Improvement of a Nominative Proxy Signature Scheme for Mobile Communication

KEON-JIK LEE1, BYEONG-JIK LEE2 and JEONG-HOON LEE1
Dept. of Electrical&Computer Engineering, Kangwon National University, Chuncheon, KOREA1
Dept. of Computer Engineering, Kyungpook National University, Daegu, KOREA2

Abstract: - Recently, Seo and Lee proposed a modification to the Park and Lee’s nominative proxy signature scheme for mobile communication such that the original signer enables a proxy signer to nominate the verifier. However, the original signer can generate a valid nominative proxy signature without the proxy signer’s knowing. In this paper, we show that Seo and Lee’s modification is insecure against the original signer’s forgery attack, and then propose an improved scheme to repair the security flaw.

Key-Words: - authentication, digital signature, discrete logarithm

1 Introduction
Digital signature confirms that the document originated from the signer and has not been altered. That is, it allows only one entity to sign messages in such a way that any receiver can verify the validity of the obtained signatures, but no one can forge signatures at will. In 1996, Mambo et al. [1] proposed the concept of the proxy signature scheme which enables a proxy signer to sign messages on behalf of the original signer. Delegating the signature power of the original signer to a proxy signer has been shown to be useful in many cases. Based on the delegation type, they classified proxy signatures as full delegation, partial delegation, and delegation by warrant. In full delegation, the original signer gives his secret key to the proxy signer, so the proxy signer has the same signature power as the original signer. But this is obviously not practical in most circumstances. In partial delegation, the proxy signature key is generated by the original signer and proxy signer. However, this does not set limits to the signature power of the proxy signer. This problem is solved by using a warrant. In delegation by warrant, the original signer issues the warrant which defines the relative rights and information between the original signer and proxy signer, what kinds of messages are delegated, and valid period of delegation, etc. When verifying the signature, the warrant is used as a part of verification information for the verifier. Among them, the partial delegation by warrant scheme is an issue of considerable practical significance and deserves a special notice.

Furthermore, due to its importance, many variations of proxy signature scheme have been proposed [2–7]. In 2001, Park and Lee [6] proposed the nominative proxy signature scheme for mobile communication which enables a proxy signer to nominate the verifier (nominee) and only the nominated verifier can verify the nominative proxy signature. Unfortunately, Seo and Lee [7] pointed out that Park and Lee’s scheme is vulnerable to the original signer’s forgery attack and proposed a new scheme to enhance Park and Lee’s scheme and claimed that their scheme can withstand this attack. In this paper, we will review the scheme proposed by Seo and Lee and show that Seo and Lee’s scheme still suffers from the original signer’s forgery attack. Then, we will further propose an improved scheme and analyze the security.

2 Review of Seo and Lee’s scheme
There are three communicating parties in the scheme: the original signer O, the proxy signer P, and the verifier V. Some notations are defined as follows:

- $p, q$ large prime number with $q \mid (p - 1)$
- $g$ an element of order $q$ in $\mathbb{Z}_p^*$
- $h(\cdot)$ be a secure one-way hash function
- $M$ a message
- $T$ a time stamp
- $W$ a warrant which contains the identities of the original signer and proxy signer and valid period of delegation, etc
\(X_U\) the private key of user \(U\)
\(Y_U\) the public key of user \(U\), where \(Y_U = g^{X_U} \mod p\)

Seo and Lee’s scheme consists of three phases: the original signer phase, the proxy signer phase, and the verifier phase. Detailed description of each phase is given below.

**Original Signer Phase**
The original signer \(O\) generates a delegation key by using his private key.

Step 1: \(O\) selects \(r_0 \in \mathbb{Z}_q^*\) and computes \(K_O = g^{r_0} \mod p\).

Step 2: \(O\) computes \(e = h(W, T, K_O)\) and \(S_O = X_O e + r_0 K_O \mod q\), and then sends \((W, T, K_O, S_O)\) to \(P\). This phase is depicted as Fig. 1.

\[
\begin{array}{l}
\text{Step 1: } O \text{ selects } r_0 \in \mathbb{Z}_q^* \text{ and computes } K_O = g^{r_0} \mod p. \\
\text{Step 2: } O \text{ computes } e = h(W, T, K_O) \text{ and } S_O = X_O e + r_0 K_O \mod q, \text{ and then sends } (W, T, K_O, S_O) \text{ to } P. \\
\end{array}
\]

![Fig. 1 Original signer phase](image)

**Proxy Signer Phase**
The proxy signer \(P\) generates the nominative proxy signature by using his private key, the delegation key and the nominee \(V\)’s public key. The proxy signer phase runs as follows.

