Universal Forgery Attack on a Strong Designated Verifier Signature Scheme

Chien-Lung Hsu[1] and Han-Yu Lin[2]
[1]Department of Information Management, Chang Gung University, Taiwan
[2]Department of Computer Science and Engineering, National Taiwan Ocean University, Taiwan

Abstract: *Based on the bilinear Diffie-Hellman assumption, in 2009, Kang et al. proposed an identity-based strong Designated Verifier Signature (DVS) scheme which only allows the intended verifier to verify the signature. Besides, the designated verifier is not capable of transferring the conviction to any third party. Their scheme was proved secure in the random oracle model. In this paper, however, we will demonstrate that their scheme is still vulnerable to the universal forgery attack for arbitrarily chosen messages. Moreover, an efficient and provably secure improvement to eliminate the security weakness is presented.*

Keywords: *Universal forgery, identity-based, designated verifier, digital signature, bilinear pairing.*

Received September 15, 2012; accepted February 27, 2013; published online February 26, 2014

1. Introduction

In 1996, Jakobsson *et al*. [2] proposed the so-called DVS scheme. In a DVS scheme, anyone can verify the corresponding signature with signer's public key. However, only the intended verifier will be convinced of the signer's identity. Moreover, the designated verifier cannot transfer the conviction to any third party, as he also, has the ability to compute a valid DVS intended for himself. Saeednia *et al*. [7] further proposed a Strong Designated Verifier Signature (SDVS) scheme by combining the designated verifier's private key with the signature verification process, so that only the designated verifier can validate the signature. However, Lee and Chang [6] demonstrated that Saeednia *et al*.'s scheme could not fulfill the property of signer ambiguity in case that signer's private key is accidentally compromised.

Considering the identity-based systems, Susilo *et al*. [8] addressed the first identity-based SDVS scheme from bilinear pairings. Since then, several related works [1, 4, 9] have been proposed. Recently, Kang *et al*. [3] proposed an identity-based SDVS scheme which has not only lower computational costs, but also, shorter signature length. The security of their scheme is formally proved secure in the random oracle model. Yet, in this paper, we will show that their scheme is still vulnerable to the universal forgery attack for arbitrarily chosen messages. Then an efficient countermeasure to resist such an attack without increasing much computational costs is given.

The rest of this paper is organized as follows: section 2 briefly reviews Kang *et al*.'s scheme. We demonstrate the universal forgery attack on their scheme in section 3. An improvement to resist the attack is proposed in section 4. Finally, a conclusion is made in section 5.

2. Review of Kang *et al.*'s Scheme

In this section, we first define used notations in Table 1 and then briefly review Kang *et al*.'s scheme.

Table 1. The used notations.

Z_q	Integers modulo q
$x \in Z_q$	Element x in set Z_q
$x \in_R Z_q$	Element x is a random integer in set Z_q
$x \leftarrow Z_q$	Sampling element x uniformly in set Z_q
$\lvert x \rvert$	Bit-length of integer x, also, absolute value of x

- *Bilinear Pairing*: Let $(G_1, +)$ and $(G_2, \times)$ denote two groups of the same prime order q and $e: G_1 \times G_1 \rightarrow G_2$ be a bilinear map which satisfies the following properties:
  1. *Bilinearity*: For $P, Q \in G_1$ and $a, b \in Z_q$, $e(aP, bQ) = e(P, Q)^{ab}$.
  2. *Non-Degeneracy*: There exists $P, Q \in G_1$ such that $e(P, Q) \neq 1$.
  3. *Computability*: $e(P, Q)$ can be efficiently computed for $P, Q \in G_1$.

