Table VII: GNY Expression

Notation	Description
P, Q	Parties of the session
(X, Y)	Conjunction of X and Y
$H(X)$	H is a one-way function of X
$F(X_1, ..., X_n)$	F is a many-to-one computationally feasible function for any X_i
$*X$	X is a not-originated-here
$P \triangleleft X$	P is told X
$P \ni X$	P possesses, or is capable of possessing X
$P \mid\sim X$	P once conveyed formula X
$P \mid\equiv \sharp(X)$	X has not been used for the same purpose at any time before the current run of the protocol
$P \mid\equiv \emptyset(X)$	P would recognize X if P has certain expectations about the contents of X before actually receiving X
$P \xleftrightarrow{K} Q$	K is a shared secret between P and Q
LR	LR achieves leakage-resilient according to Dziembowski *et al.* [22], [31](additional expression)

Appendix B
CLR-eGNY Logic Analysis

The notations and statements are summarized in Table VII.

1) Description

The parser algorithm would produce the following description of LLRA based on above paraphrases:
$Msg_1 : S_B \triangleleft *X_A, *Y_A, *T_A, *C_A, *Auth$;
$Msg_2 : U_A \triangleleft *X_B, *Y_B, *T_B, *E_B$;
$Msg_3 : S_B \triangleleft *E_A$.

2) Goal

The shared session keys between U_A and U_B shall achieve the following goals:
Goal 1: $U_A \mid\equiv \sharp SK$;
Goal 2: $U_A \mid\equiv \phi SK$;
Goal 3: $U_A \mid\equiv U_B \ni SK$;
Goal 4: $U_B \mid\equiv \sharp SK$;
Goal 5: $U_B \mid\equiv \phi SK$;
Goal 6: $U_B \mid\equiv U_A \ni SK$.

3) Initial Assumptions

Referring to LLRA's registration phrase, we have several initialization assumptions:
A1: $U_A \mid\equiv \sharp y_A$;
A2: $U_A \mid\equiv \phi y_A$;
A3: $U_A \ni y_A, ID_A, hw_A, D_A, \overrightarrow{r_{AL}}, \overrightarrow{r_{AR}}, G, Z_A, Z_B$;
A4: $S_B \mid\equiv \sharp y_B$;
A5: $S_B \mid\equiv \phi y_B$;
A6: $S_B \ni y_B, ID_B, hw_B, D_B, \overrightarrow{r_{BL}}, \overrightarrow{r_{BR}}, G, Z_A, Z_B$;
A7: $U_A \mid\equiv S_B \ni Z_A, Z_B$;
A8: $S_B \mid\equiv U_A \ni Z_A, Z_B$;
A9: $U_A \mid\equiv U_A \overset{pw}{\leftrightarrow} S_B$;
A10: $S_B \mid\equiv S_B \overset{pw}{\leftrightarrow} U_A$;
A11: $U_A \mid\equiv S_B \mid\Longrightarrow S_B \mid\equiv *$;
A12: $S_B \mid\equiv U_A \mid\Longrightarrow U_A \mid\equiv *$;
A13: $U_A \mid\equiv S_B \mid\Longrightarrow S_B \ni (u_B, y_B)$;
A14: $S_B \mid\equiv U_A \mid\Longrightarrow U_A \ni (u_A, y_A)$;
A15: $U_A \mid\equiv \Lambda(r_A)$;
A16: $S_B \mid\equiv \Lambda(r_B)$.

4) Proof

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

According to rules T1 and P1, we can get that U_A possesses $X_B, Y_B, T_B, E_B, X_A, Y_A, T_A, E_A$.

$$\cfrac{\cfrac{U_A \triangleleft *X_B, *Y_B, *T_B, *E_B}{U_A \triangleleft X_B, Y_B, T_B, E_B}(T1)}{U_A \ni X_B, Y_B, T_B, E_B}(P1)$$

According to rules T1 and P1, we can get that U_B possesses $X_A, Y_A, T_A, C_A, Auth, E_A$.

