Cryptanalysis of a Non-interactive Deniable Authentication Protocol Based on Factoring

Razi Arshad and Nassar Ikram
(Corresponding author: Razi Arshad)

National University of Sciences and Technology, Sector H-10, Islamabad, Pakistan.
(Email: raziarshad@hotmail.com)
(Received Aug. 12, 2010; revised and accepted Oct. 4 & Dec. 17, 2010)

Abstract

A deniable authentication protocol allows a sender to transfer an authenticated message to a receiver in such a way that the receiver cannot prove to a third party about the source of the message. In recent years, many deniable authentication protocols have been proposed. In 2005, Lu et al. proposed a secure and non-interactive deniable authentication protocol based on factoring. Although Lu et al. claimed that their protocol could provide complete security and properties of a deniable authentication protocol, we will point out that Lu et al. protocol is unable to achieve the second requirement of being the deniable authentication protocol.

Keywords: Authentication, cryptography, deniable, security

1 Introduction

An authentication protocol allows a sender to send messages to a receiver through an insecure communication channel in such a way that the receiver can be convinced that the messages are indeed coming from the intended sender and the messages have not been modified by any adversary sitting in the middle of the communication channel. In short, the aim of this type of protocols is to establish an authenticated link from the sender to the receiver.

A deniable authentication protocol is an authentication protocol with an additional feature. This additional feature prevents the receiver, after receiving the message, from proving to a third party that the message has originated from a particular sender, even if he/she cooperates fully with the third party.

The deniable authentication protocol can be used in many specialized application. For example, secure negotiation over Internet [2] etc. Therefore, it has received great interests in practice.

In the past few years, researchers have done a lot of work in this field [3, 7, 9, 11, 14]. In 1998, Dwork et al. [5] proposed a notable deniable authentication protocol based on concurrent zero-knowledge proof. Aumann and Rabin [1, 2] proposed another deniable authentication protocol based on the factoring problem.

Deng *et al.* [4] showed that Dwork *et al.* protocol has timing restriction. Lately, Deng *et al.* also introduced the importance of deniable authentication protocol with the help of two applications, first one is "Freedom from Coercion in electronic voting system" and the second one is "Secure negotiations over the Internet", and developed two deniable authentication protocols.

Both Deng *et al.*'s and Aumann *et al.*'s protocols showed that they require a public directory trusted by the sender and the re-ceiver. To overcome the weakness of public directory, Fan et al. [6] proposed a sim-ple deniable authentication protocol based on the Diffie-Hellman protocol. However, there still exists a common weakness in all these protocols: all of them are interactive and less efficient. Therefore, Shao [13] has pro-posed an efficient non-interactive deniable authentication protocol based on generalized ElGamal signature scheme. Motivated from Shao protocol, Lu et al. [8, 10] proposed a new deniable authentication protocol based on factoring. Although Lu et al. claimed that their protocol is also non-interactive and sat-isfies the basic security requirements of deni-able authentication protocol. We will point out that Lu at al.'s protocol is unable to achieve the second requirement of being the deniable authentication protocol.

The subsequent paper is organized as fol-lows. Section 2 gives the review of the de-terminate Rabin cryptosystem and improved Rabin signature. Section 3 discusses Lu et al.'s protocol based on factoring. Section 4 covers our cryptanalysis for the Lu et al.'s protocol. Finally, we conclude the paper in Section 5.

2 Preliminaries

In this section, we briefly review the de-terminate Rabin cryptosystem and improved Rabin signature [8, 10].

2.1 Determinate Rabin Cryptosystem

Let n be the product of two large primes, the Rabin trapdoor function $f(x) \equiv x^2(\text{mod}n)$ is not a permutation but it is a 4-1 function. Therefore, the Rabin cryptosystem [12] has to add a con-straint to identify the uniquely right plaintext. Here, we will briefly review such a determi-nate Rabin cryptosystem. Select two large primes p, q and compute $n = p * q$, where $p \equiv q \equiv 3(\text{mod}4)$. Then, the private key is and the corresponding public key is n.

- **Encryption Algorithm**
  Suppose that plaintext $m \in Z_n^*$.The follow-ing steps will be carried out to perform en-cryption.

  1) Compute the first constraint parameter a_1, where
  $$a_1 = \begin{cases} 0, & \text{if } m < \frac{n}{2} \\ 1, & \text{if } m > \frac{n}{2}. \end{cases}$$
  2) Compute the second constraint parameter a_2, where
  $$a_2 = \begin{cases} 0, & \text{if } \frac{m}{n} = 1 \\ 1, & \text{if } \frac{m}{n} = -1. \end{cases}$$
  3) Compute $c = m^2(\text{mod}n)$, then the cipher-text is (c, a_1, a_2).

- **Decryption Algorithm**
  According to the private key (p, q), four roots $\{x_1, x_2, x_3, x_4\}$ that satisfy can be derived. Then, from the constraint parameters a_1, a_2, the right plaintext m can be immediately determined.

