ISSN 2320 -2610

Volume 12, No.3, May – June 2023

International Journal of Multidisciplinary in Cryptology and Information Security

Available Online at http://www.warse.org/IJMCIS/static/pdf/file/ijmcis011232023.pdf

https://doi.org/10.30534/ijmcis/2023/011232023

A digital signature scheme based on problem of solving polynomial congruence in residue class modulo n

HemlalSahu

Govt. J.Yoganandam Chhattisgarh College Raipur Chhattisgarh, India

hemlalsahu@gmail.com

Received Date : April 05, 2023   Accepted Date : May 15, 2023   Published Date : June 07, 2023

ABSTRACT

Many digital signature schemes have been proposed based on different mathematical problems. Some of them are based on factoring into primes, discrete logarithm problem, elliptic curve discrete logarithm problem, lattice problem, multivariate quadratic problem etc. In this work a signature scheme is proposed which security is based on problem of solving polynomial congruence modulo some positive integer. In proposed scheme degree of polynomial is not fixed, so degree can be changed to increase security. It is also efficient because in all the phases modulo addition and multiplication are used and no need to calculate higher exponent.

.

Key words:Cryptography, digital signature, polynomial congruence

1. INTRODUCTION

A digital signature is a cryptographic technique to validate the authenticity andintegrity of a message, software or digital documents. It is the digital analogue of a handwritten signature, but it offers more inherent security and applications. A digital signature is used to solve the problem of impersonation and tampering in digital communications.Digital signatures provide evidence of source, identity and status of digital documents, transactions or messages. Signers may also use digital signatures to acknowledge informed consent.

These are major reasons to apply a digital signature in communications

1) Authentication

Authenticity is a very important factor of digital communication. Messages may often include information about the sender but that information may or may not be accurate. Digital signatures can be used to authenticate the identity of the origin of messages. Digital signature secret key is bound to a specific user; a valid signature shows that the message was sent by that user.

2) Integrity

In many scenarios, the sender and receiver of a message may have a need for confidence that the message has not been altered during transmission. Although encryption hides the contents of a message, it may be possible to *change* an encrypted message without understanding it. However, if a message is digitally signed, any change in the message after signature invalidates the signature. Furthermore, there is no efficient way to modify a message and its signature to produce a new message with a valid signature, because this is still considered to be computationally infeasible by most cryptographic hash functions.

3) Non-repudiation

Non-repudiation or more specifically non-repudiation of origin is an important characteristic of digital signatures. By this property, an entity that has signed some information cannot at a later time deny having signed it. Similarly, access to only the public key fraudulent party does not enable to fake a valid signature.

How does digital signature work?

Digital signatures are based on public key or asymmetric cryptography. In public key algorithm, such as RSA [2] two mathematically linked pair of keys are generated. One of them is called private key and other public key. Digital signatures work on two mutually authenticating cryptographic keys. Signer uses a private key to encrypt signature-related data, while the only way to verify that data is with the signer's public key. If the recipient can't open the document with the signer's public key, then there is a problem with the document or the signature. Digital signature technology requires all parties trust that the individual creating the signature has kept the private key secret. If someone else has access to the private signing key, that party could create fraudulent digital signatures in the name of the private key holder.

1.1 Polynomial congruence

Solving polynomial congruence equations is a central topic in number theory. Let p(x) be an integral polynomial. Then the expression $p(x) \equiv 0 \ (\text{mod } n)$ is known as a polynomial congruence

Theorem 1.1(Lagrange) - Let a polynomial $f(x) \in Z[x]$ has degree n (mod p), with n > 1. Then the congruence $f(x) \equiv 0 \ (\text{mod } p)$ has at most n solutions.

A solution of P(x)≡0(mod n) is a residue classmodulon such that any element of that class satisfies the congruence.

Solution of the general polynomial congruence is intractable

1.2 Hensel's Lemma for polynomial congruence

Suppose $q(x)$ is a polynomial with integer coefficients. If $q(a) \equiv 0 \ (mod p^d)$ and $q^{'}(a) \neq 0 \ (mod p)$, then there is a unique $k \ (modulo p)$ such that $q(a + kp^d) \equiv 0 \ (mod q^{d+1})$. explicitly, if u is the inverse of $q^{'}(a) \ modulo p$, then $k = -u \cdot \frac{q(a)}{p^d}$.

