REMOVAL OF CERTIFICATES FROM SET PROTOCOL USING CERTIFICATELESS PUBLIC KEY CRYPTOGRAPHY

Arpita Sarkar[1] and Sachin Tripathi[1]

[1]Department of Computer Science and Engineering
Indian School of Mines, Dhanbad, Jharkhand, India
24arpitasarkar@gmail.com, var_1285@yahoo.com

ABSTRACT

Secure Electronic Transaction (SET) is a standard e-commerce protocol for securing credit card transactions over insecure networks. In a transaction using SET, all the members need public key certificates in order to authenticate their public key. Certificates are created by certificate authorities (CAs), The process of getting certificates from a certificate authority(CA) for any SET participants involves a large number of procedures like sending request to issue a certificates, getting approval or rejection of request and finally obtain the certificates, which is essentially time consuming as because these are associated with certificate management, including renew, revocation ,storage and distribution and the computational cost of certificate verification, also the chain of verification can be quite long, depending on the certificate hierarchy. So, the issues associated with certificate management are quite complex and costly.The present paper attempts the removal of the certificates using the 'certificateless public key cryptography (CL-PKC)' . The basic idea of CL-PKC is to generate a public/private key pair for a user by using a master key of a Key Generation Center (KGC) with a random secret value selected by the user. Hence, CL-PKC eliminates the use of certificates in traditional PKC and solves the key escrow problem in ID-PKC.The comparison with existing SET implementation is also addressed in the paper that shows the effectiveness of the proposal.

KEYWORDS

SET protocol, certificateless public key cryptography, Digital Certificate, Certificateless signature scheme, certificateless public key encryption

1. INTRODUCTION

The **Secure Electronic Transaction (SET)** [1][2][3]is an open encryption and security specification that is designed for protecting credit card transactions on the Internet. It relies on cryptography and digital certificate to ensure message confidentiality and security. Digital certificates, which are also called electronic credentials or digital IDs, are digital documents attesting to the binding of a public key to an individual or entity. Both cardholders and merchants must register with a certificate authority (CA)[2] before they can engage in transactions. The cardholder thereby obtains electronic credentials to prove that he or she is trustworthy. The merchant similarly registers and obtains credentials. These credentials do not contain sensitive details such as credit card numbers. Later, when the customer wants to purchases, customer and the merchant exchange their credentials. If both parties are satisfied then they can proceed with the transaction. Credentials must be renewed every few Years and presumably are not available to known fraudsters.

The present paper attempts to remove the number of certificates used in SET protocol using the CL-PKC[4].(Certificate less public key cryptography) CL-PKC combines elements from ID-PKC[5] and traditional PKI. However, when using ID-PKC[5] in practice, it is rare that the

DOI : 10.5121/ijnsa.2012.4612

public keys will depend on identities alone. On the other hand, CL-PKC avoids the key escrow problem inherent in ID-PKC by having user-specific private information involved in the key generation process. And CL-PKC does not need certificates to generate trust in public keys, instead this trust is produced in an implicit way. This would appear to make CL-PKC ideal for systems where escrow is unacceptable, but where the full weight of PKI is untenable. The main idea of CL-PKC is that a user combines two key components to form her private key: one component (the partial private key, PPK) is generated by a Key Generation Centre (KGC) using a master secret, and another component (the secret value) is generated by the user herself. The user also publishes a public key derived from her secret value; a party who wishes to encrypt to user only needs to have user's identity and public key along with the KGC's public parameters. One novel aspect of CL-PKC is the modelling of adversaries who are capable of replacing the public keys of users with keys of their choice. The present paper use CL-PKE[4] and CL-PKS[4] scheme based on the CL-PKC scheme in order to remove certificates.

The rest of this paper is organized as follows: The role of Digital Certificates in SET protocol is presented in Section II. The basic concepts of CL-PKC[4] as well as some technical background preliminaries of the protocols related to key agreement described in section III. The structure of the proposed certificateless authenticated key agreement SET protocol and the security attributes of the proposed protocol are described in Section IV. Section V discuss about the comparison between the existing and proposed SET protocol. Finally, Section VI concludes this paper.

2. DIGITAL CERTIFICATES

In a transaction using SET, all the members need a certificate in order to be authenticated. A certificate must be issued for the cardholder, merchant and payment gateway.

The Cardholder Certificate links the holder of the payment card to the account details (account number and expiration date). The Merchant Certificates represents a relationship between the merchant and a financial institution, allowing it to accept a payment card brand. These certificates are approved by the acquiring financial institution and provide assurance that the merchant has a valid agreement with an acquirer. The merchant needs two public key pairs for SET, one for digital signatures and other for encrypting key exchanges. It will therefore need two certificates for each payment card brand that it accepts. The payment gateway receives its certificates from the acquirer. During the process of purchasing, the cardholder encrypts the payment information using the public key of the payment gateway. This key was extracted from the payment gateway certificate.

There are a huge number of problems in issuing certificates from certification authority as these are involves additional cost, such as the certifying authority's subscription cost for issuing the digital certificates. Moreover there are an overhead of certification hierarchy in SET like a merchant certificate is digitally signed by the Merchant Certification Authority (MCA) which is signed by the Brand Certificate Authority (BCA). And the BCA certificate is digitally signed by the Root Certificate Authority (RCA).

Although, PKI works in practice, it has significant drawbacks. Evidently, PKI does not solve many problems as it was expected to do.

A. Firstly, the infrastructure is heavy-weight and rather expensive, because requires trusted authorities to obey strict security policies. These rules concern both digital and physical security measures to protect Certificate Authority from compromise.

B. Certificates must be verified by users (whether they match correct identity), but non-technical users usually fail to do it right. Even though the checking process is not that complicated (e .g comparing web address with holder specified in certificate) many people do not perform it.

