International Journal of Computer Applications (0975 - 8887)
Volume 121 - No. 7, July 2015

Mobile Banking System based on certificateless Chameleon Hash Function

Tejeshwari Thakur
School of Studies in Mathematics
Pt.Ravishankar Shukla University
Raipur (C.G.)492010, India

Birendra Kumar Sharma
School of Studies in Mathematics
Pt.Ravishankar Shukla University
Raipur (C.G.)492010, India

ABSTRACT

Mobile phones are most common way of communication and accessing internet based services. Currently, mobile phones are not only used for regular data communication but also, sending and receiving sensitive data. However, the security of mobile communication is very important concerns for mobile phone users. In this paper we first proposes new payment system with mobile banking, using certificateless chameleon hash function which is does not suffer from the key escrow problem. The proposed scheme is secure known key attack, key compromise attack and unknown share key attack. Also proposed more efficient and low computational cost compare the [11].

Keywords

Chameleon Hashing; Certificateless Cryptography; Mobile Banking;

1. INTRODUCTION

Electronic banking through Internet has boosted the e-trade drastically. It has decreased the time, cost and improved the customer facility. E-banking activity has become more popular when e-banking has sifted desktop to mobile such banking is knows as mobile banking, which provide the economic services through internet the business and e-commerce new trade of banks system. Mobile banking is the service that allows a mobile client to request and receive information about a personal account, or to transfer funds between accounts using the personal mobile phone. Many researchers proposed different aspect of mobile telecommunication in [7, 9, 10, 13, 14]

Mobile banking provide some facilities to conduct the bank transactions, to administer accounts and to access customized information, but mobile banking have some weaknesses which reduce the trust in the mobile banking particularly, the problem of being struggling with the task of authenticating, message leak and important task is security (for example unknown key share and key compromise attack). And this problem solve certificateless chameleon hash function because, anyone can compute the hash value but only the holder of the trapdoor is able to find the collision of the given value. Chameleon hash function introduce by Krawczyk et al.[6] in 2000, proposed new paradigm chameleon hash function, In this algorithm is a trapdoor one-way hash function without the knowledge of the associated trapdoor. The concept of ID based chameleon hash have been proposed [1, 4, 12], and it has been a useful primitive for constructing chameleon signatures [3]. Recently [5], proposed new design certificateless chameleon hash scheme which is key exposure free. we use the certificateless chameleon hash function to give a new approach of using mobile banking protocol. Our new constructions provide stronger security, avoid unknown key share and key compromise attack and also reduce the computation cost of a bank transaction.

The rest of this paper organized as follows: First we describe the background of the proposed design in section 2. The proposed algorithm and security of certificateless chameleon hashing is introduced in section 3. Proposed the mobile banking using certificateless chameleon hashing scheme and their security introduced in the section 4. Efficiency proposed design in described section 5. Finally, we conclude our opinion in section 6.

2. BACKGROUND CONCEPTS

In this section, we briefly review the basic concepts on bilinear pairings and certificateless chameleon hash scheme [5] as below.

(1) **Bilinear Pairing:** [2] Let G_1 be a cyclic additive group generated by P, whose order is a prime q and G_2 be a cyclic multiplicative group of the same order q. Let a and b be elements of Z_q^*. A bilinear pairings is a mapping $e : G_1 \times G_1 \to G_2$ with the following properties:
—Bilinear: $e(aP, bQ) = e(P, Q)^{ab}$
—Non-degenerate: There exists P and $Q \in G_1$ such that $e(P, Q) \neq 1$.
—Computable: There is an efficient algorithm to compute $e(P, Q)$ for all $P, Q \in G_1$.

