Digital Signature Development using Truncated Polynomials

P.Prapoorna roja [†] **and P.S.Avadhani** [††],

Prof. Dept of IT
G.V.P.College of Engineering
Viskhapatnam

Prof. Dept. of CSSE
A.U.College of engineering
Viskhapatnam

Abstract
Procedures used for digital signature development rely on the algorithms provided for data confidentiality. The decryption algorithms used for data confidentiality are generally inverse of the encryption algorithms and hence can be used for authentication purposes. Existing Algorithms based on truncated polynomials offer many advantages compared to RSA. At the same time these truncated polynomial algorithms suffer from the drawback that the encryption and decryption algorithms are not inverses of each other as in the case of RSA, hence require separate computation for generation of digital signature. In this paper we propose an algorithm based on truncated polynomials that combine the advantages of both RSA and the algorithms based on truncated polynomials and at the same time overcoming the difficulties faced in each. This proposed algorithm does not require either large primes to be generated or extra computational effort for digital signature generation.

Key words:
Input here the part of 4-5 keywords.

1. Introduction

Many organizations prefer going paperless by using electronic forms of sending and receiving data. In this context, it is essential that not only the sender needs to authenticate the receiver, the receiver should also authenticate the sender and ascertain himself from whom the message was received. A digital signature serves the same purpose as a handwritten signature. A handwritten signature is easy to counterfeit while a digital signature is superior to a handwritten signature in that it is very difficult to counterfeit, at the same time digital signatures are used to authenticate information: that is, to securely tie the contents of an electronic document to a signer Only the true signer should be able to produce valid signatures, and anyone should be able to verify them in order to convince oneself that the signer indeed signed the document. While many digital signature schemes have been proposed and a few are used in practice today[], research into designing schemes that are secure, efficient, or have additional properties continues. This paper presents an efficient and effective authetication scheme based on truncated polynomials, which is efficient and effective.

Manuscript received July 5, 2007
Manuscript revised July 25 2007

2. General Method

The digital signature for a message is generated in two steps:
(i) *Genration Of Message Digest* : A message digest can be treated as the 'summary' of the message we are going to transmit, i.e it will be a number unique to every message such that even the slightest change in the message produces a different digest. The message digest is generated using a set of hashing algorithms.
(ii) *Encryption* :The message digest is encrypted using the sender's *private* key. The resulting encrypted message digest is the *digital signature*. The digital signature generated by the above method is then attached to the message, and sent to the receiver.

At the receiveing end , the receiver then does the following:

1. Using the sender's public key, the receiver decrypts the digital signature to obtain the message digest generated by the sender.
2. The same message digest algorithm used by the sender is used to generate a message digest of the received message by the receiver also.
3. Compares both message digests. If they are *same*, the message is authenticated.

We can be sure that the digital signature was sent by the sender, because *only* the sender's public key can decrypt the digital signature . If decrypting through the public key renders a faulty message digest, this means that either the message or the message digest is not exactly what the sender sent.

The entire process is explained in the Figure No. 1.

