A Secure Strong Designated Verifier Signature Scheme

Asif Uddin Khan, Bikram Kesari Ratha
(Corresponding author: Asif Uddin Khan)
Department of Computer Science & Utkal University[1]
VaniVihar, Bhubaneswar, India
(Email:asif.utkal@gmail.com, b_ratha@hotmail.com)
(Received Aug. 7, 2012; revised Oct. 12, 2014 and July 18, 2015; accepted July 31, 2016)

Abstract

Recently Lee-Chang proposed a new strong designated verifier signature scheme. They claimed that their proposed scheme is more secure and suitable for the purpose of a strong designated verifier signature scheme. This paper shows that Lee-Chang scheme cannot withstand forgery attack which an adversary can forge a signature without knowing the secret key of the signer or the designated verifier and an improved scheme is presented to overcome the security weaknesses of their scheme.The security of the scheme is enhanced by adding the secret key of the signer in signature generation phase. The analysis shows that the new scheme resolves security problems in the previous scheme, meets the aspects of security feathers needed by strong designated verifier signature scheme.

Keywords: Cryptanalysis; Designated Verifier Signature Scheme; Digital Signature; Forgery Attacks

1 Introduction

Next generation wireless network is expected to include many applications and services such as voice, data and multimedia online gaming, software distribution with very high data rate. Use of new technologies and services such as internet of things cloud computing are growing rapidly day by day where numerous network based services and applications are provided through internet. Further internet of things (IOT) is the big revolution in the future networking technologies where communication for application, data and services can take place any where any time through any device. Providing guaranteed quality of service (QOS) to these applications and services is an important objective in the design of next generation network. At the same time various types of security threats in the network based services are increasing. Providing security such as confidentiality, authenticity and data integrity is a must in order to achieve guaranteed QOS.

A digital signature is very important in modern electronic data processing systems. Recently, to provide security services such as user authentication, data integrity, and non-repudiation, digital signature schemes are widely used in distributed network environments such as Internet or web. There are many variations of digital signature schemes such as proxy signature, blind signature; ring signature discussed in the papers [1, 2, 3, 10, 17, 20]. In an ordinary digital signature scheme, anyone can verify the validity of a signature using the signer's public key. However, in some scenarios, this public verification is not desired, if the signer does not want the recipient of a digital signature to show this signature to a third party at will. To address this problem above, in [6] authors introduced undeniable signature which allowed a signer to have complete control over his signature. In an undeniable signature scheme, the verification of a signature requires the participation of the signer, in order to avoid undesirable verifiers getting convinced of the validity of the signature. Motivated by the above problem, in [6] Jakobsson et al. proposed the concept of designated verifier signature (DVS) schemes. A DVS scheme is special type of digital signature which provides message authentication without non-repudiation. These signatures have several applications such as in E-voting, call for tenders and software licensing. Suppose Alice has sent a DVS to Bob. Unlike the conventional digital signatures, Bob cannot prove to a third party that Alice has created the signature. This is accomplished by the Bob's capability of creating another signature designated to him which is indistinguishable from Alice's signature. In [6] Jakobsson et al. also introduced a stronger version of DVS. In this stronger scheme, no third party can even verify the validity of a designated verifier signature, since the designated verifier's private key is required in the verifying phase. In 2003, Saeednia et al. [11] proposed a strong designated verifier signature scheme based on the Schnorr signature scheme [12] and Zheng's signcryption scheme [21].

In 2008, Lee-Chang [8], however, pointed out that Saeednia et al.'s scheme would reveal the identity of

the signer if the secret key of the signer is compromised. Then, they proposed a new strong designated verifier signature scheme based on the Schnorr signature scheme [12] and Wang et el.'s authenticated encryption scheme [15] which can be verified only with the designated verifier's secret key. Obviously, Lee-Chang's scheme provides signer ambiguity even in the situation in which the secret key of the signer is compromised since each secret key is protected under the DLP (Discrete Logarithm Problem) assumption. Lee-Chang claimed that their proposed scheme is more secure and suitable for the purpose of a strong designated verifier signature scheme,but in [5] Hyun, Suhng-Ill, Eun-Jun Yoon etal shown several attacks on Lee-Chang's scheme.In this paper we discuss the forgery attack on Lee- Chang's scheme and show that their scheme still cannot withstand forgery attack which an adversary can forge a signature without knowing the secret key of the signer or the designated verifier based on [5] and we then propose an improved designated verifier signature scheme which is more secure and safe.

The paper is organized as follows:In section-2 we discuss the related work, Section-3 reviews Lee-Chang's designated verifier signature scheme. Section-4 shows forgery attack on Lee-Chang's scheme. Section-5 shows the improved scheme, section-6 shows analysis of improved scheme and finally the conclusion comes in Section-7.

2 Related Work

Several researches have been conducted to design efficient strong designated verifier signature scheme (SDVS) for achieving Quality of service (QOS) for the next generation networks. In this section, we discuss the recent developments in SDVS. In [7] authors propose a strong designated verifier signature scheme with message recovery mechanism based on the discrete logarithm problem.In [18] a novel construction of a SDVS scheme with secure disavow ability is proposed which utilizes a chameleon hash function and supports the signer to have a complete control of his signature. In [9] authors propose an efficient ID-based strong designated verifier signature schemes with message recovery and give its rigorous security proof in the random oracle model based on the hardness assumptions of the computational Bilinear Diffie-Hellman problem. This scheme can be used in some special environments where the bandwidth is one of the main concerns, such as PDAs, cell phones, RFID etc.[16] proposed a strong designated verifier signature in certificateless public key settings strong designated verifier signature in certificateless public key settings. [13] present a stronger security notion for the SDVS schemes, full non-delegatability, which not only needs the non-delegatability of signing, but also requires that non-delegatability of verifying. In [4], Huang, Susilo, Mu et.al proposed a variant of designated verifier signature scheme, i.e short strong designated verifier signature scheme and its variant scheme which is a identity based scheme. In [19] Yang and Liao proposed a strong designated verifier signature scheme, using key distribution mechanism where both sender and designated receiver share encryption/decryption key to fulfill encryption/decryption algorithm with low cost of communication and computation respectively and they proved their security based on Deffi-Helman assumptions. [14] provides general CL-SDVS schemes and instances, and discusses their security briefly.

3 Review of Lee-Chang's Strong Designated Verifier Scheme

This section reviews Lee-Chang's strong designated verifier signature scheme as shown in Figure 1. The common parameters used in Lee-Chang's scheme are as follows:

- Alice: The signer.
- Bob: The designated verifier.
- p : A large prime.
- q : A prime factor of $p-1$.
- g : A generator $\varepsilon\ Zq^*$ of order q.
- m : A message.
- $H(.)$: A secure one-way hash function such as SHA-2 that outputs values in Zq^*
- (x_A, y_A) : Alice's key pair, where x_A is a randomly selected secret key in Zq^* and the corresponding Public key $y_A = g^{x_A} \bmod p$.
- (x_B, y_B) : Bob's key pair, where x_B is a randomly selected secret key in Zq^* and the corresponding public key $y_B = g^{x_B} \bmod p$.

There are three phases in Lee-Chang's strong designated verifier signature scheme ie. signature generation, signature verification and signature simulation.

3.1 Signature Generation

1) Alice selects a random value $k\ \varepsilon\ Zq^*$;
2) Alice computes r, s and t as follows:

$$\begin{aligned} r &= g^k \bmod p \\ s &= k + x_A r \bmod q \\ t &= H(m, y_B^s \bmod p). \end{aligned}$$

3) The signature is then $\sigma = (r, t)$.

3.2 Signature Verification

Upon receiving m and $\sigma = (r, t)$, Bob can verify the validity of the signature by checking whether

$$t = H(m, (r y_A{}^r)^{x_B} \bmod p).$$

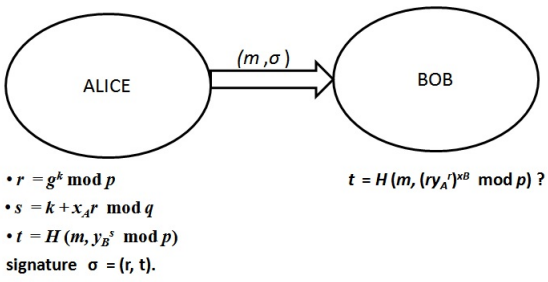

Figure 1: Lee-Chang's scheme

3.3 Signature Simulation

Now Bob can simulate the transcript (r_s, t_s) for the message m by selecting a random number $k_s \; \varepsilon \; Zq^*$ and computes r_s and t_s as follows

$$\begin{aligned} r_s &= g^{ks} \bmod p \\ t_s &= H(m, (r_s {y_A}^{r_s})^{x_B}) \bmod p). \end{aligned}$$

