International Journal of Engineering Science Invention
ISSN (Online): 2319 – 6734, ISSN (Print): 2319 – 6726
www.ijesi.org Volume 2 Issue 1 ǁ January. 2013 ǁ PP.18-22

A Model On Dynamic Threshold Proxy Digital Signature Scheme By Using Pell's Equation With Jacobi Symbols For Multimedia Authentication

[1]M Kondala Rao, [2]P S Avadhani, [3]D Lalitha Bhaskari, [4]K V S S R S S Sarma

[123]*Department of Computer Science and Systems Engineering, Andhra University, India*
[4]*Department of Computer Information Science, University of Hyderabad, Hyderabad, India*

ABSTRACT: *In this paper we propose a model on dynamic threshold digital signature scheme by using Pell's Equation with Jacobi symbols to authenticate multimedia content. Multimedia authentication deals with genuineness of the structure and content of the multimedia such as text, image, audio, video etc. The proposed scheme uses an efficient key distribution scenario where, the private key of the group is distributed as unique shares among the group members. The shares are calculated and distributed based on the ID of the group members by using efficient Pell's equation with Jacobi symbols in threshold digital signature scheme. This paper demonstrates algorithms for key generation, encryption and decryption based on Pell's equation with Jacobi symbols.*

Keywords - *Digital Signature, Threshold Signature, Multimedia Authentication, Pell's Equation, Secret Sharing.*

I. INTRODUCTION

In recent times, the usage of multimedia data and its exchange have increased enormously. In order to ensure trust worthiness, multimedia authentication technique [1] is to be used. It protects multimedia data by verifying the information integrity, the alleged source of data and the reality of data. The multimedia data includes text documents, images, video, audio clips, etc. We propose a multimedia authentication technique using Pell's threshold digital signature. It deals with proving the genuineness of the structure and also on the content of multimedia data.

In cryptography, a digital signature [2] or electronic signature scheme is a type of asymmetric cryptography. It will attach the attributes of the signer to the e-document. A valid digital signature gives a recipient reason to believe that the message was created by a known share, and that it was not altered in transit. Digital signature schemes normally use two keys: private key or secret key and the public key. The private key is used to sign the multimedia document and the public key is used to verify the signature. The public key is usually exposed directly to the group members. The private key is securely shared as a secret among the group members. The digital signature scheme provides authentication, integrity and confidentiality of the multimedia information. The existing Digital Signature Scheme (DSS) [3] which is based on discrete logarithm problem can only be used for signature generation/verification and cannot be used for multimedia authentication purposes. Also the verification process is very slow. Hence, we propose a scheme based on Pell's Equation for key generation, generation/verification of signature and it can also be used for encryption.

The idea of threshold cryptography is to protect information by fault tolerant distribution among a cluster of cooperating computers.

Secret sharing scheme [9, 10] refers to the method of distributing a secret/private key among the group members. Each member will receive a unique share of a secret/private key. The secret can be reconstructed with a sufficient number of shares given by the group members. The shares are reconstructed by using Pell's polynomial. Individual shares are of no use on their own. The computed shares are given to the group member based on their ID.

The proposed technique addresses the above problems and enhances all the basic security requirements such as authentication, confidentiality, non-repudiation and message integrity with an efficient threshold digital signature scheme. The goal of multimedia authentication is to authenticate the content alone and the specific representation of the information is not taken into consideration. The secret sharing scheme used here is modified by calculating the individual shares based on unique ID given to the group members.

II. PRAPOSED SCHEME

A. Pell's Equation on threshold digital signature

A threshold digital signature scheme based on Pell's Equation algorithm[11] is presented in this section. The scheme can be used to generate the group private and public keys, signature generation and verification and for encryption and decryption process.

B. Pell's Equation

In number theory, for any constant integer D the equation $x^2 - D y^2 \equiv 1$ is called the Pell's equation. This has many applications in various branches of science. The set of all pairs(x, y) describes cyclic group G_p over the Pell's equation $x^2 - D y^2 \equiv 1 \pmod P$, where P is an odd prime.