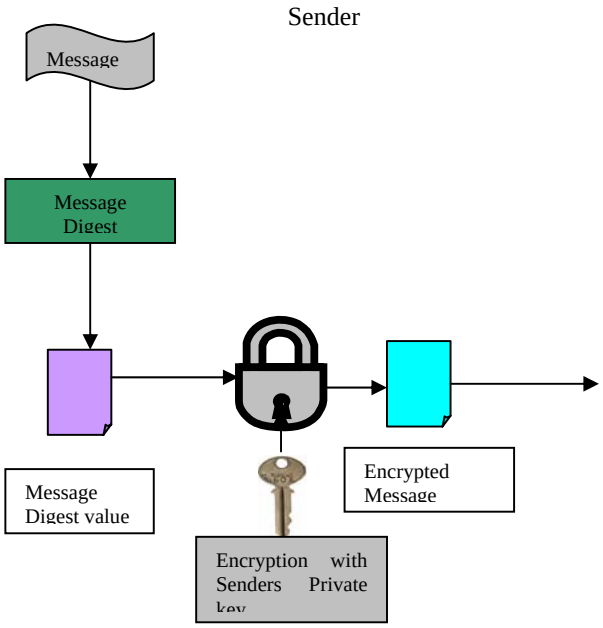

Fig. 1 : General method for Digital Signature Generation at sending end

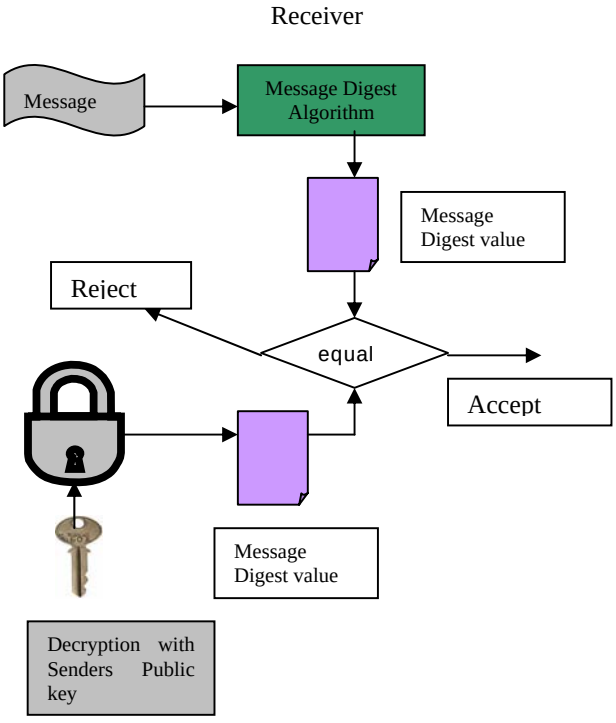

Fig. 2 General method for Digital Signature Generation at receiving end

3. Motivation

The Authentication algorithms required to generate digital signature, mainly rely on the concept of encrypting data with the private key and decryption using public key [7,8]. This process is exactly the reverse of the process for providing data confidentiality. Hence public key cryptosystems are much preferred for signature generation [9]. A major benefit of public key cryptography is that it provides a method for not only for providing data integrity but also for authentication [8]. Authentication using digital signature also provides *non-repudiation*, which means that it prevents the sender from claiming that he or she did not actually send the information. These features are fundamental to cryptography and need to be taken care of by any cryptographic algorithm. The encryption process based on truncated polynomials like NTRU [11,14] solved some of the problems of generation of large prime numbers and the mathematical functions involved with them, which are required in a few algorithms[2]. The NTRU key generation also requires prime and relative prime numbers but they are not as bigger as those of RSA, and the security of the algorithm, does not depend on the knowledge of these numbers by the intruder. The main security of the NTRU algorithm rests on factorization of polynomials in a ring [5,10,12]. Most of the mathematical work in NTRU depends on the multiplication of polynomials. The public key and the private keys generated here are polynomials, and the data needs to be represented in a polynomial form for encryption. In the bare NTRU algorithm, the number of parameters in the public is only one (h(x)) compared to , two parameters present in the private key (f(x), fp(x))[1,13]. This has led to problems for obtaining the digital signature, since the digital signature requires encryption with the private key, as opposed to encryption with public key, which is the procedure for data encryption. In the proposed algorithm presented in the next section, this problem is taken care of. The algorithm presented in this paper, can be used for encryption, data confidentiality and also for signature generation to solve authentication algorithms. These algorithms are presented in the next section.

4. The signature generation algorithm based on truncated polynomials

The Algorithm presented in this paper assumes a ring of polynomials Z(x) of degree less than N. Most of the terms used here bear resemblance to the terms used in the NTRU algorithm. To generate the signature, the message digest value needs to be computed. The message digest value could be generated using any one of the hash functions

like MD5 or SHA. In the implementation for testing the algorithm, we have used MD5 algorithm to generate the digest value. This Digest value needs to be expressed in the form of a polynomial like any other normal data for NTRU algorithm .

4.1 Terminology Used

Let this message digest value be m(x). The sender needs to generate a polynomial f(x) of degree less than N. $f_q(x)$ is the inverse of f mod q, where q is a relative prime to prime p. Similar to NTRU , f(x) needs to be carefully chosen such that $f_q(x)$ exists. g(x) is another small polynomial which needs to be care fully chosen. r(x) is a random polynomial and N is a multiple of prime p. The values of p and q may be made public.

