Applied Mathematics & Information Sciences
An International Journal

Cryptanalysis of an ID-based proxy signature scheme with message recovery

M. Tian, L. Huang and W. Yang

School of Computer Science and Technology, University of Science and Technology of China, Hefei 230026, China

Received: Dec. 13, 2011; Revised Feb. 4, 2012; Accepted Feb. 16, 2012
Published online: 1 Sep. 2012

Abstract: ID-based message recovery signature is a kind of lightweight signature. In such a signature scheme, a complicated certification system is discarded and the total length of the message and the appended signature is also shortened. Proxy signature allows an original signer to delegate a proxy signer to sign messages on its behalf, which has found numerous practical applications such as grid computing and mobile agent systems. Recently, Singh and Verma proposed the first ID-based proxy signature scheme with message recovery. They proved that their scheme is secure in the random oracle model and believed that it can be used widely. Unfortunately, by giving two concrete attacks, we demonstrate that their ID-based message recovery proxy signature scheme is not secure. The result implies that the security for ID-based message recovery proxy signature schemes needs to be carefully examined.

Keywords: Cryptanalysis, ID-based cryptography, Message recovery, Proxy signature.

1. Introduction

Digital signature scheme with message recovery is a kind of useful signature scheme, in which the message itself is not required to be transmitted together with a signature. In fact, the message is embed in the signature and can be recovered by anyone according to the verification/message-recovery process. In this way, the total length of the message and the appended signature can be shortened. Such signature schemes are usually used when small messages should be signed. For instance, to sign a postcard, one can employ the signature scheme to minimize the total length of the message and the appended signature.

In 2005, Zhang *et al.* [1] proposed the first ID-based message recovery signature scheme. In this scheme, a user's public key can be derived from his identity (e.g., his name or email address) and his secret key is generated by a trusted third party called the Private Key Generator (PKG). Therefore, ID-based message recovery signatures are more compelling since they avoid to employ a complicated certification system which is mandatory in traditional message recovery signature schemes.

The concept of proxy signature was introduced by Mambo *et al.* [2] in 1996. Proxy signatures allow an original signer to delegate a proxy signer to sign messages on its behalf. Proxy signature schemes have found numerous applications such as grid computing [3] and mobile agent systems [4,5]. Recently, combining the advantages of ID-based message recovery signatures and proxy signatures, Singh and Verma [6] proposed an ID-based proxy signature scheme with message recovery. They proved its security in the random oracle model and believed that it can be used in wireless e-commerce, mobile agent systems and mobile communication. Unfortunately, by giving two concrete attacks, we will show that their ID-based message recovery proxy signature scheme is not secure.

The rest of this paper is organized as follows. In Section 2, we present some preliminaries used throughout the paper. We review Singh-Verma ID-based proxy signature scheme with message recovery in Section 3. Two concrete attacks on their scheme are provided in Section 4. Finally, we conclude this paper in Section 5.

2. Preliminaries

2.1. Bilinear pairing

Let $\mathbb{G}_1$ and $\mathbb{G}_2$ be two cyclic groups of the same prime order q. We will view $\mathbb{G}_1$ as an additive group and $\mathbb{G}_2$ as a

* Corresponding author: miaotian@mail.ustc.edu.cn

multiplicative group. A bilinear pairing is a map $e : \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$ with the following three properties.
Bilinearity: For all $a, b \in \mathbb{Z}$ and $P, Q \in \mathbb{G}_1$, the map $e : \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$ satisfies $e(aP, bQ) = e(P, Q)^{ab}$.
Non-degeneracy: There are $P, Q \in \mathbb{G}_1$ such that $e(P, Q) \neq 1$.
Computability: There exists an efficient algorithm to compute $e(P, Q)$ for all $P, Q \in \mathbb{G}_1$.

