Symbolic Verification of the Needham-Schroeder-Lowe Protocol

1 Symbolic Execution of NSL in Our Framework

1. $A \to B : \{N_1, A\}_{eK_B}$
2. $B \to A : \{N_1, N_2, B\}_{eK_A}$
3. $A \to B : \{N_2\}_{eK_B}$

In this analysis, we assume that A executes initiator sessions only, and B executes responder sessions only. We further assume that they don't initiate sessions with themselves. We also assume that all agents other than A and B are corrupted, that is to say, faked by the adversary. Clearly, if we prove security in this case, it also holds with other honest agents. We use the convention $\langle x, y, z\rangle \equiv \langle x, \langle y, z\rangle\rangle$. We show that in a symbolic execution, violating the secrecy of nonces N_1 and N_2, as well as violating the agreement and authentication properties are inconsistent with our axioms.

For the verification purposes, let c_i be a special function symbol, that takes as arguments A, B, N_1, N_2: who commits for who and the corresponding nonces. $c_i(A, B, N_1, N_2)$ is sent along with $\{N_1, N_2, B\}_A$. For the responder, there is a similar commitment: at the end of the protocol, B emits (as a last message) $c_r(A, B, N_1, N_2)$.

1.1 Roles

The initiator, communicating with intended party Q, does the following sequence of steps in session i which we will informally denote by $Init^A_{NSL}[A, i, Q, N_1, h_1, h_3, R_1, R_3]$:

- Receives some h_1 from the adversary that triggers the start of the session with intended party Q
- A generates nonce N_1.
- A sends $\{N_1, A\}^{R_1}_{eK_Q}$
- A receives h_2, and checks
  - $\pi_1\left(\mathit{dec}(h_3, dK_A)\right) = N_1$
  - $\pi_2\left(\pi_2\left(\mathit{dec}(h_3, dK_A)\right)\right) = Q$
- A sends $\{\pi_1\left(\pi_2\left(\mathit{dec}(h_3, dK_A)\right)\right)\}^{R_3}_{eK_Q}$
- A sends $c_i\big(A, Q, N_1, \pi_1\left(\pi_2\left(\mathit{dec}(h_3, dK_A)\right)\right)\big)$

The responder does the following sequence of steps in session i' which we will informally denote by $Resp^B_{NSL}[B, i', N_2, h_2, h_4, R_2]$:

- B receives some h_2 from the adversary and checks

- $W(\pi_2\,(dec(h_2, dK_B)))$ (Checks that it is a name of someone)

- B generates nonce N_2.
- B sends $\{\pi_1\,(dec(h_2, dK_B))\,, N_2, B\}^{R_2}_{eK_{\pi_2(dec(h_2,dK_B))}}$
- B receives h_4, and checks
  - $dec(h_4, dK_B) = N_2$
- B sends $c_r(\pi_2\,(dec(h_2, dK_B))\,, B, \pi_1\,(dec(h_2, dK_B))\,, N_2)$

1.2 Our General Symbolic Execution Framework

A *symbolic state* of the network consists of:

- a control state $q \in Q$ together with a sequence of names (that have been generated so far) $n_1, \ldots, n_k$
- a sequence constants called *handles* $h_1, \ldots, h_n$ (recording the attacker's inputs)
- a ground frame ϕ (the agents outputs)
- a set of formulas Θ (the conditions that have to be satisfied in order to reach the state).

A *symbolic transition sequence* of a protocol Π is a sequence

$$(q_0(\overline{n_0}), \emptyset, \phi_0, \emptyset) \to \ldots \to (q_m(\overline{n_m}), \langle h_1, \ldots, h_m\rangle\,, \phi_m, \Theta_m)$$

if, for every $m - 1 \geq i \geq 0$, there is a transition rule

$$(q_i(\overline{\alpha_i}), q_{i+1}(\overline{\alpha_{i+1}}), \langle x_1, \ldots, x_i\rangle\,, x, \psi, s)$$

such that $\overline{n} = \overline{\alpha_{i+1}} \setminus \overline{\alpha_i}$, $\phi_{i+1} = (\nu\overline{n}).(\phi_i \cdot p \mapsto s\rho_i\sigma_{i+1})$, $\overline{n_{i+1}} = \overline{n_i} \uplus \overline{n}$, $\Theta_{i+1} = \Theta_i \cup \{\phi_i \rhd h_{i+1}, \psi\rho_i\sigma_{i+1}\}$ where $\sigma_i = \{x_1 \mapsto h_1, \ldots, x_i \mapsto h_i\}$ and ρ_i is a renaming of the sequence $\overline{\alpha_i}$ into the sequence $\overline{n_i}$.

We assume a renaming that ensures the freshness of the names $\overline{n}$: $\overline{n} \cap \overline{n_i} = \emptyset$.

Given an interpretation $\mathcal{M}$, a transition sequence of Π

$$(q_0(\overline{n_0}), \emptyset, \phi_0, \emptyset) \to \ldots \to (q_m(\overline{n_m}), \langle h_1, \ldots, h_m\rangle\,, \phi_m, \Theta_m)$$

is *valid w.r.t.* $\mathcal{M}$ if, for every $m - 1 \geq i \geq 0$,

$$\mathcal{M} \models \Theta_{i+1}$$

Initialization

For technical purposes, we always take $\phi_0 = \nu\overline{n}()$, where $\overline{n}$ contains the honest random items to be generated, and that is followed by an empty list of terms. ϕ_1 will contain the output of the initialization, that is, the names and the public keys. We will also assume for technical purposes that all honestly generated items (nonces, random inputs of encryptions etc.) are all generated upfront.

1.3 Examples for NSL Executions

Example 1.1 We show the beginning of a possible branch in the symbolic execution of NSL.

$$(q_0, \emptyset, \phi_0, \emptyset) \quad (q_1, H_1, \phi_1, \Theta_1)\ (q_2, H_2, \phi_2, \Theta_2)\ (q_3, H_3, \phi_3, \Theta_3)\ (q_4, H_4, \phi_4, \Theta_4)$$

Where $\overline{n} = N_1, N_2, R_1, R_2, R_3$, $q_0 = (q_0^A, q_0^B)(\overline{n})$, and $q_1 = (q_1^A, q_0^B)(\overline{n})$, $q_2 = (q_1^A, q_1^B)(\overline{n})$, and $q_3 = (q_2^A, q_1^B)(\overline{n})$ and $q_4 = (q_2^A, q_2^B)(\overline{n})$. In other words, we interleave the actions of A and B, as in an expected execution and assume that the two processes were first activated (if not, we could introduce two transitions activating the processes).

- $\phi_0 = \nu_{K_A K_B}()$,
  $\Theta_0 = \emptyset$
- $H_1 = \emptyset$,
  $\phi_1 = \nu_{K_A K_B}(A, B, eK_A, eK_B)$,
  $\Theta_1 = \emptyset$
- $H_2 = \langle h_1 \rangle$,
  $\phi_2 = \nu_{K_A K_B N_1 R_1}((A, B, eK_A, eK_B), \{\langle N_1, A\rangle\}^{R_1}_{eK_B})$,
  $\Theta_2 = \{\phi_1 \rhd h_1\}$
- $H_3 = \langle h_1, h_2 \rangle$,
  ϕ_3 extends ϕ_2 with $\{\langle \pi_1(\mathit{dec}(h_2, dK_B)), \langle N_2, B\rangle\rangle\}^{R_2}_{eK_{\pi_2(\mathit{dec}(h_2, dK_B))}}$,
  $\Theta_3 = \Theta_2 \cup \{\phi_2 \rhd h_2, W(\pi_2(\mathit{dec}(h_2, dK_B)))\}$
- $H_4 = \langle h_1, h_2, h_3 \rangle$,
  ϕ_4 extends ϕ_3 with $\{\pi_1(\pi_2(\mathit{dec}(h_3, dK_A)))\}^{R_3}_{eK_B}$,
  $\Theta_4 = \Theta_3 \cup \{\phi_3 \rhd h_3, \pi_1(\mathit{dec}(h_3, dK_A)) = N_1, \pi_2(\pi_2(\mathit{dec}(h_3, dK_A))) = B\}$
- $H_5 = \langle h_1, h_2, h_3, h_4 \rangle$, $\phi_5 = \phi_4$,
  $\Theta_5 = \Theta_4 \cup \{\phi_4 \rhd h_4, \mathit{dec}(h_4, dK_B) = N_2\}$

