Cryptanalysis of an Efficient Deniable Authentication Protocol Based on Generalized ElGamal Signature Scheme

Chi-Yu Liu[1], Cheng-Chi Lee[2], Tzu-Chun Lin[3]
(Corresponding author: C. C. Lee)

Department of Library and Information Science, Fu Jen Catholic University[2]
510 Jhongjheng Road, Taipei 24205, Taiwan, R.O.C. (Email: cclee@blue.lins.fju.edu.tw)
Department of Applied Mathematics, Feng Chia University[3]
100 Wenhwa Rd, Seatwen, Taichung, Taiwan, R.O.C.
Graduate Institute of Networking and Communication Engineering, Chaoyang University of Technology[1]
168 Gifeng E. Rd., Wufeng Taichung County, Taiwan, R.O.C.
(Received Jan. 12, 2010; revised and accepted Mar. 9, 2010)

Abstract

In 1998, Dwork et al. first proposed an application of zero-knowledge, deniable authentication protocol. Thereafter, there were many researches about the deniable authentication schemes. In 2004, Shao demonstrated out that the previous schemes had a common weakness in which any third party can impersonate the intended receiver to verify the signature of the given message, and they proposed a new scheme based on ElGamal signature scheme. Although Shao claimed that his scheme could provide complete security and properties of a deniable authentication scheme, we will point out that Shao's scheme is unable to achieve the second requirement of the deniable authentication scheme.

Keywords: Deniable authentication, e-cash, impersonation attack, security

1 Introduction

In the cryptographic research, the property of non-deniable is imperative for a secret algorithm. It can provide protection for both the right of the sender and the receiver [8, 16, 17]. However, some situations may require the sender to deniable his signature of a given message.

In 1998, Dwork et al. [6] first proposed an application of zero-knowledge, deniable authentication protocol. Afterward, Aumann and Rabin [1, 2] proposed another scheme based on factoring. Although Dwork et al. provided a new application, but Deng et al. [4] showed their scheme has timing restriction. In addition, Deng et al. also introduced the importance of deniable authentication scheme with two applications about deniable authentication schemes: *(1) A coerced electronic voting system*, and *(2) Secure negotiations over the Internet*, and developed two deniable authentication protocols.

Both Deng et al.'s and Aumann et al.'s schemes showed that they require a public directory which there is a trust between the sender and the receiver by Fan et al. [7] in 2002. Fan et al. proposed a simple scheme based on Diffie-Hellman [5]. The scheme can provide opposites man-in-the-middle attacks with the public key cryptosystem. However, Shao [12] claimed that there is a common drawback of the previous deniable authentication schemes that any third party can impersonate the intended receiver to verify the signature of the given message.

According to the above description, a completed deniable authentication encryption scheme should provide two requirements [3, 9, 10, 11, 14, 15, 18]:

1) The signature of a given message should been verified only by an intended receiver.

2) The intended receiver can not prove the source of the given message to any third party, even if he/she fully-cooperates with the third party.

Although Shao claimed that his scheme could provide complete security and properties of a deniable authentication scheme, we will point out that Shao's scheme is unable to achieve the second requirement of the deniable authentication scheme. The remainder of this article is organized as follows. In Section 2, we will briefly review Shao's scheme, and then propose our cryptanalysis for Shao's scheme in Section 3. In Section 4, we made a conclusion of this article.

2 Review of Shao's Scheme

In Shao's protocol which is based on ElGamal signature scheme, the authors claimed that their scheme has no weakness in that a third party can verify the identity of the sender. They showed that the disadvantages of Deng et al.'s and Fan et al.'s deniable authentication schemes, and then proposed an improvement scheme which is shown later.

For convenience sake, we pre-defined some public parameters which are used in Fan et al.'s scheme. First, p and q are two large prime numbers, where the length of p is 1024 $\sim$ 2048 bits, and q is 160 bits, and g is a generator of order $q \in GF(p)$. We denote a collision-free hash function to $H(\cdot)$ such as SHA-1. Then, each should select his/her own private key x in $GF(q)$, and calculates his/her public key by computing $y = g^x \bmod p$ [13].

