International Journal of Innovation and Scientific Research
ISSN 2351-8014 Vol. 10 No. 2 Oct. 2014, pp. 438-442
© 2014 Innovative Space of Scientific Research Journals
http://www.ijisr.issr-journals.org/

An ID-Based Anonymous Proxy Chameleon Signature Based on Bilinear Pairings

Tejeshwari Thakur, Swati Verma, and Birendra Kumar Sharma

School of Studies in Mathematics,
Pt. Ravishankar Shukla University, Raipur,
Chhattisgarh, India

ABSTRACT: Anonymous proxy signature is suitable for the situation where the proxy signer's identity needs to be kept secret. The verifier needs to reveal the real identity of the proxy signer with the help of the original signer. A new ID-based anonymous proxy chameleon signature scheme based on bilinear pairing is proposed in this paper. This scheme is based on Gap Diffie-Hellman group and meets the security requirements such as verifiability, un-forge ability, anonymity, traceability, Prevention of misuse, non-repudiation and Message hiding.

KEYWORDS: Anonymous Proxy Chameleon Signature, Chameleon Hashing, Gap Diffie-Hellman Group, Bilinear Pairing.

1 INTRODUCTION

The concept of proxy signature was introduced by Mambo et al. [6] in 1996. In a proxy signature scheme, the original signer delegates his/her signing right to a proxy signer who can sign a message on behalf of the original signer. Proxy signature can be verified using a modified verification equation where the verifier is convinced that the signature is generated by the authorized proxy signer. In 2009, Yu et al. [8] further proposed an anonymous proxy signature scheme (APSS) which provides anonymity property for proxy multi-signature. In their scheme, there is a group of proxy signers, but only one proxy signer can anonymously sign the message. By using a group of signers, Yu et al. [8] provide privacy and anonymous protection for the proxy signer such that any other proxy signer cannot know who is the real signer.

Krawczyk and Rabin [5] proposed the concept of chameleon hash function in 2000. A chameleon hash function is a trapdoor one-way hash function where it is hard to find collision without the knowledge of the trapdoor. However, with the knowledge of the trapdoor, collision hash function and the pre-images hash function can be found easily.

In 1984, Shamir [7] proposed ID-based encryption and signature scheme to simplify key management procedures in certificate-based public key setting. The main idea of ID-based cryptosystem is that the user's public key can be calculated directly from his/her identity rather than being extracted from a certificate issued by a certificate authority (CA). ID-based public key setting can be a good alternative for certificate-based public key setting, especially when efficient key management and moderate security are required.

Zhang et al. [9] proposed proxy chameleon signature scheme based on bilinear pairing which is secure against existential forgery under adaptive chosen message attack in the random oracle model. The bilinear pairings, namely the weil-pairing and the tate-pairing of algebraic curves, are important tools for research in algebraic geometry. They have been found various applications in cryptography [1, 2, 3, 4].

Our Contribution: We propose an efficient ID-based anonymous proxy chameleon signature scheme based on bilinear pairing with Gap Diffie-Hellman group. Security analysis and efficiency of the proposed scheme is given.

Organization: We describe the preliminaries in section 2. Proposed ID-based anonymous proxy signature scheme introduced in section 3. The analysis of proposed scheme is described in section 4. The security analysis is given in section 5. Efficiency in our scheme in section 6. Finally, we conclude our opinion in section 7.

2 PRELIMINARIES

In this section, we briefly describe the basic definitions, properties of bilinear pairings and Gap Diffie-Hellman Group.

(1)Definition: (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^* . A bilinear pairings is a mapping $e : G_1 \times G_1 \to G_2$ with the following properties:

* **Bilinear:** $e(aP, b, Q) = e(P, Q)^{ab}$

* **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) Definition: (Gap Diffie-Hellman Group). Let G1 be a cyclic additive group generated by P, whose order is a prime q. Assume that the inversion and multiplication in G_1 can be computed efficiently. The following properties are satisfied:

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

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

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

(3) Definition (Gap Diffie-Hellman Problem (GDHP)) . DDHP is easy, but CDHP is difficult on the group, which is called a Gap Diffie-Hellman Group [2,3]. Meanwhile, there exists a difficult problem to solve the inverse algorithm of bilinear pairings, i.e., given $P \in G_1$ to find an element, $r \in G_2$, such that $Q \in G_2$, r = (P;Q) whenever such an element exists.

3 PROPOSED SCHEME

Our proposed scheme is given in five phases i.e., Setup, Extraction, Key Generation, Signature Generation and Signature Verification as below:

1. **Setup:** Let two cryptography hash function, $H_0 : \{0,1\}^* \to G_1^*$, $H_1 : \{0,1\}^* \times G_2 \to Z_q^*$, and $H_2 : \{0,1\}^* \to Z_q^*$, and PKG choose random integer $s \in Z_q^*$ and Ppub = sP, PKG publishes system parameters = $\{G_1, G_2, e, q, P, P_{pub}, H_0, H_1\}$, here PKG keeps s secretly as the master key.

