Application Study on Public Key Cryptography in mobile payment

XIAOYAN YANG, XUANPING LI, JIFANG LI
Computer Science and Information Technology College,
Zhejiang Wanli University, Ningbo, 315100
China

Abstract: - With mobile terminal increase, E-Commerce is transforming to M-Commerce. However, mobile security is one of the most urgent, and complex challenges to mobile payment because of mobile networks openness. The suitable cryptosystem of mobile communication equipment should possesses small amount of data calculating and rapid operation velocity because of its inherent limitations of small volume, low calculating capability. The purpose of this paper is to explore mobile payment and security. The paper discribes an elliptic curve methods in enciphering / deciphering , authentication of security wireless environment. Compare to traditional RSA cryptosystem, an elliptic curve has shorter key lengths , shorter signature size , low calculating ,rapid velocity and high security in use. In the final sections we briefly discuss quantum protocol.

Key-Words: - RSA, elliptic curve cryptosystem, quantum cryptography， digital signature, encryption, decryption

1 Introduction

According to Mobile Payment Forum, mobile payment is defined a new terminal transaction payment method using a mobile device on the existing technology such as wireless LAN(IEEE 802.11), Bluetooth and so on .

Mobile payment, a major component of m-commerce, is defined as the process of two parties exchanging financial value using a mobile device in return for goods or services, [1]. Security is regarded as a huge issue for mobile payment that can be challenged during sensitive and confidential payment information handling and transmission.

Although there are a number of papers discussing businesses markets, payment process, payment methods and standards in wireless payment [2][2][3][4], there are a very few papers discussing how to build wireless payment systems, including protocols, design issues,and security solutions[5][6][7][8][9].

2 Problem Formulation

According to the Wireless World Forum, mobile payment on wireless devices will provide excellent business opportunities in the coming years, but also with new challenges. Mobile security is one of the most urgent, and complex challenges to mobile payment. How to build secured wireless payment systems to support mobile payment transactions becomes a hot research topic. Keep the user sensitive information and transaction data in the situation of security and privacy. Provide evidence and mechanism to resolve dispute when either the customer or the merchant denies the transaction.

Therefore, creating secure and cost-effective wireless payment solutions to support mobile device users not only provides good business opportunities, but also brings new technical challenges and issues to engineers. End –to –End security Requirements is shown below.

Authentication: Allow the issuer to verify the consumer credentials. All merchants and mobile customers must be able to trust claimed identities[10].

The recipient should be able to identify the sender, and verify that the purported sender actually did send the message.

Confidentiality: Only an authorised recipient should be able to extract the contents of the message from its encrypted form. Otherwise, it should not be possible to obtain any significant information about the message contents[10][11].

Data Integrity: Ensure that payment data is not should be able to determine if the message has been altered during transmission.

Non-repudiation: Bind the parties to the transaction. Users should not be able to claim that a transaction occurred without their knowledge. The sender should not be able to deny sending the message.

3 Problem Solution

With mobile terminal increase, E-Commerce is transforming to M-Commerce. However, Mobile security is one of important challenges to mobile payment because of mobile networks openness. The suitable cryptosystem of mobile communication equipment should possesses small amount of data calculating and rapid operation velocity because of itself small volume, low calculating capability.

3.1 Mobile Payment System Model

Secure environments for mobile payment is shown in Fig 1. It consists of six elements: customer, merchant, MNO, bank, trusted third party (TTP), DC.

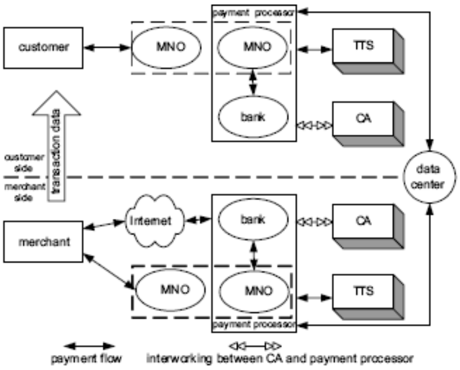


Fig.1 Mobile payment system

As mentioned in the previous section, Mobile Network Operator (MNO),

Certificate Authority (CA), Data Center (DC), TTPs are the elements, such as CA and Time-stamping server (TSS), to provide notarization from the neutral perspective when dispute occurs.

