A New Variant Blind Multisigature Scheme

***M.Sreedevi and **Prof. M.Padmavathamma**

Abstract
One of the advanced public key cryptographic scheme is a digital signature scheme. These are more significant in development of public key cryptography. In this article we concentrate on properties of Jordan totient function of index 2 and apply them to modify the blind multi signature scheme.
Key words:
Variant, Blind, Multisignature Scheme

1. Introduction

In this article we present a new variant blind multi signature scheme which is the extension of a blind multi signature scheme (1) with the help of the properties of Jordan Totient function J_2 (n). We briefly, discussed the possibility and validity and security analysis of this new scheme.

2. Jordan Totient function J_2 (n)

2.1 Definition

Jordan Totient function of index 2 is denoted by J_2 (n) and is defined as

$$J_2(n) = n^2 \prod_{p/n}\left(1 - \frac{1}{p^2}\right), n \in Z^+$$

Where p is a prime divisor of n
The conjugate of this function is defined by

$$\overline{J_2(n)} = n^2 \prod_{p/n}\left(1 + p^{-2}\right), n \in Z^+$$

2.2 Properties

1. $J_2(1) = 1$, $J_2(2) = 3$
2. $J_2(n)$ is even iff $n \geq 3$
3. If p is a prime number then
$$J_2(p) = \left(p^2 - 1\right)$$
$$J_2\left(p^\alpha\right) = p^{2(\alpha-1)}\left(p^2 - 1\right)$$
4. If $n = p_1^{\alpha_1}.p_2^{\alpha_2}\,..........p_r^{\alpha_r}$ then

$$J_2(n) = p_1^{2(\alpha_1-1)}.p_2^{2(\alpha_2-1)}..........p_r^{2(\alpha_r-1)}.\left(p_1^{\,2}-1\right)\left(p_2^{\,2}-1\right)...\left(p_r^{\,2}-1\right)$$

2.3 Definition (multiplicative function)

A function f defined over the set of positive integers is said to be multiplicative if for each pair m, n with gcd (m, n) =1 then

$$f(mn) = f(m)f(n)$$

2.4 Theorem

$J_2(n)$ is multiplicative

2.5 Theorem

Let p, q be two positive distinct prime numbers and n = pq. If ‘a’ be any positive integer such that gcd (a, n) =1 then

$$a^{J_2(n)} \equiv 1 (\bmod n)$$

2.6 Theorem

Suppose p_1, p_2, …. p_r are any r distinct positive prime numbers and $n = p_1 p_2, \ldots\ldots\ldots\ldots p_r$, if ‘a’ be any positive integer such that gcd (a,n) = 1 then

$$a^{J_2(n)} \equiv 1 (\bmod n)$$

3. Digital Signature

The digital signature concept was first proposed by Diffie Hellman. The ability to construct a digital signature scheme is a great advantage of public key cryptography. A digital signature scheme can be described as follows.

Key Generation: The signer Alice creates her private key and public key pair, which we denote by SK_A and PK_A respectively.

Signature generation: Using her private key SK_A, Alice creates a signature ‘ σ ’ on her message M.
Signature verification: Having obtained the signature ‘ σ ’ and the message M from Alice, the verifier Bob

Manuscript received November 5, 2009
Manuscript revised November 20, 2009

checks whether 'σ' is a genuine signature on M using Alice's public key PK_A. If it is he returns "Accept" otherwise he returns "Reject".
Since only a single entry is able to sign a message and the resulting signature can be verified by any body a dispute over who created the signature can be easily settled. This often called 'non-repudiation" is one of the important security services that digital signature schemes can provide. Indeed, non repudiation is an essential security requirement in electronic commerce applications.

4. J_2 -ERSA Cryptosystem

To make RSA cryptosystem more for the design of cryptosystems in a group oriented or distributed communication environment, Feng [ ] proposed an extension of the RSA cryptosystem called the ERSA cryptosystem. Now we extend this system with the help of the properties of J_2 (n). The modified key generation, encryption and decryption are given below.