(2) **Certificateless Chameleon Hashing:** A certificateless chameleon hash scheme [5, 8] consists of following phases:
—**Setup:** This algorithm, run by the KGC, takes a security parameter as an input, and then returns the master secret key, and system parameter.
—**Partial-Private-Key-Extract:** This algorithm, run by the KGC, takes parameter, and a users identity ID as inputs. It generates a partial-private-key D_{ID}, and sends it to the user via a secure channel.
—**Set-Secret-Value:** This algorithm, run by a user, returns a secret value,x_{ID}.

—**Set-Secret-Key:** This algorithm, run by a user, takes the users partial private- key D_{ID} and the secret value x_{ID} as inputs, then returns the users full secret key, sk_{ID}.
— **Set-Public-Key:** This algorithm, run by a user, takes parameter and the users full secret key as inputs, and returns a public key PK_{ID} for the user.
—**Hash:** A probabilistic polynomial algorithm which, on input an identity string ID, message m and random string r, outputs the hashed value

$$h = Hash(ID, PK_{ID}, m, r)$$

Note that H does not depend on TK.
—**Forge:** A deterministic polynomial algorithm F is that, on input the trapdoor key TK associated to the identity string ID, a hash value h of a message m, a random string r, and another message $m' \neq m$, outputs a string r' that satisfies $h = Hash(ID, PK_{ID}, m, r) = Hash(ID, PK_{ID}, m', r')$. Moreover, if r is uniformly distributed in a finite space R, then the distribution of r' is computationally indistinguishable from uniform in R.

(3) **Security Requirements of Certificateless Chameleon Hash Scheme:** A secure chameleon hashing scheme [5] satisfies the following properties:

—**Collision Resistance:** Without the knowledge of trapdoor key TK, there exists no efficient algorithm which on input, a message m, a random string r, and another message m', outputs a string r' that satisfy $Hash(ID, m', r', PK_{ID}) = Hash(ID, m, r, PK_{ID})$, with non-negligible probability.
—**Semantic Security:** For all pairs of messages m and m', the probability distributions of the random values $Hash(ID, m', r')$ and $Hash(ID, m, r)$ are computationally indistinguishable.
—**Key Exposure Freeness:** If a recipient has never computed a collision under ID, then there is no efficient algorithm for an adversary to find a collision for a given chameleon hash value $Hash(ID, m, r)$. This must remain true even if the adversary has oracle access to F and is allowed polynomially many queries on triples (ID_i, m_i, r_i) of his choice, except that ID_i is not allowed to equal the challenge ID.
—**Message Hiding:** For all identity strings ID, assume that the recipient has computed a collision (m', r') such that

$$h = Hash(ID, PK_{ID}, m', r') = Hash(ID, PK_{ID}, m, r)$$

, where m is the original message that was hashed. Then the signer, upon seeing the claimed values (m', r'),can successfully compute another collision $(m", r")$ such that $h = Hash(ID, PK_{ID}, m", r")$, without revealing the message m.

2.1 Process of Mobile Banking and proposed scheme

In this section, first explain the methods of mobile client can access the mobile banking services and second proposed scheme are introduced.

(1) **Process of Mobile Banking**

The mobile banking system contain data processing center and mobile banking unit. The data processing unit is mainframe for storing the data and processing the transactions. The mobile banking includes different terminals like ATM machines, number of wireless connections from handsets/PDAs etc..A typical design of mobile banking is shown below.

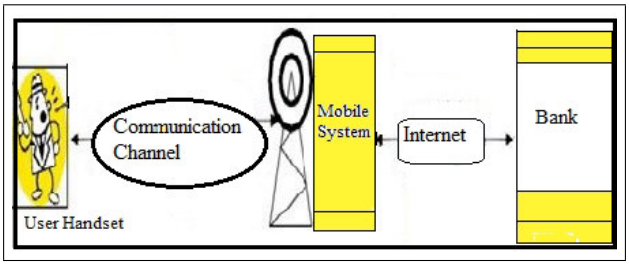

Fig. 1. Process for Mobile Banking.