$$\cfrac{\cfrac{U_B \triangleleft *X_A, *Y_A, *T_A, *C_A, *Auth, *E_A}{U_B \triangleleft X_A, Y_A, T_A, C_A, Auth, E_A}(T1)}{U_B \ni X_A, Y_A, T_A, C_A, Auth, E_A}(P1)$$

Goal 1: According to A1 and the rule F1, we can get that U_A believes that $((u_A + y_A) \cdot G)$ is fresh. and $Y_A = (u_A + y_A) \cdot G$.

$$\frac{U_A \mid\equiv \sharp y_A}{U_A \mid\equiv \sharp((u_A + y_A) \cdot G)}(F1)$$

According to the rule F1, we can get that U_A believes that $(X_A||Y_A||X_B||Y_B)$ is fresh. and $sid_A = Z_A||Y_A||Z_B||Y_B$.

$$\frac{U_A \mid\equiv \sharp Y_A}{U_A \mid\equiv \sharp(Z_A||Y_A||Z_B||Y_B)}(F1)$$

According to the rule F1, we can get that U_A believes that $(sk_A||sid_A)$ is fresh.

$$\frac{U_A \mid\equiv \sharp sid_A}{U_A \mid\equiv \sharp(sk_A||sid_A)}(F1)$$

According to A3 and the rule P2, we can get that $U_A \ni (\overrightarrow{v_A}, \overrightarrow{w_A})$.

$$\cfrac{\cfrac{U_A \ni y_A, \overrightarrow{r_{AL}}, \overrightarrow{r_{AR}}}{U_A \ni (\overrightarrow{v_A}, \overrightarrow{w_A})}(P2)}{U_A \ni u_A}(P2)$$

According to A3 and the rule P4, we can get that $U_A \ni H_2(s_A)$.

$$\frac{U_A \ni s_A}{U_A \ni H_2(s_A)}(P4)$$

According to A3 and the rule P2, we can get that $U_A \ni H_2(s_A) \oplus ID_A$, so we can get that $U_A \ni D_A$.

$$\frac{U_A \ni H_2(s_A), ID_A}{U_A \ni H_2(s_A) \oplus ID_A}(P2)$$

According to the A3 and rule P2, we can get that $U_A \ni hw_A \oplus D_A \oplus u_A \oplus y_A$.

$$\frac{U_A \ni hw_A, D_A, u_A, y_A}{U_A \ni hw_A \oplus D_A \oplus u_A \oplus y_A}(P2)$$

According to the rule P4, we can get that $U_A \ni H_2(hw_A \oplus D_A \oplus u_A \oplus y_A)$.so we can get that $U_A \ni X_A$.

$$\frac{U_A \ni hw_A \oplus D_A \oplus u_A \oplus y_A}{U_A \ni H_2(hw_A \oplus D_A \oplus u_A \oplus y_A)}(P2)$$

According to the A3 and the rule P2, we can get that $U_A \ni ((u_A + y_A) \cdot Y_B)$, so we can get that $U_A \ni V_A$.

$$\frac{U_A \ni u_A, y_A, Y_B}{U_A \ni ((u_A + y_A) \cdot Y_B)}(P2)$$

According to the rule P4, we can get that $U_A \ni H_3(V_A)$.

$$\frac{U_A \ni V_A}{U_A \ni H_3(V_A)}(P4)$$

According to the A3 and the rule P2, we can get that $U_A \ni ((u_A + y_A) \cdot G)$, so we can get that $U_A \ni Y_A$.

$$\frac{U_A \ni u_A, y_A, G}{U_A \ni ((u_A + y_A) \cdot G)}(P2)$$

According to the rule P2, we can get that $U_A \ni (X_A||Y_A||X_B||Y_B)$, so we can get that $U_A \ni sid_A$.

$$\frac{U_A \ni Z_A, Y_A, Z_B, Y_B}{U_A \ni Z_A||Y_A||Z_B||Y_B}(P2)$$

According to the A3 and the rule P2, we can get that $U_A \ni (X_A \oplus X_B \oplus H_3(V_A))$, so we can get that $U_A \ni sk_A$.

