Remarks on Zhang et al.'s Analysis on a Short Signature Scheme and Their Improvement

Kitae Kim[1], Hyungdon Kim[1], Seungho Kim[2], and Ikkwon Yie[1]
(Corresponding author: Ikkwon Yie)

Department of Mathematics, Inha University, 253, Yonghyun Dong, Nam Gu, Incheon, Republic of Korea[1]
Graduate School of IT&T, Inha University, 253, Yonghyun Dong, Nam Gu, Incheon, Republic of Korea[2]
(Email: ikyie@inha.ac.kr)

(Received Jan. 24, 2011; revised and accepted Nov. 11, 2011)

Abstract

We first give an analysis on Zhang et al.'s attack on a short signature scheme so called ZCSM scheme and point out their forgery attack is not correct one. Furthermore, we present a forgery attack under the chosen message and public key attacks on ZCSM scheme, in the sense of Zhang et al.'s attack. We also analyze Zhang et al.'s improved signature scheme suggested to resist their attacks and point out the proposed scheme, in fact, does not work properly.

Keywords: Cryptanalysis, digital signature, short signature

1 Introduction

Digital signatures allow a signer who has established a public key to sign a message in such a way that any other party who knows the public key, as well as the origin of the public key, can verify that the message originated from the signer and has not been modified [3]. Digital signature schemes are used to ensure the integrity and authenticity in which signatures are publicly verifiable. Moreover, secure digital signature schemes also provide an additional property called the non-repudiation. To be secure, digital signature schemes should be existentially unforgeable, which means that it is infeasible for an attacker to create a valid signature on a message that has not been signed before. As in the case of public key encryption, traditional signature schemes assume an authority called the certificate authority(CA) which has an important role in distribution of public keys of members in the system.

Recently, several digital signature schemes have been proposed by using bilinear pairings to take advantages of such pairings defined in the group of elliptic curves over finite fields. As compared to earlier signature schemes, most of those schemes were turned out to have merits of being shorten the size of signatures. After the breakthrough by Boneh, Lynn and Shacham [2], Zhang, Chen, Susilo, and Mu proposed another short signature scheme under the new hardness assumption called the square roots problem(SRP) [4]. Later, Zhang, Yang, Zhong, Li and Takagi introduced two attacks against Zhang et al.'s scheme, namely a forgery attack and a key replacement attack [5]. Usually, key replacement attacks have been considered in certificateless cryptography(CL-PKC) [1]. Due to the lack of authenticating information for public keys, CL-PKC schemes are sometimes suffer from key replacement attacks in which an adversary has the ability to substitute public keys of members in the system. In order to resist their attacks, Zhang et al., furthermore, suggested an improvement of the Zhang-Chen-Susilo-Mu scheme mentioned above.

In this paper, we revisit Zhang et al.'s forgery attack and key replacement attack on the Zhang-Chen-Susilo-Mu scheme, and make an analysis on their improvement. In fact, they made a mistake in using properties of bilinear pairing, which result in incorrectness of their forgery attack. Moreover, their improved scheme is not correct in that any signature generated by legitimate users cannot be verified whether it is valid or not.

2 Zhang *et al.*'s Attack on the Zhang-Chen-Susilo-Mu Signature Scheme

In this section, we briefly review Zhang-Chen-Susilo-Mu short signature scheme (ZCSM for short), and then give some comments on the cryptanalysis introduced by Zhang, Yang, Zhong, Li and Takagi in [5].

2.1 The ZCSM Short Signature Scheme

Setup: Pick a bilinear group and associate parameters $(G, G_T, \hat{e}, g, q)$ where g is a generator of G and $q \equiv 3 \bmod 4$. The message space is $\mathcal{M} = \{1, \dots, (q-1)/2\}$. The system parameter set is $(G, G_T, \hat{e}, g, q)$.

Key Generation: Pick $x, y \in \mathbb{Z}_q$ at random and compute $u = g^x, v = g^y$. The private key is (x, y) and the corresponding public key is (u, v).

Sign: Given a message $m \in \mathcal{M}$, a user with private key (x, y) generates a signature as follows:

First, randomly picks $r \in \mathbb{Z}_q$;

If m is a quadratic residue modulo q, computes

$$\sigma = g^{(x+my+r)^{1/2}}.$$

Otherwise, if m is a quadratic non-residue modulo q, then computes

$$\sigma = g^{(x-my+r)^{1/2}}.$$

The signature is (σ, r).

