Symbolic Verification of the Amended Needham-Schroeder Shared-Key Protocol

February 8, 2013

1 Symbolic Execution of Amended Needham-Schroeder Shared-Key Protocol in Our Framework

1. $A \to B : A$
2. $B \to A : \{A, N_1\}_{K_{BT}}$
3. $A \to T : \langle A, B, N_2, \{A, N_1\}_{K_{BT}} \rangle$
4. $T \to A : \{N_2, B, K, \{K, N_1, A\}_{K_{BT}}\}_{K_{AT}}$
5. $A \to B : \{K, N_1, A\}_{K_{BT}}$
6. $B \to A : \{N_3\}_K$
7. $A \to B : \{N_3 - 1\}_K$

1.1 Roles

The initiator, communicating with intended party Q, trusted server T, does the following sequence of steps in session i which we will informally denote by $Init^A_{sNS}[i, Q, T, N_2, h_1, h_3, h_5, h_7, R_5]$:

- Receives some h_1 from the adversary that triggers the start of the session with intended party Q
- A sends A
- A receives h_3
- A generates nonce N_2.
- A sends $\langle A, B, N_2, h_3 \rangle$
- A receives h_5, and checks
  - $\pi_1 (sdec(h_5, K_{AT})) = N_2$
  - $\pi_1 (\pi_2 (sdec(h_5, K_{AT}))) = Q$
- A sends $\pi_2 (\pi_2 (\pi_2 (sdec(h_5, K_{AT}))))$

- A sends $c_i\big(A, Q, T, N_2, \pi_1\left(\pi_2\left(\pi_2\left(\mathit{sdec}(h_5, K_{AT})\right)\right)\right)\big)$
- A receives h_7
- A sends $\{\!|\mathit{sdec}(h_7, \pi_1\left(\pi_2\left(\pi_2\left(\mathit{sdec}(h_5, K_{AT})\right)\right)\right) - 1|\!\}^{R_5}_{\pi_1(\pi_2(\pi_2(\mathit{sdec}(h_5, K_{AT}))))}$
- A sends $d_i\big(A, Q, T, N_2, \pi_1\left(\pi_2\left(\pi_2\left(\mathit{sdec}(h_5, K_{AT})\right)\right)\right), \mathit{sdec}(h_7, \pi_1\left(\pi_2\left(\pi_2\left(\mathit{sdec}(h_5, K_{AT})\right)\right)\right)\big)$

The responder does the following sequence of steps in session i' which we will informally denote by $\mathit{Resp}^B_{sNS}[i', h_2, T, N_1, N_3, h_6, h_8, R_1, R_4]$:

- B receives some h_2 from the adversary and checks
  - $W(h_2)$ (Checks that it is a name of someone)
- B generates nonce N_1.
- B sends $\{\!|h_2, N_1|\!\}^{R_1}_{K_{BT}}$
- B receives some h_6 from the adversary and checks
  - $\pi_1\left(\pi_2\left(\mathit{sdec}(h_6, K_{BT})\right)\right) = N_1$
  - $\pi_2\left(\pi_2\left(\mathit{sdec}(h_6, K_{BT})\right)\right) = h_2$
- B sends $c_r\big(h_2, B, T, N_1, \pi_1\left(\mathit{sdec}(h_6, K_{BT})\right)\big)$
- B generates nonce N_3.
- B sends $\{\!|N_3|\!\}^{R_4}_{\pi_1(\mathit{sdec}(h_6, K_{BT}))}$
- B receives h_8, and checks
  - $\mathit{sdec}(h_8, \pi_1\left(\mathit{sdec}(h_6, K_{BT})\right)) + 1 = N_3$
- B sends $d_r\big(h_2, B, T, N_1, \pi_1\left(\mathit{sdec}(h_6, K_{BT})\right), N_3\big)$

