A Secure ID-based Proxy Signature Scheme from Bilinear Pairings

Pankaj Sarde
Department of Mathematics
Rungta College of Engg. & Technology
Raipur(CG), India

Amitabh Banerjee
Department of Mathematics
Govt. D. B. Girl's PG College
Raipur(CG), India

ABSTRACT

In a proxy signature scheme, a user delegates his/her signing capability to another user in such a way that the latter can sign messages on behalf of the former. Proxy signature helps the proxy signer to sign messages on behalf of the original signer. It is very useful when the original signer is not available to sign a specific document. In this paper, we propose a secure an identity based proxy signature scheme from bilinear pairings. The proposed scheme satisfy all the security property of proxy signature scheme.

Keywords

Proxy Signature, Bilinear Pairings, ID-Based Cryptography

1. INTRODUCTION

In 1984, Shamir [1] introduced the concept of ID-based cryptography to simplify key management procedures in public key infrastructures. Joux [2] gave a simple tripartite Diffie-Hellman protocol based on the Weil pairing on super-singular elliptic curves. Boneh and Franklin [3] proposed the first practical ID-based encryption scheme in Crypto'2001. Since then, ID-based cryptography has been one of the most active research areas in cryptography and numerous ID-based encryption and signature schemes have been proposed that use bilinear pairings [12, 13, 15, 16]. ID-based cryptography helps us to simplify the key management process in traditional public key infrastructures. In ID-based cryptography any public information such as email address, name, etc., can be used as a public key. Since public keys are derived from publicly known information, their authenticity is established inherently and there is no need for certificates in ID-based cryptography. The private key for a given public key is generated by a trusted authority and is sent to the user over a secure channel. In 1996, Mambo, Usuda, and Okamoto introduced the concept of proxy signature [4, 7]. In such a scheme an original signer delegates his signing authority to proxy signer in such a way that the proxy signer can sign any messages on behalf of the original signer. For example, a company's manager wants to go for a long trip. He/She would need an agent called a proxy agent, to whom He/she would assign her signing capability, and after the delegation,i.e. power assignment, the proxy agent would sign the documents on behalf of the manager. There are three types of delegation: full delegation; partial delegation and delegation by warrant. In the full delegation, the original signer just gives his signing (private) key to the proxy signer as the proxy signing key. Therefore, the signature generated between the original signer and the proxy signer is indistinguishable. In the case of partial delegation, the proxy singing key is derived from the original signer's private key by the original signer. On the other side, it is computational hard for the proxy signer to derive the private key of the original signer. However, the original signer can still forge a proxy signature of the proxy signer. In the delegation by warrant, the original signer signs a warrant that certifies the legitimacy of the proxy signer. Since then number of proxy signatures and their improvement have been proposed [6, 8, 9, 10, 11]. Lee et al. [5] defined security properties that a strong proxy signature scheme should provide:

—**Distinguishability:** Proxy signatures are distinguishable from normal signatures by everyone.

—**Verifiability:** From the proxy signature, the verifier can be convinced of the original signers agreement on the signed message.

—**Strong non-forgeability:** A designated proxy signer can create a valid proxy signature for the original signer. But the original signer and other third parties who are not designated as a proxy signer cannot create a valid proxy signature.

—**Strong identifiability:** Anyone can determine the identity of the corresponding proxy signer from the proxy signature.

—**Strong non-deniability:** Once a proxy signer creates a valid proxy signature of an original signer, he/she cannot repudiate the signature creation.

—**Prevention of misuse:** The proxy signer cannot use the proxy key for other purposes than generating a valid proxy signature. That is, he/she cannot sign messages that have not been authorized by the original signer.

A proxy signature scheme is a cryptographic primitive, that contains three entities: the original signer, the proxy signer and the verifier (at a later time). It allows the original signer to delegate her signing capability to a designated proxy signer. The proxy signer can sign some messages on behalf of the original signer. After receiving the proxy signature, the verifier, which knows the public keys of the original and proxy signers, verified the validity of the proxy signature. Generally, a proxy signature consists of four algorithms [14].

—**Setup:** On input of a security parameter l, this probabilistic algorithm outputs two secret/public key pairs (x_A, y_A) and (x_B, y_B) for the original signer Alice and the proxy signer Bob.

