Formal Security of an Identity-Based Proxy Signature Scheme in the Random Oracle Model

Mohammad Beheshti-Atashgah, Mahmoud Gardeshi, and Majid Bayat

***Abstract*—Currently, ID-based public key cryptography has got many useful achievements and attracted much attention. Proxy signature scheme enables an original signer to delegate his\her signing capability to a proxy signer to sign messages on behalf of the original signer. In this paper, we will theoretically discuss on the provable security of an ID-based proxy signature scheme. In fact, we analyze the ID-based proxy signature scheme proposed by Mala et al.'s and show that this scheme is secure in the random oracle model. We show that their scheme's security can be reduced to the hardness of CDHP.**

***Index Terms*—ID-based proxy signature scheme, provable security, random oracle model, pairing.**

I. Introduction

The concept of proxy signature scheme was first introduced by Mambo et al.'s in 1996 [1]. In a proxy signature scheme, an original signer can delegate his\her signing power to a proxy signer and then the proxy signer can create a valid signature on behalf of the original signer. In order to introduce a secure proxy signature, each proxy signature scheme should satisfy these security requirements [2,3]: *Verifiability*, *Strong Unforgeability*, *Strong Undeniability*, *Strong Identifiability* and *Prevention of misuse*.

Although. many proxy signature scheme provide the above requirements, but their security meaning are unclear. Recently, a method has been developed that called Provable-Security [4]. This method has been widely used to support standard. Boldyreva et al. [5] used this theory to help the security analysis of the proxy signature schemes, and provide methods to prove the security of such schemes.

ID-based proxy signature scheme (IBPS Scheme or IBPSS) is a special ID-based public key cryptography (ID-PKC). Shamir [6] was first proposed the idea of ID-PKC in 1984. So far, many ID-based proxy signature scheme have been proposed [7,8] and some of IBPSS have provable security in the random oracle model such as [9], [10] and [11].

In this paper, we will analyze the IBPS scheme proposed by Mala et al. [7]. We will show that their scheme can be proven to be secure in the random oracle model and their scheme's security can be reduced to the hardness of CDHP.

The rest of paper is organized as follows: In the next section, we present the basic definitions. In the section 3, we review the Mala et al.'s IBPS scheme. Section 4, presents the attack model and security proof of the IBPS scheme. Finally, section 5 concludes this article.

Manuscript received May 3, 2012; revised May 31, 2012.

Mohammad Beheshti-Atashgah is with the Research Center of Intelligent Signal Processing, Tehran, Iran. (e-mail: M.Beheshti.A@ gmail.com).

Mahmoud Gardeshi is with Department of Electrical and Computer Engineering, Imam Hossein University, Tehran, Iran (e-mail: mgardeshi@ihu.ac.ir).

Majid Bayat is with Department of Mathematics & Computer Science, Tarbiat Moallem University, Tehran, Iran (e-mail: Bayat@tmu.ac.ir).

II. Bilinear Pairings

Let G_1 be a additive cyclic group with prime order q, G_2 be a multiplicative cyclic group with the same order. Bilinear pairing $e: G_1 \times G_1 \rightarrow G_2$ is a map with the following properties:

1) *Bilinearity*: $\forall P, Q \in G_1, a, b \in \mathbb{Z}_q$, $e(aP, bQ) = e(P, Q)^{ab}$;
2) *Non-degenerate*: There exists $P, Q \in G_1$, $e(P, Q) \neq 1_{G_2}$;
3) *Computable*: There is an efficient algorithm to compute $e(P, Q)^{ab}$ for any $P, Q \in G_1$.

We now describe two mathematical problems: the Decisional Diffie-Hellman Problem ($DDHP$) and the Computational Diffie-Hellman Problem ($CDHP$).

1) Decisional Diffie-Hellman Problem ($DDHP$). Given (P, aP, bP, cP), decide whether $c = ab \ mod \ q$.
2) Computational Diffie-Hellman Problem ($CDHP$). Given (P, aP, bP), compute abP.

III. The Mala et al.'s Scheme

The complete description of the Mala et al.'s scheme [4] is given as follows:

Setup: Let G_1 be a CDH group of prime order q introduced by P, G_2 be a multiplicative cyclic group of the same order, and $e: G_1 \times G_1 \rightarrow G_2$ be a bilinear map. PKG chooses a random master key $s \in_R \mathbb{Z}_q^*$ and sets $P_{pub} = sP$. Then he\she chooses hash functions: $H_1: \{0,1\}^* \rightarrow G_1$, $H: \{0,1\}^* \rightarrow \mathbb{Z}_q^*$. Then he\she publishes these parameters as the system parameters:

$$\Omega = \left(q, G_1, G_2, e, P, H_1, H_2, H_3, H_4, P_{pub}\right)$$

Key Extract: For a given identity ID , PKG computes $Q_{ID} = H_1(ID) \in G_1$ and the corresponding private key $S_{ID} = sQ_{ID} \in G_1$.