(2) **Process of Proposed scheme**

The proposed scheme present the communication between mobile client and bank web server following the procedures: The first steps customer register to mobile banking. The registration process is different way such that customer meet the bank's employer and apply the mobile banking service in our mobile and employer provides his account number(s) and mobile subscriber directory number, which is considered the customer's identity. Then the bank's employee opens off-line connections with both the bank's database server(and check if there exists such customer with such account number(s) in the database).

—The bank's database server store the records and information of the bank's customers. Bank's web-server which is a center point 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 off-line connection with the bank's database server.

—Mobile banking have some weak point which decrease the trust in the mobile banking, particularly, the problem of being struggling with the task of authenticating a users identity. Therefore, the customers serious deception about mobile banking is the safety of using mobile banking. This situation need to KGC (The Key Generation Center server) is trusted third party because KGC server to the customers information and generates a user name, pass word for this new subscriber. KGC has an off-line connection with the public directory server in which it publishes the system public parameters, private key public keys and to compute the partial private keys of the banks customers.

—**Starting The Process:**-The mobile client and the banks web-server obtain the same per-session secure symmetric key. The mobile client generates a random positive number and identity of bank web-server and uses the hash value. Encrypt the message using random no. and send to bank web-server.

—Bank web-server decrypt the mobile client random no. using private key and compute the message, sends back to the mobile client.

—The mobile client encrypt its user name and pass word using the key obtain the bank-web server and send to the encrypted message(cipher text) bank-web server.

—The banks web-server decrypts the message (cipher text) using the corresponding decryption function.

—The banks 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.

3. CERTIFICATELESS CHAMELEON HASHING SCHEME:

Propose a certificateless chameleon hash scheme consists of following phases:

(1) **Setup:** Let the security parameter k as input and G_1 be a GDH group generated by P, whose order is a prime q and G_2 be a cyclic multiplication group of some order q and $e : G_1 \times G_1 \rightarrow G_2$ is a pairing. KGC choose a random integer from Z_q^* and set $P_{pub} = sP$. Let $H_1 : \{0,1\}^* \rightarrow G_1$ and $H_2 : G_2 \rightarrow \{0,1\}^n$ be a full domain collision-resistant hash function, where n is the bit length of plain-texts taken from some message space $M = \{0,1\}^n$ with a corresponding cipher text space $C = G_1 \times \{0,1\}^n$. The system parameter are $SP = \{G_1, G_2, e, q, n, P, P_{pub}, H_1, H_2\}$

(2) **Extract:** Given an identity string ID on message m. It select random number $x_m \in Z_q^*$, where x_m is secret value. Then, the entity m computes $X_m = x_m P$ and send X_m to KGC. KGC computes the partial private key $D_{ID_m} = sH_1(ID \parallel X_m) = sQ_{ID_m}$. The trapdoor key is $SK_{ID_m} = \{x_m D_{ID_m}\}$ and public key is $PK_{ID_m} = \{X_m, Y_m\}$, where $X_m = x_m P$ and $Y_m = x_m P_{pub} = x_m sP$.

(3) **Hash:** On input the identifier ID on message m and the hash key PK_{ID_m}, the random integer $x_b \in Z_q^*$ and computes $r = x_m X_b = x_m x_b P = x_b x_m P = x_b X_m$. Our proposed chameleon hash function is defined as below:

$$h = Hash(b, m, r, PK_{ID}) = e(r, P)e(mQ_{ID_b}, P_{pub})$$

Note: h does not depend on trapdoor key SK_{ID_m}.

(4) **Forge:** For any hash value h, the algorithm F can be used to compute a string with the trapdoor key $SK_{ID_m} = x_m D_{ID_m}$ as follows:

$$r' = Forge(b, m, m', x_{ID}, D_{ID}, PK_{ID}) = X'_m = x_b^{-1}(m - m')D_{ID_b} + X_m$$

Note that if $Hash(ID, m, r, PK_{ID}) = Hash(ID, m', r', PK_{ID})$ then forgery is successful.

