A New Variant Blind Multisigature Scheme

*M.Sreedevi and **Prof. M.Padmavathamama

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, Multisigature 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 J2 (n). We briefly discussed the possibility and validity and security analysis of this new scheme.

2. Jordan Totient function J2 (n)
2.1 Definition
Jordan Totient function of index 2 is denoted by J2 (n) and is defined as

\[ J_2(n) = n^2 \prod_{\substack{p \mid n \nmid \frac{n}{p}}} \left( 1 - \frac{1}{p^2} \right), n \in \mathbb{Z}^+ \]

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

\[ J_2^*(n) = n^2 \prod_{\substack{p \mid n \nmid \frac{n}{p}}} (1 + p^{-2}), n \in \mathbb{Z}^+ \]

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
   \[ J_2(p) = (p^2 - 1) \]
   \[ J_2(p^a) = p^{2a-1}(p^2 - 1) \]
4. If \( n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_r^{\alpha_r} \) then
   \[ J_2(n) = p_1^{2(\alpha_1-1)} \cdot p_2^{2(\alpha_2-1)} \cdot \ldots \cdot p_r^{2(\alpha_r-1)} \cdot (p_1^2 - 1) \cdot (p_2^2 - 1) \cdot \ldots \cdot (p_r^2 - 1) \]

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

\[ a^{J_2(n)} \equiv 1 \pmod{n} \]

2.6 Theorem
Suppose \( p_1, p_2, \ldots, p_r \) are any r distinct positive prime numbers and \( n = p_1p_2\ldots p_r = n \), if \( a \) be any positive integer such that gcd (a, n) = 1 then

\[ a^{J_2(n)} \equiv 1 \pmod{n} \]

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 SKA and PKA respectively.

Signature generation: Using her private key SKA, Alice creates a signature ‘\( \sigma \)’ on her message M.

Signature verification: Having obtained the signature ‘\( \sigma \)’ and the message M from Alice, the verifier Bob...
checks whether ‘σ’ is a genuine signature on M using Alice’s public key PKA. 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. J₂ -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 J₂(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 
   \( J_\text{2}(n) = (p^2 - 1)(q^2 - 1) \)
2. Select two vectors \(< e_1, e_2, \ldots \ldots \ldots e_r >\) and \(< d_1, d_2, \ldots \ldots \ldots d_r >\) whose inner product satisfies the property
   \( e_i d_1 + e_2 d_2 + \ldots \ldots \ldots + e_r d_r \equiv 1 \pmod{J_\text{2}(n)} \)

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

Encryption: Given plaintext M and the public key = \( (n, < e_1, e_2, \ldots \ldots \ldots e_r>) \) compute the cipher text vector \( C = < c_1, c_2, \ldots \ldots \ldots, c_r > \) by using the formula
\[ c_i \equiv M^{e_i} \pmod{n} \]

Decryption: Given a cipher text vector \( C = < c_1, c_2, \ldots \ldots \ldots, c_r > \) and the private key = \( (n, < d_1, d_2, \ldots \ldots \ldots, d_r>) \) compute the plaintext M by using the formula.
\[ \prod_{i=1}^{r} c_i^{d_i} \equiv \prod_{i=1}^{r} (M^{e_i})^{d_i} \pmod{n} \]

5. The J₂-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 J₂-ERSA based blind multi signature scheme.

Suppose that there are signers \( A_i \)'s \( 1 \leq i \leq r \), 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 
   \( J_\text{2}(n) = (p^2 - 1)(q^2 - 1) \)
2. Select two vectors \(< e_1, e_2, \ldots \ldots \ldots e_r >\) and \(< d_1, d_2, \ldots \ldots \ldots d_r >\) such that their inner product satisfies the equality
   \( e_i d_1 + e_2 d_2 + \ldots \ldots \ldots + e_r d_r \equiv 1 \pmod{J_\text{2}(n)} \)
   Where \( \gcd(e_i, e_j) > \alpha, i \neq j \) and \( \alpha \equiv 1 \pmod{4} \)
3. The KGC publishes n and distributes \( e_i \) and \( d_i \) to each \( A_i, 1 \leq i \leq r \), as his public and private keys respectively.

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

Blind Multi Signature Generation:

Suppose B wants \( A_i \), \( 1 \leq i \leq r \), to sign a message M blindly, where \( M \in \mathbb{Z}_n \)

\[ \prod_{i=1}^{r} c_i^{d_i} \equiv \prod_{i=1}^{r} (M^{e_i})^{d_i} \pmod{n} \]
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 $1 \leq i \leq r$, B computes

$$R_{i1} \equiv p^i M \pmod{n}$$

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

And sends $(R_{i1}, R_{2i})$ to $A_i$.

3. Once receiving $(R_{i1}, R_{2i})$ from B, each $A_i, 1 \leq i \leq r$ computes $W_{i1} \equiv R_{i1}^d \pmod{n}$

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

As his blind signature for $M$. Then he sends $(W_{i1}, W_{2i})$ back to B.

4. After receiving all pairs $(W_{i1}, W_{2i})$ from $A_i, 1 \leq i \leq r$, B computes $W_1, W_2$ and $T$ as

$$W_i \equiv \prod_{i=1}^{r} W_{i1} \pmod{n}$$

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

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

Where T is served as the blind multi signature of $M$ from $A_i, 1 \leq i \leq r$ 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 $A_i, 1 \leq i \leq r$ computes $W_{i1}$ and $W_{2i}$ with his genuine private key $d_i$, then in step (4) we will have

$$W_i \equiv \prod_{i=1}^{r} W_{i1} \equiv p^{d_1 e_{i1} + e_{i2} + \cdots + e_{it}} M^{-d_1 e_{i2} + \cdots - d_t} \pmod{n}$$

$$W_2 \equiv \prod_{i=1}^{r} W_{2i} \equiv q^{e_{i1} + e_{i2} + \cdots + e_{it}} M^{d_1 e_{i2} + \cdots - d_t} \pmod{n}$$

$$T \equiv p^{-1} W_1 \equiv M^{d_1 e_{i2} + \cdots - d_t} \pmod{n}$$

Accordingly if $W_1 W_2 \equiv pq \pmod{n}$ holds the blind multi signature $T$ for the message $M$ is indeed verified.

The security of the above proposed scheme is based on the J2 – 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 $\geq 3$. 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**


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 Security, Distributed Systems and privacy Preserving data Mining. She Published 25 research papers in national/international journals and conferences. She published two text 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