Security Analysis of a Suite of Deniable Authentication Protocols

Haibo Tian[1], Xiaofeng Chen[2], Baodian Wei[1], and Yi Liu[3]
(Corresponding author: Haibo Tian)
Department of School of Information Science and Technology, Sun Yat-sen University, Guangdong, China[1]
No. 135, Xin Gang West Road, Guangzhou, China, 510275
Department of School of Telecommunications Enginnering, Xidian University, Xi'an, China[2]
No. 6, Tai Bai South Road, Xi'an, China, 710071
Department of Faculty of Computer, Guangdong University of Technology[3]
No. 100 Waihuan Xi Road, Guangzhou Higher Education Mega Center, Guangzhou, China, 510006
(tianhb@mail.sysu.edu.cn)

(Received May 18, 2011; revised and accepted Jan. 11, 2012)

Abstract

A deniable authentication protocol allows a sender to transfer an authenticated message to a receiver, and the receiver cannot prove to a third party about the source of the message. In 2006, Zhu et al. analyzed deniable authentication protocols proposed by Deng et al. in 2001, which were based on a protocol proposed by Aumann et al. in 1998. In this paper, we show that the modified protocols by Zhu et al. suffer from a Byzantine attack when two sessions run concurrently. We also suggest methods to solve the problem.
Keywords: Byzantine attack, deniable authentication protocols, security analysis

1 Introduction

Authentication protocols enable a message receiver to make sure that it is communicating with an intended sender even in the presence of an adversary who controls the communication channel. A deniable authentication protocol is an authentication protocol, and it leaves no evidence to the receiver to prove that the sender took part in a particular protocol run. The deniability is a private property that can be used to enhance the privacy of Internet Key Exchange protocols, or to provide freedom from coercion in an electronic voting system and a fair negotiation application over the Internet. Recently, Bouassida [2] discussed authentication and privacy problems in vehicular Ad Hoc networks.

The notion of deniable authentication was introduced by Dwork et al. [8]. Deniable authentication replaces the non-interactive digital signature algorithms with a communication protocol. A protocol transcript can be simulated by a simulator so that the sender can deny its participation. Later Boyd et al. [3] gave out an informal definition of deniability that either user in a protocol run could have produced all the messages in the run. Then Raimondo et al. [18] considered receiver's privacy by introducing the concept of "forward deniability" that if the sender acted honestly during a protocol run, the sender is unable to claim the messages as authentic at a later stage. This property can be guaranteed if the distributions of a simulated transcript and a real one are identical or statistically close. Finally, Dodis et al. [7] introduced on-line deniability, where deniability should hold even when one of the parties colluded with a third party during the execution of a protocol.

The constructions of deniable authentication protocols can be classified into several approaches:

1) Dwork et al. [8] gave a protocol by using encryption algorithms. The algorithms should be secure against adaptive chosen ciphertext attack (CCA). Raimondo et al. [19] showed that the CCA definition was not satisfactory for concurrent deniability. A stronger assumption on the underlying encryption scheme was needed, namely plaintext awareness (PA-2). This construction is usually referred to as CCA-paradigm.

2) Aumann et al. [1] proposed a multi-round deniable authentication protocol without using encryption schemes. The authentication is multilevel according to the number of rounds. In each round, a zero knowledge (ZK) proof is executed. We refer to this fashion as ZK-paradigm. The enhanced protocols [6,24], although used encryption schemes, should be classified into the ZK-paradigm.

3) Boyd et al. [3] gave protocols by using long term symmetric key (SK) derived from public information. Lim et al. [16] improved their protocols. We refer to this approach as SK-paradigm. The protocol of Dodis et al. [7] used a dual-receiver encryption (DRE) scheme. The DRE scheme gives the sender and receiver equal abilities to extract plaintext from a ciphertext. So the protocol can be classified to the SK-paradigm. Protocols [4, 5, 12, 13, 15, 21–23] used key establishment techniques to produce a dynamic symmetric key for deniable message transmission, which could also be classified to the SK-paradigm.

4) Raimondo et al. [18] gave two approaches by using commitment schemes (CS) and projective hash functions (PHF). We refer to them separately as CS-paradigm and PHF-paradigm. Protocols of Pass [17] and Jiang [14] can be considered to fall into the CS-paradigm. The protocol of Feng et al. [10] can be classified to PHF-paradigm.

5) Dwork et al. [8] also gave a relaxed version of deniable authentication protocols by using signature schemes. Raimondo et al. [19] pointed out that the SIGMA protocol enjoyed partial deniability, which used signature schemes. Both signature schemes must be existential unforgeable (EU). This paradigm can be referred to as EU-paradigm.