Key generation:

1. Select two prime numbers sufficiently large and compute n = p.q and
$$J_2(n) = (p^2 - 1)(q^2 - 1)$$
2. Select two vectors < e_1, e_2, ………. e_r > and < d_1, d_2………. d_r > whose inner product satisfies the property
$$e_1 d_1 + e_2 d_2 + \dots\dots\dots + e_r d_r \equiv 1\left(\bmod J_2(n)\right)$$

Public key = (n, < e_1, e_2,……… e_r>)
Private key = (n, < d_1, d_2, ... d_r >)

Encryption: Given plaintext M and the public key = (n, < e_1, e_2……….. e_r >) compute the cipher text vector C = < c_1, c_2, ….. c_r> by using the formula

$$c_1 \equiv M^{e_1} \pmod n$$
$$c_2 \equiv M^{e_2} \pmod n$$
$$\dots\dots\dots\dots\dots\dots$$
$$c_r \equiv M^{e_r} \pmod n$$

Decryption: Given a cipher text vector C = < c_1, c_2,……………. c_r > and the private key = (n, < d_1, d_2…………….. d_r >) compute the plaintext M by using the formula.

$$\prod_{i=1}^{r} c_i^{d_i} \equiv \prod_{i=1}^{r} \left(M^{e_i}\right)^{d_i} \pmod n$$
$$\equiv M^{\sum_{i=1}^{r} e_i d_i} \pmod n$$
$$\equiv M^{e_1 d_1 + e_2 d_2 + \dots\dots\dots e_r d_r} \pmod n$$
$$\prod_{i=1}^{r} c_i^{d_i} \equiv M \pmod n$$

5. The J_2-ERSA Based Blind Multi Signature Scheme

The concept of Blind Signature scheme was introduced by chaum in 1982 [ ]. In a blind signature scheme a signer shall have no idea of what he signs. It means a signer must not be able to find a relationship between some blinded and unblinded parameters. This property is usually referred as the un linkability property. Accordingly, blind signatures are widely used to construct anonymous electronic election schemes.
Now we propose a J_2-ERSA based blind multi signature scheme.
Suppose that there are signers A_i's $1 \le i \le r$, a signature requester denoted as B, and a trusted key generation centre (KGC). Then, the generation and verification of our blind multi signature scheme can be described as follows.

Key generation:

[1] Select two suitably large random prime numbers p, q and compute n = p. q and $J_2(n) = (p^2 - 1)(q^2 - 1)$

[2] Select two vectors < e_1, e_2, …….. e_r > and <d_1, d_2, ………… d_r > such that their inner product satisfies the equality
$$e_1 d_1 + e_2 d_2 + \dots\dots\dots e_r d_r \equiv 1\left(\bmod J_2(n)\right)$$
Where gcd $(e_i, e_j) > \alpha, i \ne j$ and $\alpha \equiv 1 \pmod 4$

[3] The KGC publishes n and distributes e_i and d_i to each $A_i, 1 \le i \le r,$ as his public and private keys respectively.

Public key = (n, < e_1, e_2, ... e_r>)
private key = (n, <d_1, d_2........... d_r >)

Blind Multi Signature Generation:

Suppose B wants A_i, $1 \le i \le r,$ to sign a message M blindly, where $M \in Z_n$

1. B determines two large strong primes p and q such that it is computationally infeasible to factor the value of their product.
2. For each $1 \le i \le r$, B computes

$$R_{1i} \equiv p^{e_i} M \pmod n$$

$$R_{2i} \equiv q^{e_i} M^{-1} \pmod n$$

And sends (R_{1i}, R_{2i}) to A_i

3. Once receiving (R_{1i}, R_{2i}) from B, each $A_i, 1 \le i \le r$ computes

$$W_{1i} \equiv R_{1i}{}^{d_i} \pmod n$$

$$W_{2i} \equiv R_{2i}{}^{d_i} \pmod n$$

As his blind signature for M. Then he sends $(W_{1i},\ W_{2i})$ back to B.

4. After receiving all pairs $(W_{1i},\ W_{2i})$ from A_i, $1 \le i \le r$, B computes W_1, W_2 and T as

$$W_1 \equiv \prod_{i=1}^{r} W_{1i} \pmod n$$

$$W_2 \equiv \prod_{i=1}^{r} W_{2i} \pmod n$$

$$T \equiv P^{-1} W_1 \pmod n$$

Where T is served as the blind multi signature of M from A_i, $1 \le i \le r$ and (W_1, W_2) is presented for verifying the blind multi signature.

Blind multi signature verification:

After obtaining the values of W_1, W_2 and T, B can make sure the validity of T by checking whether $W_1 W_2 \equiv pq \pmod n$

If it holds, the blind multi signature T is proved to be correct.

