Volume : 2 | Issue : 5 | May 2013 • ISSN No 2277 - 8179

Research Paper

Application of Certificate Less Digital Signature Scheme in E-cash System

Computer Science

KEYWORDS : Certificate less digital signature (CDS), public key, e-cash, private key generator(PKG), Trusted third party.t

Sridevi Assistant Professor, Department of Computer Science, Karnatak University, Dharwad

ABSTRACT

This paper introduces the concept of certificate less digital signature scheme and e-cash system.In this paper we propose an improved version of the CDS scheme provided by Harn, Ren, Lin. Our scheme provides signatures of lesser length for input of any file size. Signature generation and verification time are significantly minimized. Then we use this improved CDS scheme in the e-cash model. The main idea behind CDS is that there's a private key generator (PKG) which generates a partial private key for the user .Then using that key and some of its own private information the user computes its actual private key. PKG's public parameters and the user's private key together calculate the user's public key. Harn, Ren and Lin in 2008 proposed a CDS model which consisted of four generic modules namely PKG, user key generation, signature generation and verification. In this paper, we propose an improvement of the aforesaid CDS scheme in terms of time complexity and signature length and implement the new scheme in an e-cash model proposed by Popescu and Oros.

1. INTRODUCTION

Public key cryptosystems are one of the most essential parts of modern communication frameworks. Traditional public key cryptography requires each party which wants to send an encrypted message or a signed document should generate its own public key/private key pair. However the public of an entity needs to be authenticated by means of digital certificate which is provided by a recognized certification authority. However this method of attaching a certificate to authenticate a public key incurs unnecessary bandwidth and computation overhead for a wireless communication device that has a greater limitation in terms of computational power and speed of data transmission. In 1984 Shamir proposed a scheme where a party has to register at a private key generator (PKG) by providing its ID which can be a name or any unique combination of characters. Then the PKG provides a private key to the user or party and the ID of the user can be used as the corresponding public key. The user only needs to know the ID of his partner and the public key of the PKG to send an encrypted/signed document. But this system is not free from key escrow problem which makes the PKG itself as a potential threat of forging the signature or the attacking an encrypted document of one of its users.

However a modification to this scheme was made by involving multiple PKGs in generating the user's public key. Then self-certified public key system was proposed by Girault (1991) in which private key is generated by the user while the corresponding public key is calculated using the PKG's and the user's ID. However one still needs digital certificates for fully authenticating the partially authenticated public keys. Al-Riyami and Paterson in 2003 introduced the concept of certificate less digital signature. Their model involved a PKG module which is responsible for generating a partial private key for the user using its own master key. The user then from this private key and some of its own secret parameter calculates the actual private key. Public parameters of PKG and the private key of the user together calculate the user's public key. This method completely removes the key escrow problem as the PKG is not aware of the actual private key of the user. Public keys can be communicated to other users by publishing the same in a public directory or a website. In this way it is also not required to authenticate the public keys by issuing certificates. In 2008 Harn, Ren, Lin [1] proposed a scheme which can convert any DL-based signature scheme into a CDS scheme. According to this scheme any user who wants to produce a signature uses four modules namely; Private Key Generator (PKG), User Key Generation, Signature Generation and Verification.

Information privacy is defined as "an individual's claim to control the terms under which personal information that is information identifiable to the individual is acquired, disclosed and used"[2]. As technology advances sensitive personal information can be recorded, gathered, analyzed and misused by cyber criminals causing serious damage to customer interests. So it's an important issue in today's cyber era to provide information privacy and security to customers who constantly venture into the internet to perform their day to day activities. One of such areas which is most vulnerable to security attack is online transaction systems like e-cash systems used by e-commerce companies. In general three parties are involved in any online transaction; customer, merchant and bank. According to Brickell [3] and Stadler[4] a fair electronic cash system should prevent banks and merchants to obtain vital user information like credit card number, password, transaction history of the customers etc. In cases where there are suspected criminal activities the trusted third party with the help of the bank can revoke the anonymity of the customer or the coin. Popescu and Oros [5] proposed a fair offline e-cash system which implements coin tracing and owner tracing protocol. Trusted third party checks bank's signature of e-coin and stores the tracing information.

