ISSN 2319-2720

Volume 2, No.2, April - June 2013

International Journal of Computing, Communications and Networking

Available Online at http://warse.org/pdfs/2013/ijccn03222013.pdf

A New Construction of Lattice based on RSA Public Key Cryptosystem

Sushma Pradhan[1] and Birendra Kumar Sharma[2]

[1]School of studies in Mathematics, Pt. Ravi Shankar Shukla University, Raipur, Chhattisgarh, India

sushpradhan@gmail.com

[2]School of studies in Mathematics, Pt. Ravi Shankar Shukla University, Raipur, Chhattisgarh, India

sharmabk07@gmail.com

ABSTRACT

In this paper, we present a new lattice-based public-key cryptosystem mixed with a factoring (RSA), which has reasonable key size and quick encryption and decryption. We consider the situation that the RSA secret key d is small and a sufficient amount of the LSBs (least significant bits) of d are known by the attacker. We show that our lattice construction is theoretically more efficient than known attacks proposed in [7, 14]. Moreover, we can use the same module strategy to construct a framework for some GGH-type cryptosystems to improve their security.

Keywords: Lattice, RSA, Public-key Cryptosystem, Subset sum problem, factorization.

1. INTRODUCTION

In 1978 Rivest, Shamir and Adleman published their idea of a public key cryptosystem which has been named after their surnames since then: RSA [35].

Generally a public key (or asymmetric) cryptosystem makes use of key pairs consisting of a secret private key and a public key. A main advantage compared to symmetric cryptosystems is that there is no need of an initial key exchange. The public key is used for encryption whereas the private key is used for decryption. Additionally, messages may be signed by the private key and this signature can be verified by the public key.

The RSA cryptosystem was the first algorithm which could be used for signing and encryption. Its security relies on the hardness of the problem to take the e-th roots modulo a composite integer N of unknown factorization. This task can be reduced to the problem of factoring the integer N. Until now it is not known whether these problems are equivalent. However, there may be other ways to compute the e-th roots modulo N. Depending on the choice of the RSA key parameters there are in fact other possibilities to break RSA (see e.g. the survey by Boneh [6]).

Furthermore, an attacker might gain additional information on the private keys because of implementation mistakes or so-called side-channel attacks. These attacks are applied to physical implementation of cryptosystems. An attacker may analyze e.g. the power consumption, timing information or reaction to faults or electromagnetic radiation in order to get knowledge of the private keys. Heninger and Shacham introduced a new RSA private key reconstruction algorithm [21] that requires fewer bits of the private keys to be known and is more efficient.

Since the seminal work of Ajtai [2] connecting the average-case complexity of lattice problems to their complexity in the worst case, cryptographic constructions based on lattices have drawn considerable attention. Ajtai and Dwork [4] proposed the first lattice-based public-key cryptosystem whose security is based on the worstcase hardness assumptions. After their results, several lattice-based cryptosystems [16, 20, 10, 31, 32, 3, 17, 30] have been proposed.

Lattice-based cryptosystems have many advantages: first, the computations involved are very simple and usually require only modular addition; second, by now they resist the cryptanalysis by quantum algorithms while there already exist the efficient quantum algorithms [36] for factoring integers and computing discrete logarithms. However, most of the presented lattice-based cryptosystems which are efficient have no security proofs based on the worst-case hardness while most of those which have security proofs are not efficient. Recently, some efficient lattice-based cryptosystems [17, 30] with security proofs have been presented.

In Crypto97, Goldreich, Goldwasser and Halevi [16] proposed a public key cryptosystem based on the closest vector problem, which is NP-hard. Although the cryptosystem GGH has not a security proof, it has efficient encryption and decryption. Moreover, it has a natural signature scheme. However, Nguyen [28] showed there is a major flaw in it, and it cannot provide sufficient security without being impractical.

The NTRU cryptosystem proposed by Hoffstein, Pipher, Silverman [20] is the most practical scheme known to date. It features reasonably short, easily created keys, high speed, and low memory requirements. By the results of Coppersmith and Shamir [9], the security of NTRU can be based on, but not equivalent to, the hardness of some lattice problems. To date, the chosen-ciphertext attacks against NTRU may be the most dangerous and most of the ciphertext-only attacks [9, 24, 19] against NTRU relies on the special cyclical structure.

