Generating a Proxy Signature on a Confidential Message

Ji-Seon Lee¹, Jik Hyun Chang²
Dept. Computer Science, Sogang University, Seoul, Korea
jslee702@sogang.ac.kr¹, jchang@alglab.sogang.ac.kr²

1. Introduction
In this paper, we propose a proxy signature scheme which provides message confidentiality. Even if the signature is generated by the proxy signer, only the designated recipient recovers the message with his secret key and checks the validity of the signature with the proxy signature verification key which is composed of the public keys of the original signer and the proxy signer. Our scheme would be useful when the proxy signer needs to generate a signature on behalf of the original signer while keeping the message confidential.

2. Proposed Scheme
Let \( p \) and \( q \) be two large primes such that \( q \mid p-1 \). Let \( g \) be a generator of order \( q \) and \( H \) be a one-way hash function. The proxy signer Alice chooses a secret key \( x_A \in Z_q^* \) and publishes her public key \( y_A = g^{x_A} \mod p \).

Similarly, the proxy signer Bob has his key pair \((x_B, y_B)\) and the designated recipient Cindy has her key pair \((x_C, y_C)\). \( m \) is the message to be signed and \( m_w \) is the message warrant composed of the identities of the original signer, the proxy signer, and the designated recipient and some other information related on the proxy delegation.

[Proxy Delegation] Alice generates a transcript \((m_w, r_A, s_A, m_A, c_A)\) as follows and sends it to Bob.

\[
\begin{align*}
k_A &\in_R Z_q^* \\
r_A &= g^{k_A} \mod p \\
s_A &= x_A H(m_w, r_A) + k_A \mod q \\
c_A &= m y_C^{k_A} H(m_w, r_A) \mod p \\
m_A &= H(m, m_w, c_A, y_C^{k_A})
\end{align*}
\]

[Proxy Signature Key Generation] At first Bob checks that \( g^{x_A} = y_A^{H(m_w, r_A)} r_A \mod p \) and generates a proxy signature key \( x_p \) as follows:

\[
x_p = s_A + x_B H(m_w, r_A) \mod p.
\]

The corresponding proxy signature verification key \( y_p \) is then \( y_p = g^{x_p} = (y_A y_B)^{H(m_w, r_A)} r_A \mod p \).

[Proxy Signature Generation] Bob generates a proxy signature \((m_w, r_A, c, r, s)\) as follows:

\[
k \in_R Z_q^* \\
c &= c_A y_C^{k} \mod p \\
r &= H(m_A, g^k, c) \\
s &= x_p r + k \mod q.
\]

[Message Recovery and Proxy Signature Verification] With \((m_w, r_A, c, r, s)\), Cindy computes the proxy signature verification key \( y_p \) at first. She then recovers the message and checks the signature as follows:

\[
c_A = c y_p^r g^{-s} y_C^k \mod p \\
m = c_A (y_A^{-H(m_w, r_A)} y_C^k) \mod p \\
w = r_A x_C^k \mod p \\
r = H(H(\cdot, c_A, w), y_p^{-r} g^s, c).
\]

3. Conclusions
We propose a proxy signature scheme which guarantees that only the original signer and the designated recipient can know the message and the proxy signer should generate a signature without knowing the message itself.