3.1 Security Feature:

The above certificateless chameleon hash scheme enjoys the properties of collision resistance, message hiding, semantic security, and key-exposure freeness. For detail one can reffer to Hou [5].

4. PROPOSED MOBILE BANKING SYSTEM USING CERTIFICATELESS CHAMELEON HASH FUNCTION:

Using the chameleon hashing scheme described in Section 3, we proposed Mobile Banking System. First proposed the session secret key computed at both sides of mobile client and banks web-server signed by digital signature using chameleon hash function. The full decryption of algorithm is given below:
Our algorithm consisting in four phases. we start by assuming that a mobile client has a private key $SK_{ID_m} = x_m D_{ID_m}$, a public key $PK_{ID_m} = \{X_m, Y_m\}$ and the bank web-servers private key is $SK_{ID_b} = x_b D_{ID_b}$ and public key is $PK_{ID_b} = \{X_b, Y_b\}$.

—**Phase 1:** The mobile client generate random positive integer j and uses it to compute.

$$C_m = H_2(h, D_{ID_m}, D_{ID_b}, PK_{ID_m}, PK_{ID_b}, jx_m X_b)$$

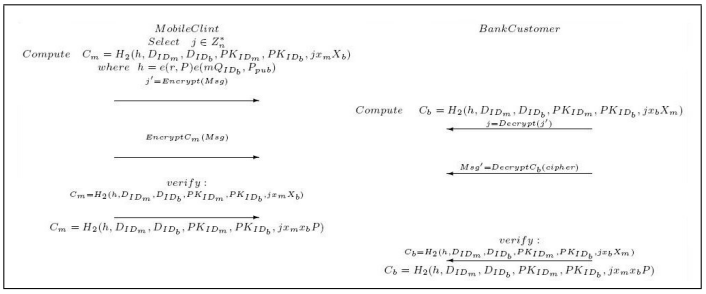

Fig. 2. Process for Mobile Client and Banking Web Server.

In such a protocol run, the session ID and chameleon hash function of the protocol and instance is:

$D_{ID_m} \parallel D_{ID_b} \parallel PK_{ID_m} \parallel PK_{ID_b}$. And
$h = e(r, P)e(mQ_{ID_b}, P_{pub}) = e(x_m X_b, P)e(mQ_{ID_b}, P_{pub})$
where, $Q_{ID_m} = sH_1(ID_m \parallel X_m), Q_{ID_b} = sH_1(ID_b \parallel X_b)$.

-encryption $j' = Encyt_{PK_{ID_b}}(j)$ using bank web-server public key and send Hii message to the bank web-server including j'.

—**Phase 2:** The bank's web server decrypt j' to obtain $j = Decy_{SK_{ID_b}}(j')$ using his private key and computes

$$C_b = H_2(h, D_{ID_m}, D_{ID_b}, PK_{ID_m}, PK_{ID_b}, jx_b X_m),$$

and send Hii message back to the mobile client.

—**Phase 3:** The mobile client encrypt its user name and password using the key C_m to obtain the cipher key $Encyt_{C_m}(Msg)$ where Msg denote the username/password and sends cipher text (encrypted the message) to the bank's web-server.

—**Phase 4:** The bank web-server decrypt, the message (cipher text) using the corresponding decryption function to obtain $Msg' = Decy_{C_b}(Cipher)$. The bank web-server verifies the validity of the user name and pass word from the data base server. If valid, Then successfully transactions otherwise fail.
It can be easily proven that the two computed keys C_m and C_b are equal:

$$\begin{aligned} C_m &= H_2(h, D_{ID_m}, D_{ID_b}, PK_{ID_m}, PK_{ID_b}, jx_m X_b) \\ &= H_2(h, D_{ID_m}, D_{ID_b}, PK_{ID_m}, PK_{ID_b}, jx_m x_b P) \\ &= H_2(h, D_{ID_m}, D_{ID_b}, PK_{ID_m}, PK_{ID_b}, jx_b x_m P) \\ &= H_2(h, D_{ID_m}, D_{ID_b}, PK_{ID_m}, PK_{ID_b}, jx_b X_m) = C_b \end{aligned}$$

4.1 Security of Mobile Banking using Certificateless Chameleon Hashing Schemes

—**Authentication:** The shared per-session secret key is generated using public parameters, mobiles client private key and banks web server public key, then authentication of entities are provided.