The properties are also found in the group G_N over the Pell's equation $x^2 - D y^2 \equiv 1 \pmod N$, where N is a product of two primes. This group G_N then developed to be a public key crypto scheme based on Pell's equations over the ring Z_N^*.

From the group G_N, we find a group isomorphism mapping $f : G_N \rightarrow Z_N^*$ such that a solution (x, y) of the Pell's equation $x^2 - D y^2 \equiv 1 \pmod N$, can easily be transformed to unique element u in Z_N^*. This implies that the plain texts/cipher texts in the in the group G_N can easily transformed to the corresponding plain texts/cipher texts in the RSA scheme.

Let p be an odd prime and D be a non zero quadratic residue element modulo p, which we denote if with Fp. Gp the set of solutions $(x, y) \in F_p \times F_p$ to the Pell equation

$$x^2 - D y^2 \equiv 1 \pmod P.$$

We then define an addition operation " $\oplus$ " on G_p as follows.

If two pairs (x_1, y_1), $(x_2, y_2) \in G_p$, then the third pair (x_3, y_3) can be computed as

$$(x_3, y_3) \equiv (x_1, y_1) \oplus (x_2, y_2)$$
$$\equiv (x_1 x_2 + D y_1 y_2, x_1 y_2 + x_2 y_1) \pmod P.$$

It is easy to verify that the Gp together with the operation " $\oplus$ " is an abelian group with the identity element by (1, 0) and the inverse of the element (x, y) by (x,-y). Further it can be proved that <Gp, $\oplus$ > is a cyclic group of order p-1. Now we want to prove that the group Gp is isomorphic to Fp*, Where Fp*, is all non-zero elements of Fp denotes a multiplicative group of Fp.

Theorem1:

G_p together with the operation " $\oplus$ " is a cyclic group of order p-1. Now we want to prove that the group Gp is isomorphic to F_p^*, where F_p^* denotes a multiplicative group of F_p.

Theorem2:

Two groups G_p and F_p^* are isomorphic Now we define another operation " $\otimes$ " as follows :

$$i \otimes (x, y) = (x, y) \oplus (x, y) \oplus \ldots\ldots\ldots \oplus (x, y) \text{ i times over } G_p.$$

If $(x_i, y_i) = i \otimes (x_i, y_i)$, we expand the above expression and have

$$x_i = \sum_{\substack{0 \le k \le i \\ k \text{ is even}}} \binom{i}{k} D^{\lfloor k/2 \rfloor} x^{i-k} y^k ;$$

$$y_i = \sum_{\substack{0 \le k \le i \\ k \text{ is odd}}} \binom{i}{k} D^{\lfloor k/2 \rfloor} x^{i-k} y^k$$

According to the definition of the mapping f, we have

$$f((x_i, y_i)) \equiv x_i - a\, y_i$$
$$\equiv \sum_{\substack{0 \le k \le i \\ k \text{ is even}}} \binom{i}{k} D^{\lfloor k/2 \rfloor} x^{i-k} y^k - a \sum_{\substack{0 \le k \le i \\ k \text{ is odd}}} \binom{i}{k} D^{\lfloor k/2 \rfloor} x^{i-k} y^k$$

$$\equiv \sum_{\substack{0\le k\le i \\ k\,even}} \binom{i}{k} D^{\lfloor k/2 \rfloor} x^{i-k} y^{k} + \sum_{\substack{0\le k\le i \\ k\,odd}} \binom{i}{k} D^{\lfloor k/2 \rfloor} x^{i-k} (-a\,y)^{k}$$

$$\equiv (x-ay)^{i}$$

Because Gp is a cyclic group of order p-1, we have that if $k \equiv 1 \pmod{P-1}$, then $(x,y) = k \otimes (x, y)$, for all $(x, y) \in G_p$

Let N be a product of two large primes p and q. Zn^* denotes a multiplicative group of Z_N. From the above theorem, it is easy to develop the following theorem.

Theorem3:

The mapping $f: G_N \rightarrow Z_N^*$ satisfying $f((1,0)) \equiv (1 \bmod N)$, $f((x, y)) \equiv x - ay \pmod N$, where $(x, y) \in G_N$ and $a^2 \equiv D \pmod N$, is a group isomorphism . Its inverse mapping $f^{-1}(1) \equiv (1,0) \pmod N$, $f^{-1}(u) \equiv ((u + u^{-1})/2, (u^{-1} - u)/2a \pmod N$, where $u \in Z_N^*$.

