Security Pitfalls of a Provably Secure Identity-based Multi-Proxy Signature Scheme

Maryam Rajabzadeh Asaar[1], Mahmoud Salmasizadeh[2], and Willy Susilo[3]

[1] Department of Electrical Engineering,
[2] Electronics Research Institute (Center),
Sharif University of Technology, Tehran, Iran.
[3] Centre for Computer and Information Security Research,
University of Wollongong, Australia.
asaar@ee.sharif.ir, salmasi@sharif.edu, wsusilo@uow.edu.au

Abstract. An identity-based multi-proxy signature is a type of proxy signatures in which the delegation of signing right is distributed among a number of proxy signers. In this type of cryptographic primitive, cooperation of all proxy signers in the proxy group generates the proxy signatures of roughly the same size as that of standard proxy signatures on behalf of the original signer, which is more efficient than transmitting individual proxy signatures. Since identity-based multi-proxy signatures are useful in distributed systems, grid computing, presenting a provably secure identity-based multi-proxy scheme is desired.

In 2013, Sahu and Padhye proposed the first provably secure identity-based multi-proxy signature scheme in the random oracle model, and proved that their scheme is existential unforgeable against adaptive chosen message and identity attack. Unfortunately, in this paper, we show that their scheme is insecure. We present two forgery attacks on their scheme. Furthermore, their scheme is not resistant against proxy key exposure attack. As a consequence, there is no provably secure identity-based multi-proxy signature scheme secure against proxy key exposure attack to date.

Keywords:identity-based cryptography, forgery attack, multi-proxy signature, provable security.

1 Introduction

Proxy signatures. The notion of proxy signatures for the first time was introduced by Mambo et al. [17] in 1996. In a proxy signature scheme, an original signer, Alice, can delegate her signing right for signing messages to another signer, Bob, called the proxy signer. Since the notion of proxy signatures has been introduced, several variants of proxy signatures have been proposed. These include proxy signatures from RSA and integer factorization problem [25, 24, 39, 18, 15, 7], identity-based proxy signature schemes based on the bilinear pairings [3, 38, 33, 4, 12, 1, 35, 26], designated verifier proxy signatures [16, 36, 27], short proxy signatures [8], proxy verifiably encrypted signatures [37], proxy signature schemes without random oracles [9], multi-proxy signatures [10, 14, 32], proxy multi-signatures [14], multi-proxy multi-signatures

[11, 5], identity-based multi-proxy signatures [1, 13, 34, 21], identity-based proxy multi-signatures [13, 30, 2, 31, 28] and identity-based multi-proxy multi-signature schemes [13, 6, 19, 20, 29]. In this letter, we focus on identity-based multi-proxy signature schemes. In a multi-proxy signature scheme, an original signer can delegate her signing right for signing messages to a group of n-proxy signers, called the proxy agent, such that only cooperation of all proxy signers in the proxy group generates the proxy signatures of roughly the same size as that of standard proxy signatures on behalf of the original signer instead of transmitting n individual proxy signatures. This primitive can be used in a company when the boss of the company is on a business trip and some important documents have to be signed. Hence, the boss delegates her signing capability to every department manager of the company such that only all managers jointly can sign important documents on behalf of the boss. Various multi-proxy signatures [10, 14, 32] have been proposed till now. However, a verifier still needs the certified public keys of $n + 1$ signers in a multi-proxy signature to verify its validity. If these public keys and their certificates are transmitted with these signatures, it defeats the main purpose of a multi-proxy signature to save bandwidth. On the other hand, these kinds of schemes in their basic formats require extensive public-key infrastructure for practical use. In order to save bandwidth and provide more flexible management of public keys since the identity-based cryptography has been introduced by Shamir [23], several identity-based multi-proxy signature schemes [1, 13, 34, 21] have been proposed. In the proxy key exposure attack [22] proposed by Schuldt et al., it is assumed that temporal secret keys of proxy signers stored in a less trusted device can be leaked, while secure storage (for example in a TPM within a laptop) is available for long term secret keys of proxy signers. With this attack not only long term secret keys of proxy signers are compromised but also an adversary (with having proxy secret keys) can generate valid (identity-based) proxy signatures. Therefore, it is vital to consider the proxy key exposure attack when we present other extensions of proxy signatures, (identity-based) multi-proxy signatures.