In our paper we propose an improved version of the CDS scheme provided by Harn, Ren, Lin. Our scheme provides signatures of lesser length for input of any file size. Signature generation and verification time are significantly minimized. Then we use this improved CDS scheme in the e-cash model proposed by [5].

2. PROPOSED CERTIFICATE LESS DIGITAL SIGNATURE AND E-CASH SYSTEM

In this scheme the PKG creates a partial private and public key pair, which is sent to the user and the user then calculates its own private and public key pair using DLP based algorithm. Thus the trusted PKG is unaware of the key pair that the user uses. Also it implements the IBS (Identity Based Signature) by using the user's unique ID in producing its private and public key. As we are not using certificates, so in order to distribute the keys the public keys are placed in a public directory or transmit-

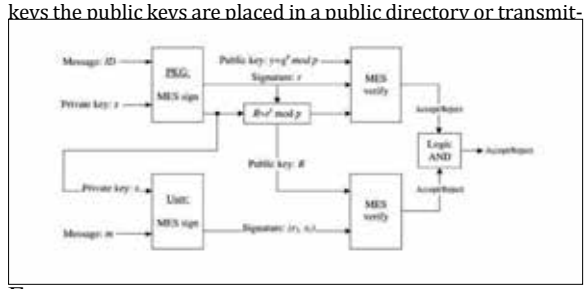

Fig. 1: Harn's CDS Scheme

The existing CDS scheme of Harn et al [1] contains four algorithms:
1. PKG key generation
2. User key generation,
3. Message signing
4. Signature verification

2.1 PKG Key Generation

• Generate a large prime p and a generator f of Z_p^*

• Run the random oracle to select a random private key x€Zp* and computes the public key y=gx mod p.

• Return params=(p,g,y) as the public parameters of PKG, while keeping x as the master private key.

2.1.2 User key generation
INPUT: params, ID
OUTPUT: Public Key Pair (r, R)

• User selects a random private key v€Z*p-1 with gcd(v, p -1) = 1, and computes u = gv mod p. {ID, u} is sent to PKG.
• PKG first selects a k€Z*p-1 With gcd(k,p -1)=1 then com putes t = gk mod p and r = uk mod p.
• PKG solves the linear equation h(ID, r) = xr + kz mod(p -1) ⇒z = k-1(h(ID,r)-xr)mod(p-1). The output (r,R) is sent to User.
• User computes s = v-1z mod(p-1) and R = rsmod p. s is each User's private key and (r, R) is each user's public key.

2.1.3 Message signing Sign
INPUT: params, message m, private key
OUTPUT: Signature σ

• Chooses a random l€Z*p-1 with gcd(l, p -1) = 1 and com putes r1 = r' mod p.
• s1 = l-1 (h(m,r1) - sr1) mod(p -1)
• Return σ =(r, R, r1, s1) as the complete CDS on m.

2.1.4 Signature verification
INPUT: params,m,σ
OUTPUT: Accept / Reject

1) gh(ID,r) =yrR mod p, and
2) rh(m,r1) = Rr1rs1 mod p.

If both equations hold, then the CDS will be Accepted, otherwise the CDS will be rejected.

2.2 THE PROPOSED CDS SCHEME
The proposed scheme is having four phases for creating the signature and verifying it. Those are:

1) PKG Key generation
2) User key generation
3) Signature generation
4) Signature Verification

2.2.1PKG Key generation:
• p is a large prime and q is a prime factor of p -1.
• g is generator belongs to Zq* of order q .
• PKG chooses its private key xA€ Zq*
• y =gXa mod p is public key

2.2.2 User Key generation:
• User selects its private key xB€ Zq* and computes his pub lickey y2=gxBmod p.
• User sends his ID along with y2 to PKG.
• PKG selects k€Zq* and computes r =gkmod p
• s = (k + r × xA) mod p and sends s to user along with ID.

2.2.3 Signature Generation:
• After receiving s, user chooses l€Zq* and computes u = gl mod p
• Then he computes t = H(m, ux"xl × yBSX-1 mod p)
• Certificate less Signature on message m is σ=(t, s).

2.2.4 Signature Verification:
Any verifier obtaining signature σ on message m can verify the authenticity by checking t'=H(m, yB × gs mod p)

If t' and t are equal then the CDS is accepted otherwise it is rejected.

