APPENDIX A
GNY LOGIC ANALYSIS

This section analyzes PEO scheme's security in GNY logic.

A. Description

The parser algorithm would produce the following description of PEO:
$Msg_1 : S \triangleleft *DID_U, *M_{TC}, *H_{TC}, *TS_{TC};$
$Msg_2 : TC \triangleleft *XDID_U^*, *M_S, *H_S;$
$Msg_3 : S \triangleleft *H_{TC}^{ack}.$
$Msg_4 : U \triangleleft *H_{TC}^{ack}.$
$Msg_3 : S \triangleleft *H_{TC}^{ack}.$

B. Goal

The shared session keys between TC and S shall achieve the following goals:
Goal 1: $TC \mid\equiv \sharp SK_{TC}^S;$
Goal 2: $TC \mid\equiv \phi SK_{TC}^S;$
Goal 3: $TC \mid\equiv S \ni SK_{TC}^S;$
Goal 4: $S \mid\equiv \sharp SK_{TC}^S;$
Goal 5: $S \mid\equiv \phi SK_{TC}^S;$
Goal 6: $S \mid\equiv TC \ni SK_{TC}^S.$

C. Initial Assumptions

Referring to LRDIDAKA's registration phrase, we have several initialization assumptions:
A1: $TC \mid\equiv \sharp\alpha;$
A2: $TC \mid\equiv \phi\alpha;$
A3: $TC \ni \alpha, a_U, b_U, TS_{TC}, ID_U, PW_U, X_U^1;$
A4: $TC \mid\equiv TC \overset{ID_U}{\leftrightarrow} S;$
A5: $S \mid\equiv \sharp\beta;$
A6: $S \mid\equiv \phi\beta;$
A7: $S \ni \beta, b_S, a_S, ID_U, sk, BID_U;$
A8: $S \mid\equiv S \overset{ID_U}{\leftrightarrow} TC.$

D. Proof

Then, we start the formal proof of **Goal 1** to **Goal 6** in GNY logic.

Based on rules T1 and P1, we can get that S possesses $DID_U, M_{TC}, H_{TC}, TS_{TC}, H_{TC}^{ack}$.

$$\cfrac{\cfrac{S \triangleleft *DID_U, *M_{TC}, *H_{TC}, *TS_{TC}, *H_{TC}^{ack}}{S \triangleleft DID_U, M_{TC}, H_{TC}, TS_{TC}, H_{TC}^{ack}}(T1)}{S \ni DID_U, M_{TC}, H_{TC}, TS_{TC}, H_{TC}^{ack}}(P1)$$

Based on rules T1 and P1, we can get that TC possesses $XDID_U^*, M_S, H_S$.

$$\cfrac{\cfrac{TC \triangleleft *XDID_U^*, *M_S, *H_S}{TC \triangleleft XDID_U^*, M_S, H_S}(T1)}{TC \ni XDID_U^*, M_S, H_S}(P1)$$

Goal 1: Based on A1 and the rule F1, we can get that TC believes that $(PW_U||b_U||\alpha)$ is fresh.

$$\frac{TC \mid\equiv \sharp\alpha}{TC \mid\equiv \sharp(PW_U||b_U||\alpha)}(F1)$$

Based on A3 and the rule P2, we can get that $TC \ni (PW_U||b_U||\alpha)$.

$$\frac{TC \ni \alpha, b_U, PW_U}{TC \ni (PW_U||b_U||\alpha)}(P2)$$

Based on the rule F10, we can get that TC believes that A is fresh. Based on the rule P4, we can get that $TC \ni A$, and $A = H(PW_U||b_U||\alpha)$.

$$\frac{TC \mid\equiv \sharp(PW_U||b_U||\alpha), TC \ni (PW_U||b_U||\alpha)}{TC \mid\equiv \sharp H(PW_U||b_U||\alpha)}(F10)$$

$$\frac{TC \ni (PW_U||b_U||\alpha)}{TC \ni H(PW_U||b_U||\alpha)}(P4)$$

Based on the rule F1, we can get that TC believes that $(M_S \times (A + H(ID_U||b_U)))$ is fresh.

$$\frac{TC \mid\equiv \sharp A}{TC \mid\equiv \sharp(M_S \times (A + H(ID_U||b_U)))}(F1)$$