In 2005, Li and Chen proposed the first identity-based multi-proxy signature scheme [13]. However, their scheme does not support provable security. In 2009, Cao and Cao presented the first provably secure identity-based multi-proxy signature scheme [1]. Unfortunately, their scheme is not secure against the Xiong et al.'s attack [34]. In 2013, Sahu and Padhye [21] proposed the first provably secure identity-based multi-proxy signature scheme in the random oracle model, and proved that the presented scheme is existential unforgeable against adaptive chosen message and identity attack.

Our Contributions

In this paper, we demonstrate that Sahu and Padhye's scheme is indeed insecure, by presenting two forgery attacks. Furthermore, we show that it is not secure against proxy key exposure attack. As a consequence, there is no provably secure identity-

based multi-proxy signature scheme with security against proxy key exposure attack to date.

Organization of the paper
The rest of this paper is organized as follows. Section 2 presents preliminaries employed as the signature foundation. Sahu and Padhye's scheme [21] is reviewed in Section 3. In Section 4, we demonstrate the insecurity of Sahu and Padhye's scheme. Finally, we conclude the paper in Section 5.

2 Preliminaries

In this section, we review some preliminaries on bilinear pairings that will be used throughout this paper.

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. Let a, 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: $e(aP, bQ) = e(P, Q)^{ab}$ for all $a, b \in Z^*{}_q$ and $P, Q \in G_1$.
2. non-degenerate: There exists $P, Q \in G_1$ such that $e(P, Q) \neq 1$
3. computable: There is an efficient algorithm to compute $e(P, Q)$ for all $P, Q \in G_1$.

3 Review of Sahu and Padhye's identity-based multi-proxy signature scheme [21]

In this section, we briefly review Sahu and Padhye's identity-based multi-proxy signature scheme [21], which is based on the identity-based multi-proxy signature scheme [13].

– Setup. Given a security parameter k, the PKG chooses two groups G_1 and G_2 of a prime order q, a generator P of G_1, a bilinear map $e : G_1 \times G_1 \rightarrow G_2$ and hash functions $H_1 : \{0,1\}^* \rightarrow G_1$, $H_2 : \{0,1\}^* \rightarrow Z_q^*$ and $H_3 : \{0,1\}^* \times \{0,1\}^* \rightarrow Z_q^*$. It chooses a master-key $s \in_R Z_q^*$, and computes $P_{pub} = sP$. The PKG publishes system's public parameters $\{k, G_1, G_2, q, P, e, H_1, H_2, H_3, P_{pub}\}$, and keeps the master-key s secret.

– Extraction. Given an identity ID, the PKG computes its public key as $Q_{ID} = H_1(ID)$ and its corresponding secret key as $S_{ID} = sQ_{ID}$. Thus, the original signer A has Q_{ID_A} and S_{ID_A} as its public and secret key, respectively. Similarly, public and secret keys of n proxy signers are $Q_{ID_{B_i}}$ and $S_{ID_{B_i}}$, $1 \leq i \leq n$, respectively.

– Proxy key generation. This phase consists of delegation generation, delegation verification and proxy key generation which are described as follows.
  1. Delegation generation: To delegate the signing capability to a group of proxy signers, the original signer A chooses $t \in_R Z_q^*$, computes $V = tP$, $h = H_2(\omega)$ and $W = hS_{ID_A} + tP_{pub}$, and broadcasts (W, V, ω) through a secure channel to the proxy signers, where the warrant ω specifies the delegation period, what kind of messages is delegated, the identity information of the original signer and the proxy signers.
  2. Delegation verification: Each proxy signer B_i accept the delegation (W, V, ω) if the relation $e(W, P) = e(hQ_{ID_A} + V, P_{pub})$ holds. Otherwise, terminates the protocol.
  3. Proxy key generation: Each proxy signer B_i computes its proxy signing key as $S_{pk_i} = W + hS_{ID_{B_i}}$ with having a valid delegation (W, V, ω).