We concentrate on the ZK-paradigm here. It has multiple rounds and its communication cost decreases in an online authentication scenario. Aumann et al. [6] proposed two deniable authentication protocols. Deng et al. [7] reviewed the one based on an integer factoring (IF) problem, and improved it. They also proposed a discreet logarithm (DL) problem based version. From the two literatures, we know that Aumann et al. gave a coding method to generate an expanded code from a message. A sender and a receiver then selected a few bits from the code. And one bit was randomly selected from the few bits for deniable authentication. The one-bit authentication procedure repeated several times. The procedure was a perfect ZK proof. To improve efficiency, Deng et al. [7] hashed a message to an m-block authenticator. To authenticate one block, a ZK proof was executed. Zhu et al. [24] pointed out a flaw in Deng et al.'s schemes and gave an improvement.

However, we show that the improvement of Zhu et al. [24] is unsatisfactory. An adversary can send an arbitrary message to a receiver. And the receiver will be convinced that the message comes from a sender while the sender has never sent the message. To do this, an adversary should be a qualified receiver. So we call the adversary as a Byzantine attacker. The attack also applies to the protocols of Deng et al. [6]. We show the problem in Figure 1, where Alice is an honest sender, and Bob is a dishonest receiver, and Cancy is cheated by Bob!

We then explore the similarity of the ZK-paradigm and some identification schemes [11, 20], and directly use the construction of the schemes to give two simpler protocols.

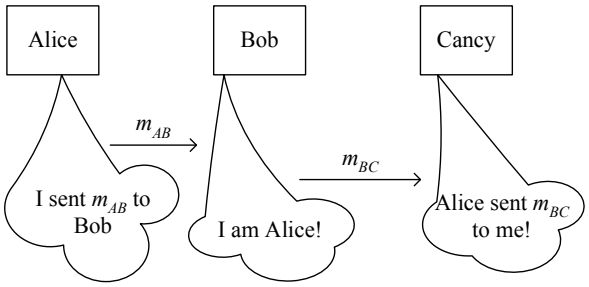

Figure 1: An illustration of a Byzantine attack

Organization. Section 2 specifies a model for deniable authentication protocols. Section 3 reviews and analyzes Zhu et al.'s protocols. The improvement protocols are in Section 4. Section 5 presents a simple comparison. Section 6 concludes the paper.

2 Model

We adopt the definitions and descriptions in [1,6,24] with small modifications to include a Byzantine attacker.

A system consists of n honest parties and a trusted third party (TTP). When two parties execute a protocol π, one is as a sender S and the other as a receiver R. The TTP sets system parameters and publishes public keys of parties and their identities. The public key of a sender is denoted by PK_S and a receiver by PK_R.

A sender S runs a protocol on input a message m, public system parameters, public information of a receiver R and private information of S. Receiver R interacts with S on input public system parameters, public information of a sender S and private information of R. Finally, S outputs "Finish", and R outputs "Accept" to indicate that R believes the corresponding user is the sender S or "Reject" vice versa.

An adversary $\mathcal{A}$ fully controls a communication channel between honest senders and receivers. Sender S and receiver R give protocol messages to $\mathcal{A}$ that is free to replay, modify or inject protocol messages. It also can choose any party as a receiver, and trigger a sender to run a protocol with the receiver for an arbitrary message. As a Byzantine attacker, $\mathcal{A}$ is qualified as a receiver or a sender.

With small modifications of definitions in [24], the meaning of security is as follows.

Definition 1 *A protocol is resistant to a Byzantine attack if it is negligible for R to accept a message while S has never sent the message.*

For deniability property, two games are considered. Game 1 executes a normal run of the protocol π between a sender S (on input message m) and a receiver R. The game output is a transcript of the run. Game 2 has only a simulator Sim that has all the information known by

R in a real world. However, the simulator has no private information of S. *Sim* takes as input the same message m. It also outputs a transcript which serves as a game output. The deniability definition is as follows.

Definition 2 *A protocol is deniable if the output of Game 1 executed by S and R is computationally indistinguishable between the output of Game 2 simulated by Sim.*

The model includes a description about a completeness property. It is about correctness, not related to our analysis. Interested readers can refer to [24].

3 Review and Security Analysis

Zhu et al. [24] analyzed and improved Deng et al.'s protocols. Their improvement lies in the computation method about v_i that is a component in a last message for one-round authentication. They compute $v_i = H(u_i||z_i)$ where symbol $||$ denotes binary string concatenation. Their protocols are as follows.