The model is based on the SEMOPS (Secure Mobile Payment Service, www.semops.com), but enhancements to the SEMOPS are made to tackle the signature validating and privacy issues.

In the model, MNO maybe acts as the user payment processor besides the role of wireless access provider. Generally, the bank is the user accounts holder. So the bank is more suitable as the payment processor. TTPs are the elements, such as CA and Time-stamping server (TSS), to provide notarization from the neutral perspective when dispute occurs. Data center is the same as in SEMOPS. It is responsible for routing and delivering notifications to addressee payment processor.

3.2 Public Key Cryptography

Symmetric key encryption has a troublesome drawback — two people who wish to exchange confidential messages must share a secret key. The key must be exchanged in a secure way, and not by the means they would normally communicate. This is usually inconvenient, and public key (or asymmetric) cryptography provides an alternative. In public key encryption there are two keys used, a public and a private key, for encryption and decryption respectively. It must be "difficult" to derive the private key from the public key. This means that someone can freely send their public key out over an insecure channel and yet be sure that only they can decrypt messages encrypted with it.

Public key algorithms are usually based on hard mathematical problems. RSA, for example, relies on the (conjectured) difficulty of factorisation. For efficiency reasons, hybrid encryption systems are used in practice; a key is exchanged using a public key cipher, and the rest of the communication is encrypted using a symmetric key algorithm (which is typically much faster). Elliptic curve cryptography is a type of public key algorithm that may offer efficiency gains over other schemes.

Asymmetric cryptography also provides mechanisms for digital signatures, which are way to establish with high confidence (under the assumption that the relevant private key has not been compromised in any way) that the message received was sent by the claimed sender. Such signatures are often, in law / by implicit inference, as the digital equivalent of physical signatures on paper documents. In a technical sense, they are not as there is no physical contact nor connection between the 'signer' and the 'signed'. Properly used high quality designs and implementations are capable of a very high degree of assurance, likely exceeding any but the most careful physical signature. Examples of digital signature protocols include DSA and ElGamal. Digital signatures are central to the operation of public key infrastructure and many network security schemes (eg, Kerberos, most VPNs, etc).

Cryptographic hash functions produce a hash of a message. While it should be easy to compute, it must be very difficult to invert (one-way), though other properties are usually needed as well. MD5 and SHA-1 are well-known hash functions.

Message authentication codes (MACs), also known as keyed-hash functions, are similar to hash functions, except that a key is needed to compute the hash. As the name suggests, they are commonly used for message authentication. They are often constructed from other primitives, such as block ciphers, unkeyed-hash functions or stream ciphers.

Unlike conventional cryptosystems, public key cryptography is applicable on a large scale base, in principle allowing secure and authorised communication between any two persons in the world.

3.3 RSA Algorithm

By Comparison ,public key cryptography has an advantage over traditional cryptography in key transmission and management.

RSA(Rivest-Shamir-Adleman) is in the following .

Key Generation[12]:

1)Generate two large prime numbers, p and q

2)Let $n = pq$

3)Let $m = (p-1)(q-1)$

4)Choose a small number e, coprime to m

5)Find d, such that $de \% m = 1$

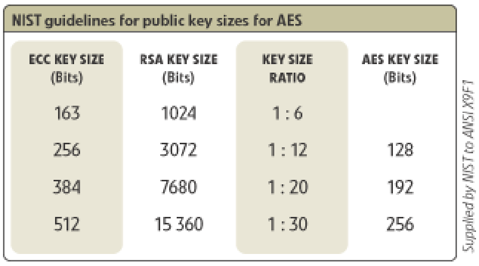
Publish e and n as the public key.
Keep d and n as the secret key.Encryption

Encryption:$C = P^e \% n$
Decryption:$P = C^d \% n$
$x \% y$ means the remainder of x divided by y

3.4 Elliptic Curve Cryptology

Elliptic curve cryptography (ECC) was discovered in 1985 by Victor Miller (IBM) and Neil Koblitz (University of Washington) as an alternative mechanism for implementing public key cryptography. Public key algorithms create a mechanism for sharing keys among large numbers of participants or entities in a complex information system. Unlike other popular algorithms such as RSA, ECC is based on discrete logarithms that much more difficult to challenge at equivalent key lengths[13][14]

In ECC, its key bytes are less than RSA . It can let computer performance and network transmission be good and fast. AS in the following Fig2, [15].



