Public Key Cryptography for mobile payment

T K Mohanta[1], R K Samantaray[2], (Dr) R P Panda[3]

1. Dept.of Electronics & Communication Engg, Sudhananda Engg & Research center, Bhubaneswar, Odisha, India.
2. Dept.of Electronics & Communication Engg, REC, Bhubaneswar, Odisha, India.
3. Vssut, Burla, Odisha, India.
samantaray.ranjan75@gmail.com

Abstract: Since the mobile systems are growing quickly, the e-commerce will change gently to m-commerce. As a result, mobile security will become the one of the most important part of mobile system and will become the hottest area facing the mobile payment due to mobile networks directness. However, the appropriate encryption scheme for mobile communication must have small amount of data calculating and quick operation as of its inherent restrictions of small quantity and low calculating ability. The objectives of this paper are to look at mobile payment and its security. Also, to explain elliptic curve with public key encryption, authentication of security wireless milieu. Compare with the RSA scheme, an elliptic curve has shorter key size, smaller signature length, low calculating, fast operations and high security working.
[T K Mohanta, R K Samantaray, R P Panda. **Public Key Cryptography for mobile payment.** *Researcher* 2013;5(5):9-13]. (ISSN: 1553-9865). http://www.sciencepub.net/researcher. 2

Keywords: RSA, elliptic curve scheme, digital signature, encryption and decryption.

1. INTRODUCTION

As indicated by the mobile payment report (IEEE IRI, 8-10), mobile payment is defined as a new transaction payment method employing a mobile terminal on the existing tools for example wireless LAN and Bluetooth. Also, the mobile payment as an important part of m-commerce is defined as the process of two participants exchanging monetary values employing a mobile device in response for merchandise or services, [1]. Mobile security is considered to be a major issue for mobile payment that can be faced through sensitive payment. Actually, there are many research papers discussing businesses markets, payment processing and payment schemes [2, 4], out in fact there are a few papers that deal with the construction of wireless payment schemes, involving protocols and security protection solutions [5, 6, 8].

2. PROBLEM FORMULATIONS

As stated by the Wireless World report [11], mobile payment on wireless solutions will give great business opportunities in the upcoming years. But, with new challenges mobile security is one of the most critical, and difficult challenges to mobile payment. To construct secured wireless payment scheme and to support mobile payment transactions becomes a hot area of research; we should keep the user with the sensitive and transaction data and in the state of security and confidentiality. Give facts and mechanism to solve the challenge if either the client or the merchant declines the transaction. Therefore, generating secure and cost effective wireless payment scheme to aid mobile device by not just gives great business opportunities, but also carries new practical challenges and issues.

3. PROBLEM SOLUTIONS

The appropriate solution for mobile communication equipment is public key encryption but must have a small amount of data calculating and fast operations because of its small volume and low calculating ability.

3.1 Mobile Payment Scheme

Secure milieu for mobile payment scheme is shown in figure 1. It includes seven components: customer, merchant, mobile network operator (MNO), bank, trusted authority (TA), information center (IC) and certificate authority (CA). Time stamping server (TSS) gives notarization from the neutral viewpoint if challenge happens. The system is relied on the SEMOPS (Secure Mobile Payment Service), but enhancements to the SEMOPS are made to deal with the signature validation and confidentiality issues. In the system, MNO can be work as the user payment processor in addition to the role of wireless access provider. In general, the bank is the customer accounts holder. So the bank is more appropriate as the payment processor. TA is the part, where CA and TSS, to give notarization from the neutral viewpoint if challenge happens. IC is similar as in SEMOPS; it is in charge for routing and distributing notifications to recipient payment processor.