4.2 The Algorithm For Signature Generation

The public key h is calculated as

$$h(x) = f_q(x) + N * g(x)$$

Where N is a multiple of prime p

The private key is f(x), and the values of $f_q(x)$ needs to be maintained in secrecy.

Encrypt the message digest value m(x) as

$$e(x) = f(x)(m(x) + r(x)*q)$$

Where r(x) is a random polynomial .

The encrypted message digest value has to be opened with the public key h(x). The method for decryption is as follows

Let the receiver calculate a(x) = h(x) * e(x) mod q

Compute b(x) = a(x) mod p where the retrieved message digest value expressed as a polynomial is b.

4.3 Analysis Of The Signature Generataion Algorithm

In the encryption process since a random polynomial r(x) is added to the message digest value and then multiplied by f(x), it is exponentially complex to find the private key f(x), even if the message digest value is known by the receiver after decryption. Hence this proposed algorithm is secure even if the values of N, p, q and h are known to everybody.

At the receiving end the receiver calculates

$a(x) = h(x) * e(x) \bmod q$

$= (f_q + N * g) * (f(x) (m(x) + r(x) . q)) \pmod q$

$= m(x) + r(x).q + f(x) \{m(x) + r(x) . q\}.N.g \pmod q$

$= m(x) + f(x)*m(x).N.g \pmod q$

Then the receiver computes

$b(x) = a(x) \bmod p$

$= \{m(x) + f(x)*m(x). N .g \pmod q \} \pmod p$

$= m(x)$

Since p is much less than q and N is a multiple of prime p.

Example :

Let p=3, q =32, N=6

Let $f(x) = -1 + x + x^4$ Its corresponding inverse modulo q denoted by f_q

$f_q = 27 + 33x + 14x^2 + 28x^3 + 23x^4 + 14x^5$

Let $r = -1 + x^2 - x^3 + x^5$ and $g = -1 + x^2 + x^3 - x^5$

The public key

$h(x) = f_q(x) + N * g(x)$

$= 21 + 21x + 20x^2 + 34x^3 + 23x^4 + 8x^5$

Private key is $f(x) = -1 + x + x^4$

Consider a message m(x) of the form $1+x^2$

The cipher text

$e(x) = f(x)(m(x) + r(x)*q)$

$= 97 - 63x - 33x^2 + 98x^3 - 63x^4 - 33x^5$

At the receiving end the decryption process takes place

$a(x) = h(x) * e(x) \bmod q$

$= 7 + 6x + x^2 - 6x^3 - 6x^4$ (after balancing the polynomial)

$b(x) = a(x) \bmod p$

$= 1+x^2$

4.4 Algorithm For Providing Data Confidentiality

As described in section 3.2 the public is h(x) and its corresponding private key (f(x), $f_q(x)$) . Let the message be m(x) .

Encryption: The encryptio here is the same as above except that te role of public and private keys are exchanged.

Hence the e(x) which is the cipher text generated is

$e(x) = h(x)(m(x) + r(x) * q)$

This cipher text that has been generated is now dcrypted at the receiving end using the receivers public key.

Let $a(x) = f(x) * e(x) \bmod q$

$b(x) = a(x) \bmod p$

$= m(x)$

4.5 Analysis of The Algorithm

At the receiving end

$a(x) = f(x) *E(x) \bmod q$

$= f(x) * \{ h(x)(m(x) + r(x) * q) \} \bmod q$

$= f(x) * h(x)*m(x) \bmod q$

$= f(x) * m(x) *\{ f_q(x) + N * g(x) \} \bmod q$

$= m(x) \bmod q + N*f(x) *m(x) *g(x) \bmod q$

Since all the above polynomialls are small

$a(x) = m(x) + N*f(x) *m(x) *g(x)$

$b(x) = a(x) \bmod p$

= m(x) mod p since N is a multiple of p

As m(x) is has cofficients in binary

b(x) = m(x)

5.0 Conclusions

In this paper we have proposed an authentication scheme based on Digital Signatures using truncated polynomials. The parameters f(x), r(x) and g(x) need to be chosen for encryption with care. The mathematical process involved requires a lot of polynomial artihmetic, to be performed. For better security large values of N need to be chosen, which in turn leads to complex and time consuming mathematical operations. To simplify this montgomery methods may be applied to reduce the overheads invloved in arithmetic operations. The algorithm presented in this paper can be used for both signature generation and for providing data confidentiallity unlike a few other algorithms working on polynomial arithmetic.