2. **Extraction:** Original signer A submits his identity information ID_A to PKG. PKG computes the signer's public key as $Q_{ID_A} = H_0(ID_A)$, and returns to A as his private key and sends it via a secure channel $S_{ID_A} = sQ_{ID_A}$. Same to proxy signer, proxy signer's public and private key is (Q_{ID_B}, S_{ID_B}) . Given identity information of proxy signer, recipient, and verifier from customized identity $(ID_B \parallel ID_{\text{Re}cipent} \parallel ID_{Tran\sec tion})$ and transaction.

3. **Key Generation:** To delegate the signing capacity to proxy signers, the original signer uses the signed warrant m_w and A do the following operations:

- The original signer random chooses $k_A \in Z_q^*$, Computes $r_A = e(P, P_{pub})^{k_A}, c_A = H_1(m_w \| r_A), U_A = c_A S_{ID_A} + k_A P_{pub}$ and $U_p = c_A(Q_{ID_A} + Q_{ID_B}) + k_A P$ where m_w is warrant message, and makes U_p public in the system as public key of proxy chameleon signature.
- A sends (m_w, c_A, U_A) to proxy signer B in a secure way.
- After receiving (m_w, c_A, U_A), the proxy chameleon signer B first computes $r_A = e(U_A, P)e(Q_{ID_A}, P_{pub})^{-c_A}$, accepts it if and only if $c_A = H_1(m_w \| r_A)$. If it is right, he accepts it as a valid proxy, and uses the privilege of signature on behalf of A, then computes $S_p = c_A S_{ID_B} + U_A$ and takes Sp as a private key of proxy signature, and stores (U_p, ID_B). Otherwise he rejects it.

4. **Signature Generation:**

- **Hash:** Given a message $m \in \{0,1\}^*$, cash Proxy signer choose a random element R from G_1 and calculate the Chameleon hash function $h = Hash\,(P_{pub}, m, R, ID_j) = e(P, R)e(H_2(m)H_0(ID_j), P_{pub})$
- **Forge:** Recipient can make a forgery $R = Forge(P_{pub}, ID_j, S_j, m, R, m') = (H_2(m) - H_2(m')Q_j + R)$, and accepts this signature if and only if $c_p = H_1(h \| r_p)$. The proxy signer wants to sign a delegated message m on behalf of the original signer. Each proxy signer generates the partial proxy signature to generate proxy signature.

  Each: Proxy signer B randomly chooses, $k_B \in Z_q^*, k_B \neq 1$ and computes $r_B = e(P, P_{pub})^{k_B}, c_B = H_1(h \| r_B), U_B = c_B S_p + k_B P_{pub}$. Hence the first final proxy signature is $(m_w, c_B, U_B, U_p, m, R)$.

5. **Verification Phase:** Phase the receiving the proxy blind signature $(m, c_B, U_B, U_p, m_w, R)$, the verifier V computes $r_B^{'} = e(U_B, P)e(U_p, P_{pub})^{-c_A}$, then computes $c'_B = H_1(h \| r_B)$, the signature holds true if and only if $c_B = c'_B$.

4 ANALYSIS OF THE PROPOSED SCHEME

The correctness of the ID-based Proxy signature is justified by the following proof of correctness the forgery equation as below:

$$
\begin{aligned}
& Hash(P_{pub}, m', R', ID_j) \\
& = e(R' P)e(H_2(m')H_0(ID_j) + P_{pub}) \\
& = e(H_2(m) - H_2(m')Q_j + R, P)e(H_2(m')Q_j, P_{pub}) \\
& = e(H_2(m) - H_2(m')Q_j, P)e(R, P)e(H_2(m')Q_j, P_{pub}) \\
& = e(R, P)e(H_2(m) - H_2(m')H_0(ID_j), P_{pub})e(H_2(m')H_0(ID_j), P_{pub}) \\
& = e(R, P)e(H_2(m)H_0(ID_j), P_{pub}) \\
& = Hash(P_{pub}, m, R, ID_j)
\end{aligned}
$$

The verification of the signature is justified by the following equation:

$$
\begin{aligned}
& r'_B \\
& = e(U_B, P)e(U_B, P_{pub})^{-c_B} \\
& = e(c_B S_p + k_B P_{pub}, P)e(U_p, P_{pub})^{-c_B} \\
& = e(c_B s U_p + k_B P_{pub}, P)e(U_p, P_{pub})^{-c_B} \\
& = e(c_B U_p, P_{pub})e(k_B P_{pub}, P)e(U_p, P_{pub})^{-c_B} \\
& = e(P, P_{pub})^{k_B}
\end{aligned}
$$

So, we have $c_B = c'_B$.

5 Security Analysis

1. **Verifiability**: In anonymous proxy chameleon signature verification phase, after verifier checking and verifying the anonymous proxy chameleon signature tuple (m,R,U_B,c_B,U_p,m_w) the verifier calculate the equation $r_B = e(U_B,P)e(U_p,P_{pub})$ hold. The verifier can convinced that the received message is signed by the proxy signer has original signer signature on the m_w . The warrant contains satisfies the verification equation the limit of the delegated signing capacity and also give the identity information.

