Bulletin de la Société des Sciences de Liège, Vol. 85, 2016, *p.* 1235 - 1240

Cryptanalysis of an Improvement of Robust Deniable Authentication Protocol

Mahshid SADEGHPOUR [*]

Iran University of Science and Technology

Abstract

Keywords: deniable authentication, electronic voting system, ElGamal cryptosystem

1. INTRODUCTION

Security is an integral part of every communication network, absence of which could lead to catastrophic consequences. For this concern, deniable authentication has become a field of interest for cryptographers and cryptanalysts in recent years. Compared to traditional authentication protocols, deniable authentication has two fundamental features: 1) only intended receiver can identify the original source of a given message, 2) the receiver cannot prove the source of the message to a third party.

Deniable authentication protocols have several applications. For instance, Deng et al. [2] provided two examples of its applications in coerced electronic voting system, and secure negotiation over the internet.

In 1998, Dwork et al. [4] proposed a deniable authentication protocol based on concurrent zero-knowledge proof. However, the postponement caused by its multi round communication requirement and the cost of its computing make it quite inefficient in real-time applications. In the same year, Aumman and Rabin [1] developed another scheme based on the factoring problem. In 2001, Deng et al [2] proposed two schemes based on the factoring problem and the discrete logarithm problem, respectively. Both Aumman-Rabin and Deng et al. protocols require a public directory. Later, Fan et al. [6] proposed a new deniable authentication protocol to remove the weakness of requiring a public directory. All these four mentioned protocols had the same deficiency; in these schemes the sender (S) of a message does not authenticate the identity of the receiver (R). This, in turn, could cause receiver's impersonation attack. Two years later, Shao [12] designed a non-interactive deniable authentication protocol based on generalized ElGamal signature scheme [5]. However, in 2011, Liu et al. [8] showed that their scheme is unable to achieve the second requirement of a deniable authentication scheme. In 2005, Lu and Cao [10] designed a non-interactive deniable authentication protocol based on the factoring problem. In the same year, Wang et al. [13] proposed a simple deniable authentication protocol (WLT) based on the inverse of the ElGamal cryptosystem [5]. A year later, Shao et al. [11] proved that WLT is insecure against person-in-the-middle-attack (PIM), and proposed an improvement of this scheme (SCL). Albeit, in 2010, Yoon et al [14] showed that SCL and WLT are insecure against receiver's impersonation attack, and designed an improved deniable authentication protocol based on ElGamal cryptosystem [5] and the Diffie-Hellman key distribution protocol [3]. In 2013, Li and Takagi [9] demonstrated that Yoon et al's scheme does not satisfy the deniable authentication property, since the receiver can prove the source of a given Deniable authentication protocol, as an advanced method of authentication, enables the intended receiver of a given message to identify the source of the message while preventing the receiver to prove this source to a third party. In 2013, Li and Takagi proposed an enhanced model of Yoon et al's robust deniable authentication protocol and claimed that their model could achieve the property of deniable authenticity. The present study reviews and

analyses Li and Takagi's suggested model and argues that this model still needs improvement to satisfy deniability.
message to a third party. They also proposed an improvement to overcome this flaw. However, in this paper it is demonstrated that Li-Takagi's protocol is unable to achieve the second requirement of a deniable authentication scheme. The rest of this paper is organized as follows. Section 2 is the review of Li-Takagi's scheme. The cryptanalysis of this scheme is proposed in section 3. Eventually, conclusion is made in section 4.

2. Li-Takagi's Protocol

The Li-Takagi's protocol has three participants: A sender S, a receiver $R$and an inquisitor INQ. INQ is a person-in-the-middle (PIM), sitting on the insecure link between S and R, intercepting their transitions and injecting his own messages.
Assume p and c are two large random prime numbers in a way that $q|(p-1)$. Also, g is a primitive element in GF(p). H(.) and H_1(.) are two distinct collision free hash functions, and H_1(.): $\{0,1\}^* \rightarrow \{0,1\}^n$, where n denotes the bits number of the given message M. $x_S \in \mathbb{Z}_q^*$is sender's private key and $y_s = g^{x_s} \bmod p$is sender's public key. $x_r$is receiver's private key and $y_r = g^{x_r} \bmod p$is the corresponding public key. The symbol "||" demonstrates concatenation. The process of this protocol is given in Fig.1. There are three steps in this protocol.

Step1. R chooses a random number $a \in \mathbb{Z}_q^*$,and computes $A = g^a \bmod p$, $B = y_s^{a} mod\, p$. R also computes Diffie-Hellman mutual key $DH = y_s^{x_r} mod\, p$and $C_1 = H(A \parallel B \parallel DH)$. At last, R sends (A,C_1) to S and keeps a as a secret.