—**Confidentiality:** Given by the scheme is confidentiality because the encryption and decryption process use symmetric key cryptosystem.

—**Integrity and non-repudiation:** The mobile client signs the message using the bilinear pairing algorithm, its private key and public key, 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 private key using chameleon hash function.

—**Long-term binding of public key with corresponding private key:** The mobile client/banks web server can create only one long term public key for the corresponding private key where the long term public key $PK_{ID_m} = \{X_m, Y_m\}$ is related to the partial private key D_{ID_m}, since $D_{ID_m} = sH_1(ID \parallel X_m)$. And the one-to-one correspondence between the public key and the partial private key of mobile client or the banks web-server. The two valid public key for the same identity is mobile client or bank web-server guarantees that the KGC. And the KGC will be identified to misbehaved in issuing both mobile client or web server corresponding partial private keys.

—**Known key secrecy:** Each run of the protocol between mobile client and bank server shall produce a unique session key, because both the mobile client and the banks web-server use a random number j which is generated in each protocol run. Even if the adversary Eve has learned some other session keys, he can not compute the j.

—**Unknown key share resilience:** The public key PK_{ID_m} and PK_{ID_b} are built-in the computation of the common secret key. There fore, the mobile client and the banks web-server know who they share the key with.

—**No-Key-compromise attack:** Suppose the adversary compromised the long-term private keys of the mobile client m, but adversary is unable to impersonate other party to mobile client m, because this scheme use in certificateless chameleon hash function. Anyone can compute the value of hash value, However, there exists no efficient algorithm for anyone except the holder of the secret key i.e only the holder of the trapdoor (secret key) is able to find the collision of the given value. Hence this scheme in mobile banking, the holder of register mobile only he/her is gain the secret information.

$$C_m = H_2(h, D_{ID_m}, D_{ID_b}, PK_{ID_m}, PK_{ID_b}, jx_m X_b)$$
$$= H_2(e(r,P)e(mQ_{ID_b}, P_{pub}), D_{ID_m}, D_{ID_b}, PK_{ID_m}, PK_{ID_b}, jx_m X_b)$$
$$= H_2(e(x_m X_b, P)e(mQ_{ID_b}, P_{pub}), D_{ID_m}, D_{ID_b}, PK_{ID_m}, PK_{ID_b}, jx_m X_b)$$
$$= H_2(e(x_m x_b P, P)e(mQ_{ID_b}, P_{pub}), D_{ID_m}, D_{ID_b}, PK_{ID_m}, PK_{ID_b}, jx_m x_b P)$$
$$= H_2(e(x_b X_m, P)e(mQ_{ID_b}, P_{pub}), D_{ID_m}, D_{ID_b}, PK_{ID_m}, PK_{ID_b}, jx_b X_m)$$

now $x_m X_b$ is depend the chameleon hash function. The chameleon hash value is same $x_m X_b$ the transection is valid other then fail.

—**Weak perfect forward secrecy:** Suppose that an outside adversary has compromised long-term secret keys $C_m, C_b, x_m, x_b, r, r', D_{ID_m}, D_{ID_b}$. He cannot obtain the secret random value j, because use of chameleon hash primitive is chameleon signature [6], given a security "No party can produce a valid chameleon signature not previously generated by the signer" it means no adversary can produce a j not previously session keys generated by the either client.

—**Key control:** Neither entity should be able to force the session key to a preselected value.