Step 1: \(P\) computes \(e = h(W, T, K_O)\) and accepts \((W, T, K_O, S_O)\) if \(g^{s_Y} = Y_O K_O^{s_Y} \mod p\) holds.

Step 2: \(P\) computes the proxy signature key \(S_P = S_O + X_P K_O \mod q\).

Step 3: \(P\) selects \(r_1, r_2 \in \mathbb{Z}_q^*\) and computes \(K_P = g^{2^{-r_1}} \mod p, D = Y_P^{r_1} \mod p, E = h(Y_P, K_P, D, M, W), \) and \(S = r_1 - S_P E \mod q\). Next, \(P\) sends the nominative proxy signature \((M, Y_P, W, T, K_O, K_P, D, S)\) to \(V\). We depict this phase as Fig. 2.

![Fig. 2 Proxy signer phase and verifier phase](image)

**Verifier Phase**
The verifier (nominee) \(V\) verifies the acquired nominative proxy signature by using his private key, the original signer’s public key and the proxy signer’s public key. The verification scenario is described as follows.

Step 1: \(V\) computes \(e = h(W, T, K_O)\) and \(E = h(Y_P, K_P, D, M, W)\).

Step 2: \(V\) accepts \((M, Y_P, W, T, K_O, K_P, D, S)\) as the nominative proxy signature if \((g^{s_Y}(Y_O (Y_P K_O)^{s_Y} K_P)^{r_Y}) \mod D = \mod p\) holds. This phase is depicted as Fig. 2.

\[
\begin{array}{l}
\text{Step 1: } V \text{ computes } e = h(W, T, K_O) \text{ and } E = h(Y_P, K_P, D, M, W). \\
\text{Step 2: } V \text{ accepts } (M, Y_P, W, T, K_O, K_P, D, S) \text{ as the nominative proxy signature if } (g^{s_Y}(Y_O (Y_P K_O)^{s_Y} K_P)^{r_Y}) \mod D = \mod p. \\
\end{array}
\]

Note that \(V\)’s private key \(X_V\) is used in Step 2 of verifier phase. This means that only the nominee \(V\) can verify the validity of the nominative proxy signature.

The correctness of Step 2 verification is described as follows:

\[
\begin{align*}
(g^{s_Y}(Y_O (Y_P K_O)^{s_Y} K_P)^{r_Y}) \mod p &= (g^{r_1 - S_P E} Y_O^{s_Y} g^{r_1 - r_2} E g^{r_1}) \mod p \\
&= (g^{r_1 - S_P E} Y_O^{s_Y} e + x_P K_O + r_2 K_O E g^{r_1}) \mod p \\
&= (g^{r_1 - S_P E} Y_O^{s_Y} g^{r_2 - r_1}) \mod p \\
&= (g^{r_1 - S_P E} Y_O^{s_Y} g^{r_2 - r_1}) \mod p \\
&= (g^{r_1}) \mod p \\
&= D \mod p
\end{align*}
\]

3 Cryptanalysis and Improvement
In this section, we show that Seo and Lee’s nominative proxy signature scheme is insecure against the original signer’s forgery. The security flaw of Park and Lee’s original nominative proxy signature scheme is caused by the fact that the verifier does not use the public key of the proxy signer. To strengthen Park and Lee’s scheme, Seo and Lee employed the public key
of the proxy signer to prevent the original signer’s forgery. However, Seo and Lee’s scheme is still insecure against the original signer’s forgery, that is, the original signer can generate a valid nominative proxy signature without the cooperation of the proxy signer. In the following, we will describe this attack.

