International Journal of Computer Applications (0975 - 8887)
Volume 74 - No. 9, July 2013

A Secure Mobile Banking Scheme Based on Certificateless Cryptography in the Standard Security Model

Mohammed Hassouna
Faculty of Computer Studies,
National Ribat University,
P.O.Box 22, Khartoum, Sudan
m.fateh@ribat.edu.sd

Nashwa Mohamed
Faculty of Mathematical Sciences,
University of Khartoum,
P.O.Box 321, Khartoum, Sudan
nafarah@uofk.edu

Eihab Bashier
Faculty of Sciences ant Arts,
Albaha University, P.O. Box: 1988,
Baljurashi, Saudi Arabia
eihabbashier@gmail.com

ABSTRACT

Providing the security services (authenticity, integrity, confidentiality and non-repudiation) all together in mobile banking has remained a problematic issue for both banks and their customers. Both the public key infrastructure (PKI) and the identity-based public key cryptography (IB-PKC) which have been thought to provide solutions to these security services, have their own limitations. While the PKI suffers the scalability and certificate management problems, the identity-based cryptography suffers the key escrow problem. This paper proposes a secure web-based mobile banking scheme using certificateless public key cryptography. Within this scheme, the key generating center(KGC) has an offline connection with a public directory server. Both of the client and the bank's web-server use the identities of each other to obtain the public key of each from the KGC's public directory server. Then, each party computes an authenticated per-session shared secret symmetric key. By using this shared secret key the client can encrypt his username and password to access his banking account and carry out signed banking transactions. As a result, the proposed scheme is secure in the standard model and provides authentication, confidentiality, integrity and non-repudiation. Moreover, the scheme is secure against known key attack, resilient against unknown key share and key-compromise impersonation, and secure against weak perfect forward secrecy.

General Terms:

Certificateless cryptography, Mobile banking

Keywords:

Certificateless cryptography, Key generating center, Mobile banking, Standard security model, Security services

1. INTRODUCTION

Mobile banking is a way for a bank's customer to access banking services using its cell phone to carry out bank transactions. It makes life of customer easier by being able to access his/her accounts anytime anywhere. From the side of bank, it reduces time and effort costs at the different bank branches. Also, quality services mobile banking brings more customers to the bank and makes it competent to the other banks.

Usually, banks enable customers to access their banking accounts through one of four technologies. These technologies are the interactive voice response(IVR), the short messaging service(SMS), the web-based mobile applications and the standalone mobile application clients.

The mobile phones can be connected to the Internet through WAP or Wi-Fi technologies. Because mobile banking have some weaknesses which reduce the trust in the mobile banking, particularly, the problem of being struggling with the task of authenticating a user's identity. Therefore, the customer's serious fraud about mobile banking is the safety of using mobile banking. The customer wants to guarantee that no one else will impersonate his identity to perform banking transactions on his/her banking accounts. On the other hand, the main bank's fraud is whether the customer who claims that he is, is really he is. Also, the bank wants to guarantee that the customer will not deny a transaction that he has performed using mobile banking. Both the bank and the customer would like to be sure that the bank has performed the exact transaction that the customer has carried out.

Public Key Infrastructure (PKI) has been thought of as the most practical solution for the problem of mobile banking security. Based on this thought, many mobile banking systems based on PKI have been proposed (see for example [2, 5, 6, 15] and [22]). Generally, the PKI suffers two problems: scalability and certificate management[1]. The identity-based cryptography [9] came to address these two problems, but could not offer true non-repudiation due to the key escrow problem [1] and [3]. However, few researchers introduced solutions to the problem of the security of mobile banking based on the identity based cryptography. For example Zhao and Aggarwal [21] proposed an end-to-end secure messaging in mobile networks based on identity-based cryptography. Shubat et. al [10] presented an encryption mechanism based on the identity based scheme using elliptic curves to provide end-to-end SMS. The same work of Zhao and Aggrawal [21] was re-introduced by Parasad et. al in [12] in which a secure end-to-end messaging in mobile networks based on identity based cryptography was presented.