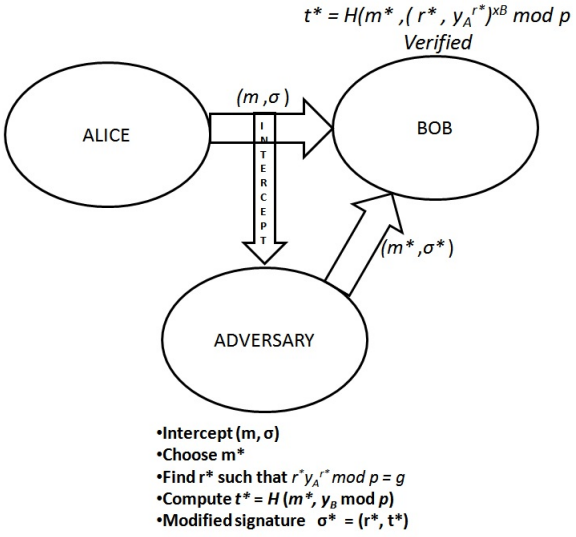

Figure 2: Forgery attack on Lee-Chang's scheme

4 Forgery Attack on Lee-Chang's Scheme

Based on [5] this section shows that Lee-Chang's scheme still cannot withstand forgery attack which an adversary can forge a signature without knowing the secret key of the signer or the designated verifier.

Suppose that an adversary E intercepts the signature m, $\sigma = (r, t)$ sent from Alice to Bob and then E can per-form the following forgery attack:

1) Chooses a forged message m^*.
2) Find an integer r^* which satisfies $r^* y_A^{r^*} \bmod p = g$
3) Compute $t^* = H(m^*, y_B \bmod p)$.
4) Send a forged signature $\sigma^* = (r^*, t^*)$ with m^* to Bob.
5) Upon receiving the forged message m^* and the modified signature $\sigma^* = (r^*, t^*)$, Bob will verify the validity of the signature by checking whether

$$t^* = H(m^*, (r^*, y_A r^*) x_B \bmod p). \quad (1)$$

Its correctness can be seen as follows: Left hand side is

$$t^* = H(m^*, y_B \bmod p)$$

and the right-hand side is

$$\begin{aligned} H(m^*, (r^* y_A^{r^*}) x_B \bmod p) &= H(m^*, (g)^{x_B} \bmod p) \\ &= H(m^*, y_B \bmod p). \end{aligned}$$

We can see that Equation (1) is always confirmed as a legal signature of Alice by Bob. Therefore, Bob will believe that the real singer is Alice. However, the signature $\sigma^* = (r^*, t^*)$ is signed by an adversary E. As a result, since the message m^* is obviously not the Alice's original message m, Lee-Chang's scheme is vulnerable to the forgery attack.Figure 2 shows the attack on Lee-Chang's scheme. The following example taken from [5] shows the forgery attack.

Let the parameters $p = 23, q = 11, g = 2, x = 8$, $y_A = 2^8 \bmod 23 = 3$, then it is easy to find an integer r^* which satisfies $r^* y_A^{r^*} \bmod p = g$. For example, If $r = 4$, then $r^* y_A^{r^*} \bmod p = 4.3^4 \bmod 23 = 324 \bmod 23 = 2 = g$. If $r = 8$, then $r^* y_A^{r^*} \bmod p = 8.3^8 \bmod 23 = 52488 \bmod 23 = 2 = g$. If $r = 13$, then $r^* y_A^{r^*} \bmod p = 13.3^{13} \bmod 23 = 20726199 \bmod 23 = 2 = g$.

5 Improved Scheme

Since Lee-Chang scheme is not secure against forgery attack, in this section we propose an improved scheme which is more secure than the previous one. Figure 3 illustrate the improved scheme.