A Protocol Based on IF Problem. Let m be a long message sent from S to R. Let n be a security parameter. Let H be a collision-free hash function whose output is ts bits, where $2 \leq t \leq \log\log n$ and $s > 0$. Suppose $n = 1024$ and $ts = 256$. Any integers t and s can be chosen if their product is equal to 256.

Let Enc_R be a CCA secure public key encryption algorithm. R has a private key for decryption. Let $N = pq$ where p and q are two large prime numbers such that the factoring problem is intractable. A TTP publishes N and safely destroys p and q. Suppose a sender hashes a message into t blocks, $z_1, \ldots, z_t$, where $|z_j| = s$ and $1 \leq j \leq t$. The sender then randomly chooses $g_j \in_R \mathbb{Z}_N^*$ for $j = 1, \ldots, t$, computes $G_j = g_j^2 \mod N$, and gives $G_1, \ldots, G_t$ to the TTP as its public keys.

Suppose S sends R a long message m. R obtains S's public keys from the TTP and wants to make sure the message is from S. They run the following protocol multiple times. To authenticate a block of $H(m)$ deniably, the protocol proceeds as follows:

$$S \to R : \Lambda = \alpha^2 \bmod N$$
$$S \leftarrow R : i$$
$$S \to R : Enc_R(u_i), v_i = H(u_i||z_i),$$

where $\alpha \in_R \mathbb{Z}_N^*$ is chosen randomly by S, $i \in_R \{1, \ldots, t\}$ is chosen randomly by R, and $u_i \leftarrow \alpha g_i \bmod N$. At the end of the protocol, S sends the last message and outputs "Finish". R decrypts the ciphertext in the last protocol message to obtain u_i, then checks whether $u_i^2 = \Lambda G_i \bmod N$, and $v_i = H(u_i||z_i)$. If both equations hold, R outputs "Accept"; otherwise, R outputs "Reject".

Remark 1 *There is a trivial attack for a one-block authentication. An attacker can guess a value i, and randomly generate $u_i \in_R \mathbb{Z}_N^*$, and compute $\Lambda = u_i^2/G_i \bmod N$, and send Λ to R. If i is guessed correctly, the attacker succeeds. Since i is randomly chosen from $\{1, \ldots, t\}$, the success probability is $1/t$. So we say that a one-block authentication is secure against a Byzantine attack if the success probability is just negligibly greater than $1/t$.*

To see that a protocol is secure against a Byzantine attack in the context of Definition 1, we consider that it runs c times for fixed message m and public keys $\{G_i\}_{1 \leqslant i \leqslant t}$. The probability is t^{-c} for a Byzantine attack to succeed c times. As $t \geq 2$, we can choose a suitable value c to assure a negligible success probability of an attacker.

A Protocol Based on DL Problem. Let $\mathbb{Z}_p^*$ be a large group such that the DL problem is intractable. Let g be a generator of a subgroup of $\mathbb{Z}_p^*$ with a prime order q. Similar to the IF problem based version, a sender hashes a message into t blocks. Sender S randomly chooses $r_j \in_R \mathbb{Z}_q$, computes $G_j = g^{r_j} \bmod p$, and gives G_j to a TTP as its public keys.

Suppose S sends R a long message m. R obtains S's public keys from the TTP, and wants to make sure the message is from S. They run the following one-block authentication protocol multiple times.

The protocol proceeds in the same way as the IF problem based protocol except that Λ and u_i are now computed as

- $\Lambda = g^{\alpha} \bmod p$, and
- $u_i = (\alpha + r_i) \bmod q$ where $\alpha \in_R \mathbb{Z}_q$ is randomly chosen by S.

At the end of the protocol, S sends the last message and outputs "Finish". R decrypts the ciphertext to obtain u_i, and checks whether $g^{u_i} = \Lambda G_i \bmod p$, and $v_i = H(u_i||z_i)$. If both hold, R outputs "Accept". Otherwise, R outputs "Reject".

3.1 Byzantine Attack

We show that their protocols are not secure against a Byzantine attack. We use the IF problem based version as an example to show an attack procedure.

