International Journal of Database Theory and Application
Vol.7, No.3 (2014), pp.23-30
http://dx.doi.org/10.14257/ijdta.2014.7.3.03

Efficient design of Certificateless Chameleon Signature from Bilinear Pairing

Tejeshwari Thakur[1], Neetu Sharma[2] and Birendra Kumar Sharma[3]

School of Studies in Mathematics, Pt. Ravishankar Shukla University
Raipur (C.G.), India
[1]tejeshwari31@gmail.com, [2]sharmabk07@gmail.com

Abstract

Certificateless public key cryptography (CL-PKC), does not require the use of the certificate to guarantee the authenticity of public keys. It does rely upon the use of a trusted third party (TTP), who is in possession of a master key. CL-PKC does not suffer from the key escrow property. Thus, CL-PKC can be seen as a model for the use in public key cryptography. In this paper, we proposed a new certificateless Chameleon signature scheme based on bilinear pairings. The proposed scheme is more efficient than AL-Riyami and Pateson [10] schemes. And our scheme is un-forgeable under the hardness assumption of the q-strong Diffie-Hellman problem and Computational Diffie-Hellman problem.

Keywords: *Certificateless Signature, Chameleon Hashing, Bilinear pairings, ID-based, cryptography*

1. Introduction

The traditional public key cryptosystem uses a certificate, which is a digitally signed statement issued by the CA (Certificate Authority). Such certificate can be verified by anyone and guarantees the authenticity of a user's public key. In implementation the management of public key certificates requires a large amount of computation, storage, and communication cost.

To handle this situation of public key certificate, Shamir [11] proposed another approach named "Identity Based Public Key Cryptography(ID-PKC)" in 1984. In this cryptosystem, the user's public key is some unique information about the identity of that user (e.g. an email address), which is assumed to be publicly known. Therefore, the need of certification can be eliminated. A trusted third party, called the Private Key Generator (PKG), generates private keys for all users in an ID-based system as in [11]. The PKG first publishes a master public key and retains the corresponding master secret key. To obtain a private key, one should contact PKG, which will use the master secret key to generate the corresponding private key. This approach however creates a new inherent problem namely the key escrow of a user's private key as PKG has the master secret key and thus has any user's private key in an ID-based system. The escrow problem could be partially solved by the introduction of multiple PKGs and the use of threshold technique which requires extra communication and infrastructure.

In 2003, AL-Riyami and Pateson [10] proposed a new paradigm called Certificateless public key cryptography. Like ID-PKC, certificateless cryptography does not use the public key certificate [10, 9, 13]. Although it also needs a third party called Trusted Authority (TA) to help a user to generate his private key but the TA do not require to access the user's full private key. It just generates a user's partial private key from the user's identity as the PKG in

ISSN: 2005-4270 IJDTA

ID-PKC does. A user computes his full private key by combining his partial private key and a secret value chosen by himself. The public key of a user is computed from the TA's public parameters and the secret value of the user, and then it is published by the user himself.

In the original paper of Al-Riyami and Paterson presented [10] a certificateless signature scheme. Huang *et. al.*, [6] pointed out a security drawback in it [10] and proposed a secure one. They defined the security model of certificateless signature scheme in the same paper. Further improvement in this direction are due to Zhang *et. al.*, [14], Yum [13], Hu *et. al.*, [7], Gorantla *et. al.*, [5] and Yap *et. al.*, [12]. Although, last two constructions [5, 12] are the efficient certificateless signature scheme but they suffer from universal forgery and involve large amount of pairing computation during verification. In our opinion, said two short comings could be substantially reduced if we construct a certificateless signature based on bilinear pairing using the chameleon hash function.

The concept of chameleon hashing was first introduced by Krawczyk and Rabin [8]. It was based on well established hash-and-sign paradigm, where a chameleon hash function is used to compute the cryptographic message digest. A chameleon hash function is a trapdoor one-way hash function which prevents everyone except the holder of the trapdoor information from computing the collisions for a randomly given input. Chameleon signatures simultaneously provide the properties of non-repudiation and non-transferability for the signed message.