The common parameters used in the improved scheme can be summarized as follows:

- Alice: The signer;
- Bob: The designated verifier;
- p : A large prime;
- q : A prime factor of $p - 1$;
- g : A generator $\varepsilon \; Zq^*$ of order q which is greater than 2;
- m : A message;
- $H(.)$: A secure one-way hash function such as SHA-2 that outputs values in Zq^*;

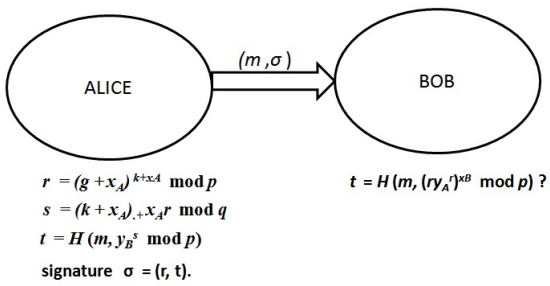

Figure 3: Improved scheme

- (x_A, y_A) : Alice's key pair, where x_A is a randomly selected secret key in Zq^* and the corresponding Public key $y_A = g^{x_A} \bmod p$;
- (x_B, y_B) : Bob's key pair, where x_B is a randomly selected secret key in Zq^* and the corresponding public key $y_B = g^{x_B} \bmod p$.

There are three phases in the improved scheme. The security is enhanced by adding the secret key of Alice in signature generation phase during calculating r and s as follows.

5.1 Signature Generation

1) Alice selects a random value $k \; \varepsilon \; Zq^*$;

2) Alice computes r, s and t as follows:

$$\begin{aligned} r &= (g + x_A)^{k+x_A} \bmod p \\ s &= (k + x_A) + x_A r \bmod q \\ t &= H(m, y_B^s \bmod p). \end{aligned}$$

3) The signature is then $\sigma = (r, t)$.

5.2 Signature Verification

Upon receiving m and $\sigma = (r, t)$, Bob can verify the validity of the signature by checking whether

$$t = H(m, (ry_A{}^r)^{x_B} \bmod p). \quad (2)$$

5.3 Signature Simulation

Now Bob can simulate the transcript (r_s, t_s) for the message m by selecting a random number $k_s \; \varepsilon \; Zq^*$ and computes r_s and t_s as follows.

$$\begin{aligned} r_\Psi &= g^{k_\Psi} \bmod p \\ t_\Psi &= H(m, (r_\Psi y_A^{r_\Psi})^{x_B} \bmod p). \end{aligned}$$

5.4 Correctness Proof

In order to verify the signature as mentioned in Equation (2), we have to prove that

$$t = H(m, (ry_A^r)^{x_B} \bmod p).$$

But $t = H(m, y_B^s \bmod p)$, so if we can prove that $y_B^s = (ry_A^r)^{x_B}$, then Equation (2) is proved.

$$\begin{aligned} (ry_A^r)^{x_B} &= (r(g^{x_A})^r)^{x_B} \\ y_B^s &= y_B^{(k+x_A)+x_A r} \\ &= (g^{x_B})^{(k+x_A)+x_A r} \\ &= (g^{x_B})^{(k+x_A)}.(g^{x_B})^{x_A r} \\ &= (g^{(k+x_A)})^{x_B}.((g^{x_A})^r)^{x_B} \\ &= r^{x_B}.((y_A)^r)^{x_B} \\ &= (ry_A^r)^{x_B}. \end{aligned}$$

So from the above we observe that Equation (2) is proved and the signature is verified.

6 Analysis of The Improved Scheme

6.1 Security Analysis

Basic Unforgeability: Because the problem of getting Private Key x_A from the public key y_A equals to solving DLP, no one else can create normal digital signature of the original signer.

6.2 Unforgeability

Because the private key x_A of the signer Alice is added ie $r = (g + x_A)^{k+x_A} \bmod p$ and $s = (k + x_A) + x_A r \bmod q$, any adversary cannot forge the signature without knowing x_A and also finding x_A from y_A is same as solving DLP which is a hard problem. Therefore our scheme is provably secure.In the previous example of we have seen that Adversary can only forge the signature if he/she find r^* such that $r^* y_A^{r_A^*} \bmod p = g$.

