Appendix B
Proof of Theorem 1

Proof: We define a sequence of games [33] starting with the real attack game $\mathcal{G}_0$ and ending with the game $\mathcal{G}_9$. Let $Succ_i$ be the event that the adversary guesses bit b correctly involved in a test query in $\mathcal{G}_0$, where $i = 0, 1, \ldots, 9$. Let Δ_i be the distance between $\mathcal{G}_i$ and $\mathcal{G}_{i+1}$. Then, we have

$$\begin{aligned} Adv_{\mathcal{D}}^{LRDID}(\mathcal{A}) &\leq 2\Pr[Succ_0] - 1 \\ &= 2\Pr[Succ_n] - 1 - 2\Pr[Succ_9] \\ &\quad + 2\Pr[Succ_0] \\ &\leq 2\Pr[Succ_n] - 1 + 2\sum_{i=0}^{n-1}\Delta_i, \end{aligned} \tag{1}$$

which implies that if the difference in success probability between any two consecutive games Δ_i is negligible, then $\mathcal{A}$'s advantage in the original game $\mathcal{G}_0$ will be almost the same as that in the final game $\mathcal{G}_9$ [22]. That means if we can show that the value of $\Pr[Succ_n]$ is negligible, then so is $\Pr[Succ_0]$, and therefore $Adv_{\mathcal{D}}^{LRDID}(\mathcal{A})$ too.

Game $\mathcal{G}_0$: This game models the real attack scenario. By definition, we have

$$Adv_{\mathcal{D}}^{LRDID}(\mathcal{A}) = 2\Pr[Succ_0] - 1. \tag{2}$$

Game $\mathcal{G}_1$: In this game, we simulate oracles for $\mathcal{A}$ to query. Obviously, the simulation of this game is indistinguishable from the real execution of the protocol so we have

$$\begin{aligned} \Pr[Succ_1] &= \Pr[Succ_0], \\ \Delta_0 = |Pr[Succ_1] - \Pr[Succ_0]| &= 0. \end{aligned} \tag{3}$$

Game $\mathcal{G}_2$: This game is the same as $\mathcal{G}_1$ except that we halt the game if a collision occurs in transcripts

$$(\{DID_U, M_{TC}, H_{TC}, TS_{TC}\}, \\ \{XDID_U^*, M_S, H_S\}, \{H_{HCR}^{ack}\}).$$

Specifically, the transcript can be generated by $Send(\cdot,\cdot)$ or $Execute(\cdot,\cdot)$-oracle, the number of which is $q_{send} + q_{exe}$ at most [42]. There are $\binom{q_{send} + q_{exe}}{2}$ events in total, each of which occurs with probability $\frac{1}{|\mathcal{T}|}$. Therefore, based on the birthday paradox, we have

$$\begin{aligned} \Delta_1 = |Pr[Succ_2] - \Pr[Succ_1]| &\leq \binom{q_{send} + q_{exe}}{2}\frac{1}{|\mathcal{T}|} \\ &\leq \frac{(q_{send} + q_{exe})^2}{|\mathcal{T}|}. \end{aligned} \tag{4}$$

Game $\mathcal{G}_3$: In this game, we consider the situation that $\mathcal{A}$ targets PW_U after only querying $Corrupt^{SC}(\Pi_U^i)$ to get $(ID_{SC}, DID_U, X_U^1, X_U^2, a_U, EB_U)$. $\mathcal{A}$ can get the $H_1(AID_U)$ from $X_U^2 \oplus PK$; while $AID_U = H(ID_U \parallel PW_U \parallel a_U)$, $\mathcal{A}$ can only try one alternative password together with one identity, the probability of which is bounded by q_{send} with probability $\frac{1}{|\mathcal{D}|\cdot|\mathcal{T}|}$. We use the output of $H(\cdot)$ to response to the query to $H(\cdot)$ on $\{ID_U \parallel PW_U \parallel a_U\}$, i.e., to exclude the opportunity of online testing. Therefore, we have

$$\Delta_2 = |Pr[Succ_3] - \Pr[Succ_2]| \leq \frac{q_{send}}{|\mathcal{D}|\cdot|\mathcal{I}|}. \tag{5}$$

Game $\mathcal{G}_4$: In this game, we consider the session key security. The goal of this game is to verify the perfect forward secrecy and known session-specific temporary information attack resistance. To this end, the following two scenarios are considered. We consider the situation that $\mathcal{A}$ targets SK in several strategies:

Strategy 1 (known session-specific temporary information attack). Holding α and β from $Corrupt^E(\cdot)$, $\mathcal{A}$ cannot get A or u_S from querying $H(\cdot)$ or manipulating M_{TC} and M_S. Thus, strategy 1 strategy does not give $\mathcal{A}$ advantage.

Strategy 2 (forward security). Holding ID_U, PW_U and sk from $Corrupt^L(\cdot)$, $\mathcal{A}$ cannot compute the session key SK_{TC}^S without corresponding A and B. Thus, strategy 2 does not give $\mathcal{A}$ advantage.