– Multi-proxy signature generation. To generate a multi-proxy signature on a message m that conforms to the warrant ω, one proxy signer in the proxy group is designated as a clerk, whose task is to combine partial proxy signatures to generate the final multi-proxy signature. The process of multi-proxy signature generation is as follows.
  1. For $1 \leq i \leq n$, the proxy signer B_i chooses $x_i \in_R Z_q^*$, computes $U_{B_i} = x_iP$, and broadcasts its U_{B_i} to the clerk.
  2. For $1 \leq i \leq n$, the proxy signer B_i computes $h' = H_3(m, \omega)$ and $\sigma_{B_i} = h'S_{pk_i} + x_iP_{pub}$, and broadcasts σ_{B_i} to the clerk as its partial proxy signature on the message m.
  3. The clerk first computes the public value $Q_{pk_i} = h(Q_{ID_A} + Q_{ID_{B_i}}) + V$, then, verifies if $e(\sigma_{B_i}, P) = e(h'Q_{pk_i} + U_{B_i}, P_{pub})$ holds for $1 \leq i \leq n$. If so, it computes the identity-based multi-proxy signature on the message m as $(\sigma_B, V, U_B, \omega)$, where $U_B = \sum_{i=1}^{n} U_{B_i}$ and $\sigma_B = \sum_{i=1}^{n} \sigma_{B_i}$.

– Multi-proxy signature verification. Given the identity-based multi-proxy signature $(\sigma_B, V, U_B, \omega)$ on a message m, a verifier operates as follows.
  1. Checks whether or not the message m conforms to the warrant ω. If not, stop. Otherwise, continue.
  2. Checks if proxy signers are authorized by the original signer A in the warrant ω. If not, stop. Otherwise, continue.
  3. Computes $h = H_2(\omega)$, $h' = H_3(m, \omega)$ and $Q_{pk} = \sum_{i=1}^{n} Q_{pk_i} = h[nQ_{ID_A} + \sum_{i=1}^{n} Q_{ID_{B_i}}] + nV$, and accepts the signature if $e(\sigma_B, P) = e(h'Q_{pk} + U_B, P_{pub})$ hold.

4 Cryptanalysis of Sahu and Padhye's identity-based multi-proxy signature scheme

In this section, by presenting two forgery attacks, we show that Sahu and Padhye's identity-based multi-proxy signature scheme [21] is insecure, despite the fact that they provided its security proof. In the first attack, we show that malicious proxy signers with having a valid delegation can forge valid delegations for arbitrary warrants as many as they want, and consequently generate valid multi-proxy signatures. Hence, this attack shows that malicious proxy signers can forge identity-based multi-proxy signatures for messages and warrants that the original signer has not delegated for them. In the second attack, we show that an original signer or everyone with having a valid identity-based multi-proxy signature can forge valid multi-proxy signatures for new messages in the warrant. In addition, we show that it is not secure against proxy key exposure attack [22]. In presented attacks, we use the fact that Z_q^* is a group which means that for each $h, \widetilde{h} \in Z_q^*$, $h^{-1}.\ \widetilde{h} \bmod q \in Z_q^*$.

4.1 The first forgery attack

Assume that an adversary (one of the proxy signers) has obtained a valid delegation (W, V, ω). Then, the adversary can forge valid delegations on arbitrary warrants as follows. First, they choose a new warrant $\widetilde{\omega}$, computes $h = H_2(\omega)$, $\widetilde{h} = H_2(\widetilde{\omega})$, $\widetilde{W} = \frac{\widetilde{h}}{h}W$ and $\widetilde{V} = \frac{\widetilde{h}}{h}V$. Hence, the forged delegation is $(\widetilde{W}, \widetilde{V}, \widetilde{\omega})$.
Now, we need to show that $(\widetilde{W}, \widetilde{V}, \widetilde{\omega})$ is a valid delegation. To do so, it is necessary to show that $e(\widetilde{W}, P) = e(\widetilde{h}Q_{ID_A} + \widetilde{V}, P_{pub})$. Since we have

$$e(\widetilde{W}, P) = e(\frac{\widetilde{h}}{h}W, P) = e(\frac{\widetilde{h}}{h}(hS_{ID_A} + tP_{pub}), P) =$$

$$e(\widetilde{h}S_{ID_A} + t\frac{\widetilde{h}}{h}P_{pub}, P) = e(\widetilde{h}Q_{ID_A} + \frac{\widetilde{h}}{h}V, sP) =$$

$$e(\widetilde{h}Q_{ID_A} + \widetilde{V}, P_{pub}),$$

the forged delegation is valid.