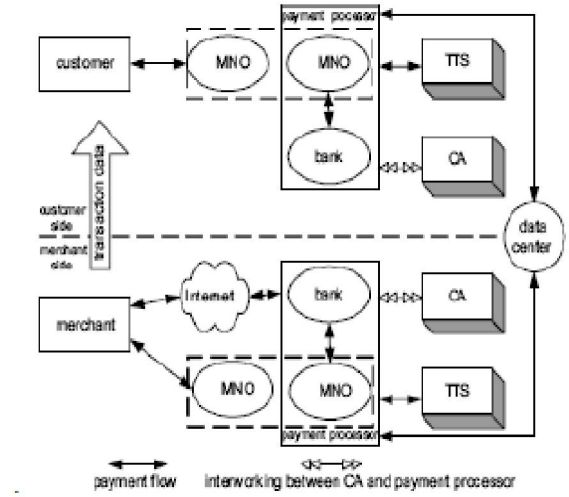

Figure 1: mobile payment scheme

3.2 Public Key Cryptography

Symmetric cryptography has a weakness; two individuals who want to exchange secret messages should share a common secret key. The key should be exchanged in a protected channel, and not via the way they would generally communicate. This is mostly inconvenient, and asymmetric cryptography gives a choice. In public key cryptography there are two keys employed, an exponent key and a private key, the exponent for encryption and the private for decryption respectively. It should be hard to obtain the private key from the exponent key. This denotes that an entity can freely send their exponent key out over an unsafe channel and however be certain that only they can recover messages encrypted with it. Public key cryptography is typically relied on difficult computational problems. RSA, for instance, bases on the guessed intricacy of factoring. For efficiency purposes, hybrid encryption schemes are employed in practice; the key is exchanged employing a public key encryption, and the rest of the communication is encrypted employing the symmetric key encryption which is naturally much quicker. Elliptic curve encryption is a form of public key encryption that can provide efficiency acquires over other schemes. In addition asymmetric cryptography offers methods for digital signature, which is a way to create high trust under the assumption that the applicable private key will not be compromised in any means in which a message received is sent via the claimed sender. Such signature is, in principle via implicit inference, as the digital equivalent of handwritten signatures on paper messages. In a practical meaning, there is no physical communication or association between the signer and the signed. Properly utilized high quality designs and implementations will able of a very high level of assurance, likely exceeding any but the most careful handwritten signature. For instance, digital signature schemes such as ElGamal and DSS digital signatures are keys to the function of public key infrastructure and many others network security protocols for example Kerberos and Virtual Private Network (VPN). Cryptography hash functions create a hash of a message. While it must be easy to calculate, it should be too hard to inverse one-way, though other characteristics are generally wanted too. For example, MD5 and SHA-1 are well known hash methods. Also, Message authentication code (MAC) known as based-hash function, is similar to hash function, except that the key is required to calculate the hash. As the name proposed, they are usually employed for message authentication. They are generally built from other primitives, like block ciphers or stream ciphers. Unlike symmetric cryptography, public key encryption is appropriate to a large scale base, in theory letting secure and authorized communication between any two individuals in anywhere.

3.3 Standard RSA Scheme

Public key cryptography has an advantage over traditional cryptography in key transmission and management. In 1978, RSA [8] developed a public key cryptosystem that is based on the difficulty of integer factoring. The RSA public key encryption scheme is the first example of a provably secure public key encryption scheme against chosen massage attacks. Assuming that the factoring problem is computationally intractable and it is hard to find the prime factors of n = p *q . The RSA scheme is as follows:

Key generation algorithm

To generate the keys entity A must do the following:

1. Randomly and secretly choose two large prime numbers p and q with equally likely.
2. Compute the modulus n = p * q .
3. Compute Ø(n) = (p -1)(q -1)
4. Select random integer e,1 < e < n where gcd(e,Ø) =1
5. Use Baghdad method [17] to compute the unique decrypted key d,1 < d <θ (n) where e * d 1mod Ø(n)
6. Determine entity A public and private key. The pair (d,Ø) is the private key. While the pair (n, e) is the public key.

Public key encryption algorithm

Entity B encrypts a message m for entity A which entity A decrypts.