5. EFFICIENCY

Certificateless chameleon hash function in mobile banking is executed as per following table:

Table 1: Computational cost of certificateless chameleon hashing.

Phase	Exponent	Multiplication	Hash Function
Setup	*1 Exp*	*1 Mul*	*2 H*
Extract	*0 Exp*	*4 Mul*	*1 H*
Hash generation	*0 Exp*	*6 Mul*	*1 H*
Forge	*1 Exp*	*1 Mul*	*0 H*

In the above table, Exp-Exponential, Mul-Multiplication and H-Hash Function. The setup phase having 1E+1M+2H, the extract phase is 0E+4M+1H, hash generation is 0E+6M+1H and forge is 1E+1M+0H in computational aspect.

Compare Table:

Table 2: Computational cost of proposed scheme. Our scheme is low computation cost as compare wang scheme[11], we describe only mobile client and bank web-server process, now given by following table. Computational aspect is our scheme 0Exp+3Mul+2H.

	Scheme	Exponent	Multiplication	Hash Function
Wang Scheme[11]	**RSA**	*5 Exp*	*1 Mul*	*1 H*
Our Scheme	**Pairing**	*0 Exp*	*3 Mul*	*2 H*

6. CONCLUSION

In this paper, we have proposed a new certificateless chameleon hash scheme in mobile banking. This scheme secure key compromise and unknown key attack and reduce computational cost and efficient in other one. Moreover, proposed algorithm is key exposure free and this scheme is very efficient e-payment system.

7. ACKNOWLEDGEMENT

The authors would like to thank the reviewers for giving valuable suggestions and comments.

8. REFERENCES

[1] G. Ateniese and B. de Medeiros. Identity-based chameleon hash and applications, FC 2004, Lecture Notes in Computer Science 3110, Springer-Verlag 2004, pages 164-180, 2004.

[2] D. Boneh, M. Franklin, Identity-based encryption from the Weil pairing, Advances in Cryptology-Crypto 2001, Lecture Notes in Computer Science 2139, Springer-Verlag 2001, pages 213-229, 2001.

[3] X. Chen, F. Zhang, H. Tian, B. Wei, K. Kim, Discrete logarithm based chameleon hashing and signatures without key exposure. Computers and Electrical Engineering, 37(4): pages 614- 623, 2011.

[4] X. Chen, F. Zhang, W. Susilo, H. Tian, J. Li, K. Kim, Identity based chameleon hash scheme without key exposure, In: Proc. of ACISP10, Lecture Notes in Computer Science 6168, Springer-Verlag 2010, pages 200-215, 2010.

[5] H. Hongxia, Certificateless based chameleon hash scheme, IEEE computer soiceity, pages 1126-1129, 2012.

[6] H. Krawczyk and T. Rabin, Chameleon hashing and signatures, Proc. of NDSS 2000, pages 143-154, 2000.

[7] 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.

[8] S. A. Riyami, K. Paterson, Certificateless public key cryptography, Asiacrypt 2003, Lecture Notes in Computer Science 2894, Springer Heidelberg 2003, pages 452-473, 2003.

[9] S.A. Shubat and M.A.Ashraf. Secure protocol for short message service. In Proc. of world academy of science, engineering and technology, 3(1): pages 745-749, 2009.

[10] 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(4): pages 166-169, 2011.

[11] J-S. Wang, F-Yi Yang, and I-Paik, A Novel E-cash Payment Protocol Using Trapdoor Hash Function on Smart Mobile Devices, International Journal of Computer Science and Network Security, Volume.11, No.6,pages 12-19, 2011.

[12] F. Zhang, R. Safavi-Naini, W. Susilo. ID-Based chameleon hashes from bilinear pairings. Cryptology ePrint Archive, Report 2003/208, available at http://www.iacr.org/2003/208.

[13] 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.

[14] 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) 2011, pages 1057-1060, 2011.