Sign: For the private key S_d of the original signer ID_d, in order to sign the warrant m_W, he\she uses Hess's signature scheme:

1) Chooses $k_d \in_R \mathbb{Z}_q^*$ at random and computes $r_d = e(P, P)^{k_d}$ and $c_d = H(m_W, r_d)$.
2) Computes $U_d = c_d S_d + k_d P \in G_1$. The signature on m_W is the warrant $W = \langle c_d, U_d \rangle$.

Verify: to verify the signature $\langle c_d, U_d \rangle$ on a message m_W for the identity ID_d, the verifier

1) First should computes $Q_{ID_d} = H_1(ID_d)$ and $r' = e(U, P) e\left(Q_{ID}, P_{pub}\right)$.

2) Then he\she accepts the signature if and only if $c_d = H(m_W, r')$.

Proxy designation: In order to designate user ID_p as a proxy signer, the original signer sends user ID_p a message m_W and corresponding warrant W. The proxy signer ID_p verifies this signature W. If the signature is valid, then the proxy signer computes the proxy signing key $sk_p = c_d S_p$.

Proxy signing: the proxy signer can sign a message m on behalf of the original signer as follows:

1) Picks $k_p \in_R \mathbb{Z}_q^*$ at random and computes $r_p = e(P,P)^{k_p}$ and then puts $c_p = H(m, r_p r_d)$.
2) Computes $U_p = c_p sk_p + k_p P$.

The proxy signature on message m will be $(m_W, ID_p, ID_d, U_p, U_d, c_p, c_d)$.

Proxy Verification: The verifier first takes $Q_{ID_p} = H_1(ID_p) \in G_1$, $Q_{ID_d} = H_1(ID_d) \in G_1$ and then computes:

$$r' = e(U_p + U_d, P) \cdot e(Q_d + c_p Q_p, P_{pub})^{-c_d} \quad (1)$$

Then he\she accepts the signature as a valid proxy signature if and only if the follow equation hold.

$$c_p = H(m, r') \quad (2)$$

IV. Security Proof

A. Attack Model for an IBS

We consider a polynomial-time adversary $\mathcal{A}$. The security model of identity-based proxy signature is defined as follows:

Definition. An IBPS scheme is existentially unforgeable under adaptive chosen message and identity attack (EUF-ACMIA) if no probabilistic polynomial time adversary $\mathcal{A}$ has non-negligible advantage in the game. For an identity-based proxy signature (IBPS), we define an $Exp_{\mathcal{A}}^{IBPS}(k)$ of adversary $\mathcal{A}$ and security parameter k as follows:

1) A challenger $\mathcal{C}$ runs Setup algorithm and gives the system parameters Ω to $\mathcal{A}$.
2) $E_{list} \leftarrow \phi$, $D_{list} \leftarrow \phi$, $G_{list} \leftarrow \phi$, $S_{list} \leftarrow \phi$.
3) Adversary $\mathcal{A}$ can make the following queries.
   - $Extract(\cdot)$: This oracle takes as input a user's ID_i, and outputs the corresponding private key S_i. Let $E_{list} \leftarrow E_{list} \cup \{(ID_i, d_i)\}$.
   - $Delegate(\cdot)$: This oracle takes as input the designator's ID and a warrant m_W, and returns a delegation W. Let $D_{list} \leftarrow D_{list} \cup \{(ID, m_W, W)\}$.
   - $PKgen(\cdot)$: This oracle takes as input the delegation W and a message $m \in \{0,1\}^*$, and outputs a proxy signing key sk_p. Let $G_{list} \leftarrow G_{list} \cup \{(ID, m_W, sk_p)\}$.
   - $PSign(\cdot)$: This oracle takes as input the proxy signer's ID and a delegation W, and outputs a proxy signature introduced by the proxy signer. Let $S_{list} \leftarrow S_{list} \cup \{(W, m, \tau)\}$.
4) Adversary $\mathcal{A}$ outputs (ID, m_W, W) or (W, m, τ).
5) $\mathcal{A}$'s output should satisfy one of the following cases till $\mathcal{A}$'s attack be successful.
   - (ID, m_W, W) satisfies: $DVerify(W, ID) = 1$, $(ID, .) \notin E_{list}$, $(ID, ., .) \notin G_{list}$ and $(ID, m_W, .) \notin D_{list}$. $Exp_{\mathcal{A}}^{IBPS}(k)$ returns 1.
   - (W, m, τ) satisfies: $PVerify((m, \tau), ID_i) = 1$, $(W, m, .) \notin S_{list}$, $(ID_j, .) \notin E_{list}$, $(ID_j, W, .) \notin G_{list}$ where ID_i and ID_j are the identities of the original signer and the proxy signer, respectively. $Exp_{\mathcal{A}}^{IBPS}(k)$ returns 2.