Hence, proxy signers can generate valid identity-based multi-proxy signatures following the real protocol.

4.2 The second forgery attack

Everyone who has obtained a valid identity-based multi-proxy signature $(\sigma_B, V, U_B, \omega)$ on a message m can forge valid identity-based multi-proxy signatures on arbitrary

messages in the warrant ω. To forge an identity-based multi-proxy signatures, first an adversary chooses a message $\widetilde{m}$ in the warrant ω, computes $h' = H_3(m, \omega)$, $\widetilde{h'} = H_3(\widetilde{m}, \omega)$, $\widetilde{\sigma_B} = \frac{\widetilde{h'}}{h'}\sigma_B$ and $\widetilde{U_B} = \frac{\widetilde{h'}}{h'}U_B$. Therefore, the forged identity-based multi-proxy signature is $(\widetilde{\sigma_B}, V, \widetilde{U_B}, \omega)$ on the message $\widetilde{m}$. Now, we need to show that the forged signature is a valid identity-based multi-proxy signature. To do so, it is necessary to show that $e(\widetilde{\sigma_B}, P) = e(\widetilde{h'}Q_{pk} + \widetilde{U_B}, P_{pub})$. Since we have

$$e(\widetilde{\sigma_B}, P) = e(\frac{\widetilde{h'}}{h'}\sigma_B, P) =$$

$$e(\frac{\widetilde{h'}}{h'}(\sum_{i=1}^{n}\sigma_{B_i}), P) = e(\frac{\widetilde{h'}}{h'}\sum_{i=1}^{n}(h'S_{pk_i} + x_iP_{pub}), P) =$$

$$e(\sum_{i=1}^{n}(\frac{\widetilde{h'}}{h'}h'S_{pk_i} + x_i\frac{\widetilde{h'}}{h'}P_{pub}), P) = e(\sum_{i=1}^{n}(\widetilde{h'}S_{pk_i} + x_i\frac{\widetilde{h'}}{h'}P_{pub}), P)$$

$$e(\sum_{i=1}^{n}(\widetilde{h'}Q_{pk_i} + x_i\frac{\widetilde{h'}}{h'}P), sP) = e(\widetilde{h'}\sum_{i=1}^{n}Q_{pk_i} + \frac{\widetilde{h'}}{h'}\sum_{i=1}^{n}U_{B_i}, P_{pub})$$

$$e(\widetilde{h'}Q_{pk} + \frac{\widetilde{h'}}{h'}U_B, P_{pub}) = e(\widetilde{h'}Q_{pk} + \widetilde{U_B}, P_{pub}),$$

the forged signature is valid.

As a consequence, the adversary can forge a valid identity-based multi-proxy signature on a new message in the warrant with having a valid signature.

Remark 1. Sahu and Padhye's identity-based multi-proxy signature scheme [21] is also not secure against proxy key exposure attack [22] since if S_{pk_i} of each proxy signer B_i is leaked, other proxy signers with having delegations (W, V, ω) can extract long-term secret key of that proxy signer through computing $S_{ID_{B_i}} = h^{-1}(S_{pk_i} - W)$, where $h = H_2(\omega)$.

5 Conclusion

In 2013, Sahu and Padhye proposed the first provably secure identity-based multi-proxy signature scheme in the random oracle model, and proved that their scheme is existential unforgeable against adaptive chosen message and identity attack. Unfortunately, we have demonstrated that their scheme is indeed insecure by presenting two forgery attacks, and also it is insecure against proxy key exposure attack. Therefore, there is no provably secure identity-based multi-proxy signature with security against proxy key exposure attack, which leads to an open research problem in this area of research.