Step2. When S receives (A,C_1) from R, he calculates $B = A^{x_s}\, mod\, p$and the Diffie-Hellman mutual key $DH = y_r^{x_s}\, mod\, p$. Then he checks if the equation below holds:

$$C_1 = H(A \parallel B \parallel DH) \qquad (1)$$

If Eq. (1) holds, then S authenticates R. If S decides to send a message M to R, he chooses a random number $u\epsilon\mathbb{Z}_q^*$and computes $U = g^u mod\, p$, $V = y_r^{u} mod\, p$. S also computes (C_2, C_3) as follows:

$$C_2 = H_1(B) \oplus M$$

And

$$C_3 = H(A \parallel B \parallel U \parallel V \parallel M)$$

Then S sends (U, C_2, C_3) to R.

Step3. Upon receiving (U, C_2, C_3), R can achieve the message M by computing

$$M = H_1(B) \oplus C_2$$

Then R computes $V = U^{x_r} mod\, p$and checks out if the following equation holds:

$$C_3 = H(A \parallel B \parallel U \parallel V \parallel M) \qquad (2)$$

If Eq. (2) holds, R accepts the message M. otherwise he rejects it.

The sender S — The receiver R

$A = g^a mod\ p$
$B = y_s{}^a mod\ p$
$DH = y_s{}^{x_r} mod\ p$
$C_1 = \mathrm{H}(A \parallel \mathrm{B} \parallel \mathrm{DH})$

$$\xleftarrow{(A,C_1)}$$

$B = A^{x_s} mod\ p$
$DH = y_r{}^{x_s} mod\ p$
$C_1 = \mathrm{H}(A \parallel \mathrm{B} \parallel \mathrm{DH})$
$U = g^u mod\ p$
$V = y_r{}^u mod\ p$
$C_2 = H_1(B) \oplus M$
$C_3 = H(A \parallel B \parallel U \parallel V \parallel M)$

$$\xrightarrow{(U,C_2,C_3)}$$

$M = H_1(B) \oplus C_2$
$V = U^{x_r} mod\ p$
$C_3 = H(A \parallel B \parallel U \parallel V \parallel M)$

Fig.1 *The Li-Takagi's protocol*

3. Cryptanalysis of Li-Takagi's Protocol

As Deng et al [2] has demonstrated the very basic characteristics and applications of deniable authentication in their article in 2001, in applying a deniable authentication scheme, R must be sure that the message 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. The idea of full cooperation of receiver and the third party makes sense in both applications of deniable authentication. In secure negotiations between a merchant (R) and the customer (S), it is logical that the merchant fully cooperates with a third party (another customer) to elicit a better offer. Also, in electronic voting systems, the third party could pay the receiver of coerced votes to compensate his loss of private key. Then, the third party is able to check whether the coerced voters have chosen the predominated candidate or not. In this case, the receiver can apply for a new pair of keys to the certification authority (CA). Therefore, it is rational that in some cases of deniable authentication schemes, the receiver is fond of fully collaboration with the third party.

Suppose R and T (third party) fully cooperate. The following attack shows that the receiver can prove the source of a given message to a third party. The process of this attack is shown in Fig.2. The attack is as follows.

Step1. The receiver sends his private key, x_r, to the third party.

Step2. After receiving x_r from R, T chooses a random number $a \epsilon \mathbb{Z}_q{}^*$ and computes $A = g^a mod\ p$, $B = y_s{}^a mod\ p$, $DH = y_s{}^{x_r} mod\ p$, then he computes

$$C_1 = \mathrm{H}(A \parallel \mathrm{B} \parallel \mathrm{DH})$$

And sends the pair (A,C$_1$) to R, while keeping a and B secret.

Step3. After receiving (A, C_1), R sends this pair to S.

Step4. In this step, S computes $B = A^{x_s} mod\ p,\ DH = {y_r}^{x_s}\ mod\ p$

Then he checks the following equation

$$C_1 = H(A \parallel B \parallel DH) \qquad (3)$$

If Eq.3 holds, then S chooses a random $u \epsilon \mathbb{Z}_q^*$ and computes $U = g^u mod\ p,\ V = {y_r}^u mod\ p$, and he computes

$$C_2 = H_1(B) \oplus M$$

and

$$C_3 = H(A \parallel B \parallel U \parallel V \parallel M)$$

and sends (U, C_2, C_3) to R.

Step5. R sends (U, C_2, C_3) to T.

Step6. T can obtain M with the following equation

$$M = H_1(B) \oplus C_2$$

, and computes $V = U^{x_r} mod\ p$ and checks the validity of the following equation

$$C_3 = H(A \parallel B \parallel U \parallel V \parallel M) \qquad (4)$$

If Eq.4 holds, T accepts M. Otherwise he rejects it.