Encryption: entity B should do the following:

- Obtain entity A 's public key (n, e) .
- Represent the message m as an integer in the interval [0...n −1]
- Compute $c= m^e \mod n$
- Send the encrypted message c to entity A .

Decryption: To recover the message m from the cipher text c . Entity A must do the following:

- Obtain the cipher text c from entity B
- Recover the message m= c^d mod n

Example

Key generation: suppose that entity A selects the prime numbers p = 23 and q = 71 . Then he finds the RSA modulus n = p *q = 1633 , Ø(n) = (p -1)(q -1) = 1540 . Entity A chooses e = 23 and using the Baghdad method for multiplicative inverse [18] to find the decrypted key d = 67 where e * d ≅ mod Ø . So A' s public key is the pair (n = 1633, e = 23) while entity A' s private key is (Ø = 1540, d = 67) .

Encryption: Suppose entity B obtain A' s public key (n = 1633) and he determines a message m = 741 to be encrypted, entity B uses repeated square and multiply algorithm [19] of modular exponentiation to compute 741^{23} mod = 1633 = 1109 and send this c = 1109 to entity A .

Decryption: To recover and obtain the original message m entity A should first obtain c = 1109 from entity B then recover the message m = c^d mod n = 1109^{67} mod 1633 = 741 using repeated square and multiply algorithm [18] for exponentiation.

3.4 Elliptic Curve Cryptography

Elliptic curve encryption was introduced in 1985 by Victor Miller and Neil Koblitz as a different scheme for using public key encryption. Public key encryption generates a method for exchanging keys between numbers of entities in a complicated system. Unlike other common schemes such as RSA, elliptic curve cryptography is relied on discrete a logarithm that is harder to face at the same key size [13]. Also, its key bytes are less than RSA scheme. It can allow computer operation and network broadcast is sound and fast, figure 2 shown the key size comparison.

ECC KEY SIZE (Bits)	RSA KEY SIZE (Bits)	KEY SIZE RATIO
163	1024	1 : 6
256	3072	1 : 12
384	7680	1 : 20
512	15 360	1 : 30

Figure 2: NIST Key size comparison for public key

In addition, Elliptic curve cryptography needs less bandwidth, less storage space and less computing time, compared with the other schemes. This lets to apply encryption in platforms that are restricted, such as wireless devices, smart cards, and thin-clients. It also gives a large win in states where efficiency is significant. Elliptic curve cryptography is shown in figure 3.

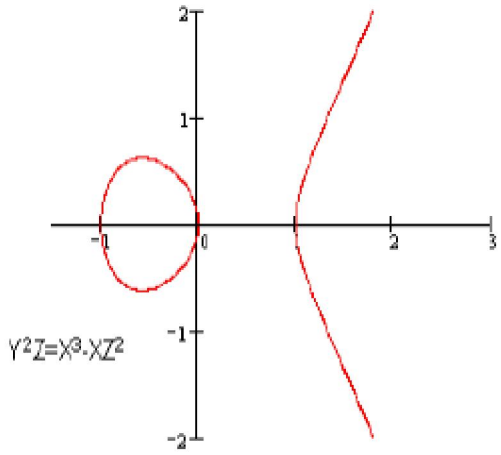

Figure 3: Elliptic curve cryptography

Suppose p is prime number finite field F_p includes p elements 0,1,2...p -1

Addition is: a + b ≡ c mod p (1)

Multiplication is : a *b ≡ c mod p (2)

Law is : $\frac{a}{b}$ namely $a*b^{-1}$ (3)

Unit element is 1, Zero element is 0. The elliptic curve point is defined as:

$$E_p(a,b) = \left\{(x,y)Y^2 = X^3 + ax + b \bmod p\right\}$$ such that $(x, y) \in z_p$ (4)

$z_p = \{0,1,..., p -1\}$

∞, express infinite far point.

