Appendix A Language Theorem Proofs

T1 $R(x, \phi \wedge \psi) \rightarrow R(x, \phi) \wedge R(x, \psi)$

Proof.

1. $R(x, \phi \wedge \psi)$	*assumption*
2. $\phi \wedge \psi \rightarrow \phi$	*tautology*
3. $R(x, \phi)$	*1,2 Axiom* ***R2***
4. $\phi \wedge \psi \rightarrow \psi$	*tautology*
5. $R(x, \psi)$	*1,4 Axiom* ***R2***
6. $R(x, \phi) \wedge R(x, \psi)$	*3* $\wedge$ *5*
7. $R(x, \phi \wedge \psi) \rightarrow R(x, \phi) \wedge R(x, \psi)$	*1,6* $\rightarrow$ *intro*

□

T2 $B(x, \phi) \rightarrow R(x, \phi)$

Proof.

1. $B(x, \phi)$	*assumption*
2. $B(x, \top \rightarrow \phi)$	*FOL*
3. $B(x, \top)$	*FOL*
4. $\neg B(x, \neg \top)$	*3, FOL*
5. $B(x, \top \rightarrow \phi) \wedge \neg B(x, \neg \top)$	*2* $\wedge$ *4*
6. $R(x, \top) \rightarrow R(x, \phi)$	*5, Axiom* ***BR1***
7. $R(x, \top)$	*by definition of R*
8. $R(x, \phi)$	*6,7* $\rightarrow$ *elim*
9. $B(x, \phi) \rightarrow R(x, \phi)$	*1,8* $\rightarrow$ *intro*

□

T3 $R(x, \phi) \leftrightarrow R(x, R(x, \phi))$

Proof.

1. $R(x, \phi)$	*assumption*
2. $R(x, \phi) \rightarrow B(x, R(x, \phi))$	*Axiom* ***BR2***
3. $B(x, R(x, \phi))$	*1,2* $\rightarrow$ *elim*
4. $R(x, R(x, \phi))$	*3, Theorem* ***T2***
5. $R(x, \phi) \rightarrow R(x, R(x, \phi))$	*1,4* $\rightarrow$ *intro*
6. $R(x, R(x, \phi))$	*assumption*
7. $R(x, \phi)$	*6, Axiom* ***R3***
8. $R(x, R(x, \phi)) \rightarrow R(x, \phi)$	*6,7* $\rightarrow$ *intro*
9. $R(x, \phi) \leftrightarrow R(x, R(x, \phi))$	*5,8* $\leftrightarrow$ *intro*

□

T4 $B(x, \phi) \rightarrow B(x, R(x, \phi))$

Proof.

1. $B(x, \phi)$	*assumption*
2. $B(x, B(x, \phi))$	*1, FOL*
3. $B(x, B(x, \phi) \rightarrow R(x, \phi))$	*Axiom* ***T2***
4. $B(x, R(x, \phi))$	*2,3 K Axiom for B*

5. $B(x,\phi) \rightarrow B(x,R(x,\phi))$ *1,4 → intro*

□

T5 $B(x,R(x,\phi)) \rightarrow R(x,\phi)$
Proof.

1. $B(x,R(x,\phi))$ *assumption*
2. $R(x,R(x,\phi))$ *1, Theorem* ***T2***
3. $R(x,\phi)$ *2, Axiom* ***R3***
4. $B(x,R(x,\phi)) \rightarrow R(x,\phi)$ *1,3 → intro*

□

T6 $B(x,\neg R(x,\phi)) \rightarrow \neg R(x,\phi)$
Proof.

1. $B(x,\neg R(x,\phi))$ *assumption*
2. $\neg B(x,R(x,\phi))$ *1, D Axiom for B*
3. $\neg R(x,\phi)$ *2, Axiom* ***BR2***
4. $B(x,\neg R(x,\phi)) \rightarrow \neg R(x,\phi)$ *1,3 → intro*

□

T7 $R(x,B(x,\phi)) \rightarrow B(x,R(x,\phi))$
Proof.

1. $R(x,B(x,\phi))$ *assumption*
2. $B(x,\phi) \rightarrow R(x,\phi)$ *Theorem* ***T2***
3. $R(x,R(x,\phi))$ *1,2 Axiom* ***R2***
4. $R(x,\phi)$ *3, Theorem* ***T3***
5. $B(x,R(x,\phi))$ *4, Axiom* ***BR2***
6. $R(x,B(x,\phi)) \rightarrow B(x,R(x,\phi))$ *1,5 → intro*

□

Appendix B Proofs of the Theorem on Secrets

Theorem 1 *1.* $\Sigma \vdash \forall x[R(x,S \wedge \exists y Mem(y,K,t)) \rightarrow R(x,\phi)]$.
Proof.

1. $S \wedge Mem(A,K,t)$ assumption
2. $\neg NFE(K,t) \wedge \forall x Mem(x,K,t) \rightarrow B(x,\phi \wedge \psi \wedge \neg NFE(N,t),t) \wedge$ $\neg \mathcal{B}(\phi,x,N,t) \wedge \mathcal{I}(\phi,x,N,\psi,t)$ 1, $\wedge$ elim, S definition
3. $Mem(A,K,t)$ 1, $\wedge$ elim
4. $B(A,\phi \wedge \psi \wedge \neg NFE(N,t),t)$ 2,3 $\rightarrow, \wedge$ elim
5. $B(A,\phi,t)$ 4, FOL
6. $S \wedge Mem(A,K,t) \rightarrow B(A,\phi,t)$ 1,5 $\rightarrow$ intro
7. $\exists x[S \wedge Mem(x,K,t) \rightarrow B(x,\phi,t)]$ 6, $\exists$ intro
8. $R(x,S \wedge \exists y Mem(y,K,t),t)$ assumption
9. $R(x,B(y,\phi,t),t)$ 7,8 Axiom **R2**
10. $R(x,R(y,\phi,t),t)$ 8, Theorem **T2**,Axiom **R2**
11. $R(x,\phi,t)$ 10, Axiom **R3**

12. $R(x, S \wedge \exists y Mem(y, K, t)) \rightarrow R(x, \phi)$ 8,11 $\rightarrow$ intro
13. $\forall x[R(x, S \wedge \exists y[Mem(y, K, t)], t) \rightarrow R(x, \phi)]$ 12, $\forall$ intro

□

2. $\Sigma \vdash S \wedge Mem(x, K, t) \rightarrow \neg B(x, \exists y[Mem(y, N, t) \wedge R(y, S \wedge \exists z Mem(z, K, t), t)], t)$

Proof.

1. $S \wedge Mem(x, K, t) \wedge B(x, \exists y[Mem(y, N, t) \wedge R(y, S \wedge \exists z Mem(z, K, t), t)], t)$ assumption
2. $B(A, Mem(Y, N, t) \wedge R(Y, S \wedge \exists z[Mem(z, K, t)], t), t)$ 1, $\wedge$, $\exists$ elim
3. $B(A, R(Y, S \wedge \exists z Mem(z, K, t), t), t)$ 2, FOL
4. $B(A, Mem(Y, N, t) \wedge R(Y, \phi, t), t)$ 2,3, Theorem 1.1, FOL
5. $S \wedge Mem(A, K, t)$ 1, $\wedge$, $\forall$ elim
6. $\neg B(A, \exists y[Mem(y, N, t) \wedge R(y, \phi, t)], t)$ 5,S def $\rightarrow$ elim
7. $B(A, \exists y[Mem(y, N, t) \wedge R(y, \phi, t)], t)$ 4, $\exists$ intro
8. $\neg B(A, \exists y[Mem(y, N, t) \wedge R(y, \phi, t)], t) \wedge B(A, \exists y[Mem(y, N, t) \wedge R(y, \phi, t)], t)$ $7 \wedge 8$
9. $S \wedge Mem(x, K, t) \rightarrow \neg B(x, \exists y[Mem(y, N, t) \wedge R(y, S \wedge \exists z[Mem(z, K, t), t)]], t)$ 1,8 $\neg$ intro

□

Theorem 2 *1.* $\Sigma \vdash S \wedge K' \sqsubseteq K \wedge N' \sqsubseteq N \wedge \neg NFE(K', t) \wedge \forall x[Mem(x, K', t) \rightarrow B(x, \neg NFE(N', t), t)] \rightarrow Secret_0(\phi, K', N', \psi, t)$

Proof.