$$\frac{U_A \ni X_A, X_B, H_3(V_A)}{U_A \ni (X_A \oplus X_B \oplus H_3(V_A))}(P2)$$

According to the rule P2, we can get that $U_A \ni (sk_A||sid_A)$.

$$\frac{U_A \ni sk_A, sid_A}{U_A \ni sk_A||sid_A}(P2)$$

According to the rule F10, we can get that U_A believes that SK is fresh.

$$\frac{U_A \mid\equiv \sharp(sk_A||sid_A), U_A \ni (sk_A||sid_A)}{\dfrac{U_A \mid\equiv \sharp H(sk_A||sid_A)}{U_A \mid\equiv \sharp SK}}(F10)$$

Goal 2: According to A1 and the rule R1, we can get that U_A believes that $((u_A + y_A) \cdot G)$ is recognizable.

$$\frac{U_A \mid\equiv \phi y_A}{U_A \mid\equiv \phi((u_A + y_A) \cdot G)}(R1)$$

According to the rule R1, we can get that U_A believes that $(Z_A||Y_A||Z_B||Y_B)$ is recognizable.

$$\frac{U_A \mid\equiv \phi Y_A}{U_A \mid\equiv \phi(Z_A||Y_A||Z_B||Y_B)}(R1)$$

According to the rule R1, we can get that U_A believes that $(sk_A||sid_A)$ is recognizable.

$$\frac{U_A \mid\equiv \phi sid_A}{U_A \mid\equiv \phi(sk_A||sid_A)}(R1)$$

According to the rule R10, we can get that U_A believes that SK is recognizable.

$$\frac{U_A \mid\equiv \phi(sk_A||sid_A), U_A \ni (sk_A||sid_A)}{\dfrac{U_A \mid\equiv \phi H(sk_A||sid_A)}{U_A \mid\equiv \phi SK}}(R5)$$

Goal 3: According to A1 and the rule F10, we can get that S_A believes that X_A is fresh, and $X_A = H_2(hw_A \oplus D_A \oplus u_A \oplus y_A)$.

$$\frac{U_A \mid\equiv \sharp y_A, U_A \ni (hw_A \oplus D_A \oplus u_A \oplus y_A)}{U_A \mid\equiv \sharp H_2(hw_A \oplus D_A \oplus u_A \oplus y_A)}(F10)$$

According to the rule F1, we can get that U_A believes that sk_A is fresh, and $sk_A = X_B \oplus X_A \oplus H_3(V_A)$.

$$\frac{U_A \mid\equiv \sharp X_A}{U_A \mid\equiv \sharp(X_B \oplus X_A \oplus H_3(V_A))}(F1)$$

According to A2 and the rule R5, we can get that U_A believes that X_A is recognizable, and $X_A = H_2(hw_A \oplus D_A \oplus u_A \oplus y_A)$.

$$\frac{U_A \mid\equiv \phi y_A, U_A \ni (hw_A \oplus D_A \oplus u_A \oplus y_A)}{U_A \mid\equiv \phi H_2(hw_A \oplus D_A \oplus u_A \oplus y_A)}(R5)$$

According to the rule R1, we can get that U_A believes that sk_A is recognizable.

$$\frac{U_A \mid\equiv \phi X_A}{U_A \mid\equiv \phi(T_B, hw_B, y_B, X_A, V_B, T_A)}(R1)$$

According to A9 and the rule I1, we can get that U_A believes that S_B once conveyed $(T_B, hw_B, y_B, X_A, V_B, T_A)$, and U_A owns sk_B.

$$\frac{\begin{array}{l} U_A \triangleleft *E_B, U_A \ni sk_B, U_A \mid\equiv U_A \overset{pw}{\leftrightarrow} S_B, \\ U_A \mid\equiv \phi(T_B, hw_B, y_B, X_A, V_B, T_A), U_A \mid\equiv \sharp sk_B \end{array}}{U_A \mid\equiv S_B \mid\sim (T_B, hw_B, y_B, X_A, V_B, T_A), U_A \mid\equiv S_B \ni sk_B}(I1)$$

According to the rule I7, we can get that U_A believes that S_B once conveyed V_B.