Note that the original signer O knows the fact that the verifier V uses $K_O$ in the signature verification. The original signer O chooses $Y_o$ and computes $K'_O = Y_o^{-1} \mod p$, $E' = h(W, T, K'_O)$, $S'_O = X_{0E'} \mod q$, and $S'_P = S'_O \mod q$. Next, O selects $r'_1$, $r'_2 \in \mathbb{Z}_q^*$ and computes $K' = g^{r'_1 - r'_2} \mod p$, $D'_O = Y'_r \mod p$, $E'_O = h(Y'_r, K'_O, D'_O, M, W)$, $S'_O = r'_1 - S'_PE' \mod q$, and sends $(M, Y'_r, W, T, K'_O, K'_P, D'_O, S'_O)$ to V. Therefore, $(g^{S'_O}(Y'_rK'_O)^{K'_O}K'_P)^{VP} = D'_O \mod p$ holds and $(M, Y'_r, W, T, K'_O, K'_P, D'_O, S'_O)$ is a valid nominative proxy signature. This is because:

$$
\begin{align*}
& (g^{S'_O}(Y'_rK'_O)^{K'_O}K'_P)^{VP} \\
& = (g^{r'_1 - S'_PE'}(g^{xO}(Y'_rY^{-1}K'_O)^{E'}g^{r'_1 - r'_2})^{E'} \mod p \\
& = (g^{r'_1 - S'_PE'}(g^{xO}g^{r'_1 - r'_2})^{E'} \mod p \\
& = (g^{r'_1})^{VP} \mod p \\
& = D'_O \mod p
\end{align*}
$$

To overcome this forgery attack, the improved nominative proxy signature scheme is given as follows: The original signer phase in the proposed scheme is the same as that of the Seo and Lee’s scheme. The step 3 of the proxy signer phase is modified as follows.

Step 3: $P$ selects $r_1, r_2, r_3 \in \mathbb{Z}_q^*$ and computes $K_P = g^{r_2 - r_1} \mod p$, $C_P = g^{r_1} \mod p$, $Q_P = X_PK_P h(T, C_P) + r_1 \mod q$, $D = Y_r^{-1} \mod p$, $E = h(Y_r, K_P, C_P, Q_P, D, M, W)$, and $S = r_1 - S_P \mod q$. Next, $P$ sends the nominative proxy signature $(M, Y_r, W, T, K_O, C_P, Q_P, K_P, D, S)$ to V.

Next, the verifier phase is modified as mentioned below.

Step 1: $V$ accepts $K_O$ if $g^{Q_P} = Y_PK_O h(T, C_P) \mod p$ holds, and then computes $e = h(W, T, K_O)$ and $E = h(Y_r, K_P, C_P, Q_P, D, M, W)$.

Step 2: $V$ accepts $(M, Y_r, W, T, K_O, C_P, Q_P, D, S)$ as the nominative proxy signature if $(g^{S'_O}(Y'_rK'_O)^{K'_O}K'_P)^{VP} = D'_O \mod p$ holds.

4 Discussions and Conclusion

According to the forgery attack in the previous section, we assume that the transmitted $K_O$ in the original signer phase has been altered by the dishonest original signer $O$. That is, $O$ modifies $K_O$ with $K'_O = (Y_r^{-1} \mod p)$. Furthermore, $O$ has to compute $C'_P = g^{r'_1} \mod p$ and $Q'_P = X_PK'_O h(T, C'_P) + r'_1 \mod q$ to convince V in the verifier phase, where $Q'_P$ includes two unknown parameters. Obviously, $O$ needs to know $X_P$ and $r_1$ before computing $Q'_P$. However, this is computationally infeasible, because that $O$ has to solve the discrete logarithm problem. An incorrect $K_O$ can be detected in Step 1 of the verifier phase. That is, it is impossible for the original signer alone to alter $K_O$ without the proxy signer’s knowing. Therefore, the original signer’s forgery attack cannot work in the proposed scheme.

The nominative proxy signature scheme should resist the original signer’s forgery attack in which the original signer can cheat the honest verifier into believing a forged signature. We have shown that the modified nominative proxy signature scheme proposed by Seo and Lee still suffers from the original signer’s forgery attack. In other words, the original signer can generate a valid nominative proxy signature without the proxy signer’s help. The problem within Seo and Lee scheme is that the verifier cannot judge the correctness of $K_O$ from the received signature. This paper further purposes an improvement to repair the security flaw.

Acknowledgements

This work was supported by the Brain Korea 21 Project of Kangwon National University in 2005.

References:


