EFFICIENT DESIGN OF ID-BASED MULTI PROXY CHAMELEON SIGNATURE FROM BILINEAR PAIRING

TEJESHWARI THAKUR, BIRENDRA KUMAR SHARMA

Abstract: Hash-sign-paradigram is the base of chameleon signature. In this Paradigm, cryptographic message digest is computed through a Chameleon hash function. This property like non-repudiation and non-transferability are the main feature of any chameleon signature. The object is the paper is to introduce a multi proxy chameleon signature scheme in which bilinear pairing is used for the purpose of the security.

Keyword: Multi-proxy Chameleon signature, Bilinear pairings, ID-based cryptography.

Introduction: Krawczyk and Rabin [8], introduced chameleon signature. It is in fact a signature based on hash and sign paradigm where chameleon hash function is a trapdoor collision resistant. Chameleon signatures provide non-repudiation and non-transferability of for the signed message as the undeniable signatures [4] do, but Chameleon signature allows for simpler and more efficient realization than the undeniable signature. It is well known fact that Chameleon hash function is used to calculate the message digest.

In 1996, the concept of proxy signature was introduce by Mambo et al.[9]. Proxy signatures means electronic authentication in essential in other ward, in the proxy signature the designated person can sign on behalf of the original signer. Since the invention of the proxy signature, several type of proxy signatures have been designed.

One among them is noteworthy the proxy signature introduced by Yi et al.[11] The

beauty of this proxy signature lies with the fact that the original signer can delegate his signing power to many persons not only one. This type of signature scheme is known as multi proxy signature scheme. However, such multi proxy signature scheme fails to provide features like non-repudiation and non-transferability of the signed message. Since chameleon had the capacity to deal with such situation, Zhang et al.[13] were designed Chameleon signature. It was ID-based which Ateniese and Medeiros [1] were introduced as ID-based Chameleon hash function. Here, Identity information of public key could be directly calculated rather then extracted from the a certificate include in authenticity. Now in this paper, we propose an ID based proxy signature based on chameleon hash function involving multi-e-signer.

Our design maintain the security at Para with Zheng et al.[13]even when we involved multi signer are involve the organization of the paper is as follows The required preliminaries for proposing the design in given in section 2. In section3, proposed identity-based multi proxy chameleon signature his given. In section 4, the analysis of security and efficiency of our scheme is discussed finally conclusion on new design is given in section 5.

Preliminaries:

In this section, we will briefly describe the basic definitions, properties of bilinear pairings and Gap Diffie-Hellman group respectively. We also present ID-based public key setting from pairings.

Bilinear Pairing: 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^* . We assume that the discrete logarithm problems (DLP) in both G_1 and G_2 are hard. A bilinear pairings is a map e: $G_1 \times G_1 \rightarrow G_2$ with the following properties:

1. Bilinear: e(aP, bQ) = $e(P, Q)^{ab}$

2. Non-degenerate: There exists P and Q $\in G_1$ such that e(P,Q) $\neq$ 1.

3. Computable: There is an efficient algorithm to compute e(P,Q) for all P,Q$\in G_1$

Gap Diffie-Hellman Group: Let G_1 be a cyclic additive group generated by P, whose order is a prime q. A assume that the inversion and multiplication in G_1 can be computed efficiently. We first introduce the following problems in G_1.

1. 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.

2. Computation Diffie-Hellman Problem (CDHP): Given P, aP, bP for a, b$\in Z_q^*$ to compute abP.

3. Decision Diffie-Hellman Problem (DDHP): Given P, aP, bP, cP for a, b, c $\in Z_q^*$ to decide whether c $\equiv$ ab mod q.

We call G_1 a Gap Diffie-Hellman Group if DDHP can be solved in polynomial time but there is no polynomial time algorithm to solve CDHP or DLP with non-negligible probability. Such group can be found in super singular elliptic curve or hyper elliptic curve over finite field, and the bilinear pairings can be derived from the Weil or Tate pairings. For more details, see [2, 4, 5].

Definitions: The notations given in on [3], [12],[13]

we define as below:

(A)ID-based Multi proxy Chameleon signature scheme:A Multi proxy Chameleon signature scheme consists of four entities: original signer, proxy signer group ,verifier and other party as in charge called Judge will watch the communication proxy group and verifier. Next we define the algorithm for ID-based Multi Proxy Chameleon signatures as below:

Setup:- The private key generator(PKG) runs this probabilistic polynomial-time algorithm to generate a pair of keys(SK,PK) defining the scheme. PKG publishes the system parameters of SP including the public key PK, and keeps the master key SK secret. The input to this algorithm is a security parameter k.