1.3 Chinese Remainder Theorem

if $n = p_1^{e_1} p_2^{e_2} p_3^{e_3} \dots \dots . p_k^{e_k}$ is a prime decomposition of n, then of course for each polynomial f(t) we have (for any x modulo n)

$f(x) = 0 \ mod(n)$ if and only if

$f(x) = 0 \ mod\left(p_1^{e_1}\right)$

$f(x) = 0 \ mod(p_2^{e_2})$

$f(x) = 0 \ mod\left(p_k^{e_k}\right)$

Although Hansel's Lemma and Chinese Remainder theoremprovided technique to reduce equation to solve but they don't provide solution of polynomial congruence i.e. there is no polynomial time algorithm to solve *P(x) ≡0(modn).* Difficulty of this is explained in Rabin Cryptosystem [6].

1.4 Rabin Cryptosystem

The security of Rabin cryptosystem is related to the difficulty of factorization. It has the advantage over the others that the problem on which it banks has proved to be hard **as** integer factorizationIt has been proven that any algorithm which finds one of the possible plaintexts for every Rabin-encrypted ciphertext can be used to factor the modulus n. Thus, Rabin decryption for random plaintext is at least as hard as the integer factorization problem, something that has not been proven for RSA. It is generally believed that there is no polynomial-time algorithm for factoring, which implies that there is no efficient algorithm for decrypting a random Rabin-encrypted value without the private key.

Security of Rabin Cryptosystem depends on solution of $x^2 \equiv a \ (\text{mod } n)$.

1.5 Literature review

RSA [2] Digital Signature uses the modulo arithmetic to sign a Algorithm. ElGamal [3] digital signature is the asymmetric approach of authentication mechanism based on discrete logarithm problem. Digital signature algorithm is generated using various domain parameters. The Rabin signature algorithm [6] was one of the first digital signature schemes proposed. By introducing the use of hashing as an essential step in signing, it was the first design to meet what is now the modern standard of security against forgery. Elliptic Curve Digital signature [4] is cryptographic version of Digital Signature Algorithm Signature Algorithm i.e ECDSA..The Digital Signature Algorithm (DSA) is a asymmetric cryptosystem for digital signatures, based on the mathematical concept of modular exponentiation and the discrete logarithm problem, it was proposed by the National Institute of Standards and Technology (NIST) In August 1991.A BLS digital signature [10] isa cryptographic signature scheme which allows a user to verify that a signer is *authentic*. The scheme uses a bilinear pairing for verification, and signatures are elements of an elliptic curve group.NTRU Signature Algorithm [11] is a digital signature algorithm based on the lattice problem.

2. PROPOSED DIGITAL SIGNATURE SCHEME

2.1 Initialization

Select a large number N. Plaintext, ciphertext and keys are numbers between 1 to N. Sender Alice chooses n numbers between 1 to N. Suppose $(a_1, a_2, a_3, \dots \dots . , a_n)$ are those numbers. Then calculate

$$s_1 = \sum_i^n a_i \ mod(N$$

$$\boldsymbol{s_2 = \sum_{i,j}^n a_i a_j \ mod(N)}$$

$$\boldsymbol{s_3 = \sum_{i,j,k}^n a_i \, a_j a_k \, mod(N)}$$

$$\boldsymbol{s_n = a_1 . a_2 \dots . a_{n-1} . a_n \, mod(N)}$$

$(\boldsymbol{a_1, a_2, a_3}, \dots \dots . , \boldsymbol{a_n})$ is private key and $(\boldsymbol{s_1, s_2, s_3}, \dots . , \boldsymbol{s_n})$ is public key for Alice