NIST guidelines for public key sizes for AES

ECC KEY SIZE (Bits)	RSA KEY SIZE (Bits)	KEY SIZE RATIO	AES KEY SIZE (Bits)
163	1024	1 : 6	
256	3072	1 : 12	128
384	7680	1 : 20	192
512	15 360	1 : 30	256

Supplied by NIST to ANSI X9F1

Fig 2 Key size comparison

ECC devices require less storage, less power, less memory, and less bandwidth than other systems. This allows you to implement cryptography in platforms that are constrained, such as wireless devices, handheld computers, smart cards, and thin-clients. It also provides a big win in situations where efficiency is important. ECC is shown as follows Fig 3.

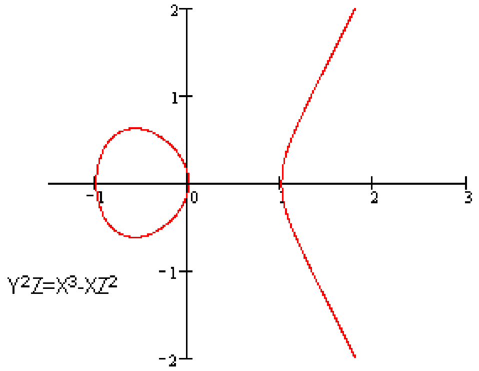


Fig 3 Elliptic curve

Suppose, p is prime number ， a finite field F_p includs p elements: 0， 1， 2…p-1,

plus in F_p is： $a + b \equiv c (\bmod p)$ (1)

Multiplication in F_p is：

$a \times b = c (\bmod p)$ (2)

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

Unit element is 1 in F_p， Zero element is 0。 The elliptic curve on F_p is defined as

$$E_p(a,b) = \left\{ \begin{matrix} (x,y) \mid y^2 = x^3 + ax + b (\bmod p) \\ and \quad (x, y) \in z_p \times z \end{matrix} \right\} \bigcup \infty \quad (4)$$

with $z_p = \{0,1,..., p-1\}$， ∞ expresses infinite far point.

with a and b are no-negative integer less than p and $4a^2 + 27b^2 \neq 0 (\bmod p)$， $F_p(a,b)$ is about plus Abelian group,

Infinite far point ∞ is zero element， also namely $\infty + \infty = \infty, \infty + p = p + \infty = p$

If $p = (x, y)$ ， then its negative element is: $-p = (x, -y), also$ namely $p + (-p) = \infty$

Plus in F_p（a,b）is defined as：

If $p=(x_1,y_1)$, Q=(x_2,y_2) ，

$P,Q\in F_p(a,b)$ then

If $x_1=x_2$， $y_2=-y_1$ also satisfying Q= $-p$， $P+Q=\infty$ ， othwise P+Q=(x_3,y_3) with

$$\begin{cases} x_3=\lambda^2-x_1-x_2(\bmod p) & (5) \\ y_3=\lambda(x_1-x_3)-y_1(\bmod p) & (6) \end{cases}$$

$$\lambda=\begin{cases} (y_2-y_1)(x_2-x_1)^{-1} & P\neq Q \quad （7） \\ (3x_1{}^2+a)(2y_1)^{-1} & P=Q \quad （8） \end{cases}$$

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

ECC will widely use in wireless secure communication protocol because of shorter key length , fast digital signature, small computing, rapid operating speed and so on.

Elliptic Curve Cryptography represents a different way to do public key cryptography—an alternative to the older RSA system—and also offers certain advantages.

ECC security：

1) Relies on elliptic curve logarithm problem Fastest method is “Pollard rho method”

2) Compared to factoring, can use much smaller key sizes than with RSA etc

3) For equivalent key lengths computations are roughly equivalent

4) Hence for similar security ECC offers significant computational advantages.