Now, there are two participants, a sender S, and a receiver R in their proposed scheme. If sender S wants to transmit a message M to R, he/she can perform the procedure as follows. First, S should select a random number $k \in_R Z_p$, and then computes $r_1 = y_R^k \bmod p$, and $r_2 = H(r_1)$. Next, she/he obtains $MAC = H(r_1 \parallel M)$, and $s = k - x_s r_2 \bmod q$, where "$\parallel$" denotes a concatenate operator.

After receiving the signature (r_2, s, MAC) of the given message M from S, R obtains r_1 with his/her private key x_R by computing $r_1 = (g^s y_s^{r_2})^{x_R} \bmod p$. Then R can verify the message M by the following equations: $r_2 \stackrel{?}{=} H(r_1)$ and $MAC \stackrel{?}{=} H(r_1 \parallel M)$.

3 Cryptanalysis of Shao's Scheme

In Shao's scheme, there is a drawback which does not satisfy the second requirement of a deniable authentication scheme. In Deng et al.'s paper, in the second application, there is a point that should be paid close attention to and that is *"Note that R should be sure that this offer M really comes from S, but it should be unclear for a third party whether M comes from S or is created by R itself, even if R and the third party cooperated fully."*, where S is a customer, R is a merchant, and M is a price offer. The details about the application and description can be referred to [4].

We provided an example to explain the situation why the receiver is willing to cooperate fully with a third party. In the first application of a deniable authentication scheme, if a third party wants to ensure that all coerced voters have selected predetermined candidates, he/she can pay a remuneration for the loss of the receiver which leaks his private key, and checks all results of the voters with the receiver's private key. For the receiver, he only reapplies for a new key pair to any certification authority.

According to the above example, we inspected Shao's scheme whether it can provide the precaution against a third party fully-cooperated with a third party or not. In the verification phase, the receiver can identity the source of the given message M by computing $r_1 = (g^s y_s^{r_2})^{x_R} \bmod p$, and executing $r_2 \stackrel{?}{=} H(r_1)$ with his/her private key x_R. If the receiver wants to cooperate fully with the third party, he/she can deliver his/her private key to the third party. After the third party obtains R's private key, he/she can ensure the source of the given message which comes from the sender S with the same verification equations as the receiver.

The focus of attention is that the verification equations imply the sender's public key. If a deniable authentication protocol can get rid of the public key in the verification equations, the protocol can go against the weakness of the full cooperation.

4 Conclusions

In this paper, we have proposed a cryptanalysis on Shao's scheme. If a receiver has fully-cooperated with a third party and wants to prove the source of the given message, he/she can provide his/her private key to the third party, and the third party can verify the sender's identity with $r_1 = (g^s y_s^{r_2})^{x_R} \bmod p$, and $r_2 \stackrel{?}{=} H(r_1)$. Therefore, Shao's scheme cannot achieve the second requirements of a deniable authentication scheme.

Acknowledgments

This research was partially supported by the National Science Council, Taiwan, R.O.C., under contract no.: NSC98-2221-E-468-002. The authors are grateful to the anonymous reviewers for valuable comments.

References

[1] Y. Aumann, and M. Rabin, "Authentication enhanced security and error correcting codes," *Lecture Notes In Computer Science, Proceedings of the 18th Annual International Cryptology Conference on Advances in Cryptology*, **1462**, pp. 299–303, 1998.

[2] Y. Aumann, and M. Rabin, " Efficient deniable authentication of long messages," *International Conference on Teoretical Computer Science in Honor of Professor Manuel Blum's 60th Birthday*, Hong Kong, China, Apr. 1998.

[3] Zhenfu Cao, "Universal encrypted deniable authentication protocol," *International Journal of Network Security*, vol. 8, no. 2, pp. 151–158, 2009.

[4] X. Deng, C. H. Lee and H. Zhu, " Deniable authentication protocols," *IEE Proceedings of Computers and Digital Techniques*, vol. 148, no. 2, pp. 101–104, 2001.

[5] W. Diffie, and M. E. Hellman, " New directions in cryptography," *IEEE Transactions on Information Theory*, vol. IT-22, no. 6, pp. 644–654, 1976.

