Now consider the case $\lambda = \lambda' = \Delta_E$ with $\Delta_E | \Delta_{s1}$ and $\Delta_E | \Delta_{t1}$. Note that this implies that $\Delta_E | \Delta_{s2}$ and $\Delta_E | \Delta_{t2}$ as well.

Define $x_1 = \Delta_{s1}/\Delta_E$, $\rho_1 = \Delta_{s2}/\Delta_E$, $\alpha_1 = (e\hat{s}_1 - \hat{es}_1)/\Delta_E$, $\rho'_1 = (e\hat{s}_2 - \hat{es}_2)/\Delta_E$, $y_1 = \Delta_{t1}/\Delta_E$, $\sigma_1 = \Delta_{t2}/\Delta_E$, $\gamma_1 = (e\hat{t}_1 - \hat{et}_1)/\Delta_E$ and $\tau_1 = (e\hat{t}_2 - \hat{et}_2)/\Delta_E$.

Define $x'_1 = x_1 \bmod N$ and $y'_1 = y_1 \bmod N$. Note that by definition

$$c_1^{x'_1} \Gamma^{y'_1} \kappa^N = c_2 \bmod N^2$$

for some κ as needed. And $g^{x_1} = X \in G$. So we have extracted the required x, y. As in the previous proof we can establish that $x_1, x'_1 \in [-q^3, q^3]$.

Honest-Verifier Zero-Knowledge. The simulator proceeds as in [27] and in the previous ZK proof.

A.3 Respondent ZK Proof for MtA

This proof is run by Bob (the responder) in the MtA protocol. It is a simpler version of the previous protocol where Bob only proves that x is small (without proving that it is the discrete log of any public value).

The input for this proof is a Paillier public key N, Γ and two values $c_1, c_2 \in Z_{N^2}$.

The prover knows $x \in Z_q$, $y \in Z_N$ and $r \in Z_N^*$ such that $c_2 = c_1^x \Gamma^y r^N \bmod N^2$ where q is the order of the DSA group.

At the end of the protocol the Verifier is convinced of the above and that $x \in [-q^3, q^3]$.

- The Prover selects $\alpha \in_R Z_{q^3}$, $\rho \in_R Z_{q\tilde{N}}$, $\rho' \in_R Z_{q^3\tilde{N}}$, $\sigma \in Z_{q\tilde{N}}$, $\beta \in_R Z_N^*$, $\gamma \in_R Z_N^*$ and $\tau \in_R Z_{q\tilde{N}}$.
  The Prover computes $z = h_1^x h_2^\rho \bmod \tilde{N}$, $z' = h_1^\alpha h_2^{\rho'} \bmod \tilde{N}$, $t = h_1^y h_2^\sigma \bmod \tilde{N}$, $v = c_1^\alpha \Gamma^\gamma \beta^N \bmod N^2$, and $w = h_1^\gamma h_2^\tau \bmod \tilde{N}$.
  The Prover sends z, z', t, v, w to the Verifier.
- The Verifier selects a challenge $e \in_R Z_q$ and sends it to the Prover.
- The Prover computes $s = r^e \beta \bmod N$, $s_1 = ex + \alpha$, $s_2 = e\rho + \rho'$, $t_1 = ey + \gamma$ and $t_2 = e\sigma + \tau$.
  The Prover sends s, s_1, s_2, t_1, t_2 to the Verifier.
- The verifier checks that $s_1 \leq q^3$, $h_1^{s_1} h_2^{s_2} = z^e z' \bmod \tilde{N}$, $h_1^{t_1} h_2^{t_2} = t^e w \bmod \tilde{N}$, and $c_1^{s_1} s^N \Gamma^{t_1} = c_2^e v \bmod N^2$.

The proof is immediate from the previous one.