Let $\mathcal{M}$ be a model in which such that $\pi_2(\mathit{dec}(h_2, dK_B)) = A$ and

$$h_2 =_{\mathcal{M}} \{\langle N_1, A\rangle\}^{R_1}_{eK_B}, \qquad h_3 =_{\mathcal{M}} \{\langle N_1, \langle N_2, B\rangle\rangle\}^{R_2}_{eK_A}, \qquad h_4 =_{\mathcal{M}} \{N\}^{R_3}_{eK_B},$$

and $\rhd_{\mathcal{M}}$ is simply the classical Dolev-Yao deduction relation. Then the execution sequence is valid w.r.t. $\mathcal{M}$, and this corresponds to the correct execution of the NSL protocol between A and B.

There are however other models in which this transition sequence is valid. For instance let $\mathcal{M}'$ be such that $h_2 =_{\mathcal{M}'} N_1$ and $\phi_1 \rhd_{\mathcal{M}'} h_2$ and $N_1 =_{\mathcal{M}'} \{\langle N_1, A\rangle\}^{R_1}_{eK_B}$, (and h_3, h_4 as above). We get again a valid transition sequence w.r.t. $\mathcal{M}'$. Though, in what follows, we will discard such sequences, thanks to some axioms.

Example 1.2 Consider again the transitions of the example 1.1. Now consider a model $\mathcal{M}$ in which $N_0, \{N_1, N_2, B\}^{R_2}_{eK_A} \rhd_{\mathcal{M}} \{N_1, N_0, B\}^{r}_{eK_A}$ for an honestly generated nonce n_0 that can be chosen by the attacker: the transition sequence of the previous example is also valid w.r.t. this model. This will yield an attack, using a malleability property of the encryption scheme.

Discarding such attacks requires some properties of the encryption scheme (for instance IND-CCA). It can be ruled out by a non-malleability axiom.

2 First Order Formulation of the Properties We Need

2.1 Predicates and satisfaction at step n

- Predicates: $x = y$; $\quad \hat{\phi}, x_1, ..., x_m \rhd x$;
- Constraints: $\mathsf{RandGen}(x)$; $\quad x \sqsubseteq \hat{\phi}, \vec{x}$; $\quad x \preccurlyeq \hat{\phi}$;
  $\mathsf{fresh}(x; \hat{\phi}, \vec{x}) \equiv \mathsf{RandGen}(x) \ \wedge \ \neg(x \sqsubseteq \hat{\phi}, \vec{x})$
- Let $\mathcal{M}$ be any first-order structure, which interprets terms and the predicates $=$ and $\rhd$ such that $=$ is interpreted as the equality in the underlying domain $D_{\mathcal{M}}$.

  Given a assigment σ of elements in $D_{\mathcal{M}}$ to the free variables of term t, we write $[\![t]\!]^{\sigma}_{\mathcal{M}}$ for the interpretation of t in $\mathcal{M}$ ($[\![\_]\!]^{\sigma}_{\mathcal{M}}$ is the unique extension of σ into a homomorphism of $\mathcal{F}$-algebras).

  For any first order structure $\mathcal{M}$ over the functions $\mathcal{F}$ and predicates $\mathcal{P}$, the satisfaction relation $\mathcal{M}, \sigma \models \theta$, where σ is an assignment of the free variables of θ in the domain of $\mathcal{M}$, is defined as usual. $\mathcal{M}$ includes in particular a relation $\rhd_{\mathcal{M}}$ that interprets the deducibility predicate $\rhd$.
- Interpretation of predicates by $\mathcal{M}, \sigma, \langle t_1, \ldots, t_m \rangle, (n_1, \ldots, n_k)$, where σ is substitution as above, $t_1, ..., t_m$ are closed terms, $n_1, ..., n_k$ are names (note that the interpretation depends on the model $\mathcal{M}$):
  - $t = t'$
    $\mathcal{M}, \sigma, \langle t_1, \ldots, t_m \rangle, (n_1, \ldots, n_k) \models x = y$
    if $\mathcal{M}, \sigma \models t = t'$
  - $\hat{\phi}, s_1, \ldots, s_n \rhd t$, where $\hat{\phi}$ is part of the syntax of the predicate (not an input), intuitively, it aims at ranging over frames:
    $\mathcal{M}, \sigma, \langle t_1, \ldots, t_m \rangle, \overline{n} \models \hat{\phi}, s_1, \ldots, s_n \rhd t$ if $\mathcal{M}, \sigma \models s_1, \ldots, s_n, t_1, \ldots, t_m \rhd t$
- Interpretation of constraints by $\mathcal{M}, \sigma, \langle t_1, \ldots, t_m \rangle, (n_1, \ldots, n_k)$, where σ is substitution as above, $t_1, ..., t_m$ are closed terms, $n_1, ..., n_k$ are names (note that the interpretation does not depend on the model $\mathcal{M}$):
  - $\mathsf{RandGen}(s)$ for s closed term (name):
    $\mathcal{M}, \sigma, \langle t_1, \ldots, t_m \rangle, (n_1, \ldots, n_k) \models \mathsf{RandGen}(s)$
    if $\mathcal{M}, \sigma \models s = n_1 \vee \ldots \vee x = n_k$.
  - $t \sqsubseteq \hat{\phi}, s_1, ..., s_n$, where $s_1, ..., s_n$ and t are closed terms:
    $\mathcal{M}, \sigma, \langle t_1, \ldots, t_m \rangle, \overline{n} \models t \sqsubseteq \hat{\phi}, s_1, ..., s_n$ if t is a subterm of some t_i or some s_i
  - $t \preccurlyeq \hat{\phi}$, where t is closed:
    $\mathcal{M}, \sigma, \langle t_1, \ldots, t_m \rangle, \overline{n} \models t \preccurlyeq \hat{\phi}$ if for every handle h of t, $\hat{\phi} \rhd h$.
  - We also may use the derived predicate (as an abbreviation):

    $$\mathsf{fresh}(x; \hat{\phi}, \vec{x}) = \mathsf{RandGen}(x) \wedge x \not\sqsubseteq \hat{\phi}, \vec{x}$$
- Interpretation by $\mathcal{M}, \langle t_1, \ldots, t_m \rangle, (n_1, \ldots, n_k)$ (where σ is substitution as above) of any FOL formula in which there are no free variables under constraints is defined recursively:
  - Interpretations of $\theta_1 \wedge \theta_2$ and $\theta_1 \vee \theta_2$ and $\neg\theta$ are defined as usual in FOL
  - If x does not occur under a constraint in θ, interpretations of $\forall x\theta$ and $\exists\theta$ is defined as usual in FOL.
  - If x occurs under a constraint in θ, then
    - $\mathcal{M}, \sigma, \langle t_1, \ldots, t_n \rangle, (n_1, \ldots, n_k) \models \forall x\theta$ iff for every ground term t, $\mathcal{M}, \sigma, \langle t_1, \ldots, t_n \rangle, (n_1, \ldots, n_k) \models \theta\{x \mapsto t\}$

$*$ $\mathcal{M}, \sigma, \langle t_1, \ldots, t_n \rangle, (n_1, \ldots, n_k) \models \exists x \theta$ iff there is a ground term t, $\mathcal{M}, \sigma, \langle t_1, \ldots, t_n \rangle, (n_1, \ldots, n_k) \models \theta\{x \mapsto t\}$

- Satisfaction at step m:

$$\mathcal{M}, (q, \langle h_1, \ldots, h_m \rangle, \overline{n}, \phi_m, \Theta) \models \theta \quad \text{iff} \quad \mathcal{M}, \phi_m, \overline{n} \models \theta.$$

Computational interpretations of predicates are defined. Soundness theorem says that if a FOL formula is computationally satisfied in some execution, then there is a symbolic trace on which it is consistent with the agent checks and the computationally sound axioms (and the satisfaction of the checkable predicates).