In the improved scheme the private key x_A of the signer Alice is added ie ie $r = (g + x_A)^{k+x_A} \bmod p$ and $s = (k + x_A) + x_A r \bmod q$ in Step-2.

In order to do forgery attack adversary has to guess r^* such that $r^* y_A r^* \bmod p = g + x_A$.

Because of addition of x_A in Step-2 of signature generation adversary cannot guess r^* which satisfies $r^* y_A r^* \bmod p = g + x_A$, as it does not know the value of x_A which is used in signature generation phase,only the original signer knows the value of x_A. Adversary can only forge the signature if and only if he/she get x_A from y_A which is same as DLP a Hard problem with large prime. Hence this proves that our improved scheme is safe and secure.

Table 1: Performance comparison between improved scheme and Lee Chang's scheme

Computations Cost	Lee-Chang's Scheme	Improved Scheme
Signature Generation	2TE+TM+TH	2TE+TM+TH
Signature Verification	2TE+TM+TH	2TE+TM+TH
Signature Simulation	3TE+TM+TH	3TE+TM+TH

TE = Time taken for an exponential operation.
TM = Time taken for a modular multiplication.
TH = Time taken for a one-way hash function.

6.3 Performance Comparison of The Improved Scheme with Lee Chang's Scheme

In this section, we compare the computational costs of different phases of our scheme with those for Lee Chang's scheme. We have compared the computational costs of different phases of our scheme with those for Lee Chang's scheme in Table 1 where TE = Time taken for an exponential operation, TM = Time taken for a modular multiplication and TH = Time taken for a one-way hash function.From this table, we see that both schemes have same computational costs.

7 Conclusions

In this paper, we discuss the drawbacks of Lee Chang's strong designated verifier signature scheme and proposed a new strong designated verifier signature scheme based on DLP.The improved scheme can remedy the weaknesses of Lee Chang's scheme and meets the security aspects needed by the strong designated verifier signature scheme. In other words, the new scheme is more secure than the existing scheme keeping the computational cost same as the previous scheme.

Acknowledgments

We would like to thank the anonymous reviewers for their valuable comments and suggestions which have helped us to improve the contents and presentation of the paper significantly.

References

[1] S. G. Aki, "Digital signatures: a tutorial survey," *Computer*, vol. 16, no. 2, pp. 15–24, 1983.

[2] T. Cao, D. Lin, and R. Xue, "Security analysis of some batch verifying signatures from pairings," *International Journal of Network Security*, vol. 3, no. 2, pp. 138–143, 2006.

[3] M. L. Das, A. Saxena, and D. B. Phatak, "Algorithms and approaches of proxy signature: A survey," *arXiv preprint cs/0612098*, 2006.

[4] X. Huang, W. Susilo, Y. Mu, and F. Zhang, "Short designated verifier signature scheme and its identity-based variant," *International Journal of Network Security*, vol. 6, no. 1, pp. 82–93, 2008.

[5] S. I. Hyun, E. J. Yoon, and K. Y. Yoo, "Forgery attacks on lee-chang's strong designated verifier signature scheme," in *IEEE Second International Conference on Future Generation Communication and Networking Symposia (FGCNS'08)*, vol. 2, pp. 5–8, 2008.

[6] M. Jakobsson, K. Sako, and R. Impagliazzo, "Designated verifier proofs and their applications," in *International Conference on the Theory and Applications of Cryptographic Techniques*, pp. 143–154, 1996.

[7] J. S. Lee and J. H. Chang, "Strong designated verifier signature scheme with message recovery," in *The 9th International Conference on Advanced Communication Technology*, vol. 1, pp. 801–803, 2007.

[8] J. S. Lee and J. H. Chang, "Comment on saeednia et al.'s strong designated verifier signature scheme," *Computer Standards & Interfaces*, vol. 31, no. 1, pp. 258–260, 2009.

[9] M. Li and T. Fang, "Provably secure and efficient id-based strong designated verifier signature scheme with message recovery," in *2014 17th International Conference on Network-Based Information Systems*, pp. 287–293, 2014.

[10] C. Pan, S. Li, Q. Zhu, C. Wang, and M. Zhang, "Notes on proxy signcryption and multi-proxy signature schemes," *International Journal of Network Security*, vol. 17, no. 1, pp. 29–33, 2015.

