Appendix A
Proof of Theorem 1

Proof. We present the formal proof using a sequence of games from the real security game G_0 to the random game G_9. The games run in time at most t, and involve at most n_p honest parties. We also define an event $\xi_i (0 \le i \le 9)$ as $\mathcal{A}$ winning game G_i by breaching the semantic security of LLRA. Additionally, we assume $\mathcal{S}$ is the solver of ECCDHP and $\mathcal{T}$ is the solver of ECDLP.

We also define an event $\xi_i (0 \le i \le 9)$ as $\mathcal{A}$ winning game G_i by breaching the semantic security of the LLRA. Note that event Z, which is independent of ξ_i, may occur during $\mathcal{A}$'s computation. Games G_i and G_{i+1} are indistinguishable unless Z occurs. Thus, we have:

$$|\text{Prob}\left[\xi_{i+1}\right] - \text{Prob}\left[\xi_i\right]| \le \text{Prob}[Z]$$

Game G_0**:** This game corresponds to a real attack scenario where all oracle queries are answered honestly in accordance with the protocol specifications. Based on the security definition, we obtain:

$$\mathbf{Adv}_{\mathcal{A}}^{LLRA}(k) = |2\Pr\left[b' = b\right] - 1|$$

Game G_1**:** This game simulates the hash oracle H. The execution of the $Reveal$, $Send$, $Corrupt$, and $Test$ queries in this game is equivalent to executing an actual attack. Thus, we have:

$$\text{Prob}\left[\xi_1\right] = \text{Prob}\left[\xi_0\right]$$

Game G_2**:** In this game $\mathcal{A}$ replaces Y_A with the value x_{Y_A} chosen uniformly at random. The protocol runs honestly to generate x_{Y_A}. By the ECDLP problem, $\mathcal{A}$ executes n_s times with probability$\mathbf{Adv}_{\mathcal{A}}^{ECDLP}(\mathcal{T})$, the value Y_A and xY_A are indistinguishable. Then, we have:

$$|\text{Prob}\left[\xi_2\right] - \text{Prob}\left[\xi_1\right]| \le n_s \mathbf{Adv}_{\mathcal{A}}^{ECDLP}(\mathcal{T})$$

Game G_3**:** In this game, $m = 1$, the condition $n > 20$ guarantees that $n > 20{\cdot}m$, $n \ge m/3$ and $n > 16$. The leakage-resilient storage $\Lambda_{Z_q^*}^{n,1}$ is $(2\lambda, \epsilon)$-secure leakage-resilient and the refreshing protocol $Refresh_{Z_q^*}^{n,1}$ is (l, λ, ϵ'), $l \in N$, ϵ and ϵ' is negligible, and $\lambda = (0.15n\log q, 0.15n\log q)$. Thus, we have:

$$|\text{Prob}\left[\xi_3\right] - \text{Prob}\left[\xi_2\right]| \le n_p \cdot \epsilon'$$

Game G_4**:** In this game, a collision occurs based on the birthday attack. The probability of collisions in the content simulation is at most $\begin{pmatrix} n_e + n_s \\ 2 \end{pmatrix}$ events, each of which occurs with a probability of $\frac{1}{n_p}$. The probability of collisions in the hash oracle simulation is at most $\begin{pmatrix} n_h \\ 2 \end{pmatrix}$ events, each of which occurs with probability $\frac{1}{2^l}$. Thus, we have:

$$\begin{aligned} |\text{Prob}\left[\xi_4\right] - \text{Prob}\left[\xi_3\right]| &\le \begin{pmatrix} n_e + n_s \\ 2 \end{pmatrix} \cdot \frac{1}{n_p} + \begin{pmatrix} n_h \\ 2 \end{pmatrix} \cdot \frac{1}{2^l} \\ &\le \frac{(n_e + n_s)^2}{2n_p} + \frac{n_h^2}{2^{l+1}} \end{aligned}$$

Game G_5**:** In this game, the ciphertext E_A is replaced with an encryption of hw_A. If E_A is a valid ciphertext, sets the session key identical to that of S_B^j; else, sets the session key as an uniformly chosen element from dictionary $|X|$. There are $n_s + n_h$ events in total, each of which occurs with probability $\frac{1}{|X|}$. Under the semantic security of authenticated encryption, we have:

$$|\text{Prob}\left[\xi_5\right] - \text{Prob}\left[\xi_4\right]| \le \frac{n_s + n_h}{|X|}$$

Game G_6**:** In this game, the ciphertext E_B is replaced with an encryption of hw'_B. If the $\mathcal{A}$ can distinguish game G_6 from game G_5, then the semantic security of authenticated encryption will be broken at most $n_e + n_h$ with probability $\frac{1}{|X|}$. Thus, we have:

$$|\text{Prob}\left[\xi_6\right] - \text{Prob}\left[\xi_5\right]| \le \frac{n_e + n_h}{|X|}$$

Game G_7**:** In this game, we show that the adversary $\mathcal{A}$ can distinguish a real session key from a random number if the following situations occur.