The certificateless cryptography is considered a cross between PKI and identity based cryptography[1]. It combines the best features of the PKI and ID-PKC, such as lack of certificates, no key escrow problem, reasonable trust to trust authority and lightweight infrastructure[19]. It provides a solution to the non-repudiation problem, through enabling a user to generate his full long-term private key, where the trusted third party is unable to impersonate the user. However, as far as we know, the use of certificateless cryptography schemes has not appeared in the literature in association with applications. This includes the uses of certificateless encryption[3], [7]; certificateless signatures [13], [18] and [20] and certificateless signcryption[8],[16] and [17].

This paper proposes a secure web-based mobile banking system based on Al-Riyami and Paterson's certificateless cryptography scheme. In the proposed scheme, the KGC server has offline connection with a public directory server. The public directory server holds the system's parameters and the public and partial private keys of the bank's mobile customers. The public directory server can authenticate itself to the mobile clients through a challenge. The mobile client runs handshake protocol with the bank's web-server to first authenticate each other and generate a per-session shared symmetric key, using this key to encrypt the transactions that mobile client does later.
The rest of this paper is organized as follows. Section 2 gives backgrounds about mobile banking technologies. In Section 2.5, we introduce the concept of certificateless public key cryptography. In Section 3, we introduce the proposed secure mobile banking scheme using certificateless cryptography. Section 0**??** discusses security properties provided by the proposed scheme. Finally, Section 5 concludes the paper.

2. BACKGROUNDS

In this section, backgrounds about the methods by which a mobile client can access the mobile banking services are introduced. As stated in the previous section, there are four technologies to access the mobile banking services. These technologies are interactive voice response, the short messaging service, the web-based and the stand-alone mobile application clients.

2.1 Interactive Voice Response

The interactive voice response (IVR) enables the communication between a customer and a service provider (which is a bank in our case). After the customer calls some predefined number to activate a service, a computer program at the service provider side provides a list of given choices to the customer using voice and the customer responds via touch-tone selection. The interaction continues between the customer and his service provider until he gets the service(s) done.

2.2 Short Messaging Service

In the short messaging service (SMS), the customer requests a service or specific information by sending an SMS containing the service command to a prespecified number. Then the bank responds to the customer by a message informing the delivery of the service or containing the specific information.

2.3 Web-based Mobile Banking

Mobile phones have very limited resources (CPUs, memories, display capabilities, input facilities and battery powers) and the wireless networks have narrower bandwidths compared to the wired networks. Moreover, the mobile networks can utilize the WAP protocol which is not IP-based and therefore they do not support the standard Internet protocols. The Wireless Application Protocol (WAP) aimed at enabling the mobile phones and the other wireless devices to access the Internet contents and web services. The WAP does allow the use of the Extensible Hypertext Markup Language (XHTML) to build platform-independent wireless applications. The different releases of the WAP support the standard Internet protocols, such as TCP, IP and HTTP and can operate over all the wireless technologies, such as the Code Division Multiple Access (CDMA), the General Packet Radio Service (GPRS) and the third generation (3G) cellulars. WiFi is a wireless technology brand owned by the Wi-Fi Alliance intended to improve the operating of wireless products. Common applications for Wi-Fi include Internet and VoIP phone access, gaming, and network connectivity for consumer electronics such as mobile phones, laptops, game consoles, MP3 players and PDA's. Wi-Fi also allows connectivity which enables devices to connect directly with each other. This connectivity mode is useful in consumer electronics and gaming applications.

2.4 Standalone Mobile Application

Standalone mobile applications allow accessing mobile services (including mobile banking) through user's interfaces. It enables the implementation of secure and reliable channel of communication.
Running mobile applications require that the mobile device does support at least one development environment, such as J2ME, android or Qualcomm's BREW. The mobile applications clients require being downloaded (from the service provider's website) on the client device before they can be used.
The major disadvantage of mobile application clients is that the applications need to be customized to each mobile phone on which it might finally run, for example J2ME ties together the API for mobile phones which have the similar functionality in what it calls 'profiles', android applications need Dalvik Virtual Machine(DVK) to be installed and run in any mobile device.