ECC Encryption/Decryption : Suppose, user A wants to send message M encrypted to B ， user A may execute operations as fellows ：

1)use A chooses an elliptic curve $E_p(a,b)$, namely first take a,b and p ， moreover take elliptic curve a point G(order of G is n, and n is prime number), it is base point.

2)User A first chooses a secret k (k should be positive integer and more less order of n), and creates public key parameter $\beta=kG$.

3) Then A again open public key p,a,b,G,β ， and transfer to B.

4)After user B receives public key，will code plaintext x to elliptic curve one point m of $E_p(a,b)$, and choose a random number γ among 1 ，2，…,n-1.

5) User B computing point $y_1=\gamma G,$ $y_2=m+\gamma\beta$.

6) User B will send cryptograph （y_1， y_2） to A.

7) After user A received cryptograph （y_1， y_2） ， computing

y_2-ky_1， the result is m.

8) decoding point of m is just plain text x .

During encryption communication procedure, if H wants to eavesdrop, he only sees Ep(a,b)、β 、G、 y_1、 y_2, however, it is very difficult to solve k using β 、G, or solve γ using y_2 , G. Therefore, H can’t obtain the plain message between A and B.

ECC Digital Signature : Digital signatures can ensure the authenticity of transaction parties, integrity, and non-repudiation of transmissions. ECC is looming at the horizon to be the next generation public key cryptosystem and digital signature scheme, also providing an excellent one way function relying on a different type of computations.

Signing: Alice wants to sign a message m(which might actually be the hash of o long message). Assume

M is an integer. It 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 $0\le m<n$ (if not, choose a large p). Alice also choeses a private integer a and computes $B=aA$. The prime p, the curve E, the integer n,and the points A and B are made public. To sign the message, Alice does the following:

1) Chooses a random integer k with $1\le k<n$ and gcd(k, n)=1, and computes *R=kA=(x,y)*

2) Computes $s\equiv k^{-1}(m-ax)(\bmod n)$

3) Sends the signed message *(m ,R, s*) to Bob.

Verification: Bob verifies the signature as follows:

1) Downloads Alice’s public information *p, E, A, B*

2) Computes $V_1=xB+sR \;\; and \;\; V_2=mA$

3) Declares the signature valid if $V_1=V_2$

The verification procedure works because

$$V_1=xB+sR=xaA+k^{-1}(m-ax)(kA)= xaA+(m-ax)A=mA=V_2 \quad （9）$$

$$k^{-1}kA = (1+tn)A = A + t(nA) = A + t\infty = A \quad (10\ )$$

3.5 An Protocol based on quantum cryptography

ECC and RSA cryptography use sophisticated mathematic methods to change basic information. This methods is more security but not absolutely secure. Quantum cryptography is very different cryptography. It mainly use quantum state as the key. Anyone of decoding will obtains insignificance information because of quantum state change . Theoretically, quantum cryptography impossibly is tapped and has very high security. Quantum cryptography network is first run in USA in 2004[15]

As described by Bennett et al. [1991] (see [Henle WWW] for an online demonstration). Quantum cryptography uses polarization of photons as its units of information. Polarization can be measured using three different bases, which are conjugates: rectilinear (horizontal or vertical), circular (left-circular or right-circular), and diagonal (45 or 135 degrees). Only the rectilinear and circular bases are used in the protocol.

1) The light source, often a light-emitting diode (LED) or laser, is filtered to produce a polarized beam in short bursts with a very low intensity. The polarization in each burst is then modulated randomly to one of four states (horizontal, vertical, left-circular, or right-circular) by the sender, Alice.

2) The receiver, Bob, measures photon polarizations in a random sequence of bases (rectilinear or circular).

3) Bob tells the sender publicly what sequence of bases were used.

4) Alice tells the receiver publicly which bases were correctly chosen.

5) Alice and Bob discard all observations not from these correctly-chosen bases.

6) The observations are interpreted using a binary scheme: left-circular or horizontal is 0, and right-circular or vertical is 1.

