An anonymous proxy signature scheme without random oracles

Rahim Toluee[1], Maryam Rajabzadeh Asaar[1], Mahmoud Salmasizadeh[2]
[1]Department of Electrical Engineering, Sharif University of Technology
[2]Electronics Research Institute, Sharif University of Technology
toluee@ee.sharif.edu, asaar@ee.sharif.edu, salmasi@sharif.edu

***Abstract*—The concept of proxy signature was introduced in 1996, up to now many proxy signature schemes have been proposed. In order to protect the proxy signer's privacy, the concept of anonymous proxy signature, which is also called proxy ring signature, was introduced in 2003. Some anonymous proxy signature schemes, which are provable secure in the random oracle model, have been proposed. However, provable security in the random oracle model is doubtful when the random oracles are instantiated with hash functions in their implementation. Hence, we propose the first secure anonymous proxy signature scheme without random oracles.**

Keywords-proxy signature; ring signature; bilinear pairings; provable security; proxy ring signature;anonymous proxy signature

I. INTRODUCTION

The concept of proxy signature was first introduced by Mambo, Usuda and Okamoto in 1996 [1, 2]. It's very useful in cases when an original signer, wishes to delegate his signing rights to the other one, called a proxy signer.

Proxy signatures can be combined with other special signatures to obtain several variants of proxy signatures such as threshold proxy signatures [3, 4], blind proxy signatures [5, 6], proxy ring signatures [7, 8, 20] and ring proxy signatures [19]. (The ring proxy signature provides the anonymity of the original signer while the proxy ring signature provides the anonymity of the proxy signer.)

The concept of ring signature was first introduced by Rivest, Shamir and Tauman [10]. A ring signature same as group signature [11] provides the anonymity of a signer, which means that the verifier knows that the signer is a member of a ring, but he doesn't know exactly who the signer is. There is also no way to revoke the anonymity of the signer.

Another property of ring signatures is setup free which makes distinction between ring signatures and group signatures. In group signature schemes, there exists a trusted third party (TTP) or group manager who manages the joining of group members. In ring signature schemes does not exist such trusted party and the rest of the $n-1$ members in the ring are totally unaware of being involved in the ring. These two properties make ring signatures widely applicable to many cryptographic schemes [12].

Ring signatures can be combined with other special signatures to obtain several variants of ring signatures such as threshold ring signatures [16], Identity-based ring signatures [17] and universal designated verifiable ring signatures [18].

Anonymous proxy signatures, also called proxy ring signatures, are useful in cases when an entity delegates his signing capability to many proxies, called proxy signers group, while it provides anonymity of proxy signers. A choice is using the group signature to solve it (take the group manger as the original entity), but in some applications, unconditional anonymity is necessary. If the proxies hope that nobody (including the original signer) can open their identities, the group signature is not suitable for this situation. So we can use the ring signature to solve this problem and gain the anonymous proxy signature [8, 13, 14, 15], which was first proposed by Zhang et al. in 2003 [20].

Yong Yu, Chunxiang Xu, Xinyi Huang and Yi Mu, in 2009 proposed an efficient anonymous proxy signature scheme with provable security in the random oracle models [15]. However, provable security in the random oracle model is doubtful when the random oracles are instantiated with hash functions in their implementation. Hence, in this paper we propose the first anonymous proxy signature scheme secure without random oracles. In this way we make use of two signature schemes: the first one is a proxy signature scheme in standard model, which was proposed by Ying Sun, Chunxiang Xu, Yong Yu and Yi Mu in 2011 [21], and the second one is a ring signature scheme without random oracles, which was proposed by H. Shacham and B. Waters in 2007[22].

Roadmap: The rest of this paper is organized as follows. Preliminary is given in section II. Some definitions are described in Section III. Our anonymous proxy signature scheme is presented in Section IV. In Section V, a brief discussion on security analysis of our scheme is given. Finally, conclusions are given in Section VI.