Although the Ajtai-Dwork cryptosystem was thought to be secure if a particular lattice problem is difficult in the worst-case, Nguyen and Stern [27] gave a heuristic attack to show that in order to be secure, the implementations of the Ajtai-Dwork cryptosystem would require very large keys, making it impractical in a real-life environment. In 1998, Cai and Cusick [10] proposed another efficient lattice-based public-key cryptosystem with much less data expansion by mixing the Ajtai-Dwork cryptosystem with a knapsack. However, an efficient ciphertext-only attack presented by Pan and Deng [29] shows that it's not secure.

In this paper, we also propose a new lattice-based public key cryptosystem mixed with a RSA scheme. This paper deals with RSA key reconstruction by the means of lattice techniques. For all reconstruction methods a certain fraction of random bits of the private keys is given. The remainder of the paper is organized as follows. In the second section the mathematical basics e.g. on RSA and lattices are briefly described. In Section 3, we describe our lattice-based public key cryptosystem. The algorithm can be transformed into a subset sum problem and hence, a lattice problem. This is the first approach. Section 4, we give the security analysis and some experimental evidence. Finally, we give a short conclusion in Section 5.

2 PRELIMINARIES

Given an n-bit string $x = (x_{n-1}....x_0) \in \{0,1\}^n$ where xo is the least significant bit of x, let x[i] = xi denote the i-th bit of x.

2.1 RSA

The RSA cryptosystem was published by Rivest, Shamir and Adleman in 1978 [35] and was the first public key cryptosystem. Nowadays it is the de facto standard and described in the Public Key Cryptography Standard (PKCS) #1 [33]. A public key cryptosystem in general is defined by

Definition2.1. A public key cryptosystem is a tuple (P; C; K; E; D) such that:
• P is a finite set of possible plaintexts.
• C is a finite set of possible ciphertexts.
• K is a finite set of possible keys.
• For each k 2 K there is an encryption function $e_k \in \varepsilon$;
ek: P →C and a decryption function $d_k \in D$; dk : C → P
Such that dk(ek(m)) = m for all mЄ P.
• The encryption function ek is public; the decryption function dk is secret.

The following notation will be useful to introduce the RSA cryptosystem.

Remark2.2. Let N be a positive integer.
• Then the ring of integers modulo N is denoted by ZN: = {0, 1, 2... N − 1}.
• and its unit group is denoted by Z_N .
• The unit group consists of all integers in Z_N which is coprime to N and forms an abelian group under multiplication.
• The Euler Totient Function '(N) describes the number of elements of Z^*_N .

Definition2.3.RSA Cryptosystem Let p and q be two primes. Then N = pq (the RSA-modulus) defines P=C: = Z_N and

K: = {(N, e, d) | ed = 1modφ (N)} (1)

The public encryption function ek: $Z_N \to Z_N$ is defined by

$$e_k(m) = m^e \bmod N \forall m \in P \quad (2)$$

And the secret decryption function dk : $Z_N \to Z_N$ is defined by $d_k(c) = c^d \bmod N \forall c \in C$ (3)

e is called public exponent, the tuple (N, e) is called public key and d is called private exponent or private key.

Remark2.4. According to the PKCS #1 [33] an RSA private key must at least contain the following information:
• the public key (N, e)
• the prime factors p and q of N
• the private exponent d
• dp := d mod p − 1 and dq := d mod q − 1
• the inverse of q mod p, denoted by q−1p .

The usual decryption operation can be accelerated by using dp, dq and q−1p: One computes (c mod p)dp and (c mod q)dq and then combines the results by the Chinese remainder theorem and q−1p . This method is about four times faster than the original one [26]. With regard to the best known factorization algorithms and the capability of modern computers the key elements have to be chosen large enough to provide security. Currently the recommended bit length for the modulus N is 2048, i.e., p and q are of bit length 1024 as they should be of the same size (but also not too close to each other). To prevent attacks that take advantage of a too small private exponent d (see Wiener's attack [38] and the improvement by Boneh and Durfee [6]) d is chosen large, i.e., of the same size like N.

