Efficient Signature Scheme for Secure Electronic Transaction

G. Jai Arul Jose[1], Adalia Martin[2]
[1,2]*Assistant Professor, Department of Computer Science,*
Oman College of Management and Technology,
Barka, Sultanate of Oman
[1]*g.jai.areul@omancollege.edu.om*
[2]*adalia.martin@omancollege.edu.om*

***Abstract* – Secure Electronic Transaction (SET) is an important E-commerce protocol designed to provide security of credit card purchases over internet. Many companies were involved in developing the initial specification, including IBM, Microsoft, Netscape, RSA, Terisa, and Verisign. Beginning in 1996, there have been numerous tests of the concept, and by 1998 the first wave of SET-compliant products was available. Important innovation introduced in SET is the dual signature. The purpose of the dual signature is to link two messages that are intended for two different recipients. In this case, the customer wants to send the order information (OI) to the merchant and the payment information (PI) to the bank. The merchant does not need to know the customer's credit card number, and the bank does not need to know the details of the customer's order. Currently, the dual signature is signed and verified by the traditional RSA or ECDSA signature schemes. This paper will introduce "certificateless" signature scheme which use bi-linear pairing for verifying process that will avoid the use of Certificate Authority or Key Distribution Centre.**

***Keywords* – Cryptography, Key Distribution, Digital Signature, SET, Bilinear Pairing.**

I. INTRODUCTION

Electronic commerce is an Internet-based business transactions performed electronically by individuals, companies, corporations and governments utilizing information and communications technologies. The most important obstacle to further expansion for e-commerce has been the lack of adequate security protections. When sending secure data via the Web, no any security which secures the transaction.

Any business transactions business requirements for secure payment processing with credit cards over the Internet and other networks are required and this includes confidentiality of payment and ordering information, integrity of all transmitted data, authentication that a cardholder is a legitimate user of a credit card account, authentication that a merchant can accept credit card transactions through its relationship with a financial institution, use of the best security practices and system design techniques to protect all legitimate parties in an electronic commerce transaction, availability of protocol that neither depends on transport security mechanisms nor prevents their use, and interoperability among software and network providers.

Secure Electronic Transaction (SET) is a system for ensuring the security of financial transactions on the Internet. With SET, a user is given an electronic wallet and a transaction is conducted and verified using a combination of digital certificates among purchaser, merchant, and purchaser's bank in a way that ensures privacy and confidentiality. SET's makes use of Secure Socket Layer (SSL), Secure Transaction Technology, and Secure-Hypertext Text Transfer Protocol (S-HTTP). SET uses some but not all aspects of public key infrastructure (PKI).

In this study, the authors develops security feature using SET which uses an efficient certificateless scheme using bi-linear pairing.

The following section, Yu at al's cetificateless signature scheme which is based on bilinear pairings was reviewed. The following describes the bi-linear pairing:

II. BILINEAR PAIRINGS

Let $(G_1,+)$ be an additive cyclic group of a large prime order q, and $(G_2,\bullet)$ be a multiplicative cyclic group of the same prime order q. A bilinear pairing is a function map $e: G_1 \times G_1 \rightarrow G_2$, which satisfies the following properties:

- Bilinear: $e(aU,bV) = e(U,V)^{ab}$ for all $U,V \in G_1$ and $a, b \in Z^*_q$.
- Non-degenerate: If P is a generator of G_1, then e(P,P) is a generator of G_2. In other words, $e(P,P) \neq 1_{G_2}$.
- Computable: There exists an efficient algorithm to compute e(U,V) for all U,V $\in G_1$.

Generally, the map e should be derived from either Weil or Tate pairing on an elliptic curve over a finite field.

III. METHODOLOGY

In traditional PKI, it needs a certificate issued by certification authority (CA) to achieve user's public key authentication. In 1984, Shamir's study proposed the notion of identity-based cryptography (IBC), in which the user's public key is derived directly from its name, email address, the user's public key is generated by a trusted third party called Key Generation Center (KGC). Such cryptosystem eliminates the need for public key certificate (Shamir, 1984). But, it suffers from the key escrow problems, the KGC knows the user's private key. A malicious KGC can decrypt any ciphertext and forge the signature of any user. To overcome the drawback of key escrow in IBC, Al-Riyami and Paterson introduced certificateless public cryptography (CL-PKC) in 2003 where the user's private key is a combination of partial private key computed by KGC and some user-chosen secret value. Hence, CL-PKC avoids usage of certificates and resolves the key escrow problem. However, most of these certificateless signature schemes are probably secure in random oracle model, which only be considered as a heuristic argument. The first certificateless signature scheme in the standard model is proposed by Liu et al in 2007. Unfortunately, in 2008, Xiong et al. showed that Liu's scheme is insecure against a "malicious-but-passive" KGC attack in the standard model. However, Xia et al showed that both Xiong improved scheme and Yuan scheme are vulnerable to key replacement attack. To overcome this security weakness, Yu propose a new certificateless signature scheme which is an improved version of the existing schemes. Compared with the previous schemes, their scheme offers shorter system parameters and higher computational efficiency.

