ISSN(Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2015

NSS: An NTRU Lattice –Based Signature Scheme

S.Esther Sukila

Department of Mathematics, Bharath University, Chennai, Tamil Nadu, India

ABSTRACT: Whenever a PKC is designed, it is also analyzed whether it could be used as a signature scheme. In this paper, how the NTRU concept can be used to form a digital signature scheme [1] is described.

I. INTRODUCTION

Digital Signature Schemes

The notion of a digital signature may prove to be one of the most fundamental and useful inventions of modern cryptography.

A digital signature or digital signature scheme is a mathematical scheme for demonstrating the authenticity of a digital message or document. The creator of a message can attach a code, the signature, which guarantees the source and integrity of the message. A valid digital signature gives a recipient reason to believe that the message was created by a known sender and that it was not altered in transit. Digital signatures are commonly used for software distribution, financial transactions etc. Digital signatures are equivalent to traditional handwritten signatures. Properly implemented digital signatures are more difficult to forge than the handwritten type.

1.1A digital signature scheme typically consists of three algorithms

A *key generation*algorithm, that selects a private key uniformly at random from a set of possible private keys. The algorithm outputs the private key and a corresponding public key.

A *signing* algorithm, that given a message and a private key produces a signature.

A *signature verifying* algorithm, that given a message, public key and a signature either accepts or rejects. In other words, the algorithm returns True if the signature for the message is associated with the private key, otherwise it returns False.

Two main properties are required for digital signature schemes. First, a signature generated from a fixed message and fixed private key should verify on that message by the corresponding public key (recipients must be able to verify them). Secondly, it should be computationally infeasible to generate a valid signature for a party who does not possess the private key (it must not be forgeable)[7].

A signature scheme provides a way for each user to sign messages so that the signature can later be verified by anyone else. More specifically each user can create a matched pair of private and public keys so that only he can create a signature for a message (using the private key) but anyone can verify the signature for the message (using the signer's public key). The verifier can convince himself that the message contents have not been altered since the message was signed using plaintext. Also the signer cannot later repudiate having signed the message since no one but the signer possesses his private key[1].

1.2 History of NTRUSign Signature Scheme (NSS)

NTRU has been received remarkable attention because of its encryption and decryption speed and the easiness of creating public key/secret key pairs which makes it practical to change keys frequently. Its security is based on the hard mathematical problem of finding short and / or close vectors in a certain class of lattices called NTRU lattices. Since the advent of NTRU encryption scheme, several related signature schemes, such as NSS and R-NSS (revised version of NSS) have been proposed. A fast authentication and digital signature schemes called NSS based on the same underlying hard problem and using keys of the same form, was presented at Euro-crypt 2001. However this scheme was broken by Mironov and Gentry. In their Euro-crypt presentation the authors of NSS sketched a revised version of NSS called R-NSS and published in the preliminary cryptographic standard document EESS. The

ISSN(Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2015

weaknesses of NSS and R-NSS arose from the fact that the signer did not possess a complete basis of short vectors for the NTRU lattice. Later on Hoffstein proposed a new NTRU based signature scheme called NTRUSign. Unlike previous signature scheme the link in NTRUSign between the signature and the underlying approximate closest vector problem is clear and direct.

The NTRUSign algorithm is based on the difficulty of finding a point in a lattice which is close to a random vector in space. This is known as Approximate Closest Vector Problem or appr-CVP. The signer knows a good basis for the entire lattice and use this to solve appr-CVP for an arbitrary point in space which is linked to the document to be signed[6]. The verifier knows a bad, public, basis for the lattice and so can verify that the signature is a lattice point and that it close to the point associated with the signed document[1].

The underlying idea of basing a signature scheme on the use of good basis to find close vectors in a lattice was proposed by Goldreich, Goldwasser and Halevi in their 1998 paper, Public Key Cryptography from lattice reduction problems. However in that case the keys and signatures were of size $N^2 \log N$ (where N is the dimension of the lattice) making the keys impractically large if the scheme was to be secured[2].