2.2 Subset sum problems

The subset sum problem is an important problem in computer science and mathematics, in particular in complexity theory, operations research and cryptography.

Definition2.5. Let $a_1....a_n \in Z > 0, A = \max_{1<i<n} a_i$ and $e := (e_1...e_n) \in \{0,1\}^n$. Define $s := \sum_{i=1}^{n} e_i a_i$.

Then the subset sum problem (SSP) P is to find x1 ...xn Є {0, 1} satisfying $\sum_{i=1}^{n} a_i x_i = s$ given a1 ...an and s.

The density of the set of weights a1 ...an is defined by d: = n/log n (A).

Definition2.6. Let 0 < aij Є Z; i = 1, ...,m; j = 1, ..., n, $A_i = \max_{1<ij<n} a_{ij}$; i = 1, ...m; and $e := (e_1 \ldots e_n) \in \{0,1\}^n$. Define $s_i := \sum_{j=1}^{n} e_j a_{ij}$; i = 1 ...m.
The m-dim SSP is: Given aij ; i = 1, ...m; j = 1, ...n and s1, ...sm find x1, ...xn Є {0, 1}satisfying $\sum_{j=1}^{n} a_{ij} x_j = s_i$ for i = 1, ...m.
The density of the set of weights aij; i = 1 ...m; j = 1 ...n is defined by $d := \frac{n}{Log_2(\prod_{i=1}^{n}(Aij))}$.

Remark2.7. It was shown that the SSP is NP-complete (in its feasibility recognition form) [22]. However, there are lattice-based methods which solve almost all SSP of a certain low density in polynomial time [8, 11, and 23].

2.3 Lattices

Lattice theory has important applications in cryptography. Perhaps the most widely known are attacks against many knapsack based cryptosystems, RSA, and DSA. But lattice theory has also been used in security proofs and in the construction of new cryptosystems. In contrast to cryptosystems based on factoring or discrete logarithms, there are no known quantum algorithms that allow attacking lattice based cryptosystems significantly faster than with classical algorithms. Lattice based cryptography may therefore serve as a long term alternative to established cryptosystems.

We will give a brief introduction to lattices and lattice problems.

Definition2.8. Let b1, b2... bk Є Rn, k≤n linearly independent. Then the set $L := \{\sum_{i=1}^{k} \lambda_i b_i / \lambda_1 \ldots \lambda_k \in Z\}$ (4)
is a lattice of dimension k. It is called lattice of full rank if k =n.

Definition2.9.d (L):= $\det(b_i{}^t b_j)_{1<i,j<k}^{1/2}$ is called discriminant of the lattice.

Theorem 2.10 (Minkowski). Let L be a full-rank lattice. Then there exists a vector x Є L {0} with $\|x\| \le \sqrt{n} d(L)^{1/n}$ where $\|x\|$ denotes the Euclidean norm of x.

Remark2.11. As a lattice is discrete it has a shortest non-zero vector. Though Minkowski's theorem does not result in a constructive method to determine shortest vectors of lattices, we sometimes use the following heuristic assumption.

Assumption2.12. In a full-rank lattice L, a vector 0 6= v 2 L that satisfies Minkowski's bound is the only vector 6= 0 in L with this property, and hence the smallest vector in L.

We will see soon that the subset sum problem can be reduced to the problem of finding the shortest vector of a lattice.

Definition2.13. (Shortest vector problem (SVP)) given a basis of a lattice L and a norm N, find the shortest non-zero vector x ЄL, as measured by N.

Definition2.14. (Closest vector problem (CVP)) Given a basis of a lattice L, a metric M and a vector v Є Rn, find a lattice vector x ЄL minimizing the distance to v, as measured by M.