In this paper, we propose a first certificateless signature scheme based on bilinear pairings using chameleon hash function. The proposed scheme is more efficient then other CLS and it is unforgeable under the hardness assumption of the q-strong Diffie-Hellman problem and computational Diffie-Hellman Problem.

The rest of the paper is organized as follows. In Section 2, we describe background concepts of bilinear pairing and related mathematical problems. In Section 3, we propose our scheme. The security analysis of our propose scheme is given in Section 4. Efficiency of our scheme in section 5. Finally, conclusion is made in Section 6.

2. Background Concepts

In this section, we briefly review the basic concepts on bilinear pairings and some related mathematical problems.

Definition 2.0.1 (Bilinear Pairing [4]). Let G_1 be an additive cyclic group of prime order q, be a multiplicative cyclic group of the same order and **P** be a generator of G_1. A bilinear map is defined as $e: G_1 \times G_1 \to G_2$ with the following properties:

• **Bilinear**: $e(aR,bS) = e(R,S)^{ab} \forall R,S \in G_1$ and $a,b \in Z_q^*$. This can be restated as $\forall R,S,T \in G_1$, e(R + S, T) = e(R, T)e(S, T) and e(R, S + T) = e(R, S)e(R, T).

• **Non-degenerate**: There exists $R,S \in G_1$ such that $e(R,S) \neq IG_2$ where IG_2 denotes the identity element of the group G_2.

• **Computable**: There exists an efficient algorithm to compute $e(R,S) \forall R,S \in G_1$.

In general implementation G_1 will be a group of points on an elliptic curve and G_1 will denote a multiplicative subgroup of a finite field. Typically, the mapping **e** will be derived from either the Weil or the Tate pairing on an elliptic curve over a finite field. We refer [2]

for more comprehensive description on how these groups, pairings and other parameters are defined.

Definition 2.0.2 (Mathematical Problems[4]). Here we discuss some mathematical problems, which form the basis of security for our scheme.

• Discrete Logarithm Problem (DLP): Given two elements P and Q, to find an integer $n \in Z_q$ such that Q = nP whenever such an integer exists.

• Computational Diffie-Hellman Problem (CDHP): For any $a,b \in Z_q^*$, given < P, aP, bP >, compute abP.

• Decisional Diffie-Hellman Problem (DDHP): For any $a,b,c \in Z_q^*$ given < P, aP, bP, cP >, decide whether c = ab mod q.

• Gap Diffie-Hellman Problem(GDHP): A class of problems where CDHP is hard while DDHP is easy.

• The q-Strong Diffie-Hellman problem(q-SDHP): Given a (q + 2)-tuple $(P,Q,\alpha Q,\alpha^2 Q.....\alpha^q Q)$ find a pair $(c,(c+\alpha)^{-1}P)$ with $c \in Z_q^*$

3. Proposed Scheme

Now we propose a certificate less signature scheme based on bilinear pairing using chameleon hash function. It consists of five algorithms namely Setup, Extract, Sign, Verify and Dispute.

Setup: The TA performs the following step.

Let **k** be a security parameter and let G_1 is a cyclic additive group generated by **P** with prime order **q**, G_2 is a cyclic multiplicative group of the same order **q**, and $e: G_1 \times G_1 \to G_2$ is a bilinear pairing H_1 cryptography hash function, such that $H_1 : \{0,1\}^* \to Z_q^*$ and another cryptography hash function, $H_2 : G_2 \times G_1 \to Z_q^*$. Choose $s \in_R Z_q^*$ and compute $P_{pub} = sP$. The system parameter is params = $\{G_1, G_2, e, q, P, P_{pub}, H_1, H_2, k\}$ and keep **s** secretly as the master-key.

Extraction: This algorithm takes as input, the system parameters, the master key, and an identifiable information and returns its corresponding partial private key when Alice gives as identity, ID_A, the TA computes partial private key $D_{ID_A} = (H_1(ID_A) + s)^{-1} P$. Alice then chooses $x_A \in_R Z_q^*$ and generates output x_A as her secrete value. The trapdoor key is $SK_{ID_A} = x_A D_{ID_A} = x_A (H_1(ID_A) + s)^{-1} P$ and the public key is $PK_{ID_A} =< X_A, Y_A >$ where $X_A = x_A^{-1} P$ and . $Y_A = x_A^{-1} P_{pub}$.