1.3 Comparison of NTRUSign and NTRUEncrypt Based on Lattices

In both NTRUSign and NTRUEncrypt key generation starts by generating two small private polynomials f and g and the larger public polynomial $h = \frac{g}{f} \bmod q$. All of these polynomial have the same form in NTRUSign as they do in NTRUEncrypt and they form a good basis for half of the NTRU lattice. However in NTRUSign, the person generating the key must also find a good basis for the other half of the lattice[3]. This means that NTRUSign private keys are larger than the corresponding private keys for NTRUEncrypt. However the underlying lattice problem is the same.

1.4 Security Analysis of NSS

There are various ways in which an attacker might try to break the system. For example he might attempt to discover the private key f or a useful imitation, either directly from the public key h or from a long transcript of valid signatures. He might also try to forge signature on a message without first finding the private key[5].

II. KINDS OF ATTACKS

We distinguish two basic kinds of attacks:

- Key-Only Attacks in which the enemy knows only the real signer's public key and Message Attacks where the enemy is able to examine some signatures corresponding to either known or chosen-messages before his attempt to break the scheme.

The following are four kinds of message attacks, describing how the messages are chosen by the attacker to create a set of signatures. Here A denotes the user whose signature method is being attacked.

- Known Message Attack: The enemy is given access to signatures for a set of messages $m_1, \dots, m_t$. The messages are known to the enemy but are not chosen by him.
- Generic Chosen Message Attack: Here the enemy is allowed to obtain from A valid signatures for a chosen list of messages $m_1, \dots, m_t$ before he attempts to break A's signature scheme. These messages are chosen by the enemy, but they are fixed and independent of A's public key (for example the $m_i's$may be chosen at random). This attack is nonadaptive: the entire message list is constructed before any signatures are seen. This attack is "generic" since it does not depend on the A's public key; the same attack is used against everyone.
- Directed Chosen Message Attack: This is similar to the generic chosen-message attack, except that the list of messages to be signed may be created after seeing A's public key but before any signatures are seen. (The attack is still nonadaptive) This attack is "directed" against a particular user A.
- Adaptive Chosen Message Attack: This is more general yet: here the enemy is also allowed to use A as an "oracle"; not only may he request from A signatures of messages which depend on A's public key but he may also request signatures of messages which depend additionally on previously obtained signatures.

ISSN(Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2015

REFERENCES

[1] J. Hoffstein, J. Piper, H. Silverman, NSS – An NTRU Lattice Based Signature Scheme, NTRU Cryptosystems, Inc. , 5 Burlington Woods, Burlington, MA 01803 USA, 2001, pp. 211-226

[2] C. Gentry, J. Jonsson, J. Stern and M. Szydlo, Cryptanalysis of the NTRU Signature Scheme (NSS) from Eurocrypt, 2001, pp. 9,10

[3]Serane T.V., Zengeya S., Penford G., Cooke J., Khanna G., McGregor-Colman E., "Once daily dose gentamicin in neonates - Is our dosing correct?", ActaPaediatrica, International Journal of Paediatrics, ISSN : 0803-5326, 98(7) (2009) PP.110-1105.

[4]Sharmila S., Jeyanthi Rebecca L., Das M.P., Saduzzaman M., "Isolation and partial purification of protease from plant leaves", Journal of Chemical and Pharmaceutical Research, ISSN : 0975 – 7384, 4(8) (2012) PP. 3808-3812.

[5]Rajasulochana P., Dhamotharan R., Murugakoothan P., Murugesan S., Krishnamoorthy P., "Biosynthesis and characterization of gold nanoparticles using the alga kappaphycusalvarezii", International Journal of Nanoscience, ISSN : 1793-5350, 9(5) (2010) pp.511-516.

[6]Tamilselvi N., Krishnamoorthy P., Dhamotharan R., Arumugam P., Sagadevan E., "Analysis of total phenols,total tannins and screening of phytocomponents in Indigoferaaspalathoides (ShivanarVembu) Vahl EX DC", Journal of Chemical and Pharmaceutical Research, ISSN : 0975 – 7384, 4(6) (2012) pp.3259-3262.

[7]Tamilselvi N., Krishnamoorthy P., Dhamotharan R., Arumugam P., Sagadevan E., "Analysis of total phenols,total tannins and screening of phytocomponents in Indigoferaaspalathoides (ShivanarVembu) Vahl EX DC", Journal of Chemical and Pharmaceutical Research, ISSN : 0975 – 7384, 4(6) (2012) pp.3259-3262.