A universal forgery of Hess's second ID-based signature against the known-message attack

Jung Hee Cheon

Information and Communications University (ICU), Taejon, Republic of Korea
jhcheon@icu.ac.kr, http://vega.icu.ac.kr/ jhcheon

March, 3rd. 2002

Abstract. In this paper we propose a universal forgery attack of Hess's second ID-based signature scheme against the known-message attack.

Keywords: ID-based signature, Elliptic curve, Bilinear maps

Recently, several ID-based signature schemes based on binary maps on elliptic curves were proposed [CC02,Hes02,Pat02,SOK01]. In [Hes02], he proposed two ID-based signature schemes and provided a formal proof for the first scheme, but only sketch of proof for the second scheme. In this paper, we propose a universal forgery attack of Hess's second ID-based signature scheme against the known-message attack.

First, we introduce Hess's second ID-based signature scheme.

Let $(G, +)$ and $(V, \cdot)$ be groups of prime order ℓ and $e : G \times G \to V$ be a bilinear non-degenerate pairing. We further assume two hash functions $H : \{0,1\}^* \to G \setminus \{0\}$ and $h : \{0,1\}^* \times G \to \mathbb{F}_l^*$.

1. **Setup**. The TA picks a random element $P \in G \setminus \{0\}$ and a secret integer $t \in \mathbb{F}_l^*$. The TA then compute
$$Q_{TA} = tP$$
and publishes (P, Q_{TA}). The value t is stored by the TA.
2. **Extract**. Given an identity ID of a user, the algorithm computes his public key $Q_{ID} = H(ID)$ and his private key $S_{\mathrm{ID}} = tQ_{ID}$.
3. **Sign**. To sign a message m the signer picks a random integer $k \in \mathbb{F}_l^*$ and then compute
   (a) $r = kP$
   (b) $v = h(m, r)$
   (c) $u = (v/k)S_{ID}$
4. **Verify**. On receiving a message m and signature (u, r) the verifier computes:
   (a) $v = h(m, r)$
   (b) Accept the signature if and only if $e(u, r) = e(Q_{ID}, Q_{TA})^v$.

This completes the description of the second ID-based signature scheme. That this verification equation holds for a valid signature follows from the following algebra:

$$e(u, r) = e((v/k)S_{ID}, kP) = e(S_{ID}, P)^v = e(Q_{ID}, Q_{TA})^v.$$

Now, we give a universal forgery attack of the above ID-based signature scheme against the known-message attack.

Assume we have a valid signature (u, r) of a message m. For arbitrary message m', compute $v' = h(m', r)$ and $v = h(m, r)$. Also, we compute $u' = (v'/v)u = (v'/k)S_{ID}$. Then (u', r) is a valid signature of m' since

$$e(u', r) = e((v'/k)S_{ID}, kP) = e(S_{ID}, P)^{v'} = e(Q_{ID}, Q_{TA})^{v'}$$

and $v' = h(m', r)$.

References

[CC02] J. Cha and J. Cheon, *An Identity-Based Signature from Gap Diffie-Hellman Groups*, Available from `http://eprint.iacr.org`, 2002.

[Hes02] F. Hess, *Exponent group signature schemes and efficient identity based signature schemes based on pairings*, Available from `http://eprint.iacr.org`, 2002.

[Pat02] K. Paterson, *ID-based signatures from pairings on elliptic curves*, Available from `http://eprint.iacr.org`, 2002.

[SOK01] R. Sakai, K. Ohgishi, and M. Kasahara, *Cryptosystems based on pairing*, Proc. of SCIS '00, Okinawa, Japan, Jan. pp. 26-28, 2001.