- $x \sqsubseteq \hat{\phi}, \vec{x} \;\equiv\; x \sqsubseteq \hat{\phi} \vee x \sqsubseteq \vec{x}$
- $\mathsf{fresh}(x; \hat{\phi}, \vec{x}) \;\equiv\; \mathsf{RandGen}(x) \wedge x \not\sqsubseteq \hat{\phi} \wedge x \not\sqsubseteq \vec{x}$
- $\vec{x} \preccurlyeq \hat{\phi} \;\equiv\; h \sqsubseteq \vec{x} \wedge \mathsf{Handle}(h) \rightarrow \hat{\phi} \rhd h$

$\mathsf{fresh}(x; \hat{\phi}, h)$ holds even if $h = x$.

2.2 Computationally Sound Axioms Used

- Derivability implies corruption: $\hat{\phi}, \vec{x} \rhd dK \;\longrightarrow\; \hat{\phi}, \vec{x} \blacktriangleright K$
- Increasing capabilities for key corruption: $\hat{\phi}, \vec{x} \blacktriangleright K \;\longrightarrow\; \hat{\phi}, \vec{x}, x \blacktriangleright K$
- Commutativity: If $\vec{x}'$ is a permutation of $\vec{x}$, then $\hat{\phi}, \vec{x} \blacktriangleright K \;\longrightarrow\; \hat{\phi}, \vec{x}' \blacktriangleright K$
- Transitivity: $\hat{\phi}, \vec{x} \rhd \vec{y} \;\wedge\; \hat{\phi}, \vec{x}, \vec{y} \blacktriangleright K \;\longrightarrow\; \hat{\phi}, \vec{x} \blacktriangleright K$
- Function application: $\hat{\phi}, f(\vec{x}) \blacktriangleright K \;\longrightarrow \hat{\phi}, \vec{x} \blacktriangleright K$
- Fresh keys are not corrupted: $\mathsf{keyfresh}(K; \hat{\phi}) \;\longrightarrow\; \hat{\phi} \not\blacktriangleright K$.
- Fresh items do not corrupt:

$$\mathsf{fresh}(x; \hat{\phi}, \vec{x}, y) \;\wedge\; \vec{x} \preccurlyeq \hat{\phi} \;\wedge\; y \preccurlyeq \hat{\phi} \;\wedge\; \hat{\phi}, \vec{x}, x \blacktriangleright K \;\longrightarrow\; \hat{\phi}, \vec{x} \blacktriangleright K$$

- Uncorrupted keys securely encrypt.
  - Secrecy of asymmetric IND-CCA2 encryption:

$$\mathsf{RandGen}(K) \;\wedge\; eK \sqsubseteq \hat{\phi} \;\wedge\; \mathsf{fresh}(R; \hat{\phi}, \vec{x}, x, y) \;\wedge\; \vec{x}, x, y \preccurlyeq \hat{\phi}$$
$$\wedge\; \hat{\phi}, \vec{x}, \{x\}^R_{eK} \rhd y \;\longrightarrow\; \hat{\phi}, \vec{x}, x \blacktriangleright K \;\vee\; \hat{\phi}, \vec{x} \rhd y$$

  - Non-malleability of asymmetric IND-CCA2 encryption.

$$\mathsf{RandGen}(N) \;\wedge\; \mathsf{RandGen}(K) \;\wedge\; eK \sqsubseteq \hat{\phi} \;\wedge\; \vec{x} \preccurlyeq \hat{\phi} \;\wedge\; N \sqsubseteq \hat{\phi}, \vec{x}$$
$$\wedge\; \hat{\phi}, \vec{x} \rhd y \;\wedge \hat{\phi}, \vec{x}, \mathit{dec}(y, dK) \rhd N \;\wedge\; \forall x R(y = \{x\}^R_{eK} \rightarrow \{x\}^R_{eK} \not\sqsubseteq \hat{\phi}, \vec{x})$$
$$\longrightarrow\; \hat{\phi}, \vec{x} \blacktriangleright K \;\vee\; \hat{\phi}, \vec{x} \rhd N$$

- Encryptions with uncorrupted keys do not korrupt.

$$\mathsf{RandGen}(K) \wedge \mathsf{RandGen}(K') \wedge eK \sqsubseteq \hat{\phi} \wedge eK' \sqsubseteq \hat{\phi} \wedge \mathsf{fresh}(R; \hat{\phi}, \vec{x}, x)$$
$$\wedge\; \vec{x}, x \preccurlyeq \hat{\phi} \;\wedge\; \hat{\phi}, \vec{x}, \{x\}^R_{eK'} \blacktriangleright K \;\longrightarrow\; \hat{\phi}, \vec{x}, x \blacktriangleright K' \;\vee\; \hat{\phi}, \vec{x} \blacktriangleright K$$

- $x = x$, and the substitutability (congruence) property of equal terms holds.
- Self derivability: $\hat{\phi}, \vec{x}, x \rhd x$
- Increasing capabilities: $\hat{\phi}, \vec{x} \rhd y \longrightarrow \hat{\phi}, \vec{x}, x \rhd y$
- Commutativity: If $\vec{x}'$ is a permutation of $\vec{x}$, then $\hat{\phi}, \vec{x} \rhd y \longrightarrow \hat{\phi}, \vec{x}' \rhd y$
- Transitivity of derivability: $\hat{\phi}, \vec{x} \rhd \vec{y} \wedge \hat{\phi}, \vec{x}, \vec{y} \rhd \vec{z} \longrightarrow \hat{\phi}, \vec{x} \rhd \vec{z}$
- Functions are derivable: $\hat{\phi}, \vec{x} \rhd f(\vec{x})$
- No telepathy: $\mathsf{fresh}(x; \hat{\phi}) \longrightarrow \hat{\phi} \not\rhd x$
- Fresh items are independent:

  $\mathsf{fresh}(x; \hat{\phi}, \vec{x}) \wedge \mathsf{RandGen}(N) \wedge \vec{x} \preccurlyeq \hat{\phi} \wedge \hat{\phi}, \vec{x}, x \rhd N \longrightarrow \hat{\phi}, \vec{x} \rhd N \vee x = N$

- Special to IND-CCA encryption:
- Secrecy:

$$\hat{\phi}, \vec{x}, \{x\}^R_{eK} \rhd y \longrightarrow dK \sqsubseteq \hat{\phi}, \vec{x}, x \vee \hat{\phi}, \vec{x} \rhd y$$

- Non-malleability (assuming there is only one kind of encryption and pairing):

$$\begin{aligned}&\mathsf{RandGen}(N) \wedge \mathsf{RandGen}(K) \wedge eK \sqsubseteq \hat{\phi} \wedge \vec{x} \preccurlyeq \hat{\phi} \wedge N \sqsubseteq \hat{\phi}, \vec{x} \\ &\wedge \hat{\phi}, \vec{x} \rhd y \wedge \hat{\phi}, \vec{x}, \mathit{dec}(y, dK) \rhd N \wedge \forall x R(y = \{x\}^R_{eK} \rightarrow \{x\}^R_{eK} \not\sqsubseteq \hat{\phi}, \vec{x}) \\ &\longrightarrow dK \sqsubseteq \hat{\phi}, \vec{x} \vee \hat{\phi}, \vec{x} \rhd N\end{aligned}$$