C. Another drawback is certificate management and revocation of old/compromised keys. The main problem of key validation is how to quickly check whether particular key is up-to-date. Much of computational overhead comes from validation of full certification paths. So called Certificate Revocation Lists are original mechanism utilized by Public- Key Infrastructure. In practice, they might grow rapidly and become awkward to manage, which is usually the case in big deployments of PKI. Alternatively, there exists an on-line approach which moves much of the validation overhead from clients to dedicated servers that constitute to additional infrastructure.

D. If certificate is to match particular person, it must contain personal details such as name, surname, but in global world this still might not be precise enough, because names can repeat. The problem can be resolved by leaning towards local namespaces and providing more identity details. Unfortunately, the latter can lead to privacy compromise and might not be accepted by individual users.

E. Finally When a SET participant presents its certificates; it includes the complete certificate chain up to the root. The recipient of the message can follow this chain and as long as it has the root certificate, can establish trust in the certificate .This process creates an extra overhead in the protocol.

3. PRELIMINARIES

This section first revisits some basic concepts.

3.1 Concepts of certificateless Public key cryptography

Certificateless cryptography (CL-PKC)[4] was firstly presented by Al-Riyami and Paterson The key feature of the model certificateless public key cryptography (CL-PKC) is that it completely eliminates the need for certificates, The technical means by which it does so is a user A's private key is composed in two stages. In the first stage, an identity-dependent partial private key is received over a confidential and authentic channel from a trusted authority (called a key generation centre, KGC). In the second stage, the user produces his private key by combining the partial private key with some secret known only to the user.

The user also publishes a public key which matches the private key. However, this public key need not be supported by a certificate.

3.2 Now this section recall some notions and definitions that will be used in the rest of the paper. As the proposed schemes use a bilinear map, which is often called “pairing” as well, so the Bilinear group and some computational assumptions are discussed below

A. Bilinear Groups:

Let G_1 be a cyclic additive group and G_2 be a cyclic multiplicative group of same order q, .Let ê be a bilinear map such that ê: G_1X G_2.-->G_2 A map ê has the following properties:

1. Bilinear: $\hat{e}(aP, bQ) = \hat{e}(P, Q)^{ab}$, for all P,Q € G1 and a, b € Zq*

2. Non-degeneracy: $\hat{e}(P, Q) \neq 1$

3. Computable: The map e is efficiently computable.

B. Some Computational Assumptions

The security of the proposed protocol relies on the standard Computational Diffie-Hellman (CDH) and Bilinear Diffie- Hellman (BDH) problem assumptions which are understood to be computed with minor probability.

1) Discrete Logarithm Problem (DLP): Given P, Q€G1, find n € Zq* such that P = nQ whenever such n exists.

2) Computational Diffie–Hellman Problem (CDHP): Given a tuple (P, aP, bP)€G1 for a, b€ Zq*, find the element abP.

3) Bilinear Diffie–Hellman Problem (BDHP): Given (P, xP, yP, zP) €G1 for some x, y, z chosen at random from Zq*, compute $e(P, P)^{xyz}$ €G2.

4. PROPOSED SCHEME FOR DIGITAL CERTIFICATES REMOVAL

In SET, the public key cryptography is only used to encrypt DES keys and for authentication (digital signature). So each set participant possesses two asymmetric key pairs a “key exchange" pair, which is used in the process of session key encryption and decryption and a“signature pair “for the creation and verification of digital signature.

These public key-exchange key and signature key needs to be authenticated from CA. But in this proposed scheme each entity run directly or indirectly the following algorithms involved in CL-PKC, in order to remove certificates.

- Key Generation Technique
- Certificateless Public Key Encryption scheme
- Certificateless Signature Scheme

A. Key Generation Technique

KGC executes Setup algorithm to generate master-key and system parameters. Then, it runs Partial-Private-Key-Extract algorithm to extract the partial private key for each entity. Every entity chooses a secret value and computes its public and private key.

Setup and Partial-Private-Key-Extract:-

1) At first KGC performs the following steps during the Setup process:

a) KGC select a cyclic additive group G1 of prime order q, a cyclic multiplicative group G2 of the same order, a generator P of G1, and a bilinear map e: $G1 \times G1 \rightarrow G2$.

b) KGC choose a random master-key, s €Zq* and set P_0=sP.

c) KGC choose cryptographic hash functions, H_1: $\{0,1\}^* \rightarrow G_1$, H_2: $G_2 \rightarrow \{0, 1\}^n$.

2) After that Entity A sends its identity ID_A to KGC.

3) KGC generates the partial private key for entity A using the following steps:

a) Compute $Q_A = H1 (ID_A)$.

b) Generate the partial private key $D_A = sQ_A$.

4) The system parameters (G1, G2, e, P, P0, H1, H2, n) are published while the master-key s €Zq* is kept in KGC.

5) After receiving the partial key from KGC Entity A executes:

a) Set-Secret-Value: choose a random value, X_A €Zq* as the entity A's secret value.

b) Set-Private-Key: generate the private key, $S_A = x_A D_A$.

c) Set-Public-Key: compute the public key, $P_A = x_A Q_A$.

Each SET participant generates their two public/private key pair by contact directly or indirectly to the KGC (key generation centre). The key generation technique for the cardholder depicted using the above mentioned algorithm.