Suppose that S sends a message $m_{S\mathcal{A}}$ to an adversary $\mathcal{A}$ (a Byzantine attacker). Then $\mathcal{A}$ sends a new message $m_{\mathcal{A}R}$ to a receiver R impersonating the sender S. When the receiver R wants to authenticate the message $m_{\mathcal{A}R}$, the adversary $\mathcal{A}$ asks sender S to prove the authorship of message $m_{S\mathcal{A}}$. Let $H(m_{S\mathcal{A}}) = z_1, \ldots, z_t$ and $H(m_{\mathcal{A}R}) = z'_1, \ldots, z'_t$, each of z_j and z'_j is s bits and $1 \leq j \leq t$. Then the attack is illustrated as follows:

$$\begin{aligned}
s1:&\ S \to \mathcal{A} : \Lambda = \alpha^2 \bmod N \\
&\ s2:\ \mathcal{A}(S) \to R : \Lambda \\
&\ s2:\ \mathcal{A}(S) \leftarrow R : i \\
s1:&\ S \leftarrow \mathcal{A} : i \\
s1:&\ S \to \mathcal{A} : Enc_{\mathcal{A}}(u_i), v_i = H(u_i||z_i) \\
&\ s2:\ \mathcal{A}(S) \to R : Enc_R(u_i), v_i = H(u_i||z'_i)
\end{aligned}$$

There are two sessions labeled by $s1$ and $s2$. The session $s1$ has two players S and $\mathcal{A}$ where $\mathcal{A}$ is a receiver. The session $s2$ also has two players $\mathcal{A}$ and R, where $\mathcal{A}$ impersonates a sender S, denoted by $\mathcal{A}(S)$. Both $s1$ and $s2$ can terminate normally. The attack can be executed for each block of the message with a perfect success probability. After the attack, R will be convinced that S has sent the message $M_{\mathcal{A}R}$ while S has never done that. This result violates the Definition 1.

4 Our Methods

Zhu et al.'s protocols have a problem that the value u_i has no relationship to the message to be authenticated. This provides an opportunity for an insider attacker to make the authentication goal fail.

4.1 IF Problem Based Version

The identification schemes [9, 11] motivate us to suggest the following IF problem based protocol.

$$S \rightarrow R : \Lambda = \alpha^2 \bmod N$$
$$S \leftarrow R : i$$
$$S \rightarrow R : u_i = \alpha \prod_{(H_1(z_i))_j=1} g_j$$

We introduce an additional secure hash function $H_1 : \{0,1\}^s \rightarrow \{0,1\}^k$, where k is a security parameter. For example, $k = 128$. The symbol $(H_1(\cdot))_j$ means the j-th bit in the output of function H_1. The modification is about the last protocol message that is similar to the construction in [9, 11], where sender S computes the cumulative product of g_j indexed by the hashing output of a block z_i, and then S multiplies the cumulative product by the random value α to generate a response u_i. After the last protocol message is sent, S outputs "Finish". After receiving the message, R checks the equation $(u_i)^2 = \Lambda \prod_{(H_1(z_i))_j=1} G_j \bmod N$. If the equation holds, R outputs "Accepts". Otherwise, R outputs "Reject".

Remark 2 *Note that the number of keys has been changed to k, the length of an output of H_1. If k is too small, an adversary can efficiently compute another message m' so that $H(m') = z'_1, \cdots, z'_t$ and $H_1(z_i) = H_1(z'_i)$ for all $1 \leq i \leq t$. The computation cost of the adversary is bounded by $2^{k/2}$.*

Lemma 1 *The improved IF problem based scheme satisfies Definition 1.*

The modified protocol can be proven by resembling the proof of Theorem 3 in [9] if we view the hash function H_1 as a random oracle. The key point is that a simulator can manipulate an adversary's random tape to control the adversary to use the same value α for two different challenges.

Lemma 2 *The improved IF problem based scheme satisfies Definition 2.*

The deniability property also can refer the proof of Theorem 3 in [9] about its zero-knowledge argument. The trick of a simulator is to try all possible challenges to satisfy the verification equation by changing the random response. Note that $i \in_R \{1, ..., t\}$ and $2 \leq t \leq loglogn$.

As the two proofs just resemble the proof of Theorem 3 in [9] except that the hash function H_1 is modeled as a random oracle, we omit the proofs here.

Although the security can be guaranteed, the efficiency of the modified protocol is not good as the keys are a little too many. In fact, the identification scheme in [11] is good enough to fulfil the task of deniable message authentication in the multi-round fashion according to the remark 3 in that literature. So we stop our further considerations about the IF problem based version.