- Special to c_i, c_r (Let c be either of them):
  - c does not help the adversary: $\mathsf{RandGen}(N) \wedge \hat{\phi}, \vec{x}, c(x, y, z, w) \rhd N \rightarrow \hat{\phi}, \vec{x} \rhd N$
  - c cannot be forged and cannot be subparts of terms (not used in the proof I think):

    $$\hat{\phi}, \vec{x} \rhd c(x, y, z, w) \longrightarrow c(x, y, z, w) \sqsubseteq \hat{\phi} \vee x_1 = c(x, y, z, w) \vee ... \vee x_l = c(x, y, z, w)$$

  - c cannot be equal with anything else (not used in the proof I think): If the outermost function symbol of a term T something different from c, then $c(x, y, z, w) \neq T$.
- Equations for the function symbols
  - Equations for encryption/decryption:
    - Decryption of an encryption results the plaintext: $\mathit{dec}(\{x\}^R_{eK}, dK) = x$
  - Equations for pairing/projections:
    - First projection: $\pi_1(\langle x, y \rangle) = x$
    - Second projection: $\pi_2(\langle x, y \rangle) = y$

Further Needed Axiom (The implementation needs to satisfy this too)
For this protocol, we need an additional axiom, namely that for an honestly generated nonce N,

$$\mathsf{RandGen}(N) \rightarrow \neg W(\pi_2(N)).$$

That is, the second projection of a nonce can never be a name (by overwhelming probability on a non-negligible set). We assume that the implementation of the pairing is such that this condition is satisfied.

Executions and Consistency
Only those traces and those properties are possible that are consistent with the above axioms at each step (including step 0). This means that when we derive the inconsistency of a property at step m, we can assume consistency at every step before m.

3 Examples for Proving Inconsistency

In order to make the rather complex general security proof more understandable, we first look at three small example proofs.

Example 3.1 For example, we can use the axioms to derive that in NSL execution of Example 1.1, $\phi_2 \not\rhd A$ is inconsistent with the axioms. The reason the following: Observe that

$$\phi_2 \equiv A, B, eK_A, eK_B, \{\langle N_1, A\rangle\}^{R_1}_{eK_B} \equiv \phi_0, A, B, eK_A, eK_B, \{\langle N_1, A\rangle\}^{R_1}_{eK_B}.$$

From the self-derivability axiom at step 0,

$$\phi_0, B, eK_A, eK_B, \{\langle N_1, A\rangle\}^{R_1}_{eK_B}, A \rhd A$$

By the commutativity axiom at step 0,

$$\phi_0, A, B, eK_A, eK_B, \{\langle N_1, A\rangle\}^{R_1}_{eK_B} \rhd A,$$

which means that

$$\phi_0, A, B, eK_A, eK_B, \{\langle N_1, A\rangle\}^{R_1}_{eK_B} \not\rhd A$$

is inconsistent with the axioms. That means, for any model,

$$\mathcal{M}, \sigma \not\models A, B, eK_A, eK_B, \{\langle N_1, A\rangle\}^{R_1}_{eK_B} \not\rhd A.$$

This in turn means that

$$\phi_2 \not\rhd A$$

is inconsistent with the axioms.

Example 3.2 We can also derive, that $\phi_2 \rhd N_1$ is inconsistent with the axioms in our NSL example above. As

$$\phi_2 \equiv A, B, eK_A, eK_B, \{\langle N_1, A\rangle\}^{R_1}_{eK_B} \equiv \phi_1, \{\langle N_1, A\rangle\}^{R_1}_{eK_B},$$

it is enough to show that $\phi_1, \{\langle N_1, A\rangle\}^{R_1}_{eK_B} \rhd N_1$ is inconsistent with the axioms. Suppose that it is true, and we will get a contradiction. So suppose

$$\phi_1, \{\langle N_1, A\rangle\}^{R_1}_{eK_B} \rhd N_1. \tag{1}$$

By a similar derivation as in Example 3.1, we have that $\phi_1 \rhd A$ follows from the axioms. Then, by the increasing capabilities axiom, we have

$$\phi_1, \{\langle N_1, A\rangle\}^{R_1}_{eK_B} \rhd A \tag{2}$$

Equations (1) and (2) together are written as a shorthand

$$\phi_1, \{\langle N_1, A\rangle\}^{R_1}_{eK_B} \rhd N_1, A \tag{3}$$

By the functions derivable axiom, we also have

$$\phi_1, N_1, A \rhd \langle N_1, A\rangle \tag{4}$$

Again, by the increasing capabilities axiom, we have

$$\phi_1, N_1, A, \{\langle N_1, A\rangle\}^{R_1}_{eK_B} \rhd \langle N_1, A\rangle, \tag{5}$$

and by commutativity,

$$\phi_1, \{\langle N_1, A\rangle\}^{R_1}_{eK_B}, N_1, A \rhd \langle N_1, A\rangle. \tag{6}$$

Then, from (3) and (6), and the transitivity axiom (with roles $\vec{x} \equiv \{\langle N_1, A\rangle\}^{R_1}_{eK_B}$ and $\vec{y} \equiv N_1, A$ and $\vec{z} \equiv \langle N_1, A\rangle$), we have

$$\phi_1, \{\langle N_1, A\rangle\}^{R_1}_{eK_B} \rhd \langle N_1, A\rangle \tag{7}$$

Then, by the secrecy axiom, we get

$$\phi_1 \rhd \langle N_1, A\rangle. \tag{8}$$

By the functions are derivable axiom for π_1, we have

$$\phi_1, \langle N_1, A\rangle \rhd \pi_1\left(\langle N_1, A\rangle\right). \tag{9}$$

Since $\pi_1\left(\langle N_1, A\rangle\right) = N_1$, we have by the congruence property of $=$ that

$$\phi_1, \langle N_1, A\rangle \rhd N_1. \tag{10}$$

Equations (8) and (10) together with the transitivity axiom, we get

$$\phi_1 \rhd N_1. \tag{11}$$

But at step 1, we have $\mathsf{fresh}(N_1; \phi_1)$, so

$$\mathsf{fresh}(N_1; \phi_1) \wedge \phi_1 \rhd N_1. \tag{12}$$

But this contradicts the no telepathy axiom.

Example 3.3 From the axioms, we can also derive the following statement: For any m and x, if $\phi_m \rhd x$ is derivable from the axioms and agent checks, then $\phi_{m+1} \rhd x$ is also derivable from the axioms and agent checks. The proof is the following. Assume that $\phi_m \rhd x$ is derivable from the axioms and agent checks. Let t be the message sent by A or B in the $m+1$'th step. Then $\phi_{m+1} \equiv \phi_m, t$. The increasing capabilities axiom applied to step m means $\phi_m \rhd x$ implies

$$\phi_m, t \rhd x.$$

But that is the same as

$$\phi_{m+1} \rhd x,$$

so we are done, because we only used an axiom and that the list ϕ_{m+1} is the same as the list ϕ_m, t.

Note that from the above and from Example 3.1 it also follows that for any m, it follows from axioms that $\phi_m \rhd A$. It is clear from Example 3.1, that $\phi_2 \rhd A$ follows from axioms. Then from the above, by induction, $\phi_m \rhd A$ follows from axioms.

4 Correctness Proof

We first give an overview about how the proof goes. Our proof works for any (bounded) number of sessions. We first show secrecy of nonces. That is, we show that nonces that were generated by honest initiator A and sent to honest responder B or vice versa remain secret throughout the entire execution. Both A and B are allowed to have other sessions running with possibly corrupted agents.