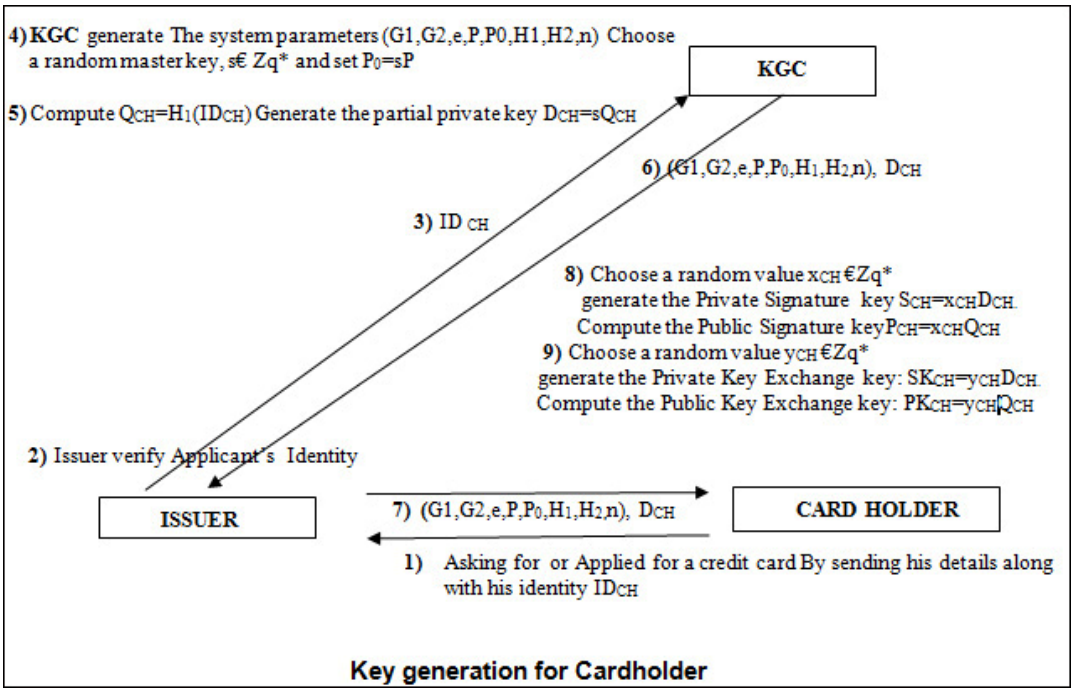


Figure- 1

B. Certificateless Public Key Encryption scheme (CL-PKE)[4]

The SET participants in order to encrypt the symmetric key and decrypt the same use this scheme. To encrypt a message, the sender uses the receiver's digital identifier and the receiver's public key. The receiver decrypts the ciphertext using the secret value generated by the receiver and the partial private key supplied by the key generation centre. The intuition is that the sender does not require a digital certificate as the creation of a false public key for an identity will not help an attacker break the confidentiality of a transmitted message because the attacker does not know the partial private key for that identity. (This logic is similar to that of an identity-based

encryption scheme.) The key generation centre cannot break the confidentiality of a transmitted message as it does not know the secret value corresponding to the receiver's public key. Of course, this makes the assumption that key generation centre will not publish a false public key for a receiver, but this attack seems unavoidable (and comparable to a CA publishing a false certificate for an identity).

Advantage of CL-PKE: Certificateless encryption schemes are characterised by two properties: (a)the scheme provides security without the need for a public key to be verified via a digital certificate, and (b) the scheme remains secure against attacks made by any third party (including a key generation centre or a certificate authority).

A CL-PKE scheme is specified by seven randomized algorithms: Setup, Partial-Private-Key-Extract, Set-Secret-Value, Set-Private-Key, Set-Public-Key, Encrypt and Decrypt: the first five steps are same as the previous key generation technique mentioned above. So the remaining Encryption and Decryption algorithm are:-

Encrypt:

1) At first this algorithm takes as inputs params (System Parameters getting from KGC), a message m €M, and the public key P_A and identifier ID_A of an entity A.

2) It returns either a cipher text c € C or the null symbol _ indicating an encryption failure.

Decrypt:

1) This algorithm takes as inputs params, c €C, and a private key S_A

2) It returns a message m €M or a null symbol _ indicating a decryption failure.

Naturally, the output M should result from applying algorithm Decrypt with inputs params, S_A on a ciphertext C generated by using algorithm Encrypt with inputs params, P_A, ID_A on message M.

C. Certificateless Signature Scheme

In this scheme[4] after signing to the message digest and generating the digital signature with the sender's private key instead of sending public signature key certificates to the receiver(SET participant) the sender (SET participant)only send his public key, params, and identity in order to verify the digital signature with the following steps:

Sign: At first this algorithm takes as inputs params, a message m€M to be signed and a private key S_A. It outputs a signature Sig € S.

Verify: This algorithm takes as inputs params, a message m €M, the identifier ID_A and public key P_A of an entity A, and Sig€ S as the signature to be verified. It outputs valid, invalid or _|

The total SET PAYMENT TRANSACTION PROCESS is a vast topic which consists of three modules:
1 .Purchase process
2 .Payment authorization process
3. Payment capture process
So, only the first module is described below .The purchase process not using any kind of public key certificates for authentication.

1. PURCHASE PROCESS:-

1A. Cardholder Initiates Request:-

Cardholder software creates a purchase initiate request, containing the name of the credit card brand that the cardholder has elected to use. This request is effectively asking for which payment gateway the merchant will use. The cardholder sends the initiate request to the merchant.

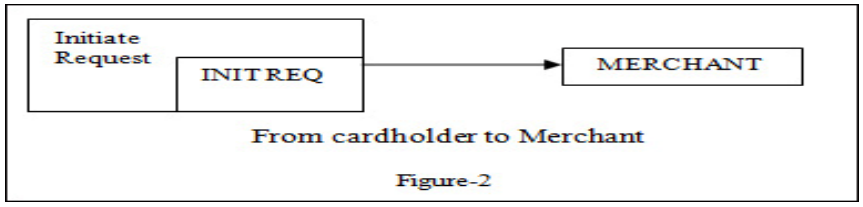


Figure-2

1B) Merchant Sends Response:-

1. The merchant receives the initiate request.
2. The merchant generates the response message and digitally signs it bypassing the response through a hash function. The message digest created by this is encrypted using certificateless public key encryption, resulting in a digital signature.
3. The merchant sends the initiate response, the digital signature, the merchant public signature key etc. and the payment gateway information to the Cardholder