Remark2.15. In 1981 it was shown by van Emde Boas that the CVP is NP-hard [37] and in 1996 Ajtai proved that the SVP is NP-hard under so-called randomized reductions [1]. The best known polynomial time algorithm for SVP and CVP is the L3 lattice basis reduction algorithm by Lenstra, Lenstra and Lov`asz [22]. In practice L3 performs a lot better than its worst case bounds suggest. Hence, it is reasonable to distinguish the reduction from SSP to SVP from the problem of finding a shortest vector in a lattice.

3 OUR LATTICE BASED RSA KEY RECONSTRUCTION

There have been many approaches to factoring and RSA private key reconstruction in the case of a low public exponent e. As attacks on cryptosystems often result in partial key exposures, this scenario seemed worthwhile to examine.

In one model a subset of consecutive bits of the factors or private keys is given. The first ones who solved this problem were Rivest and Shamir [34] who efficiently factored N = pq given a consecutive 2 3 -fraction of the most or least significant bits of a factor p or q by means of integer programming. Coppersmith [13] applied lattice reduction techniques to the reconstruction problem and improved the bound to 1 2 of the most or least significant bits of a factor. Boneh, Durfee and Frankel [5] used similar techniques to reconstruct d given 1 4 of the least significant bits of d. These lattice-based methods compute consecutive bits as small integer solutions to modular equations.

In our case we are not given consecutive bits but a fully random subset of the private key bits. Hence, the missing bits are randomly scattered over the private key bits as well and the lattice techniques mentioned above are not usable. However, there is another approach to this reconstruction problem that relates it to lattices:

One can transform the problem into a multidimensional subset sum problem which is solvable by lattice techniques.

3.1 Deduction of a subset sum problem from RSA equations

Let (N, e) be an RSA public key and (d, dp, dq) the corresponding private key. As above let p and q be two n 2 -bit primes, i.e., N is an n-bit modulus and dp and dq are n 2 -bit numbers d can be represented by at most n bits.

Key Generation

First, we divide the bits of the private key elements into the unknown and known bits.

• Let $I := \{i \in \mathrm{N} : 0 \le i \le n/2-1; p[i] is known\}$ be the index set of known bits of p and $\bar{I} := \{i \in \mathrm{N} : 0 \le i \le n/2-1; p[i]\ is\ unknown\} := \{i_1 .... i_\alpha\}$, where $i_k < i_l$ if k < l, be the index set of unknown bits of p.

$$p = \sum_{i=0}^{n/2-1} 2^i p[i]$$

$$= \underbrace{\sum_{i \in I} 2^i p[i]}_{=:c_1 = cons\tan t} + \sum_{i \in I} 2^i p[i]$$

$$= c_1 + \sum_{v=1}^{\alpha} 2^{i_v} p[i_v]$$

• Let $J := \{ j \in \mathrm{N} : 0 \le j \le n/2-1; p[j] is known\}$ be the index set of known bits of q and $\bar{J} := \{ j \in \mathrm{N} : 0 \le j \le n/2-1; p[j]\ is\ unknown\} := \{ j_1 .... j_\beta \}$, where $j_k < j_l$ if k < l, be the index set of unknown bits of q.

$$q = \sum_{j=0}^{n/2-1} 2^j q[j]$$

$$= \underbrace{\sum_{j \in J} 2^j q[j]}_{=:c_2 = cons\tan t} + \sum_{j \in \bar{J}} 2^j q[j]$$

$$= c_2 + \sum_{v=1}^{\beta} 2^{j_v} p[j_v]$$

• Let $R := \{r \in \mathrm{N} : 0 \le r \le n/2-1; d[r] is known\}$ be the index set of known bits of d and $\bar{R} := \{r \in \mathrm{N} : 0 \le r \le n/2-1; d[r]\ is\ unknown\} := \{r_1 .... r_k\}$, where $r_k < r_l$ if k < l, be the index set of unknown bits of d.