[6] C. Dwork, M. Naor and A. Sahai, " Current zero-knowledge," *Proc. 30th ACM STOC's98*, pp. 409–418, Dallas, TX, USA.
[7] L. Fan, C. X. Xu and J. H. Li, " Deniable authentication protocol based on Diffie-Hellman algorithm," *Electronics Letters*, vol. 38, no. 14, pp. 705–706, 2002.
[8] M. S. Hwang, S. F. Tzeng and C. S. Tsai, " Generalization of proxy signature based on elliptic curves," *Computer Standards & Interfaces*, vol. 26, no. 2, pp. 73–84, 2004.
[9] Maged Hamada Ibrahim, "A method for obtaining deniable public-key encryption," *International Journal of Network Security*, vol. 8, no. 1, pp. 1–9, 2009.
[10] Maged Hamada Ibrahim, "Receiver-deniable public-key encryption," *International Journal of Network Security*, vol. 8, no. 2, pp. 159–165, 2009.
[11] Rongxing Lu and Zhenfu Cao, "Group Oriented Identity-based Deniable Authentication Protocol from the Bilinear Pairings," *International Journal of Network Security*, vol. 5, no. 3, pp. 283–287, 2007.
[12] Z. Shao, " Efficinet deniable authentication protocol based on generalized ElGamal signature scheme," *Computer Standards & Interfaces*, vol. 26, no. 5, pp. 449–454, 2004.
[13] Michal Sramka, "Cryptanalysis of the cryptosystem based on DLP $\gamma = \alpha^a \beta^b$," *International Journal of Network Security*, vol. 6, no. 1, pp. 80–81, 2008.
[14] Tony Thomas and Arbind Kumar Lal, "A zero-knowledge undeniable signature scheme in non-abelian group setting," *International Journal of Network Security*, vol. 6, no. 3, pp. 265–269, 2008.
[15] Haibo Tian, Xiaofeng Chen, and Yong Ding, "Analysis of two types deniable authentication protocols," *International Journal of Network Security*, vol. 9, no. 3, pp. 242–246, 2009.
[16] S. F. Tzeng, M. S. Hwang and C. Y. Yang, " An improvement of nonrepudiable threshold proxy signature scheme with known signers," *Computers & Security*, vol. 23, no. 2, pp. 174–178, 2004.
[17] S. F. Tzeng, C. Y. Yang and M. S. Hwang, " A new digital signature scheme based on factoring and discrete logarithms," *International Journal of Computer Mathematics*, vol. 81, no. 1, pp.9–14, 2004.
[18] Wei Zhao, "On the security of Yuan et al.'s undeniable signature scheme," *International Journal of Network Security*, vol. 11, no. 3, pp. 134–1379, 2010.

Chi-Yu Liu received the B.S. degree in Information Management from Chaoyang University of Technology (CYUT), Taichung, Taiwan, Republic of China, in 2003. She is currently pursuing her M.S. degree in Graduate Institute of Networking and Communication Engineering from CYUT. Her current research interests include applied cryptography and mobile communications.

Cheng-Chi Lee received the B.S. and M.S. in Information Management from Chaoyang University of Technology (CYUT), Taichung, Taiwan, in 1999 and in 2001. He researched in Computer and Information Science from National Chiao Tung University (NCTU), Taiwan, Republic of China, from 2001 to 2003. He received the Ph.D. in Computer Science from National Chung Hsing University (NCHU), Taiwan, in 2007. He was a Lecturer of Computer and Communication, Asia University, from 2004 to 2007. From 2007, he is an assistant professor of Photonics and Communication Engineering, Asia University. From 2009, he is an Editorial Board member of International Journal of Network Security and International Journal of Secure Digital Information Age. His current research interests include information security, cryptography, and mobile communications. Dr. Lee had published over 60+ articles on the above research fields in international journals.

Tzu-Chun Lin is an assistant professor in the Department of Applied Mathematics of Feng Chia University in Taiwan, R.O.C. She received her PhD in Mathematics from GLottingen University in Germany. Her current research interests include Invariant Theory of Finite Groups and Elliptic Curve Cryptography.