1. $S \wedge K' \sqsubseteq K \wedge N' \sqsubseteq N \wedge \neg NFE(K', t) \wedge \forall x[Mem(x, K', t) \rightarrow B(x, \neg NFE(N', t), t)] \wedge \neg Secret_0(\phi, K', N', \psi, t)$ assumption
2. $\neg Secret_0(\phi, K', N', \psi, t)$ 1, $\wedge$ elim
3. $\neg[\neg NFE(K', t) \wedge \forall x[Mem(x, K', t) \rightarrow B(x, \phi \wedge \psi \wedge \neg NFE(N', t), t) \wedge \neg \mathcal{B}(\phi, x, N', t) \wedge \mathcal{I}(\phi, x, N', \psi, t)]$ 2, S definition
4. $NFE(K', t) \vee \exists x Mem(x, K', t) \wedge \neg[B(x, \phi \wedge \psi \wedge \neg NFE(N', t), t) \wedge \neg \mathcal{B}(\phi, x, N', t) \wedge \mathcal{I}(\phi, x, N', \psi, t)]$ 3, $\neg$ elim
5. $NFE(K', t)$ 4, assumption
6. $\neg NFE(K', t)$ 1, $\wedge$ elim
7. $NFE(K', t) \wedge \neg NFE(K', t)$ $4 \wedge 5$
8. $\neg NFE(K', t)$ 5,7 $\neg$ intro
9. $\exists x Mem(x, K', t) \wedge \neg[B(x, \phi \wedge \psi \wedge \neg NFE(N', t), t) \wedge \neg \mathcal{B}(\phi, x, N', t) \wedge \mathcal{I}(\phi, x, N', \psi, t)]$ 4,8 $\vee$ elim
10. $Mem(A, K', t) \wedge \neg[B(A, \phi \wedge \psi \wedge \neg NFE(N', t), t) \wedge \neg \mathcal{B}(\phi, A, N', t) \wedge \mathcal{I}(\phi, A, N', \psi, t)]$ 9, $\exists$ elim
11. $Mem(A, K', t) \wedge K' \sqsubseteq K \wedge S$ 1,10, $\wedge$ elim
12. $B(A, \phi \wedge \psi \wedge \neg NFE(N, t), t)$ 11,K' $\sqsubseteq$ K, Lemma 1
13. $\forall x[Mem(x, K', t) \rightarrow B(x, \neg NFE(N', t), t)]$ 1, $\wedge$ elim
14. $B(A, \phi \wedge \psi \wedge \neg NFE(N', t), t)$ 11,12,13 $\rightarrow$ elim, FOL
15. $\neg \mathcal{B}(\phi, A, N', t)$ 11, K' $\sqsubseteq$ K, Lemma 1
16. $\mathcal{I}(\phi, A, N', \psi, t)$ 11, K' $\sqsubseteq$ K, Lemma 1
17. $Mem(A, K', t) \wedge B(A, \phi \wedge \psi \wedge \neg NFE(N', t), t) \wedge \neg \mathcal{B}(\phi, A, N', t) \wedge \mathcal{I}(\phi, A, N', \psi, t)$ 11,14,15,16 $\wedge$ intro

18. $Mem(A, K', t) \wedge \neg[B(A, \phi \wedge \psi \wedge \neg NFE(N', t), t) \wedge \neg \mathcal{B}(\phi, A, N', t) \wedge \mathcal{I}(\phi, A, N', \psi, t)] \wedge Mem(A, K', t) \wedge B(A, \phi \wedge \psi \wedge \neg NFE(N', t), t) \wedge \neg \mathcal{B}(\phi, A, N', t) \wedge \mathcal{I}(\phi, A, N', \psi, t)$ 10,17 $\wedge$ intro

19. $S \wedge K' \sqsubseteq K \wedge N' \sqsubseteq N \wedge \neg NFE(K', t) \wedge \forall x[Mem(x, K', t) \rightarrow B(x, \neg NFE(N', t), t)] \rightarrow Secret_0(\phi, K', N', \psi, t)$ 1,18 $\neg$ intro

□

2. $\Sigma \vdash Secret_0(\phi, K1, N1, \psi, t) \wedge Secret_0(\phi, K2, N2, \psi, t) \wedge \neg NFE(K1 \sqcap K2, t) \rightarrow Secret_0(\phi, K1 \sqcap K2, N1 \sqcup N2, \psi, t)$

Proof.

1. $Secret_0(\phi, K1, N1, \psi, t) \wedge Secret_0(\phi, K2, N2, \psi, t) \wedge \neg NFE(K1 \sqcap K2, t)$ assumption
2. $Secret_0(\phi, K1, N1, \psi, t)$ 1, $\wedge$ elim
3. $\forall x[Mem(x, K1, t) \rightarrow B(x, \phi \wedge \psi \wedge \neg NFE(N1, t), t) \wedge \neg \mathcal{B}(\phi, x, N1, t) \wedge \mathcal{I}(\phi, x, N1, \psi, t)]$ 2, S def, $\wedge$ elim
4. $Secret(\phi, K2, N2, \psi, t)$ 1, $\wedge$ elim
5. $\forall x[Mem(x, K2, t) \rightarrow B(x, \phi \wedge \psi \wedge \neg NFE(N2, t), t) \wedge \neg \mathcal{B}(\phi, x, N2, t) \wedge \mathcal{I}(\phi, x, N2, \psi, t)]$ 4, S def, $\wedge$ elim
6. $\forall x[Mem(x, K1, t) \rightarrow B(x, \phi \wedge \psi \wedge \neg NFE(N1, t), t)]$ 3, $\wedge$ elim
7. $\forall x[Mem(x, K2, t) \rightarrow B(x, \phi \wedge \psi \wedge \neg NFE(N2, t), t)]$ 5, $\wedge$ elim
8. $\forall x[Mem(x, K1 \sqcap K2, t) \rightarrow B(x, \phi \wedge \psi \wedge \neg NFE(N2, t), t) \wedge B(x, \phi \wedge \psi \wedge \neg NFE(N1, t), t)]$ 6,7 $\sqcap$ intro
9. $\forall x[Mem(x, K1 \sqcap K2, t) \rightarrow B(x, \phi \wedge \psi \wedge \neg NFE(N1 \sqcup N2, t), t)]$ 8, $\sqcup$ intro
10. $\forall x[Mem(x, K1, t) \rightarrow \neg \mathcal{B}(\phi, x, N1, t)]$ 3 $\wedge$ elim
11. $\forall x[Mem(x, K2, t) \rightarrow \neg \mathcal{B}(\phi, x, N2, t)]$ 5, $\wedge$ elim
12. $\forall x Mem(x, K1 \sqcap K2, t) \rightarrow \neg \mathcal{B}(\phi, x, N1 \sqcup N2, t)$ 10,11 $\sqcap$, $\sqcup$ intro
13. $\forall x[Mem(x, K1, t) \rightarrow \mathcal{I}(\phi, x, N1, \psi, t)]$ 3 $\wedge$ elim
14. $\forall x[Mem(x, K2, t) \rightarrow \mathcal{I}(\phi, x, N2, \psi, t)]$ 5, $\wedge$ elim
15. $\forall x Mem(x, K1 \sqcap K2, t) \rightarrow \mathcal{I}(\phi, A, N1 \sqcup N2, \psi, t)$ 13,14 $\sqcap$ intro
16. $\neg NFE(K1 \sqcap K2, t)$ 1, $\wedge$ elim
17. $Secret(\phi, K1 \sqcap K2, N1 \sqcup N2, \psi, t)$ 9,12,15,16 S def
18. $Secret_0(\phi, K1, N1, \psi, t) \wedge Secret_0(\phi, K2, N2, \psi, t) \wedge \neg NFE(K1 \sqcap K2, t) \rightarrow Secret(\phi, K1 \sqcap K2, N1 \sqcup N2, \psi, t)$ 1,17 $\rightarrow$ intro

□

3. $\Sigma \vdash Secret_0(\phi, K1, N1, \psi, t) \wedge Secret_0(\phi, K2, N2, \psi, t) \wedge \forall x[Mem(x, K1 \sqcup K2, t) \rightarrow B(x, \neg NFE(N1 \sqcap N2, t), t)] \rightarrow Secret_0(\phi, K1 \sqcup K2, N1 \sqcap N2, \psi, t)$

Proof.

1. $Secret(\phi, K1, N1, \psi, t) \wedge Secret(\phi, K2, N2, \psi, t) \wedge \forall x[Mem(x, K1 \sqcup K2, t) \rightarrow B(x, \neg NFE(N1 \sqcap N2, t), t)]$ assumption
2. $Secret(\phi, K1, N1, \psi, t)$ 1, $\wedge$ elim
3. $\neg NFE(K1, t) \wedge \forall x[Mem(x, K1, t) \rightarrow B(x, \phi \wedge \psi \wedge \neg NFE(N1, t), t) \wedge$

$\neg\mathcal{B}(\phi, x, N1, t) \wedge \mathcal{I}(\phi, x, N1, \psi, t)]$ 2, S def

4. $Secret(\phi, K2, N2, \psi, t)$ 1, $\wedge$ elim

5. $\neg NFE(K2, t) \wedge \forall x[Mem(x, K2, t) \rightarrow B(x, \phi \wedge \psi \wedge \neg NFE(N2, t), t) \wedge$
$\neg\mathcal{B}(\phi, x, N2, t) \wedge \mathcal{I}(\phi, x, N2, \psi, t)]$ 4, S def

6. $\forall x[Mem(x, K1, t) \rightarrow B(x, \phi \wedge \psi \wedge \neg NFE(N1, t), t)]$ 3, $\wedge$ elim

7. $\forall x[Mem(x, K2, t) \rightarrow B(x, \phi \wedge \psi \wedge \neg NFE(N2, t), t)]$ 5, $\wedge$ elim

8. $\forall x[Mem(x, K1 \sqcup K2, t) \rightarrow B(x, \phi \wedge \psi \wedge \neg NFE(N1, t), t) \vee$
$B(x, \phi \wedge \psi \wedge \neg NFE(N2, t), t)]$ 5,6 $\sqcup$ intro

9. $\forall x[Mem(x, K1, t) \rightarrow \neg\mathcal{B}(\phi, x, N1, t)]$ 3, $\wedge$ elim

10. $\forall x[Mem(x, K2, t) \rightarrow \neg\mathcal{B}(\phi, x, N2, t)]$ 4, $\wedge$ elim

11. $\forall x[Mem(x, K1 \sqcup K2, t) \rightarrow \neg\mathcal{B}(\phi, x, N1, t) \vee$
$\neg\mathcal{B}(\phi, x, N2, t)]$ 8,9 $\sqcup$ intro

12. $\forall x[Mem(x, K1, t) \rightarrow \mathcal{I}(\phi, x, N1, \psi, t)]$ 3, $\wedge$ elim

13. $\forall x[Mem(x, K2, t) \rightarrow \mathcal{I}(\phi, x, N2, \psi, t)]$ 4, $\wedge$ elim

14. $\forall x[Mem(x, K1 \sqcup K2, t) \rightarrow \mathcal{I}(\phi, x, N1, \psi, t) \vee$
$\mathcal{I}(\phi, x, N2, \psi, t)]$ 11,12 $\sqcup$ intro

15. $\forall x[Mem(x, K1 \sqcup K2, t) \rightarrow B(x, \neg NFE(N1 \sqcap N2, t), t)]$
1, $\wedge$ elim

16. $\neg NFE(K1, t) \wedge \neg NFE(K2, t)$ 3,5 FOL

17. $Secret(\phi, K1 \sqcup K2, N1 \sqcap N2, \psi, t)$ 8,11,14,16 $\sqcap$ intro, S def

18. $Secret(\phi, K1, N1, \psi, t) \wedge Secret(\phi, K2, N2, \psi, t) \wedge$
$\forall x[Mem(x, K1 \sqcup K2, t) \rightarrow B(x, \neg NFE(N1 \sqcap N2, t), t)] \rightarrow$
$Secret(\phi, K1 \sqcup K2, N1 \sqcap N2, \psi, t)$ 1,17 $\rightarrow$ intro

□

Theorem 3 *1.* $\Sigma \vdash S \rightarrow \neg\exists x[Mem(x, K, t) \wedge B(x, \psi \rightarrow \neg\phi)]$

Proof.