$$d = \sum_{r=0}^{n/2-1} 2^r d[r]$$

$$= \underbrace{\sum_{r \in R} 2^r d[r]}_{=:c_3 = cons\tan t} + \sum_{r \in \bar{R}} 2^r d[r] \quad \text{d =}$$

$$= c_3 + \sum_{v=1}^{k} 2^{r_v} d[r_v]$$

• Let $S := \{s \in \mathrm{N} : 0 \le s \le n/2-1; d_p[s] is known\}$ be the index set of known bits of dp and $\bar{S} := \{s \in \mathrm{N} : 0 \le s \le n/2-1; d_p[s]\ is\ unknown\} := \{s_1 .... s_\lambda\}$,where sk < sl if k < l, be the index set of unknown bits of dp.

$$d_p = \sum_{s=0}^{n/2-1} 2^s d_p[s]$$

$$= \underbrace{\sum_{s \in S} 2^s d_p[s]}_{=:c_4 = cons\tan t} + \sum_{s \in \bar{S}} 2^s d_p[s] \quad \text{dp =}$$

$$= c_4 + \sum_{v=1}^{\lambda} 2^{s_v} d_p[s_v]$$

• Let $T := \{t \in \mathrm{N} : 0 \le t \le n/2-1; d_q[t] is known\}$ be the index set of known bits of dq and $\bar{T} := \{t \in \mathrm{N} : 0 \le t \le n/2-1; d_q[t]\ is\ unknown\} := \{t_1 .... t_\mu\}$, where tk < tl if k < l, be the index set of unknown bits of dq.

$$d_q = \sum_{t=0}^{n/2-1} 2^t dq[t]$$

$$= \underbrace{\sum_{t \in T} 2^t d_q[t]}_{=:c_5 = cons\tan t} + \sum_{t \in \bar{T}} 2^t d_q[t]$$

$$= c_5 + \sum_{v=1}^{\mu} 2^{t_v} d_q[t_v]$$

We will be concerned with the case where e is small. This case is very common in RSA applications and particularly e = 216 + 1 = 65537 is widely-used. When e is small each of the elements of the private key (d, dp, dq) alone suffices to reveal the factorization of N [12]. Accordingly, the private key includes highly redundant information. There are a few relations between the parameters:

$$N = pq \quad (5)$$

$$ed \equiv 1 \bmod \varphi(N) \quad (6)$$

$$edp \equiv 1 \bmod \varphi(p) \quad (7)$$

$$edq \equiv 1 \bmod \varphi(q) \quad (8)$$

The three congruence's can be transformed into equations over the integers with three unknowns' k, kp and kq:

$$ed = k'(N) + 1 = k(p-1)(q-1) + 1 \text{ by equation (5)}$$

$$= k(N - p - q + 1) + 1 \quad (9)$$

$$edp = kp'(p) + 1 = kp(p-1) + 1 \quad (10)$$

$$edq = kq'(q) + 1 = kq(q-1) + 1 \quad (11)$$

Encryption

For any message $M \in \{0,1\}^n$, first, we uniformly choose a vector r from $\{0,1\}^n$, and then compute the cipher text:

$$C = M^e + r \bmod N$$

Decryption

Compute the original message $M = C^d \bmod N$ and e is called public exponent, the tuple (N, e) is called public key and (d, dp, dq) is called private exponent or private key.

4 COMPARISION WITH STANDARD RSA CRYPTOSYSTEM

We can compare the new cryptosystem to the RSA cryptosystem. For the latter, the natural security parameter is k = the logarithm of the RSA modulus. The public and secret keys of RSA have size O (k), and both encryption and decryption require time $O(k^3)$ (using ordinary multiplication algorithms). For the lattice-based cryptosystem, the natural security parameter is the dimension n. The keys for the new system are relatively large: size $O(n^3)$ for the public key and $O(n^2)$ for the secret key. However, the time required for encryption is only O (n) and no multiplications are needed. Decryption requires time $O(n^3)$, comparable to RSA (again using ordinary multiplication algorithms).

5 SECURITIES AND EFFICIENCY ANALYSIS

We divided the factors into blocks of equal size of known or unknown bits and required that a total of 2 3 of the bits of p and q are known. In some cases knowledge of fewer bits suffices as enough bits can be pre-computed by alternating divisions (modulo powers of N). The described heuristic method works for almost all possible forms of p and q and makes use of a lattice of dimension less than 9. Only if p and q have the same form and two blocks of unknown bits are separated by exactly one block of known bits; the method does not yield the right solution.