We pick any step m of the execution tree, we list all possible execution rounds (according to the protocol) at the next step $m+1$ and we derive essentially that in all possibilities, $\phi_m \not\vdash N$ together with the axioms and the agent checks imply $\phi_{m+1} \not\vdash N$. In other words, $\phi_m \not\vdash N$ and the axioms and the agent checks and $\phi_{m+1} \rhd N$ are inconsistent. Since initially $\phi_0 \not\vdash N$ holds, by induction, we have $\phi_m \not\vdash N$ after any finite number of steps m. The reader can see below that the induction hypothesis is a little more complex than $\phi_m \not\vdash N$, but essentially this is what we do.

Once secrecy is proven, authentication and agreement is shown. We pick the point on the execution tree when the responder finished his task. Then, using that nonces remain secret, together with non-malleability imply that the initiator also had finished his task and the corresponding values that the two parties see have to match. In other words, B finished and (A not finished or values don't match) and the axioms and the agent checks are inconsistent.

a) Secrecy.

The aim of the secrecy proof is to show that nonces sent between A and B stay secret. This can be expressed the following way. If N is a nonce sent by A to B means that

$$\exists R\big(\{N, A\}^R_{eK_B} \sqsubseteq \hat{\phi}\big).$$

If B sent it to A, that means that

$$\exists hR\big(\{\pi_1\left(dec(h, dK_B)\right), N, B\}^R_{eK_A} \sqsubseteq \hat{\phi}\big).$$

Let us introduce the condition

$$C[N] \equiv \mathsf{RandGen}(N) \wedge \exists R\big(\{N, A\}^R_{eK_B} \sqsubseteq \hat{\phi}\big) \ \vee \ \exists hR\big(\{\pi_1\left(dec(h, dK_B)\right), N, B\}^R_{eK_A} \sqsubseteq \hat{\phi}\big)$$

Then the secrecy property takes the form

$$\forall N\big(C[N] \longrightarrow \hat{\phi} \not\vdash N\big)$$

We have to show that the negation of this,

$$\exists N\big(C[N] \wedge \hat{\phi} \rhd N\big), \tag{13}$$

is inconsistent with the axioms and the agent checks on every possible symbolic trace.

Suppose the total length of the symbolic trace in question is n. At the end of the trace, the frame, ϕ, contains n terms, let us denote the final frame by ϕ_n. Furthermore, let us denote the frames at each nodes of this trace by ϕ_0, ϕ_1, ϕ_2, etc. Each frame contains one more term than the previous one.

The satisfaction of $C[N]$ on this trace means that either the term $\{N, A\}^R_{eK_B}$ appears in the frame ϕ_n for some R, or the term $\{\pi_1\left(dec(h, dK_B)\right), N, B\}^R_{eK_A}$ appears in ϕ_n for some h, R. Let us fix such an N. Furthermore, if $\vec{x}$ is a list of a finite number of nonces $\vec{x} \equiv N_1, ..., N_l$ such that they were all generated by either A or B, and they are all different from N, then we say condition $C'[\vec{x}, N]$ is satisfied. This can be written as a first order formula like

$$C'[N_1, ..., N_l, N] \equiv \bigwedge_{i=1}^{l} \Big(\mathsf{RandGen}(N_i) \wedge \exists QR\big(\{N_i, A\}^R_{eK_Q} \sqsubseteq \hat{\phi}\big) \vee \exists QhR\big(\{\pi_1\left(dec(h, dK_B)\right), N_i, B\}^R_{eK_Q} \sqsubseteq \hat{\phi}\big) \wedge N \neq N_i\Big)$$

We will carry out an inductive proof on the length of ϕ. As it turns out, in order to avoid loops in the proof, instead of (14), it is better to prove that

$$\exists N \exists \vec{x}\big(C[N] \wedge C'[\vec{x}, N] \wedge \hat{\phi}, \vec{x} \rhd N\big) \tag{14}$$

is inconsistent with the axioms and agent checks. On the symbolic trace, this means that

$$\exists N \exists \vec{x} \big(C[N] \wedge C'[\vec{x}, N] \wedge \phi_l, \vec{x} \rhd N \big)$$

is inconsistent with the axioms and agent checks.

For the induction, we fix an arbitrary N satisfying $C[N]$, and for this fixed N, we do an induction on the length of ϕ. Namely, we show that having fixed N, if for some $m < l$,

$$\exists \vec{x} \big(C'[\vec{x}, N] \wedge \phi_m, \vec{x} \rhd N \big)$$

is inconsistent with the axioms and agent checks, then

$$\exists \vec{x} \big(C'[\vec{x}, N] \wedge \phi_{m+1}, \vec{x} \rhd N \big)$$

is inconsistent with the axioms and agent checks. But showing this is equvalent with the following proposition:

Proposition 4.1 *In the above execution of NSL protocol, let N be such that $C[N]$ is satisfied, and let $m < l$. If for all $\vec{x}$ such that $C'[\vec{x}, N]$ holds, the axioms and agent checks imply (by FOL deduction rules) that $\phi_m, \vec{x} \not\rhd N$, then for all $\vec{x}$ such that $C'[\vec{x}, N]$ holds, the axioms and agent checks imply (by FOL deduction rules) that $\phi_{m+1}, \vec{x} \not\rhd N$ holds.*

Proof. Suppose the claim is not true. That is, let us assume that there is a finite set of nonces $\vec{x} \equiv N_1, ...N_l$ such that $C'[\vec{x}, N]$ and

$$\phi_{m+1}, N_1, ..., N_l \rhd N$$

is satisfied in some semantics. We will show show that this, together with the honest agent tests and the axioms, imply that for some nonces $x' \equiv N'_1, ...N'_{l'}$ with $C'[\vec{x}', N]$,

$$\phi_m, N'_1, ..., N'_{l'} \rhd N$$

satisfied. But, as according to our assumption, this was inconsistent, so $\phi_{m+1}, N_1, ..., N_l \rhd N$ must also have been inconsistent.

Let the last term in ϕ_{m+1} be t. t was sent either by A or B. That is, $\phi_{m+1} \equiv \phi_m, t$. So suppose

$$\phi_m, t, N_1, ..., N_l \rhd N$$

holds. By commutativity axiom, this means

$$\phi_m, N_1, ..., N_l, t \rhd N$$

holds.

1.) Assume that t was sent by A. Then, according to the role of A, for some N'_1, R_1, h_3, R_3, Q,

$$t \equiv \{N'_1, A\}^{R_1}_{eK_Q} \ \vee \ t \equiv \{\pi_1 (\pi_2 (dec(h_3, dK_A)))\}^{R_3}_{eK_Q} \ \vee \ t \equiv c_i\big(A, Q, N_1, \pi_1 (\pi_2 (dec(h_3, dK_A)))\big)$$

1.1.) If $t \equiv \{N'_1, A\}^{R_1}_{eK_Q}$, then, since A is following the initiator role honestly, A generated N'_1 earlier.

1.1.1.) If $N'_1 \equiv N$, then $C[N'_1]$ is satisfied (because $C[N]$ was assumed to be satisfied). But that means that N'_1 was sent to B. As A does only the initiator role and nothing else, each message by A, if it looks like $\{N'_1, A\}^{R_1}_{eK_Q}$, then N'_1 is a freshly generated nonce, and different each time. So if $N' \equiv N$, that means that the messages themselves must also be the same.

$$\{N'_1, A\}^{R_1}_{eK_Q} \equiv \{N, A\}^{R_1}_{eK_B},$$

that is,

$$Q \equiv B.$$

So we get

$$\phi_m, N_1, ..., N_l, \{N'_1, A\}^{R_1}_{eK_B} \rhd N.$$

As A was put out in ϕ_1, we have $\phi_m \rhd A$ by Example 3.3. Then, by an argument, similar to the one in Example 3.2, we get

$$\phi_m, N_1, ..., N_l, \{N_1', A\}^{R_1}_{eK_B} \rhd \langle N, A \rangle.$$

Clearly, for $x \equiv N_1, ..., N_l$, the predicate $x \preccurlyeq \phi_m$ holds, as are all names. Moreover, $dK_B \not\sqsubseteq \phi_m, N_1, ..., N_l, N_1', A$ and $\mathsf{fresh}(R_1; \phi_m, N_1, ..., N_l, N_1', A)$ also hold. So the secrecy axiom implies that

$$\phi_m, N_1, ..., N_l \rhd N,$$

Which is exactly what we had to show.