1. $S \wedge \exists x[Mem(x, K, t) \wedge B(x, \psi \rightarrow \neg\phi, t)]$ assumption

2. $[Mem(A, K, t) \wedge B(A, \psi \rightarrow \neg\phi)]$ 1, $\exists$, $\wedge$ elim

3. $\forall x Mem(x, K, t) \rightarrow B(x, \phi \wedge \psi \wedge \neg NFE(N, t), t) \wedge$
$\neg\mathcal{B}(\phi, x, N, t) \wedge \mathcal{I}(\phi, x, N, \psi, t)$ 1, S def, $\wedge$ elim

4. $Mem(A, K, t)$ 2, $\wedge$ elim

5. $B(A, \phi \wedge \psi \wedge \neg NFE(N, t), t)$ 3,4, $\rightarrow$ elim

6. $B(A, \psi, t)$ 5, FOL

7. $B(A, \phi, t)$ 5, FOL

8. $B(A, \neg\phi, t)$ 2,6 K axiom for B

9. $B(A, \phi, t) \wedge B(A, \neg\phi, t)$ 7 $\wedge$ 8

10. $S \rightarrow \neg\exists x[Mem(x, K, t) \wedge B(x, \psi \rightarrow \neg\phi)]$ 1,9 $\neg$ intro

□

2. $\Sigma \vdash S \rightarrow \neg\exists x[Mem(x, K, t) \wedge B(x, \psi \rightarrow NFE(N, t), t)]$

Proof.

1. $S \wedge \exists x[Mem(x, K, t) \wedge B(x, \psi \rightarrow NFE(N, t), t)]$ assumption

2. $Mem(A, K, t) \wedge B(A, \psi \rightarrow NFE(N, t), t)$ 1, $\exists$,$\wedge$ elim

3. $\forall x Mem(x, K, t) \rightarrow B(x, \phi \wedge \psi \wedge \neg NFE(N, t), t) \wedge$
$\neg\mathcal{B}(\phi, x, N, t) \wedge \mathcal{I}(\phi, x, N, \psi, t)$ 1, S def, $\wedge$ elim

4. $Mem(A, K, t)$ — 2, $\wedge$ elim
5. $B(A, \phi \wedge \psi \wedge \neg NFE(N, t), t)$ — 3,4, $\rightarrow$ elim
6. $B(A, \psi, t)$ — 5, FOL
7. $B(A, \neg NFE(N, t), t)$ — 5, FOL
8. $\neg B(A, NFE(N, t), t)$ — 7, D Axiom for B
9. $B(A, NFE(N, t), t)$ — 2,6 $\rightarrow$ elim
10. $B(A, NFE(N, t), t) \wedge \neg B(A, NFE(N, t), t)$ — 8 $\wedge$ 9
11. $S \rightarrow \neg\exists x[Mem(x, K, t) \wedge B(x, \psi \rightarrow NFE(N, t), t)]$ — 1,10 $\neg$ intro

□

3. $\Sigma \vdash S \rightarrow \neg\exists x[Mem(x, K, t) \wedge B(x, \psi \rightarrow \mathcal{B}(\phi, x, N, t), t)]$

Proof.

1. $S \wedge \exists x[Mem(x, K, t) \wedge B(x, \psi \rightarrow \mathcal{B}(\phi, x, N, t), t)]$ — assumption
2. $Mem(A, K, t) \wedge B(A, \psi \rightarrow \mathcal{B}(\phi, A, N, t), t)$ — 1, $\exists$,$\wedge$ elim
3. $\forall x Mem(x, K, t) \rightarrow B(x, \phi \wedge \psi \wedge \neg NFE(N, t), t) \wedge \neg\mathcal{B}(\phi, x, N, t) \wedge \mathcal{I}(\phi, x, N, \psi, t)$ — 1, S def, $\wedge$ elim
4. $Mem(A, K, t)$ — 2, $\wedge$ elim
5. $B(A, \phi \wedge \psi \wedge \neg NFE(N, t), t)$ — 3,4, $\rightarrow$ elim
6. $B(A, \psi, t)$ — 5, FOL
7. $\neg\mathcal{B}(\phi, x, N, t)$ — 3,4, $\rightarrow$ elim
8. $B(A, \mathcal{B}(\phi, x, N, t), t)$ — 2,6 K axiom for B
9. $\mathcal{B}(\phi, x, N, t)$ — 8, FOL
10. $\neg\mathcal{B}(\phi, x, N, t) \wedge \mathcal{B}(\phi, x, N, t)$ — 7 $\wedge$ 9
11. $S \rightarrow \neg\exists x[Mem(x, K, t) \wedge B(x, \psi \rightarrow \mathcal{B}(\phi, x, N, t), t)]$ — 1,10 $\neg$ intro

□

4. $\Sigma \vdash S \rightarrow \neg\exists x[Mem(x, K, t) \wedge B(x, \psi \rightarrow \mathcal{I}(\phi, x, N, \psi, t), t)]$

Proof.

1. $S \wedge \exists x[Mem(x, K, t) \wedge B(x, \psi \rightarrow \mathcal{I}(\phi, x, N, \psi, t), t)]$ — assumption
2. $Mem(A, K, t) \wedge B(A, \psi \rightarrow \mathcal{I}(\phi, A, N, \psi, t), t)$ — 1, $\exists$,$\wedge$ elim
3. $\forall x Mem(x, K, t) \rightarrow B(x, \phi \wedge \psi \wedge \neg NFE(N, t), t) \wedge \neg\mathcal{B}(\phi, x, N, t) \wedge \mathcal{I}(\phi, x, N, \psi, t)$ — 1, S def, $\wedge$ elim
4. $Mem(A, K, t)$ — 2, $\wedge$ elim
5. $B(A, \phi \wedge \psi \wedge \neg NFE(N, t), t)$ — 3,4, $\rightarrow$ elim
6. $B(A, \psi, t)$ — 5, FOL
7. $\mathcal{I}(\phi, A, N, \psi, t)$ — 3,4, $\rightarrow$ elim
8. $B(A, \neg\mathcal{I}(\phi, A, N, \psi, t), t)$ — 2,6 K Axiom for B
9. $\neg\mathcal{I}(\phi, A, N, \psi, t)$ — 8, Axiom **IB1**
10. $\mathcal{I}(\phi, A, N, \psi, t) \wedge \neg\mathcal{I}(\phi, A, N, \psi, t)$ — 7 $\wedge$ 9
11. $S \rightarrow \neg\exists x[Mem(x, K, t) \wedge B(x, \psi \rightarrow \mathcal{I}(\phi, A, N, \psi, t), t)]$ — 1,10 $\neg$ intro

□

Theorem 4 $\Sigma \vdash S \rightarrow \neg\exists x[Mem(x, K, t) \wedge B(x, \exists y, t'[t < t' \wedge Mem(y, N, t') \wedge \forall t''[t < t'' \leq t' \rightarrow H(\psi, t'')] \wedge R(y, \phi, t')], t)]$

Proof.

1. $S \wedge \exists x[Mem(x,K,t) \wedge B(x, \exists y, t'[t < t' \wedge Mem(y,N,t') \wedge$
$\forall t''[t < t'' \leq t' \rightarrow H(\psi, t'')] \wedge R(y,\phi,t')], t)]$ assumption
2. $\forall x Mem(x,K,t) \rightarrow B(x, \phi \wedge \psi \wedge \neg NFE(N,t), t) \wedge$
$\neg \mathcal{B}(\phi, x, N, t) \wedge \mathcal{I}(\phi, x, N, \psi, t)$ 1, $\wedge$ elim, S def
3. $Mem(A,K,t) \wedge B(A, \exists y, t'[t < t' \wedge Mem(y,N,t') \wedge$
$\forall t''[t < t'' \leq t' \rightarrow H(\psi, t'')] \wedge R(y,\phi,t')], t)$ 1, $\wedge, \exists$ elim
4. $\neg I(A, \forall y, t'[t < t' \wedge Mem(y,N,t') \wedge$
$\forall t''[t < t'' \leq t' \rightarrow H(\psi, t'')] \rightarrow \neg R(y,\phi,t')], t)$ 3, $\wedge$ elim, Axiom **IB3**
5. $\mathcal{I}(\phi, A, N, \psi, t)$ 2,3 $\rightarrow$ elim
6. $\neg \mathcal{I}(\phi, A, N, \psi, t) \wedge \mathcal{I}(\phi, A, N, \psi, t)$ 4 $\wedge$ 5

7. $S \rightarrow \neg \exists x[Mem(x,K,t) \wedge B(x, \exists y, t'[t < t' \wedge Mem(y,N,t') \wedge$
$\forall t''[t < t'' \leq t' \rightarrow H(\psi, t'')] \wedge R(y,\phi,t')], t)]$ 1,6 $\neg$ intro

□

Theorem 5 1. $\Sigma \vdash S \wedge Secret_0(\xi, K, N, \psi, t) \rightarrow Secret_0(\phi \wedge \xi, K, N, \psi, t)$

Proof.

