International Journal of Research in Engineering and Science (IJRES)
ISSN (Online): 2320-9364, ISSN (Print): 2320-9356
www.ijres.org Volume 1 Issue 1 ǁ May. 2013 ǁ PP.17-20

An Identity Based Encryption Scheme based on Pell's Equation With Jacobi Symbol

Department of Computer Science and Systems Engineering, Andhra University, India
Kondala Rao M, kondalaraom@gmail.com
Department of Computer Science and Systems Engineering, Andhra University, Visakhapatnam, India
P S Avadhani, psavadhani@yahoo.com
Department of Computer Science and Systems Engineering, Andhra University, Visakhapatnam, India
D Lalitha Bhaskari, lalithabhaskari@yahoo.co.in
Department of Computer Information Science, University of Hyderabad, Hyderabad, India
K V S S R S S Sarma, kss@uohyd.ernet.in

Abstract:- In this paper, we propose a novel public key cryptosystem in which the public key of a subscriber can be chosen to be a publicly known value, such as his identity. Identity based encryption scheme developed is a public key cryptosystem and it is based on Pell's equation. This paper demonstrates algorithms for key generation, encryption and decryption based on Pell's equation with Jacobi symbol.

Keywords:- pells equation, Legendre symbol, Jacobi symbol, permanent private secret.

I. INTRODUCTION

In an offline public key system, in order to send encrypted data it is necessary to know the public key of the recipient. This usually necessitates the holding of directories of public keys. In an identity based system a user's public key is a function of his identity (for example his email address), thus avoiding the need for a separate public key directory. The possibility of such a system was first mentioned by Shamir[4]. But it has proved difficult to find implementations that are both practical and secure, although recently an implementation based on elliptic curves has been proposed[3]. This paper describes an identity based cryptosystem which uses Pell's equation.

The system has an authority which generates a universally available public M. This modulus is a product of two primes p and q held privately by the authority. Also, the system will make use of a universally available secure hash function. Then, if user Alice wishes to register in order to be able to receive encrypted data she presents her identity (e.g. email address) to the authority. In return she will be given a private key with properties. A user Bob who wishes to send encrypted data to Alice will be able to do this knowing only Alice's public identity and the universal system parameters. There is no need for a public key directory.

There were some methods developed in which administer verifies the information, such as RSA. In recent years, because of the development of public key cryptography functions, a new method of verification is accordingly being created. When comparing RSA with Pell's Equation, Proposed scheme is more secure and faster than RSA Public Key Cryptography to achieve the same level of security as Pell's Equation.

II. PROPOSED SCHEME

1.1 Pell's equation based encryption system

Our scheme is based on Pell's equation, and to begin with, we briefly introduced this scheme. We can divide Pell's schemes into four parts, Pell's equation, Key Management, Encryption and Decryption. This scheme also needs a trusted third party can decide the contents of the published information, whereas others can only download without permission to modify it.

1.2 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[1]. 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[2].

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 :

$i \otimes (x, y) = (x, y) \oplus (x, y) \oplus \ldots\ldots\ldots \oplus (x, y)$ 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

$$f((x_i, y_i)) \equiv x_i - a\, y_i$$

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

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

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

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 $u \in Z_N^*$.

Theorem 4:

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

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

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{if p divides a} \\ 1 & \text{if a is QR mod p} \\ -1 & \text{if a NQR mod p} \end{cases}$$

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.

1.3 Key Management

In this step, the Bob chooses the Secrete Key Generation[5], and computes and publishes some auxiliary information on the bulletin. The Bob will perform the following steps:

1.3.1 Key Generation:

Assume that the Bob to send messages E (cipher text) and Alice case receive the messages E and M.

1. The Bob chooses two primes p and q $(p \neq q)$

2. The Bob compute $\eta_p = p \bmod 4$ and $\eta_q = q \bmod 4$ where $\eta_p, \eta_q \in \{1,-1\}$

3. The Bob find non square integer D > 0 such that Legender symbols

$(D/p) = -\eta_p$ and $(D/p) = -\eta_q$

4. The Bob compute $n = p * q$ and $m= (p+\eta_p)(q+\eta_q) / 4$

5. The Bob 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. The Bob select a integer value for e such that (e, m) =1. and makes {n, e, S, D} as public.

7. The Bob compute $d * e \equiv (m+1)/2 \bmod m$ for d and keeps as private key

8. D is Key for the Cipher Text.

1.4 Encryption:

The Bob changes the messages M to E.

1. The Bob get the M be a message to communicate / encrypt
2. The Bob compute $j_1 = (M^2-D)/n$
3. The Bob compare If $j_1 = 1$ go to step (4) else go to step (6)
4. The Bob 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. The Bob compare If $j_1 = -1$ go to step (7) else go to stop().
7. The Bob 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. The Bob 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. The Bob Put $X_l = x$ and $Y_l = y$
10. The Bob 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 $2\, X_i^2 - 1$ and $Y_{2i} = 2\, X_i\, Y_i$

11. The Bob 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.

1.5 Decryption

After receiving the ciphertext (E, j_1, j_2), the Alice checks that $x^2 - D\, y^2 \equiv 1$

If yes, Alice can continue

1. The Alice compute

$X_{2l} = (E^2 + D) / (E^2 - D) \pmod n$ and

i. $Y_{2l} = (2E / (E^2 - D)) \pmod n$

2. The Alice 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. The Alice 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. The Alice compute

$M \equiv (t^1+1)\,(\sqrt{D}) / (t^1-1) \pmod n$

The Bob 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 Bob's private key to form the result. Both the message and the result are prepended and then transmitted. The Alice takes the message (M) and produces a secure private key (D). The Alice also decrypts the result using the Bob's public key. If the calculated secure private key (D) matches the decrypted results, the result is accepted as valid. Because only the Bob knows the private key and only the Bob could have produced a valid result.

III. CONCLUSION

In this paper, we have proposed an Identity based encryption scheme using Pell's equation with Legendre and Jacobi symbols. This scheme is a multi-use scheme, which means every Alice only needs to keep one private secrete. The Alice just use the public information and their own private information to get the information back. When then identity is changed, the Bob only needs to adjust the private key. And one of the benefits of this scheme is that the Bob will not ask for some extra information from all the Alice while in the information updating stage. We also show how to verify the information which comes from other Alice. Furthermore, because this scheme is constructed on the pells equation, we attain a much higher level of security comparing with the original public key problem in the same bits length.

REFERENCES

[1]. Chen C.Y., Chang C.C. Yang W.P.,"*Fast RSA type cryptosystem based on Pell equation"*, Proceeding of International Conf. On Cryptology and Information Security Taiwan, Dec.1-5, 1996

[2]. C Cocks Split "*Generation of RSA Parameters with multiple participants"* proceeding of 6th IMA conference on Cryptography and Coding, Spring LNCS 1355.

[3]. A. Shamir, *"Identity- Based Cryptosystems and Signature schemes advances in Cryptology*" – Proceeding of Crypto'84.

[4]. D. Boneh and M. Franklin, "*Identity-based encryption from the Weil paring*," Advances in Cryptology-Crypto'2001, Lecture Notes on Computer Science 2139, Springer-Verlag (2001), pp.213-229.

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