References

1. F. Cao and Z. Cao. A secure identity-based multi-proxy signature scheme. *Computers & Electrical Engineering*, 35(1):86–95, 2009.
2. F. Cao and Z. Cao. A secure identity-based proxy multi-signature scheme. *Information Sciences*, 179(3):292–302, 2009.
3. C. Gu and Y. Zhu. Provable security of ID-based proxy signature schemes. In *Proc. of the 3rd Int. Conf. on Networking and Mobile Computing (ICCNMC 2005)*, pages 1277–1286, Zhangjiajie, China, 2-4 August 2005. Springer-Verlag, Berlin.
4. C. Gu and Y. Zhu. An efficient ID-based proxy signature scheme from pairings. In *Proc. of 3rd SKLOIS Conf. on Information Security and Cryptology (Inscrypt 2007)*, pages 40–50, Xining, China, 31 August- 5 September 2008. Springer-Verlag, Berlin.
5. L. Guo and G. Wang. Insider attacks on multi-proxy multi-signature schemes. *Computers & Electrical Engineering*, 33(2):88–93, 2007.
6. S. Guo, Z. Cao, and R. Lu. An efficient ID-based multi-proxy multi-signature scheme. In *Proc. of the 1st Int. Multi-Symp. on Computer and Computational Sciences (IMSCCS 2006)*, pages 81–88, Hangzhou, China, 20-24 June 2006. IEEE Xplore, NY.
7. X. Hu, H. Xu, and T. Si. Analysis and improvement of proxy-protected signature secure against the undelegated proxy signature attack. *Computational Information Systems*, 6(9):2997–3002, 2010.
8. X. Huang, Y. Mu, W. Susilo, F. Zhang, and X. Chen. A short proxy signature scheme: efficient authentication in the ubiquitous world. In *Proc. of Embedded and Ubiquitous Computing–EUC 2005 Workshops*, pages 480–489, Nagasaki, Japan, 6-9 December 2005. Springer-Verlag, Berlin.
9. X. Huang, W. Susilo, Y. Mu, and W. Wu. Proxy signature without random oracles. In *Proc. of 2nd Int. Conf. on Mobile Ad-hoc and Sensor Networks (MSN 2006)*, pages 473–484, Hong Kong, China, 13-15 December 2006. Springer-Verlag, Berlin.
10. S. Hwang and C. Shi. A simple multi-proxy signature scheme for electronic commerce. In *Proc. of the 10th National Conf. on Information Security*, pages 57–67, Hualien, Taiwan, China, 15-18 March 2000. Springer-Verlag, Berlin.
11. S.-J. Hwang and C.-C. Chen. New multi-proxy multi-signature schemes. *Applied Mathematics and Computation*, 147(1):57–67, 2004.
12. H. Ji, Y. Wang, W. Han, and L. Zhao. An identity-based proxy signature from bilinear pairings. In *WASE Int. Conf. on Information Engineering (ICIE 2009)*, pages 14–17, Taiyuan, Shanxi, 10-11 July 2009. IEEE Xplore, NY.
13. X. Li and K. Chen. ID-based multi-proxy signature, proxy multi-signature and multi-proxy multi-signature schemes from bilinear pairings. *Applied Mathematics and Computation*, 169(1):437–450, 2005.
14. X. Li, K. Chen, and S. Li. Multi-proxy signature and proxy multi-signature schemes from bilinear pairings. In *Proc. of 5th Int. Conf. on Parallel and Distributed Computing: Applications and Technologies (PDCAT 2005)*, pages 61–62, Singapore, Singapore, 8-10 December 2005. Springer-Verlag, Berlin.
15. Y.-C. Liu, H.-A. Wen, C.-L. Lin, and T. Hwang. Proxy-protected signature secure against the undelegated proxy signature attack. *Computers & Electrical Engineering*, 33(3):177–185, 2007.
16. R. Lu and Z. Cao. Designated verifier proxy signature scheme with message recovery. *Applied Mathematics and Computation*, 169(2):1237–1246, 2005.
17. M. Mambo, K. Usuda, and E. Okamoto. Proxy signatures: Delegation of the power to sign messages. *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, 79(9):1338–1354, 1996.
18. J. H. Park, B. G. Kang, and J. W. Han. Cryptanalysis of Zhou et al.'s proxy-protected signature schemes. *Applied Mathematics and Computation*, 169(1):192–197, 2005.

