Attack on Okamoto *et al.*'s New Short Signature Schemes

Fangguo Zhang[1] and Xiaofeng Chen[2]

[1] Department of Electronics and Communication Engineering,
Sun Yat-Sen University, Guangzhou 510275, P.R.China
isdzhfg@zsu.edu.cn
[2] Department of Computer Science,
Sun Yat-Sen University, Guangzhou 510275, P.R.China
isschxf@zsu.edu.cn

Abstract. We present an attack on a new short signature scheme from bilinear pairing proposed by Okamoto *et al.* at ITCC'05. We show that any one can derive the secret key of the signer from any two message-signature pairs and so can forge the signer's signature for any message. This means the scheme is totally broken.

Keywords: Short Signature, Bilinear Pairing, Cryptanalysis.

1 Introduction:

Digital signature schemes allow a signer to transform any arbitrary message into a signed message, such that anyone can verify the validity of the signed message using the signer's public key, but only the signer can generate signed messages.

Proxy signature is a type of signature, it was first introduced by Mambo, Usuda, and Okamoto in 1996 [3]. The proxy signature schemes allow proxy signers to sign messages on behalf of an original signer. Such signatures have found numerous applications, particularly in distributed computing where delegation of rights is quite common.

Short digital signatures are always desirable. They are necessary in situations in which humans are asked to manually key in the signature or when working in low-bandwidth communication environments. They are also useful in general to reduce the communication complexity of any transmission.

Recently, T. Okamoto, A. Inomata and E. Okamoto proposed a new and short signature scheme at ITCC'05, they also proposed a new proxy signature scheme based on their signature scheme. They claimed that their schemes were secure and efficient, especially for signing phase. However, in this letter, we present an attack on Okamoto *et al.*'s short signature scheme. We show that any one can derive the secret key of the signer from two message-signature pairs and so can forge signature for any message. Since Okamoto *et al.*'s proxy signature scheme is based on their new signature scheme, so the proxy signature scheme is not secure too.

2 Okamoto *et al.*'s New Short Signature Scheme

We first review Okamoto *et al.* [4]'s short signature scheme at ITCC'05 in brief.

Let $\mathbb{G}_1$ be an additive group whose order is a prime q, and $\mathbb{G}_2$ be a multiplicative group of the same order q. Let $e : \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$ be the bilinear pairing with the following properties (For more knowledge about bilinear pairing, refer to [1, 2]):

1. **Bilinearity:** $e(aP, bQ) = e(P, Q)^{ab}$ for all $P, Q \in \mathbb{G}_1, a, b \in \mathbb{Z}_q$
2. **Non-degeneracy:** There exists $P, Q \in G_1$ such that $e(P, Q) \neq 1$, in other words, the map does not send all pairs in $\mathbb{G}_1 \times \mathbb{G}_1$ to the identity in $\mathbb{G}_2$;
3. **Computability:** There is an efficient algorithm to compute $e(P, Q)$ for all $P, Q \in \mathbb{G}_1$.

Let P be a generator of $\mathbb{G}_1$.

The system parameters are $(\mathbb{G}_1,\ \mathbb{G}_2,\ e,\ q,\ P, \mathcal{H})$, here $\mathcal{H} : \{0, 1\}^* \rightarrow \mathbb{Z}_q$ is a hash function.

Key Generation. Randomly select $r, s \in_R \mathbb{Z}_q^*$, and compute $g = e(P,\ P)$, $V_1 = sP$, $v_2 = g^r$ and $S = \frac{1}{s}P$. The public key is $(g,\ V_1,\ v_2)$. The secret key is (r, S).

Signing: Given a message m, compute $e = \mathcal{H}(m)$ and $\sigma = (r + e)S$. The signature for the message m is σ.

Verification: Compute $e = \mathcal{H}(m)$ and verify that

$$e(V_1,\ \sigma) = v_2 g^e.$$

About the correctness and the security analysis of the scheme refer to [4].

3 Cryptanalysis of Okamoto *et al.*'s Signature Scheme

In this section, we show that Okamoto *et al.*'s signature scheme is not secure. Any one can recover the secret key of the signer from any two message-signature pairs and so can forge the signer's signature for any message.

Assume that $\mathcal{A}$ is an adversary. The details of this cryptanalysis are described as follows:

$\mathcal{A}$ obtains two different message-signature pairs (this is easy), e.g., (m_1, σ_1) and (m_2, σ_2), then $\mathcal{A}$ can compute

$$((\mathcal{H}(m_1) - \mathcal{H}(m_2))^{-1} \bmod q)(\sigma_1 - \sigma_2).$$

In fact, this is the secret key S of the signer. This is because

$$\begin{aligned}
&((\mathcal{H}(m_1) - \mathcal{H}(m_2))^{-1} \bmod q)(\sigma_1 - \sigma_2) \\
&= (e_1 - e_2)^{-1}((r + e_1)S - (r + e_2)S) \\
&= (e_1 - e_2)^{-1}(e_1 S - e_2 S) \\
&= S
\end{aligned}$$

Then $\mathcal{A}$ can obtain $rS = \sigma_1 - \mathcal{H}(m_1)S$. Now, $\mathcal{A}$ can forge the signer's signature for any message using $S,\ rS$: For any message m, $\mathcal{A}$ can forge the signature as $\sigma = rS + \mathcal{H}(m)S$. This means that we totally broke Okamoto *et al.*'s short signature scheme. Our attack can be used to break Okamoto *et al.*'s proxy signature scheme because the proxy signer uses Okamoto *et al.*'s short signature scheme to issue proxy signature, so their proxy signature scheme is not secure too.

4 Conclusion:

Short signatures are important in low-bandwidth communication environments. In this letter, we showed that Okamoto *et al.*'s short signature scheme from bilinear pairing proposed at ITCC'05 is not secure. We proposed an attack on it such that any one can derive the secret key of the signer from any two message-signature pairs.

References

1. D. Boneh and M. Franklin, *Identity-based encryption from the Weil pairing*, Advances in Cryptology-Crypto 2001, LNCS 2139, pp.213-229, Springer-Verlag, 2001.
2. D. Boneh, B. Lynn, and H. Shacham, *Short signatures from the Weil pairing*, In C. Boyd, editor, Advances in Cryptology - Asiacrypt 2001, LNCS 2248, pp.514-532, Springer-Verlag, 2001.
3. M. Mambo, K. Usuda, and E. Okamoto, *Proxy signature: Delegation of the power to sign messages*, In IEICE Trans. Fundamentals, Vol. E79-A, No. 9, Sep., pp. 1338-1353, 1996.
4. T. Okamoto, A. Inomata and E. Okamoto, *A proposal of short proxy signature using pairing*, In the proceedings of the International Conference on Information Technology: Coding and Computing (ITCC05), pp. 631- 635, 2005.