1. $S \wedge Secret_0(\xi, K, N, \psi, t)$ assumption
2. $Secret_0(\xi, K, N, \psi, t)$ 1, $\wedge$ elim
3. $\neg NFE(K,t) \wedge \forall x[Mem(x,K,t) \rightarrow B(x, \phi \wedge \psi \wedge \neg NFE(N,t), t) \wedge$
$\neg \mathcal{B}(\phi, x, N, t) \wedge \mathcal{I}(\phi, x, N, \psi, t)]$ 1, $\wedge$ elim, S def
4. $\neg NFE(K,t) \wedge \forall x Mem(x,K,t) \rightarrow B(x, \xi \wedge \psi \wedge \neg NFE(N,t), t) \wedge$
$\neg \mathcal{B}(\xi, x, N, t) \wedge \mathcal{I}(\xi, x, N, \psi, t)$ 2, S def
5. $\neg NFE(K,t)$ 4, $\wedge$ elim
6. $\forall x Mem(x,K,t) \rightarrow B(x, \phi \wedge \psi \wedge \neg NFE(N,t), t)$ 3, $\wedge$ elim
7. $\forall x Mem(x,K,t) \rightarrow B(x, \xi \wedge \psi \wedge \neg NFE(N,t), t)$ 4, $\wedge$ elim
8. $\forall x Mem(x,K,t) \rightarrow B(x, \xi \wedge \psi \wedge \neg NFE(N,t), t) \wedge$
$B(x, \phi \wedge \psi \wedge \neg NFE(N,t), t)$ 6 $\wedge$ 7
9. $\forall x Mem(x,K,t) \rightarrow B(x, \xi \wedge \phi \wedge \psi \wedge \neg NFE(N,t), t)$ 8, FOL
10. $\forall x[Mem(x,K,t) \rightarrow \neg \mathcal{B}(\phi, x, N, t)]$ 3, $\wedge$ elim
11. $\forall x[Mem(x,K,t) \rightarrow \neg \mathcal{B}(\xi, x, N, t)]$ 4, $\wedge$ elim
12. $\forall x[Mem(x,K,t) \rightarrow \neg \mathcal{B}(\phi, x, N, t) \wedge \neg \mathcal{B}(\xi, x, N, t)]$ 10 $\wedge$ 11
13. $\forall x[Mem(x,K,t) \rightarrow \neg \mathcal{B}(\phi \wedge \xi, x, N, t)]$ 12, FOL
14. $\forall x[Mem(x,K,t) \rightarrow \mathcal{I}(\phi, x, N, \psi, t)]$ 3, $\wedge$ elim
15. $\forall x[Mem(x,K,t) \rightarrow \mathcal{I}(\xi, x, N, \psi, t)]$ 4, $\wedge$ elim
16. $\forall x[Mem(x,K,t) \rightarrow \mathcal{I}(\xi, x, N, \psi, t) \wedge \mathcal{I}(\phi, x, N, \psi, t)]$ 14 $\wedge$ 15
17. $\forall x[Mem(x,K,t) \rightarrow \mathcal{I}(\phi \wedge \xi, x, N, \psi, t)$ 16, FOL
18. $Secret_0(\phi \wedge \xi, K, N, \psi, t)$ 5, 9, 13, 17 S def
19. $S \wedge Secret_0(\xi, K, N, \psi, t) \rightarrow Secret_0(\phi \wedge \xi, K, N, \psi, t)$ 1,18 $\rightarrow$ intro

□

2. $\Sigma \vdash S \rightarrow Secret(\exists x R(x, \phi, t), K, N, \psi, t)$

Proof.

1. $S \wedge \neg Secret(\exists x R(x, \phi, t), K, N, \psi, t)$ assumption
2. $NFE(K,t) \vee \exists x[Mem(x,K,t) \wedge [\neg B(x, \exists x R(x, \phi, t) \wedge \psi \wedge$
$\neg NFE(N,t), t) \vee \mathcal{B}(\exists x R(x, \phi, t), x, N, t) \vee \neg \mathcal{I}(\exists x R(x, \phi, t), x, N, \psi, t)]$
1, $\wedge$ elim, $\neg$ S def

3. $\exists x[Mem(x,K,t) \wedge \neg B(x, \exists x R(x,\phi,t) \wedge \psi \wedge \neg NFE(N,t),t)]$ 2, assumption

4. $\neg NFE(K,t) \wedge \forall x Mem(x,K,t) \rightarrow B(x, \phi \wedge \psi \wedge \neg NFE(N,t),t) \wedge \neg\mathcal{B}(\phi,x,N,t) \wedge \mathcal{I}(\phi,x,N,\psi,t)$ 1, $\wedge$ elim, S def

5. $Mem(A,K,t) \wedge \neg B(A, \exists x R(x,\phi,t) \wedge \psi \wedge \neg NFE(N,t),t)$ 3, $\exists$ elim

6. $Mem(A,K,t)$ 5, $\wedge$ elim

7. $B(A, \phi \wedge \psi \wedge \neg NFE(N,t),t)$ 4,6 $\rightarrow$ elim

8. $B(A,\phi,t)$ 7, FOL

9. $B(A, B(A,\phi,t),t)$ 8, FOL

10. $B(A, R(A,\phi,t),t)$ 9, Theorem **T2**

11. $B(A, \exists x R(x,\phi,t),t)$ 10, $\exists$ intro

12. $Mem(A,K,t) \wedge B(A, \exists x R(x,\phi,t) \wedge \psi \wedge \neg NFE(N,t),t)$ 6,7,11 $\wedge$ intro, FOL

13. $Mem(A,K,t) \wedge B(A, \exists x R(x,\phi,t) \wedge \psi \wedge \neg NFE(N,t),t) \wedge Mem(A,K,t) \wedge \neg B(A, \exists x R(x,\phi,t) \wedge \psi \wedge \neg NFE(N,t),t)$ 5 $\wedge$ 12

14. $\forall x[Mem(x,K,t) \rightarrow B(x, \exists x R(x,\phi,t) \wedge \psi \wedge \neg NFE(N,t),t)]$ 3,13 $\neg$ intro

15. $NFE(K,t) \vee \exists x[Mem(x,K,t) \wedge [\mathcal{B}(\exists x R(x,\phi,t),x,N,t) \vee \neg\mathcal{I}(\exists x R(x,\phi,t),x,N,\psi,t)]$ 2,14 $\vee$ elim

16. $\exists x[Mem(x,K,t) \wedge \mathcal{B}(\exists x R(x,\phi,t),x,N,t)$ 15, assumption

17. $\neg\mathcal{B}(\phi,x,N,t)$ 1,16 $\rightarrow$ elim

18. $\neg\mathcal{B}(\exists x[R(x,\phi,t),x,N,t)$ 17, Theorem **T3**

19. $\mathcal{B}(\exists x[R(x,\phi,t)],x,N,t) \wedge \neg\mathcal{B}(\exists x[R(x,\phi,t),x,N,t)$ 16 $\wedge$ 18

20. $\forall x[Mem(x,K,t) \rightarrow \neg\mathcal{B}(\exists x[R(x,\phi,t)],x,N,t)]$ 16,19 $\neg$ intro

21. $NFE(K,t) \vee \exists x[Mem(x,K,t) \wedge \neg\mathcal{I}(\exists x R(x,\phi,t),x,N,\psi,t)]$ 15,20 $\vee$ elim

22. $\exists x[Mem(x,K,t) \wedge \neg\mathcal{I}(\exists x[R(x,\phi,t)],x,N,\psi,t)]$ 21, assumption

23. $\forall x[Mem(x,K,t) \rightarrow I(x, R(y, R(z,\phi,t),t) \rightarrow R(y,\phi,t),t)]$ N-rule for I, Axiom **R3**

24. $Mem(A,K,t) \wedge \neg\mathcal{I}(\exists x[R(x,\phi,t)],A,N,\psi,t)$ 22, $\exists$ elim

25. $\mathcal{I}(\phi,A,N,\psi,t)$ 1, 24 $\rightarrow$ elim

26. $\mathcal{I}(\exists x[R(x,\phi,t)],A,N,\psi,t)$ 23,25 FOL

27. $\neg\mathcal{I}(\exists x[R(x,\phi,t)],A,N,\psi,t) \wedge \mathcal{I}(\exists x[R(x,\phi,t)],A,N,\psi,t)$ 24,26 $\wedge$ intro

28. $\forall x[Mem(x,K,t) \rightarrow \mathcal{I}(\exists x[R(x,\phi,t)],x,N,\psi,t)]$ 22,27 $\neg$ intro

29. $NFE(K,t)$ 21,28 $\vee$ elim

30. S 1, $\wedge$ elim

31. $\neg NFE(K,t)$ 30, S def, $\wedge$ elim

32. $NFE(K,t) \wedge \neg NFE(K,t)$ 29,31 $\wedge$ intro

33. $S \rightarrow Secret(\exists x R(x,\phi,t),K,N,\psi,t)$ 1,32 $\neg$ intro

□

3. $\Sigma \vdash \forall x[B(x, S \wedge Mem(x, K, t), t) \rightarrow Secret(\phi, [x], N, \psi, t)]$
Proof.