A. Computational Problems

The followings are the computational problems that form the basis of the security of the certificateless signature scheme:

- Discrete Logarithm Problem (DLP): Given a cyclic group G of a large prime order q, its one generator P, and an arbitrary $h \in G$, to find an integer $a \in Z^*_q$, such that $h = P^a$.
- Computational Diffie-Hellman Problem (CDHP): Considering a cyclic group G of a large prime order q and its one generator P, for any $a,b \in Z^*_q$, given aP, bP∈G , to compute abP∈G.
- Decisional Diffie-Hellman Problem (DDHP): Considering a cyclic group G of a large prime order q and its one generator P, for any $a,b,c \in Z^*_q$, given aP, bP, cP∈G, to decide whether or not c = ab(mod q).
- Gap Diffie-Hellman (GDH) Group: We define G as a GDH group if G is a group on which DDHP can be solved in polynomial time, but no algorithm can solve CDHP with unnegligible probability within polynomial time.
- The q-Strong Diffie-Hellman problem (q-SDHP): Considering a cyclic group G of a large prime order q and its one generator P, given an arbitrary $a \in Z^*_q$ and a (q + 1)-tuple $(P, aP, a^2P, \ldots, a^qP)$, to find a pair $(c,(c + a)^{-1}P)$ with $c \in Z^*_q$.

IV. THE PROPOSED SCHEME

A certificateless signature scheme has seven polynomial time algorithms including *Setup*, *Partial-Private-Key-Extract*, *Set-Secret-Value*, *Set-Private-Key*, *Set-Public-Key*, *Sign* and *Verify*. The Setup and Partial-Private-Key- Extract algorithms are performed by a KGC. Since Set-Secret-Value, Set-Private-Key, and Set-Public-Key algorithms are executed by the user himself, the key-escrow of the users' private keys is not inherent in a certificateless signature scheme.

Let G_1 and G_2 be an additive cyclic group, multiplicative cyclic group respectively, and e be a bilinear pairing map. Let $H_1:\{0, 1\}^* \rightarrow G_1$ and $H_2:\{0,1\} \times G_1 \rightarrow Z^*_q$ be two hash functions. These are used as a part of the system parameters generated by the KGC. Now the certificateless signature scheme can be described as follows:

Setup:

Let k be the given security parameter.

Let the KGC choose an arbitrary generator $P \in G_1$, and a random $s \in Z^*_q$.

Now set $P_0 = sP$.

Then the system parameters are set as *params* = $<G_1, G_2, e, q, P, P_0, H_1, H_2>$.

The message space is $M = \{0,1\}^*$.

The master secret key is mk=s.

Partial-Private-Key-Extract:

Let *params*, mk and a user Alice's identifier ID_A be given.

The KGC computes $Q_A=H_1(ID_A) \in G_1$

And outputs a partial private key $D_A = s \cdot Q_A \in G_1$.

Set-Secret-Value:

Let *params* be given.

The user Alice selects a random value $x_A \in Z^*_q$ as her secret value.

Set-Private-Key:

Let *params* and the partial private key D_A be given.

Then the user Alice generates her private key as $S_A = x_A \cdot D_A \in G_1$.

Set-Public-Key:

Let *params* and the secret value x_A be given.

Then the user Alice generates her public key as $P_A = x_A \cdot P_0 \in G_1$.

Sign:

Let *params*, ID_A, a message m and the private key S_A be given.

The user Alice randomly chooses a $r \in Z^*_q$ and sets $U = r \cdot Q_A \in G_1$.
Then she computes a signature $\sigma = (U, V)$ for the message m with $V=(r+h)\cdot S_A \in G_1$ and $h=H_2(m, U+P_A) \in Z^*_q$.

Verify:
Let a signature $\sigma=(U,V)$ for the message m, the signer's identity ID_A, and the signer's public key P_A be given.

Then the verifier computes $h=H_2(m, U+P_A) \in Z^*_q$, and then checks whether or not the equation $e(P,V)=e(P_A, U+h\cdot Q_A)$ holds. If not, she rejects the signature. Otherwise, she accepts it.