2.2 Improved Rabin Signature

Let p and q be the two large primes, satisfying $p \equiv q \equiv 3(\text{mod}4)$. Compute $n = p * q$ and select a parameter satisfying Jacobi symbol $(\frac{a}{n} = -1)$. Then, the private key is (p, q) and the corresponding public key is (p, q). In addition, a one-way hash functions $H : \{0, 1\}^* \rightarrow Z_n^*$ is also published.

- **Signing Algorithm**
  Suppose that a message $m \in \{0, 1\}^*$ should be signed. The signer will perform the following steps for signing operation.

  1) Compute the first parameter b_1, where
  $$b_1 = \begin{cases} 0, & \text{if } \frac{H(m)}{n} = 1 \\ 1, & \text{if } \frac{H(m)}{n} = -1. \end{cases}$$
  2) Compute $t = b^{b_1}$ and the second parameter b_2, where
  $$b_2 = \begin{cases} 0, & \text{if } (\frac{t}{p}) = (\frac{t}{p}) = 1 \\ 1, & \text{if } (\frac{t}{p}) = (\frac{t}{p}) = -1. \end{cases}$$
  3) Compute $u = (-1)^{b_2} a^{b_1}$ and s, where $s^2 \equiv$ $(\text{mod}n)$.

  In this way, the signature on the message m is (s, b_1, b_2).

- **Verifying Algorithm**
  Any verifier can verify the signature by using the following equation
  $$s^2 \equiv (-1)^{b_2} a^{b_1} H(m)(\text{mod}n).$$
  If it holds, the signature will be accepted, otherwise rejected.

3 Review of Lu *et al.*'s Protocol

In this section, we will review the Lu *et al.*'s protocol based on factoring. In Lu *et al.* protocol, there are two participants, a sender S and a receiver R respectively. Given a security parameter k, sender S chooses two large prime p_s and q_s as his/her private key, where $|p_S| = |q_S| = k$ and $p_S \equiv q_S \equiv 3(\text{mod}4)$. Then he/she computes $n_S = p_S * q_S$ as his/her public key. Moreover, he/she also publishes another random number a, such that $\frac{a}{n_S} = -1$.

Receiver R also chooses two large prime p_R and q_R such that $|p_R| = |q_R| = k$ and $p_S \equiv q_S \equiv 3(\text{mod}4)$ and computes $n_R = p_R * q_R$. Then, he/she keeps (p_R, q_R) as his/her private key and publish n_R as the corresponding public key. Furthermore, three secure one-way hash functions $H_S : \{0, 1\}^* \rightarrow Z_{n_S}^*$, $H_R : \{0, 1\}^* \rightarrow Z_{n_R}^*$ and $H_c(\cdot)$ should be published. Here, note that both (n_S, a) and n_R should be certified by a trusted authority.

Suppose, sender S wants to send a deni-able authentication message m to receiver R, then he/she should run the following steps:

1) Choose a random number $r \in Z_{n_R}^*$ and compute $H_S(r)$.
2) Use the improved Rabin signature to compute (s, b_1, b_2), satisfying
$$s^2 \equiv (-1)^{b_2} a^{b_1} H_S(r)(\text{mod}n_S).$$
3) Use the determinate Rabin cryptosystem to compute (c, a_1, a_2), where
$$c \equiv (H_R(s)r)^2(\text{mod}n_R).$$
4) Compute $MAC = H_c(m, r)$;
5) Send $(s.b_1, b_2, c, a_1, a_2, MAC)$ together with m to receiver R.

After $receiving(s, b_1, b_2, c, a_1, a_2, MAC)$, receiver R uses his private key (p_R, q_Q) to verify it by the following steps:

1) Compute d from (c, a_1, a_2), where $d^2 \equiv c(\mathrm{mod} n_R)$;

2) Compute r by the following equation:

$$r \equiv \frac{d}{H_R(s)} = \frac{H_R(s).r}{H_R(s)}(\mathrm{mod} n_R).$$

3) Check whether

$$s^2 \stackrel{?}{=} (-1)^{b_2} a^{b_1} H_S(r)(\mathrm{mod} n_S).$$

and

$$MAC \stackrel{?}{=} H_c(m, r).$$

If they both hold, $(s, b_1, b_2, c, a_1, a_2, MAC)$ can be accepted, otherwise rejected.

4 Cryptanalysis of Lu *et al.*'s Protocol

In Lu et al.'s protocol, there is a drawback which does not satisfy the second requirement of a deniable authentication protocol that is, the specific receiver cannot prove the source of a given message to any third party. In the second application of Deng et al.'s paper, there is an important point 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 M is a price offer, R' is a merchant and S'' is a customer. For details about the application and description, [4] can be referred.

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 Deng *et al.*'s paper, if a third party wants to ensure that all coerced voters have selected predetermined candidates, he/she can pay remuneration for the loss of the receiver which leaks his private key, and checks all results of the voters with the receiver private key. For the receiver R, he only reapplies for a new key pair to trusted authority.