II. PRELIMINARY

- *Bilinear Pairing*

We make use of bilinear groups of composite order. These were introduced by Boneh, Goh and Nissim [9]. Let n be a composite with factorization $n = pq$. We have:

- G is a multiplicative cyclic group of order n;
- G_p is its cyclic order-p subgroup, and $G_q$is its cyclic order-q subgroup;
- g is a generator of G, while h is a generator of G_q;
- G_T is a multiplicative group of order n;
- $e : G \times G \to G_T$ is efficiently computable map with the following properties:
    - Bilinear: for all $u, v \in G$ and $a, b \in Z$ we have

$$e(u^a, v^b) = e(u, v)^{ab} \quad (1)$$

    - Non-degenerate: $e(g, g)$ is generator of G_T whenever g is generator of G;

III. DEFINITIONS

A. Adversaries Types

To discuss the unforgeability of anonymous proxy signature schemes, we categorize the adversaries into three types.

Type1: An adversary only has the public keys of the original signer and proxy signers.

Type2: An adversary has the public keys of the original signer and proxy signers; besides he has the secret keys of some proxy signers.

Type3: An adversary has the public keys of the original signer and proxy signers; besides he has the secret key of the original signer.

It can be found that if an anonymous proxy signature scheme is unforgeable against Type2 and Type3 adversary, it is also unforgeable against Type1 adversary.

B. Model of anonymous proxy signature schemes

An anonymous proxy (APS) signature scheme consists of the following algorithms.

1. Setup: Given the system security parameter k, this algorithm outputs system's parameters. For instance, we can assign this part to a trusted third party.
2. Key Generation: On input a security parameter k, this probabilistic polynomial time (PPT) algorithm generates a personal public-private key pair (Y, x).
3. Delegation Generation: On input a warrant m_w and the original signer's private key x_o, this algorithm generates a signature $\sigma_w$on m_w.
4. Delegation Verification: On input the original signer's public key Y_o and his signature σ_w on the warrant m_w, this algorithm outputs "accept" if the signature is valid, and "reject" otherwise.
5. APS Generation: On input a message m, the public key $Y_o$of the original signer, the public keys $Y_1, \dots, Y_n$ of the n proxy signers, the warrant m_w, signature σ_w on m_w and one proxy signer's secret key, this algorithm generates an anonymous proxy signature σ for the message m.
6. APS Verification: On input a message m, an anonymous proxy signature σ, the public key Y_o of the original signer, the public keys $Y_1, \dots, Y_n$ of the n proxy signers, the warrant m_w and the signature σ_w on m_w this algorithm outputs "accept" if the signature is valid, and "reject" otherwise.

IV. OUR SCHEME

A. Setup

The trusted setup algorithm first constructs a group G of composite order $n = pq$as described in section II. It then chooses exponents $(a, b_0 \overset{R}{\leftarrow} Z_n)$ and sets

$$A = g^a$$

$$B_0 = g^{b_0}$$

$$A' = h^a$$

Let $H : \{0,1\}^* \to \{0,1\}^k$ be a collision-resistant hash function. The setup algorithm chooses generators

$$u', u_1, u_2, \dots, u_k \overset{R}{\leftarrow} G$$

Let (G, G_T) be bilinear groups where $|G| = |G_T| = n$, g is the generator of G. Parameter e denotes an admissible pairing $G \times G \to G_T$.

The published common reference string includes a description of the groups G and G_T and of the collision-resistant hash H, along with (A, B_0, A') and $(u', u_1, u_2, \dots, u_k)$. The factorization of n is not revealed .Note that anyone can use the pairing to verify that the pair (A, A') is properly formed [22].

B. Key Generation

Original signer picks $x_a \overset{R}{\leftarrow} Z_n$ and sets his secret key $sk_a = A^{x_a}$and his public key $pk_a = g^{x_a}$. In the same way, the proxy ring members compute their private keys and public keys.