2.5 Certificateless Public Key Cryptography (CL-PKC)

In 2003 Al-Riyami and Paterson [1] introduced the concept of Certificateless Public Key Cryptography (CL-PKC) to overcome the key escrow limitation of the identity-based cryptography. In CL-PKC a trusted third party called Key Generation Center (KGC) supplies a user with partial private key, the user then combine the partial private key with a secret value (unknown to the KGC) to obtain his full private key. In this way the KGC does not know users private keys. Then the user combines the same secret value with the KGC's public parameters to compute his public key.
Compared to identity based public key cryptography (ID-PKC), the trust assumptions made of the trusted third party in CL-PKC are much reduced. In ID-PKC, users must trust the private key generator (PKG) not to abuse its knowledge of private keys in performing passive attacks(decrypting the traffic that sent to the customer), while in CL-PKC, users need only trust the KGC not to actively propagate false public keys[1].
In CL-PKC users can generate more than one pair of key(pubic/private) for the same partial private key. To guarantee that KGC does not replace user's public keys Al-Riyami and Paterson[1] introduced a binding technique to bind a user's public key with his identity. In their binding scheme, the user first fixes his secret value and his public key and supplies the KGC his public key. Then the KGC redefine the identity of the user to be the user's identity concatenated with his public key. By this binding scheme the KGC replacement of a public key apparent, and equivalent to a CA forging a certificate in a traditional PKI.

Al-Riyami and Paterson Scheme. In this section a general description to Setup, Set-Secret-Value, Partial-Private-Key-Extract, Set-Private-Key and Set-Public-Key algorithms as introduced by Al-Riyami and Paterson [1] is introduced.
Let k be a security parameter given to the Setup algorithm and $\mathcal{IG}$ be a Bilinear Diffie-Hellman Problem (BDH) parameter generator with input k.

Setup (running by the KGC): this algorithm runs as follows:
(1) Run $\mathcal{IG}$ on input k to generate output $< G_1, G_2, e >$ where G_1 and G_2 are groups of some order q and $e : G_1 \times G_1 \longrightarrow G_2$ is a pairing.
(2) Choose an arbitrary generator $P \in G_1$.
(3) Select a master-key s uniformly at random from $\mathbb{Z}_q^*$ and set $P_0 = sP$.
(4) Choose cryptographic hash functions

$$H_1 : \{0,1\}^* \longrightarrow G_1^*$$

and

$$H_2 : G_2 \longrightarrow \{0,1\}^n$$

where n is the bit-length of plaintexts taken from some message space $M = \{0,1\}^n$ with a corresponding ciphertext space $C = G_1 \times \{0,1\}^n$.

Then, the KGC publishes the system parameters $params =< G_1, G_2, e, n, P, P_0, H_1, H_2 >$, while the secret master-key s is saved secure by the KGC.

Set-Secret-Value (running by the user): The inputs of this algorithm are *params* and entity *m's* idntifier ID_m. It selects $x_m \in \mathbb{Z}_q^*$ at random and output x_m as *m's* secret value. Then, the entity m computes $X_m = x_m P$ and sends X_m to the KGC.

Partial-Private-Key-Extract (running by the KGC): The inputs of this algorithm are an identifier $ID_m \in \{0,1\}^*$ and X_m. The algorithm carries out the following steps to construct the partial private key for entity m with identifier ID_m.

—Compute $Q_m = H_1(ID_m || X_m)$.

—Output the partial private key $D_m = sQ_m \in G_1^*$.

Entity m when armed with it's partial private key D_m, it can verify the correctness of the partial private key D_m by checking $e(D_m, P) = e(Q_m, P_0)$.