1.1.2.) Now let $N_1' \not\equiv N$. By the functions axiom, we have

$$\phi_m, N_1, ..., N_l, N_1', A, eK_Q, R_1 \rhd \{N_1', A\}^{R_1}_{eK_Q},$$

and this with

$$\phi_m, N_1, ..., N_l, \{N_1', A\}^{R_1}_{eK_Q} \rhd N$$

implies by transitivity axioms that

$$\phi_m, N_1, ..., N_l, N_1', A, eK_Q, R_1 \rhd N.$$

Since R_1 is fresh, by the fresh items are independent axiom,

$$\phi_m, N_1, ..., N_l, N_1', A, eK_Q \rhd N.$$

Since eK_Q is revealed explicitly at the beginning, we have $\phi_m, N_1, ..., N_l, N_1', A \rhd eK_Q$, and hence, by the transitivity axiom,

$$\phi_m, N_1, ..., N_l, N_1', A \rhd N.$$

Since A is revealed explicitly at the beginning, we have $\phi_m, N_1, ..., N_l, N_1' \rhd A$, and hence, by the transitivity axiom,

$$\phi_m, N_1, ..., N_l, N_1' \rhd N.$$

Since N_1' is not N, setting $\vec{x}' \equiv N_1, ..., N_l, N_1'$, $C'[\vec{x}', N]$ is satisfied, and this is exactly what we wanted.

1.2.) If $t \equiv \{\pi_1(\pi_2(\mathit{dec}(h_3, dK_A)))\}^{R_3}_{eK_Q}$, then we have by the role of A that $\pi_2(\pi_2(\mathit{dec}(h_3, dK_A))) = Q$, and that

$$\phi_m, N_1, ..., N_l, \{\pi_1(\pi_2(\mathit{dec}(h_3, dK_A)))\}^{R_3}_{eK_Q} \rhd N,$$

and hence by transitivity and function axioms,

$$\phi_m, N_1, ..., N_l, \mathit{dec}(h_3, dK_A), eK_Q, R_3 \rhd N.$$

Since R_3 is fresh, by the fresh items are independent axiom,

$$\phi_m, N_1, ..., N_l, \mathit{dec}(h_3, dK_A), eK_Q \rhd N,$$

and since eK_Q was revealed at the beginning,

$$\phi_m, N_1, ..., N_l, \mathit{dec}(h_3, dK_A) \rhd N.$$

By the non-malleability axiom (with $z = N$, $y = h_3$), we get that either

$$\exists x R(\{x\}^R_{eK_A} = h_3 \wedge \{x\}^R_{eK_A} \sqsubseteq \phi_m),$$

or

$$\phi_m, N_1, ..., N_l \rhd N.$$

1.2.1.) If $\phi_m, N_1, ..., N_l \rhd N$, then we are done.

1.2.2.) Suppose now $\exists x R(\{x\}^R_{eK_A} = h_3 \wedge \{x\}^R_{eK_A} \sqsubseteq \phi_m)$. Then $\{x\}^R_{eK_A}$ has been sent out. Since A never encrypts with its own key, it had to be B who sent it out (as the only two honest agents are A and B). Therefore, as B follows its responder role,

$$\{x\}^R_{eK_A} \equiv \{\pi_1\left(\mathit{dec}(h_2, dK_B)\right), N_2', B\}^R_{eK_A}$$

for some N_2'. Therefore,

$$\mathit{dec}(h_3, dK_A) = \langle \pi_1\left(\mathit{dec}(h_2, dK_B)\right), N_2', B\rangle.$$

But then

$$\pi_1\left(\pi_2\left(\mathit{dec}(h_3, dK_A)\right)\right) = N_2'$$

and

$$\pi_2\left(\pi_2\left(\mathit{dec}(h_3, dK_A)\right)\right) = B.$$

As we also had that $\pi_2\left(\pi_2\left(\mathit{dec}(h_3, dK_A)\right)\right) = Q$, so we get

$$Q = B$$

So the message $\{\pi_1\left(\pi_2\left(\mathit{dec}(h_3, dK_A)\right)\right)\}^{R_3}_{eK_Q} = \{N_2'\}^{R_3}_{eK_B}$. So we have by substitutability

$$\phi_m, N_1, ..., N_l, \{N_2'\}^{R_3}_{eK_B} \rhd N,$$

and by the security axiom, as R_3 is fresh and as $\vec{x} \preccurlyeq \phi_m$,

$$\phi_m, N_1, ..., N_l \rhd N,$$

which is what we wanted.

1.3.) If $t \equiv c_i\big(A, Q, N_1, \pi_1\left(\pi_2\left(\mathit{dec}(h_3, dK_A)\right)\right)\big)$, then by the c is not helpful axiom, $\phi_m, N_1, ..., N_l, t \rhd N$ follows.

2.) Assume now that t was sent by B. Then, for some h_2, N_2' and R_2,

$$t \equiv \{\pi_1\left(\mathit{dec}(h_2, dK_B)\right), N_2', B\}^{R_2}_{eK_{\pi_2\left(\mathit{dec}(h_2, dK_B)\right)}} \ \vee\ t \equiv c_r(\pi_2\left(\mathit{dec}(h_2, dK_B)\right), B, \pi_1\left(\mathit{dec}(h_2, dK_B)\right), N_2)$$

(i.e. $W(\pi_2\left(\mathit{dec}(h_2, dK_B)\right))$ holds.) Just as in the previous case, c does not help the adversary to get N, so we can assume $t \equiv \{\pi_1\left(\mathit{dec}(h_2, dK_B)\right), N_2', B\}^{R_2}_{eK_{\pi_2\left(\mathit{dec}(h_2, dK_B)\right)}}$

2.1.) If $N_2' \equiv N$, then, since $C[N]$ holds, $C[N_2']$ also holds, so as N_2' was generated by B, it was sent to A. And since B does not do anything other than executing responder sessions, and N is only generated in one session,

$$\{\pi_1\left(\mathit{dec}(h_2, dK_B)\right), N_2', B\}^{R_2}_{eK_{\pi_2\left(\mathit{dec}(h_2, dK_B)\right)}} \equiv \{\pi_1\left(\mathit{dec}(h_2, dK_B)\right), N_2', B\}^{R_2}_{eK_A},$$

and

$$\pi_2\left(\mathit{dec}(h_2, dK_B)\right) \equiv A$$

follows. But then $\phi_m, N_1, ..., N_l, t \rhd N$ means

$$\phi_m, N_1, ..., N_l, \{\pi_1\left(\mathit{dec}(h_2, dK_B)\right), N_2', B\}^{R_2}_{eK_A} \rhd N,$$

which, by the secrecy axiom implies

$$\phi_m, N_1, ..., N_l \rhd N,$$

which is what we wanted.