2.2. Scheme Model

An ID-based proxy signature scheme with message recovery consists of the following eight probabilistic polynomial-time algorithms:
Setup. On input a security parameter λ, the PKG generates a master secret key MSK and the public parameters PP. Here PP contains the PKG's public key P_{pub}.
Extract. On input the master secret key MSK and user identity ID_i, the PKG generates a secret key d_i for the user.
Delegate. On input the original signer ID_A's secret key d_A and a delegation warrant m_w which records the delegation police and the identities of the original signer and the proxy singer. The original signer generates a delegation $W_{A\rightarrow B}$ for the proxy signer ID_B.
DVerify. Given the public parameters PP, the original signer's identity ID_A and the delegation $W_{A\rightarrow B}$, the proxy signer ID_B accepts the delegation $W_{A\rightarrow B}$ if it's valid; otherwise, he requests a valid one from ID_A or terminates the protocol.
PKGen. On input the public parameters PP, the delegation $W_{A\rightarrow B}$ and the proxy signer ID_B's secret key d_B, this algorithm outputs ID_B's proxy signing key d_p.
PSign. On input a message m, the delegation $W_{A\rightarrow B}$ and the proxy signing key d_p, this algorithm outputs a proxy signature δ on m.
Verify. On input a signature δ, two identities ID_A and ID_B, a verifier accepts the signature if δ is a valid one, and rejects it otherwise.
ID. On input a valid proxy signature δ, this algorithm outputs the identity ID_B of the proxy signer.

2.3. Notations

The following notations will be used throughout this paper.
$a||b$: a concatenation of two strings a and b.
$\oplus$: X-OR computation in the binary system.
$[x]_{10}$: the decimal representation of $x \in \{0, 1\}^*$.
$[y]_2$: the binary representation of $y \in \mathbb{Z}$.
${}_{l_1}|\beta|$: the first l_1 bits of β from the left side.
$|\beta|_{l_2}$: the first l_2 bits of β from the right side.
$\mathbb{G}_1, \mathbb{G}_2$: two cyclic groups of the same order q, where $|q| = l_1 + l_2$.
$H_0 : \{0, 1\}^* \rightarrow \mathbb{G}_1^*$: a cryptographic hash function.
$H_1 : \{0, 1\}^* \times \mathbb{G}_2 \rightarrow \mathbb{Z}_q$: a cryptographic hash function.
$H_2 : \mathbb{G}_2 \rightarrow \mathbb{Z}_q^*$: a cryptographic hash function.
$F_1 : \{0, 1\}^{l_2} \rightarrow \{0, 1\}^{l_1}$: a cryptographic hash function.
$F_2 : \{0, 1\}^{l_1} \rightarrow \{0, 1\}^{l_2}$: a cryptographic hash function.

3. Review of Singh-Verma ID-based proxy signature scheme with message recovery

In this section, we briefly review Singh-Verma ID-based proxy signature scheme with message recovery [6], which is built on [1] and [7].
Setup. Given a security parameter λ, the PKG chooses a random generator P of $\mathbb{G}_1$ and the master secret key $s \in \mathbb{Z}_q^*$. Afterwards, the PKG sets $P_{pub} = sP$ as his public key and publishes the public parameters $PP = (\mathbb{G}_1, \mathbb{G}_2, e, P, P_{pub}, H_0, H_1, H_2, F_1, F_2, l_1, l_2)$.
Extract. On input the master secret key s and a user's identity $ID_i \in \{0, 1\}^*$, the PKG computes the user's private key $d_i = sH_0(ID_i)$ and sets its public key as $q_i = H_0(ID_i)$.
Delegate. The original signer ID_A takes as input his private key d_A and a delegation warrant m_w, he then picks a random value $k_A \in \mathbb{Z}_q^*$ and computes $r_A = e(P, P)^{k_A}$, $h_A = H_1(m_w, r_A)$ and $S = h_A \cdot d_A + k_A P$. It outputs the delegation $W_{A\rightarrow B} = (m_w, r_A, S)$.
DVerify. Upon receiving $W_{A\rightarrow B} = (m_w, r_A, S)$, the proxy signer ID_B computes $q_A = H_0(ID_A)$, $h_A = H_1(m_w, r_A)$ and checks if

$$e(S, P) = r_A \cdot e(q_A, P_{pub})^{h_A}.$$

If so, ID_B accepts the delegation; otherwise, he requests a valid one from ID_A or terminates the protocol.
PKGen. After accepting $W_{A\rightarrow B}$, ID_B sets $d_p = S + h_A \cdot d_B$ as his proxy signing key.
PSign. Given a message $m \in \{0, 1\}^*$ which conforms to the warrant m_w, the proxy signer ID_B with the proxy signing key d_p does the following steps:
Select a random value $k_B \in \mathbb{Z}_q^*$ and set $r_B = e(P, P)^{k_B}$.
Set $\beta = F_1(m)||(F_2(F_1(m)) \oplus m)$ and $\alpha = [\beta]_{10}$.
Compute $v = r_A \cdot r_B$ and $V_B = H_2(v) + \alpha$.
Compute $U = k_B P + d_p$.
Output the proxy signature $\delta = (m_w, r_A, V_B, U)$.
Verify. On input a proxy signature $\delta = (m_w, r_A, V_B, U)$, a verifier does:
Set $h_A = H_1(m_w, r_A)$ and $\alpha = V_B - H_2(e(U, P)e(q_A + q_B, P_{pub})^{-h_A})$.
Compute $\beta = [\alpha]_2$ and $m = F_2({}_{l_1}|\beta|) \oplus |\beta|_{l_2}$.
Accept the proxy signature δ if m conforms to m_w and ${}_{l_1}|\beta| = F_1(m)$.
ID. On input a valid proxy signature δ, the proxy signer's identity ID_B can be revealed by m_w.