6.0 References

1. Prapoorna Roja.P., Avadhani P. S. and Prasad E. V. " An Efficient Method of Shared Key Generation Based on Truncated Polynomials " International jounal of computer science and network security, Vol :6 No:8 , Aug 2006
2. Avadhani.P.S, Chalamaih.N and Prapoorna Roja.P. " Secure Transit Of Confidential Documents Over Internet Using High Speed RSA Algorithm", Proceedings Of CCCT -04, International Conference held in Texas Austin, USA, in Aug -2004
3. Padmavathy.R and Prapoorna Roja.P. "Enterprise Information Security", National seminar "BIG-2003" held by CSI in 2003
4. T.H. Cormen, C.E. Leiserson, and R.L. Rivest. *Introduction to Algorithms*. MIT Press,Cambridge,Massachusetts,1990.
5. D. Coppersmith, A.M. Odlyzko, and R. Schroeppel. Discrete logarithms in *GF(p). Algorithmica*, 1: 1-15, 1986.
6. W. Diffie and M.E. Hellman. New directions in cryptography. *IEEE Transactions on Information Theory*, IT-22: 644-654, 1976.
7. R.L. Rivest. *RFC 1321: The MD5 Message-Digest Algorithm*. Internet Activities Board, April 1992.
8. R.L. Rivest, A. Shamir, and L.M. Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21(2): 120-126,February,1978.
9. J. Hoffstein, D. Lieman, J. Silverman" Polynomial Rings and Efficient Public Key Authentication", Proceeding of the International Workshop on Cryptographic Techniques and E-Commerce (CrypTEC '99), M. Blum and C.H. Lee, eds., City University of Hong Kong Press,1999.
10. A.B.Borodin and I.Munro,"Evaluating Polynomials at Many Points", *Information Processing Letters*, 1:2, pp 66-68.1971.
11. J. Hoffstein, J. Pipher, J. Silverman "NTRU: A Ring Based Public Key Cryptosystem", *Algorithmic Number Theory (ANTS III)*, J.P. Buhler (ed.), Lecture Notes in Computer Science, Springer-Verlag, Berlin, Vol 1423,pp 267- 288, Portland, OR, June 1998.
12. J. Hoffstein, J. Silverman "MiniPASS: Authentication and Digital Signatures in a Constrained Environment", *Cryptographic Hardware and Embedded Systems-CHES 2000*, C.K. Koc and C. Paar, eds, Lecture Notes in Computer Science, Springer-Verlag, Vol : 1965 ,pp 328-339,2000.
13. Jeffry Hoffstein, and Joseph H. Silverman – "Polynomial Rings And Efficient Public Key Authentication II", *Proceedings Of A Conference On Cryptography And Number Theory (CCNT 99)*, Biskhauser, 1999.
14. Jeffry Hoffstein, Jill Pipher and Joseph H. Silverman "NTRU: A High Speed Public Key Cryptosystem", Pre Print *Presented At He Hump Session Of Euro Crypt* 96,1996.

Mrs.P.Praapoorna Roja received her B.Tech,M.Tech(control systems), M.Tech(Computer science and technology) degrees from Andhra University college of Engineering She has been in the field of teaching since 11 years and is presently working as a professor in Department. Of Information Technology in G.V.P.College of Engineering. Visakhapatnam, India She has a number of papers published in both conferences and journals and is an active researcher

Prof. P.S.Avadhani did his Masters Degree and Ph.d from IIT kanpur. He is presently working as a Professor in Department on CSSE and is heading the same in Andhra university college of Engineering in Visakhapatnam. He has 32 papers published in various national/ inetrnatioanl journals and conferences. His research areas include Cryptography, Data Security, Algorithms, and Computer Graphics. He is member for Board of studies for A.U