Considering equations 4 and 5, we have the following results over the ring Z_N^*.

Theorem 4:

If $(X_i, y_i) = i \otimes (x, y)$, over G_N, we have $x_i - a\,y_i = (x - ay)^i \pmod N$.

Theorem 5:

If $k \equiv 1 \bmod (l.c.m\,(p-1, q-1))$, we have $(x, y) = k \otimes (x, y)$, for all $(x, y) \varepsilon G_N$

Legendre symbol:

Let a be an integer and p > 2 a prime, Define the Legendre Symbol $(a/p) = 0, 1, -1$ as follows

$$(a/p) \quad (a/p) = \begin{cases} 0 & if\ p\ divides\ a \\ 1 & if\ a\ is\ QR\ mod\ p \\ -1 & if\ a\ NQR\ mod\ p \end{cases}$$ One way to

Jacobi Symbol :

If p is a positive odd integer with prime factorization

$$P = \prod_{i=1}^{r} p_i^{ai}.$$

The Jacobi symbol (n / p) is defined for all integers n by the equation

$$(n / p) = \prod_{i=1}^{r} (n / p_i)^{ai}$$

where (n / p_i) is the legendre symbol.

C. Key Generation:

Assume that the Shares to send messages E (chipper text) and Group member case receive the messages E and M.

1. Shares choose two primes P and q $(p \neq q)$
2. put $\eta_p = p \bmod 4$ and $\eta_q = q \bmod 4$ where $\eta_p, \eta_q \in \{1,-1\}$
3. Find non square integer D > 0 such that Legender symbols

$$(D/p) = -\eta_p \quad \text{and} \quad (D/p) = -\eta_q$$

4. Shares compute n = p*q and m= (p-η_p) (q-η_q) / 4
5. Select a integer value for S such that the jacobi symbol

((S^2- D)/n) = -1. As there are closely to $\varphi(n) / 2 \equiv$ such values of S.

6. Select a integer value for e such that (e, m)=1. and makes {n, e, S, D} as public.
7. Solve de ≡ (m+1)/2 mod m for d and keeps as private key
8. D is Key for the Cipher Text.

D. Encryption:

The Shares changes the messages M to E.

1. Shares create M be a message to communicate / encrypt
2. Shares compute $j_1 = (M^2-D)/n$
3. If $j_1 = 1$ go to step (4) else go to step (6)
4. Shares compute $x \equiv (M^2+D) / (M^2-D) \pmod n$
   And $y \equiv 2M / (M^2-D) \pmod n$
5. Go to step (8)
6. If $j_1 = -1$ go to step (7) else go to stop().
7. Shares compute $x \equiv ((M^2+D)(S^2 + D) + 4DMS) / ((M^2-D)(S^2- D)) \pmod n$
   And $y \equiv (2S(M^2+D) + 2M(S^2 + D)) / ((M^2-D)(S^2- D)) \pmod n$
8. Shares compute $j_2 = x \pmod 2$ where $j_2 \in \{0, 1\}$
   (nothing that $x^2 - Dy^2 = 1 \pmod n$ for these values of x,
   y and assume that $(y, n) = 1$)
9. Put $X_l = x$ and $Y_l = y$
10. Shares compute $(X_{l+1}, X_l) \pmod n$ such that

    if $i \neq j$

    $X_{i+j} = X_j + D Y_i Y_j$ and $Y_{i+j} = X_i Y_j + X_j Y_i$

    if $i = j$

    $X_{2i} = X_i^2 + D Y_i^2$ or $2X_i^2 - 1$ and $Y_{2i} = 2 X_i Y_i$
11. Shares compute $E = DYX_l (X_{l+1} - x X_l)^{-1} \bmod n$ (here E is the cipher text) with $0<E<n$
12. Send the {E, j_1, j_2) = cipher text.