Set-Private-Key (running by the user): The inputs of this algorithm are *params*, D_m (the parital private key of entity m) and $x_m \in \mathbb{Z}_q^*$ (the secret value of entity m. It transforms the partial private key D_m to a private key S_m by computing $S_m = x_m D_m = x_m s Q_m \in G_1^*$.

Set-Public-Key (running by the user): The inputs of this algorithm are *params* and $x_m \in \mathbb{Z}_q^*$ -which is the secrete value of entity m. It then constructs the public key of identity m as $P_m =< X_m, Y_m >$, where $X_m = x_m P$ and $Y_m = x_m P_0 = x_m s P$.

3. THE PROPOSED MOBILE BANKING SCHEME

This section describes the proposed certificateless web-based mobile banking scheme. In this scheme, we make use of the CL-PKC that proposed by Al-Riyami and Paterson [1] and described in the previous section. The mobile network operator has the role of an internet service provider. The scheme consists of four servers, their details are as follows:

(1) The bank's database server in which the records and information of the bank's customers are stored.

(2) The bank's web-server(or application server) which is a middleware between the bank's customer and the bank's database server and is responsible for hosting the bank's web applications that enable the banking services and handling all bank's customers transactions. The bank's web-server has an offline connection with the bank's database server. The domain name of the bank's web-server is used as its identity.

(3) The Key Generation Center server (KGC) is a trusted third party which is responsible for generating it's private and public keys, the system parameters and to compute the partial private keys of the bank's customers. The KGC has an off-line connection with the public directory server in which it publishes the system public parameters and the partial private keys and keep it's private key secure as it's master secret key, so in case of any attack made to the public directory server, the attacker will not be able to get the master secret of the KGC server.

(4) The public directory server is trusted third party in which system parameters, the identities, public keys and partial private keys of the bank's customers are stored. The partial private keys are generated by the KGC using the identities, public keys and the system's parameters.

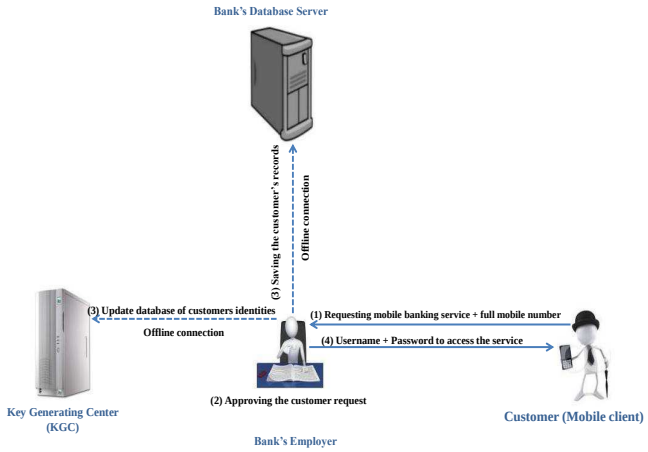

Fig. 1. Customer registration for mobile banking services.

Before being able to access mobile banking services, a customer must apply for the service by meeting the bank's employer and provides his account number(s) and mobile station international subscriber directory number(MSISDN) which is considered the customer's identity. Then the bank's employee opens offline connections with both the bank's database server(and check if there exists such customer with such account number(s) in the database) and the KGC server to insert the customer's information and generates a username, password for this new subscriber. The procedure of registering a customer for mobile banking services is explained by Fig. 1.

The public directory server authenticate itself to the bank customer through the KGC server using a challenge as follows:

—the customer sends his account number encrypted by his given password using any password-based cryptosystem to the KGC server.

—the KGC server receives the customer's encrypted message, decrypts it and sends back the customer's account number plus his username encrypted with same customer's password and using the same used password-based cryptosystem.

—if the customer can decrypt the encrypted message that received from the KGC server, then the customer trusts on the KGC server(and it's public directory), otherwise it reject the connection.

—at this point both the customer and KGC server authenticate each other.