$$\frac{U_A \mid\equiv S_B \mid\sim (T_B, hw_B, y_B, X_A, V_B, T_A)}{U_A \mid\equiv S_B \mid\sim V_B}(I7)$$

According to the rule F1, we can get that U_A believes that V_B is fresh, and $V_B = (u_B + y_B) \cdot Y_A$.

$$\frac{U_A \mid\equiv \sharp Y_A}{U_A \mid\equiv \sharp(u_B + y_B) \cdot Y_A}(F1)$$

According to our new GNY expression, we can get that $U_A \mid\equiv \Lambda(r_A)$.

$$\frac{\begin{array}{l} U_A \ni Encode_{\mathbb{Z}_q^*}^{n,m}(r_A), \\ U_A \mid\sim (f_1(r_{AL}), f_2(r_{AR})), U_A \ni SK_A, \\ U_A \ni \mathrm{Refresh}_{\mathbb{Z}_q^*}^{n,m}(r_{AL}, r_{AR}) \end{array}}{U_A \mid\equiv \Lambda(r_A)}$$

According to A11 and the rule LRJ2, we can get that U_A believes that S_B believes that S_B possesses u_B.

$$\frac{\begin{array}{l} U_A \mid\equiv S_B \mid\Longrightarrow S_B \mid\equiv *, \\ U_A \mid\equiv \mathrm{S_B} \mid\sim (V_B \rightsquigarrow (S_B \ni u_B), \\ U_A \mid\equiv \sharp V_B, U_A \mid\equiv \Lambda(r_A), S_B \mid\equiv \Lambda(r_B) \end{array}}{U_A \mid\equiv S_B \mid\equiv (S_B \ni u_B)}(LRJ2)$$

According to A13 and the rule LRJ1, we can get that U_A believes that S_B possesses u_B.

$$\frac{\begin{array}{l} U_A \mid\equiv S_B \mid\Longrightarrow S_B \ni u_B, \\ U_A \mid\equiv S_B \mid\equiv (S_B \ni u_B), \\ U_A \mid\equiv \Lambda(r_A), S_B \mid\equiv \Lambda(r_B) \end{array}}{U_A \mid\equiv S_B \ni u_B}(LRJ1)$$

According to the rationality rule from postulate P3, we can get that $U_A \mid\equiv S_B \ni y_B$.

$$\frac{U_A \mid\equiv S_B \ni u_B}{U_A \mid\equiv S_B \ni y_B}(RP3)$$

According to the rationality rule from postulate P2, we can get that $U_A \mid\equiv S_B \ni (u_B + y_B) \cdot G$, so we can obtain that $U_A \mid\equiv S_B \ni Y_B$.

$$\frac{U_A \mid\equiv S_B \ni u_B, y_B, G}{U_A \mid\equiv S_B \ni (u_B + y_B) \cdot G}(RP2)$$

According to the rule I6, we can get that $U_A \mid\equiv S_B \ni V_B$.

$$\frac{U_A \mid\equiv S_B \mid\sim V_B, U_A \mid\equiv \sharp V_B}{U_A \mid\equiv S_B \ni V_B}(I6)$$

According to the rationality rule from postulate P5, we can get that $U_A \mid\equiv S_B \ni Y_A$.

$$\frac{U_A \mid\equiv S_B \ni ((u_B + y_B) \cdot Y_A), U_A \mid\equiv S_B \ni u_B, y_B}{U_A \mid\equiv S_B \ni Y_A}(RP5)$$

According to the rationality rule from postulate P2, we can get that $U_A \mid\equiv S_B \ni Z_A||Z_B||Y_A||Y_B$, so we can obtain that $U_A \mid\equiv S_B \ni sid_B$.

$$\frac{U_A \mid\equiv S_B \ni Z_A, Z_B, Y_A, Y_B}{U_A \mid\equiv S_B \ni Z_A||Z_B||Y_A||Y_B}(RP2)$$

According to the rationality rule from postulate P2 and P4, we can get that $U_A \mid\equiv S_B \ni H(sk_B||sid_B)$, so we can obtain that $U_A \mid\equiv S_B \ni SK_B$.