3. E-Cash System
Electronic cash (e-cash) is a popular system since it realizes the digitalization of traditional cash system. This scheme enables customers to pay electronic money to merchants for different goods. There are some features that this system must implement, such as:

• Anonymity: The merchant/the spender must remain anony mous.
• Unreusability: The digital cash/e-cash cannot be reused or copied i.e. to reduce the risk involved in forgery and to establish authentication.
• Un-forgebility: Only the authentic users can produce the e-coin.
• Off-line payment: Transaction can be offline, i.e. no commu nication with the bank involved.

Electronic payment is one of the key issues of ecommerce development and many schemes has been propsed till date, but as far as the use of certificateless signature concerned to roboust the Electronic payment security aspect; a lot potential still to be exploited. .First Chaum suggested the electronic cash system in 1982.Subsequently, numerous untraceable electronic cash protocols were proposed based onthese constructs (Chaum 1983, Fan and Lei 1998, Ferguson 1994, Pointcheval and Stern 1997, Camenisch et al. 1995, Pointchval and Stern 1996)[7] .

The framework proposed incorporates all these features and is described as follows. It has four parties or entities which are Customer, The Bank, Trusted Third Party (TTP) & Merchant. The communications among these entities is shown in fig. 5.1. All these parties maintain some parameters i.e. their private and public key. Here the TTP works as if it's the PKG. It produces the partial private and public keys and using these keys the user produces its own key pair. Thus we avoid the key escrow problem that persisted in traditional schemes. Basically the e-cash system.

3.1 System parameters:
The system parameters consist of a large prime, a large prime factor of p-1 and an element g€Z^*_p of order q .

3.1.1 The Trusted Third Party
The trusted third party executes the following to set up his parameters.
• Select random secret xt€Z q
• Calculate yt = g Xt(mod p)
• The public key of the trusted third party is yt
• The corresponding secret key is xt

3.1.2 The Bank
The bank executes the following to set up his parameters.
• Select random secret xb€Zq
• Calculate yb=gxb(mod p)
• The public key of the bank is yb
• The corresponding secret key is xb

3.1.3 The Customer
The customer executes the next steps to set up his parameters.
• Select random secret xu€Zq
• Calculate yu = g Xu (mod p)
• The public key of the customer is yu

3.1.4 The Payment Protocol
The payment protocol involves the customer and the merchant in which the customer pays the electronic coin to the merchant.

3.1.5 Withdrawal Protocol
The customer contacts the Bank, requesting for a coin. The bank proves the customer's identity and produces a coin represented by the tuple (c, rb, sb , rt, st).

3.1.6 Deposit Protocol
Involves the Merchant & the Bank as follows (the merchant deposits his electronic coins to the bank):

• The merchant sends the e-cash (c, rb, s b , rt, st) to the bank.
• The bank verifies the validity of the e-coin using the same operations as the merchant.
• The bank checks whether the coin has been double spent. If the coin was not deposited before the bank accepts the coin and will deposit the e-cash to the account of the customer. Then the merchant sends the goods to the customer.

3.1.7 The Customer Tracing Protocol

It involves the Bank and the TTP. This protocol is used to determine the identity of the customer in a specific payment transaction. Money laundering can be prevented from detecting illegal customer in this protocol.

• The bank sends the e-coin(c, rb, s b, rt, st) to the trusted third party.
• The trusted third party verifies the validity of the e-coin us ing the same operations as the merchant and then sends to the bank. Note that is linked with the coin.
• The bank can find the corresponding customer from his da tabase (saved in the withdrawal protocol).

3.1.8 The Coin Tracing Protocol

The coin tracing protocol involves the bank and the trusted third party. This protocol determines the e-coin in the case when blackmailing occurs. The blackmailing can be prevented in this protocol

• The customer sends his identity, ID, to the bank.
• The bank sends to the trusted third party.
• The trusted third party finds the corresponding coin C and then sends the coin C to the bank.
• The bank can reject the coin C.

4. PERFORMANCE STUDY

It is clear from the following tables that our scheme has a lesser signature generation and verification time. The signature length is nearly same for different file sizes as we are using a hash function i.e. SHA 1 for the hashing. We have tested the Algorithm for various files and succeeded in generating and verifying the signature. Also the proposed scheme has less computational complexity as compared to the existing scheme.