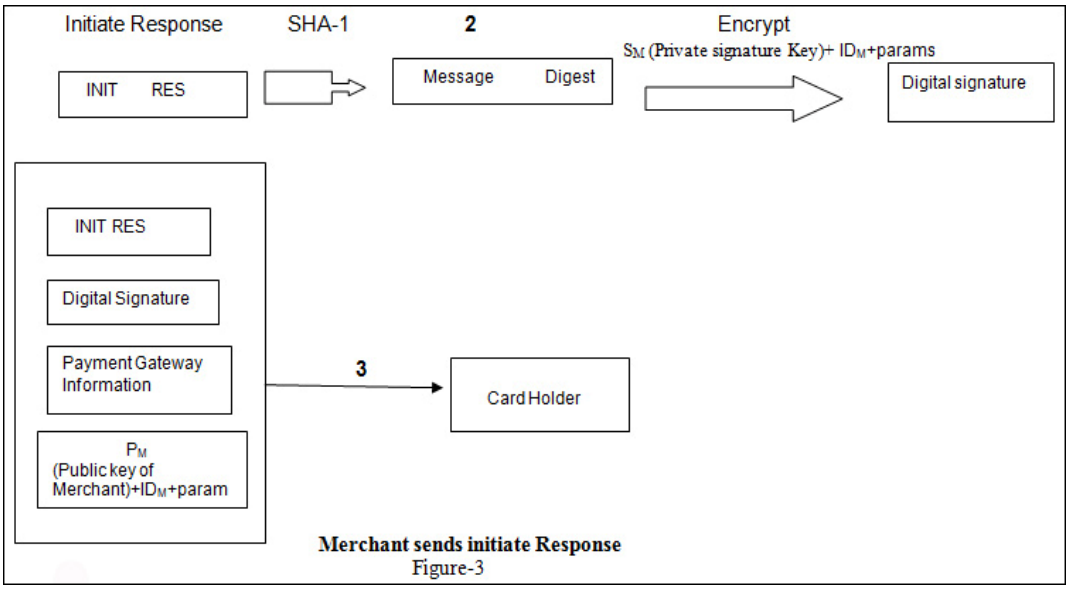


Figure-3

1C) The Cardholder sends Request:-

1. The cardholder receives the initiate response message from the merchant.

2. The merchant signature is verified by running the initiate response through a hash function and creating a message digest. The digital signature is decrypted using the certificateless

decryption procedure and the result is compared with the message digest obtained from the received message. If they are equal, the integrity of the message is assured.

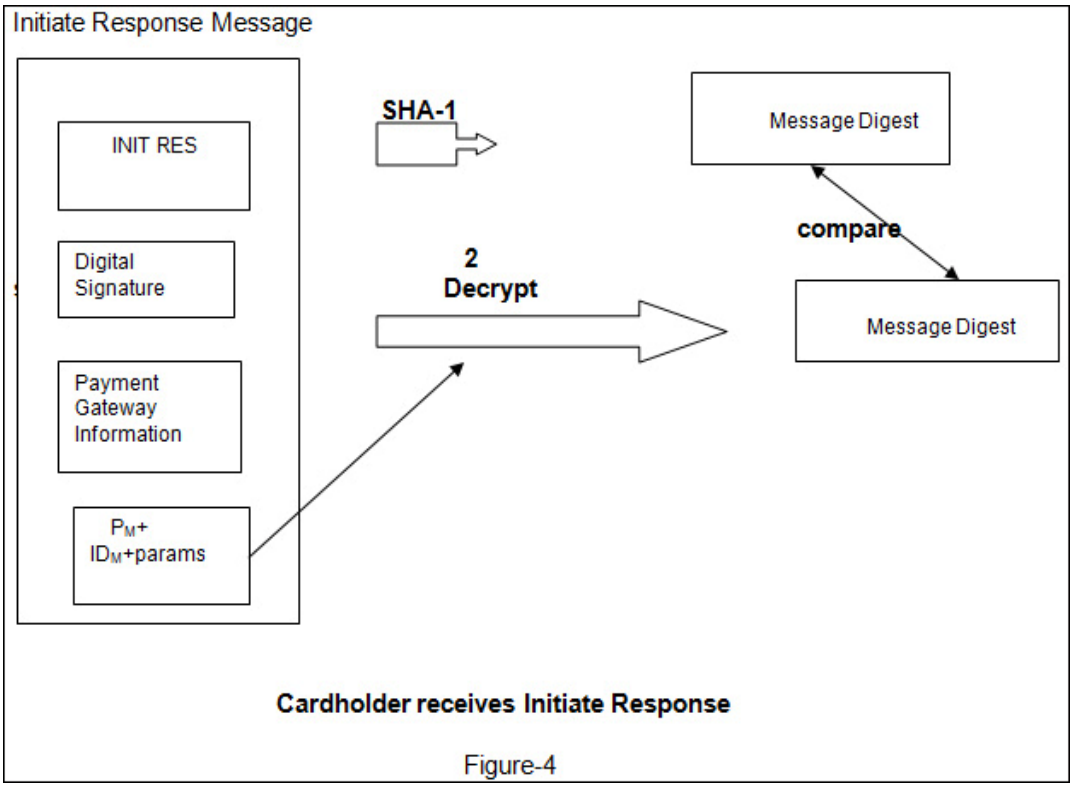


Figure-4

3. The cardholder software creates the order instruction (OI) portion of the purchase request message using information from the shopping phase. The OI does not contain the description of the goods purchased. This information was exchanged between the cardholder and the merchant during the shopping process and before the first SET message

4. The cardholder creates the second portion of the purchase request, the payment instruction (PI). This contains details of the credit card that the cardholder has chosen to use.