$$\frac{U_A \mid\equiv S_B \ni sk_B, sid_B}{U_A \mid\equiv S_B \ni sk_B||sid_B}(RP2)(RP4)$$

Goal 4:

According to the rule F1 and A4, we can get that S_B believes that Y_B is fresh, and $Y_B = (u_B + y_B) \cdot G$.

$$\frac{S_B \mid\equiv \sharp y_B}{S_B \mid\equiv \sharp\left((u_B + y_B) \cdot G\right)}(F1)$$

According to the rule F1, we can get that S_B believes that sid_B is fresh, and $sid_B = Z_A, Y_A, Z_B, Y_B$.

$$\frac{S_B \mid\equiv \sharp Y_B}{S_B \mid\equiv \sharp\left(Z_A, Y_A, Z_B, Y_B\right)}(F1)$$

According to the rule F1, we can get that S_B believes that (sk_B, sid_B) is fresh.

$$\frac{S_B \mid\equiv \sharp sid_B}{S_B \mid\equiv \sharp\left(sk_B, sid_B\right)}(F1)$$

According to A6 and the rule P2, we can get that S_B possesses $\overrightarrow{v_B}$ and $\overrightarrow{w_B}$, and $\overrightarrow{v_B} = (y_B, r_{BL_1}, \ldots, r_{BL_n}), \overrightarrow{w_B} = (1, r_{BR_1}, \ldots, r_{BR_n})$.

$$\frac{S_B \ni \overrightarrow{r_{BL}}, S_B \ni y_B}{S_B \ni \overrightarrow{v_B}}(P2)$$

$$\frac{S_B \ni \overrightarrow{r_{BR}}}{S_B \ni \overrightarrow{w_B}}(P2)$$

According to the rule P2, we can get that S_B possesses u_B, and $u_B = \overrightarrow{v_B} \cdot \overrightarrow{w_B}$.

$$\frac{S_B \ni \overrightarrow{v_B}, S_B \ni \overrightarrow{w_B}}{S_B \ni \overrightarrow{v_B} \cdot \overrightarrow{w_B}}(P2)$$

According to the rule P4, we can get that S_B possesses X_B, and $X_B = H_2(hw_B \oplus D_B \oplus u_B \oplus y_B)$.

$$\frac{S_B \ni hw_B, S_B \ni D_B, S_B \ni u_B, S_B \ni y_B}{S_B \ni H_2(hw_B \oplus D_B \oplus u_B \oplus y_B)}(P4)$$

According to A6 and the rule P2, we can get that S_B possesses Y_B, and $Y_B = (u_B + y_B) \cdot G$.

$$\frac{S_B \ni u_B, S_B \ni y_B, S_B \ni G}{S_B \ni (u_B + y_B) \cdot G}(P2)$$

According to the rule P2, we can get that S_B possesses V_B, and $V_B = (u_B + y_B) \cdot Y_A$.

$$\frac{S_B \ni Y_A, S_B \ni u_B, S_B \ni y_B}{S_B \ni (u_B + y_B) \cdot Y_A}(P2)$$

According to the rule P4, we can get that S_B possesses $H_3(V)$.

$$\frac{S_B \ni v}{S_B \ni H_3(V)}(P4)$$

According to the rule P2, we can get that S_B possesses sk_B, and $sk_B = X_A \oplus X_B \oplus H_3(V)$.

$$\frac{S_B \ni X_A, S_B \ni X_B, S_B \ni H_3(V)}{S_B \ni X_A \oplus X_B \oplus H_3(V)}(P2)$$

According to the rule P2, we can get that S_B possesses sk_B, sid_B, and $sid_B = Z_A, Y_A, Z_B, Y_B$.

$$\frac{\dfrac{S_B \ni Z_A, S_B \ni Y_A, S_B \ni Z_B, S_B \ni Y_B}{S_B \ni (Z_A||Y_A||Z_B||Y_B)}(P2)}{S_B \ni (sk_B||sid_B)}(P2)$$