C. Delegation Generation

Let $W = (w_1, w_2, \dots, w_k)$ be a k-bit warrant to be signed by the original signer. The original signer picks a random $r_a \overset{R}{\leftarrow} Z_n$ and computes the delegation $\sigma_w = (\sigma_{w1}, \sigma_{w2})$ and sends it to the proxy signer ring, where

$$\sigma_{w1} = sk_a \cdot \left(u' \prod_{i=1}^{k} u_i^{w_i}\right)^{r_a} \quad (2)$$

$$\sigma_{w2} = g^{r_a} \quad (3)$$

D. Delegation Verification

Upon receiving $(W, \sigma_{w1}, \sigma_{w2})$, each proxy signer checks that the following equation is satisfied or not

$$e(\sigma_{w1}, g) = e(\sigma_{w2}, u' \prod_{i=1}^{k} u_i^{w_i}) e(A, pk_a) \quad (4)$$

If it does not hold, the delegation will be rejected. Otherwise, it will be accepted.

E. APS Generation

The signing algorithm takes as input a message $M \in \{0,1\}^*$, a ring R of public keys of proxy signers, the signature σ_w on m_w, and a key pair $(pk, sk) \in G^2$, where

$$x_b \overset{R}{\leftarrow} Z_n$$

$$sk = A^{x_b}$$

$$pk = g^{x_b}$$

No key may appear twice in R, and R must include pk.

Signer computes $(m_1, m_2, \dots, m_k) \leftarrow H(M, R)$. Let $l = |R|$; signer parses the elements of R as $v_i \in G$ for each i, $1 \le i \le l$.

Let i^* be the index such that v_{i^*} = pk. Define

$$f_i = \begin{cases} 1 & if\ i = i^* \\ 0 & O.w \end{cases} \quad (5)$$

Now for each i, $1 \le i \le l$, signer chooses a random exponent $t_i \overset{R}{\leftarrow} Z_n$ and sets

$$C_i \leftarrow \left(\frac{v_i}{B_0}\right)^{f_i} h^{t_i} \quad (6)$$

$$\pi_i \leftarrow \left(\left(\frac{v_i}{B_0}\right)^{2f_i - 1} h^{t_i}\right)^{t_i} \quad (7)$$

$$C \leftarrow \prod_{i=1}^{l} C_i \quad (8)$$

$$t \leftarrow \sum_{i=1}^{l} t_i \quad (9)$$

Finally, signer chooses $r \overset{R}{\leftarrow} Z_n$ and computes

$$S_1 \leftarrow \sigma_{w1}.sk.\left(u' \prod_{j=1}^{k} u_j^{m_j}\right)^r . A'^t \quad (10)$$

$$S_2 \leftarrow g^r \quad (11)$$

$$S_3 \leftarrow \sigma_{w2} \quad (12)$$

The signature is output as σ, where

$$\sigma = \left((S_1, S_2, S_3), \{(C_i, \pi_i)\}_{i=1}^{l}\right) \in G^{2l+3}$$

F. APS Verification

Verifier computes $(m_1, m_2, \dots, m_k) \leftarrow H(M, R)$. Let $l = |R|$; verifier parses the elements of R as $v_i \in G$, for each $i, 1 \le i \le l$. Verifier checks that no element is repeated in R and rejects otherwise. Then verifier parses the signature σ as $\left((S_1, S_2, S_3), \{(C_i, \pi_i)\}_{i=1}^{l}\right) \in G^{2l+3}$. (If this parse fails, reject.). Verifier checks first that the $\{\pi_i\}_{i=1}^{l}$ are valid or not

$$e(C_i, C_i/(v_i/B_0)) = e(h, \pi_i) \quad (13)$$

If any of the proofs is invalid, reject. Otherwise, verifier sets $C \leftarrow \prod_{i=1}^{l} C_i$. Accept if the following equation is satisfied

$$e(S_1, g) = e(S_2, u' \prod_{j=1}^{k} u_j^{m_j})\, e(A, B_0 C) e(A, pk_a) e(S_3, u' \prod_{i=1}^{k} u_i^{w_i}) \quad (14)$$