1. $\exists x[B(x, S \wedge Mem(x, K, t), t) \wedge \neg Secret(\phi, [x], N, \psi, t)]$ assumption
2. $B(A, S \wedge Mem(A, K, t), t) \wedge \neg Secret(\phi, [A], N, \psi, t)$ 1, $\exists$ elim
3. $B(A, S \wedge Mem(A, K, t), t)$ 2, FOL
4. $Mem(A, [A], t) \wedge B(A, B(A, \phi \wedge \psi \wedge \neg NFE(N, t), t) \wedge \neg \mathcal{B}(\phi, A, N, t) \wedge \mathcal{I}(\phi, A, N, \psi, t), t)$ 3, FOL, Axiom **G1**
5. $Mem(A, [A], t) \wedge B(A, \phi \wedge \psi \wedge \neg NFE(N, t), t) \wedge \neg \mathcal{B}(\phi, A, N, t) \wedge \mathcal{I}(\phi, A, N, \psi, t)$ 4, FOL, Axiom **IB2**
6. $Secret(\phi, [A], N, \psi, t)$ 5, S def
7. $\neg Secret(\phi, [A], N, \psi, t)$ 2, $\wedge$ elim
8. $Secret(\phi, [A], N, \psi, t) \wedge \neg Secret(\phi, [A], N, \psi, t)$ 6 $\wedge$ 7
9. $\forall x[B(x, S \wedge Mem(x, K, t), t) \rightarrow Secret(\phi, [x], N, \psi, t)]$ 1,8 $\neg$ intro

□

4. $\Sigma \vdash \forall x[S \wedge Mem(x, K, t) \rightarrow B(x, Secret(\phi, [x], N, \psi, t), t)]$
Proof.

1. $\exists x[S \wedge Mem(x, K, t) \wedge \neg B(x, Secret(\phi, [x], N, \psi, t), t)]$ assumption
2. $S \wedge Mem(A, K, t) \wedge \neg B(A, Secret(\phi, [A], N, \psi, t), t)$ $\exists$ elim
3. $S \wedge Mem(A, K, t)$ 2, $\wedge$ elim
4. $B(A, \phi \wedge \psi \wedge \neg NFE(N, t), t) \wedge \neg \mathcal{B}(\phi, A, N, t) \wedge \mathcal{I}(\phi, A, N, \psi, t)$ 3, $\wedge$ elim, S def
5. $B(A, Mem(A, [A], t) \wedge B(A, \phi \wedge \psi \wedge \neg NFE(N, t), t) \wedge \neg \mathcal{B}(\phi, A, N, t) \wedge \mathcal{I}(\phi, A, N, \psi, t), t)$ 4, FOL, Axiom **IB2**, **G1**
6. $B(A, Secret(\phi, [A], N, \psi, t), t)$ 5, S def
7. $\neg B(A, Secret(\phi, [A], N, \psi, t), t)$ 2, $\wedge$ elim
8. $B(A, Secret(\phi, [A], N, \psi, t), t) \wedge \neg B(A, Secret(\phi, [A], N, \psi, t), t)$ 6 $\wedge$ 7
9. $\forall x[S \wedge Mem(x, K, t) \rightarrow B(x, Secret(\phi, [x], N, \psi, t), t)]$ 1,8 $\neg$ intro

□

5. $\Sigma \vdash S \wedge \forall x[Mem(x, K, t) \rightarrow B(x, S \wedge \exists y[Mem(y, K, t)], t)] \rightarrow Secret_0(S \wedge \exists y[Mem(y, K, t)], K, N, \psi, t)$

Proof.

1. $S \wedge \forall x[Mem(x, K, t) \rightarrow B(x, S \wedge \exists y[Mem(y, K, t)], t)] \wedge \neg Secret_0(S \wedge \exists y[Mem(y, K, t)], K, N, \psi, t)$ assumption
2. $\neg Secret_0(S \wedge \exists y[Mem(y, K, t)], K, N, \psi, t)$ 1, $\wedge$ elim
3. $\neg[\neg NFE(K, t) \wedge \forall x Mem(x, K, t) \rightarrow B(x, S \wedge \exists y[Mem(y, K, t)] \wedge \psi \wedge \neg NFE(N, t), t) \wedge \neg \mathcal{B}(S \wedge \exists y[Mem(y, K, t)], x, N, t) \wedge \mathcal{I}(S \wedge \exists y[Mem(y, K, t)], x, N, \psi, t)]$ 2, S def
4. $NFE(K, t) \vee [\exists x[Mem(x, K, t)] \wedge [\neg B(x, S \wedge \exists y[Mem(y, K, t)] \wedge \psi \wedge \neg NFE(N, t), t) \vee \mathcal{B}(S \wedge \exists y[Mem(y, K, t)], x, N, t) \vee \neg \mathcal{I}(S \wedge \exists y[Mem(y, K, t)], x, N, \psi, t)]]$ 3, $\neg$ elim

5. $NFE(K,t)$ 4, assumption

6. $\neg NFE(K,t) \wedge \forall x[Mem(x,K,t) \rightarrow B(x, \phi \wedge \psi \wedge \neg NFE(N,t),t) \wedge \neg \mathcal{B}(\phi,x,N,t) \wedge \mathcal{I}(\phi,x,N,\psi,t)]$ 1, $\wedge$ elim, S def

7. $\neg NFE(K,t)$ 6, $\wedge$ elim

8. $NFE(K,t) \wedge \neg NFE(K,t)$ 5 $\wedge$ 7

9. $\neg NFE(K,t)$ 5,8 $\neg$ intro

10. $\exists x Mem(x,K,t) \wedge [\neg B(x, S \wedge \exists y[Mem(y,K,t)] \wedge \psi \wedge \neg NFE(N,t),t) \vee \mathcal{B}(S \wedge \exists y[Mem(y,K,t)],x,N,t) \vee \neg \mathcal{I}(S \wedge \exists y[Mem(y,K,t)],x,N,\psi,t)]$ 4,9 $\vee$ elim

11. $\exists x Mem(x,K,t) \wedge \neg B(x, S \wedge \exists y[Mem(y,K,t) \wedge \psi \wedge \neg NFE(N,t),t)$ 10, assumption

12. $Mem(A,K,t) \wedge \neg B(A, S \wedge \exists y[Mem(y,K,t) \wedge \psi \wedge \neg NFE(N,t),t)$ 11, $\exists$ elim

13. $B(A, \phi \wedge \psi \wedge \neg NFE(N,t),t)$ 1, $\wedge, \forall$ elim, S def

14. $B(A, \psi \wedge \neg NFE(N,t),t)$ 13, FOL

15. $B(A, S \wedge \exists y[Mem(y,K,t)],t)$ 1, $\wedge, \forall$ elim

16. $B(A, S \wedge \exists y[Mem(y,K,t)] \wedge \psi \wedge \neg NFE(N,t),t)$ 14,15 FOL

17. $\neg B(A, S \wedge \exists y[Mem(y,K,t)] \wedge \psi \wedge \neg NFE(N,t),t)$ 12, $\wedge$ elim

18. $B(A, S \wedge \exists y[Mem(y,K,t)] \wedge \psi \wedge \neg NFE(N,t),t) \wedge \neg B(A, S \wedge \exists y[Mem(y,K,t)] \wedge \psi \wedge \neg NFE(N,t),t)$ 16 $\wedge$ 17

19. $\forall x Mem(x,K,t) \rightarrow B(x, S \wedge \exists y[Mem(y,K,t) \wedge \psi \wedge \neg NFE(N,t),t)$ 11,18 $\neg$ intro

20. $\exists x[Mem(x,K,t) \wedge [\mathcal{B}(S \wedge \exists y[Mem(y,K,t),A,N,t) \vee \neg \mathcal{I}(S \wedge \exists y[Mem(y,K,t),A,N,\psi,K,t)]]$ 10,19 $\vee$ elim

21. $\exists x[Mem(x,K,t) \wedge [\mathcal{B}(S \wedge \exists y[Mem(y,K,t),x,N,t)]$ assumption

22. $Mem(A,K,t) \wedge [\mathcal{B}(S \wedge \exists y[Mem(y,K,t)],A,N,t)$ 21, $\exists$ elim

23. $\neg \mathcal{B}(\phi,A,N,t)$ 1, S def $\wedge, \forall$ elim

24. $\forall x[\mathcal{B}(S \wedge \exists y[Mem(y,K,t)],x,N,t) \rightarrow \mathcal{B}(\phi,x,N,t)]$ Theorem 1.1

25. $\mathcal{B}(\phi,A,N,t)$ 22,24 $\rightarrow$ elim

26. $\neg \mathcal{B}(\phi,A,N,t) \wedge \mathcal{B}(\phi,A,N,t)$ 23 $\wedge$ 25

27. $\forall x[Mem(x,K,t) \rightarrow \neg \mathcal{B}(S \wedge \exists y[Mem(y,K,t)],x,N,t)]$ 21,26 $\neg$ intro

28. $\exists x[Mem(x,K,t) \wedge \neg \mathcal{I}(S \wedge \exists y[Mem(y,K,t)],x,N,\psi,t)]$ 20,27 $\vee$ elim

29. $Mem(A,K,t) \wedge \neg \mathcal{I}(S \wedge \exists y[Mem(y,K,t)],A,N,\psi,t)$ 28, $\exists$ elim

30. $\mathcal{I}(\phi,A,N,\psi,t)$ 1, S def $\wedge, \forall$ elim

31. $I(A, \forall x[R(x, S \wedge \exists y[Mem(y,K,t)]) \rightarrow R(x,\phi)],t)$ Theorem 1.1, N-rule for I

32. $\mathcal{I}(S \wedge \exists y[Mem(y,K,t)],A,N,\psi,t)$ 30,31 FOL

33. $\mathcal{I}(S \wedge \exists y[Mem(y,K,t)],A,N,\psi,t) \wedge \neg \mathcal{I}(S \wedge \exists y[Mem(y,K,t)],A,N,\psi,t)$ 29 $\wedge$ 32

34. $S \wedge \forall x[Mem(x,K,t) \rightarrow B(x, S \wedge \exists y[Mem(y,K,t)],t)] \rightarrow$

$Secret_0(S \wedge \exists y[Mem(y,K,t)],K,N,\psi,t)$ 1,33 $\neg$ intro

□

6. $\Sigma \vdash \forall x[S \wedge Mem(x,K,t) \rightarrow B(x,Secret(Secret(\phi,[x],N,\psi,t),[x],N,\psi,t),t)$ *is a corollary to the previously proven two theorems.*

Theorem 6 1. $\Sigma \vdash \forall x[S \wedge Mem(x,K,t) \rightarrow \neg B(x,Mem(x,N,t),t)]$

Proof.