Herrmann and May [18] describe a similar phenomenon in their paper"Solving Linear Equations Modulo Divisors: On Factoring Given Any Bits". For e.g. two blocks of unknown bits that are separated by only one known bit it might be better to merge these unknown blocks into one new variable. However, if we merged two unknown blocks in our approach, this would mean that we only know half of the bits. This is insufficient for our method as there would exist small linear combinations of the basis vectors.

Maitra, Sarkar and Sen Gupta [25] revisit the Heninger-Shacham algorithm and work on the problem when a large block of bits in p and q (located at the same position) is unknown. They present a lattice-based method that requires the subsequent bits, namely at least double the number of missing bits for both factors. If e.g. 60 bits are unknown their method requires at least the next 120 more significant bits to be known. This is similar to our approach where two unknown blocks have to be separated by at least two known blocks (or they are adjacent).

This approach is only applicable if just a few bits of the private keys are unknown. Otherwise, there will a priori be several solutions to the SSP and many small linear dependencies among the subset sum weights. Additionally, the more bits are unknown the higher is the dimension of the SSP lattice. In practice when a lattice basis reduction algorithm is used instead of an SVP oracle this becomes a problem because these reduction algorithms only perform well for low dimensions.

The algorithm shows better performance by using large N. On the other hand by using larger N, the lattice dimension also get larger. More specifically, the lattice dimension is $O(n^2)$ by our construction.

Remark: Comparing with GGH, to recover the message using direct lattice reduction, we need solve a CVP for a 2m-dimensional lattice instead of m-dimensional in GGH. This may allow us to use small dimensional matrix as public key to provide sufficient security.

Comparing with NTRU, there is not an obvious attack to obtain the private key in our cryptosystem while the private key of NTRU can be obtained by finding the short vector of NTRU-lattice. Moreover, it seems that we use a more random Lattice with no special cyclical structure like NTRU, this makes our scheme resist some similar attacks against NTRU which are based on the cyclical structure.

6 PROBLEMS WITH THIS METHOD

In a practical scenario where the SVP-oracle is replaced by a lattice basis reduction algorithm the lattice dimension is very important. The L3-algorithm returns a short (so-called L3-reduced) lattice basis in time $O(d^5 n \log^3 B)$ given a d-dimensional integer lattice basis that consists of n-dimensional vectors of maximum norm B. Here the lattice dimension d corresponds to the number of unknown bits from (p, q, d, dp, dq). Hence, the method is only implementable if the number of unknown bits is quite small. Then this method may sometimes return the correct private RSA key. Otherwise, the method is rather impractical.

Example: Assume the RSA key parameters are chosen as recommended in remark.2 which suggests a key size of 1024 bits for p and q and 2048 bits for d. Then dp and dq are of bit length 1024. Let a 0.8-fraction of the bits of each private key element p, q, d, dp and dq be given, i.e., a 0.2-fraction of the bits is unknown. Remember that in this situation the Heninger-Shacham algorithm requires only a 0:27 fractions of the bits of each key element. The number of unknown bits of p respectively q is approximately 200 and the number of unknowns in d is roughly 400. So, just for these three key elements the total number of unknowns is about 800 which lead to a lattice dimension of the same order. This is not efficiently computable with any lattice reduction algorithm (see [15] for an overview of lattice basis reduction algorithms and their limitations.)

7 CONCLUSION

We gave the new lattice construction for the RSA cryptography in the situation that e is small. By this construction, the theoretical recoverable range has been improved. Also, the total efficiency of the lattice based pkc has been improved significantly compared with [14] and we have shown it has reasonable key size and quick encryption and decryption. The constant c shows that it may resist the ordinary lattice attack. Moreover, we can use the same module strategy to construct a framework for some GGH-type cryptosystems to improve their security.

REFERENCES

[1] M. Ajtai.,"The shortest vector problem in L2 is NP-hard for randomized reductions (extended abstract)". In Proceedings of the 30th annual ACM symposium on Theory of computing, pages 10-19. ACM, 1998.