Extract:- A deterministic polynomial-time algorithm that, on input the master Key SK and an identity string ID, outputs the trapdoor key associated to the hash key S_{ID}.

Generation of the Proxy Key:- This is a protocol between the original signer And all multi proxy signer. The protocol works as follow: To Delegate the signing capacity to proxy group, the original signer uses public key and the warrant m_w with respect proxy group whose proxy signer's sign as the proxy signing key SK_{p_i} so that original signer and the proxy signer produce proxy chameleon signature on behalf of the original signer.

Chameleon Hash Function:- A probabilistic polynomial-time algorithm that, on input an identity string ID, message m, and a random string R, outputs the hashed value h = Hash(ID, PK, m, R).

Forge:- A deterministic polynomial-time algorithm F that, on input PK the trapdoor key S_{ID} associated to the identity string ID, a hash value h of a message m, a random string R , and another message m'≠ m, outputs a string R' that satisfies h = Hash(ID, PK, m, R) = Hash(ID, PK, m', R').

Multi-Proxy Chameleon Signature Generation (MPCS):-An probabilistic algorithm for MPCS means that Every proxy signer PS_i takes input hash value h his signing key SK_{p_i} and take the warrant m_w , and out puts the σ_{MPCS}.

Verification:- It is an algorithm in which public key of the original signer, proxy group, message M, warrant w , Judge t decides multi-proxy signature s as input and outputs 1 as valid or 0 otherwise.

Dispute: Given multi proxy chameleon signature σ_{MPCS} on message m, the proxy group computes different message m' and R', collision as pair (m', R'), where m'≠ m and with the valid signature tuple (m',R', σ'_{MPCS}),the Judge claim that multi proxy chameleon signature of message m is forgery.

(B)Security Analysis of Multi Proxy Chameleon Signature:

Multi proxy chameleon signature scheme satisfy following properties.

Distinguish-ability: Valid proxy chameleon signatures generated by the proxy signer's are distinguishable from valid normal chameleon signatures generated by the original signer.

Verifiability: From the multi proxy Chameleon signature, a verifier can be convinced of the original signers agreement on the signed message.

Unforgeability: Only the delegated proxy group can generate the proxy signature for a given message on behalf of the original signer. The Original signer and the other parties are not designated as a proxy signer cannot produce a proper Chameleon signature which is not earlier generated by the signer.

Identifiability: Any one can identify the proxy signer corresponding to a proxy chameleon signature.

Prevention of misuse: The proxy signer cannot use the proxy key for other purposes than generating a valid multi proxy chameleon signature. That other person cannot sign, with the proxy key, messages that have not been authorized by the original signer.

Non-repudiation: Once a proxy signer's creates a valid proxy chameleon signature of an original signer, he cannot repudiate the signature creation.

Non-transferability: Except for the proxy signer's himself, no one can prove to another party that the proxy signers produced a given proxy chameleon signature.

Denial: The proxy signer's can convince the judge to reject a forgery proxy chameleon signature.

Message hiding: In case of dispute, the proxy signer's can compute a new deny the forgery proxy chameleon signature and thus the original message is never revealed.

Proposed Proxy-Multi Signature Scheme: The proposed scheme involves four characters: the Private Key Generator (PKG), the original signer, a set of proxy signers $L = \{PS_1, PS_2 \ldots\ldots PS_l\}$ and the recipient. It consists of the following five algorithms:

- **Setup:** Let G_1 is a cyclic additive group generated by P with prime order q, is G_2a cyclic multiplicative group of the same order q, and e : $G_1 \times G_1 \rightarrow G_2$ is a bilinear pairing, and cryptography hash function, $H_0: \{0,1\}^* \rightarrow G_1^*$ and $H_1: \{0,1\}^* \rightarrow Z_q^*$ and another cryptography hash function, $H_2: G_2 \times G_1 \rightarrow Z_q^*$, Ppub = sP ,PKG publishes system parameters params = {G1,G2, e, q, P, Ppub, H_0, H_1, H_2} here PKG keeps s secretly as the master-key.
- **Private key extraction**: Let Alice be the original signer with ID_A, identity, private key be the $S_A = sQ_A = sH_0(ID_A)$, (PS_i) be the proxy signers with identity (ID_{PS_i}) and customized identity: $ID_j = (ID_c \,||\, ID_B \,||\, IDt)$, where the identity of the recipient, proxy signer, transection, and the private key $(S_{PS_i}) = sQ_{PS_i} = sH_0(ID_{PS_i})$