2.2 Signature Generation

Suppose Alice wants to sign a message $m \in \{\boldsymbol{1, 2, 3} \dots \dots , \boldsymbol{N}\}$. She will calculate

$$\boldsymbol{d_1 = r_1(m + a_1) mod(N)}$$

$$\boldsymbol{d_2 = r_2(m + a_2) mod(N)}$$

$$\boldsymbol{d_3 = r_3(m + a_3) mod(N)}$$

$$\boldsymbol{d_n = r_n(m + a_n) mod(N}$$

Let $\boldsymbol{r = r_1 . r_2, \dots . . r_n \ mod(N)}$

$\boldsymbol{s = (r_1 + r_2 + \cdots . + r_n) mod(N)}$, and

$\boldsymbol{t = (r_1 a_1 + r_2 a_2 + \dots . + r_n a_n) mod(N)}$

$\big((\boldsymbol{d_1, d_2, d_3}, \dots \dots . , \boldsymbol{d_n}), \boldsymbol{r, s, t, m}\big)$ is a signature for message $\boldsymbol{m}$.

2.3 Signature Verification

After receiving signature $((\boldsymbol{d_1}, \boldsymbol{d_2}, \boldsymbol{d_3}, ., \boldsymbol{d_n}), \boldsymbol{r}, \boldsymbol{s}, \boldsymbol{t}, \boldsymbol{m})$, Bob can verify message with the help of Alice public key $(\boldsymbol{s_1}, \boldsymbol{s_2}, \boldsymbol{s_3}, \dots \dots, \boldsymbol{s_n})$by following formula

$$\boldsymbol{d_1}.\boldsymbol{d_2}.\dots..\boldsymbol{d_n} = \boldsymbol{r}(\boldsymbol{m^n} + \boldsymbol{s_1}\boldsymbol{m^{n-1}} + \boldsymbol{s_2}\boldsymbol{m^{n-2}} + \boldsymbol{s_3}\boldsymbol{m^{n-3}} + \dots\dots\dots..+\boldsymbol{s_n})\boldsymbol{mod}(\boldsymbol{N})$$

$$\boldsymbol{d_1} + \boldsymbol{d_2} + \cdots..+\boldsymbol{d_n} = (\boldsymbol{sm} + \boldsymbol{t})\boldsymbol{mod}(\boldsymbol{N})$$

2.4 *If above equation verifies then message is valid*

$$(\ \boldsymbol{d_1}.\boldsymbol{d_2}.\dots..\boldsymbol{d_n})\boldsymbol{mod}(\boldsymbol{N}) = \boldsymbol{r_1}(\boldsymbol{m} + \boldsymbol{a_1})\,\boldsymbol{r_2}(\boldsymbol{m} + \boldsymbol{a_2})\dots\dots\dots..\boldsymbol{r_n}(\boldsymbol{m} + \boldsymbol{a_n})\boldsymbol{mod}(\boldsymbol{N})$$

$$= \boldsymbol{r_1}.\boldsymbol{r_2},\dots..\boldsymbol{r_n}\,(\boldsymbol{m} + \boldsymbol{a_1})\,(\boldsymbol{m} + \boldsymbol{a_2})\dots\dots\dots.\,(\boldsymbol{m} + \boldsymbol{a_n})\boldsymbol{mod}(\boldsymbol{N})$$

$$= \boldsymbol{r}(\ \boldsymbol{m^n} + \textstyle\sum_i^n \boldsymbol{a_i}\,\boldsymbol{m^{n-1}} + \sum_{i,j}^n \boldsymbol{a_i}\boldsymbol{a_j}\,\boldsymbol{m^{n-1}} + \dots\dots..+\boldsymbol{a_1}.\boldsymbol{a_2}\dots.\boldsymbol{a_{n-1}}.\boldsymbol{a_n})\ \boldsymbol{mod}(\boldsymbol{N})$$

$$= \boldsymbol{r}(\boldsymbol{m^n} + \boldsymbol{s_1}\boldsymbol{m^{n-1}} + \boldsymbol{s_2}\boldsymbol{m^{n-2}} + \boldsymbol{s_3}\boldsymbol{m^{n-3}} + \dots\dots\dots..+\boldsymbol{s_n})\boldsymbol{mod}(\boldsymbol{N})$$