a , b are no-negative integer less than p

$4a^2 + 27b^2 \neq 0 \bmod p$

$F_p(a,b)$ is about plus Abelian group

Infinite far point ∞ is zero elements also namely

$\infty + \infty = \infty, \infty + p + \infty = p$

p = (x, y) then its negative element is - p = (x-y) , also namely p+ (-p) = ∞ plus in $F_p(a,b)$ is defined as if $p = (x_1, y_1)$, $q = (x_2, y_2)$ p,q ∈ $F_p(a,b)$ then if $x_1 = x_2$, $y_2 = -y_1$ also satisfying q=-p, p+q= ∞ otherwise p + q= (x_3, y_3) with $x_3 = \lambda^2 - x_1 - x_2 \bmod p$ (5)

$y_3 = \lambda(x_1 - x_3) - y_1 \bmod p$ (6)

$\lambda = \{(y_2 - y_1)(x_2 - x_1)^{-1}$ if p≠q (7)

$\lambda = (3x_1^2 + a)\,(2y_1)^{-1}$ if p=q (8)

In it $(x_2 - x_1)^{-1}$ $(2y_1)^{-1}$ is $x_2 - x_1$ and $2y_2$ multiplication reverse element in F_P.

Elliptic curve cryptography will extensively use in wireless secure communication scheme due to smaller key size, quick signature, less computing, and fast

operating pace. Elliptic curve cryptography acts for a different technique to perform public key encryption, as an alternative to the standard RSA scheme and also provides certain advantages. However, elliptic curve cryptography has the following characteristics :

1. Fastest method compare with other schemes.
2. Use much smaller key size compare with RSA scheme.
3. Provides significant computational advantages

Encryption and Decryption Scheme

Suppose entity A wants to send an encrypted message x to entity B . Thus entity B chooses a large prime p and an integer a mod p . Also, entity B chooses a secret integer i and computes c a p i ≡ mod . Entity B then makes p, a, c public and keeps i secret. Entity A chooses a random k and computes y_1 and y_2 as follows:

$y_1 \equiv a^k \bmod p$
$y_2 \equiv x^* c^k \bmod p$

Enity a sends (y_1, y_2) to entity B , who the decrypts by calculating $x \equiv y_2 * y_1^{-i} \bmod p$. Now we describe the elliptic curve version. Entity B chooses an elliptic curve E mod p where p is a large prime. Entity B chooses a point a on E and a secret integer i .Entity B computes c = a *a(= a + a +...+ a) . The points a and c are made public, while i kept secret. Entity A expresses its message as a point x on E . Entity A then chooses a random integer k , computes y_1 k *a mod p and y_2 = x+ k *c then sends the pair (y_1, y_2) to Entity B . Entity B decrypts by calculating 2 1 x = y − a * y .

Example

We must first generate a curve. Let's use the prime p = 8831 , the point G = (x, y) = (4,11) and a = 3 . To make G lie on the curve $y^2 \equiv x^3 + b^*x + c \bmod p$, we take b = 45 . Entity A has a message, represented as a point P_m= (5,1743) that she wishes to send the entity B . Here is how entity A does it.

Entity B has chosen a random number a_B = 3 and has published the point a_B * G = (413,1808) . Entity A downloads this and chooses a random number k = 8 . Entity A sends to entity B k*G = (5415,6321) and $p_m + k(a_B^*G)$ (6626,3576) . Entity B calculates a_B (k *G) =3(5415,6321) = (673,146) . Entity B now subtracts this from (6626,3578) (6626,3576)-(673,146) =(6626,3576)+(673,-146) =(5,1743) Note that we subtracted points by using the rule P -Q = P + (-Q) .Through encryption communication process, when adversary needs to eavesdrop, can only sees E_p (a, b), c,G, y_1 , y_2 , but, it is very hard to solve k utilizing c,G or solve y by y2 ,G . Therefore, adversary cannot get the original message between entity A and entity B .