1. $\exists x[S \wedge Mem(x,K,t) \wedge B(x,Mem(x,N,t),t)]$ assumption
2. $\neg NFE(K,t) \wedge \forall x Mem(x,K,t) \rightarrow B(x,\phi \wedge \psi \wedge \neg NFE(N,t),t) \wedge \neg\mathcal{B}(\phi,x,N,t) \wedge \mathcal{I}(\phi,x,N,\psi,t)$ 1, $\wedge$ elim, S def
3. $S \wedge Mem(A,K,t) \wedge B(A,Mem(A,N,t),t)$ 1, $\exists$ elim
4. $B(A,\phi \wedge \psi \wedge \neg NFE(N,t),t)$ 2, $\wedge$, $\rightarrow$ elim
5. $B(A,\phi,t)$ 4, FOL
6. $B(A,B(A,\phi,t),t)$ 5, FOL
7. $B(A,R(A,\phi,t),t)$ 6, Theorem **T2**
8. $\neg B(\phi,A,N,t)$ 2, $\wedge$, $\rightarrow$ elim
9. $B(A,Mem(A,N,t),t)$ 3, $\wedge$ elim
10. $\neg B(A,R(A,\phi,t),t)$ 8,9 FOL
11. $B(A,R(A,\phi,t),t) \wedge \neg B(A,R(A,\phi,t),t)$ 7 $\wedge$ 10
12. $\forall x[S \wedge Mem(x,K,t) \rightarrow \neg B(x,Mem(x,N,t),t)]$ 1,11 $\neg$ intro

□

2. $\Sigma \vdash \forall x[S \wedge Mem(x,K,t) \wedge \forall y[Mem(y,N,t) \rightarrow B(x,Mem(y,N,t),t)] \rightarrow \neg Mem(x,N,t)]$

Proof.

1. $\exists x[S \wedge Mem(x,K,t) \wedge \forall y[Mem(y,N,t) \rightarrow B(x,Mem(y,N,t),t)] \wedge Mem(x,N,t)]$ assumption
2. $S \wedge Mem(A,K,t) \wedge \forall y[Mem(y,N,t) \rightarrow B(A,Mem(y,N,t),t)] \wedge Mem(A,N,t)$ 1, $\exists$ elim
3. $Mem(A,N,t)$ 2, $\wedge$ elim
4. $\forall y[Mem(y,N,t) \rightarrow B(A,Mem(y,N,t),t)]$ 2, $\wedge$ elim
5. $B(A,Mem(A,N,t),t)$ 3,4 $\rightarrow$ elim
6. $S \wedge Mem(A,K,t)$ 2, $\wedge$ elim
7. $\neg B(A,Mem(A,N,t),t)$ 5, Theorem 6.1
8. $B(A,Mem(A,N,t),t) \wedge \neg B(A,Mem(A,N,t),t)$ 5 $\wedge$ 7
9. $\forall x[S \wedge Mem(x,K,t) \wedge \forall y[Mem(y,N,t) \rightarrow B(y,Mem(y,N,t),t)] \rightarrow \neg Mem(x,N,t)]$ 1,8 $\neg$ intro

□

3. $\Sigma \vdash \forall x[S \wedge Mem(x,K,t') \rightarrow B(x,t \leq t' \wedge [R(C,\phi,t) \rightarrow R(C,\phi,t')] \wedge S \wedge Mem(x,K,t') \wedge Mem(C,K,t) \wedge Mem(C,N,t'),t') \rightarrow B(x,\neg S',t')]$

Proof.

1. $Mem(x,K,t') \wedge B(x,t \leq t' \wedge [R(C,\phi,t) \rightarrow R(C,\phi,t')] \wedge S \wedge Mem(x,K,t') \wedge Mem(C,K,t) \wedge Mem(C,N,t'),t')$ assumption

2. $B(x, S \wedge Mem(C,K,t), t')$ — 1, $\wedge$ elim FOL
3. $B(x, B(C,\phi,t), t')$ — 2, FOL
4. $B(x, R(C,\phi,t), t')$ — 3, Theorem **T2**
5. $B(x, R(C,\phi,t) \rightarrow R(C,\phi,t'), t')$ — 1, FOL
6. $B(x, R(C,\phi,t'), t')$ — 4,5 K Axiom for B
7. $B(x, Mem(C,N,t'), t')$ — 1, FOL
8. $B(x, Mem(C,N,t') \wedge R(C,\phi,t'), t')$ — 6,7 FOL
9. $\mathcal{B}(\phi, x, N, t')$ — 8, $\exists$ intro
10. $B(x, Mem(x,K,t'), t')$ — 1, FOL
11. $B(x, \mathcal{B}(\phi,x,N,t'), t')$ — 9, FOL
12. $B(x, \exists x Mem(x,K,t') \wedge \mathcal{B}(\phi,x,N,t'), t')$ — 10,11 FOL
13. $B(x, \neg S', t')$ — 12, FOL
14. $\forall x[Mem(x,K,t') \wedge B(x, t \leq t' \wedge [R(C,\phi,t) \rightarrow R(C,\phi,t')] \wedge S \wedge Mem(x,K,t') \wedge Mem(C,K,t) \wedge Mem(C,N,t'), t') \rightarrow B(x, \neg S', t')]$ — $1 \rightarrow 13$, $\forall$ intro

□

Theorem 7 $\Sigma \vdash \forall x[S \wedge Mem(x,K,t) \wedge B(x, \forall y[Mem(y,N,t) \rightarrow \neg B(y, \neg\xi, t) \wedge B(y, \xi \rightarrow \phi, t)], t) \rightarrow \neg\mathcal{B}(\xi,x,N,t) \wedge \neg\mathcal{I}(x, \forall y, t'[t \leq t' \wedge Mem(y,N,t') \wedge \forall t''[t \leq t'' \leq t' \rightarrow H(\psi,t'')] \rightarrow R(y,\xi,t')], t)]$

Proof.

1. $\exists x[S \wedge Mem(x,K,t) \wedge B(x, \forall y[Mem(y,N,t) \rightarrow \neg B(y,\neg\xi,t) \wedge B(y,\xi\rightarrow\phi,t)],t) \wedge [\mathcal{B}(\xi,x,N,t) \vee \mathcal{I}(x, \forall y, t'[t \leq t' \wedge Mem(y,N,t') \wedge \forall t''[t \leq t'' \leq t' \rightarrow H(\psi,t'')] \rightarrow R(y,\xi,t')], t)]]$ — assumption
2. $\exists x[S \wedge Mem(x,K,t) \wedge B(x, \forall y[Mem(y,N,t) \rightarrow \neg B(y,\neg\xi,t) \wedge B(y,\xi\rightarrow\phi,t)],t) \wedge \mathcal{B}(\xi,x,N,t)$ — assumption
3. $S \wedge Mem(A,K,t) \wedge B(A, \forall y[Mem(y,N,t) \rightarrow \neg B(y,\neg\xi,t) \wedge B(y,\xi\rightarrow\phi,t)],t) \wedge \mathcal{B}(\xi,A,N,t)$ — 2, $\exists$ elim
4. $B(A, \forall y[Mem(y,N,t) \rightarrow \neg B(y,\neg\xi,t) \wedge B(y,\xi\rightarrow\phi,t)],t) \wedge \mathcal{B}(\xi,A,N,t)$ — 3, $\wedge$ elim
5. $B(A, \exists y Mem(y,N,t) \wedge R(y,\phi,t), t)$ — 4, Axiom **BR1**
6. $S \wedge Mem(A,K,t)$ — 3, $\wedge$ elim
7. $\neg\mathcal{B}(\phi,A,N,t)$ — 6, FOL
8. $B(A, \exists y Mem(y,N,t) \wedge R(y,\phi,t), t) \wedge \neg\mathcal{B}(\phi,A,N,t)$ — $5 \wedge 7$
9. $\forall x[S \wedge Mem(x,K,t) \wedge B(x, \forall y[Mem(y,N,t) \rightarrow \neg B(y,\neg\xi,t) \wedge B(y,\xi\rightarrow\phi,t)],t)] \rightarrow \neg\mathcal{B}(\xi,x,N,t)$ — 2,8 $\neg$ intro
10. $\exists x[S \wedge Mem(x,K,t) \wedge B(x, \forall y[Mem(y,N,t) \rightarrow \neg B(y,\neg\xi,t) \wedge B(y,\xi\rightarrow\phi,t)],t) \wedge \mathcal{I}(x, \forall y, t'[t \leq t' \wedge Mem(y,N,t') \wedge \forall t''[t \leq t'' \leq t' \rightarrow H(\psi,t'')] \rightarrow R(y,\xi,t')], t)]$ — 1,9 $\vee$ elim
11. $S \wedge Mem(A,K,t) \wedge B(A, \forall y[Mem(y,N,t) \rightarrow \neg B(y,\neg\xi,t) \wedge B(y,\xi\rightarrow\phi,t)],t)] \wedge \mathcal{I}(A, \forall y, t'[t \leq t' \wedge Mem(y,N,t') \wedge \forall t''[t \leq t'' \leq t' \rightarrow H(\psi,t'')] \rightarrow R(y,\xi,t')], t)$ — 10, $\exists$ elim
12. $S \wedge Mem(A,K,t)$ — 11, $\wedge$ elim
13. $I(A, \forall y, t'[t \leq t' \wedge Mem(y,N,t') \wedge \forall t''[t \leq t'' \leq t' \rightarrow H(\psi,t'')] \rightarrow \neg R(y,\phi,t')], t)$ — 12, FOL
14. $B(A, \forall y[Mem(y,N,t) \rightarrow \neg B(y,\neg\xi,t) \wedge B(y,\xi\rightarrow\phi,t)], t)$ — 11, $\wedge$ elim