Blindness Discussion and Security Analysis

Observe step (3) of the Signature generation phase to see if each A_i, $1 \le i \le r$ computes W_{1i} and W_{2i} with his genuine private key d_i, then in step (4) we will have

$$W_1 = \prod_{i=1}^{r} W_{1i} \equiv p^{e_1 d_1 + e_2 d_2 + \dots\dots\dots + e_r d_r} M^{d_1 + d_2 + \dots\dots\dots d_r} \pmod n$$

$$\equiv p M^{d_1 + d_2 + \dots\dots d_r} \pmod n$$

$$W_2 = \prod_{i=1}^{r} W_{2i} \equiv q^{e_1 d_1 + e_2 d_2 + \dots\dots\dots + e_r d_r} M^{-(d_1 + d_2 + \dots\dots\dots d_r)} \pmod n$$

$$\equiv q M^{-(d_1 + d_2 + \dots\dots + d_r)} \pmod n$$

For $p^{e_1 d_1 + e_2 d_2 + \dots\dots + e_r d_r} \equiv p \pmod n$

$q^{e_1 d_1 + e_2 d_2 + \dots\dots + e_r d_r} \equiv q \pmod n$

In this case we also have in step (4)

$$T \equiv p^{-1} W_1 \equiv M^{d_1 + d_2 + \dots\dots + d_r} \pmod n$$

Accordingly if $W_1 W_2 \equiv pq \pmod n$ holds the blind multi signature T for the massage M is indeed verified.
The security of the above proposed scheme is based on the $J_2 - ERSA$ cryptosystem which is guaranteed by the computationally infeasibility of factoring the used modulus. An attacker is hard to force a legitimate blind multi signature unless he knows the factoring of n.

6. Conclusion

In this paper, we proposed a new variant Blind multi signature scheme based on J_2 – ERSA Cryptosystem. This scheme can also extend by using the same properties of another Jordan – Totient functions of index $\ge$ 3. This scheme more significant and computationally infeasible to attacker than original scheme using the proposed scheme we can also develop a multi authority voting system.

References

[1] Jian –liang lin, Hsiu – feng Lin, chih-ying chen, chen – chen chang, “ A multiauthority Electronic voting protocol. Based upon a blind Multi signature scheme” . IJCSNS, Vol. 6, No. 12, December 2006. pages 266 to 274.

[2] J. Benaloh, D Tuinstra, “Receipt free secret ballot elections,” Proc of the 26th Annual ACM Sump, on the Theory of Computing, pp 544 to 553, 1994.

[3] C. Boyd, “Digital multi signatures”, Cryptography and Coding pp. 241-246, Claredon Press, 1989.

[4] D. Chaum, “Untraceable electronic mail, return addresses, and digital pseudonyms,” Communications of the ACM, vol. 24, No. 2, pp. 84-88, 1981.

[5] D. Chaum, “Blind signatures for untraceable payments,” advance in Cryptology – Crypto’ 82 , Springer – Verlag, pp. 199-203, 1983.

[6] D. Chaum, “Elections with unconditionally – secret ballots and disruption equivalent to breaking RSA,” Advances in Cryptology – EUROCRYPT 88 proceedings, Lecture notes

in Computer science, vol. 330, (C.G. Gunther, Editor), Springer – Verlag, pp. 177-182, 1980.
[7] R. Cramer, M. Franklin, B. Schoenmakers, and M. Yung "Multi –authority secret-ballot elections with linear work," Advances in Cryptology – EUROCRYPT" 96, Springer – Verlag pp. 72-83, 1996.
[8] Apostal T.M, introduction to analytic number theory, Springer International Students Edition 1980.
[9] Thajoddin. S & Vangipuram S; A Note on Jordan's Totient function Indian J.Pure apple. Math. 19(12): 1156-1161, December, 1988.
[10] Boneh D and Shacham H: Fast variants of RSA. RSA laboratories 2002.

Prof. M. Padmavathamma M.Sc, M.Phil, M.Ed, Ph.D, M.S.
Currently working as Head, Department of computer Science, S.V.University, Andra Pradesh, India. Her research interests lie in the areas of number theory, Cryptography, Network Securiity, Distributed Systems and privacy Preserving data Mining. She Published 25 research papers in national/international journals and conferences. She published two twxt books as one of the authors. Also she is life member of Cryptology research society of india(CRSI) and andra Pradesh Association Mathematical teachers(APAMT).

M. Sreedevi M.CA,M.Phil,(Ph.D)
Currently working as a Assistant Professor, Department of Computer Science, S.V.University, Tirupati