5. A transaction identifier, received from the merchant in the initiate response, is placed in the OI and PI. This identifier will be used by the payment gateway to link the OI and PI when the merchant requests payment authorization.

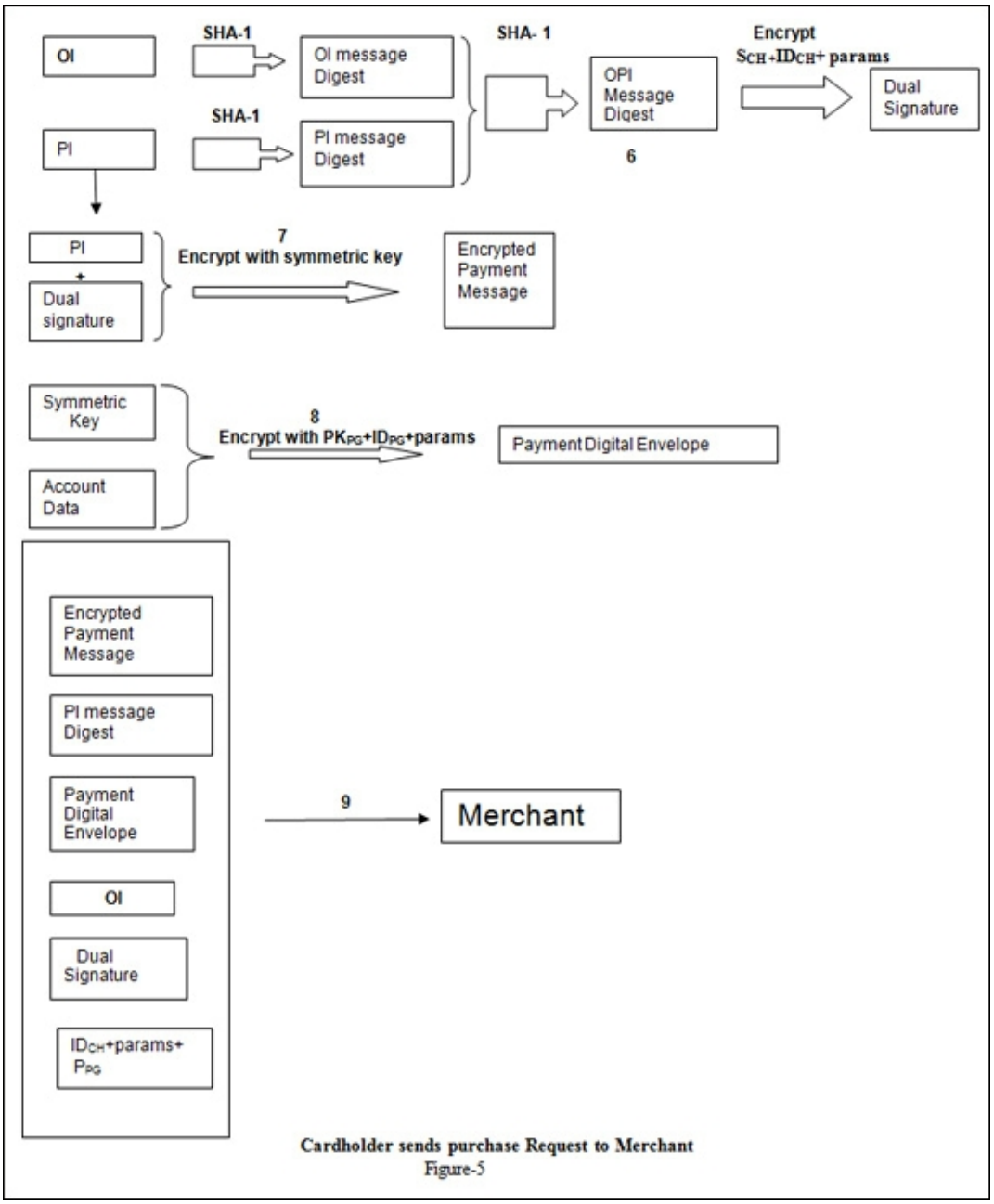
6. The cardholder generates a dual signature by passing the order instruction and payment instruction through a hash function. The two message digests created (OI message digest and PI message digest) are concatenated. The resulting message is run through a hash function and is encrypted with the certificateless public key encryption technique. This is the dual signature.

7. The PI, dual signature and OI message digest are encrypted using a randomly generated symmetric key. This is the encrypted payment message, which will be passed on to the payment gateway.

8. The symmetric key used to construct the payment message and the cardholder's account number are encrypted with the payment gateway public key-exchange key using certificateless public key encryption algorithm(Assume that after receiving about the information of the payment gateway from the merchant ,the cardholder contact to the payment gateway and

collect payment gateway's all information which is needed for CL-PKE), generating the payment digital envelope.

9. The encrypted payment message, PI message digest, order instruction (OI) message, payment digital envelope, dual signature and the cardholder identity ID_{CH}, params and public signature key of cardholder are sent to the merchant.