Otherwise, $Exp_{\mathcal{A}}^{IBPS}(k)$ returns 0.

The success probability of $\mathcal{A}$ is defined as:

$$\mathbf{Adv}_{\mathcal{A}}^{IBPS} = \Pr[Exp_{\mathcal{A}}^{IBPS}(k) outputs\ 1\ or\ 2]$$

B. The Security proof of Mala et al.'s Scheme

Theorem. Assume that the Mala et al. ID-based Proxy signature scheme be a $IBPSS$. In the random oracle model, let $\mathcal{A}$ be a polynomial-time adversary who manages an $Exp_{\mathcal{A}}^{IBPS}(k)$ within a time bounded T, and gets return 2 by un-negligible probability ε. Assume that $\mathcal{A}$ makes at most q_{H_1}, q_H queries to random oracles H_1, H respectively, q_K queries to $PKgen$ oracle, q_D queries to $Delegate$ oracle and q_S queries to $PSign$ oracle. Let t_m be the time of one scalar multiplication in G_1.

Assume that $\varepsilon \geq 10(q_S + 1)(q_H + q_S)q_{H_1}/q$, then there is an adversary $\mathcal{A}$ who can solve $CDHP$ within time $T' \leq T + (q_{H_1} + q_K + 3q_D + 4q_S)t_m$.

$Proof$. Without loss of generality, we assume that for any ID , $\mathcal{A}$ queries $H_1(ID)$ before querying $Extract(\cdot)$, $Delegate(\cdot)$, $PKgen(\cdot)$ and $PSign(\cdot)$. Our algorithm $\mathcal{B}$ takes a random tuple (P, aP, Q) , where P is a random generator of G_1 . The simulator $\mathcal{B}$ will interact with the adversary $\mathcal{A}$ as follows:

1) A challenger $\mathcal{C}$ runs setup algorithm to generate system parameters Ω and gives it to $\mathcal{B}$.

2) $\mathcal{B}$ sets $P_{pub} = aP$ and $i = 1$.

3) $\mathcal{B}$ sets lists: $E_{list} \leftarrow \phi$, $D_{list} \leftarrow \phi$, $G_{list} \leftarrow \phi$, $S_{list} \leftarrow \phi$.

4) $\mathcal{B}$ chooses randomly $t, 1 \leq t \leq q_{H_1}$ and $x_i \in \mathbb{Z}_q, i = 1,2,\cdots,q_{H_1}$.

5) $\mathcal{B}$ gives $\mathcal{A}$ system parameters Ω and lets $\mathcal{A}$ manages $\mathrm{Exp}_{\mathcal{A}}^{\mathrm{IBPS}}(\mathrm{k})$. During the execution of game, $\mathcal{B}$ simulates $\mathcal{A}$'s oracles as follows:

$H_1(\cdot)$: For input ID, $\mathcal{B}$ checks if $H_1(ID)$ defined. If not, he\she defines

$$H_1(ID) = \begin{cases} Q & i = t \\ x_i P & i \neq t \end{cases} \quad (3)$$

And sets $ID_i \leftarrow ID$, $i \leftarrow i + 1$. $\mathcal{B}$ returns $H_1(ID)$ to $\mathcal{A}$.

$H(\cdot)$: If $\mathcal{A}$ makes a query (m, r) to random oracle $H(\cdot)$, $\mathcal{B}$ checks if $H(m, r)$ defined. If not, he\she chooses $c \in \mathbb{Z}_q$ at random and sets $H(m, r) \leftarrow c$. Then he\she returns $H(m, r)$ to $\mathcal{A}$.

$Extract(\cdot)$: For ID_i, if $i = t$, then $\mathcal{B}$ aborts. Otherwise, $\mathcal{B}$ replies to $\mathcal{A}$ with $S_i = x_i \cdot P_{pub}$ and sets $E_{list} \leftarrow E_{list} \cup \{(ID_i, S_i)\}$.