The sender S		The receiver R		The third party T
			$\xrightarrow{x_r}$	
				$A = g^a mod\ p$ $B = {y_s}^a mod\ p$ $DH = {y_s}^{x_r} mod\ p$ $C_1 = H(A \parallel B \parallel DH)$
	$\xleftarrow{(A,C_1)}$		$\xleftarrow{(A,C_1)}$	
$B = A^{x_s} mod\ p$ $DH = {y_r}^{x_s} mod\ p$ $C_1 = H(A \parallel B \parallel DH)$ $U = g^u mod\ p$ $V = {y_r}^u mod\ p$ $C_2 = H_1(B) \oplus M$ $C_3 = H(A \parallel B \parallel U \parallel V \parallel M)$				
	$\xrightarrow{(U,C_2,C_3)}$		$\xrightarrow{(U,C_2,C_3)}$	
				$M = H_1(B) \oplus C_2$ $V = U^{x_r} mod\ p$ $C_3 = H(A \parallel B \parallel U \parallel V \parallel M)$

Fig.2 *Attack to Li-Takagi's protocol*

In this protocol when R sends (U, C_2, C_3) to T, T is sure that this triple is generated by S because R is not aware of a and B, and cannot produce a fake (U, C_2, C_3).

The flaw of Li-Takagi's scheme is that sender's public key, y_s, is used in the verification equations. As Liu et Al [10] has noted in their paper, if a deniable authentication protocol can get rid of the public key in the verification equations, the scheme is able to withstand the flaws of full cooperation.

It is worth noting that T can only benefit from this attack in the first example of applications of a deniable authentication protocol (coerced electronic voting systems). This is because in this attack, R is unable to recover the message M since he does not know B. R transfers the received data to T without knowing the original message M, therefore; in the second example of applications of Li-Takagi's deniable authentication scheme, if a merchant fully cooperates with the third party as of the mentioned attack, he would send the offer M received from a customer without knowing the amount of it. It is obvious that a merchant does not accept such cooperation for he is willing to elicit the better offer.

4. CONCLUSION

In this paper, the security analysis of Li-Takagi's deniable authentication protocol is presented. It is demonstrated that their protocol does not satisfy confidentiality if a receiver gives his own private key to the third party to fully collaborate. Thus, even though Li and Takagi have claimed that their protocol is deniable, it is not secure to apply this protocol in coerced electronic voting systems.

REFERENCES

. [1] Y. Aumann, M. Rabin, Authentication enhanced security and error correcting codes, in: Advances in Cryptology–Proceedings of Crypto'98, Lecture Notes in Computer Sciences, 1462, Springer-Verlag, (1998), pp. 299–303.

. [2] X. Deng, C.H. Lee, H. Zhu, Deniable authentication protocols, IEE Proceedings – Computers and Digital Techniques 148 (2), (2001), pp. 101–104.

. [3] W. Diffie, M. Hellman, New directions in cryptography. *IEEE Transactions on Information Theory, 22,* (1976), pp. 644–654.

. [4] C. Dwork, M. Naor, A. Sahai, Concurrent zero-knowledge, in: Proceedings of 30th ACM STOC'98, (1998), pp. 409–418.

. [5] T. ElGamal, A public-key cryptosystem and a signature scheme based on discrete logarithms. *IEEE Transactions on Information Theory, 31*, (1985), pp.469–472.

. [6] L. Fan, C.X. Xu, J.H. Li, Deniable authentication protocol based on Diffie–Hellman algorithm, Electronics Letters 38 (4) (2002), pp. 705– 706.

. [7] Y. Harn, Design of generalized ElGamal type digital signature scheme based on discrete logarithm. *Electronics Letters, 31,* (1995), pp. 2025–2026.

. [8] C. Liu, C. Lee, T. Lin, Cryptanalysis of an efficient deniable authentication protocol based o generalized ElGamal signature scheme, in: International Journal of Network Security, 12, (2011), pp. 34-36.

. [9] F. Li, T. Takagi, Cryptanalysis and improvement of robust deniable authentication protocol, Wireless Pres Commun, (2013), pp. 1391-1398.

. [10] R. Lu, Z. Cao, A new deniable authentication protocol from bilinear pairings, Applied Mathematics and Computation 168 (2) (2005), pp. 954–961.

. [11] J. Shao, Z. Cao, R. Lu, An improved deniable authentication protocol. *Networks, 48*, (2006), pp.179–181.

. [12] Z. Shao, Efficient deniable authentication protocol based on generalized ElGamal signature scheme, Computer Standards & Interfaces 26 (5) (2004), pp. 449–454.

. [13] Y. Wang, J. Li, L. Tie, A simple protocol for deniable authentication based on ElGamal cryptography. *Networks*, *45*, (2005), pp. 193–194.

. [14] E. J. Yoon, K.Y. Yoo, S.S. Yeo, C. Lee, Robust deniable authentication protocol. *Wireless Personal Communications*, *55*, (2010) pp. 81–90.