And

$$(\boldsymbol{d_1} + \boldsymbol{d_2} + \cdots..+\boldsymbol{d_n})\boldsymbol{mod}(\boldsymbol{N}) = \boldsymbol{r_1}(\boldsymbol{m} + \boldsymbol{a_1}) + \boldsymbol{r_2}(\boldsymbol{m} + \boldsymbol{a_2})\dots\dots\dots.+\boldsymbol{r_n}(\boldsymbol{m} + \boldsymbol{a_n})\boldsymbol{mod}(\boldsymbol{N})$$

$$= (\boldsymbol{r_1} + \boldsymbol{r_2} + \boldsymbol{r_3} + \cdots\boldsymbol{r_n})\boldsymbol{m} + (\boldsymbol{r_1}\boldsymbol{a_1} + \boldsymbol{r_2}\boldsymbol{a_2} + \dots\dots\dots..+\boldsymbol{r_n}\boldsymbol{a_n})\boldsymbol{mod}(\boldsymbol{N})$$

$$= (\boldsymbol{sm} + \boldsymbol{t})\boldsymbol{mod}(\boldsymbol{N})$$

2.5 Example

Let N = 1729. Alice selects private key $(\boldsymbol{a_1}, \boldsymbol{a_2}, \boldsymbol{a_3}, \boldsymbol{a_4})$ = (11, 23, 29, 31). Calculate

$$s_1 = (\mathbf{11} + \mathbf{23} + \mathbf{29} + \mathbf{31})\boldsymbol{mod}(\mathbf{1729})$$

= 94

$$s_2 = (\mathbf{11}\boldsymbol{x}\mathbf{23} + \mathbf{11}\boldsymbol{x}\mathbf{29} + \mathbf{11}\boldsymbol{x}\mathbf{31} + \mathbf{23}\boldsymbol{x}\mathbf{29} + \mathbf{23}\boldsymbol{x}\mathbf{31} + \mathbf{29}\boldsymbol{x}\mathbf{31}\boldsymbol{mod}(\mathbf{1729})$$

$$= \mathbf{3192}\boldsymbol{mod}(\mathbf{1729}) = \mathbf{1463}$$

$$\boldsymbol{s_3} = \mathbf{11}\boldsymbol{x}\mathbf{23}\boldsymbol{x}\mathbf{29} + \mathbf{11}\boldsymbol{x}\mathbf{23}\boldsymbol{x}\mathbf{31} + \mathbf{11}\boldsymbol{x}\mathbf{29}\boldsymbol{x}\mathbf{31} + \mathbf{23}\boldsymbol{x}\mathbf{29}\boldsymbol{x}\mathbf{31}\boldsymbol{mod}(\mathbf{1729})$$

$$= \mathbf{45746}\boldsymbol{mod}(\mathbf{1729})$$

$$= \mathbf{792}$$

$$s_4 = (\mathbf{11}\boldsymbol{x}\mathbf{23}\boldsymbol{x}\mathbf{29}\boldsymbol{x}\mathbf{31})\boldsymbol{mod}(\mathbf{1729})$$

$$= \mathbf{227447}\boldsymbol{mod}(\mathbf{1729})$$

$$= \mathbf{948}$$

Public key for Alice is $(\boldsymbol{s_1}, \boldsymbol{s_2}, \boldsymbol{s_3}, \boldsymbol{s_4}) = (\mathbf{94}, \mathbf{1463}, \mathbf{792}, \mathbf{948})$

Suppose Alice wants to sign a message$\boldsymbol{m} = \mathbf{105}$, she will select $(\boldsymbol{r_1}, \boldsymbol{r_2}, \boldsymbol{r_3}, \boldsymbol{r_4})$ = (5, 7, 4, 9) calculate

$$d_1 = \mathbf{5}\boldsymbol{x}(\mathbf{105} + \mathbf{11})\boldsymbol{mod}(\mathbf{1729})$$

$$= \mathbf{580}\boldsymbol{mod}(\mathbf{1729})$$

$$= \mathbf{580}$$

$$d_2 = \mathbf{7}\boldsymbol{x}(\mathbf{105} + \mathbf{23})\boldsymbol{mod}(\mathbf{1729})$$