Kang *et al*.'s scheme is composed of five phases (Setup, KeyExtract, Sign, Verify, Transcript simulation) described as follows:

- *Setup*: The Private Key Generation center (PKG) chooses a master secret key $s \in_R Z_q$, computes the corresponding public key $P_{TA} = sP$ and then selects two groups $(G_1, +)$ and $(G_2, \times)$ of the same prime order q. Let P be a generator of order q over G_1, $e: G_1 \times G_1 \rightarrow G_2$ a bilinear pairing, $H: \{0, 1\}^* \rightarrow G_1$ and $F: \{0, 1\}^* \rightarrow Z_q$ cryptographic hash functions [5]. The PKG announces public parameters *params* $= \{P_{TA}, G_1, G_2, q, P, e, H, F\}$

- *KeyExtract*: Given an identity ID, the PKG computes the private key $S_{ID} = sQ_{ID}$ where $Q_{ID} = H(ID)$ is the corresponding public key. The private key is then sent to the user via a secure channel.
- *Sign*: Let Alice be a signer and Bob the designated verifier. For signing a message m intended for Bob, Alice chooses $k \in_R Z_q$ to compute:

$$t = e(P, Q_B)^k \tag{1}$$

$$T = kP + F(m, t)S_A \tag{2}$$

$$\sigma = e(T, Q_B) \tag{3}$$

  The SDVS for m is (t, σ).
- *Verify*: Given (m, t, σ), Bob verifies whether:

$$\sigma = t \cdot e(Q_A, S_B)^{F(m,\, t)} \tag{4}$$

  If it holds, Bob is convinced that (t, σ) is a valid SDVS for m.
- *Transcript Simulation*: To generate another SDVS intended for himself, Bob first chooses $k^* \in_R Z_q$ and then computes $t^* = e(P, Q_B)^{k^*}$ and $\sigma^* = t^* \cdot e(Q_A, S_B)^{F(m,\, t^*)}$. The derived (t^*, σ^*) is another valid SDVS for m.

3. Universal Forgery Attack on Kang *et al.*'s Scheme

To launch the universal forgery attack on Kang *et al.*'s scheme for an arbitrarily chosen message m'', a malicious adversary first intercepts an SDVS intended for Bob, say (m, t, σ), and then chooses $t'' \in_R G_2$ to compute:

$$\sigma'' = t'' \cdot ((t^{-1}\sigma)^{F(m,\, t)^{-1}})^{F(m'',\, t'')} \tag{5}$$

The forged SDVS for m'' is (t'', σ''). We claim that (t'', σ'') will pass the signature verification, as the shared secret between Alice and Bob can be easily derived by computing:

$$e(Q_A, S_B) = (t^{-1}\sigma)^{F(m,\, t)^{-1}} \tag{6}$$

Consequently, Bob will believe that the forged SDVS (t'', σ'') for m'' is generated by Alice.

4. An Efficient and Provably Secure Improvement

To withstand above universal forgery attacks, we can adopt a cryptographic hash function, h: $G_2 \rightarrow G_2$, to rewrite Equation 3 as:

$$\sigma = h(e(T, Q_B)) \tag{7}$$

Then the corresponding Equation 4 would become:

$$\sigma = h(t \cdot e(Q_A, S_B)^{F(m,\, t)}) \tag{8}$$

Hence, the universal forgery attack cannot work any longer in the improved mechanism, as any malicious adversary is not able to derive the shared secret $e(Q_A, S_B)$. The underlining security notion of Kang *et al.*'s scheme and our improvement is based on the Bilinear Diffie-Hellman Problem (BDHP) stated below:

- *Bilinear Diffie-Hellman Problem*: The BDHP is, given an instance $(P, X, Y, Z) \in G_1^4$ where P is a generator, $X = xP$, $Y = yP$ and $Z = z$
- P for some $x, y, z \in Z_q$, to compute $e(P, P)^{xyz} \in G_2$.
- *Bilinear Diffie-Hellman (BDH) Assumption*: For every probabilistic polynomial-time algorithm D, every positive polynomial $Q(\cdot)$ and all sufficiently large k, the algorithm D can solve the BDHP with the advantage at most $1/Q(k)$, i. e., $\Pr[D(P, xP, yP, zP) = e(P, P)^{xyz};\ x, y, z \leftarrow Z_q,\ (P, xP, yP, zP) \leftarrow G_1^4] \leq 1/Q(k)$.