Digital Signature Scheme

Digital signatures can ensure the authenticity of transaction participants, integrity, and non-repudiation of transmissions. Elliptic curve cryptography is threatening at the possibility to be the next generation digital signature scheme, also offering a great one way function relying on a different form of computations.

Signing: Entity A needs to sign a message m (which might actually be the hash of a long message). Assume m is an integer. Entity A fixes an elliptic curve E mod p where p is a large prime, and a point A on E . Assume that the number of points n on E has been calculated and assume 0 ≤ m < n (if not, choose a larger p). Entity A also cheeses a private integer i and computes c = i * A . The prime p the curve E , the integer n , and the points A and c are made public. To sign the message, Entity A does the following:

1. Chooses a random integer k with $1 \le k \le n$, gcd(k, n) = 1 , and computes R = kA = (x, y)
2. Computes s k^{-1} (m i-* x)mod n
3. Sends the signed message (m, R, s) to entity B Note that R is a point on E , m and s are integers.

Verification: Entity B verifies the signature as follows:

1. Downloads Entity A public information p, E, n, A, c
2. Computes $v_1 = x^*c + s^*R$ and $v_2 = m^* A$
3. Declares the signature valid if $v_1 = v_2$ The verification procedure works because $v_1 = x^*c + s^*?R = X^*a^* A + K^{-1}(m - a^* x)$ (k*A) = $X^*a^* A + (m - a^* x)^*$ A= $m^*A = V_2$ (9)

There is a subtle point that should be mentioned. We have used k^{-1} in this verification equation as the integer mod n satisfying $K^{-1^*}K \equiv 1 \bmod n$. Therefore, $K^{-1^*}K$ not 1 but rather an integer congruent to1mod n , so $K^{-1^*}K = 1 + t^*n$ for some integer t , it can be shown that $n^*A = \infty$

Therefore,
$K^{-1^*}K\ A=(81+t^*n)^*\ A=A+t^*\ (n^*A) = A + t^*\infty = A$
this shows that k^{-1} , k cancel each other in the verification equation, as we implicitly assumed above.

4 CONCLUSION

In this paper we depicted mobile payment scheme using public key encryption and described the digital signature using elliptic curve encryption. As a result, the suggested security scheme can conquer mobile milieu restrictions and has advantages over existing standard payment schemes.

References

[1] Nambiar, S., and Liang, L., IEEE IRI, 8-10, 475-480, November 2004.

[2] L. Antovski, and M. Gusev, "M-Payments", Proceedings of the 25th International Conference Information Technology Interfaces, 2003 (ITI'03).

[3] S. Nambiar, and T.L. Chang, "M-Payment Solutions and M-Commerce Fraud Management", Retrieved September 9, 2004.

[4] X. Zheng, and D. Chen, "Study of Mobile Payments System", Proceedings of the IEEE International Conference on E-Commerce, 2003 (CEC'03).

[5] S. Kungpisdan, B. Srivnivasan, and P.D. Le, "A Secure Account-Based Mobile Payment Protocol", Proceedings of the International Conference on Information Technology: Coding and Computing, 2004 (ITCC'04).

[6] A. Fourati, H.K.B. Ayed, F. Kamoun, and A. Benzekri, "A SET Based Approach to Secure the Payment in Mobile Commerce", In Proceedings of 27th Annual IEEE Conference on Local Computer Networks (LCN'02), November 06 - 08, 2002, Tampa, Florida

[7] Jerry Gao, Krishnaveni Edunuru, Jacky Cai, and Simon Shim, "P2P-Paid: A Peer-to-Peer Wireless Payment System" Proceedings of the 2005 Second IEEE International Workshop on Mobile Commerce and Services (WMCS'05).

[8] ZHAO Lianggang, CHEN Kefei, "Application of Elliptic Curve Cryptosystem for Security Protocol of Wireless Communication", Computer Engineering, Volume 28 No.3, 2002, pp 128-129, shanghai, China.

3/30/2013