This protocol is complicated by the presence of noise, which may occur randomly or may be introduced by eavesdropping. When noise exists, polarizations observed by the receiver may not correspond to those emitted by the sender. In order to deal with this possibility, Alice and Bob must ensure that they possess the same string of bits, removing any discrepancies. This is generally done using a binary search with parity checks to isolate differences; by discarding the last bit with each check, the public discussion of the parity is rendered harmless. This process is:

1) The sender, Alice, and the receiver, Bob, agree on a random permutation of bit positions in their strings (to randomize the location of errors).

2)The strings are partitioned into blocks of size *k* (*k* ideally chosen so that the probability of multiple errors per block is small).

3）For each block, Alice and Bob compute and publicly announce parities. The last bit of each block is then discarded.

4）For each block for which their calculated parities are different, Alice and Bob use a binary search with log(*k*) iterations to locate and correct the error in the block.

5）To account for multiple errors that might remain undetected, steps 1-4 are repeated with increasing block sizes in an attempt to eliminate these errors.

6）To determine whether additional errors remain, Alice and Bob repeat a randomized check:

First, Alice and Bob agree publicly on a random assortment of half the bit positions in their bit strings.

Secondly, Alice and Bob publicly compare parities (and discard a bit). If the strings differ, the parities will disagree with probability 1/2.

Thirdly, If there is disagreement, Alice and Bob use a binary search to find and eliminate it, as above.

7）If there is no disagreement after *l* iterations, Alice and Bob conclude their strings agree with low probability of error (2^-*l*).

4 Conclusion

This paper has described mobile payment security model and encryption/decryption, digital signature based on ECC, moreover, briefly discribed protocol based on Quantum cryptography. As a result, the proposed security framework may overcomes mobile environments' constraints and has advantages over existing classical payment system.

References:

[1] Nambiar, S., Lu, C.T., and Liang, L.R., 2004, *IEEE IRI*, November 8-10, 475-480

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

[3] K. Pousttchi, and M. Zhenker, “Current Mobile Payment Procedures on the German Market from the View of Customer Requirements”, *Proceedings of the 14th International Workshop on Database and Expert Systems Application,* 2003 (DEXA’03).

[4] S. Nambiar, and T.L. Chang, “M-Payment Solutions and M-Commerce Fraud Management”, Retrieved September 9, 2004 from *http://europa.nvc.cs.vt.edu/~ctlu/Publication/M-Payment-Solutions.pdf*

[5] X. Zheng, and D. Chen, “Study of Mobile Payments System”, *Proceedings of the IEEE International Conference on E-Commerce*, 2003 (CEC’03).

[6] 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).

[7] Y. Lin, M. Chang, and H. Rao, “Mobile prepaid phone services”, *IEEE Personal Communications*, 7(3): 6-14, June 2000.

[8] 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.

[9] D. Hennesy, “The Value of the Mobile Wallet”, Retrieved on 2/16/2005 at:*http://www.valista.com/downloads/whitepaper/mobile_wallet.pdf*

[10] Z. Huang, and K. Chen, “Electronic Payment in Mobile Environment”, In *Proceedings of 13th International Workshop on Database and Expert Systems Applications* (DEXA'02) September 02 - 06, 2002. Aix-en-Provence,France.

[11] Jerry Gao, Ph.D., Krishnaveni Edunuru, Jacky Cai, and Simon Shim, Ph.D., “P2P-Paid: A Peer-to-Peer Wireless Payment System” *Proceedings of the 2005 Second IEEE International Workshop on Mobile Commerce and Services* (WMCS’05).

[12] Douglass R. Stinson, Dengguo Feng, *“Cryptogtaphy Theory and Practice”* [M],Publishing House of Electronics Industry, 2003.

[13] ZHAO Lianggang, CHEN Kefei, “Application of Elliptic Curve Cryptosystem for Security Protocol of Wireless Communication”, *Computer Engineering,* Vol .28 No.3, 2002,pp 128-129,shanghai,China.

[14] Charles H. Bennett, François Bessette, Gilles Brassard, Louis Salvail, and John Smolin, "Experimental Quantum Cryptography" , *J. of Cryptology* ***5****, 1992. An excellent description of a protocol for quantum key distribution, along* with a description of the first working system.

[15] Gilles Brassard, " A Bibliography of Quantum Cryptography", *Brief introductions for various aspects of quantum cryptography with references (some for on-line papers).* Somewhat dated, 1993.