Blind Sig

Abstract. ...

Keywords: ...

1 HSM-CL Cryptosystem

review HSM-CL group and encryption scheme...

2 The Blind ECDSA over HSM-CL

Suppose that the group generator $\hat{G}$ of the elliptic curve used by the elliptic curve digital signature algorithm (ECDSA) has a large prime order q. Assume that the recipient wishes the signer (with the public key $\mathsf{PK} = \hat{G}^{\mathsf{SK}}$) to produce a blind signature on the hash value $h = H(m)$ of his message m, the blind ECDSA between the recipient $\mathcal{R}$ and the signer $\mathcal{S}$ can be described as follows:

- Step 1. The signer $\mathcal{S}$ randomly chooses an integer $k_1 \in \mathbb{Z}_q$ and computes $K_1 = \hat{G}^{k_1}$ and sends it to the recipient $\mathcal{R}$.

- Step 2. After receiving K_1 from $\mathcal{S}$, the recipient $\mathcal{R}$ randomly chooses $k_2 \in \mathbb{Z}_q$ and computes $K = K_1^{k_2}$ and denote by (K_x, K_y) the x-coordinator and y-coordinator of ECC point K.

  Next, the recipient $\mathcal{R}$ randomly picks $\mathsf{sk} \in \mathbb{Z}_q$ and computes $\mathsf{pk} = g_q^{\mathsf{sk}}$ (key generation for HSM-CL encryption scheme).

  Then $\mathcal{R}$ randomly chooses $r_1, r_2 \in \mathbb{Z}_q$ and computes (follow HSM-CL Enc)

  $$C_1 = (x_1, x_2) = (g_q^{r_1}, f^h \mathsf{pk}^{r_1}), \quad C_2 = (y_1, y_2) = (g_q^{r_2}, f^{K_x} \mathsf{pk}^{r_2})$$

  and generate a NIZK proof π for the well-formedness of C_1 and C_2.

- Step 3. After receiving C_1, C_2, π, $\mathcal{S}$ firstly checks the validity of (C_1, C_2) by π. If invalid, reject and abort; if valid, $\mathcal{S}$ randomly chooses $r_1', r_2', r_3' \in \mathbb{Z}_q$ and computes

  $$\begin{aligned}
  \alpha &= (\alpha_1, \alpha_2) = (y_1^{\mathsf{SK}} g_q^{r_1'}, y_2^{\mathsf{SK}} \mathsf{pk}^{r_1'}) \\
  \beta &= (\beta_1, \beta_2) = (\alpha_1 x_1 g_q^{r_2'}, \alpha_2 x_2 \mathsf{pk}^{r_2'}) \\
  \gamma &= (\gamma_1, \gamma_2) = (\beta_1^{k_1} g_q^{r_3'}, \beta_2^{k_1} \mathsf{pk}^{r_3'})
  \end{aligned}$$

and sends γ to $\mathcal{R}$.

– Step 4. After receiving γ, the recipient $\mathcal{R}$ computes

$$s = k_1^{-1} \frac{\gamma_2}{\gamma_1^{\mathsf{sk}}}$$

In the end, the recipient $\mathcal{R}$ obtains a blind signature (K_x, s).

3 Zero-knowledge Proof

Let $(\tilde{s}, g, f, g_q, \tilde{G}, G, F, G^q) \leftarrow \mathsf{Gen}_{\mathrm{HSM},q}(1^\lambda)$. The ECC group generated by generator $\hat{G}$ has a large prime order q. We need to prove the following relation when sending (C_1, C_2):

$$\begin{aligned}&\mathcal{R}_{\mathsf{Enc}} = \{(x_1, x_2, y_1, y_2, \mathsf{pk}, f, g_q) : (h, K_x, r_1, r_2, \mathsf{sk})| \\ &x_1 = g_q^{r_1} \wedge x_2 = f^h \mathsf{pk}^{r_1} \wedge y_1 = g_q^{r_2} \wedge y_2 = f^{K_x} \mathsf{pk}^{r_2}.\}\end{aligned}$$

where $B = 2^{\lambda+\epsilon_d+2}\tilde{s}$, $\epsilon_d = 80$.