- **Proxy key generation**: To delegate the signing capacity to proxy signers, the Alice uses the signed warrant mw and there each proxy signer PS_i computes his proxy key S_{P_i}.
- -Alice computes $r_A = e(P,P)^k$, where k $\in_R$ Z_q^* , and computes $C_A = H_2\ (m_w || r_A)$ and $U_A = c_A S_A$ + kP. Then Alice sends (m_w, c_A, U_A) to the proxy group L.
- -Each $PS_i \in$ L verifies the validity of the signature on m_w and Computes r_A=e(U_A, P) $e(Q_A, \text{Ppub})^{c_A}$,, there accepts this signature if and only if $C_A = H_2\ (m_w || r_A)$. If the signature is valid, PS_i computes the proxy key SP_i as $S_{P_i} = c_A S_{PS_i} + U_A$.

Multi Proxy chameleon signature generation:

- -**Hash**: Given a message m ∈ {o, 1}, cash PSi choose a random element R from G_1 and calculate the Chameleon hash ***h*** = Hash(Ppub, m, R, IDj) = e(R, P)e(H_1 (m) H_0(IDj), Ppub).
- -**Forge:** Recipient can make a forgery R = Forge (Ppub, IDj, Sj, m, R, m') = (H_1(m) - H_1(m')Qj + R) , and accepts this signature if and only if $c_p = H_2(hIIr_p)$. The proxy group L wants to sign a delegated message m on behalf of the original signer. Each proxy signer PS_i generates the partial proxy signature to generate multi proxy signature.
- -Each PS_i randomly selects an integer $k_{P_i} \in_R Z_q^*$, compute $r_{p_i} = e(P,P)^{k_{p_i}}$ and broadcasts r_{p_i} to the remaining l – 1 proxy singers. Then compute $r_p = \prod_{i=1}^{l} r_{p_i}$ and $U_{p_i} = c_p S_{p_i} + k_{p_i} P$. Finally, the individual proxy signature of the message m is (c_p, U_{p_i}). And $c_p = H_2(hIIr_p)$. Once all individual proxy chameleon signatures are correct, and then thus compute $U_p = \sum_{i=1}^{l} U_{p_i}$. The valid multi-proxy chameleon signature is there for the tuple: $< m, c_p, U_p, m_w, r_A >$.
- **Verification**: the recipient can verify the validity of the multi proxy chameleon signature as follows:

$$r_p = e(U_p, P)(e(\sum_{i=1}^{l}(Q_A + Q_{PS_i}), P_{pub})^{H_2(m_w IIr_A)}.r_A^l)^{-c_p}$$

and accepts the signature if and only if $c_p = H_2(hIIr_p)$.

- **Dispute**: In the process of dispute on the validity of the signature the following case arises: to generate collision in the chameleon hash function, given a forgery $< m', R', c_p, U_p, m_w, r_A >$, recipient employees uses to compute the multi proxy chameleon signature on original message m.
- **Input**:- The process is Hash(Ppub, m, R, IDj) = Hash(Ppub, m, R', IDj) where m'≠ m and poxy signers compute t = $\frac{R'-R}{H_1(m)-H_1(m')}$.

1. Proxy signer's choose any message $\tilde{m}$ and computes

$$\tilde{R} = \left(H_1(m) - H_1(m')Q_j + \tilde{R}\right)$$

2. Output : Output is $(\tilde{m}$,R).

With the tuple$(\tilde{m}, R, c_p, U_p, m_w, r_A)$, proxy signer can convince the judge to reject the false proxy chameleon signature $\left(m', R', c_p, U_p, m_w, r_A\right)$.

3. Judge applies the above verification algorithm. If this verification fails then the alleged signature is rejected by J. Otherwise,

4. J summons the proxy signer to deny/accept.

Analysis of the proposed Scheme: The correctness of the signature is justified by the following equations: chameleon signature and multi proxy chameleon signature same algorithm chameleon hashing, therefore the following proofs of correctness owes much to the [7, 12]. The forgery equation is.