—then the customer send

When a customer wants to request a banking service, it does the following:

—downloads the public key of the bank's web-server from the public directory server.

—generates a random number $t \in Z_q^*$, encrypts it with the public key of the bank's web-server and send it to the bank's web-server in a hello message.

—the customer also computes a shared secret symmetric key using the public key of the web-server, its own private key and the random number t.

—on the other hand, when the bank's web-server receives the hello message of the mobile client, it validates the identity of the mobile client from the database server.

—requests the public key of the mobile clients, decrypts the encrypted value of t and use its own private key, the mobile

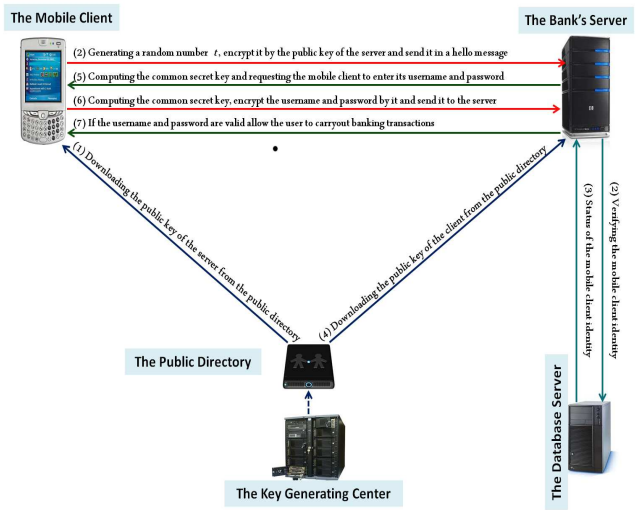

Fig. 2. The certificateless mobile banking scheme.

client's public key and the value t to compute the per-session symmetric key.

—at this point, phase two of the protocol is initiated by using the shared session key to secure the channel between the mobile client and the bank's web-server.

—hence, the bank's web-server requests the mobile client to provide its username and password. The mobile client then encrypts its username and password with the computed symmetric key and sends it to the bank's web-server, where it is decrypted and verified before enabling the customer to carry out banking transactions.

—all the subsequent message exchanges between the mobile client and the bank's web-server are signed, by using an elliptic curve digital signature.

The full description of the procedure of enabling a mobile client to access mobile banking services is explained by Figure 2.
To show that the mobile client and the bank's web-server obtain the same per-session secure symmetric key, we start by assuming that a mobile client has a private key $S_m = x_m D_m$, a public key $P_m =< X_m, Y_m >$ and the bank's web-server's private key is $S_b = x_b D_b$ and public key is $P_b =< X_b, Y_b >$. Then, the common authenticated per session secret key can be computed at both sides of mobile client and bank's web-server as follows(handshake phase).

(1) The mobile client:
—generates a random positive integer t, uses it to compute

$$K_{mb} = H_2(Q_m||Q_b||tx_mX_b),$$

where $Q_m = H_1(ID_m||X_m)$ and $Q_b = H_1(ID_b||X_b)$.
—encrypts $t^* = E_{P_b}(t)$ using bank web-server's public key and sends hello message to the bank web-server including t^*.

(2) The bank's web-server decrypts t^* to obtain $t = D_{S_b}(t^*)$ using his private key, and computes

$$K_{bm} = H_2(Q_m||Q_b||tx_bX_m),$$

Then, sends hello message back to the mobile client.

(3) The mobile client encrypts its username and password using the key K_{mb} to obtain the cipher text $C = E_{K_{mb}}(M)$, where M denotes the username/password and sends C(the encrypted message) to the bank's web-server.

(4) The bank's web-server decrypts the message C using the corresponding decryption function to obtain $M' = D_{K_{bm}}(C)$.

(5) The bank's web-server verifies the validity of the username and password from the database server. If valid, it enables the mobile client to carry out banking transactions.