- $\mathcal{A}$ made $Corrupt(U_A^i)$ query but no $Send(S_B^j)$ query. If an adversary $\mathcal{A}$ successfully forges a valid message E_A, they can obtain hw_A and D_A by issuing n_c Corrupt query on U_A^i. However, $\mathcal{A}$ cannot retrieve any identity information or data about y_A from X_A, hw_A, D_A, and Y_A. Therefore, if $\mathcal{A}$ can correctly calculate the value sk_A with negligible advantage, they can forge a valid ciphertext with the same advantage.
- $\mathcal{A}$ made $Corrupt(U_A^i)$ query and $Send(S_B^j)$ query. Assuming the adversary $\mathcal{A}$ successfully forges a valid message E_A and obtains hw_A and D_A of U_A^i by issuing a $Corrupt$ query, they can set x_{y_A} and x_{u_A} and request a valid message msg'_2 using the $Send(S_B^j, msg'_1)$ query. To forge a valid E_A, $\mathcal{A}$ must accurately calculate the value $x_{sk_A} = X_A \oplus X_B \oplus H_3(Y_B \cdot x_{u_A})$. If the adversary executes $n_s - 1$ $Send$ queries to guess ID_A, the probability that $\mathcal{A}$ produces a valid E_A is bounded by $\frac{1}{|X|}$.

Therefore, we have:

$$\begin{aligned} &|\text{Prob}\left[\xi_7\right] - \text{Prob}\left[\xi_6\right]| \\ &\le \frac{n_s - 1}{|X|} + n_c(\mathbf{Adv}_{\mathcal{A}}^{ECDLP}(\mathcal{T}) + \mathbf{Adv}_{\mathcal{A}}^{ECCDH}(\mathcal{S})) \end{aligned}$$

Game G_8**:** In this game, the adversary $\mathcal{A}$ issues a $Corrupt(S_B^j)$ query and then requests a valid message $msg_1 = (X_A, Y_A, T_A, C_A, Auth)$ by using the $Send(U_A^i, S_B^j)$ query. Assuming that $\mathcal{A}$ successfully forges a valid ciphertext E_B, they can distinguish between a real session key and a random number. After obtaining hw_B and D_B of S_B^j via the Corrupt query, $\mathcal{A}$ sets x_{y_B} and x_{u_B} and computes $x_{sk_B} = X_A \oplus X_B \oplus H_3(Y_A \cdot x_{u_B})$. To forge a valid E_B, $\mathcal{A}$ must correctly calculate the value x_{sk_B}, as well as know the identity ID_B. If $\mathcal{A}$ executes $n_s - 1$ $Send$ queries to guess ID_B, the probability that $\mathcal{A}$ outputs a valid E_B is bounded by $\frac{1}{|X|}$. Therefore, we obtain:

$$|\text{Prob}\left[\xi_8\right] - \text{Prob}\left[\xi_7\right]| \le \frac{n_s - 1}{|X|}$$

Game G_9**:** This game serves as a bridging step where the advantage of $\mathcal{A}$ in guessing b is completely eliminated. This is achieved by making the outputs of $Test(\cdot,\cdot)$ queries indistinguishable in the previous sequence of games, unless the game is halted. Therefore, we obtain:

$$\mathrm{Prob}\left[\xi_9\right] = \mathrm{Prob}\left[\xi_8\right] = \frac{1}{2}$$

Thus, we have:

$$\begin{aligned}&\mathbf{Adv}_{\mathcal{A}}^{LLRA}(k) \leq 2n_p \cdot \epsilon' + \frac{(n_e+n_s)^2}{n_p} + \frac{n_h^2}{2^l} \\ &+ 2(\frac{n_s+n_h}{|X|} + \frac{n_e+n_h}{|X|}) + \frac{4(n_s-1)}{|X|} \\ &+ 2(n_s+n_c)\mathbf{Adv}_{\mathcal{A}}^{ECDLP}(\mathcal{T}) + 2n_c\mathbf{Adv}_{\mathcal{A}}^{ECCDH}(\mathcal{S})\end{aligned}$$

□