New Lattice Based Signature Using The Jordan Normal Form

Hemlata Nagesh[1] and Birendra Kumar Sharma[2]

School of Studies in Mathematics,Pt.Ravishankar Shukla University Raipur(C.G.).
E-mail:5Hemlata5@gmail.com[1]
School of Studies in Mathematics,Pt.Ravishankar Shukla University Raipur(C.G.).
E-mail:sharmabk07@gmail.com[2]

Abstract

In this paper it is shown that the use of Jordan normal form instead of Hermite normal form would improve substantially the efficiency and the security of the lattice based signature scheme. In this scheme we also use a new hash function in such a way that the efficiency improved is obtain without decreasing the security of the function.

Keywords: *Lattices; Jordan Normal Form;Digital Signature Scheme.*
MSC No: 94A60

1 Introduction

In the advent of quantum computers, todays widespread signature schemes-most importantly RSA and DSAare rendered utterly insecure due to the seminal work of Shor [6]. Digital signatures, however, have become a supporting pillar of the worlds economy. Thus, endangering their security results in a potential collapse of electronic commerce and secure Internet communication as a whole.

Due the conjectured intractability of lattice problems, like approximating the shortest lattice vector (SVP), even in the quantum-era and because of their computational efficiency, lattice-based signature schemes seem to be one of the most promising replacements for current constructions.

The first proposal for a lattice-based signature was given at CRYPTO 1997 by Goldreich et al. [2]. Their idea was to use a lattice for which a bad basis, whose vectors are long and almost parallel is public, and a good basis with short and nearly orthogonal vectors is private. To employ their scheme, messages need to be hashed into the space spanned by the lattice, and the signature for a given hash in this space is the closest lattice point. The scheme did not

come with a formal proof of security and was broken in its basic variant in 1999 by Nguyen [4]. In 2006 a modified variant was broken again by Nguyen and Regev [5].

In this paper we give a new type of signature scheme using the Jordan Normal form , for this we organized our paper as follows ,first we define some basic notation.than we define a new hash function that significantly improves the security and efficiency of the new signature scheme,in our next section we describe the new signature scheme using the jordan normal form, in our last section we describe the security and efficiency of the new signature scheme.

2 Preliminaries

2.1 Lattice

Let B=$\{b_1, b_2, b_3.....\}$ be a set of n linearly independent vectors in $\mathbb{R}^m$ The lattice generated by B is the set $L\{B\}= \{\sum_i x_i b_i | x_i \epsilon \mathbb{Z}\}$ of all integer linear combinations of the vectors in B. The set B is called basis and it is usually identified with the matrix B=$[b_1,b_2,b_3.....b_n]$ $\epsilon \mathbb{R}^{m\times n}$ having the vectors.$b_i$as columns.

The matrix $L\{B\}$ is full rank if n=m,i.e. if B spans the entire vector space $\mathbb{R}^m$. over the reals for simplicity, in the rest of this paper we will consider only full rank lattices.

2.2 Jordan Normal Form

A Jordan normal form (often called Jordan canonical form) of a linear operator on a finite-dimensional vector space is an upper triangular matrix of a particular form called a Jordan matrix, representing the operator on some basis. The form is characterized by the condition that any non-diagonal entries that are non-zero must be equal to 1, be immediately above the main diagonal (on the superdiagonal), and have identical diagonal entries to the left and below them.

An $n \times n$ matrix A is diagonalizable if and only if the sum of the dimensions of the eigenspaces is n.there is an invertible matrix P such that $A = PJP^{-1}$, where The matrix J is almost diagonal This is the Jordan normal form of A. Every square matrix A can be put in Jordan normal form is equivalent to the claim that there exists a basis consisting only of eigenvectors and generalized eigenvectors of A

2.3 Digital Signature Scheme

A digital signature scheme DS is a triple (Kg, Sig, Vf) where $Kg(n)$ outputs a private signing key sk and a public verification key pk; $Sig(sk, M)$ outputs a signature σ on a message M from the message space $\mathcal{M}$ under sk;

$Vf(pk, \sigma, M)$ outputs 1

if σ is a valid signature on M under pk and otherwise 0. Signature schemes are complete if for all

$(sk, pk) \longleftarrow Kg(n)$, all messages.

Signature schemes are complete if for all $(sk, pk) \longleftarrow Kg(n)$, all messages$M \epsilon \mathcal{M}$, and any $\sigma \longleftarrow Sig(sk, M)$, we have$Vf(pk, \sigma, M) = 1$.