2.2.) If $N_2' \not\equiv N$, by the transitivity and the functions derivability axioms, we have

$$\phi_m, N_1, \ldots, N_l, \pi_1\left(\mathit{dec}(h_2, dK_B)\right), N_2', B, eK_{\pi_2(\mathit{dec}(h_2, dK_B))}, R_2 \rhd N.$$

By the independence axiom (and the commutativity), as N_2' and R_2 are fresh, we can drop them:

$$\phi_m, N_1, \ldots, N_l, \pi_1\left(\mathit{dec}(h_2, dK_B)\right), B, eK_{\pi_2(\mathit{dec}(h_2,dK_B))} \rhd N.$$

B and $eK_{\pi_2(\mathit{dec}(h_2,dK_B))}$ were published at the beginning, so we can drop them too:

$$\phi_m, N_1, \ldots, N_l, \pi_1\left(\mathit{dec}(h_2, dK_B)\right) \rhd N.$$

By the transitivity and the functions derivability axioms, we have

$$\phi_m, N_1, \ldots, N_l, \mathit{dec}(h_2, dK_B) \rhd N. \tag{15}$$

By the non-malleability axiom, we have either

$$\phi_m, N_1, \ldots, N_l \rhd N$$

or

$$\exists x R(h_2 = \{x\}^R_{eK_B} \wedge \{x\}^R_{eK_B} \sqsubseteq \phi_m).$$

In the first case, we have done. In the other case, since B does not encrypt messages by the key eK_B, h_2 is sent by A. Then, we have either

$$\{x\}^R_{eK_B} \equiv \{N_1', A\}^{R_1}_{eK_Q}$$

or

$$\{x\}^R_{eK_B} \equiv \{\pi_1\left(\pi_2\left(\mathit{dec}(h_3, dK_A)\right)\right)\}^{R_3}_{eK_Q}$$

for some Q, N_1', R_1, R_3, and h_3. This implies

$$Q \equiv B.$$

2.2.1.) If $\{x\}^R_{eK_B} \equiv \{N_1', A\}^{R_1}_{eK_B}$, then

$$N_1' \equiv \pi_1\left(\mathit{dec}(h_2, dK_B)\right)$$

and

$$t \equiv \{N_1', N_2', B\}^R_{eK_A}.$$

By the secrecy axiom,

$$\phi_m, N_1, ..., N_l, \{N_1', N_2', B\}^R_{eK_A} \rhd N$$

implies

$$\phi_m, N_1, ..., N_l \rhd N.$$

2.2.2.) If $\{x\}^R_{eK_B} \equiv \{\pi_1\left(\pi_2\left(\mathit{dec}(h_3, dK_A)\right)\right)\}^{R_3}_{eK_B}$, then

$$\mathit{dec}(h_2, dK_B) = \pi_1\left(\pi_2\left(\mathit{dec}(h_3, dK_A)\right)\right),$$

and by Equation 15, we have

$$\phi_m, N_1, \ldots, N_l, \pi_1\left(\pi_2\left(\mathit{dec}(h_3, dK_A)\right)\right) \rhd N,$$

and hence

$$\phi_m, N_1, \ldots, N_l, \mathit{dec}(h_3, dK_A) \rhd N.$$

This, with the non-malleability axiom implies that either

$$\exists x' R'(\{x'\}^{R'}_{eK_A} = h_3 \wedge \{x'\}^{R'}_{eK_A} \sqsubseteq \phi_m),$$

or

$$\phi_m, N_1, ..., N_l \rhd N.$$

In the latter, we are done. If $\exists x' R'(\{x'\}^{R'}_{eK_A} = h_3 \wedge \{x'\}^{R'}_{eK_A} \sqsubseteq \phi_m)$, then, since only B encrypts with eK_A, and since it follows its responder role, we have

$$\{x'\}^{R'}_{eK_A} \equiv \{\pi_1\left(dec(h'_2, dK_B)\right), N''_2, B\}^{R'_2}_{eK_{\pi_2\left(dec(h'_2, dK_B)\right)}},$$

and

$$\pi_2\left(dec(h'_2, dK_B)\right) \equiv A.$$

Therefore, as $\{x'\}^{R'}_{eK_A} = h_3$, we have

$$\pi_1\left(\pi_2\left(dec(h_3, dK_A)\right)\right) \equiv N'_2,$$

meaning

$$x \equiv N'_2.$$

But, we also had that $x = dec(h_2, dK_B)$, and and the beginning of 2.), the assumption was $W(\pi_2\left(dec(h_2, dK_B)\right))$. Putting these three together, we get

$$W(\pi_2\left(N'_2\right)),$$

which contradicts our necessary axiom for the NSL, $\neg W(\pi_2\left(N'_2\right))$.

This concludes our proof.

□

At step 0, N, N_1... are still fresh, so by the no telepathy axiom combined with the independence of fresh items,

$$\phi_{m_0}, N'_1, ..., N'_{l'} \rhd N$$

holds by the freshness axiom. Then the induction step in **a.)** proves that this property always holds. In particular, we have the following theorem.

Theorem 4.2 (Secrecy) *Consider a symbolic execution of the NSL protocol, with two honest (and possible other dishonest) participants A, B such that they follow the initiator and responder roles correspondingly, and they are only executing these roles in each of their bounded number of sessions and are forbidden to initiate communications with themselves. Further, we use the convention $\langle x, y, z\rangle \equiv \langle x, \langle y, z\rangle\rangle$. Our axioms together with the agent checks and $\neg W(\pi_2\left(N\right))$ imply that for any nonce N that was either generated by A and sent to B or vice versa, for all n,*

$$\phi_n \not\rhd N$$

holds. That is, the nonces that were generated by A or B and intended to be sent between each other, remain secret. In other words, the formula

$$\exists N\big(C[N] \wedge \hat{\phi} \rhd N\big)$$

and the axioms and the agent checks and $\neg W(\pi_2\left(N\right))$ are inconsistent on any symbolic trace. In other words, secrecy of nonces satisfying $C[N]$ is not broken.

b) Agreement and Authentication

We now prove agreement from the responder's viewpoint. That is, we will show that

$$\begin{array}{r} Resp^B_{NSL}[B, i', N_2, h_2, h_4, R_2] \ \text{ AND} \\ \pi_2\left(dec(h_2, dK_B)\right) = A \end{array} \implies \begin{array}{l} \text{EXIST } \ i, N_1, h_1, h_3, R_1, R_3 \ \text{ SUCH THAT} \\ Init^A_{NSL}[A, i, B, N_1, h_1, h_3, R_1, R_3] \ \text{ AND} \\ dec(h_2, dK_B) = \langle N_1, A\rangle \ \text{ AND} \\ dec(h_3, dK_A) = \langle N_1, N_2, B\rangle \ \text{ AND} \\ dec(h_4, dK_B) = N_2 \end{array}$$

Where by the implication sign we mean that the agent checks, and axioms imply this. We can also write this within our syntax:

$$c_r(\pi_2\left(\mathit{dec}(h_2, dK_B)\right), B, \pi_1\left(\mathit{dec}(h_2, dK_B)\right), N_2) \sqsubseteq \hat{\phi} \ \wedge \ A = \pi_2\left(\mathit{dec}(h_2, dK_B)\right) \longrightarrow$$
$$\exists N_1 h_3 \big(c_i(A, B, N_1, \pi_1\left(\pi_2\left(\mathit{dec}(h_3, dK_A)\right)\right)) \sqsubseteq \hat{\phi} \ \wedge \ N_2 = \pi_1\left(\pi_2\left(\mathit{dec}(h_3, dK_A)\right)\right) \ \wedge \ N_1 = \pi_1\left(\mathit{dec}(h_2, dK_B)\right)\big)$$

What we have to prove is that the negation of this is inconsistent with the axioms and agent checks. But for that it is sufficient to show that the agent checks and axioms and the premise of the formula imply the conclusion of this formula.