Therefore, $\mathcal{G}_4$ and $\mathcal{G}_3$ are indistinguishable unless that $\mathcal{A}$ luckily guesses the output of $H(\cdot)$, the probability of which is bounded by q_{hash} with probability $ADV_{\mathcal{A}}^{ECCDH}(t)$. So we have

$$\Delta_3 = |Pr[Succ_4] - \Pr[Succ_3]| \leq q_{hash}ADV_{\mathcal{A}}^{ECCDH}(t). \tag{6}$$

Game $\mathcal{G}_5$:The goal of this game is to verify the key compromise impersonation attack resistance. The simulation of this game is the same as the game $\mathcal{G}_4$ except that this game will be aborted if $\mathcal{A}$ issues a $H(ID_u \| PW_u \| a_u)$ or $H(ID_u \| sk \| a_S)$ query. There are $q_{hash}\cdot q_{hash}$ events in total, each of which occurs with probability $\frac{1}{2^l}$. As a result, the difference between game $\mathcal{G}_4$ and game $\mathcal{G}_5$ is:

$$\Delta_4 = |Pr[Succ_5] - \Pr[Succ_4]| \leq q_{hash}^2 \cdot \frac{1}{2^l} = \frac{q_{hash}^2}{2^l} \tag{7}$$

Game $\mathcal{G}_6$: The only difference between this game and the previous one is that this game will be aborted if $\mathcal{A}$ issues an $Test^{ID}(ID_U)$ or q_{send} $Send$ query with probability $\frac{1}{|\mathcal{D}|}$ to get the real identity of user or his/her password. Thus, we have

$$\Delta_5 = |Pr[Succ_6] - \Pr[Succ_5]| \leq Adv_{\mathcal{A}}^{SEnc}(t) + \frac{q_{send}}{|\mathcal{D}|} \tag{8}$$

Game $\mathcal{G}_7$: The only difference between this game and the previous one is that the leakage of the long-term private key sk of S is a leakage of a random value. Hence, the difference between the two games is

$$\Delta_6 = |Pr[Succ_7] - \Pr[Succ_6]| \leq \epsilon \tag{9}$$

Game $\mathcal{G}_8$: The only difference between this game and the previous one is that this game will be halted if $\mathcal{A}$ issues an H query. Since $\mathcal{A}$ can get the session key SK, the probability of which is bounded by $\binom{q_{hash}}{2}$ with probability $\frac{1}{2^l}$, the difference between the two games is

$$\Delta_7 = |Pr[Succ_8] - \Pr[Succ_7]| \leq \binom{q_{hash}}{2} \cdot \frac{1}{2^l} \leq \frac{q_{hash}^2}{2^{l+1}} \tag{10}$$

Game $\mathcal{G}_9$: In this game, we consider the situation that $\mathcal{A}$ targets ID_U before querying any corrupt oracle. $\mathcal{A}$ may solve an $ECCDH$ to get the session key SK; or, $\mathcal{A}$ may directly compromise the ciphertext DID_U (or DID_U^*). We use private

$Test_p^{ID}(\Pi_U^i)$ to replace $Test^{ID}(\Pi_U^i)$. Therefore, the output of $Test^{ID}(\Pi_U^i)$ is independent from DID_U and DID_U^*. Then, we have

$$\Pr[Succ_9] = \frac{1}{2}. \tag{11}$$

Without SK, $\mathcal{A}$'s advantage in distinguishing $\mathcal{G}_8$ and $\mathcal{G}_9$ is upper bounded to compromise the symmetric encryption scheme or an ECCDH instance. There are $q_{send} + q_{exe}$ events in total, each of which occurs with probability $Adv_{\mathcal{A}}^{SEnc}(t) + Adv_{\mathcal{A}}^{ECCDH}(t)$. Thus, we have

$$\begin{aligned}\Delta_8 =& \Pr[Succ_9] - \Pr[Succ_8] \\ \leq& (q_{send} + q_{exe})(Adv_{\mathcal{A}}^{SEnc}(t) + Adv_{\mathcal{A}}^{ECCDH}(t)).\end{aligned} \tag{12}$$

After substituting (3)-(12) into inequality (1), we have

$$\begin{aligned}&Adv_{\mathcal{D}}^{LRDID}(\mathcal{A}) \leq 2\Pr[Succ_8] - 1 + 2\sum_{i=0}^{8} \Delta_i \\ \leq& \frac{2(q_{send} + q_{exe})^2}{|\mathcal{T}|} + \frac{2q_{send}}{|\mathcal{D}| \cdot |\mathcal{I}|} + \frac{2q_{send}}{|\mathcal{D}|} + \frac{3q_{hash}^2}{2^l} \\ &+ 2(q_{send} + q_{exe} + q_{hash})Adv_{\mathcal{A}}^{ECCDH}(t) + 2\epsilon \\ &+ 2(q_{send} + q_{exe} + 1)Adv_{\mathcal{A}}^{SEnc}(t).\end{aligned}$$

Theorem 1 is proved. ■