Based on A3 and the rules P2 and P4, we can get that $TC \ni H(ID_U||b_U)$.

$$\frac{TC \ni ID_U, b_U}{TC \ni H(ID_U||b_U)}(P2)(P4)$$

Based on the rule P2, we can get that $TC \ni (M_S \times (A + H(ID_U||b_U)))$.

$$\frac{TC \ni M_S, TC \ni A, TC \ni H(ID_U||b_U)}{TC \ni (M_S \times (A + H(ID_U||b_U)))}(P2)$$

Based on the rule F10, we can get that TC believes that SK_{TC}^S is fresh, and $SK_{TC}^S = H(M_S \times (A + H(ID_U||b_U)))$. Goal 1 is proved.

$$\frac{\begin{array}{l} TC \mid\equiv \sharp(M_S \times (A + H(ID_U||b_U))), \\ TC \ni (M_S \times (A + H(ID_U||b_U))) \end{array}}{TC \mid\equiv \sharp H(M_S \times (A + H(ID_U||b_U)))}(F10)$$

Goal 2: Based on A2 and the rule R1, we can get that TC believes that $(PW_U||b_U||\alpha)$ is recognizable.

$$\frac{TC \mid\equiv \phi\alpha}{TC \mid\equiv \phi(PW_U||b_U||\alpha)}(R1)$$

Based on the rule R5, we can get that TC believes that A is recognizable, and $A = H(PW_U||b_U||\alpha)$.

$$\frac{TC \mid\equiv \phi(PW_U||b_U||\alpha), TC \ni (PW_U||b_U||\alpha)}{TC \mid\equiv \phi H(PW_U||b_U||\alpha)}(R5)$$

Based on the rule R1, we can get that TC believes that $SK_{TC}^S = (M_S \times (A + H(ID_U||b_U)))$ is recognizable.

$$\frac{TC \mid\equiv \phi A}{TC \mid\equiv \phi(M_S \times (A + H(ID_U||b_U)))}(R1)$$

Based on the rule R5, we can get that TC believes that SK_{TC}^S is recognizable, and $SK_{TC}^S = H(M_S \times (A + H(ID_U||b_U)))$. Goal 2 is proved.

$$\frac{\begin{array}{l} TC \mid\equiv \phi(M_S \times (A + H(ID_U||b_U))), \\ TC \ni (M_S \times (A + H(ID_U||b_U))) \end{array}}{TC \mid\equiv \phi H(M_S \times (A + H(ID_U||b_U)))}(R5)$$

Goal 3: Based on A3, the rules P2 and P4 , we can get that TC posses AID_U, and$AID_U = H(ID_U||PW_U||a_U)$.

$$\frac{TC \ni ID_U, PW_U, a_U}{TC \ni H(ID_U||PW_U||a_U)}(P2)(P4)$$

Based on A3 and the rule P2, we can get that TC posses X_U^0, and $X_U^0 = X_U^1 \oplus AID_U$.

$$\frac{TC \ni X_U^1, AID_U}{TC \ni X_U^1 \oplus AID_U}(P2)$$

Based on the proof of Goal 1 and the rule P4, we can get that TC posses SK_{TC}^S, and $SK_{TC}^S = H(M_S \times (A + H(ID_U||b_U)))$. Then, according to rule P4 again, we can get that TC posses $H(SK_{TC}^S)$.

$$\frac{TC \ni (M_S \times (A + H(ID_U||b_U)))}{TC \ni H(M_S \times (A + H(ID_U||b_U)))}(P4)$$

$$\frac{TC \ni SK_{TC}^S}{TC \ni H(SK_{TC}^S)}(P4)$$

Based on the rule P2, we can get that TC posses DID_U^*, and $DID_U^* = XDID_U^* \oplus H(SK_{TC}^S)$.

$$\frac{TC \ni XDID_U^*, TC \ni H(SK_{TC}^S)}{TC \ni XDID_U^* \oplus H(SK_{TC}^S))}(P2)$$

Based on A3 and the rule P2, we can get that TC posses $(X_U^0||DID_U^*||SK_{TC}^S||TS_{TC})$.

$$\frac{TC \ni X_U^0, TC \ni DID_U^*, TC \ni TS_{TC}}{TC \ni (X_U^0||DID_U^*||SK_{TC}^S||TS_{TC})}(P2)$$