2.4 One-time signatures

A OTS scheme is defined in the same manner as a regular signature scheme. The only difference is that each key pair is not allowed to be used more than once. Otherwise, the security of the scheme would be reduced. The notion of (strong) unforgeability can be reused, when the number of queries to the signature oracle is restricted to one.

3 The New Hash Function

we now put all pieces together and define a new hash function.Let R be a private key choose in such a way that $\rho = \frac{1}{2} min_i \parallel r_i^* \parallel$ is relatively big key is the jordan normal form of R.one can see the basis that the public basis B and the corresponding orthogonalized parallelepiped $\mathcal{P}(B^*)$ are very skewed .The public basis B defines a new hash function with domain the set of vectors of length at most ρ. The result applying the function to vector r is the point in the parallelepiped $\mathcal{P}(B^*)$ congruent to r modulo the lattice.Notice that even if we always start from a vector r close to the origin, the result of performing the reduction operation is a point of $\mathcal{P}(B^*)$ possibly closet to some other lattice point. Notice that recovering the input vector r from f(r) involves finding the lattice point closet to f(r),which is conjectured to be infeasible using only the public key B.However the lattice vector closet to $rmodB$ can be computed using the private key R because $dis(f(r), L) = dis(r, L) \leq \rho$. the orthogonalized parallelepiped $\mathcal{P}(B^*)$ centered at every lattice point.Notice that the lattice point closet to f(r) is just the center of the parallelepiped $\mathcal{P}(B^*)$ containing f(r) which can be found using the private key R.

4 New Signature Scheme Using The Jordan Normal Form

We will give a formal description of the scheme. The security parameter is n. We will describe the key generation with security improvements due to Micciancio [3]

4.1 Key generation

The main security parameter is an integer n. Both the public key B and private key R in the scheme are matrices in $Z^{n\times n}$. Two distributions for choosing the private key were suggested by Goldreich et al [2]

random lattice: choose R uniformly at random from $-l, ..., l^{n\times n}$, for some integer l. In [2], the authors suggest using l = 4. , In [3] Micciancio suggests

almost rectangular lattice: choose R' uniformly at random from $.l, ..., l^{n\times n}$ and add a multiple of the identity matrix $R = R' + kI_n$. In [3], the authors suggest l = 4, $k = \lceil l\sqrt{n} \rfloor$.Micciancio notes in [3] that this distribution discloses the rough direction of the vectors in R to an attacker.

In this paper we use the Jordan Normal form $B = JNFR$ as public key.

Choose a public threshold parameter $\tau \epsilon \mathbb{R}$. Two possibilities are outlined by Goldreich et al. [2] :

no signing failure: let γ be the maximum l_1-norm of the rows in R. Choose$\tau = \gamma\sqrt{n}/2$.

low-probability signing failure: let n_{max} be the entry in R with largest absolute value. In order to guarantee that signing failures have probability less than ϵ, choose $\tau = \rho_{max} ln(\frac{2N}{\epsilon})\frac{\sqrt{n}}{2}$.

4.2 Signing

Hash the message from the new hash function into $m \epsilon Z^n$. A signature s is computed via a CVP approximation algorithm, e.g. Babai's round-off algorithm,

$s = R\lceil R^{-1}m \rfloor$

If signing failures are possible due to a small threshold parameter, we need to check whether$\|s - m\| \leq \tau$, and fail if this is not the case.

4.3 Verification

First check that the signature is a lattice vector with the public key $s \epsilon \Lambda(B)$ using basic linear algebra. Then check whether$\|s - m\| \leq \tau$. If both checks pass, the signature is valid.

5 Security Considerations

We now discuss the security of the new lattice signature using the jordan normal form under passive attacks.

5.1 Computing a Private Key

For the first attack, we simply run a lattice basis reduction algorithm on the public basis B'.If we are lucky then it will output a basis B'' that is good enough to allow the efficient solution of the required closest vector instances.

To prevent such an attack it is necessary that the dimension of the lattice be sufficiently large.since we consider dimension of new signature scheme n$\geq$ 200 so the new scheme is secure from first attack.