According to the above example, we inspected Lu *et al.*'s protocol whether it can provide the precaution against a third party fully-cooperated with a third party or not. Assume Alice and Bob are the sender and the receiver respectively. Alice wants to send a deniable message M to Bob. Alice chooses a random number and compute $H_S(r)$. Now, Alice uses improved Rabin signature to compute (s, b_1, b_2) and determinate Rabin cryptosystem to compute (c, a_1, a_2). Finally, Alice computes $MAC = H_c(M, r)$ and sends $(s, b_1, b_2, c, a_1, a_2, MAC)$ together with M to Bob. In the verification phase, Bob can identify the source of the given message M by computing d and and executing $s^2 \stackrel{?}{=} (-1)^{b_2} a^{b_1} H_S(r)(\mathrm{mod} n_S)$ and $MAC \stackrel{?}{=} H_c(M, r)$ with his private key (p_R, q_R). If Bob wants to cooperate fully with the third party, he can deliver his private key to the third party. After the third party obtains Bob's private key, he/she can ensure the source of the given message which comes from Alice with the same verification equations as the Bob.

The focus of attention is that the verification equations imply the sender's public key. This violated the property of deniable authentication protocol that a receiver cannot prove the source of the given message to any third party, even if he/she can construct another MAC for a different message. 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 with the third party.

5 Conclusion

In this paper, we have proposed a cryptanalysis on Lu et al.'s protocol. 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 by computing d and r and executing

$$s^2 \stackrel{?}{=} (-1)^{b_2} a^{b_1} H_S(r)(\mathrm{mod} n_S).$$

and

$$MAC \stackrel{?}{=} H_c(m, r).$$

Therefore, Lu *et al.*'s protocol cannot achieve the second requirements of a deniable authentication protocol.

References

[1] Y. Aumann and M. Rabin, "Efficient deniable authentication of long messages," *International Conference on Theoretical Computer Science in Honour of Professor Manuel Blums 60th Birthday*, pp. 20-24, Hong Kong, China, Apr. 1998.

[2] Y. Aumann and M. Rabin, "Authentication enhanced security and error correcting codes," *Proceedings of the 18th Annual International Cryptology Con-ference on Advances in Cryptology*, LNCS 1462, pp. 299-303, 1998.

[3] Z. Cao, "Universal en-crypted deniable authentication proto-col," *International Journal of Network Security*, vol. 8, no. 2, pp. 151-158, 2009.

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

[5] C. Dwork, M. Naor, and A. Sahai, "Concurrent zero knowledge," *Proceedings of the 30th ACM STOC '98*, pp. 409-418, Dallas, TX, USA, 1998.

[6] L. Fan, C. X. Xu, and J. H. Li, "Deni-able authentication protocol based on Diffie-Hellman algorithm," *Electronics Letters*, vol. 38, no. 14, pp. 705-706, 2002.

[7] C. Y. Liu, C.C. Lee, and T.C. Lin, "Cryptanalysis of an efficient deniable authentication protocol based on gener-alized ElGamal signature scheme," *International Journal of Network Security*, vol. 12, no. 1, pp. 34-36, 2011.

[8] R. Lu and Z. Cao, "Non-interactive deniable authentication pro-tocol based on factoring," *Computer Standards & Interfaces*, vol. 27, pp. 401-405, 2005.

[9] R. Lu and Z. Cao, "A new deniable authentication protocol from bilinear pairings," *Applied Mathematics and Computation*, vol. 168, pp. 954-961, 2005.

[10] R. Lu and Z. Cao, Erratum to "Non-interactive deniable authentication protocol based on factoring," *Computer Standards & Interfaces*, vol. 29, pp. 275, 2007.

[11] R. Lu and Z. Cao, "Group oriented identity-based deniable authentication protocol from the Bilinear Pair-ings," *International Journal of Network Security*, vol. 5, no. 3, pp. 283-287, 2007.

[12] M. O. Rabin, *Digitalized Signatures and Public-Key Functions as Intractable as Factorization*, MIT/LCS/TR-212, MIT Laboratory for Computer Science, 1979.

[13] Z. Shao, "Efficient deniable authentica-tion protocol based on generalized El-Gamal signature scheme," *Computer Standards & Interfaces*, vol. 26, pp. 449-454, 2004.

[14] H. Tian, X. Chen, and Y. Ding, "Analysis of two types deniable authentication protocols," *International Journal of Network Security*, vol. 9, no.3, pp. 242-246, 2009.

Razi Arshad received his M.Sc. degree in Mathematics from Quaid-i-Azam University, Islamabad, Pakistan in 2001; the M.Sc. degree in Computer Science from International Islamic University, Islamabad, Pakistan in 2004; the M.S. degree in Information Security from Sichuan University, Chengdu, China in 2007. He is currently research associate in National University of Sciences and Technology (NUST), Pakistan. His current research interest includes Network Security and Cryptography.

Nassar Ikram graduated in Electrical Engineering from NED, Karachi, Pakistan in 1987. He received his M.Sc. in Military Electronics and Systems Engineering from Royal Military College of Sciences, Shrivenham, Cranfield University, UK in 1995 and PhD in information Security from Bradford University, UK in 1999. He is currently professor at National University of Sciences and Technology, Islamabad, Pakistan. His current research interests include Network Security and Cryptography.