- **Proxy Key Pair Generation:** The original signer Alice and the proxy signer Bob execute this interactive randomized algorithm to generate a proxy key pair (x_P, y_P) for Bob, such that only Bob knows the value of x_P , while y_P is public or publicly recoverable.
- **Proxy Signature Generation:** The proxy signer Bob runs this (possibly probabilistic) algorithm to generate a proxy signature σ for a message m by using the proxy secret key x_P.
- **Proxy Signature Verification:** A verifier runs this deterministic algorithm to check whether an alleged proxy signature σ for a message m is valid with respect to a specific original signer and a proxy signer.

The rest of the paper is organized as follows. Section 2 discusses some preliminaries. Section 3 presents the proposed scheme. Section 4 analyzes the security properties and in section 5 we present the performance analysis. Finally, we conclude the paper in Section 6.

2. PRELIMINARIES

2.1 Bilinear Pairings

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. A bilinear pairing is a map $e : G_1 \times G_1 \rightarrow G_2$ with the following properties:

- **Bilinear:** $e(aP, bQ) = e(P, Q)^{ab}$
- **Non-degenerate:** There exists $P, Q \in G_1$ such that $e(P, Q) \neq 1$
- **Computable:** There is an efficient algorithm to compute $e(P, Q)$ for all $P, Q \in G_1$.

When the DDHP (Decision Diffie-Hellman Problem) is easy but the CDHP (Computational Diffie-Hellman Problem) is hard on the group G, we call G a Gap Diffie-Hellman (GDH) group. Such groups can be found on supersingular elliptic curves or hyperelliptic curves over finite field, and the bilinear parings can be derived from the Weil or Tate pairing. We can refer to [3, 12, 13] for more details.

3. PROPOSED SCHEME

In this section, we propose a secure ID-based proxy signature scheme. The participating entities and their roles in the proposed scheme are defined as follows:

- **Private Key Generator:** A trusted authority who receives signer's identity(ID) along with other parameters and generate public and private key of corresponding signer's.
- **Original Signer:** Entity who delegates his signing rights to a proxy signer.
- **Proxy Signer:** Entity who signs the message on behalf of the original signer.
- **Verifier:** Entity who verifies the proxy signature and decide to accept or reject.

The proposed scheme consists of five phases:

- **System Setup:** It takes as input a security parameter and outputs system parameters **params** and master key of PKG. Let G_1 be GDH group of order q generated by P. Let G_2 be multiplicative cyclic group of same order and $e : G_1 \times G_1 \rightarrow G_2$ be a bilinear map. PKG picks a random master key $s \in Z_q^\star$ and sets $P_{pub} = sP$. Then he chooses hash function $H_1 : \{0,1\}^\star \rightarrow G_1$, $H_2 : \{0,1\}^\star \rightarrow Z_q^\star$,$H_3 : \{0,1\}^\star \times G_1 \rightarrow Z_q^\star$. Then he publishes parameters of system **params** $= (P, q, G_1, G_2, e, H_1, H_2, H_3, P_{pub})$
- **Key Extract:** Original signer and proxy signer submit his/her identity information ID_0, ID_p respectively to PKG. PKG computes the signer's private key as $S_{ID_0} = sQ_{ID_0}$ to original signer as his private key and send it via a secure channel. Same to proxy signer, proxy signer's public key and private key is (Q_{ID_P}, S_{ID_P}).
- **Generation of Proxy Key:** To delegate the signing capacity to proxy signer, the original signer do the following operation:
  Step 1: First original signer randomly chooses $r_1 \in Z_q^\star$ and computes $U = rP, V = r_1 Q_{ID_0}$
  Step 2: Now take w(warrant) and c(Common information between original signer and proxy signer) and computes

$$\begin{aligned} U_0 &= H_1(ID_0, m_w) \in G_1 \\ h_1 &= r_1 H_2(c) + H_3(w, U) \\ T &= h_1 S_{ID_0} + U_0 r_1 \end{aligned}$$

  Thus signature on m_w is $\{U, V, T, U_0, H_2(c)\}$ send it proxy signer via a secure channel.
  Step 3: Proxy signer verify a signature on m_w such that

$$e(T, P) = e(Q_{ID_0}, P_{pub})^{H_3(w,U)} e(V, P_{pub})^{H_2(c)} e(U_0, U) \quad (1)$$