V. ANALYSIS

Correctness of the proposed scheme is satisfied. In effect, if $\sigma = (U, V)$ is a valid signature of Alice for a message m with the public key P_A, then $h=H_2(m, U+P_A) \in Z^*_q$. The verification is correct, since

$$\begin{aligned} e(P, V) &= e(P, (r+h).S_A) \\ &= e(P, (r+h).X_A.s.Q_A) \\ &= e(X_A.s.P, (r+h).Q_A) \\ &= e(X_A.P_0.r.Q_A+h.Q_A) \\ &= e(P_A, U+h.Q_A) \end{aligned}$$

VI. RESULT AND FINDINGS

With the certificateless scheme, the public key was put into the inputs of the strong anti-collision hash function, and the operation leads to the adversary's failure to replace the user's public key. Considering the one-way property of the hash function, given the public key P_A, it is impossible in computation costs for the adversary of the scheme to find a new public key P_A' and the matched U', V' to satisfy the equation $e(P,V') = e(P_A', U'+h\cdot Q_A)$. And so, our scheme has the security to resist the public key replacement attack under the hardness assumptions of *q*-strong Diffie-Hellman problem and the computational Diffie-Hellman problem. In this proposed scheme, we avoid the special MaptoPoint hash functions, and this improves the efficiency of the proposed scheme. In the signing phase, no bilinear pairings are needed, which also boosts the efficiency of the proposed scheme. Furthermore, in the verifying phase, only two bilinear pairings are needed, which, to some degree, contributes to the efficiency of the proposed scheme.

VII. CONCLUSION

Security and Privacy are the major factors that affect consumers trust in secure electronic transaction. Even though the SET protocol is safe in electronic, it is vulnerable by public key replacement attack under the hardness assumptions of *q*-strong Diffie-Hellman problem and the computational Diffie-Hellman problem. In this paper the certificateless signature scheme is introduced in SET by replacing dual signature. Since the signing and verifying phases are less complexity, the scheme is more efficient. The scheme is simple to be adopted by every parties involved in secure transaction.

REFERENCES

[1] S. S. Al-Riyami, K. G. Paterson, Certificateless Public Key Cryptography. In Proc. Asiacrypt'03, LNCS 2784, Springer Verlag. Lecture Notes in Computer Science Series, 2003.

[2] A. Shamir, Identity-based cryptosystems and signature schemes, Proceedings of Crypto'84, LNCS 196, pp. 47-53, Springer-Verlag, 1985.

[3] P. S. L. M. Barreto, "Efficient and provably-secure identity-based signatures and signcryption from bilinear maps," in Proceedings of Asiacrypt'2005, LNCS 3788, pp. 515-532, Springer-Verlag, 2005.

[4] D. Boneh, B. Lynn, and H. Shacham, "Short signatures from the weil pairings, in Proceedings of Asiacrypt'01," LNCS 2248, pp. 514-532, Springer-Verlag, 2001.

[5] F. Hess, "Efficient identity based signature scheme based on pairings," Selected Areas in Cryptography-SAC 2002, LNCS 2595, pp. 310-324, Springer-Verlag, 2003.

[6] X. Li, K. Chen, and L. Sun, "Certificateless signature and proxy signature schemes from bilinear pairings," Lithuanian Mathematical Journal, vol. 45, no. 1, pp.95-103, 2005.

[7] D. Yum and P. Lee, Generic construction of certificateless signature, Proceedings of ACISP'04, LNCS 3108, pp. 200-211, 2004.

[8] H. Xiong, Z. Qin and F. Li, "An improved certificateless signature scheme secure in the standard model," Fundamenta Informaticae, 88:193-206, 2008.

[9] J.K. Liu, M.H Au, and W. Susilo, "Self-generated-certificate public key cryptography and certificateless signature/encryption scheme in the standard model", Proceedings of 2nd ACM symposium on ICCS, pages 273-283, 2007.

[10] Q. Xia, C.X.Xu and Y.Yu. Key replacement attack on two certificateless signature schemes without random oracles, Key engineering Materials, 439-440:1606-1611, 2010.

[11] Y. Yuan, D. Li, L. Tian and Zhu H., "Certificateless signature scheme without random oracles", ISA 2009, LNCS vol. 5576, Springer, pages 31-40, 2009.

[12] Y. Yu, Mu. G. Wang, Q. Xia and B. Yang, "Improved certifucateless signature scheme provably secure in the standard model, IET Information Security, 6:102-110, 2012.