According to the rule F10, we can get that S_B believes that SK is fresh, and $SK = H(sk_B||sid_B)$. Goal 4 is proved.

$$\frac{S_B \mid\equiv \sharp(sk_B||sid_B), S_B \ni (sk_B||sid_B)}{S_B \mid\equiv \sharp H(sk_B||sid_B)}(F10)$$

Goal 5: According to the rule R1 and A5, we can get that S_B believes that Y_B is recognizable, and $Y_B = (u_B + y_B) \cdot G$.

$$\frac{S_B \mid\equiv \phi y_B}{S_B \mid\equiv \phi\left((u_B + y_B) \cdot G\right)}(R1)$$

According to the rule R1, we can get that S_B believes that sid_B is recognizable, and $sid_B = Z_A, Y_A, Z_B, Y_B$.

$$\frac{S_B \mid\equiv \phi Y_B}{S_B \mid\equiv \phi\left(Z_A, Y_A, Z_B, Y_B\right)}(R1)$$

According to the rule R1, we can get that S_B believes that (sk_B, sid_B) is recognizable.

$$\frac{S_B \mid\equiv \phi sid_B}{S_B \mid\equiv \phi\left(sk_B, sid_B\right)}(R1)$$

According to the rule R5, we can get that S_B believes that SK is recognizable, and $SK = H(sk_B||sid_B)$. Goal 5 is proved.

$$\frac{S_B \mid\equiv \phi(sk_B||sid_B), S_B \ni (sk_B||sid_B)}{S_B \mid\equiv \phi H(sk_B||sid_B)}(R5)$$

Goal 6: According to A4 and the rule F10, we can get that S_B believes that X_B is fresh, and $X_B = H_2(hw_B \oplus D_B \oplus u_B \oplus y_B)$.

$$\frac{S_B \mid\equiv \sharp y_B, S_B \ni (hw_B \oplus D_B \oplus u_B \oplus y_B)}{S_B \mid\equiv \sharp H_2(hw_B \oplus D_B \oplus u_B \oplus y_B)}(F10)$$

According to the rule F1, we can get that S_B believes that sk_B is fresh, and $sk_B = X_A \oplus X_B \oplus H_3(V_B)$.

$$\frac{S_B \mid\equiv \sharp X_B}{S_B \mid\equiv \sharp(X_A \oplus X_B \oplus H_3(V_B))}(F1)$$

According to A5 and the rule R5, we can get that S_B believes that X_B is recognizable, and $X_B = H_2(hw_B \oplus D_B \oplus u_B \oplus y_B)$.

$$\frac{S_B \mid\equiv \phi y_B, S_B \ni (hw_B \oplus D_B \oplus u_B \oplus y_B)}{S_B \mid\equiv \phi H_2(hw_B \oplus D_B \oplus u_B \oplus y_B)}(R5)$$

According to the rule R1, we can get that S_B believes that sk_B is recognizable.

$$\frac{S_B \mid\equiv \phi X_B}{S_B \mid\equiv \phi(T_B, hw_A, y_A, u_A, X_B, V_A)}(R1)$$

According to A10 and the rule I1, we can get that S_B believes that U_A once conveyed $(T_B, hw_A, y_A, u_A, X_B, V_A)$, and U_A owns sk_A.

$$\frac{\begin{array}{l} S_B \triangleleft *E_A, S_B \ni sk_A, S_B \mid\equiv S_B \overset{pw}{\leftrightarrow} U_A, \\ S_B \mid\equiv \phi(T_B, hw_A, y_A, u_A, X_B, V_A), S_B \mid\equiv \sharp sk_A \end{array}}{S_B \mid\equiv U_A \mid\sim (T_B, hw_A, y_A, u_A, X_B, V_A), S_B \mid\equiv U_A \ni sk_A}(I1)$$

According to the rule I7, we can get that S_B believes that U_A once conveyed V_A.

$$\frac{S_B \mid\equiv U_A \mid\sim (T_B, hw_A, y_A, u_A, X_B, V_A)}{S_B \mid\equiv U_A \mid\sim V_A}(I7)$$