$$\begin{aligned}
&Hash(P_{pub}, m', R', ID_j)\\
&= e(R'P)e(H_1(m') - H_0(ID_j), P_{pub})\\
&= e((H_1(m) - H_1(m')Q_j + R), P)e(H_1(m')Q_j, P_{pub})\\
&= e(H_1(m) - H_1(m')Q_j, P)e(R, P)e(H_1(m')Q_j, P_{pub})\\
&= e(R, P)e(H_1(m) - H_1(m')H_0(ID_j), P_{pub})e(H_1(m')H_0(ID_j), P_{pub})\\
&= e(R, P)e(H_1(m)H_0(ID_j), P_{pub})\\
&= Hash(P_{pub}, m, R, ID_j)
\end{aligned}$$

Verifiability: The verification and correctness of the multi proxy chameleon signature is justified the equation:

$$\begin{aligned}
&e(U_p, P)(e(\sum_{i=1}^{l} Q_A + Q_{PS_i}), P_{pub})^{H_2(m_w IIr_A)}.r_A^l)^{-c_p}\\
&= e(\sum_{i=1}^{l} U_{p_i}, P)(e(\sum_{i=1}^{l}(S_A + S_{PS_i}), P)^{c_A}.r_A^l)^{-c_p}\\
&= e(\sum_{i=1}^{l} U_{p_i}, P)(e(\sum_{i=1}^{l} S_{p_i} - kP), P).r_A^l)^{-c_p}\\
&= e(\sum_{i=1}^{l}(c_p S_{p_i} + k_{p_i} P), P)(e(\sum_{i=1}^{l} S_{p_i} P))^{-c_p}\\
&= e(\sum_{i=1}^{l} k_{p_i} P, P)\\
&\prod_{i=1}^{l} r_{p_i}\\
&r_p
\end{aligned}$$

Security Analysis:

Theorem 4.1. The above multi proxy chameleon signature scheme enjoys all advantages of the previous schemes [13]: Distinguish ability, Verifiability, identifiability, Prevention of misuse, Non-forge ability, non-repudiation, Non-transferability, Denial, Message hiding.

Proof.

Distinguish ability: It is evident that the valid multi-proxy chameleon signatures are distinguishable from normal valid proxy chameleon signatures generated by anyone.

Verifiability: The verifier can be convinced that the proxy signer's has the original signers signature on

the warrant mw and warrant contain identity verification tuple $(m, R, c_{p,} U_p, m_w, r_A)$ from the construction of $(c_{p,} U_p, r_A)$) in multi proxy chameleon signature verification scheme.

Non-forgeability: The proxy group can generate the proxy chameleon signature for a given message m'.Original signer signature on warrant mw. Even this, he forges the multi-proxy signature of the message m' for the proxy group L and the original signer Alice, this is equivalent to forge a Hesss ID-based signature with some public Key Q, here $e(Q, P_{pub}) = (e(\sum_{i=1}^{l} c_A(Q_A + Q_{PS_i}), P_{pub}).r_A^l)$ .On the other hand, the original signer cannot create a

Identifiability: The identity of public key of all proxy signer's are involved in the verification of the multi proxy chameleon signature, anyone can identity all theproxy chameleon signature.

Prevention of misuse: In multi proxy chameleon signature scheme due to using the warrant m_w, the proxy group can only sign message that have been authorized by the original signer.

Non-repudiation: The proxy signer's generated by valid multi proxy chameleon signature $(m, R, c_{p,} U_p, m_w, r_A)$, but proxy signer's can not generate other signature $(m', R', c_{p,} U_p, m_w, r_A)$ where $m' \neq m$ this is equivalent to finding a collision of the Id-based chameleon hash function, assuming CDHP hard.

Non-transferability: Proxy signers Generate multi proxy chameleon signature for recipient compute a random value on message m' then the equation R' = (H_1(m) –H_1(m')Qj + R) the hash value Hash(Ppub, m,R, IDj) = Hash(Ppub, m', R', IDj) hence our scheme multi Proxy chameleon signature verify and correct value is the $(m', R', c_{p,} U_p, m_w, r_A)$, thus we see that the recipient can not the convince a third party because m' have exactly value R' and R produce proper signature tuple is nothing efficient computation.