[11] S. Saeednia, S. Kremer, and O. Markowitch, "An efficient strong designated verifier signature scheme," in *International conference on information security and cryptology*, pp. 40–54, 2003.

[12] C. P. Schnorr, "Efficient signature generation by smart cards," *Journal of Cryptology*, vol. 4, no. 3, pp. 161–174, 1991.

[13] F. Tang, C. Lin, Y. Li, and S. Zhang, "Identity-based strong designated verifier signature scheme with full non-delegatability," in *2011 IEEE 10th International Conference on Trust, Security and Privacy in Computing and Communications*, pp. 800–805, 2011.

[14] H. Tian, "General certificateless strong designated verifier signature schemes," in *2013 5th International Conference on Intelligent Networking and Collaborative Systems*, pp. 392–397, 2013.

[15] G. Wang, F. Bao, C. Ma, and K. Chen, "Efficient authenticated encryption schemes with public verifiability," in *2004 IEEE 60th International Conference on Vehicular Technology (VTC'04)*, vol. 5, pp. 3258–3261, 2004.

[16] Z. Xiao, Bo Yang, and S. Li, "Certificateless strong designated verifier signature scheme," in *2010 IEEE 2nd International Conference on E-business and Information System Security*, pp. 1–5, 2010.

[17] Hu Xiong, Ji Geng, Z. Qin, and G. Zhu, "Cryptanalysis of attribute-based ring signcryption scheme," *International Journal of Network Security*, vol. 17, no. 2, pp. 224–228, 2015.

[18] Bo Yang, Y. Sun, Y. Yu, and Qi Xia, "A strong designated verifier signature scheme with secure disavowability," in *4th International Conference on Intelligent Networking and Collaborative Systems (INCoS'12)*, pp. 286–291, 2012.

[19] F.-Yi Yang and C.-M. Liao, "A provably secure and efficient strong designated verifier signature scheme," *International Journal of Network Security*, vol. 10, no. 3, pp. 220–224, 2010.

[20] X. Zhang, R. Lu, H. Zhang, and C. Xu, "A new digital signature scheme from layered cellular automata," *International Journal of Network Security*, vol. 18, no. 3, pp. 544–552, 2016.

[21] Y. Zheng, "Digital signcryption or how to achieve cost (signature & encryption) cost (signature)+ cost (encryption)," in *Annual International Cryptology Conference*, pp. 165–179, 1997.

Biography

Asif Uddin Khan received BE in Computer Science and Engineering from C.V Raman College of Engineering, Bhubaneswar BPUT, India. M.Tech in Computer Science and Engg from IIIT Bhubaneswar, India.Presently he is working towards his PhD in Computer Science form Department of Computer science, Utkal University, Bhubaneswar, Odisha, India.His research interest includes cryptography and network security, mobile ad-hoc network, software defined network, vehicular ad hoc networks and cloud computing.

Bikram Kesari Ratha born on 20th May 1965. He completed his MCA (Tech) from NIT Rourkela, India in 1988 and subsequently completed his Master Of Engineering (CSE) from the same institute. Under the able guidance of Prof.Rajib Mall of IIT Kharagpur he completed his PhD from Utkal University Bhubaneswar, India. He has teaching experience over 25yeras in several program such as B.E (CSE), MCA, MSc. (CS), M.E. (K.E0, M.Tech(CS) in in different Univeversities and Institutes. He has worked as a Professor in Nepal Engineering College a constituent college of Pokhra University, Kathmandu, Nepal from 2000-2005.During this period he has worked hard to spread IT in the country with active support from His Majesties Government of Nepal. Further he has worked as a Professor in SRTM University's Latur sub centre. During his tenure apart from teaching and research he was actively involved in social work such as empowering women through ICT on various issues by organizing road shows, workshops and drama. He has delivered many invited lectures on the environment, impact of technology on health and society at large. For these activities he has been awarded the best technocrat award by Green Forum an NGO working on environment in the year 2015. He has published about 50 research papers and delivered many talks on cyber space in various forums in India. His research interest is Software Engineering, Data Mining and ICT Applications, Computer Networks,computer security and image Processing.