Based on Goal 1 and the rule F1, we can get that TC believes that $(X_U^0||DID_U^*||SK_{TC}^S||TS_{TC})$ is fresh.

$$\frac{TC \mid\equiv \sharp SK_{TC}^S}{TC \mid\equiv \sharp(X_U^0||DID_U^*||SK_{TC}^S||TS_{TC})}(F1)$$

Based on the rule I3, we can get that TC believes that S once conveyed $(X_U^0||DID_U^*||SK_{TC}^S||TS_{TC})$, and $H_S = H(X_U^0||DID_U^*||SK_{TC}^S||TS_{TC})$.

$$\frac{\begin{array}{l} TC \triangleleft *H_S, TC \ni (X_U^0||DID_U^*||SK_{TC}^S||TS_{TC}), \\ TC \mid\equiv TC \overset{ID_U}{\leftrightarrow} S, \\ TC \mid\equiv \sharp(X_U^0||DID_U^*||SK_{TC}^S||TS_{TC}) \end{array}}{TC \mid\equiv tc \mid\sim (X_U^0||DID_U^*||SK_{TC}^S||TS_{TC})}(I3)$$

Based on the rule I7, we can get that TC believes that S once conveyed SK_{TC}^S.

$$\frac{TC \mid\equiv S \sim (X_U^0||DID_U^*||SK_{TC}^S||TS_{TC})}{TC \mid\equiv S \sim SK_{TC}^S}(I7)$$

Based on the rule I6, we can get that TC believes that S possesses SK_{TC}^S. Goal 3 is proved.

$$\frac{TC \mid\equiv S \mid\sim SK_{TC}^S, TC \mid\equiv \sharp SK_{TC}^S}{TC \mid\equiv S \ni SK_{TC}^S}(I6)$$

Goal 4:

Based on the rule F1, we can get that S believes that $\overrightarrow{v_S}$ is fresh, and $\overrightarrow{v_S} = (\beta, sk_{L_1}, \ldots, sk_{L_n})$.

$$\frac{S \mid\equiv \sharp\beta}{S \mid\equiv \sharp\,(\beta, sk_{L_1}, \ldots, sk_{L_n})}(F1)$$

Based on the rule F1, we can get that S believes that u_S is fresh, and $u_S = \overrightarrow{v_S} \cdot \overrightarrow{w_S}^\top$.

$$\frac{S \mid\equiv \sharp\overrightarrow{v_S}}{S \mid\equiv \sharp\overrightarrow{v_S} \cdot \overrightarrow{w_S}^\top}(F1)$$

Based on the rule F1, we can get that S believes that $(u_S \times (BID_U + M_{TC}))$ is fresh.

$$\frac{S \mid\equiv \sharp u_S}{S \mid\equiv \sharp(u_S \times (BID_U + M_{TC}))}(F1)$$

Based on A7 and the rule P2, we can get that S possesses $\overrightarrow{v_S}$ and $\overrightarrow{w_S}$, and $\overrightarrow{v_S} = (\beta, sk_{L_1}, \ldots, sk_{L_n}), \overrightarrow{w_S} = (1, sk_{R_1}, \ldots, sk_{R_n})$.

$$\frac{S \ni sk, S \ni \beta}{S \ni (\beta, sk_{L_1}, \ldots, sk_{L_n})}(P2)$$

$$\frac{S \ni sk}{S \ni (1, sk_{R_1}, \ldots, sk_{R_n})}(P2)$$

Based on the rule P2, we can get that S possesses u_S, and $u_S = \overrightarrow{v_S} \cdot \overrightarrow{w_S}^\top$.

$$\frac{S \ni \overrightarrow{v_S}, S \ni \overrightarrow{w_S}}{S \ni \overrightarrow{v_S} \cdot \overrightarrow{w_S}^\top}(P2)$$

Based on A7 and the rule P2, we can get that S possesses $(u_S \times (BID_U + M_{TC}))$.

$$\frac{S \ni u_S, S \ni BID_U, S \ni M_{TC}}{S \ni (u_S \times (BID_U + M_{TC}))}(P2)$$

Based on the rule F10, we can get that S believes that SK_{TC}^S is fresh, and $SK_{TC}^S = H(u_S \times (BID_U + M_{TC}))$. Goal 4 is proved.