$Delegate(\cdot)$: For input ID_i and warrant m_W (assume that the proxy identity is ID_j), if $i \neq t$, $\mathcal{B}$ uses $S_i = x_i \cdot P_{pub}$ (as the private key) to sign in m_W with Hess's scheme [12] and gets (r_0, U_0) . Otherwise, $\mathcal{B}$ simulates ID_t 's proxy-designation as follows:

- Choose $U_0 \in G_1$, $c_0 \in \mathbb{Z}_q$ at random.

- Compute $r_0' = e(U_0, P)\left(e(Q, P_{pub})\right)^{-c_0}$.
- If $\mathcal{A}$ has made the query (m_W, r_0') to $H(\cdot)$, then $\mathcal{B}$ aborts and report fail (because a collision appears). Otherwise, $\mathcal{B}$ sets $H(m_W, r_0') = c_0$.

Assume that $W = (m_W, r_0', U_0)$ be the reply, and set $D_{list} \leftarrow D_{list} \cup \{(ID_i, m_W, W)\}$.

$PKgen(\cdot)$: For input ID_j (proxy signer's ID) and delegation $W = (m_W, r_0', U_0)$, if $j = t$, then $\mathcal{B}$ aborts. Otherwise, $\mathcal{B}$ computes $sk_p = H(m_W, r_0')x_j P_{pub} + U_0$ as the reply to adversary $\mathcal{A}$. Let $G_{list} \leftarrow G_{list} \cup \{(ID_j, sk_p, W)\}$.

$PSign(\cdot)$: For input $W = (m_W, r_0', U_0)$ and message m, original signer's identity be ID_i and proxy signer's identity be ID_j. If $j \neq t$, $\mathcal{B}$ computes the proxy signature (r_P, U_P) on m with signing key $sk_p = H(m_W, r_0')x_j P_{pub} + U_0$, and return (m, r_P, U_P, m_W, r_0') to $\mathcal{A}$ as the reply. Otherwise, $\mathcal{B}$ simulates ID_t's proxy signature (on behalf of ID_i) as follows:

- Choose $U \in G_1$, $c \in \mathbb{Z}_q$ at random.
- Check whether $H(m_W, r_0')$ is defined. If not, request oracle $H(\cdot)$ with (m_W, r_0'). Let $H(m_W, r_0') = e$.
- Compute $r = e(U, P)\left(r_0' \cdot e(x_i P + Q, P_{pub})^e\right)^{-c}$.
- If $\mathcal{A}$ has made the query (m, r) to $H(\cdot)$, then $\mathcal{B}$ aborts and report fail (because a collision appears). Otherwise, $\mathcal{B}$ sets $H(m, r) = c$.
- Let (m, r, U, m_W, r_0') be the reply of $PSign(\cdot)$. Let $S_{list} \leftarrow S_{list} \cup \{(W, m, r, U, m_W, r_0')\}$. (the simulation has the same distribution that the real one)

1) If $\mathcal{A}$'s output is $(W, m, \tau) = \left((m_W, r_0', U_0), m, (m_W, r_0', r, U)\right)$ with original signer's identity ID_i and proxy signer's identity ID_j, satisfying: $PVerify\left((m, \tau), ID_i\right) = 1$, $(W, m, .) \notin S_{list}$, $(ID_j, .) \notin E_{list}$, $(ID_j, W, .) \notin G_{list}$, and $j = t$, $\mathcal{B}$ can get a forgery (m, r, c, U) of GDS (generic digital signature) scheme corresponding to private key $sk_p = eaQ$, where $e = H(m_W, r_0')$ and $c = H(m, r)$.

2) If $\mathcal{B}$ have got two GDS signatures corresponding to private key $sk_p = eaQ$: (m, r, c, U) and (m, r, c', U'), $\mathcal{B}$ can outputs aQ as follows:

$$aQ = e^{-1}[(c - c') \cdot (U - U')] \qquad (4)$$

Otherwise, $\mathcal{B}$ sets $H(m_W, r_0') = e$, $i = 1$, and returns to step 5.

During $\mathcal{B}$'s execution, if $\mathcal{A}$ manages an $Exp_{\mathcal{A}}(k)$ and gets return 2, collisions appear with negligible probability, as showed in [8]. So, $\mathcal{B}$'s simulations are indistinguishable from $\mathcal{A}$'s oracles. Because t is chosen at random, $\mathcal{B}$ can output a forgery of proxy signature corresponding to private key $sk_p = eaQ$ within expected time T with probability ε / q_{H_1}. Based on the *Forking lemma*[8], $\mathcal{B}$ can produce two valid signatures (m, r, U, c) and (m, r, c', U') such that $c \neq c'$ within expected time $T' \leq T + \left(q_{H_1} + q_K + 3q_D + 4q_S\right)t_m$. So $\mathcal{B}$ can output aQ. Thus we prove the theorem.