The probability is taken over the uniformly and independently chosen instance and over the random choices of $\mathcal{D}$.

- *Definition 1*: The (t, ε)-BDH assumption holds if there is no polynomial-time adversary that can solve the BDHP in time at most t and with the advantage ε.

By applying the similar proof techniques of Kang *et al.*'s scheme, we can also, formally prove the security of our improved mechanism in the random oracle model as follows:

- *Theorem 1*: The improved SDVS scheme is $(t, q_H, q_F, q_h, q_{Extract}, q_S, q_V, \varepsilon)$-secure against EF-CMA in the random oracle model if there is no probabilistic polynomial-time adversary that can (t', ε')-break the BDHP, where: $\varepsilon' \geq 2(\varepsilon - 2^{-|G_2|})(q_S^2 - q_S)^{-1}$, $t' \approx t + t_\lambda(2q_S + q_V)$.

Here, t_λ is the time for performing one bilinear pairing operation.

- *Proof*: Suppose that a probabilistic polynomial-time adversary D can $(t, q_H, q_F, q_h, q_{Extract}, q_S, q_V, \varepsilon)$ - break the improved SDVS scheme with non-negligible advantage ε under adaptive chosen message attacks after running at most t steps and making at most q_H H, q_F F, q_h h, $q_{Extract}$ KeyExtract, q_S Sign and q_V Verify oracle queries. Then we can construct another algorithm C that can (t', ε') - break the BDHP by taking D as a subroutine. The objective of C is to obtain $e(P, P)^{abc}$ by taking (P, aP, bP, cP) as inputs. For all the queries of (H, F, KeyExtract, Sign, Verify), C responds as those defined in Kang *et al.*'s scheme, i. e., $P_{TA} = bP$, $Q_A = aP$, $Q_B = cP$, *etc.,*When D queries an h oracle of $h(z)$, C first checks the h_list for a matched entry. Otherwise, C chooses $v \in_R G_2$, adds the entry (z, v) to the h_list, and returns v as a result.

Finally, D outputs a valid forgery (t^*, σ^*) for m^* with respect to the signer's identity ID_i and the designated verifier's identity ID_j. C first searches the h_list for a matched entry (z, σ) where $\sigma = \sigma^*$ and then outputs the value $(t^{*-1}z)^{F(m^*,\, t^*)^{-1}} = e(P, P)^{abc}$ as the answer to the BDHP. The probability that D guesses the correct random value without asking $h(z^*)$ oracle is not greater than $2^{-|G_2|}$. Besides, the probability that $(i, j) = \{(A, B)$ or $(B, A)\}$ is $2(q_S(q_S - 1))^{-1} = 2(q_S^2 - q_S)^{-1}$. Therefore, we can express the probability that C solves the BDHP as $\varepsilon' \geq 2(\varepsilon - 2^{-|G_2|})(q_S^2 - q_S)^{-1}$. The computational steps required for C are $t' \approx t + t_\lambda(2q_S + q_V)$.

5. Conclusions

Although, Kang *et al.*'s identity-based SDVS scheme has the advantages of lower computational costs and shorter signature length. They also, formally proved the security of their scheme in the random oracle model. Nevertheless, we demonstrated that their scheme still cannot resist universal forgery attacks for arbitrarily chosen messages. Additionally, we gave an efficient and provably secure improvement by adopting a cryptographic hash function to eliminate such a security weakness. It is evident that the improved mechanism also, preserves the computational and communicational merits of Kang *et al.*'s scheme.

Acknowledgment

We would like to thank anonymous referees for their valuable suggestions. We thank HARC of Chang Gung University for excellent technical assistance. This work was supported in part by the Chang Gung University Grant UARPD3B0061 and in part by the National Science Council of Republic of China under the contract numbers NSC 100-2628-H-182-001-MY3 and NSC 101-2218-E-019-005.