Cardholder sends purchase Request to Merchant

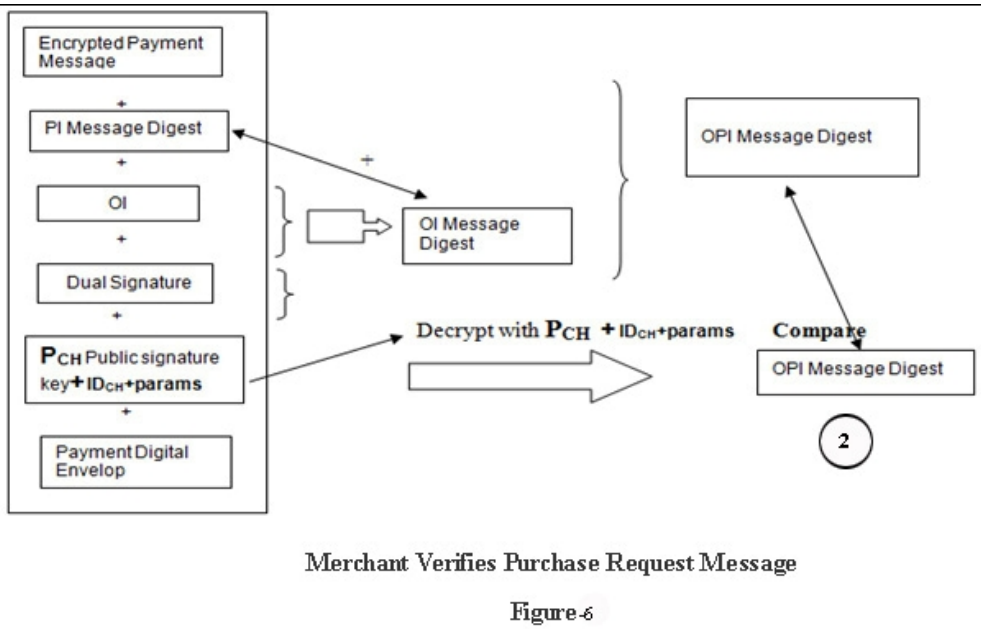
Figure-5

1D) Merchant Processes Purchase Request Message:-

1. The merchant receives the request message

2. The dual signature is verified by running the order instruction (OI) through a hash function and creating the OI message digest. This message digest is concatenated with the PI message digest that was received within the request message. The dual signature is decrypted using the cardholder public signature key, using the certificateless digital signature decryption algorithm and the result is compared with the OPI message digest obtained locally. If they are equal, the merchant can be assured of the integrity of the request.

3. The merchant processes the order request, and forwards the encrypted payment message and payment digital envelope to the payment gateway for payment authorization .The merchant does not need to wait for a response to its authorization request before it sends a response to the cardholder's purchase request.



Merchant Verifies Purchase Request Message

Figure-6

4. The merchant creates the response message and digitally signs it bypassing it through a hash function. The message digest so created is encrypted with the merchant private signature key using CL-PKE method, resulting in a digital signature.

5. The Merchant sends the purchase response, the digital signature, all his identity, params, public signature key to the cardholder .This message only indicates that the merchant received the order. The services or goods purchased by the cardholder will only be executed or shipped when the merchant receives a payment authorization response from the payment gateway. After the cardholder receives the confirmation that the merchant received the order information, he or she can send inquiries to the merchant to know if the authorization has been performed.