Proof of b.)
$c_r(\pi_2\left(\mathit{dec}(h_2, dK_B)\right), B, \pi_1\left(\mathit{dec}(h_2, dK_B)\right), N_2) \sqsubseteq \hat{\phi}$ means (by the role of B) that $Resp^B_{NSL}[B, i', N_2, h_2, h_4, R_2]$ was carried out. By $Resp^B_{NSL}[B, i', N_2, h_2, h_4, R_2]$ and $\pi_2\left(\mathit{dec}(h_2, dK_B)\right) = A$, we have

$$\{\pi_1\left(\mathit{dec}(h_2, dK_B)\right), N_2, B\}^{R_2}_{eK_A} \sqsubseteq \phi_m$$

(for m step, when it is sent), and

$$\mathit{dec}(h_4, dK_B) = N_2.$$

Then, by the self derivability axiom, we have

$$\phi_m, \mathit{dec}(h_4, dK_B) \rhd N_2.$$

By the non-malleability axiom, we have either

$$\phi_m \rhd N_2$$

or

$$\exists x R(h_4 = \{x\}^R_{eK_B} \wedge \{x\}^R_{eK_B} \sqsubseteq \phi_m).$$

The first is impossible by the previous Theorem. In the second case, by decrypting h_4, we have

$$x = N_2.$$

Since B does not send a message encrypted by eK_B, $\{N_2\}^R_{eK_B}$ is sent by A in some session i.

1.) Case $\{x\}^R_{eK_B} \equiv \{N_1, A\}^{R_1}_{eK_Q}$ for some N_1 and R_1: In this case we get

$$x \equiv \langle N_1, A\rangle,$$

and so $N_2 = \langle N_1, A\rangle$. This implies by the self-derivability, that for any m',

$$\phi_{m'}, N_1, A \rhd N_2,$$

which, as A is public, implies

$$\phi_{m'}, N_1 \rhd N_2.$$

This is true for all m', so it is also true for the one when N_1 or N_2 is fresh. But, that contradicts either the no telepathy, or the freshness axiom is violated. So the assumption in 1.) is not possible.

2.) Case $\{x\}^R_{eK_B} \equiv \{\pi_1\left(\pi_2\left(\mathit{dec}(h_3, dK_A)\right)\right)\}^R_{eK_B}$: Since A follows the initiator role, we have

$$\pi_1\left(\mathit{dec}(h_3, dK_A)\right) = N_1 \ \text{ AND } \ \pi_2\left(\pi_2\left(\mathit{dec}(h_3, dK_A)\right)\right) = B \tag{16}$$

where N_1 is honestly generated by A. That is, session i of A is with agent B. Putting these together with $x \equiv \pi_1\left(\pi_2\left(\mathit{dec}(h_3, dK_A)\right)\right)$ and $x = N_2$, we have

$$\pi_1\left(\pi_2\left(\mathit{dec}(h_3, dK_A)\right)\right) = N_2 \tag{17}$$

and

$$\mathit{dec}(h_3, dK_A) = \langle N_1, N_2, A\rangle.$$

So we have $Init^A_{NSL}[A, i, B, N_1, h_1, h_3, R_1, R_3]$.

The only thing left to be proven is

$$dec(h_2, dK_B) = \langle N_1, A\rangle.$$

By the self derivability axiom, we have for any m'',

$$\phi_{m''}, \pi_1\left(dec(h_3, dK_A)\right) \rhd N_1,$$

and by the functions derivability and transitivity axioms, we have

$$\phi_{m''}, dec(h_3, dK_A) \rhd N_1.$$

By the non-mallability axiom, we have

$$\exists x' R'(h_3 = \{x'\}^{R'}_{dK_A} \wedge \{x'\}^{R'}_{dK_A} \sqsubseteq \phi_{m''})$$

or

$$\phi_{m''} \rhd N_1,$$

but this latter is not possible by the previous theorem as N_1 was generated by A in session i in which the intended party is B as we have shown. Then, we have

$$dec(h_3, dK_B) = x'. \tag{18}$$

Let tr' be the shortest trace that satisfies this and is a prefix of the trace tr we are considering.

Since A does not encryptes a message by eK_A, $\{x'\}^{R'}_{eK_A}$ is sent by B. Then we have

$$\{x'\}^{R'}_{eK_A} = \{\pi_1\left(dec(h'_2, dK_B)\right), N'_2, B\}^{R'_2}_{eK_A} \tag{19}$$

for some h'_2, N'_2, and R'_2. From 16, 18 and 19, we get

$$\pi_1\left(dec(h'_2, dK_B)\right) = \pi_1\left(dec(h_3, dK_A)\right) = N_1.$$

From 17, 18 and 19, we get

$$N'_2 = \pi_1\left(\pi_2\left(dec(h_3, dK_A)\right)\right) = N_2.$$

Since B, according to its role, always generates a new nonce before sending its message, it does not use N_2 in more than one session. And we have already concluded that in the session where N_2 is sent, the message is

$$\{\pi_1\left(dec(h_2, dK_B)\right), N_2, B\}^{R_2}_{eK_A}.$$

Therefore,

$$\{\pi_1\left(dec(h'_2, dK_B)\right), N_2, B\}^{R'_2}_{eK_A} \equiv \{\pi_1\left(dec(h_2, dK_B)\right), N_2, B\}^{R_2}_{eK_A},$$

and so

$$h'_2 \equiv h_2,$$

which means

$$\pi_1\left(dec(h_2, eK_A)\right) = N_1.$$

Putting all these together, we have

EXIST $i, N_1, h_1, h_3, R_1, R_3$ SUCH THAT
$Init^A_{NSL}[A, i, B, N_1, h_1, h_3, R_1, R_3]$ AND
$dec(h_2, dK_B) = \langle N_1, A\rangle$ AND
$dec(h_3, dK_A) = \langle N_1, N_2, B\rangle$ AND
$dec(h_4, dK_B) = N_2$

which immediately implies

$$\exists N_1 h_3\big(c_i(A, B, N_1, \pi_1\left(\pi_2\left(dec(h_3, dK_A)\right)\right)) \sqsubseteq \hat{\phi} \wedge N_2 = \pi_1\left(\pi_2\left(dec(h_3, dK_A)\right)\right) \wedge N_1 = \pi_1\left(dec(h_2, dK_B)\right)\big)$$

□

We have shown:

Theorem 4.3 (Agreement and Authentication) *Consider a symbolic execution of the NSL protocol, with two honest (and possible other dishonest) participants A, B such that they follow the initiator and responder roles correspondingly, and they are only executing these roles in each of their bounded number of sessions and are forbidden to initiate communications with themselves. Further, we use the convention $\langle x, y, z\rangle \equiv \langle x, \langle y, z\rangle\rangle$. Our axioms and agent checks and $\neg W(\pi_2(N))$ are inconsistent with the negation of the formula*

$$c_r(\pi_2(\mathit{dec}(h_2, dK_B)), B, \pi_1(\mathit{dec}(h_2, dK_B)), N_2) \sqsubseteq \hat{\phi} \wedge A = \pi_2(\mathit{dec}(h_2, dK_B)) \longrightarrow$$
$$\exists N_1 h_3 \big(c_i(A, B, N_1, \pi_1(\pi_2(\mathit{dec}(h_3, dK_A)))) \sqsubseteq \hat{\phi} \wedge N_2 = \pi_1(\pi_2(\mathit{dec}(h_3, dK_A))) \wedge N_1 = \pi_1(\mathit{dec}(h_2, dK_B))\big).$$

Discussion
Without the assumption $\neg W(\pi_2(N))$, there is an attack discussed in Bana et al. For a convention different from $\langle x, y, z\rangle \equiv \langle x, \langle y, z\rangle\rangle$, the proof has to be redone. One way would be to have a separate triplet function symbol, and list the properties that it has to satisfy for not having an attack. For example, it has been shown that if the triple is associative, then there is an attack. Finally, the proof can also be done for the situation when the agents are allowed to run both roles and are allowed to have sessions with themselves, but it is a much longer proof, and needs a much more complicated induction hypothesis in a.).