(6) All subsequent transactions between the mobile client and bank's web-server are processed as follows.
   (a) The mobile client
   —encrypts the message Msg using symmetric algorithms to obtain $Cipher = E_{K_{mb}}(Msg)$.
   —signs the encrypted message C using an elliptic curve digital signature algorithm (ECDSA) algorithm [14], [4], its private key and public parameters obtaining the signature (r, s).
   —sends $Cipher$ and the signature (r, s) to the bank's web-server.
   (b) The bank's web-server verifies the signature (r, s), if valid, the bank's web-server decrypts the message $Cipher$ using the corresponding symmetric decryption algorithm $Msg = E_{K_{bm}}(Cipher)$.

It can be easily proven that the two computed keys K_{mb} and K_{bm} are equal:

$$\begin{aligned} K_{mb} &= H_2(Q_m||Q_b||tx_mX_b) \\ &= H_2\left(Q_m||Q_b||tx_mx_bP)\right) \\ &= H_2(Q_m||Q_b||tx_bx_mP) \\ &= H_2(Q_m||Q_b||tx_bX_m) = K_{bm} \end{aligned}$$

4. SECURITY ANALYSIS

Since our CTAKA protocol is based on the Elliptic Curve Discrete Logarithm(ECDLP) and Collision Resistant hash function standard cryptographic primitives, then it is secure against standard security model, in this section the cryptographic primitives or assumptions that we based our protocol on are discussed. Also, stated some of the security properties that are provided by the proposed scheme. The following general definition of negligible function is required.
Definition. A real-valued function $\epsilon(k)$ is said to be *negligible* in k if for all $c > 0$, there exists $k_c > 0$ such that $k > k_c$ implies $\epsilon(k) < \frac{1}{k_c}$. A function that is not negligible is known as *non-negligible*.

4.1 Collision Resistant Hash Function Assumption

A hash function $H \longrightarrow H(k)$ is collision resistant if for all probabilistic polynomial time(PPT) algorithms A the advantage

$$\begin{aligned} Adv_A^{CR}(k) &= Pr[H(x) = H(y) \wedge x \\ &\neq y \mid (x, y) \longrightarrow A(1^k, H) \wedge H \longrightarrow H(k)] \end{aligned}$$

is negligible as a function of the security parameter k.

4.2 Ellitpic Curve Discrete Logarithm Problem(ECDLP) Assumption

Given two points $P, Q \in E(F_q)$ on an elliptic curve, ECDLP determines the integer a, satisfying $Q = aP$, where P has order n, provided that such $k < n$ exists. So the advantage of any PPT algorithm A to find a given P, Q is negligible as function of security parameter k or $Adv_A^{ECDLP}(k) = Pr[find\ a$ such that $Q = aP] \leq \epsilon$.
Also the proposed system provides the following security properties. We follow Swanson and Jao [11] in the statement of some of these properties in terms of our scheme.

(1) **Long-term binding public key with corresponding private key:** the long term public key $P_m = (X_m, Y_m)$

is related to the partial private key D_m, since $D_m = sH_1(ID_m||X_m)$. Therefore, there is one-to-one correspondence between the public key and the partial private key of either the mobile client or the bank's web-server, and insures that mobile client/bank's web server can create only one long term public key for the corresponding private key. The existence of two valid public keys for the same identity (mobile client or bank's web-server) guarantees that the KGC will be identified to misbehaved in issuing both corresponding partial private keys.

(2) **Key agreement without interactions:** the most probable attack during the run of a key agreement protocol, is the man-in-the-middle attack. Our proposed key agreement provides resistance against the man-in-the-middle attack, by enabling both the mobile client and the bank's web-server to compute the shared secret key using its own private key, the other party's public key and a randomly generated number (by the mobile client), without any interaction between the two communicating parties (mobile client and bank's web-server).

(3) **Authentication:** since the shared per-session secret key is generated using Mobile's client private key and bank's web-server public key and public parameters, then authentication of entities are provided. Also any party can check the authenticity of the public key by running the pairing operation.