Note that, there is exactly one non-zero value amongst $\{f_i\}$, and we have

$$B_0 C = (v_{i^*})(h^t) \quad (15)$$

The correctness of the scheme can be verified directly, as the following equations

$$e(S_1, g) = e(\sigma_{w1}.sk.\left(u' \prod_{j=1}^{k} u_j^{m_j}\right)^r . A'^t, g)$$

$$= e(\sigma_{w1}, g) e(sk, g) e\left(\left(u' \prod_{j=1}^{k} u_j^{m_j}\right)^r, g\right) e(A'^t, g)$$

$$= e\left(\left(u' \prod_{i=1}^{k} u_i^{w_i}\right)^{r_a}, g\right) e(sk_a, g) e(sk, g) e\left(\left(u' \prod_{j=1}^{k} u_j^{m_j}\right)^r, g\right) e(A'^t, g)$$

$$= e(u' \prod_{i=1}^{k} u_i^{w_i}, g^{r_a}) e(A, g^{x_a}) e(A, g^{x_b}) e(u' \prod_{j=1}^{k} u_j^{m_j}, g^r) e(h^{at}, g)$$

$$= e(S_3, u' \prod_{i=1}^{k} u_i^{w_i}) e(A, pk_a) e(S_2, u' \prod_{j=1}^{k} u_j^{m_j}) e(A, g^{x_b}) e(h^{at}, g)$$

$$= e(S_3, u' \prod_{i=1}^{k} u_i^{w_i}) e(A, pk_a) e(S_2, u' \prod_{j=1}^{k} u_j^{m_j}) e(A, v_{i^*}) e(A, h^t)$$

$$= e(S_2, u' \prod_{j=1}^{k} u_j^{m_j})\, e(A, B_0 C) e(A, pk_a) e(S_3, u' \prod_{i=1}^{k} u_i^{w_i})$$

V. A BRIEF DISCUSSION ON SECURITY ANALYSIS

We will analyze the security of our anonymous proxy signature scheme in this section. Since the proposed scheme is warrant based, some properties such as distinguishability (distinguishable from normal signatures), verifiability and nondeniability can be achieved naturally. Therefore, we mainly

give a brief discussion on the unforgeability and anonymity of our scheme.

A. *Anonymity*

In our anonymous proxy signature scheme, the proxies sign as ring members and we use the ring signature scheme given by H. Shacham and B. Waters [22], which is anonymous against full key exposure. Therefore the anonymity of our anonymous proxy signature scheme can be shown by the similar method as [22].

B. *Unforgeability*

It means that any entity, including the original signer, other than the proxy signers themselves cannot generate a valid anonymous proxy signature. In the delegation generating part of our scheme, we use the proxy signature scheme given by Ying Sun, Chunxiang Xu, Yong Yu and Yi Mu [21], which is strongly unforgeable against type2 and type3 adversaries under the adaptive chosen message attack in the standard model. In the signing algorithm part of our scheme, we use for proxies signing the ring signature scheme given by H. Shacham and B. Waters [22], which is unforgeable with respect to insider corruption. Therefore the unforgeability of our anonymous proxy signature scheme can be shown by the similar method as [21, 22].

VI. CONCLUSIONS

In order to protect the proxy signer's privacy, we proposed the first anonymous proxy signature scheme without random oracles. The signature in our scheme is of size $2l + 3$ group elements for l members in a ring. Proposing an anonymous proxy signature scheme, which is independent of l, is an open problem.

As a future work, we will focus on security analysis of our anonymous proxy signature scheme to show that the proposal is the first provable secure anonymous proxy signature scheme in the standard models.

REFERENCES

[1] M.Mambo, K.Usuda, E.Okamoto,"Proxy signatures for delegating signing operation," 3rd ACM Conference on Computer and Communications Security (CCS'96), pp. 48-57, 1996.

[2] M.Mambo, K.Usuda, and E.Okamoto, "Proxy signature: Delegation of the power to sign messages,"IEICE Transactions on Fundamentals, vol. E79-A,no. 9, pp. 1338-1353, 1996.

[3] C.Ma and J.Ao, "Group-based proxy re-encryption scheme secure against chosen ciphertext attack," International Journal of Network Security, vol. 8, no.3, pp. 266-270, 2009.

[4] K. Zhang,"Threshold proxy signature schemes," Proceedings of the First International Workshop on Information Security, pp. 282-290, 1997.