4.2 DL Problem Based Version

The identification scheme [20] motivates us to suggest the following DL problem based protocol.

$$S \rightarrow R : \Lambda = g^{\alpha} \bmod p$$
$$S \leftarrow R : i$$
$$S \rightarrow R : u_i = \alpha + H_2(z_i) r_i \bmod q$$

We introduce an additional secure hash function $H_2 : \{0,1\}^s \rightarrow \mathbb{Z}_q$. We modified the last protocol message that is now similar to the construction in [20], where sender S computes a hashing output of a block z_i, and then S multiplies the hash value by the i-th private key r_i, and adds the random value α to generate a response u_i. After the last protocol message is sent, S outputs "Finish". After receiving the last message, R checks the equation $g^{u_i} = \Lambda G_i^{H_2(z_i)} \bmod p$. If the equation holds, R outputs "Accepts". Otherwise, R outputs "Reject".

Remark 3 *Note that if $s = |z_i|$ is too small, an adversary has a non-negligible probability to select two messages of whom the hashing outputs have identical blocks. An adversary then has a better successful probability than $1/t$ for each round. For example, suppose that two blocks are identical. Then the adversary can use an honest sender as an oracle for the two blocks when they are challenged. For other challenged blocks, the adversary can just guess a challenge value with a probability $1/(t-2)$, better than $1/t$.*

Lemma 3 *The improved DL based version satisfies Definition 1.*

The modified protocol can be proven secure by using the same techniques as in [20]. The key point is also to control the random tape of an adversary.

Lemma 4 *The improved DL based version satisfies Definition 2.*

Table 1: Comparison of improved protocols with old ones

Scheme	Problem	Encryption	Hash Tag
[6]	IF	Yes	Yes
[24]	IF	Yes	Yes
[24]	DL	Yes	Yes
Ours	IF	No	No
Ours	DL	No	No

The deniability property also can refer the proof of Theorem 3 in [9]. The trick of a simulator is to try all possible challenges to satisfy the above verification equation by changing the random response.

Due to the same reason of the IF based version, we omit the proofs.

5 Comparison

We compare the improved protocols with old ones considering a one round authentication. The "Problem" denotes an underlying hard problem of a scheme. The "Encryption" indicates that an encryption algorithm is used or not. The "Hash Tag" shows whether a hash tag is in the last protocol message.

The efficiency is better than the protocols in [6,24] due to the removal of encryption algorithms and a hash tag.

6 Conclusion

This paper analyzed a suite of deniable authentication protocols inspired by the original work of Aumann and Rabin [1]. We analyzed the last improved protocols of this type in [24]. We illustrated that the last protocols suffered from a Byzantine attack, and gave a method to improve those protocols.

Acknowledgments

This work is supported by the National Natural Science Foundation of China (Grant Nos. 61272455, 61003244), Fundamental Research Funds for the Central Universities (Grant Nos. 11lgpy71, 11lgzd06), Science and Technology Planning Project of Guangdong Province (Grant No. 2012B010100032), and the Industry-Education-Research Cooperation Project of Guangdong Province and the Ministry of Education (Grant No. 2012B091000060).

References

[1] Y. Aumann and M. O. Rabin, "Authentication, enhanced security and error correcting codes," in *LNCS 1462, 18th Annual International Cryptology Conference (Crypto'98)*, pp. 299–303, California, USA, August 1998.

[2] M. S. Bouassida, "Authentication vs. privacy within vehicular ad hoc networks, international journal of network security," *International Journal of Network Security*, vol. 13, no. 3, pp. 121–134, 2011.

[3] C. Boyd, W. Mao, and K. Paterson, "Deniable authenticated key establishment for internet protocols," in *LNCS 3364, Security Protocols, 11th International Workshop*, pp. 255–271, Cambridge, UK, April 2003.

[4] T. Cao, D. Lin, and R. Xue, "An efficient id-based deniable authentication protocol from pairings," in *Proceedings of the 19th International Conference on Advanced Information Networking and Applications*, pp. 388–391, Taipei, Taiwan, March 2005.

[5] J. S. Chou, Y. Chen, and J. C. Huang. "A id-based deniable authentication protocol on pairings,". Tech. Rep. Cryptology ePrint archive, Report 2006/335, Oct. 2006.

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

[7] Y. Dodis, J. Katz, A. Smith, and S. Walfish, "Composability and on-line deniability of authentication," in *LNCS 5444, Theory of Cryptography Conference 2009, (TCC 2009)*, pp. 146–162, San Francisco, CA, USA, March 2009.

[8] C. Dwork, M. Naor, and A. Sahai, "Concurrent zero knowledge," in *Proceedings of the Thirtieth Annual ACM Symposium on the Theory of Computing, STOC 1998*, pp. 409–418, Dallas, Texas, USA, May 1998.