19. R. Sahu and S. Padhye. An ID-based multi-proxy multi-signature scheme. In *Proc. of Int. Conf. on Computer and Communication Technology (ICCCT 2010)*, pages 60–63, Allahabad, Uttar Pradesh, 17-19 September 2010. IEEE Xplore, NY.
20. R. A. Sahu and S. Padhye. Efficient ID-based multi-proxy multi-signature scheme based on CDHP. *Journal of Applied Mathemtics and Informatics*, 5(4):275–282, 2011.
21. R. A. Sahu and S. Padhye. Provable secure identity-based multi-proxy signature scheme. *International Journal of Communication Systems*, 10(9):1–16, 2013.
22. J.C.N. Schuldt, K. Matsuura, and K.G. Paterson. Proxy signatures secure against proxy key exposure. In *Proc. of 11th Int. Workshop on Practice and Theory in Public-Key Cryptography (PKC 2008)*, pages 141–161, Barcelona, Spain, 9-12 March 2008. Springer Berlin Heidelberg.
23. A. Shamir. Identity-based cryptosystems and signature schemes. In *Proc. of 4th Annual Int. Cryptology Conf. on Advances in Cryptology-CRYPTO 1984*, pages 47–53, Santa Barbara, CA, USA, 19-22 August 1985. Springer-Verlag, Berlin.
24. Z. Shao. Proxy signature schemes based on factoring. *Information Processing Letters*, 85(3):137–143, 2003.
25. Z. Shao. Provably secure proxy-protected signature schemes based on RSA. *Computers & Electrical Engineering*, 35(3):497–505, 2009.
26. K. Shim. An identity-based proxy signature scheme from pairings. In *Proc. of 8th Int. Conf. on Information and Communications Security (ICICS 2006)*, pages 60–71, Raleigh, NC, USA, 4-7 December 2006. Springer-Verlag, Berlin.
27. K.-A. Shim. Short designated verifier proxy signatures. *Computers & Electrical Engineering*, 37(2):180–186, 2011.
28. N. Tiwari and S. Padhye. An ID-based proxy multi signature scheme without bilinear pairings. In *Proc. of the First Int. Conf. on Security Aspects in Information Technology (InfoSecHiComNet 2011)*, pages 83–92, Haldia, India, 19-22 October 2011. Springer-Verlag, Berlin.
29. N. Tiwari, S. Padhye, and D. He. Efficient ID-based multiproxy multisignature without bilinear maps in ROM. *Annals of Telecommunications - Annales des tlcommunications*, 68(3-4):231–237, 2013.
30. Q. Wang and Z. Cao. Identity based proxy multi-signature. *Journal of Systems and Software*, 80(7):1023–1029, 2007.
31. Q. Wang and Z. Cao. Improvement of identity-based proxy multi-signature scheme. *Journal of Systems and Software*, 82(5):794–800, 2009.
32. Q. Wang, Z. Cao, and S. Wang. Formalized security model of multi-proxy signature schemes. In *Proc. of the 5th Int. Conf. on Computer and Information Technology (CIT 2005)*, pages 668–672, Shanghai, China, 21-23 September 2005. IEEE Xplore, NY.
33. W. Wu, Y. Mu, W. Susilo, J. Seberry, and X. Huang. Identity-based proxy signature from pairings. In *Proc. of the 4th Int. Conf. on Autonomic and Trusted Computing*, pages 22–31, Hong Kong, China, 11-13 July 2007. Springer-Verlag, Berlin.
34. H. Xiong, J. Hu, Z. Chen, and F. Li. On the security of an identity based multi-proxy signature scheme. *Computers & Electrical Engineering*, 37(2):129–135, 2011.
35. J. Xu, Z. Zhang, and D. Feng. ID-based proxy signature using bilinear pairings. In *Proc. of Parallel and Distributed Processing and Applications-ISPA 2005 Workshops*, pages 359–367, Nanjing, China, 2-5 November 2005. Springer-Verlag, Berlin.
36. Y. Yu, C. Xu, X. Zhang, and Y. Liao. Designated verifier proxy signature scheme without random oracles. *Computers & Mathematics with Applications*, 57(8):1352–1364, 2009.
37. J. Zhang, C. Liu, and Y. Yang. An efficient secure proxy verifiably encrypted signature scheme. *Journal of Network and Computer Applications*, 33(1):29–34, 2010.
38. J. Zhang and W. Zou. Another ID-based proxy signature scheme and its extension. *Wuhan University Journal of Natural Sciences*, 12(1):33–36, 2007.

39. Y. Zhou, Z. Cao, and R. Lu. Provably secure proxy-protected signature schemes based on factoring. *Applied Mathematics and Computation*, 164(1):83–98, 2005.