[2] M. Ajtai, Gennerating hard instances of lattice problems, in Proc. of 28th STOC, New York, USA: ACM, 1996, pp. 99-108.

[3] M. Ajtai, Representing hard lattices with O(n log n) bits, in Proc. of 37th STOC, D.S. Johnson, U. Feige, Eds. New York, USA: ACM, 2005, pp. 94-103.

[4] M. Ajtai, C. Dwork, A public-key cryptosystem with worst-case/averagecase equivalence, in Proc. of 29th STOC, New York, USA: ACM, 1997, pp. 284-293.

[5] D. Boneh, G. Durfee, and Y. Frankel.,"Exposing an RSA private key given a small fraction of its bits". In Advances in Cryptology - Asiacrypt 1998, volume 1514 of LNCS, pages 233-260. Springer Verlag, 1998.

[6] D. Boneh.,"Twenty years of attacks on the RSA Cryptosystem". Notices of the American Mathematical Society, 46(2):203-213, 1999.

[7] D. Boneh and G. Durfee, "Cryptanalysis of RSA with private key d less than N0:292", IEEE Transactions on Information Theory, vol. 46, No. 4, pp. 1339- 1349, 2000.

[8] E. Brickell., "Solving low density knapsacks". In Advances in Cryptology, Proceedings of Crypto 1983, pages 25-37. Plenum Press, 1984.

[9] D. Coppersmith, A. Shamir, Lattice attacks on NTRU, in Proc of EuroCrypt 97 (Lecture Notes in Computer Science), W. Fumy, Ed. Berlin, Germany: Springer, 1997, Vol. 1233 pp. 52C-61.

[10] J.-Y. Cai, T.W. Cusick, A lattice-based public-key cryptosystem, in Proc. Of SAC98 (Lecture Notes in Computer Science), S. Tavares, H. Meijer, Eds. Berlin, Germany: Springer-Verlag, 1999, vol. 1556, pp. 219233.

[11] M. J. Coster, A. Joux, B. A. LaMacchia, A. M. Odlyzko, C. P. Schnorr, and J. Stern., "Improved low-density subset sum algorithms". Computational Complexity, 2(2):111-128, 1992

[12] J.-S. Coron and A. May., "Deterministic polynomial-time equivalence of computing the RSA secret key and factoring". Journal of Cryptology, 20(1):39-50, January 2007.

[13] D. Coppersmith.," Small solutions to polynomial equations, and low exponent RSA vulnerabilities". Journal of Cryptology, 10(4):233-260, 1997.

[14] M. Ernst, E. Jochemsz, A. May, and B.Weger, "Partial key exposure attacks on RSA up to full size exponents", in Proceedings of EUROCRYPT 2005, Lecture Notes in Computer Science, vol. 3494, pp. 371-386, 2005.

[15] N. Gama and P. Q. Nguyen."Predicting lattice reduction". In Advances in Cryptology - Eurocrypt 2008, vol 4965 LNCS, pp. 31-51. Springer Verlag, 2008.

[16] O. Goldreich, S. Goldwasser, S. Halevi, Public-key cryptosystems from lattice reduction problems, in Crypto97 (Lecture Notes in Computer Science), B.S.\ Kaliski Jr., Ed. Berlin, Germany: Springer-Verlag, 1997, vol. 1294, pp. 112131.

[17] C. Gentry, C. Peikert, and V. Vaikuntanathan, Trapdoors for hard lattices and new cryptographic constructions, In Proc. of 40th STOC, New York, USA: ACM, 2008, pp 197206.

[18] M. Herrmann and A. May., "Solving linear equations modulo divisors: On factoring given any bits". In Advances in Cryptology - Asiacrypt 2008, volume 5350 of LNCS, pages 406-424. Springer Verlag, 2008.