Chameleon Signature Generation:

Hash: As input, the identifier ID_A, the hash key PK_{ID_A}, a message m and choose random element R from G_1 compute chameleon hash as below.

$$hash = Hash(P_{pub}, m, R, ID) = e(P, H_1(m)P)e(H_1(ID) + P_{pub}, R)^{H_1(m)}$$

Forge: For any valid hash value is hash, compute a string with the trapdoor key $SK_{ID} = x_A D_{ID_A}$ as below:

$$R' = Forge(P_{pub}, ID, SK_{ID}, m, R, m') = H_1(m')^{-1}(x_A^{-1}(H_1(m) - H_1(m'))SK_{ID} + H_1(m)R)$$

Note that $Hash(ID, m, R, P_{pub}) = Hash(ID, m', R', P_{pub})$

The user chooses a message m and private key SK_{ID_A}, and sign the message in the following steps.

1. Choose $k \in_R Z_q^*$
2. Compute $r = e(P, k_A P)$
3. Set $c_A = H_2(hash \| r) \in Z_q^*$
4. Compute $U = (k_A + c_A)SK_{ID_A} \in G_1$
5. Set $sig = SING_{SK}(c_A, U)$. The signature on the message **m** consists of the signature tuple as $SIG(m) = (m, r, sig)$.

Verification:
The verification face takes the valid signature and verify the process. The signature Tuple SIG(m) = (m, r, sig) compute:
• SIG(m) = (m, r, sig)
• $r = e(U, H_1(ID_A)X_A + Y_A)e(P, -c_A P)$
accept the signature if and only if $(c_A = H_2(hash \| r), sig)$.

Dispute:
In case of a dispute on the validity of a signature, signer can turn to an authorized judge **J** is trusted party. **J** gets from signer a signature tuple SIG(m) = (m, r, sig).

- **J** applies the above verification Algorithm. If this verification fails then the alleged signature is rejected by **J**. Otherwise,
- **J** summons the signer to deny/accept the claim. **J** sends the tuple (*m, r, sig*) to recipient.
- If the recipient wants to claim that signature is invalid he will need to provide a collision in the chameleon hash function. Otherwise, recipient simply confirms to the judge this fact. The following is the process that generates collision in the chameleon hash function. $hash = Hash(P_{pub}, m, R, ID) = Hash(P_{pub}, m', R', ID)$
  Where

$$e(P,P)^{H_1(m)} e(H_1(ID) + P_{pub}, R)^{H_1(m)} = e(P,P)^{H_1(m')} e(H_1(ID) + P_{pub}, R)^{H_1(m')}$$

$$e(P,P)^{H_1(m) - H_1(m')} = e(H_1(ID) + P_{pub}, H_1(m')R' - H_1(m)R)$$

$$e(P,P) = e(H_1(ID) + P_{pub}, (H_1(m) - H_1(m'))^{-1} H_1(m')R' - H_1(m)R)$$

Hence $SK_{ID} = (H_1(m) - H_1(m'))^{-1} H_1(m')R' - H_1(m)R)$

Recipient shows the collision pair *(m',R').* recipient can convince the judge to reject the forgery chameleon signature tuple *(m', r', sig).*

4. Security Analysis

4.1. Correctness. The correctness of the signature is given by the equation given below:-
The equation for forgery is:

$$
\begin{aligned}
&Hash(P_{pub}, m', R', ID)\\
&= e(P, H_1(m')P)e(H_1(ID) + P_{pub}, R')^{H_1(m')}\\
&= e(P, H_1(m')P)e(H_1(ID) + P_{pub}, H_1(m') \cdot H_1(m')^{-1}(x_A^{-1}(H_1(m) -\\
&\quad H_1(m'))SK_{ID} + H_1(m)R))\\
&= e(P, H_1(m')P)e(H_1(ID) + P_{pub}, (x_A^{-1}(H_1(m) - H_1(m'))SK_{ID})e(H_1(ID) + P_{pub}, H_1(m)R))\\
&= e(P, H_1(m')P)e(P, ((H_1(m) - H_1(m'))P)e(H_1(ID) + P_{pub}, H_1(m)R))\\
&= e(P, H_1(m)P)e(H_1(ID) + P_{pub}, R)^{H_1(m)}\\
&= Hash(P_{pub}, m, R, ID)
\end{aligned}
$$