$$= \mathbf{896}\boldsymbol{mod}(\mathbf{1729})$$

$$= \mathbf{896}$$

$$\boldsymbol{d_3} = \mathbf{4}\boldsymbol{x}(\mathbf{105} + \mathbf{29})\boldsymbol{mod}(\mathbf{1729})$$

$$= \mathbf{536}\ \boldsymbol{mod}(\mathbf{1729})$$

$$= \mathbf{536}$$

$$\boldsymbol{d_4} = \mathbf{9}\boldsymbol{x}(\mathbf{105} + \mathbf{31})\boldsymbol{mod}(\mathbf{1729})$$

$$= \mathbf{1224}\boldsymbol{mod}(\mathbf{1729})$$

= 1224

$$\boldsymbol{r} = \boldsymbol{r_1}.\boldsymbol{r_2}.\boldsymbol{r_3}.\boldsymbol{r_4}\boldsymbol{mod}(\boldsymbol{N})$$

$$= \mathbf{5}.\mathbf{7}.\mathbf{4}.\mathbf{9}\ \boldsymbol{mod}(\mathbf{1729})$$

$$= \mathbf{1260}$$

$$\boldsymbol{s} = (\boldsymbol{r_1} + \boldsymbol{r_2} + \boldsymbol{r_3} + \boldsymbol{r_4})\boldsymbol{mod}(\boldsymbol{N})$$

$$= (\ \mathbf{5} + \mathbf{7} + \mathbf{4} + \mathbf{9})\boldsymbol{mod}(\mathbf{1729})$$

$$= \mathbf{25}$$

$$\boldsymbol{t} = (\boldsymbol{r_1}\boldsymbol{a_1} + \boldsymbol{r_2}\boldsymbol{a_2} + \boldsymbol{r_3}\boldsymbol{a_3} + \boldsymbol{r_4}\boldsymbol{a_4})\boldsymbol{mod}(\boldsymbol{N}) = (\ \mathbf{5}\boldsymbol{x}\mathbf{11} + \mathbf{7}\boldsymbol{x}\mathbf{23} + \mathbf{4}\boldsymbol{x}\mathbf{29} + \mathbf{9}\boldsymbol{x}\mathbf{31})\boldsymbol{mod}(\mathbf{1729})$$

$$= \mathbf{611}$$

$((\boldsymbol{d_1}, \boldsymbol{d_2}, \boldsymbol{d_3}, \boldsymbol{d_4}), \boldsymbol{r}, \boldsymbol{s}, \boldsymbol{t}, \boldsymbol{m}) = ((\mathbf{548}, \mathbf{1295}, \mathbf{1453}, \mathbf{132}), \mathbf{1260}, \mathbf{25}, \mathbf{611}, \mathbf{105})$is a signature for message $\boldsymbol{m}$.

Verification-

$$(\ \boldsymbol{d_1}.\boldsymbol{d_2}.\boldsymbol{d_3}.\boldsymbol{d_4})\boldsymbol{mod}(\boldsymbol{N}) = \mathbf{580}.\mathbf{896}.\mathbf{536}.\mathbf{1224}\boldsymbol{mod}\ (\mathbf{1729})$$

$$= \mathbf{340}.\mathbf{943}.\mathbf{339}.\mathbf{520}\boldsymbol{mod}\ (\mathbf{1729})$$

$$= \mathbf{238}$$

$$(\boldsymbol{d_1} + \boldsymbol{d_2} + \cdots..+\boldsymbol{d_n})\boldsymbol{mod}(\boldsymbol{N}) = (\mathbf{580} + \mathbf{896} + \mathbf{536} + \mathbf{1224})\ \boldsymbol{mod}\ (\mathbf{1729})$$

$$= \mathbf{3236}\boldsymbol{mod}\ (\mathbf{1729})$$

= 1507

$$\boldsymbol{r}(\boldsymbol{m^4} + \boldsymbol{s_1}\boldsymbol{m^3} + \boldsymbol{s_2}\boldsymbol{m^2} + \boldsymbol{s_3}\boldsymbol{m} + \boldsymbol{s_4})\boldsymbol{mod}(\boldsymbol{N})$$

$$= 1260(\ 105^4 + 94x105^3 + 1463x105^2 + 792x105 + 948)\ mod\ (1729)$$

$$= 1260x(196 + 94x924 + 1463x651 + 792x105 + 948)\ mod\ (1729)$$

$$= 1260x(1716 + 406 + 1463 + 168 + 948)\ mod\ (1729)$$

$$= 1260x1452 mod\ (1729)$$

= 1829520mod (1729)