[5] W. D. Lin, J. K. Jan, "A security personal learning tools using a proxy blind signature scheme," Proceedings of International Conference on Chinese Language Computing, pp.273-277, Illinois, USA, July 2000.

[6] G. K. Verma, "A proxy blind signature scheme over braid groups," International Journal of Network Security, vol. 9, no. 3, pp. 214-217, 2009.

[7] A. K. Awasthil, S. Lal, "ID-based ring signature and proxy ring signature schemes from bilinear pairings," International Journal of Network Security, vol. 4, no.2, pp. 187-192, Mar. 2007.

[8] J. Li, T. H. Yuen, X. F. Chen, et al, "Proxy ring signature: Formal definitions, efficient construction and new variant," Proceedings of International Conference of Computational Intelligence and Security (CIS'06), vol. 2, pp. 1259-1264, 2006.

[9] D.Boneh, E.-J. Goh, K. Nissim, "Evaluating 2-DNF formulas on ciphertexts," In J. Kilian,editor, Proceedings of TCC 2005, number 3378 in LNCS, pages 325-41. Springer-Verlag, Feb.2005.

[10] R. Rivest, A. Shamir, Y. Tauman, "How to leak a secret," AsiaCrypt'01, LNCS 2248, pp. 552-565,Springer-Verlag, 2001.

[11] D. Chaum, E. Hevst, "Group signature," EUROCRYPT 1991, LNCS 547, pp. 257-265, Springer-Verlag, 1991.

[12] R. Rivest, A. Shamir, Y. Tauman, "How to leak a secret: Theory and applications of ring signatures," Essays in Theoretical Computer Science: in Memory of Shimon Even, LNCS 3895, pp. 164-186, Springer-Verlag, 2006.

[13] A. K. Awasthil, S. Lal, "A new proxy ring signature scheme," Proceeding of RMS 2004, Agra, INDIA, 2004.

[14] H. Xiong, Z. Qin, F. Li, "A Certificateless Proxy Ring Signature Schemewith Provable Security" International Journal of Network Security, Vol.12, No.2, PP.92-106, Mar. 2011 .

[15] Y. Yu, C. Xu, X. Huang,Y. Mu, "An efficient anonymous proxy signature scheme with provable security" ,Computer Standards & Interfaces 31 (2009) 348–353 .

[16] E. Bresson, J. Stern, M. Szydlo, "Threshold ring signatures and applications to ad-hoc groups," In CRYPTO 2002,Proceedings, volume 2442 of Lecture Notes in Computer Science, pages 465–480. Springer, 2002.

[17] S. Chow, S. Yiu, L. Hui, "Efficient identity based ring signature," In ACNS 2005, Proceedings, volume 3531 of Lecture Notes in Computer Science. Springer, 2005.

[18] J. Li , Y. Wang, "Universal designated verifier ring signature (proof) without random oracles," In Emerging Directions in Embedded and Ubiquitous Computing 2006, Proceedings, volume 4097 of Lecture Notes in Computer Science, pages 332–341. Springer, 2006.

[19] W. Baodian, Z. Fangguo, C. Xiaofeng, "Ring Proxy Signatures,"Journal of Electronics(China), Vol.25 No.1, January 2008.

[20] F. Zhang, R. Safavi-Naini, C. Lin, "New Proxy Signature, Proxy Blind Signature and Proxy Ring Signature Schemes from Bilinear Pairings", IACR Cryptology ePrint Archive 2003: 104 (2003)

[21] Y. Sun, C. Xu, Y. Yu, Y. Mu, "Strongly unforgeable proxy signature scheme secure in the standard model" ,The Journal of Systems and Software 84 (2011) 1471–1479 .

[22] H. Shacham and B. Waters, "Efficient Ring Signatures Without Random Oracles." In T. Okamoto and X. Wang, eds., *Proceedings of PKC 2007*, vol. 4450 of LNCS, pages 166–80. Springer-Verlag, Apr. 2007.

[23] X. Boyen, B. Waters, "Compact group signatures without random oracles," In S. Vaudenay, editor, Proceedings of Eurocrypt 2006, volume 4004 of LNCS, pages 427-44. Springer-Verlag,May 2006.