Comparison of the new method with the method of [64].	86
3.6	Comparisons of the new method with the method of [74] for $\alpha = \log_n(2^m)$	86
4.1	Efficiency Comparison of NTRU and RSA [31].	93
4.2	NTRU Security Levels [31]	94
4.3	Extrapolation line $\log_{10}(T) = An + B$ depending on the start point n_0 , Times are in Mips-Years [34].	98
5.1	The lattice dimension depending on δ and k	112
5.2	Experimental results of Algorithm 5.1.	114

List of Figures

2.1	Relationships among computing $\phi(n)$, factoring $n = pq$, recovering d , and the RSA problem.	25
3.1	Comparison between our attack and previous attacks, where δ and α as in Theorem 3.21.	65
3.2	Regions for τ and θ for which RSA is insecure.	76
5.1	The relation between $\gamma = \ g\ /\ f\ $ and $c_{H_1, \dots, H_k}$ when $\delta = 0.67$. 111	
5.2	The relation between $\gamma = \ g\ /\ f\ $ and $c_{H_1, \dots, H_k}$ when $\delta = 0.50$. 111	

List of Algorithms

1.1	Calculating square root modulo a power of 2	6
1.2	GramSchmidt orthogonalization [33]	7
1.3	LLL [33]	9
2.1	The key generation of RSA	16
2.2	MILLER-RABIN	18
2.3	RSA encryption	19
2.4	RSA decryption	19
2.5	Repeated Squaring Method	22
2.6	The key generation of RSA-CRT	30
2.7	CRT decryption	30
2.8	The key generation of multi-prime RSA	31
3.1	Calculating t^{th} root modulo a power of 2	38
3.2	Factoring n whose primes not necessarily sharing LSB . . .	41
3.3	Factoring $n = pq$ whose primes p and q share m -LSB . . .	73
3.4	Factoring n with known approximation for $\text{LSB}(\phi(n))$. . .	78
4.1	The key generation of NTRU	88
4.2	NTRU encryption	89
4.3	NTRU decryption	89
4.4	NSS Signature [33]	91
4.5	NSS Verification [33]	92
5.1	NTRU cryptanalysis using Corollary 5.6	113

List of Abbreviations

We use the following standard notations with a short explanation.

Notation	Explanation
$\mathbb{R}$	The set of real numbers.
Z	The set of integers.
Z^n	$\{(a_1, a_2, \dots, a_n) : a_1, a_2, \dots, a_n \in Z\}$.
$\gcd(x, y)$	The greatest common divisor of the two integers x and y .
Z_m	$Z_m = \{0, 1, \dots, m-1\}$.
Z_m^*	$Z_m^* = \{x \in Z_m : \gcd(x, m) = 1\}$.
$a b$	b is divisible by a .
$a \nmid b$	b is not divisible by a .
$x \equiv y \pmod{m}$	$m (x - y)$.
$\phi(n)$	The Euler's phi function.
$\dim(L)$	The dimension of lattice L .
$\det(L)$	The determinant of lattice L .
$\ g(x)\ $	$\sqrt{\sum_i a_i^2}$ the norm of $g(x)$, where $g(x) = \sum_i a_i x^i$.
$\ (v_0, v_1, \dots, v_{k-1})\ _\infty$	$\max\{ v_0 , v_1 , \dots, v_{k-1} \}$.
$\pi(n)$	The number of primes less than or equal to n .
$f * g$	the multiplication of two polynomials f and g .
$ x $	The absolute value of x .
$ A $	The cardinality of set A .
$\lfloor a/b \rfloor$	The round of a/b to the nearest integer less than or equal to a/b .
$\lceil a/b \rceil$	The round of a/b to the nearest integer greater than or equal to a/b .
$\lfloor a/b \rfloor$	The round of a/b to the nearest integer to a/b .