(4) **Confidentiality:** confidentiality is provided by the scheme because a symmetric cryptosystem for encryption/decryption is used.

(5) **Integrity and non-repudiation:** the mobile client signs the message using the ECDSA algorithm, its private key and public parameters, so the integrity of the message is provided. Also the mobile client cannot deny sending a message because the message is signed by mobile client's private key. Also, the KGC cannot impersonate the mobile client to perform banking transactions since any transaction must be signed by the mobile client's private key.

(6) **Known key security:** Each session key is unique, because both the mobile client and the bank's web-server make use of a random number t which is generated in each protocol run, thus the knowledge of previous session keys (if it happened to be) does not help an adversary to derive information about other session keys.

(7) **Unknown key share resilience:** The public parameters Q_m and Q_b are included in the computation of the common secret key. Therefore, both the mobile client and the bank's web-server know who they share the key with.

(8) **Key-compromise impersonation resilience:** An adversary who has compromised the long-term private keys of the mobile client m is unable to impersonate other party to mobile client m because the shared key contains the identities of the mobile client and the other party.

(9) **Weak perfect forward secrecy:** Suppose that an adversary has compromised long-term secret keys $S_m, S_b, x_m, x'_m, x_b, x'_b, D_m$ and D_b, he cannot obtain the secret random number t, because these long-term secret keys are unrelated to the random number t, thus the adversary is unable to determine previously established session keys.

5. CONCLUSIONS AND REMARKS

This paper discussed the weaknesses of the existing mobile banking schemes, particularly the PKI based mobile banking schemes and schemes based on identity based cryptography. Then, it introduced a web-based a secure mobile banking scheme based on certificateless cryptography.

In the proposed certificateless web-based mobile banking scheme, the KGC server has an offline connection with the public directory server. The KGC's public directory can authenticate itself to the mobile clients through a certificate. Both the bank's service provider and the mobile client are able to compute the same secret session symmetric key. All the interactions between the mobile client and the bank's service provider are secured by encryption/decryption (using the public key of the bank's web-server and the computed symmetric authenticated key) to guarantee confidentiality, and digital signature (using an elliptic curve digital signature algorithm) to guarantee the integrity and to provide full non-repudiation.

Since our proposed CTATA based on ECDLP and Collision Resistant hash function cryptographic primitives, then it is secure against standard security model, the security features that are provided by the proposed scheme include an authenticated key agreement protocol, confidentiality which is achieved through the encryption of transactions, integrity and non-repudiation which are provided by the elliptic curve digital signature. Moreover, the scheme is secure against known key attack, resilient against unknown key share and key-compromise impersonation, secure against weak perfect forward secrecy and man-in-the-middle attacks.

Compared to the CTAKA protocol presented by Yang et. al [19], the proposed scheme in this paper is resistant to the key escrow problem. This comes in contrast to the scheme proposed by Yang et. al in [19] where the KGC can easily compute the full private key for user m by multiplying the public term Y_m by its master secret value s.

With those security properties provided by the proposed mobile banking scheme, there is no thought possible attack on the scheme at any of its stages.

6. REFERENCES

[1] S.S. Al-Riyami and K.G. Paterson. Certificateless public key cryptography. In C.S. Laih, editor, *Asiacrypt 2003*, Lecture Notes in Computer Science, pages 452–473, 2003. Full version available at Cryptology ePrint Archive.

[2] Shaghayegh Bakhtiari, Ahmad Baraani, and Mohammad-Reza Khayyambashi. Mobicash: A new anonymous mobile payment system implemented by elliptic curve cryptography. In Mark Burgin, Masud H. Chowdhury, Chan H. Ham, Simone A. Ludwig, Weilian Su, and Sumanth Yenduri, editors, *CSIE (3)*, pages 286–290. IEEE Computer Society, 2009.

[3] Alexander W. Dent, Benoît Libert, and Kenneth G. Paterson. Certificateless encryption schemes strongly secure in the standard model. In *Public Key Cryptography*, pages 344–359, 2008.