5.2 Solving The CVP Directly

For the third attack, one can consider Babai [1] nearest plane algorithm or the embedding technique for solving the CVP. To face such attacks it is necessary that the lattice dimension should be sufficiently large and that the solution to the CVP instance is not too special. In particular, the error vector should not be too short compared with the vectors the lattice. Finally, we remark that none of the above techniques are possible with polynomial asymptotic complexity as the dimension n grows. Hence, the new signature schemes cannot be broken.

5.3 Existential Forgery

Security of digital signature schemes is typically proven against existential forgery under a chosen message attack (EU-CMA),where an adversary wins if he outputs a signature on a new message M^*. after accessing a signature oracle on a polynomial number of different messages. For the described constructions,we need the notion of strong unforgeability under a chosen message attack (SU-CMA),where the adversary even wins if he is able to output a new pair $(M^*, \sigma^*.)$, i.e. he is not forced to output a signature on a new message. In the random oracle model, the adversary has access to the new hash functions H(n). The described concept is formalized in the following experiment

5.4 Nguyen Attack

Let $m \epsilon Z^n$ be the message and $s \epsilon \Lambda(R)$ the corresponding signature, which approximates CVP by use of the secret basis R. Then

$s - m \epsilon \mathcal{P}_{1/2}(R) = \{Rx : x \epsilon [-1/2, 1/2]^n\}$.

We will refer to the set $\mathcal{P}_{\frac{1}{2}}(R)$as the hidden parallelepiped.We make an experimentally justified assumption at this point that for randomly chosen m, the difference $s - m$ is uniformly distributed over$\mathcal{P}_{\frac{1}{2}}(R)$. The algorithmic problem is, given enough independent samples from $U(\mathcal{P}_{\frac{1}{2}}(R))$, recover the columns of $\pm\mathbb{R}$ or an approximation thereof.

6 space efficiency

If we now analyze the size of the keys and the signature of the new cryptosystem.we conclude that the size of the private key can be bounded by $O(n^2 logn)$.Using the Hadamard's inequality we can be also restrict the size of the determinant by $O(n)logn$ and using the restriction mentioned in [3] , we obtain $O(n^2 logn)$ as the size of the public basis and has $O(n)logn$ as the cipher text size. These estimates are based on the GGH challenges.

7 Conclusion

We have presented a new signature scheme replacing Hermite normal form by Jordan normal form. The new signature scheme is shown as secure as old one. Because the security of the new hash function reduces both the time and space requirements by a factor $O(n)$. At this point, we tried to answer the main question in the lattice based cryptography. how to choose the private key i.e. finding families of easily decodable lattices for which decoding becomes infeasible. This is answered by the lattice replacing Hermite normal form to Jordan normal form. A simple counting argument shows that the number of lattices in a certain dimension is exponential in its bit size representation of their Jordan normal form and thus the JNF representation is essentially optimal if one considers arbitrary lattices. The improved efficiency allows even bigger value of the security parameter while maintaining the scheme reasonably practical. One of the important advantages of the proposed scheme is its simplicity. The earlier scheme computes the public key and the function value using a substantial amount of randomness where as in the proposed system these operations are made simple by the deterministic procedure. This is important both from theoretical and practical point of view because it makes the algorithm easier to implement and also easier to analyze.

References

[1] L.Babai, "On Lovasz lattice reduction and the nearest lattice point problem", Combinatirica.6(1), pp.1-13 ,(1986).

[2] O.Goldreich,S.Goldwasser, and S.Halevi,"Public key cryptosystems from lattice reduction problems", In B.S.Kaliski Jr.editor Advance in cryptology-CRYPTO'97, volume 1294 of lecture notes in Computer Science,Springer Verlag.17-21,pp.112-131,(Aug1997).

[3] D. Micciancio, "Improving lattice based cryptosystems using the Hermite normal form", Cryptography and Lattices (CaLC) (J. H. Silverman, ed.), LNCS, vol. 2146 pp.126-145,(Springer, 2001)

[4] Nguyen PQ," Cryptanalysis of the Goldreich-Goldwasser-Halevi cryptosystem" from crypto97. In: Advances in cryptologycrypto1999. Lecture notes in computer science. Springer, New York, pp 288304(1999)

[5] Nguyen PQ, Regev O "Learning a parallelepiped: cryptanalysis of GGH and NTRU signatures". In: Advances in cryptologyEurocrypt 2006. Lecture notes in computer science. Springer, New York, pp. 215233(2006)

[6] Shor PW ,"Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer". SIAM J Comput 26(5):14841509(1997)