Attack on Kang et al.'s Identity-Based Strong Designated Verifier Signature Scheme

Hongzhen Du[1,2] and Qiaoyan Wen[1]

1 School of Science, Beijing University of Posts and Telecommunications,
Beijing 100876, China
2 Mathematics Departments, Baoji University of Arts and Sciences,
Baoji 721007, China
E-mail: duhongzhen@gmail.com

Abstract: In this paper, we propose a universal forgery attack on Kang et al.'s identity-based strong designated verifier signature (IBSDVS) scheme. We show any one can forge a valid IBSDVS on an arbitrary message without the knowledge of the private key of either the signer or the designated verifier.

Keywords: designated verifier signature, bilinear pairings, cryptanalysis

1 Introduction

Designated verifier signature (DVS) was first proposed by Jakobsson et al. [1] at Eurocrypt'96. Such signatures provide message authentication without non-repudiation and with the property that only designated recipient can check their validity. Designated verifier signatures have several applications such as E-voting, call for tenders and software licensing. In 2003, Saeednia et al. [2] introduced a strong designated verifier signature (SDVS), which forces the designated verifier to use his secret key at the time of verification. Thus, nobody but the designated verifier can verify the SDVS.

Recently, Kang et al. [3] proposed a new identity-based strong designated verifier signature (IBSDVS) scheme. They claimed that their scheme was secure and more efficient than previous schemes [4, 5, 6]. However, we present an attack on their scheme. We show that any one can forge an IBSDVS for any message.

2 Review of Kang et al.'s ID-based Strong Designated Verifier Signature Scheme

We first review Kang et al.'s IBSDVS scheme [3] in brief.

- **Setup**: A bilinear map e: $G_1 \times G_1 \rightarrow G_2$, for G_1 and G_2 are groups of same prime order q. And P is a generator of group G_1. Then, a Private Key Generation centre (PKG) picks a random $s \in Z_q^*$ as the master key and computes the corresponding public key $P_{pub} = sP$. H_1 and H_2 are cryptographic hash functions such that H_1: $\{0, 1\}^* \rightarrow G_1$ and H_2: $\{0, 1\}^* \rightarrow Z_q^*$. The system parameters are *params*= $<q$, G_1, G_2, e, P, P_{pub}, H_1, $H_2>$.
- **Key-Extract**: Given a user's identity ID, PKG computes $Q_{ID} = H_1(ID)$ and outputs the user's private key $d_{ID} = sQ_{ID}$.

  Assume that Alice is the signer and Bob is the designated verifier, and Alice and Bob have their private/public key pairs (d_A, Q_A) and (d_B, Q_B), respectively.
- **IBSDVS- Sign**: To sign a message m for Bob, Alice performs as below.

  1. Choose a random value $k \in Z_q^*$ and compute $t = e(P, Q_B)^k$.
  2. Set $h = H_2(m, t)$.
  3. Compute $T = kP + hd_A$ and $\sigma = e(T, Q_B)$.

  The signature on the message m is (t, σ).
- **IBSDVS-Verify**: Given *params*, the signer's public key Q_A and the signature (t, σ) on m, Bob sets $h = H_2(m, t)$ and accepts the signature if and only if the following equation holds.

$$\sigma = te(Q_A, d_B)^h$$

- **IBSDVS-Simulation**: Bob can produce the signature (t, σ) intended for himself, by performing the following:

  1. Choose a random value $k' \in Z_q^*$ and compute $t' = e(P, Q_B)^{k'}$.

2. Set $h' = H_2(m, t')$.

3. Compute $\sigma' = t'e(Q_A, d_B)^{h'}$.

Then, the tuple (t', σ') is a valid signature on message *m*.

About the correctness and the security analysis of the scheme refer to [3].

3 Cryptanalysis of Kang et al.'s IBSDVS Scheme

In this section, we propose a universal forgery attack on Kang et al.'s scheme.

Assume that Charlie is an adversary without the knowledge of the private keys of both Alice and Bob. But he can forge a valid IBSDVS on an arbitrary message as follows:

After obtaining a message-signature pair (m, (*t*, *σ*)) (It is easy), Charlie performs as below:

1. Compute $h = H_2(m, t)$.
2. Compute $e(Q_A, d_B) = (\frac{\sigma}{t})^{h^{-1}}$.

Then, Charlie can produce Alice's signature on any message using *e* (Q_A, d_B).

- IBSDVS- Sign: To sign a message *m* for Bob on behalf of the signer Alice, Charlie performs as below.

1. Choose a random value $k \in Z_q$* and compute $t = e(P, Q_B)^k$.

2. Set $h = H_2(m, t)$.

3. Compute $\sigma = te(Q_A, d_B)^h$.

The signature on the message *m* is (*t*, *σ*).The forged message-signature pair (*m*, (*t*, *σ*)) can be accepted by the designated verifier Bob since the verifying equality $\sigma = te(Q_A, d_B)^h$ always holds.

Hence, Kang et al's scheme is universal forgeable.

Our Improvement

To prevent this attack, a simple method is to add *e* (Q_B, d_A) to hash function. That is, we replace $h = H_2(m, t)$ by $h = H_2(m, t, e(Q_B, d_A))$ in the whole IBSDVS scheme. In such a way, our attack can be avoided.

4 Conclusion

We show that Kang et al's IBSDVS scheme [3] is not secure. In addition, we present an improved scheme for scheme [3] and the improved scheme satisfies security properties of unforgeability, source hiding and non-delegatability.

References

1. M. Jakobsson, K. Sako, K. R. Impaliazzo. Designated verifier proofs and their applications. In Eurocrypt 1996, LNCS 1070, Springer-Verlag, 1996, pp. 142-154.
2. S. Saeednia, S. Kreme, O. Markotwich. An efficient strong designated verifier signature scheme. CICS 2003, LNCS 2971, Springer-Verlag, 2003, pp. 40-54.
3. B. Kang, C. Boyd, E. Dawson. A novel identity-based strong designated verifier signature scheme, The Journal of Systems and Software (2008), doi: 10.1016/j.jss.2008.06.014.
4. K. Phani Kumar, G. Shailaja, Ashutosh Saxena. Identity based strong designated verifier signature scheme. http//www.eprint.iacr.org/2006/134.
5. W. Susilo, F. Zhang, Y. Mu. Identity-based strong designated verifier signature schemes, ACISP 2004, LNCS 3108, pp. 313-324.
6. J. Zhang, J. Mao, A novel ID-based designated verifier signature scheme, Information Science, 178(3), 2008, pp. 766-773.