The correctness of the scheme is justified as follows:

$$\begin{aligned}
&e(U,P)e(q_A+q_B,P_{pub})^{-h_A}\\
&=e(k_BP+d_p,P)e(q_A+q_B,P_{pub})^{-h_A}\\
&=e(k_BP+h_A\cdot d_B+S,P)e(q_A+q_B,P_{pub})^{-h_A}\\
&=e(k_BP+h_A\cdot d_B+h_A\cdot d_A+k_AP,P)\\
&\quad e(q_A+q_B,P_{pub})^{-h_A}\\
&=e((k_B+k_A)P,P)e(h_A\cdot(d_B+d_A),P)\\
&\quad e(q_A+q_B,P_{pub})^{-h_A}\\
&=e((k_A+k_B)P,P)\\
&=r_A\cdot r_B=v
\end{aligned}$$

Hence, we have

$$V_B-H_2(e(U,P)e(q_A+q_B,P_{pub})^{-h_A})=V_B-H_2(v)=\alpha.$$

Since $\beta=F_1(m)||(F_2(F_1(m))\oplus m)=[\alpha]_2$, therefore we know

$$m=F_2({}_{l_1}|\beta|)\oplus|\beta|_{l_2}.$$

Finally, the integrity of m is justified by ${}_{l_1}|\beta|=F_1(m)$.

4. Cryptanalysis of Singh-Verma signature scheme

Singh and Verma proved that their scheme is secure in an ordinary ID-based proxy signature security model. However, the ordinary ID-based proxy signature security model cannot address all the security requirements of an ID-based message recovery proxy signature scheme. In this section, by giving two concrete forgery attacks, we will demonstrate that Singh and Verma's ID-based message recovery proxy signature scheme is insecure.

4.1. Forgery attack 1

Assume that an adversary $\mathcal{A}$ has obtained a valid proxy signature $\delta=(m_w,r_A,V_B,U)$ on message m. To produce a valid proxy signature δ' on a new message m', $\mathcal{A}$ does:
Pick a random value $t\in\mathbb{Z}_q^*$, and compute $U'=U+tP$ and $v'=e(U,P)e(q_A+q_B,P_{pub})^{-h_A}\cdot e(P,P)^t=v\cdot e(P,P)^t$.
Set $\beta'=F_1(m')||(F_2(F_1(m'))\oplus m')$ and $\alpha'=[\beta']_{10}$.
Compute $V_B'=H_2(v')+\alpha'$.
Output the proxy signature $\delta'=(m_w,r_A,V_B',U')$.

Now, we show that $\delta'=(m_w,r_A,V_B',U')$ is a valid proxy signature on the message m'.

$$\begin{aligned}
&e(U',P)e(q_A+q_B,P_{pub})^{-h_A}\\
&=e(U+tP,P)e(q_A+q_B,P_{pub})^{-h_A}\\
&=e(tP,P)e(U,P)e(q_A+q_B,P_{pub})^{-h_A}\\
&=e(tP,P)\cdot v\\
&=v'
\end{aligned}$$

So, we know

$$V_B'-H_2(e(U',P)e(q_A+q_B,P_{pub})^{-h_A})=V_B'-H_2(v')=\alpha'.$$

Since $\beta'=F_1(m')||(F_2(F_1(m'))\oplus m')=[\alpha']_2$, hence we have

$$m'=F_2({}_{l_1}|\beta'|)\oplus|\beta'|_{l_2}.$$

Finally, we also have that ${}_{l_1}|\beta'|=F_1(m')$.

Consequently, the adversary $\mathcal{A}$ does forge a valid proxy signature $\delta'=(m_w,r_A,V_B',U')$ on message m'. That is Singh and Verma's ID-based proxy signature scheme with message recovery is not secure.