15. $B(A, \forall y, t'[t \leq t' \wedge Mem(y, N, t') \wedge \forall t''[t \leq t'' \leq t' \rightarrow H(\psi, t'')]$
$\rightarrow [R(y, \xi, t') \rightarrow R(y, \phi, t')]], t)$ 14, Theorem **BR1**

16. $\neg\mathcal{I}(A, \forall y, t'[t \leq t' \wedge Mem(y, N, t') \wedge \forall t''[t \leq t'' \leq t' \rightarrow$
$H(\psi, t'')] \rightarrow R(y, \xi, t')], t)$ 13,15 FOL

17. $\mathcal{I}(A, \forall y, t'[t \leq t' \wedge Mem(y, N, t') \wedge \forall t''[t \leq t'' \leq t' \rightarrow H(\psi, t'')]$
$\rightarrow R(y, \xi, t')], t)$ 11, $\wedge$ elim

18. $\neg\mathcal{I}(A, \forall y, t'[t \leq t' \wedge Mem(y, N, t') \wedge \forall t''[t \leq t'' \leq t' \rightarrow$
$H(\psi, t'')] \rightarrow R(y, \xi, t')], t) \wedge \mathcal{I}(A, \forall y, t'[t \leq t' \wedge Mem(y, N, t') \wedge$
$\forall t''[t \leq t'' \leq t' \rightarrow H(\psi, t'')] \rightarrow R(y, \xi, t')], t)$ 16 $\wedge$ 17

19. $\forall x[S \wedge Mem(x, K, t) \wedge B(x, \forall y[Mem(y, N, t) \rightarrow \neg B(y, \neg\xi, t) \wedge$
$B(y, \xi \rightarrow \phi, t)], t) \rightarrow \neg\mathcal{B}(\xi, x, N, t) \wedge \neg\mathcal{I}(x, \forall y, t'[t \leq t' \wedge Mem(y, N, t') \wedge$
$\forall t''[t \leq t'' \leq t' \rightarrow H(\psi, t'')] \rightarrow R(y, \xi, t')], t)]$ 1,18 $\neg$ intro

□

Appendix C Typology of Secrets Theorem Proofs

Theorem 8 1. $\Sigma \vdash S_2 \wedge S_3 \leftrightarrow \forall x[S \wedge Mem(x, K, t) \rightarrow B(x, S_1, t)]$

Proof.

1. $S_2 \wedge S_3$ assumption
2. $S \wedge \forall x[Mem(x, K, t) \rightarrow B(x, S, t)] \wedge S \wedge \forall x[Mem(x, K, t) \rightarrow$
$B(x, \forall y[Mem(y, N, t) \rightarrow \neg R(y, \phi, t)], t)]$ 1, S def
3. $S \wedge \forall x[Mem(x, K, t) \rightarrow B(x, S \wedge \forall y[Mem(y, N, t) \rightarrow \neg R(y, \phi, t)], t)]$
2, FOL
4. $S \wedge \forall x[Mem(x, K, t) \rightarrow B(x, S_1, t)]$ 3, S_1 def

5. $S_2 \wedge S_3 \rightarrow \forall x[S \wedge Mem(x, K, t) \rightarrow B(x, S_1, t)]$ $1 \rightarrow 4$
6. $S \wedge \forall x[Mem(x, K, t) \rightarrow B(x, S_1, t)]$ assumption
7. $S \wedge \forall x[Mem(x, K, t) \rightarrow B(x, S \wedge$
$\forall y[Mem(y, N, t) \rightarrow \neg R(y, \phi, t)], t)]$ 6, S_1 def
8. $S \wedge \forall x[Mem(x, K, t) \rightarrow B(x, S, t)] \wedge \forall x[Mem(x, K, t) \rightarrow$
$B(x, \forall y[Mem(y, N, t) \rightarrow \neg R(y, \phi, t)], t)]$ 7, FOL
9. $S_2 \wedge S_3$ 8, S defs
10. $S \wedge \forall x[Mem(x, K, t) \rightarrow B(x, S_1, t)] \rightarrow S_2 \wedge S_3$ $6 \rightarrow 9$
11. $S_2 \wedge S_3 \leftrightarrow \forall x[S \wedge Mem(x, K, t) \rightarrow B(x, S_1, t)]$ $5 \wedge 10$

□

2. $\Sigma \vdash S_5 \rightarrow S_2$

Proof.

1. $S \wedge \forall x[Mem(x, K, t) \rightarrow B(x, Mem(x, K, t) \wedge$
$\forall y[Mem(y, K, t) \rightarrow B(y, S, t)], t)]$ assumption
2. $\forall x[Mem(x, K, t) \rightarrow B(x, Mem(x, K, t), t)]$ 1, FOL
3. $\forall x[Mem(x, K, t) \rightarrow B(x, \forall y[Mem(y, K, t) \rightarrow B(y, S, t)], t)]$
1, FOL
4. $\forall x[Mem(x, K, t) \rightarrow B(x, B(x, S, t), t)]$ 2,3 FOL
5. $\forall x[Mem(x, K, t) \rightarrow B(x, S, t)]$ 4, FOL
6. S 1, $\wedge$ elim

7. $S \wedge \forall x[Mem(x,K,t) \rightarrow B(x,S,t)]$ — $5 \wedge 6$

8. $S_5 \rightarrow S_2$ — $1 \rightarrow 7$

□

3. $\Sigma \vdash S_4 \rightarrow [S_5 \leftrightarrow \forall x[Mem(x,K,t) \rightarrow B(x,S_2,t)]]$

Proof.

1. $S_4 \wedge S_5$ — assumption
2. $S \wedge \forall x[Mem(x,K,t) \rightarrow B(x,Mem(x,K,t) \wedge \forall y[Mem(y,K,t) \rightarrow B(y,S,t)],t)]$ — 1, $\wedge$ elim, S_5 def
3. $S \wedge \forall x[Mem(x,K,t) \rightarrow B(x,\forall y[Mem(y,K,t) \rightarrow B(y,S,t)],t)]$ — 2, FOL
4. $S \wedge \forall x,y[Mem(x,K,t) \wedge Mem(y,K,t) \leftrightarrow B(x,Mem(y,K,t),t)]$ — 1, $\wedge$ elim, S_4 def
5. $\forall x[Mem(x,K,t) \rightarrow B(x,Mem(x,K,t),t)]$ — 4, FOL
6. $\forall x[Mem(x,K,t) \rightarrow B(x,S,t)]$ — 3,5 FOL
7. $\forall x[Mem(x,K,t) \rightarrow B(x,S \wedge \forall y[Mem(y,K,t) \rightarrow B(y,S,t)],t)$ — 3,6 FOL
8. $\forall x[Mem(x,K,t) \rightarrow B(x,S_2,t)$ — 7, S_2 def

9. $S_4 \wedge S_5 \rightarrow \forall x[Mem(x,K,t) \rightarrow B(x,S_2,t)]$ — $1 \rightarrow 8$
10. $S_4 \wedge \forall x[Mem(x,K,t) \rightarrow B(x,S_2,t)]$ — assumption
11. $S \wedge \forall x,y[Mem(x,K,t) \wedge Mem(y,K,t) \leftrightarrow B(x,Mem(y,K,t),t)]$ — 10, $\wedge$ elim, S_4 def
12. $S \wedge \forall x[Mem(x,K,t) \rightarrow B(x,Mem(x,K,t),t)]$ — 11, FOL
13. $\forall x[Mem(x,K,t) \rightarrow B(x,S \wedge \forall y[Mem(y,K,t) \rightarrow B(y,S,t)],t)$ — 10, S_2 def
14. $S \wedge \forall x Mem(x,K,t) \rightarrow B(x,Mem(x,K,t) \wedge \forall y[Mem(y,K,t) \rightarrow B(y,S,t)],t)$ — 12, 13 FOL
15. S_5 — 14, S_5 def

16. $S_4 \wedge \forall x[Mem(x,K,t) \rightarrow B(x,S_2,t)] \rightarrow S_5$ — $10 \rightarrow 15$
17. $S_4 \rightarrow [S_5 \leftrightarrow \forall x[Mem(x,K,t) \rightarrow B(x,S_2,t)]]$ — $9 \wedge 16$

□

4. *If* $\psi \vdash \forall y[Mem(y,N,t) \rightarrow \neg R(y,\phi,t)]$ *then* $\Sigma \vdash S \rightarrow S_3$

Proof.

1. $\neg NFE(K,t) \wedge \forall x[Mem(x,K,t) \rightarrow B(x,\phi \wedge \psi \wedge \neg NFE(N,t),t) \wedge \neg \mathcal{B}(\phi,x,N,t) \wedge \mathcal{I}(\phi,x,N,\psi,t)]$ — assumption
2. $\forall x[Mem(x,K,t) \rightarrow B(x,\phi \wedge \psi \wedge \neg NFE(N,t),t)]$ — 1, $\wedge$ elim
3. $\forall x[Mem(x,K,t) \rightarrow B(x,\psi,t)]$ — 2, FOL
4. $\forall x[Mem(x,K,t) \rightarrow B(x,\forall y Mem(y,N,t) \rightarrow \neg R(y,\phi,t),t)]$ — 3, Premise FOL
5. $S \wedge \forall x Mem(x,K,t) \rightarrow B(x,\forall y Mem(y,N,t) \rightarrow \neg R(y,\phi,t),t)$ — $1 \wedge 4$
6. S_3 — 5, S_3 def

7. $S \rightarrow S_3$ — $1 \rightarrow 6$

□

Theorem 9 *1.* $\Sigma \vdash S_1 \rightarrow [\forall x[Mem(x,K,t) \rightarrow \neg Mem(x,N,t)]]$

Proof.