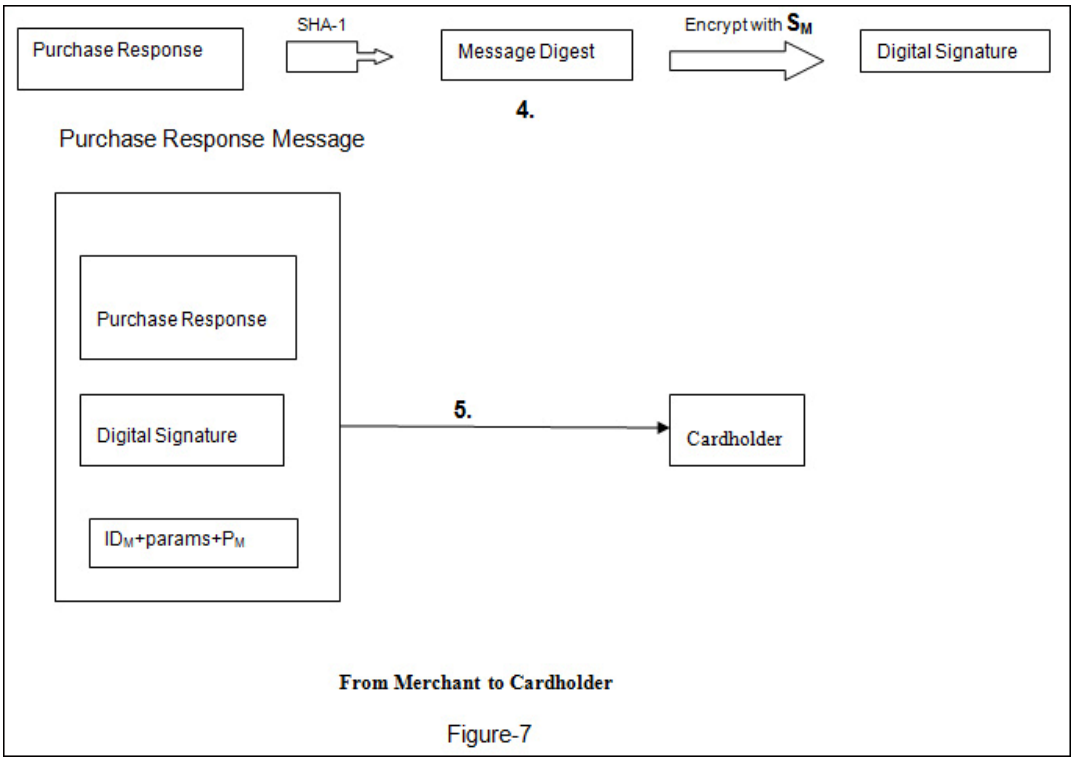


Figure-7

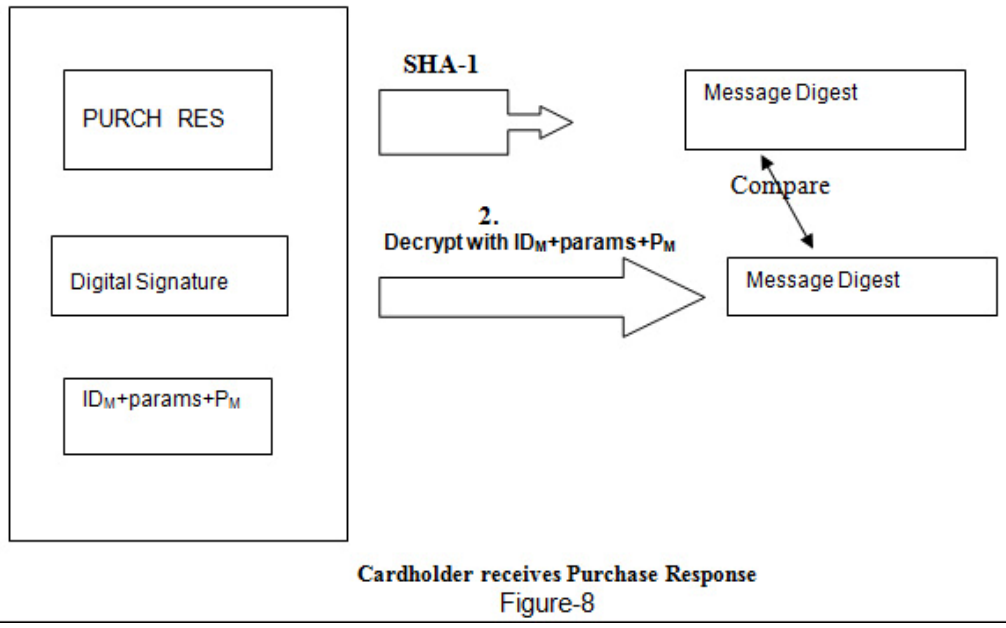
1E) Cardholder Receives Purchase Response:-

The cardholder receives the response from the merchant. This tells him or her that the purchase request has been accepted and that he or she can expect to receive the goods, as long as the card has enough credit remaining.

1. The cardholder receives the purchase response message from the merchant

2. The merchant signature received is verified by running the purchase response through a hash function and creating a message digest. The digital signature from the response is decrypted using the merchant public signature key using certificateless public key decryption algorithm and the result is compared with the message digest obtained locally. If they are equal, the cardholder is assured of the integrity of the message.

3. The cardholder stores the purchase response. The cardholder can determine the status of the order (if the payment gateway approved the transaction) by sending an order inquiry message to the merchant. If it was approved, the goods purchased will be shipped or the services will be performed



Cardholder receives Purchase Response

Figure-8

Abbreviations:

S_{CH} – card holder private signature key

P_{CH} – card holder public signature key

ID_{CH} – card holder identity

Params – System parameters generated by KGC

SK1 – symmetric key -1

SK- symmetric key

PK_{PG} – public key exchange key of payment gateway

ID_{PG}- payment gateway identity

ID_M- Merchant identity

P_M- Merchant public signature key

S_M- Merchant private signature key

SHA-1-secure hash function

Security Attributes:-

As certificateless public key cryptography is used so the security attributes are same as certificateless key agreement protocol [reference 9].

5. COMPARISON WITH EXISTING SET PROTOCOL

In the existing SET protocol two types of certificates one for authenticate the public key-exchange key and another for public signature key, so for each participants total 6 certificates

are use. Because of the certificates overhead are present in existing SET protocol it invokes the chain of Certificate Authority and issuing certificates is a big task and cost a lot.

The process of generating only one certificate for example for a cardholder involves the following steps:-

1. The cardholder software creates a request to ask for a copy of the CA's Certificates and send it to the CA.
2. The CA receives the initiate request and transmits it two Certificates.
3. Cardholder Requests Registration Form.
4. CA sends Registration Form.
5. Cardholder Requests Certificate.
6. CA receives request
7. Cardholder Receives Certificate.

The Certification process for merchant's payment gateway is nearly similar to that for cardholder. So every participant must go through 7 steps in order to obtain only one certificate from CA

The total no. of Certificates generated on SET payment transaction process are discussed on TABLE-I

TABLE-I

Transaction Process		**Signature key certificate**	**Exchange key certificate**
Existing SET	Purchase Process	3	1
	payment Authorization Process	3	1
	Payment Capture Process	2	1
Total		8	3

From the above table we observe that total 11 certificates are generated for the existing SET but for the proposed SET there required no certificates.

Now TABLE-II compares between Traditional PKC and Certificateless PKC.

TABLE II

	Existing SET	**Proposed SET**
Trusted Third Party	CA	Not required
Time to implement	Take time to issue and obtain	Easily implement
Cost for certificate	Have to pay the certificate issuer	No cost
Trust	Trust to CA	User identity
Certificate Maintenance	Certificate renew ,revocation	No Certificate maintenance
Storage of Root CA certificates in applications like Browser	Require in order to verify certificate	Not required

6. CONCLUSION

The proposed enhanced SET protocol employees CL-PKC for removing certificates, and used secure and efficient certificateless authenticated key generation technique for generating public/private 'signature' pair and a public/private "key- exchange" pair .The key generation also reduces the amount of trust on KGC. Thus the proposed scheme eliminates the overhead of sending certificates by removing several procedures of issuing certificates from a CA as well like generating certificates 4 times in purchase process, 4 times in payment authorization process and 3 times in payment capture process.

Hence the proposed protocol require less process time as because it not send and receives any certificates also remove the overhead required for authentication of key from CA ,which increases its performance.

ACKNOWLEDGEMENTS

The authors are thankful to the referee of the paper, IJNSA for their valuable comments and suggestion to enrich the paper.

REFERENCES

[1] SET Secure Electronic Transaction Specification: Formal Protocol. Definition, May 1997.

[2] SET Secure Electronic Transaction Specification: Formal Protocol, Definition, May 1997.

[3] W. Stallings, "Cryptography and Network Security 4th Ed," Prentic, 2005.

[4] Al-Riyami SS, Paterson KG. Certificateless public key cryptography. In: Laih CS, ed. Proc. Of the ASIACRYPT 2003. LNCS 2894, Berlin: Springer-Verlag, 2003. 452-473.