V. Conclusions

In this article, we discussed on the provable security of the Mala et al.'s ID-based proxy signature scheme [4]. We showed that this scheme is secure against existential forgery on adaptive chosen message and ID attacks (EUF-ACMIA), under the hardness assumption of CDHP in the random oracle model.

References

[1] M. Mambo, K. Usuda and E. Okamato, "Proxy Signature for Delegating Signing Operation", 3rd AC-Conference on Computer and Communications security (CCS96), AC-Press, New York, 1996, pp. 48-57.

[2] B. Lee, H. Kim and K. Kim, "Strong Proxy Signature and its Applications", In Proc. Of the 2001 Symposium on Cryptography and Information Security (SCIS01), vol 2/2, Oiso, japan, 2001, pp. 603-608.

[3] S.-H. Seo, K.-A. Shim and S.-H. Lee, "A Mediated Proxy Signature Scheme with Fast Revocation for Electronic Transactions", Proc. of the 2nd International Conference on Trust, Privacy and Security in Digital Business, Copenhagen Denmark, LNCS 3592. Berlin, German; Springer-Verlag, 2005, pp. 216-225.

[4] D. Pointcheval an J. Stern, "Security Arguments for Digital Signature and Blind Signatures", Journal of Cryptography, 13(3), 2000, pp. 361-369.

[5] A. Boldyreva, A. Palacio and B. Warinschi, "Secure Proxy Signature Schemes for Delegation of Signing Rights", [online]. Available: http://eprint.iacr.org/2003/096.

[6] A. Shamir, "Identity-Based Cryptosystems and Signature Schemes", In Advances in Cryptology-CRYPTO84, volume 196 of LNCS, Springer-Verlag, 1984, pp. 47-53.

[7] H. Mala, M. Dakhil-Alian and M. Brenjkoub, "A New Identity-Based Proxy Signature Scheme from Bilinear Pairings", IEEE explore, 2006, pp. 3304-3308.

[8] X. Li, K. Chen, "Certificateless Signature and Proxy Signature Schemes from Bilinear Pairings", Lithuanian Mathematical Journal, vol. 45, No.1, 2005, pp. 76-82.

[9] C. Gu, Y. Zhu, "Provable Security of ID-Based Proxy Signature Schemes", ICCNMC 2005, LNCS 3619, Springer-Verlag Heidelberg, 2005, pp. 1277-1286.

[10] H. Ji, W. Han, L. Zhao and Y. Wang, "An Identity-Based Proxy Signature from Bilinear Pairings", WASE International Conference on Information Engineering, 2009, pp. 14-17.

[11] R. Lu, Z. Cao, X. Dong and R. Su, "Designated Verifier Proxy Signature Scheme from Bilinear Pairings", Proceeding of the first International Multi-Symposiums on Computer and Computational Science (IMSCCS06), IEEE, 2006, pp 40-47.

[12] F. Hess, "Efficient Identity-Based Signature based on Pairings", In K. Nyberg and H. Heys, editors, Selected Areas in Cryptography 9th Annual International Workshop, SAC 2002, volume 2595 of LNCS, Springer-Verlag, 2003, pp. 310-324.

Mohammad Beheshti-Atashgah was born in Tehran, Iran on December 1984. He received his B.Sc. degree in Electrical Engineering in 2008 and his M.Sc. in Communication Engineering from Imam Hossein University, Tehran, Iran in 2011. Until now, he has published more than 14 papers in the National and International journals, Conferences and workshops. His research interests include: Cryptographic Protocols, Provable Security of Digital Signature Schemes, Identity-Based Cryptography, Lattice-Based Cryptography and Network Security.

Mahmoud Gardeshi received his B.Sc. degree in applied mathematics from Shiraz University in 1989 and M.Sc. degree in applied mathematics from Tabriz University in 1991. He also received his M.Pill degree from Amir Kabir University, Iran in 1999. Now, He is a researcher at the Imam Hossein University (I.H.U), Tehran, Iran. His research interest includes: Public key Cryptography, Lattice-Based Cryptography, Digital Signatures and Cryptographic Protocols.

Majid Bayat is a Ph.D. candidate in the Department of Mathematics and Computer Sciences at Kharazmi University (Tarbiat Moallem University) in Tehran, Iran. He is presently a Research Assistant of Tarbiat Moallem University and Information Systems and Security Lab (ISSL) of Sharif University in Tehran, Iran. His research interests include: Public Key Cryptography, Key Agreement Protocols and Provable Security.