References

[1] Huang X., Susilo W., Mu Y., and Zhang F., "Short Designated Verifier Signature Scheme and its Identity-Based Variant," *the International Journal of Network Security*, vol. 6, no. 1, pp. 82 - 93, 2008.

[2] Jakobsson M., Sako K., and Impagliazzo R., "Designated Verifier Proofs and their applications," *in Proceedings of Advances in Cryptology-EUROCRYPT*, Berlin, Germany, pp. 143 - 154, 1996.

[3] Kang B., Boyd C., and Dawson E., "A Novel Identity-Based Strong Designated Verifier Signature Scheme," *the Journal of Systems and Software*, vol. 82, no. 2, pp. 270 - 273, 2009.

[4] Kumar K., Shailaja G., and Saxena A., "Identity Based Strong Designated Verifier Signature Scheme," *Cryptology ePrint Archive*, available at: http://eprint.iacr.org/2006/134, last visited 2006.

[5] Lakshmanan T. and Muthusamy M., "A Novel Secure Hash Algorithm for Public Key Digital Signature Schemes," *the International Arab Journal of Information Technology*, vol. 9, no. 3, pp. 262 - 267, 2012.

[6] Lee S. and Chang H., "Comment on Saeednia *et al.*'s Strong Designated Verifier Signature Scheme," *Computer Standards & Interfaces*, vol. 31, no. 1, pp. 258 - 260, 2009.

[7] Saeednia S., Kremer S., and Markowitch O., "An Efficient Strong Designated Verifier Signature Scheme," *in Proceedings of the 6th International Conference on Information Security and Cryptology*, Seoul, Korea, pp. 40 - 54, 2003.

[8] Susilo W., Zhang F., and Mu Y., "Identity-Based Strong Designated Verifier Signature Schemes," *in Proceedings of the 9th Australasian Conference on Information Security and Privacy*, Sydney, Australia, vol. 3108, pp. 313 - 324, 2004.

[9] Zhang J. and Mao J., "A Novel ID-Based Designated Verifier Signature Scheme," *Information Sciences*, vol. 178, no. 3, pp. 766 - 773, 2008.

Chien-Lung Hsu received a BS degree in business administration, an MS degree in information management, and a PhD degree in information management from the National Taiwan University of Science and Technology, Taiwan in 1995, 1997, and 2002, respectively. He was an Assistant Professor and an Associate Professor in the Department of Information Management, Chang Gung University (CGU), Taiwan from 2004 to 2007 and from 2007 to 2011, respectively. Currently, he is a Professor in the Department of Information Management, Chang Gung University since 2011. He is also, the leader of the Ubiquitous Security and Applications Lab, the director of Chinese Cryptology Information Security Association (CCISA, Taiwan), the chair of Education Promotion Committee of CCISA, the member of Academia-Industry Cooperation Committee of CCISA, the chair of Program of RFID Applications in Logistics Supply Chain Management of CGU, the chair of Program of Information Security with Medical Applications of CGU, the director of Division of Instructional Support of Computer Center of CGU, the researcher of Healthy Aging Research Center (HARC) of CGU, the researcher of Elder Industry Development and Research Center (EIDRC) of CGU, and the senior researcher of Taiwan Information Security Center (TWISC). His current research includes cryptography, information security, wireless sensor network, mobile commerce, digital forensics, vehicular system security, healthcare system and user acceptance, smart home system, and etc.

Han-Yu Lin received BA degree in economics from the Fu-Jen University, Taiwan in 2001, his MS degree in information management from the Huafan University, Taiwan in 2003, and his PhD degree in computer science and engineering from the National Chiao Tung University, Taiwan in 2010. He has been an Assistant Professor in the Department of Computer Science and Engineering of National Taiwan Ocean University since August 2012. His research interests include cryptology, network security, digital forensics, cloud computing security and e-commerce security.