E. Decryption

After shares the ciphertext (E, j_1,j_2), the group member checks that $x^2 - D y^2 \equiv 1$
If yes, group member can continue

1. Group member compute $X_{2l} = (E^2 + D) / (E^2 - D) \pmod n$ and
   i. $Y_{2l} = (2E / (E^2 - D)) \pmod n$
2. Group member compute $X_d (X_{2e}) \equiv X_{2de} (x) \pmod n$ and
   i. $X_{d+1} (X_{2e}) \equiv X_{2de+2e} (x) \pmod n$
   ii. We have $X_{2ed} = \sigma x \pmod n$ and $j_2 \equiv x \pmod 2$
3. Group member compute σ and therefore determines x (mod n)

And find $y \equiv \sigma Y_{2de} \equiv \sigma (X_{2de+2e} - X_{2e} X_d) / DX_{2e} \bmod n$

we have $t \equiv x + y\sqrt{D} \bmod n$

Compute t^1 such that

$t^1 = t$ if $j_1 = 1$ else if $j_1 = -1$

$t^1 = t (S-\sqrt{D}) / (S+\sqrt{D})$

And $t^1 = (M+\sqrt{D}) / (M - \sqrt{D}) \bmod n$

4. Group member compute $M \equiv (t^1+1)(\sqrt{D}) / (t^1-1) \pmod n$

The Shares sends message (M) to key generation function that produces a secure private key (D). This private key is then encrypted with public key cryptosystem using the shares private key to form the result. Both the message and the result are prepended and then transmitted. The group member takes the message (M) and produces a secure private key (D). The group member also decrypts the result using the shares public key. If the

calculated secure private key (D) matches the decrypted results, the result is accepted as valid. Because only the dealer knows the private key and only the dealer could have produced a valid result.

III. CONCLUSION

In this paper, we introduce a threshold digital signature scheme which can be used for authenticating the shares and also the multimedia message. The private key of the group is shared as a secret among the group. The person acting as a share can reconstruct the private key and share the multimedia message by signing the document with the group private key. The group private key is updated when the threshold property violates. Each unique key shares and public key of the group members are distributed based on their ID. Thus the proposed scheme ensures the authenticity, integrity, non-repudiation and secret sharing for multimedia message.

REFERENCES

Ching-Yung Lin and Shih-Fu Chang. 2003 Robust Digital Signature for Multimedia Authentication: A Summary in Info lab Technical Report Series, no. 17.

[1] N. Gupta Kailash, N. Agarwala Kamlesh, and A. Agarwala Prateek Digital Signature: Network Security Practices. ISBN 81-203-2599-0

[2] Danni Liu, XingweiWang, Lei Guo, and Min Huang. 2007 A Dynamic (t, n) Threshold Signature Scheme with Provable Security in IEEE International conference on Future Computer and Communication, pages V3–322–V3–325.

[3] Raman Kumar and Harsh Kumar Verma.2010 An Advanced Secure (t, n) Threshold Proxy Signature Scheme Based on RSA Cryptosystem for Known Signers in IEEE 2nd International Conference on Advance Computing Conference (IACC), pages 293–298, 2010.

[4] W. Xiaoming, Z. Zhen, and F. Fangwei. 2006 A Secure Threshold Proxy Signature Scheme in Journal of Electronics and Information Technology, 28:1308–1311.

[5] C. Wang, C. Chang, and C. Lin. 2000 Generalization of threshold signature and authenticated encryption for group communications in IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 83:1228–1237.

[6] G. Li, X. Xin, and W. Li. 2008 Digital Signature Scheme with a (t, l) Threshold Subliminal Channel Based on RSA Signature Scheme in proceedings on International Conference on Computational Intelligence and Security, 2:342–346.

[7] J. Lee. Threshold signature scheme with multiple signing policies in Proceedings-Computers and Digital Techniques, 148:95– 99.

[8] Adi Shamir. 1979 How to Share a Secret in Communications of the ACM, 22:612–613.

[9] Feng Shen, Chonglei Mei, and Hai Jiang. Secret Sharing with Extended Coefficient Use for Improved Data Capacity in IEEE SoutheastCon 2010, pages 119–122.

[10] Michael J.JacobSon and Jr.Hugh C.Williams 2009 Solving the Pell Equation, pages 353-359.