[19] N. Howgrave-Graham, J.H. Silverman, W. Whyte, A Meet- In- The-Meddle Attack on an NTRU Private Key, available at http://www.ntru.com/cryptolab/tech notes.htm]004

[20] J. Hoffstein, J. Pipher, J.H. Silverman, NTRU: A Ring-Based Public Key Cryptosystem, in Proc. of Algorithmic Number Theory (Lecture Notes in Computer Science), J.P. Buhler, Ed. Berlin, Germany: Springer-Verlag, 1998, vol. 1423, pp. 267288.

[21] N. Heninger and H. Shacham., "Reconstructing RSA private keys from random key bits". In Advances in Cryptology - Crypto 2009, volume 5677 of LNCS, pages 1-17. Springer Verlag, 2009.

[22] A. K. Lenstra, H. W. Lenstra, and L. Lovasz.," Factoring polynomials with rational coefficients". Mathematische Annalen, 261:515-534, 1982.

[23] J. C. Lagarias and A. M. Odlyzko., "Solving low-density subset sum problems". Journal of the ACM, 32:229-246, 1985.

[24] A. May, J.H. Silverman, Dimension Reduction Methods for Convolution Modular Lattices, In Proc of Cryptography and Lattices (Lecture Notes in Computer Science), J.H. Silverman, Ed. Berlin, Germany: Springer- Verlag, 2001, vol.
2146, pp. 110125.

[25] S. Maitra, S. Sarkar., and S. Sen Gupta, "Factoring RSA modulus using prime reconstruction from random known bits". In Progress in Cryptology - Africacrypt 2010, volume 6055 of LNCS, pages 82-99. Springer Verlag, 2010.

[26] A. Menezes, P. C. van Oorschot, and S. A. Vanstone., ”Handbook of Applied Cryptography”. CRC Press, 1996.
[27] P. Nguyen, J. Stern, Cryptanalysis of the Ajtai-Dwork cryptosystem, in Crypto98 (Lecture Notes in Computer Science), H. Krawczyk, Ed. Berlin, Germany:
Springer-Verlag, 1998, vol. 1462, pp. 223242.
[28] P. Nguyen, Cryptanalysis of the Goldreich-Goldwasser-Halevi cryptosystem from Crypto97, in Proc. of Crypto99 (Lecture Notes in Computer Science), Berlin/Heidelberg, Germany: Springer-Verlag, 1999, vol. 1666, pp. 2882304.
[29] Y. Pan, Y. Deng., Cryptanalysis of the Cai-Cusick Lattice-based Publickey Cryptosystem, Cryptology ePrint Archive, Report 2008/204, available at http://eprint.iacr.org/2008/204
[30] C. Peikert, Public-Key Cryptosystems from the Worst-Case Shortest Vector Problem, In Proc. of 41th STOC, New York, USA: ACM, 2009, pp 333-342 .
[31] O.Regev, “New lattice-based cryptographic constructions”, Journal of the ACM, 51(2004), 899942.
[32] O. Regev, On lattices, learning with errors, random linear codes, and cryptography, in Proc. of 37th STOC, D.S. Johnson, U. Feige, Eds. New York, USA: ACM, 2005, pp. 8493.
[33] RSA Laboratories., PKCS]1 v2.1: RSA cryptography standard, 2002.
[34] R. L. Rivest and A. Shamir., ”Efficient factoring based on partial information”. In Ad- vances in Cryptology - Eurocrypt 1985, volume 219 of LNCS, pages 31- 34. Springer- Verlag, 1986.
[35] R. L. Rivest, A. Shamir, and L. Adleman.,” A method for obtaining digital signatures and public-key cryptosystems”. Communications of the ACM, 21(2):120-126, 1978.
[36] P. Shor, Algorithms for Quantum Computation: Discrete Logarithms and Factoring, In Proc. of 35th Annual Symposium on Foundations of Computer Science,
Santa Fe, NM, IEEE Computer Science Press, 1994, pp. 124-134.
[37] P. van Emde Boas., ”Another NP-complete problem and the complexity of computing short vectors in a lattice”. Technical Report 81-04, Department of Mathematics, University of Amsterdam, 1981.
[38] M. J. Wiener., ”Cryptanalysis of short RSA secret exponents”. IEEE Transactions on Information Theory, 36:553-558, 1990.