2. **Un-forge ability:** The third adversary who wants to forge the proxy chameleon signature of a message m′ for the proxy signer Bob and the original signer Alice, he must have the original signers signature on a warrant m_w. But he cannot forge this signature, since the original signer Alice uses Hesss ID-based signature scheme, which is proved to be secure against existential forgery on adaptive chosen message attacks under the random oracle model the chameleon signing phase, or find collision in the Id-based chameleon hash function, which in turn, implies setting the GDH problem. The recipient also cannot produce a signature with a new component, as this requires to break the regular digital signature.

3. **Anonymity:** From the verification of the signature, any one cannot judge the information about the signer. So it satisfies anonymity requirement.

4. **Non-transferability**: The proxy chameleon signature (m,R,U_B,c_B,U_p,m_w) generated by proxy signer for recipient C, the recipient cannot convince a trusted third party. In forge procedure, we can see that for every possible message m′, C can compute a value $R' = (H_2(m) - H_2(m')S_{ID_j} + R)$ such that $Hash\ (P_{pub}, ID_j, m, R) = Hash\ (P_{pub}, ID_j, m', R')$. Thus (m',R',c_B,U_B,U_p,m_w) is a correct proxy chameleon signature. Furthermore, for every possible message m′ there exists exactly one value R′ which produces a proper signature these nothing can be know about the value of m. Hence, non-transferability is achieved.

5. **Traceability:** The verifier proposes the disputation for the signature, since the original signer stores the proxy signer's the proxy signature public key and the identity, so he can reveal the real identity of the proxy signer with the help of the original signer.

6. **Prevention of Misuse:** The proxy key cannot be used for the purposes other than generating the valid proxy signatures. In the case of misuse, the responsibility of proxy signer would be determined explicitly.

7. **Non-repudiation:** The proxy signer uses his private key to sign the message m, the valid proxy signature contains the warrant mw, which is verified in the verification phase, it cannot be modified by the proxy signer. And give a valid signature (m,R,c_B,U_B,U_p,m_w) generated by the proxy signer B, B cannot create another tuple (m',R',c_B,U_B,U_p,m_w) for $m' \neq m$, as this would be equivalent to finding a collision of the ID-based chameleon hash function, which we assume to be infeasible by the hardness GDH group.

8. **Message Hiding:** We can see the anonymous proxy chameleon signature uses the false signature and the original signature to produce another false signature for any message with the same component of anonymous proxy chameleon signature without leaking anything about the contents of the original message.

6 Efficiency

Computational cost of our proposed scheme is given below:

Mul-mutiplication, H1 and H2-hash function, Exp-Exponent, Add-Addition, Pa-Pairing.

Table 1: Computational cost of proposed scheme

Phase	Mul	H1	H2	Exp	Add	Pa
Setup	1	1	1			
Extract	1					
KeyGenerartion	4	2		2	3	2
Signature Generation	3	1	1	1	1	2
Signature Verification				1		2

7 CONCLUSION

We conclude to say that, we have proposed an ID-based anonymous proxy chameleon signature scheme based on bilinear pairings with more efficiency. The proposed signature scheme is suitable in the situation where the proxy signer's identity needs to be secret. The proposed scheme satisfies the required security properties of an ID-based anonymous proxy chameleon signature, i.e., verifiability, un forge ability, anonymity, non transferability, traceability, prevention of misuse, non-repudiation and message hiding .

ACKNOWLEDGMENT

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] D. Boneh, B. Lynn, and H. Shacham, “Short signatures from the Weil pairing”, Advances in Cryptology-Asiacrypt 2001, LNCS 2248, pp. 514-532, 2001.

[2] D. Boneh, M. Franklin, “Identity-based encryption from the Weil pairing”, Advances in Cryptology-Crypto 2001, LNCS 2139, pp. 213-229, 2001.

[3] D.Boneh and X.Boyen, “Short Signatures Without Random Oracles”. Eurocrypt 2004, LNCS 3027, pp. 56-73, 2004.

[4] A. Joux, “The Weil and Tate Pairings as Building Blocks for Public Key Cryptosystems”, ANTS 2002, LNCS 2369, pp.20-32, 2002.

[5] H. Krawczyk and T. Rabin. “Chameleon hashing and signatures”, Proc. of NDSS, pp.143-154, 2000.

[6] M. Mambo, K. Usuda. E. Okamoto.” Proxy signature: Delegation of the power to sign messages”. IEICE Transaction Fundamentals, E79-A, pp. 1338-1353, 2005.

[7] A. Shamir, “Identity-based cryptosystems and signature schemes”, Advances in Cryptology-Crypto, LNCS 196, pp. 47-53, 1984.

[8] Y. Yung, “An efficient anonymous proxy signature scheme with provably security”, Computer standers and Interfaces, Elsevier, pp. 348-353, 2009.

[9] F. Zhang K. Kim. “Efficient ID-based blind signature and proxy signature from bilinear pairings” Advances in Cryptology-Crypto' 2003, LNCS2727, pp.312-323, 2003.