Comparison with Existing Scheme

Operation	Signature Generation	Signature Verification
Exponential	$3T_E$	T_E
Hash	T_H	T_H
Multiplication	$3T_M$	$3T_M$

Table1: Number of operations in proposed scheme

Operation	Proposed Scheme	Harn's Scheme
Exponential	$3T_E$	$7T_E$
Hash	$2T_H$	$3T_H$
Multiplication	$4T_M$	$4T_M$

Table 2: Comparison with existing CDS

TE -Time taken for Exponential Operation
TM - Time taken for Multiplication operation
TH - Time taken for Hash operation

Operation	Existing Scheme(Execution time)	Proposed Scheme (Execution time)
Signature generation	44 milliseconds	21 milliseconds
Signature verification	20 milliseconds	5 milliseconds

Table 3: Comparison of existing scheme and proposed scheme

5. Conclusion

Proposed a new modified Certificate less digital signature (CDS) scheme with improved signing and verification times and complexity. We also incorporated the proposed scheme in the fair off-line electronic cash system with anonymity revoking trustee. We also employed the customer tracing and the coin tracing to achieve all the features of an ideal e-cash system. This scheme confirms authenticity of the digitally signed document, anonymity of the signer and non-repudiation of the signature generation process. This scheme can also be applicable to many real life scenarios, such as, e-banking, online auction and electronic voting system.

REFERENCE

[1] Lein Harn, Jian Ren, Changlu Lin, 'Design of DL-based certificate less digital signatures', The Journal | of Systems and Software 82 (2009) 789-793. | [2] IITF principles, supra note 19, at 5. | [3] E.Brickell, P.Gemmel and D.Kravitz, 'Trustee-based tracing extensions to anonymous cash and the | making of anonymous change', proceedings of The 6th ACM-SIAM,pp.457-466,1995. | [4] B. A. Fourazan, Debdeep Mukhopadhyay,'Cryptography and Network Security', Tata McGraw Hill, | 2nd edition,2010. | [5] Constantin Popescu, Horea Orors, 'A fair off-line electronic cash system with anonymity revoking | trustee'.Proceedings of the International Conference on Theory and Application of Mathematics and | Informatics-ICTAMI 2004, Thessaloniki, Greece. | [6] Lee, Chang, 'Strong designated verifier signature scheme', Computer Standard and Interface, 31, 2009. | [7] Al-Riyami, S., Paterson, K., 2003. 'Certificateless public key cryptography'. Advances in Cryptology - | AsiaCrypt, LNCS, vol. 2894. Springer-Verlag, pp. 452-473. | [8] Bellare, M., Namprempre, C., Neven, G., 2004. 'Security proofs for identity-based identification and | signature schemes'. Advances in Cryptology - EuroCrypt'04, LNCS, vol.3027. Springer-Verlag, pp. | 268-286. | [9] Mafruz Zaman Ashrafi, 'Privacy-preserving e-payments using one-time payment details,, Journal of Systems and software 31 (2009) 321-328. | | [10] S. Brands, 'Untraceable off-line cash in wallet with observers', Advances in Cryptology- | CRYPTO'93, Lecture Notes in Computer Science, Vol. 773, Springer-Verlag, pp. 302¬318,1993. | | [11] J. Camenisch, J. Piveteau, M. Stadler, 'An efficient payment system, protecting privacy', | proceedings of ESORICS'94, Lecture Notes in computer science, Vol. 875, Springer -Verlag, pp. | 207-215, 1994. | [12] Cheng-Chi Lee , Min-Shiang Hwang , Wei-Pang Yang, 'A new blind signature based on the discrete | logarithm problem for un-traceability'. | | [13] Cha, J., Cheon, J.H., 2003. 'An identity-based signature from gap Diffie-Hellman Groups'. Public | Key Cryptography - PKC'03, LNCS, vol. 2567. Springer-Verlag, pp.18-30. | | [14] Chen, X., Zhang, F., Kim, K., 2003. A new ID-based group signature scheme from Bilinear pairings. | WISA'03, LNCS, vol. 2908. Springer-Verilag, pp. 585-592. |