  If it is true then proxy signer accept the signature on m_w.
- **Proxy Signing:** Now proxy signer chooses $\alpha \in Z_q^\star$ and $H_3(ID_0, ID_p, m_w, T) \in Z_q^\star$ and computes

$$\begin{aligned} S_1 &= \alpha H_3(ID_0, ID_P, m_w, T)P & (2) \\ h_2 &= H_3(m, S_1) \in Z_q^\star & (3) \\ S_2 &= (h_2 + \alpha)^{-1} S_{ID_P} & (4) \end{aligned}$$

  Thus proxy signature on m is $\{S_1, S_2, T, m_w\}$
- **Proxy Verification:** The verifier first takes $H_3(ID_0, ID_P, m_w, T) \in Z_q^\star$ and verifies (S_1, S_2, T, m_w) as

$$\begin{aligned} e(S_1 + H_3(m, S_1)H_3(ID_0, ID_P, m_w, T)P, S_2) = \quad (5) \\ e(P_{pub}, Q_{ID_P})^{H_3(ID_0, ID_P, m_w, T)} \end{aligned}$$

4. SECURITY ANALYSIS

A secure proxy scheme should satisfy several security properties, we examine the security of our scheme according to the requirements.

- **Correctness:** verification of (1)

$$\begin{aligned} & e(Q_{ID_0}, P_{pub})^{H_3(w,U)} e(V, P_{pub})^{H_2(C)} e(U_0, U) \\ = \; & e(S_{ID_0} H_3(m, U), P) e(r_1 S_{ID_0}, P)^{H_2(C)} e(U_0, r_1 P) \\ = \; & e((H_3(m, U) + r_1 H_2(C)) S_{ID_0}, P) e(U_0 r_1, P) \\ = \; & e(h_1 S_{ID_0} + U_0 r_1, P) \\ = \; & e(T, P) \end{aligned}$$

  and
  verification of (5)

$$\begin{aligned} & e(S_1 + H_3(m, S_1) H_3(ID_0, ID_p, m_w, T)P, S_2) \\ = \; & e(\alpha P + h_2 P, (h_2 + \alpha)^{-1} S_{ID_P})^{H_3(ID_0, ID_P, m_w, T)} \\ = \; & e(P_{pub}, Q_{ID_P})^{H_3(ID_0, ID_p, m_w, T)} \end{aligned}$$

—**Strong Unforgeability:** The third adversary who wants to forge the proxy signature of the message m' for the proxy signer and the original signer must have the original signer's signature on a warrant m_w, but can not forge this signature, since original signer uses secure one way hash function and its private key S_{ID_0}. On the other hand, the original signer can not create a valid proxy signature. Since the proxy signer uses its own private key S_{ID_p} in proxy signature.

—**Strong Identifiability:** The verification of a valid proxy signature needs the proxy signer's public key Q_{ID_P}, in turn, proves that the signature was created by the proxy signer. It contains the warrant m_w in a valid proxy signature, so any one can determine the identity of the corresponding proxy signer from the warrant m_w.

—**Verifiability:** The verifier can be convinced of the original signer's agreement from the proxy signature.
The valid proxy signature for the message m will be the tuple (m, S_1, S_2, T, m_w), and from construction of (S_1, S_2, T) and the verification phase, the verifier can be convinced that the proxy signer has the original signer's signature on the warrant m_w. In In general the warrant contains the identity information and the limit of delegated signing capacity and so satisfies the verifiability.

—**Distinguishability:** Any verifier will receive the proxy signature that contains warrant m_w and the public key of signers, by which the verifier can easily distinguish the proxy signature from normal signature.

—**Strong Undeniability:** As the identifiability the valid proxy signature contains the warrant m_w, which must be verified in the verification phase, it can not be modified by the proxy signer, he can not repudiate the signature creation.

—**Prevention of Misuse:** In our proxy signature scheme, we use m_w and c (common information between original signer proxy signer). Thus proxy signer can not sign other message which is not authorized by the original signer.