Verify: Given a public parameters (G, G_T, q, g), public key (u, v), a message $m \in \mathcal{M}$, and a signature (σ, r) by the following equation:

$$\hat{e}(\sigma, \sigma) = \hat{e}(uv^m g^r, g)$$

or

$$\hat{e}(\sigma, \sigma) = \hat{e}(uv^{-m} g^r, g).$$

2.1.1 Remarks on Zhang et al.'s Attack

In [5], Zhang et al. claimed that ZCSM scheme is not secure against forgery attack and strong key replacement attack. However we found that their forgery attack does not work well. In the following, we describe their attack and point out the reason why the attack is not correct. Furthermore, we show how one can mount such an attack as the authors mentioned.

Zhang et al.'s claimed forgery attack is the following:

"Given a valid signature (σ, r), $(\sigma', r') = (\sigma^2, 2r)$ is a forgery for the forged public key $(u', v') = (u^2, v^2)$".

We first note that the resulting values (σ', r') associated to the public key (u', v') was thought of as a forgery on the (same) message that has been previously signed using public key (u, v), and that, to succeed in forgery attack, the adversary has to replace the public key (u, v) by (u', v'). Such attacks can be considered as a combination of key replacement attack and strong existential forgery attack. On the other hand, traditional digital signature schemes, as well as ZCSM scheme, assume certificate authority implicitly, and those schemes are not designed to provide strong unforgeability security. So, to the best of our knowledge, their claimed attacks might not be practical to ZCSM scheme.

Regardless our above discussion, in the following, we point out that their so-called forgery attack under the chosen message and public key attacks does not correctly operate in the sense that the resulting forgery cannot pass the verify algorithm. Recall that the values $\hat{e}(\sigma', \sigma')$ and $\hat{e}(u'(v')^m g^{r'}, g)$ are as follows:

$$\begin{aligned} \hat{e}(\sigma', \sigma') &= \hat{e}(g^{2(x+my+r)^{1/2}}, g^{2(x+my+r)^{1/2}}) \\ &= \hat{e}(g, g)^{4(x+my+r)}. \\ \hat{e}(u'(v')^m g^{r'}, g) &= \hat{e}(g^{2x}(g^{2y})^m g^{2r}, g) \\ &= \hat{e}(g, g)^{2(x+my+r)}. \end{aligned}$$

In order for (σ', r') to pass the verification algorithm, the two values should be equal. However, since we may assume $x + my + r \not\equiv 0 \pmod{q}$, it is impossible except when $q = 2$. Note also that q was chosen to be an odd prime with $q \equiv 3 \bmod 4$. Therefore, we conclude that their assertion is not true.

Now, we present a correct attack in the sense of Zhang et al.'s attack. Indeed, it is easy to mount such an attack as shown below. Suppose that we are given a signature (σ, r) on a message m generated by using a private key $(u, v) = (g^x, g^y)$. For simplicity, we assume that the message m was chosen from quadratic residues modulo q, since the case where m is a quadratic non-residue modulo q can be treated similarly.

1) Choose a quadratic residue s modulo q with $t^2 = s$ where $s, t \in \mathbb{Z}_q^*$;

2) Set $\sigma' \leftarrow \sigma^t$ and $r' \leftarrow sr$.

Then (σ', r') is verified as valid signature on the message m with respect to the public key $(u', v') = (u^s, v^s)$:

$$\begin{aligned} \hat{e}(\sigma', \sigma') &= \hat{e}(g^{s(x+my+r)}, g) \\ &= \hat{e}(g^{xs} g^{ysm} g^{rs}, g) \\ &= \hat{e}(u'(v')^m g^{r'}, g). \end{aligned}$$

2.2 Zhang-Yang-Zhong-Li-Takagi(ZYZLT) Short Signature Scheme

Zhang et al. suggested an improvement of ZCSM scheme to resist their attacks, and gave its correctness and security proofs [5]. In this subsection, we show their improved signature scheme is not correct in that signatures generated by legitimate users cannot be verified via the verification algorithm.

The ZYZLT scheme is almost the same with ZCSM scheme except for adding $z = \hat{e}(g, g)$ into system parameters, signing and verification algorithms. The Sign and Verify algorithms are described as follows:

Sign: Given a message $m \in \mathcal{M}$, a user with secret key (x, y) produces a signatures as follows:

- randomly picks a $r \in \mathbb{Z}_q$;
- If m is a quadratic residue modulo q, compute $\sigma = g^{\frac{1}{\sqrt{x+my+r}}}$;
- Otherwise, if m is a quadratic non-residue modulo q, then compute $\sigma = g^{\frac{1}{\sqrt{x-my+r}}}$;

The signature is (σ, r).

Verify: Upon receiving public parameters (G, G_T, g, q, z), public key (u, v), a message $m \in \mathcal{M}$, and a signature (σ, r), anyone can verify the validation of the signature by the following equations: $\hat{e}(\sigma^2, ug^m v^r) \overset{?}{=} z$ or $\hat{e}(\sigma^2, ug^{-m} v^r) \overset{?}{=} z$. If either equation holds, it outputs valid. Otherwise, it outputs invalid.