$$\frac{\begin{array}{l} S \mid\equiv \sharp(u_S \times (BID_U + M_{TC})), \\ S \ni (u_S \times (BID_U + M_{TC})) \end{array}}{S \mid\equiv \sharp H(u_S \times (BID_U + M_{TC}))}(F10)$$

Goal 5: Based on the rule R1, we can get that S believes that $\overrightarrow{v_S}$ is recognizable, and $\overrightarrow{v_S} = (\beta, sk_{L_1}, \ldots, sk_{L_n})$.

$$\frac{S \mid\equiv \phi\beta}{S \mid\equiv \phi\,(\beta, sk_{L_1}, \ldots, sk_{L_n})}(R1)$$

Based on the rule R1, we can get that S believes that u_S is recognizable, and $u_S = \overrightarrow{v_S} \cdot \overrightarrow{w_S}^\top$.

$$\frac{S \mid\equiv \phi\overrightarrow{v_S}}{S \mid\equiv \phi\overrightarrow{v_S} \cdot \overrightarrow{w_S}^\top}(R1)$$

Based on the rule R1, we can get that S believes that $(u_S \times (BID_U + M_{TC}))$ is recognizable.

$$\frac{S \mid\equiv \phi u_S}{S \mid\equiv \phi(u_S \times (BID_U + M_{TC}))}(R1)$$

Based on the rule R5, we can get that S believes that SK_{TC}^S is recognizable, and $SK_{TC}^S = H(u_S \times (BID_U + M_{TC}))$. Goal 5 is proved.

$$\frac{\begin{array}{l} S \mid\equiv \phi(u_S \times (BID_U + M_{TC})), \\ S \ni (u_S \times (BID_U + M_{TC})) \end{array}}{S \mid\equiv \phi H(u_S \times (BID_U + M_{TC}))}(R5)$$

Goal 6: Based on the proof of Goal 3 and the rule P4, we can get that S possesses SK_{TC}^{S}, and $SK_{TC}^{S} = H(u_S \times (BID_U + M_{TC}))$.

$$\frac{S \ni (u_S \times (BID_U + M_{TC}))}{S \ni H(u_S \times (BID_U + M_{TC}))}(P4)$$

Based on A6 and the rule P2, we can get that S possesses $(SK_{TC}^{S}||ID_U||TS_{TC})$.

$$\frac{S \ni SK_{TC}^{S}, S \ni ID_U, TC \ni TS_{TC}}{S \ni (SK_{TC}^{S}||ID_U||TS_{TC})}(P2)$$

Based on Goal 4 and the rule F1, we can get that S believes that $(SK_{TC}^{S}||ID_U||TS_{TC})$ is fresh.

$$\frac{tc \mid\equiv \sharp SK_{TC}^{S}}{S \mid\equiv \sharp(SK_{TC}^{S}||ID_U||TS_{TC})}(F1)$$

Based on the rule I3, we can get that S believes that TC once conveyed $(SK_{TC}^{S}||ID_U||TS_{TC})$, and $H_{TC}^{ack} = H(SK_{TC}^{S}||ID_U||TS_{TC})$.

$$\frac{\begin{array}{l} S \triangleleft *H_{TC}^{ack}, S \ni (SK_{TC}^{S}||ID_U||TS_{TC}), \\ S \mid\equiv S \overset{ID_U}{\leftrightarrow} TC, \\ S \mid\equiv \sharp(SK_{TC}^{S}||ID_U||TS_{TC}) \end{array}}{S \mid\equiv TC \mid\sim (SK_{TC}^{S}||ID_U||TS_{TC})}(I3)$$

Based on the rule I7, we can get that S believes that TC once conveyed SK_{TC}^{S}.

$$\frac{S \mid\equiv TC \sim (SK_{TC}^{S}||ID_U||TS_{TC})}{tc \mid\equiv TC \sim SK_{TC}^{S}}(I7)$$

Based on the rule I6, we can get that S believes that TC possesses SK_{TC}^{S}. Goal 3 is proved.

$$\frac{S \mid\equiv TC \mid\sim SK_{TC}^{S}, S \mid\equiv \sharp SK_{TC}^{S}}{S \mid\equiv TC \ni SK_{TC}^{S}}(I6)$$