4.2. Verifiability. The verification of the signature is given by the equation as below.
The equation for verification is:

$$
\begin{aligned}
r &= e(U, H_1(ID_A)x_A^{-1}P + x_A^{-1}P_{pub})e(P, -c_A P)\\
&= e((k + c_A)SK_{ID_A}, (H_1(ID_A) + s)x_A^{-1}P)e(P, -c_A P)\\
&= e((k + c_A)(H_1(ID_A) + s)^{-1}x_A P, (H_1(ID_A) + s)x_A^{-1}P)e(P, -c_A P)\\
&= e(P, P)^{k + c_A}e(P, P)^{-c_A}\\
&= e(P, P)^{k}
\end{aligned}
$$

The proposed scheme is unforgeable under the hardness assumption of the q-strong Diffie-Hellman problem and Computational Diffie-Hellman problem.

On the one hand, even the *PKG* who knows the master key **s**, the partial private key of Alice, and the public key $< X_A, Y_A >$ of Alice, cannot compute a valid signature. If he can compute x_A from the equalities $X_A = x_A P$ or $Y_A = x_A sP$, then he can forge BLS signatures [3] which are proven to be unforgeable based on the CDH assumption.

On the other hand, any third party may try to find compute a valid signature via two ways.

- He randomly chooses the value *U* and tries to compute c_A such that $c_A = H_2(hash \| r)$ holds.
- The adversary can choose c_A at random and try to compute *U* such that the equation $c_A = H_2(hash \| r)$ holds.

However, due to the hardness of the q-strong Diffie-Hellman problem, computational Diffie-Hellman problem and the one-way property of cryptographic hash function and chameleon hashing, the adversary can not forge a valid signature by this two ways.

The formal security analysis is the same as Barreto *et al.*, provably-secure identity based signatures and signcryption from bilinear maps identity-based signatures [1], we follow the [1] for more details.

Theorem 4.3.1. *Let us assume that there exists an adaptively chosen message and identity attacker F making* q_{h_i} *queries to random oracles* $H_i(i=1,2)$ *and* q_s *queries to the signing oracle. Assume that, within a time t, F produces a forgery with probability* $\varepsilon \geq 10(q_s+1)(q_s+q_{h_2})/2^k$. *Then, there exists an algorithm B that is able to solve the q-SDHP for* $q=q_{h_1}$ *in an expected time*

$t \leq 120686 q_{h_1} q_{h_2} (t+\mathrm{O}(q_s, r_p))/(\varepsilon(1-q/2^k)) + \mathrm{O}(q^2 r_{mult})$

where r_{mult} *and* r_p *respectively denote the cost of a scalar multiplication in* G_2 *and the required time for a pairing evaluation.*

5. Efficiency

We can conclude that our scheme is a little more efficient than Al-Riyami and Paterson's certificateless signature scheme [10] is given below:

Table 1. Computational Cost of Proposed Scheme

	Phase	Pairing	Multi in G1	Add in G1	Exp in G2
Al-Riyami & Paterson's Scheme	Signing Phase	1	2	1	1
	Verification Phase	4	0	0	1
Our Proposed Scheme	Signing Phase	3	1	0	1
	Verification Phase	2	1	1	0

7. Conclusion

In the above paras, we have proposed a certificateless chameleon signature scheme based on bilinear pairings by eliminating the key escrow problem, which is an inherent drawback of ID-based cryptosystems, by using the user's chosen secret value. The scheme is proved to be secure under under the hardness assumption of the bilinear pairing inversion problem and Computational Diffie-Hellman problem.

Acknowledgements

The first author 1 is thankful to UGC, New Delhi, India for providing Rajiv Gandhi National Fellowship (F1-17.1/2010-13/RGNF-2012-13-ST-CHH-35416) as financial assistance for this Research work..