5. PERFORMANCE ANALYSIS

Notations used for proposed scheme:

—Pa: bilinear pairing operation
—MuG_1: scalar multiplication in G_1
—MuG_2: scalar multiplication in G_2
—Me: exponentiation in G_2
—H: secure one way hash function

Table 1. Comparison of proposed scheme with J. Xu et al.'s scheme [9]

Proxy Signature from bilinear pairing				
Scheme	**Phase**			
	Proxy Delegation	Signature Generation	Signature Verification	Total
Jing Xu et al. [9]	3MuG_1 + 3H + 3Pa	2MuG_1 + 1H	1MuG_1 + 5Pa + 4H +1Me	6MuG_1 + 8Pa + 8H +1Me
Proposed Scheme	4MuG_1 + 4Pa + 3H + 2Me	2MuG_1 + 2H	2Pa + 2H + 1Me	6MuG_1 + 6Pa + 7H + 3Me

5.1 Conclusion

In this paper, we presented a secure ID-based proxy signature scheme from bilinear pairing. The security of our scheme is based both on the solving CDHP as well as strength and security of hash function. Our scheme provides all the security properties like Strong Unforgeability, Strong Identifiability, Verifiability, Distinguishability, Strong Undeniability etc. From the above tables, it is clear that proposed scheme consist of minimum number of operations. Hence the computation complexity of proposed scheme is less than the existing scheme.

6. REFERENCES

[1] A. Shamir. Identity-based cryptosystems and signature schemes. In Proc. of CRYPTO84, volume 196 of LNCS, pages 4753. Springer-Verlag, 1984.

[2] A. Joux, A one round protocol for tripartite Diffie-Hellman, In Proc. of ANTS-IV, volume 1838 of LNCS, pages 385-394, 2000.

[3] D. Boneh and M. Franklin, Identity-based encryption from the Weil pairing. In Proc. of CRYPTO01, volume 2139 of LNCS, pages 213229. Springer-Verlag, 2001

[4] M. Mambo, K. Usuda, and E. Okamoto, Proxy signatures: Delegation of the power to sign messages, IEICE Trans., 1996, E79-A, (9), pp. 1338-1354.

[5] B. Lee, H. Kim, and K. Kim, Secure mobile agent using strong non-designated proxy signature, In: Information Security and Privacy (ACISP01), LNCS 2119, pp. 474-486. Springer-Verlag, 2001.

[6] J.-Y. Lee, J. H. Cheon, and S. Kim, An analysis of proxy signatures: Is a secure channel necessary? In: Topics in Cryptology - CT-RSA 2003, LNCS 2612, pp. 68-79. Springer-Verlag, 2003.

[7] M. Mambo, K. Usuda, and E. Okamoto, Proxy signatures for delegating signing operation. In: Proc. of 3rd ACM Conference on Computer and Communications Security (CCS96), pp. 48-57. ACM Press, 1996.

[8] G. Wang, F. Bao, J. Zhou, and R. H. Deng, Security analysis of some proxy signatures. In: Information Security and Cryptology - ICISC 2003, LNCS 2971, pp. 305-319. Springer-Verlag, 2004.

[9] J. Xu, Z. Zhang, and D. Feng, ID-Based Proxy Signature Using Bilinear Pairings, Available at http://eprint.iacr.org/2004/206/

[10] F. Zhang, and K. Kim, Efficient ID-based blind signature and proxy signature from bilinear pairings, in Proceedings of Australasian Conference on Information Security and Privacy, LNCS 2727, Springer-Verlag, pp.312-323, 2003

[11] H. M. Sun and B. T. Hsieh, On the security of some proxy signature schemes, Available at http://eprint.iacr.org/2003/068.

[12] J.C. Cha and J.H. Cheon, An identity-based signature from gap Diffie-Hellman groups, Public Key Cryptography - PKC 2003, LNCS 2139, pp.18-30, Springer- Verlag, 2003.

[13] F. Hess, Efficient identity based signature schemes based on pairings, SAC 2002, LNCS 2595, pp.310-324, Springer-Verlag, 2002.

[14] Wang, G., Designated-verifier proxy signature schemes, in: Security and privacy in the age of ubiquitous computing. Proc. of 20th Int. Conf. on Information Security (IFIP/SEC 2005), pp. 409-423

[15] K.G. Paterson, ID-based signatures from pairings on elliptic curves, Electron. Lett., Vol.38, No.18, pp.1025-1026, 2002.

[16] R. Sakai, K. Ohgishi, M. Kasahara, Cryptosystems based on pairing, SCIS 2000-C20, Jan. 2000, Okinawa, Japan.