[5] Shamir A. Identity-Based cryptosystems and signature schemes. In: Blakely GR, Chaum D, eds. Advances in Cryptology-Crypto'84. LNCS 196. Heidelberg: Springer-Verlag, 1985. 47-53.

[6] Al-Riyami SS, Paterson KG. CBE from CL-PKE: A generic construciton and efficient schemes. In: Vaudenay S, ed. Proc. of the PKC 2005. LNCS 3386, Berlin: Springer-Verlag, 2005. 398-415. [doi: 10.1007/978-3-540-30580-4_27]

[7] C. Gentry, "Certificate-based encryption and the certificate revocation problem," inProc.EUROCRYPT'03. Berlin, Heidelberg: Springer- Verlag, 2003, p. 272–293.

[8] T.K..Mandt and C.H.Tan,"Certificateless authenticated two-partykey agreement protocols," in Proc. ASIAN'06, Berlin, Heidelberg: Springer-Verlag, 2007, p. 37–44

[9] An enhanced Certificateless Authenticated key agreement protocol' by Razieh Mokhtarnameh, Sin Ban Ho, Nithiapidary Muthuvelu ISBN 978-89-5519-155-4 802 Feb. 13~16, 2011 ICACT2011

[10] L. Xia, S. Wang, J. Shen, and G. Xu, "Breaking and repairing the certificateless key agreement protocol from asian 2006," Wuhan University Journal of Natural Sciences, vol. 13, no. 5, pp. 562–566, Nov. 2008.

[11] D. Boneh and M. Franklin. Identity based encryption from the Weil pairing. SIAM J. of Computing, 32(3):586–615, 2003.

[12] M. Bellare and P. Rogaway, "Entity authentication and key distribution," In Advances in Cryptology - CRYPTO '93, Springer Berlin/Heidelberg, Vol. 773 of Lecture Notes in Computer Science, 1993, pp. 232-249, doi:10.1007/3-540-48329-2.

[13] S.B. Wang and Z.F Cao, "Efficient certificateless authentication and key agreement (CL-AK) for Grid computing," International Journal of Network Security, Vol.7, No.3, 2008, PP.342–347.

[14] Y.J Shi and J.H Li, "Two-party authenticated key agreement in certificateless public key cryptography," Wuhan University Journal of Natural Sciences, Vol. 12(1), 2007, pp. 71-74, doi: 10.1007/s11859-006-0194-y.

[15] S.B. Wang, Z.F Cao and L.C. Wang, "Efficient certificateless authenticated key agreement protocol from pairings," Wuhan University Journal of Natural Sciences, Vol. 11(5), 2006, pp. 1278-1282, doi: 10.1007/BF02829251.

[16] B. Libert and J-J. Quisquater, "On constructing certificateless cryptosystems from identity based encryption," Lecture Notes in Computer Science, Berlin/Heidelberg, Vol. 3958, 2006, pp. 474-490, doi: 10.1007/11745853_31.

[17] S. Blake-Wilson, D. Johnson and A. Menezes, "Key agreement protocols and their security analysis," In 6th IMA International Conference on Cryptography and Coding, Springer-Verlag, Vol. 1355 of Lecture Notes in Computer Science, 1997, pp. 30–45, doi:10.1007/BFb0024443.

[18] C.M. Swanson, "Security in key agreement: two-party certificateless schemes, " Master's thesis, University of Waterloo, Canada, 2008.

[19] C. Adams and S. Farrell, "Internet x.509 public key infrastructure: Certificate management protocols," Work in progress, 2004.

[20] C. Gentry, "Certificate-based encryption and the certificate revocation problem," In Eurocrypt'03, Vol. 2656 of LNCS, Berlin/Springer-Verlag, 2003, pp. 272-293, doi: 10.1007/3-540-39200-9.

[21] D. Boneh and X. Boyen, "Efficient selective-ID secure identity based encryption without random oracles," In Eurocrypt'04, Vol. 3027 of LNCS, Berlin/Springer-Verlag, 2004, pp. 223–238, doi: 10.1007/b97182.

[22] E.Fujisaki, and T.Okamotom, "Secure integration of asymmetric and symmetric encryption schemes", Advances in Cryptology –CRYPTO'99, Vol. 1666 of LNCS, Berlin/Springer-Verlag, 1999, pp. 535-554, doi: 10.1007/3-540-48405-1.

[23] C.J. Mitchell, M. Ward, P. Wilson, "Key control in key agreement protocols," Electronics Letters 34, 1998, pp. 980–981, doi:10.1049/el:19980686.

[24] Y.J. Shi and J.H. Li, "Constructing efficient certificateless public key encryption with pairing," International Journal of Network Security, Vol.6(1), Jan. 2008, pp. 26–32.

[25] Y.J. Shi and J.H. Li, "Provable efficient certificateless public key encryption," Cryptology ePrint Archive, Report 2005/287, 2005.

Author

ARPITA SARKAR

Research Interest

Network Security, Cryptography, Secure - E-Transaction

Ms. Arpita Sarkar Pursuing M.Tech (Computer Application) from Department of Computer Science and Engineering, Indian School of Mines, Dhanbad.

SACHIN TRIPATHI

Assistant Professor

Specialization

Multicasting , Secure E-Business.

Research Interest

Secure Multicast Applications.

Dr. Sachin Tripathi joined Indian School of Mines, Dhanbad as Lecturer in the year 2005 and has been working as an Assistant Professor in the Department of Computer Science and Engineering from January 2006. Before that he joined, Haldia Institute of Technology, Haldia, West Bengal, in July 2005, as a Lecturer in the Department of Computer Science and Engineering. He was selected in Early Faculty Induction Programme (EFIP-03) sponsored by AICTE, conducted by IIT- Chennai. He has around seven years of teaching and research experiences. He served as reviewers of international journals and conferences. He visited the Las Vegas, USA in 2008 for academic purpose.