= 238

$(sm + t)mod(1729$ = (105x25+611)$mod(1729)$

=3236$mod(1729)$

= 1507

3 SECURITY ANALYSIS

3.1 To verify signature Bob satisfies following equations

$$d_1.d_2.\ldots..d_n = r(m^n + s_1m^{n-1} + s_2m^{n-2} + s_3m^{n-3} + \cdots\ldots\ldots..+s_n)mod(N)$$

$$d_1 + d_2 + \cdots..+d_n = (sm + t)mod(N)$$

Suppose eavesdropper try to duplicate signature by replacing $r, s, tandm$ thento find$(d_1, d_2, d_3, \ldots\ldots., d_n)$he has to solve following equations

$$d_1.d_2.\ldots..d_n = xmod(N)$$

$$d_1 + d_2 + \cdots..+d_n = ymod(N)$$

But it is difficult to solve above equations.

3.2 Suppose eavesdropper try to find out private keys $(a_1, a_2, a_3, \ldots\ldots., a_n)$. He will have to solve following polynomial congruence of degree n

$$x^n + s_1x^{n-1} + s_2x^{n-2} + s_3x^{n-3} + \cdots\ldots\ldots..+s_n = 0mod(N)$$

It is also difficult.

3.3 To find out $r_1, r_2, \ldots.., r_n$ he will again face problem discussed in 3.1.

4 EFFICIENCY ANALYSIS

No need to calculate large exponent. Also public and private keys may be calculated before key generation. So proposed digital signature scheme based on problem of solving polynomial congruence is more efficient than existing systems.

5 CONCLUSION

Proposed signature scheme is new scheme based on problem of solving polynomial congruence. It is a first signature scheme based on this problem. Proposed scheme is secure as well as efficient

REFERENCES

[1]Diffie, W., and Hellman, M. New directions in cryptography. IEEE Trans. on Inform. IT-22, 6 (Nov. 1976), 644-654

[2]Rivest, R.L., Shamir, A., and Adleman, L. A method for obtaining digital signatures and public-key cryptosystems. Comm. ACM 21, 2(Feb. 1978), 120- 126.

[3]ElGamal, T, "A Public-Key Cryptosystem and a Singnature Scheme Based on Discrete Logarithms", *IEEE Trans. Information Theory (*1985), vol. 31, no. 4, pp. 469-472,.

[4]Koblitz,, N., Elliptic curve cryptosystems. Mathematics of Computation (1987) 48, 203-209.

[5]Hensel, K, Theorie der algebraischenZahlenTeubner, Leipzig (1908)

[6] Michael O. Rabin. "Digitalized Signatures and Public-Key Functions as Intractable as Factorization". In: Laboratory for Computer Science. Massachusetts Institute of Technology, Laboratory for Computer Science, 1979.

[7]Goldreich, O, Foundations of cryptography I: Basic Tools, Cambridge: Cambridge University Press, (2001), ISBN 978-0-511-54689-1

[8]Goldreich, O, Foundations of cryptography II: Basic Applications (1. publ. ed.), Cambridge [u.a.]: Cambridge Univ. Press, (2004), ISBN 978-0-521-83084-3

[9] Rafael, P, A Course in Cryptography (PDF), retrieved 31 December 2015

[10]Boneh, D*;* Lynn *B &* Shacham *H*, "Short Signatures from the Weil Pairing". Journal of Cryptology. **17** *(4):* (2004). *297–319*

[11]Jeffrey, H; Howgrave-Graham, N; Pipher, Jill; Silverman, Joseph H.; Whyte, William (2003). "NTRU Sign: Digital Signatures Using the NTRU Lattice" (PDF). *Topics in Cryptology — CT-RSA 2003*. LNCS. Vol. 2612. Springer. pp. 122–140.