Denial: In the process the proxy signer's can convince the judge to reject a forgery proxy chameleon signature other words proxy signers and recipient give the authorized to judge J. The judge gets from recipient signature tuple $(\tilde{m}, , R, c_{p,} U_p, m_w, r_A)$. If proxy signers wants to claim that the signature is invalid, he will need to provide a collision in the hash function, the value $m' \neq m$ and a value R' such that $Hash(P_{pub,}$ IDj, $\tilde{m}, R)$ = $Hash(P_{pub,}$ IDj, m, $R)$ in this case the proxy information and delegated signing capacity verify, the valid multi-proxy signature since each proxy key includes the private key SP_i of each proxy signer. Assume that the adversary wants the proxy group to sign the false message m'. He can change his r_{p_i} ,there for r_p can be changed, but from the security of the basic ID-based signature scheme and public one way hash function H1, it is impossible for the adversary to get c'_p and U'_p such that $(m', c'_{p,} U'_p, m_w, r_A)$ is valid multi-proxy chameleon signature.

chameleon signature σ_{MPC} was originally generated by proxy signers with some pair $(m, R) \neq (\breve{m}, \breve{R})$.

Message hiding: In the message hiding process in multi proxy chameleon signature, the original signer construct another false signature for any message with the same component of multi proxy chameleon signature. Original signer do not disclose the original message.

Key exposure freeness : This algorithm prove in [1, 8] If a recipient with identity ID_c has never computed a collision under a customized identity ID_j then there is no efficient algorithm for an adversary to find a collision for a given chameleon hash value in MPCS then $Hash(P_{pub}, ID_j, m, R)$. This must remain true even if the adversary has oracle access to F and is allowed polynomial many queries on triples (ID_j, m_j, R_j) of his choice, except that ID_j is not allowed to equal the challenge ID.

Efficiency: In the scheme of cost computational explain the: MulG2- multiplication in the group G2, hash function - H1 and H2, Exp-Exponent, M2P- Map-to-point, Add-Addition, Pa-Pairing, and Sum-Summation.

Table 1: Computational of cost in Our Scheme.

Conclusion: In this paper, we propose the first ID-based multi proxy chameleon signature scheme from pairing scheme secure against existential forgery under adaptive chosen message attack in the random oracle model because used the CDHP.

Phase	H 1	H2	Ex p	M2P	Mul	Add	Mul G2	Pa	Sum
Setup					1				
Extra-ct				2					
Key Generation	2		2		3	2	1	2	1
Signature Generation	1	1		1	3	1	1	2	
Verification			3			1	1	2	1

References:

1. G. Ateniese, B. de Medeiros, Identity-based chameleon hash and applications, FC 2004, LNCS 3110, Springer-Verlag, pp.164-180, 2004.
2. D. Boneh ,M. Franklin, Identity-based encryption from the Weil pairing, Advances in Cryptology 01, LNCS 2139, Springer-Verlag, pp.213-229, 2001 .
3. Boldyreva, A. Palacio, and B. Warinschi, Secure proxy signature schemes for delegation of signing rights, http://venona.antioffine.com/2003/096, 2003.
4. D. Chaum and H. van Antwerpen, Undeniable signatures, Advances in Cryptology-Crypto 1989, LNCS 435, Springer-Verlag, pp.212-216, 1989.
5. X. Chen, F. Zhang, K. Kim, Chameleon hashing without key exposure, ISC 2004, LNCS 3225, Springer-Verlag, pp. 87-98 , 2004.
6. S.D. Galbraith, K. Harrison, D. Soldera, Implementing the Tate pairings, ANTS 02, LNCS 2369, Springer-Verlag ,pp.324-337, 2002.
7. F. Hess, Efficient identity based signature schemes based on pairings, SAC 02, LNCS 2595,Springer-Verlag, pp. 310-324, 2002 .
8. H. Krawczyk, T. Rabin. Chameleon hashing and signatures, Proc. of NDSS , pp.143-154, 2000.
9. M. Mambo, K. Usuda, E. Okamoto, Proxy signature, Delegation of the power to sign messages, In IEICE Trans. undamentals, E79-A, pp.1338-1353,1996.
10. Shamir, Identity-based cryptosystems and signature schemes, Advances in Cryptology-Crypto, LNCS 196, Springer-Verlag , pp. 47-53, 1984.
11. L. Yi, G. Bai, G. Xiao, Proxy multi-signature scheme, A new type of proxy signature scheme, Electronics Letters, vol. 36(6), pp.527-528, 2000 .
12. F. Zhang, R. Safavi-Naini, W. Susilo, ID-based chameleon hashes from bilinear pairings, Cryptology ePrint Archive: Report 2003/208, 2003.
13. M. Zhang, Gongliang Chen and Jianhua Li, Efficient ID-based Proxy Chameleon Signature from Bilinear Pairings, IEEE computer security, 2005.

***

Research Scholar , Prof. /School of Studies in Mathematics
Pt. Ravishankar Shukla University Raipur (C.G.)/ tejeshwari31@gmail.com.