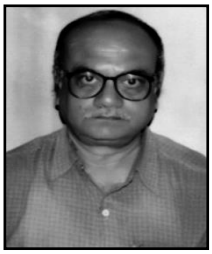
References

[1] P. S. L. M. Barreto, "Efficient and provably secure identity-based signatures and signcryption from bilinear maps", Proceedings of Asiacrypt'2005, LNCS 3788, Springer-Verlag, **(2005)**, pp. 515-532.
[2] D. Boneh and M. Franklin, "Identity-based Encryption from the Weil pairing", SIAM J. of Computing, in Proceedings of Crypto'01, LNCS 2139, Springer-Verlag, **(2001)**, pp. 213-229.
[3] D. Boneh, B. Lynn and H. Shacham, "Short signatures from the weil pairings", Proceedings of Asiacrypt'01, LNCS 2248, Springer-Verlag, **(2001)**, pp. 514-532.
[4] M. Choudary Gorantla, R. Gangishetti, M. Lals and A. Saxena, "An Effective Certificateless Signature Scheme Based on Bilinear Pairings", WOSIS, INSTICC Press, **(2005)**, pp. 31-39.
[5] M. Gorantla and A. Saxena, "An efficient certificateless signature scheme", CIS 2005. LNCS (LNAI). 3802, Springer, Heidelberg, **(2005)**, pp. 110-116.
[6] X. Huang, W. Susilo, Y. Mu and F. Zhang, "On the security of a certificateless signature scheme", CANS 2005. LNCS. 3810, Springer, Heidelberg, **(2005)**, pp. 13-25.
[7] B. Hu, B. Wong, D. Zhang and Z. Deng, "Key replacement attack against a generic construction of certificateless signature", ACISP 2006. LNCS. 4058, Springer, Heidelberg, **(2006)**, pp. 235-346.
[8] H. Krawczyk and T. Rabin, "Chameleon hashing and signatures, Proc. of NDSS, **(2000)**, pp. 143-154.
[9] B. Libert and J. Quisquater, "On constructing certificateless cryptosystems from identity based encryption", PKC 2006, LNCS 3958, Springer, Heidelberg, **(2006)**, pp. 474-490.
[10] S. A. Riyami and K. Paterson, "Certificateless public key cryptography", Proceedings of Asiacrypt'03, LNCS 2894, **(2003)**, pp. 452-473.
[11] A. Shamir, "Identity-based cryptosystems and signature schemes", Advances in Cryptology-Crypto, LNCS 196, Springer-Verlag, **(1984)**, pp. 47-53.
[12] W. Yap, S. Heng and B. Goi, "An efficient certificateless signature scheme", EUC Workshops 2006. LNCS 4097, Springer, Heidelberg, **(2006)**, pp. 322-331.
[13] D. Yum and P. Lee, "Generic construction of certificateless signature", ACISP 2004. LNCS 3108, Springer, Heidelberg, **(2004)**, pp. 200-211.
[14] Z. Zhang, D. Wong, J. Xu and D. Feng, "Certificateless public-key signature: security model and efficient construction", ACNS 2006. LNCS 3989, Springer, Heidelberg, **(2006)**, pp. 293-308.

Authors

Tejeshwari Thakur received the B.Sc., M.Sc. and M.Phil degree in Mathematics from Pt. Ravishankar Shukla University, Raipur. Chhattisgarh, India in 2008, 2010 and 2011, respectively. She is currently pursing Ph.D. degree with the department of Mathematics in Pt. Ravishankar Shulka University, Raipur, India. Her area of research interest is Crytography.

Neetu Sharma received M.Sc and M.Phil degree in mathematics from Pandit Ravishankar Shukla University Raipur, Chhattisgarh (India) in 2010 and 2012. She is doing research in Bilinear Pairing within the domain of cryptography for Ph.D degree in S.o.S in mathematics, of Pandit Ravishankar Shukla University Raipur, Chhattisgarh (India).



Birendra Kumar Sharma Professor, School of Studies in Mathematics, Pt. Ravishankar Shukla University Raipur (C. G.) India. He has been working for long time in the field of Non Linear Operator Theory and currently in Cryptography. He and his research scholars work on many branches of public key cryptography. He is a life member of Indian Mathematical Society and the Ramanujan Mathematical Society.