1. Prover chooses $s_1, s_2, s_h, s_x \xleftarrow{\$} [-B, B]$ and computes:

$$S_1 = g_q^{s_1}, \quad S_2 = f^{s_h} \mathsf{pk}^{s_1}, \quad S_3 = g_q^{s_2}, \quad S_4 = f^{s_x} \mathsf{pk}^{s_2},$$

   Prover sends (S_1, S_2, S_3, S_4) to the verifier.

2. Verifier sends $c \xleftarrow{\$} [0, q-1]$ to the prover.

3. Prover computes:

$$\begin{aligned}&u_1 = s_1 + cr_1, \quad u_2 = s_2 + cr_2, \\ &u_h = s_h + c \cdot h, \quad u_x = s_x + c \cdot Kx,\end{aligned}$$

   Prover finds $d_1, d_2, d_k \in \mathbb{Z}$ and $e_1, e_2 \in [0, q-1]$ s.t. $u_1 = d_1 q + e_1, \quad u_2 = d_2 q + e_2, \quad u_h = d_h q + e_h, \quad u_x = d_x q + e_x$. Prover computes:

$$D_1 = g_q^{d_1}, \quad D_2 = \mathsf{pk}^{d_1}, \quad D_3 = g_q^{d_2}, \quad D_4 = \mathsf{pk}^{d_2}.$$

   Prover sends $(D_1, D_2, D_3, D_4, e_1, e_2, u_\rho)$ to the verifier.

4. The verifier checks if $e_1, e_2, u_\rho \in [0, q-1]$ and:

$$\begin{aligned}&D_1^q g_q^{e_1} = S_1 x_1^c, \quad D_2^q \mathsf{pk}^{e_1} f^{u_h} = S_2 x_2^c, \\ &\qquad\qquad\qquad\qquad D_3^q g_q^{e_2} = S_3 y_1^c, \quad D_4^q \mathsf{pk}^{e_2} f^{u_x} = S_4 y_2^c\end{aligned}$$

   If so, the verifier sends $\ell \xleftarrow{\$} \mathsf{Primes}(\lambda)$.

5. Prover finds $q_1, q_2, q_k \in \mathbb{Z}$ and $\gamma_1, \gamma_2, \gamma_k \in [0, \ell - 1]$ s.t. $u_1 = q_1\ell + \gamma_1$,$u_2 = q_2\ell + \gamma_2$ and $u_k = q_k\ell + \gamma_k$. Prover computes:

$$Q_1 = g_q^{q_1}, \quad Q_2 = \mathsf{pk}^{q_1}, \quad Q_3 = g_q^{q_2}, \quad Q_4 = \mathsf{pk}^{q_2}, \quad Q_5 = g_q^{q_k}.$$

   Prover sends $(Q_1, Q_2, Q_3, Q_4, Q_5, \gamma_1, \gamma_2, \gamma_k)$ to the verifier.
6. Verifier accepts if $\gamma_1, \gamma_2, \gamma_k \in [0, \ell - 1]$ and:

$$\begin{aligned} &Q_1^q g_q^{\gamma_1} = S_1 x_1^c, \quad Q_2^q \mathsf{pk}^{\gamma_1} f^{u_h} = S_2 x_2^c, \\ &Q_3^q g_q^{\gamma_2} = S_3 y_1^c, \quad Q_4^q \mathsf{pk}^{\gamma_2} f^{u_x} = S_4 y_2^c, \quad Q_5^q g_q^{\gamma_k} = S_5 \mathsf{pk}^c, \end{aligned}$$

4 Implementation

We implement the blind ECDSA scheme and our scheme over HSM-CL. ZK part dominates the running time for both schemesur scheme but our ZK waives the need to repeat many rounds to achive a suitable soundness. (ours should be much faster than theirs)

to update the running time...

References