[4] Patrick Gallagher, Deputy Director Foreword, and Cita Furlani Director. Fips pub 186-3 federal information processing standards publication digital signature standard (dss), 2009.

[5] C. Narendiran, S.A. Rabara, and N. Rajendran. Performance evaluation on end-to-end security architecture for mobile banking system. *Wireless Days, 2008. WD '08. 1st IFIP*, pages 1–5, 2008.

[6] C. Narendiran, S.A. Rabara, and N. Rajendran. Public key infrastructure for mobile banking security. *Global Mobile Congress 2009*, pages 1–6, 2009.

[7] S. Sharmila Deva Selvi, S. Sree Vivek, and C. Pandu Rangan. Cca2 secure certificateless encryption schemes based on rsa. *IACR Cryptology ePrint Archive*, 2010:459, 2010.

[8] S. Sharmila Deva Selvi, S. Sree Vivek, and C. Pandu Rangan. Certificateless kem and hybrid signcryption schemes revisited. In *ISPEC*, pages 294–307, 2010.

[9] A. Shamir. Identity-based cryptosystems and signature schemes. In *In Advances in Cryptology-CRYPTO'84*, volume 196, pages 47–53, 1984.

[10] S.A. Shubat and M.A. Ashraf. Secure protocol for short message service. In *Proceedings of world academy of science, engineering and technology*, volume 49, 2009.

[11] C. Swanson and D. Jao. A study of two-party certificateless authenticated key-agreement protocols. In *Proceedings of the 10th International Conference on Cryptology in India: Progress in Cryptology*, INDOCRYPT '09, pages 57–71, Berlin, Heidelberg, 2009. Springer-Verlag.

[12] M.Sunanda V.R. Prasad and V. Maruthi Prasad. Secure sms with identity based cryptography in mobile telecommunication networks. *International Journal of Computer Science and Technology*, 2, 2011.

[13] C. Wang, D Long, and Y. Tang. An efficient certificateless signature from pairing. *International Journal of Network Security*, 8(1):96–100, 2009.

[14] Erik De Win, Serge Mister, Bart Preneel, and Michael J. Wiener. On the performance of signature schemes based on elliptic curves. In *Proceedings of the Third International Symposium on Algorithmic Number Theory*, pages 252–266, London, UK, 1998. Springer-Verlag.

[15] K. Wouters, G. Van Damme, and N. Luyckx. A pki-based mobile banking demonstrator, 8th european workshop on public key infrastructure. *services and applications*, 48:203–20, 2011.

[16] Wenjian Xie and Zhang Zhang. Certificateless signcryption without pairing. *IACR Cryptology ePrint Archive*, 2010:187, 2010.

[17] Wenjian Xie and Zhang Zhang. Efficient and provably secure certificateless signcryption from bilinear maps. In *WCNIS*, pages 558–562, 2010.

[18] H. Xiong, Z. Qin, and F. Li. An improved certificateless signature scheme secure in the standard model. *Fundamenta Informaticae*, 88, 2008.

[19] H. Yang, Y. Zhang, and Y. Zhou. An improved certificateless authenticated key agreement protocol. Cryptology ePrint Archive, Report 2011/653, 2011. `http://eprint.iacr.org/`.

[20] L. Zhang and F Zhang. A new provably secure certificateless signature scheme. In *08 IEEE International Conference on Communications*, pages 1685–1689, 2008.

[21] S. Zhao, A. Aggarwal, and S. Liu. Building secure user-to-user messaging in mobile telecommunication networks. In *Wireless Telecommunications Symposium (WTS) 2008*, pages 151–157, 2008.

[22] L. Zhuo, T. Wang, J. Zhong, H. Shu, L. Wang, and F. Zhu. Design of secure access system of mobile bank based on pki with smart card. In *2011 2nd International Conference on Artificial Intelligence, Management Science and Electronic Commerce (AIMSEC)*, pages 1057 – 1060, 2011.