1. S_1	assumption
2. $\exists x[Mem(x,K,t) \wedge Mem(x,N,t)$	assumption
3. $S \wedge \forall x[Mem(x,N,t) \rightarrow \neg R(x,\phi,t)]$	1, S_1 def
4. $\forall x[Mem(x,K,t) \rightarrow B(x,\phi \wedge \psi \wedge \neg NFE(N,t),t)]$	3, S def FOL
5. $\forall x[Mem(x,K,t) \rightarrow B(x,\phi,t)]$	4, FOL
6. $\forall x[Mem(x,K,t) \rightarrow R(x,\phi,t)]$	5, Theorem **T2**
7. $Mem(A,K,t) \wedge Mem(A,N,t)$	2, $\exists$ elim
8. $\neg R(A,\phi,t)$	3,7 $\wedge, \rightarrow$ elim
9. $R(A,\phi,t)$	6,7 $\wedge, \rightarrow$ elim
10. $R(A,\phi,t) \wedge \neg R(A,\phi,t)$	8 $\wedge$ 9
11. $\forall x[Mem(x,K,t) \rightarrow \neg Mem(x,N,t)]$	2,10 $\neg$ intro
12. $S_1 \rightarrow [\forall x[Mem(x,K,t) \rightarrow \neg Mem(x,N,t)]]$	1,10 $\neg$ intro

□

2. $\Sigma \vdash S_2 \rightarrow [\forall x[Mem(x,K,t) \rightarrow B(x,\neg\exists y[Mem(y,K,t) \wedge Mem(y,N,t)],t)]]$

Proof.

1. $S \wedge \forall x[Mem(x,K,t) \rightarrow B(x,S,t)]$	assumption
2. $\forall x[Mem(x,K,t) \rightarrow B(x,\neg NFE(K,t) \wedge \forall x[Mem(x,K,t) \rightarrow B(x,\phi \wedge \psi \wedge \neg NFE(N,t),t) \wedge \neg \mathcal{B}(\phi,x,N,t) \wedge \mathcal{I}(\phi,x,N,\psi,t)],t)]$	1, $\wedge$ elim, S def
3. $\forall x[Mem(x,K,t) \rightarrow B(x,\forall x[Mem(x,K,t) \rightarrow B(x,\phi,t)],t)]$	2, FOL
4. $\forall x[Mem(x,K,t) \rightarrow B(x,\forall x[Mem(x,K,t) \rightarrow R(x,\phi,t)],t)]$	3, Theorem **T2**
5. $\forall x[Mem(x,K,t) \rightarrow \neg \mathcal{B}(\phi,x,N,t)]]$	1, $\wedge$ elim, S def
6. $\forall x[Mem(x,K,t) \rightarrow \neg \mathcal{B}(\phi,x,N,t) \wedge B(x,\forall x[Mem(x,K,t) \rightarrow R(x,\phi,t)],t)]$	4 $\wedge$ 5
7. $\forall x[Mem(x,K,t) \rightarrow B(x,\neg\exists y[Mem(y,K,t) \wedge Mem(y,N,t)],t)]$	6, FOL
8. $S_2 \rightarrow \forall x[Mem(x,K,t) \rightarrow B(x,\neg\exists y[Mem(y,K,t) \wedge Mem(y,N,t)],t)]$	1 $\rightarrow$ 7

□

3. $\Sigma \vdash S_1 \rightarrow \forall y[Mem(y,N,t) \rightarrow \neg B(y,S \wedge \exists z[Mem(z,K,t)],t)]$

Proof.

1. $S_1 \wedge \exists y[Mem(y,N,t) \wedge B(y,S \wedge \exists z Mem(z,K,t),t)]$	assumption
2. $S \wedge \forall y[Mem(y,N,t) \rightarrow \neg R(y,\phi,t)]$	1, S_1 def
3. $Mem(Y,N,t) \wedge B(Y,S \wedge \exists z[Mem(z,K,t)],t)$	1, $\exists$, $\wedge$ elim
4. $Mem(Y,N,t) \wedge R(Y,S \wedge \exists z[Mem(z,K,t)],t)$	3, Theorem **T2**
5. $R(Y,\phi,t)$	4, Theorem 1.1
6. $\neg R(Y,\phi,t)$	2,4 $\forall$ elim
7. $\neg R(Y,\phi,t) \wedge R(Y,\phi,t)$	5 $\wedge$ 6

8. $S_1 \rightarrow \forall y[Mem(y,N,t) \rightarrow \neg B(y, S \wedge \exists z Mem(z,K,t),t)]$ 1,7 $\neg$ intro

□

4. $\Sigma \vdash S_3 \rightarrow \forall x[Mem(x,K,t) \rightarrow B(x, \forall y[Mem(y,N,t) \rightarrow \neg B(y, S \wedge \exists z[Mem(z,K,t)],t)],t)]$

Proof.

1. $S \wedge \forall x[Mem(x,K,t) \rightarrow B(x, \forall y[Mem(y,N,t) \rightarrow \neg R(y,\phi,t)],t)]$ assumption
2. $\forall x[R(x, S \wedge \exists y[Mem(y,K,t)]) \rightarrow R(x,\phi)]$ Theorem 1.1
3. $\forall x[Mem(x,K,t) \rightarrow B(x, \forall y[Mem(y,N,t) \rightarrow \neg R(y, S \wedge \exists z[Mem(z,K,t)]],t)]$ 1,2 FOL
4. $\forall x[Mem(x,K,t) \rightarrow B(x, \forall y[Mem(y,N,t) \rightarrow \neg B(y, S \wedge \exists z[Mem(z,K,t)]],t)]$ 3, Theorem **T2**
5. $S_3 \rightarrow \forall x[Mem(x,K,t) \rightarrow B(x, \forall y[Mem(y,N,t) \rightarrow \neg B(y, S \wedge \exists z[Mem(z,K,t)]],t)]$ 1,4 $\rightarrow$ intro

□

5. $\Sigma \vdash S_2 \rightarrow \forall x[Mem(x,K,t) \rightarrow B(x, \forall y[Mem(y,K,t) \rightarrow Secret_0(\phi,[y],N,\psi,t)],t)]$

Proof.

1. $S \wedge \forall x[Mem(x,K,t) \rightarrow B(x,S,t)]$ assumption
2. $\forall x[Mem(x,K,t) \rightarrow B(x, \neg NFE(K,t) \wedge \forall y[Mem(y,K,t) \rightarrow B(y, \phi \wedge \psi \wedge \neg NFE(N,t),t) \wedge \neg \mathcal{B}(\phi,y,N,t) \wedge \mathcal{I}(\phi,y,N,\psi,t)],t)]$ 1, S def
    3. $Mem(x,K,t)$ assumption
    4. $B(x, \neg NFE(K,t) \wedge \forall y[Mem(y,K,t) \rightarrow B(y, \phi \wedge \psi \wedge \neg NFE(N,t),t) \wedge \neg \mathcal{B}(\phi,y,N,t) \wedge \mathcal{I}(\phi,y,N,\psi,t)],t)$ 2,3 FOL
    5. $B(x, \forall y[Mem(y,K,t) \rightarrow Secret_0(\phi,[y],N,\psi,t)],t)$ 4, S def
6. $Mem(x,K,t) \rightarrow B(x, \forall y[Mem(y,K,t) \rightarrow Secret_0(\phi,[y],N,\psi,t)],t)$ 3,5 $\rightarrow$ intro
7. $S_2 \rightarrow \forall x[Mem(x,K,t) \rightarrow B(x, \forall y[Mem(y,K,t) \rightarrow Secret_0(\phi,[y],N,\psi,t)],t)]$ 1,6 $\rightarrow$ intro

□

6. $\Sigma \vdash S_4 \wedge S_2 \rightarrow \forall x[Mem(x,K,t) \rightarrow \forall y[Mem(y,K,t) \rightarrow B(x, Secret_0(\phi,[y],N,\psi,t),t)]]$

Proof.

1. $S_2 \wedge S \wedge \forall x,y[Mem(x,K,t) \wedge Mem(y,K,t) \leftrightarrow B(x, Mem(y,K,t),t)$ assumption
    2. $Mem(x,K,t)$ assumption
        3. $Mem(y,K,t)$ assumption
        4. $S_2 \wedge Mem(x,K,t) \wedge B(x, Mem(y,K,t),t)$ 1,3 FOL
        5. $B(x, Secret_0(\phi,[y],N,\psi,t),t)$ 3,4 Theorem 9.5
    6. $\forall y[Mem(y,K,t) \rightarrow B(x, Secret_0(\phi,[y],N,\psi,t),t)]$ 3,5 $\rightarrow$ intro
7. $\forall x[Mem(x,K,t) \rightarrow \forall y[Mem(y,K,t) \rightarrow$

$B(x, Secret_0(\phi, [y], N, \psi, t), t)]]$ 2,6 $\rightarrow$ intro

8. $S_2 \wedge S_4 \rightarrow \forall x[Mem(x, K, t) \rightarrow \forall y[Mem(y, K, t) \rightarrow$
$B(x, Secret_0(\phi, [y], N, \psi, t), t)]]$ $1 \rightarrow 7$

□