According to the rule F1, we can get that S_B believes that V_A is fresh, and $V_A = (u_A + y_A) \cdot Y_B$.

$$\frac{S_B \mid\equiv \sharp Y_B}{S_B \mid\equiv \sharp(u_A + y_A) \cdot Y_B}(F1)$$

According to our new GNY expression we can get that S_B achieves leakage-resilient.

$$\frac{\begin{array}{l} S_B \ni Encode^{n,m}_{\mathbb{Z}_q^*}(r_B), \\ S_B \mid\sim (f_1(r_{BL}), f_2(r_{BR})), \\ S_B \ni SK_B, S_B \ni \mathrm{Refresh}^{n,m}_{\mathbb{Z}_q^*}(r_{BL}, r_{BR}) \end{array}}{S_B \mid\equiv \Lambda(r_B)}$$

According to A12 and the rule LRJ2, we can get that S_B believes that U_A believes that U_A possesses u_A.

$$\frac{\begin{array}{l} S_B \mid\equiv U_A \mid\Longrightarrow U_A \mid\equiv *, \\ S_B \mid\equiv \mathrm{U_A} \mid\sim (V_A \rightsquigarrow (U_A \ni u_A)), \\ S_B \mid\equiv \sharp V_A, U_A \mid\equiv \Lambda(r_A), S_B \mid\equiv \Lambda(r_B) \end{array}}{S_B \mid\equiv U_A \mid\equiv (U_A \ni u_A)}(LRJ2)$$

According to A14 and the rule LRJ1, we can get that S_B believes that U_A possesses u_A.

$$\frac{\begin{array}{l} S_B \mid\equiv U_A \mid\Longrightarrow U_A \ni u_A, \\ S_B \mid\equiv U_A \mid\equiv (U_A \ni u_A), \\ U_A \mid\equiv \Lambda(r_A), S_B \mid\equiv \Lambda(r_B) \end{array}}{S_B \mid\equiv U_A \ni u_A}(LRJ1)$$

According to the rationality rule from postulate P3, we can get that $S_B \mid\equiv U_A \ni y_A$.

$$\frac{S_B \mid\equiv U_A \ni u_A}{S_B \mid\equiv U_A \ni y_A}(RP3)$$

According to the rationality rule from postulate P2, we can get that $S_B \mid\equiv U_A \ni (u_A + y_A) \cdot G$, so we can obtain that $S_B \mid\equiv U_A \ni Y_A$.

$$\frac{S_B \mid\equiv U_A \ni u_A, y_A, G}{S_B \mid\equiv U_A \ni (u_A + y_A) \cdot G}(RP2)$$

According to the rule I6, we can get that $S_B \mid\equiv U_A \ni V_A$.

$$\frac{S_B \mid\equiv U_A \mid\sim V_A, S_B \mid\equiv \sharp V_A}{S_B \mid\equiv U_A \ni V_A}(I6)$$

According to the rationality rule from postulate P5, we can get that $S_B \mid\equiv U_A \ni Y_B$.

$$\frac{S_B \mid\equiv U_A \ni ((u_A + y_A) \cdot Y_B), S_B \mid\equiv U_A \ni u_A, y_A}{S_B \mid\equiv U_A \ni Y_B}(RP5)$$

According to the rationality rule from postulate P2, we can get that $S_B \mid\equiv U_A \ni Z_A||Z_B||Y_A||Y_B$, so we can obtain that $S_B \mid\equiv U_A \ni sid_A$.

$$\frac{S_B \mid\equiv U_A \ni Z_A, Z_B, Y_A, Y_B}{S_B \mid\equiv U_A \ni Z_A||Z_B||Y_A||Y_B}(RP2)$$

According to the rationality rule from postulate P2 and P4, we can get that $S_B \mid\equiv U_A \ni H(sk_A||sid_A)$, so we can obtain that $S_B \mid\equiv U_A \ni SK_A$.

$$\frac{S_B \mid\equiv U_A \ni sk_A, sid_A}{S_B \mid\equiv U_A \ni sk_A||sid_A}(RP2)(RP4)$$