Notice that, in the above attack, $\mathcal{A}$ can forge a valid proxy signature δ' on message m' only if $\mathcal{A}$ has obtained a valid proxy signature $\delta=(m_w,r_A,V_B,U)$ and m' is in line with the warrant m_w. In the next subsection, we will present a new attack, which is more powerful than this one.

4.2. Forgery attack 2

Assume that $\mathcal{A}$ is an adversary who aims to forge a proxy signature δ on *any* message m, but he has not yet obtained a valid proxy signature. Then $\mathcal{A}$ does:
Produce a delegation warrant m_w such that m conforms to it.
Select two random values $r_A,U\in\mathbb{G}_1$, and set $h_A=H_1(m_w,r_A)$ and $v=e(U,P)e(q_A+q_B,P_{pub})^{-h_A}$.
Compute $\beta=F_1(m)||(F_2(F_1(m))\oplus m)$ and $\alpha=[\beta]_{10}$.
Compute $V_B=H_2(v)+\alpha$.
Output the proxy signature $\delta=(m_w,r_A,V_B,U)$.

We now show that $\delta=(m_w,r_A,V_B,U)$ is a valid proxy signature on the message m.

Since

$$v=e(U,P)e(q_A+q_B,P_{pub})^{-h_A},$$

So, we know

$$V_B-H_2(e(U,P)e(q_A+q_B,P_{pub})^{-h_A})=V_B-H_2(v)=\alpha.$$

As $\beta=F_1(m)||(F_2(F_1(m))\oplus m)=[\alpha]_2$, hence we have

$$m=F_2({}_{l_1}|\beta|)\oplus|\beta|_{l_2}.$$

Finally, we also have that ${}_{l_1}|\beta|=F_1(m)$.

Consequently, $\delta=(m_w,r_A,V_B,U)$ is indeed a valid proxy signature on m. Observe that $\mathcal{A}$ can forge a valid proxy signature on *any* message by using the attack process. In other words, Singh and Verma's ID-based message recovery proxy signature scheme is broken.

5. Conclusion

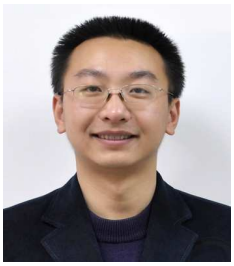
Recently, Singh and Verma [6] presented the first ID-based proxy signature scheme with message recovery and claimed that it is provably secure in the random oracle model. However, by giving two concrete attacks, we have demonstrated that their scheme is insecure. The paper shows that more effort must be made to construct a secure ID-based message recovery proxy signature scheme.

References

[1] F. Zhang, W. Susilo and Y. Mu, Identity-based partial message recovery signatures (or how to shorten ID-based signatures). Proc. 9th International Conference on Financial Cryptography and Data Security , FC, 2005, pp. 45–56.
[2] M. Mambo, K. Usuda and E. Okamoto, Proxy signature for delegating signing operation. Proc. 3rd ACM Conference on Computer and Communications Security, CCS, 1996, pp. 48–57.
[3] I. Foster, C. Kesselman, G. Tsudik and S. Tuecke, A security architecture for computational grids. Proc. 5th ACM Conference on Computer and Communications Security, CCS, 1998, pp. 83–92.
[4] B. Lee, H. Kim and K. Kim, Strong proxy signature and its applications. Proc. Symposium on Cryptography and Information Security, SCIS, 2001, pp. 603–608.
[5] H. Park and I. Lee, A digital nominative proxy signature scheme for mobile communication. Proc. 3rd International Conference on Information and Communications Security, ICICS, 2001, pp. 451–455.
[6] H. Singh and G. K. Verma, ID-based proxy signature scheme with message recovery. Journal of Systems and Software, 2012, 85, pp. 209–214.
[7] R. Tso, C. Gu, T. Okamoto and E. Okamoto, Efficient ID-Based Digital Signatures with Message Recovery. Proc. 6th International Conference on Cryptology and Network Security, CANS, 2007, pp. 47–59.

Miaomiao Tian is a Ph.D. student in School of Computer Science and Technology at University of Science and Technology of China. His research interests include cryptography and information security.

Liusheng Huang is a professor in School of Computer Science and Technology at University of Science and Technology of China. His research interests include information security, wireless sensor network and distributed computing. He is author or coauthor of more than 100 research papers and six books.



Wei Yang is a postdoctoral research fellow in School of Computer Science and Technology at University of Science and Technology of China. In 2007, he received his Ph.D. degree in computer science from University of Science and Technology of China and was awarded the Dean's Prize of Chinese Academy of Sciences. His research interests include information theory, quantum information and cryptography.