[9] U. Feige, A. Fiat, and A. Shamir, "Zero-knowledge proofs of identity," *Journal of Cryptology*, vol. 1, no. 2, pp. 77–94, 1988.

[10] T. Feng, F. H. Li, J. F. Ma, and S. J. Moon, "A new approach for uc security concurrent deniable authentication," *Science in China Series F: Information Sciences*, vol. 51, no. 4, pp. 352–367, 2008.

[11] A. Fiat and A. Shamir, "How to prove yourself: Practical solutions to identification and signature problems," in *LNCS 263, Advances in cryptology - CRYPTO'86*, pp. 186–194, California, USA, unkown 1986.

[12] R. Gnanajeyaraman and S. Sasidharan, "Chaos function based - secure deniable authentication protocol," *International Journal of Computer Applications in Engineering Sciences (IJCAES)*, vol. 1, no. 1, pp. 32–36, 2011.

[13] L. Harn, C. Y. Lee, C. Lin, and C. C. Chang, "Fully deniable message authentication protocols preserving confidentiality," *Computer Journal*, vol. 54, no. 10, pp. 1688–1699, 2011.

[14] S. Jiang and S. N. Reihaneh, "An efficient deniable key exchange protocol (extended abstract)," in *LNCS 5143, Financial Cryptography and Data Security*, pp. 47–52, Cozumel, Mexico, January 2008.

[15] M. H. Lim, S. Lee, and H. Lee, "Cryptanalysis on improved chou et al.?s id-based deniable authentication protocol," in *Proceedings of the 2008 International Conference on Information Science and Security*, pp. 87–93, Seoul, Jan. 2008.

[16] M. H. Lim, S. Lee, Y. Park, and S. Moon, "Secure deniable authenticated key establishment for internet protocols," in *Information Security and Assurance, 2008 (ISA 2008)*, pp. 3–6, Busan, April 2008.

[17] R. Pass, "On deniability in the common reference string and random oracle model," in *LNCS 2729, Advances in Cryptology - CRYPTO 2003*, pp. 316–337, Santa Barbara, California, USA, August 2003.

[18] M. D. Raimondo and R. Gennaro, "New approaches for deniable authentication," in *Computer and Communications Security (CCS'05)*, pp. 112–121, Alexandria, VA, USA, Nov. 2005.

[19] M. D. Raimondo, R. Gennaro, and H. Krawczyk, "Deniable authentication and key exchange," in *Computer and Communications Security (CCS'06)*, pp. 400–409, Taipei, Taiwan, March 2006.

[20] C.P. Schnorr, "Efficient identification and signatures for smart cards," in *LNCS 435, Advances in Cryptology - Crypto'89*, pp. 239–252, California, USA, August 1989.

[21] 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.

[22] C. Xu, L. Fan, and J. Li, "Deniable authentication protocol based on diffie-hellman algorithm," *Electronics Letters*, vol. 38, no. 4, pp. 705–706, 2002.

[23] E. J. Yoon, E. K. Ryu, and K. Y. Yoo, "Improvement of fan et al.'s deniable authentication protocol based on diffie-hellman algorithm," *Applied Mathematics and Computation*, vol. 167, no. 1, pp. 274–280, 2005.

[24] R. W. Zhu, D. S. Wong, and C. H. Lee, "Cryptanalysis of a suite of deniable authentication protocols," *Communications Letters*, vol. 10, no. 6, pp. 504–506, 2006.

Haibo Tian is currently working as a lecture in the school of information science and technology, Sun Yat-sen University, China. He is also a member of Guangdong Key Laboratory of Information Security Technology. He received his Ph.D. degree from School of Telecommunications Engineering, Xidian University in 2006. His current research interests include deniability, signatures and network security.

Xiaofeng Chen has received his Ph.D. in Cryptography from School of Telecommunications Engineering, Xidian University in 2003. He is a professor at School of Telecommunications Engineering in Xidian University, China. His research interest includes public key cryptography and applications.

Baodian Wei is an associate professor in the School of Information Science and Technology at Sun Yan-sen University, China. He obtained his Ph.D. degree from School of Telecommunications Engineering, Xidian University in 2004. His research interests include cryptology and its applications.

Yi Liu is an associate professor in the Faculty of Computer, Guangdong University of Technology. He obtained his Ph.D. degree from School of Telecommunications Engineering, Xidian University in 2005. His research interests include cryptology and its applications.