Suppose that (σ, r) is a signature on message m generated by a user with his private key $(u, v) = (g^x, g^y)$. Again, for simplicity, we assume that the message was chosen in the set of quadratic residues. Then

$$\begin{aligned} \hat{e}(\sigma^2, ug^m v^r) &= \hat{e}(g^{\frac{2}{\sqrt{x+my+r}}}, g^x g^m g^r) \\ &= \hat{e}(g^{\frac{2}{\sqrt{x+my+r}}}, g^{x+my+r}) \\ &= \hat{e}(g, g)^{\frac{2(x+my+r)}{\sqrt{x+my+r}}}. \end{aligned}$$

Note that, in their scheme, $x + my + r$ was assumed to be a quadratic residue modulo q, and that $\hat{e}(,)$ is a symmetric and non-degenerate bilinear pairing in which $\hat{e}(g, g)$ has order q. Such pairings are usually constructed from the modified Weil pairing over super-singular curves.

Let us denote $x + my + r \bmod q$ by α. Then $\beta^2 = \alpha$ for some $\beta \in \mathbb{Z}_q^*$ and the last element of G_T in the above equations can be written by $\hat{e}(g, g)^{(2\beta^2)/\beta} = \hat{e}(g, g)^{2\beta}$. In order for the signature (σ, r) to pass the verification test, the following equality should be satisfied:

$$\hat{e}(g, g)^{2\beta} = \hat{e}(g, g).$$

That is, $2\beta \equiv 1 \pmod{q}$ and hence $\beta = 2^{-1} \pmod{q}$. As a result, the verification algorithm outputs "valid" only if the square root of $x + my + r \bmod q$ equals the value $2^{-1} \bmod q$. This is impossible since x and y were randomly selected during key set up phase and r is randomly chosen each time to generate signatures. Therefore, we conclude that no one can verify signatures generated by the signing algorithm and hence ZYZLT scheme is not a correct signature scheme.

3 Conclusions

We have analyzed Zhang et al.'s forgery attack on ZCSM short signature scheme and point out that the attack is not correct one. We then fix the attack to work well in the sense of Zhang et al.'s attack. Furthermore, we show that their improvement cannot be a secure digital signature scheme even though the authors claimed it is proved in the standard model.

Acknowledgments

This research was supported by Basic Science Research Program through the National Research Foundation of Korea(NRF) funded by the Ministry of Education, Science and Technology(2012-0001604).

References

[1] S. S. Al-Riyami and K. G. Paterson, "Certificateless public key cryptography," in *Advances in Cryptology - ASIACRYPT 2003, LNCS 2894*, pp. 452–473, Taipei, Taiwan, November 2003.

[2] D. Boneh, B. Lynn, and H. Shacham, "Short signatures from the weil pairing," in *Advances in Cryptology - ASIACRYPT 2001, LNCS 2248*, pp. 514–532, Gold Coast, Australia, December 2001.

[3] L. H. Li, S. F. Tzeng, M. S. Hwang, "Improvement of Signature Scheme Based on Factoring and Discrete Logarithms," in *Applied Mathematics and Computation*, vol. 161, no. 1, pp. 49–54, Feb. 2005.

[4] F. Zhang, X. Chen, W. Susilo, and Y. Mu, "A new signature scheme without random oracles from bilinear pairings," in *Progress in Cryptology - VIETCRYPT 2006, LNCS 4341*, pp. 67–80, Hanoi, Vietnam, September 2006.

[5] M. Zhang, B. Yang, Y. Zhong, P. Li, and T. Takagi, "Cryptanalysis and fixed of short signature scheme without random oracle from bilinear parings," *International Journal of Network Security*, vol. 12, no. 3, pp. 130–136, 2011.

Kitae Kim was a postdoctoral fellow at Graduate School of IT& T in Inha University. He is a teaching professor of Department of Mathematics in Inha University. His current research interests include theory of algebraic curves, finite fields, and cryptography related to privacy enhancement.

Hyungdon Kim received Ph.D degree in Mathematics from Inha University, Korea. He is currently a teaching professor of Department of Mathematics in Inha University. His research interests include cryptography and finite fields.

Seungho Kim received his B.S. degree in Computer Science from Inha University, and M.S. degree in Graduate School of Information Technology and Telecommunications from the same university. His research interests include network security and cryptographic algorithms.

Ikkwon Yie recieved the B.S. and M.S. degrees in Mathematics from the Seoul National University, Seoul, Korea, and the Ph.D. degree in Mathematics from the Purdue University. He is currently a professor of Department of Mathematics in Inha University. His research interests include Galois theory and digital signatures.