The trusted server does the following sequence of steps in session i'' which we will informally denote by $\mathit{Trust}^T_{sNS}[i'', h_2, T, N_1, N_3, h_6, h_8, R_1, R_4]$:

- T receives some h_4 from the adversary and checks
  - $W(\pi_1\left(h_4\right))$ (Checks that it is a name of someone)
  - $W(\pi_1\left(\pi_2\left(h_4\right)\right))$ (Checks that it is a name of someone)
  - $\pi_1\left(\mathit{sdec}(\pi_2\left(\pi_2\left(\pi_2\left(h_4\right)\right)\right), K_{\pi_1(\pi_2(h_4))T})\right) = \pi_1\left(h_4\right)$
- T generates session key K.
- T sends $\Big\{\!\Big|\pi_1\left(\pi_2\left(\pi_2\left(h_4\right)\right)\right),\ \pi_1\left(\pi_2\left(h_4\right)\right),\ K,\ \Big\{\!\Big|K,\ \pi_2\left(\mathit{dec}\big(\pi_2\left(\pi_2\left(\pi_2\left(h_4\right)\right)\right), K_{\pi_1(\pi_2(h_4))T}\big)\right),\ \pi_1\left(h_4\right)\Big|\!\Big\}^{R_2}_{K_{\pi_1(\pi_2(h_4))T}}\Big|\!\Big\}^{R_3}_{K_{\pi_1(h_4)T}}$
- T sends $c_t\big(\pi_1\left(h_4\right),\ \pi_1\left(\pi_2\left(h_4\right)\right),\ T,\ \pi_2\left(\mathit{dec}\big(\pi_2\left(\pi_2\left(\pi_2\left(h_4\right)\right)\right), K_{\pi_1(\pi_2(h_4))T}\big)\right),\ \pi_1\left(\pi_2\left(\pi_2\left(h_4\right)\right)\right),\ K\big)$

1.2 Computationally Sound Axioms Used

Axioms for derivability $\rhd$:

- $x = x$, and the substitutability (congruence) property of equal terms holds for $=$ and $\rhd$.
- 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: $\hat{\phi}, \vec{x} \rhd f(\vec{x})$
  This axiom is sound as long as functions are interpreted as PT computable algorithms.
- No telepathy: $\mathsf{fresh}(x; \hat{\phi}) \longrightarrow \hat{\phi} \not\rhd x$
  This axiom is sound as long as $\mathsf{RandGen}()$ items are generated so that they can only be guessed with negligible probability.
- Fresh items do not help to compute: $\mathsf{fresh}(x; \hat{\phi}, \vec{x}, y) \wedge \vec{x}, y \preccurlyeq \hat{\phi} \wedge \hat{\phi}, \vec{x}, x \rhd y \longrightarrow \hat{\phi}, \vec{x} \rhd y$

Axioms for derivability with symmetric IND-CCA2 oracles:

- Equal terms are substitutable on the right hand side of $\rhd^{\mathrm{sic2}}$.
- More oracles help more: $\hat{\phi}, \vec{x} \rhd x \longrightarrow \hat{\phi}, \vec{x} \rhd^{\mathrm{sic2}} x$.
- Increasing capabilities: $\hat{\phi}, \vec{x} \rhd^{\mathrm{sic2}} y \longrightarrow \hat{\phi}, \vec{x}, x \rhd^{\mathrm{sic2}} y$
- Commutativity: If $\vec{x}'$ is a permutation of $\vec{x}$, then $\hat{\phi}, \vec{x} \rhd^{\mathrm{sic2}} y \longrightarrow \hat{\phi}, \vec{x}' \rhd^{\mathrm{sic2}} y$
- Transitivity: $\hat{\phi}, \vec{x} \rhd^{\mathrm{sic2}} \vec{y} \wedge \hat{\phi}, \vec{x}, \vec{y} \rhd^{\mathrm{sic2}} \vec{z} \longrightarrow \hat{\phi}, \vec{x} \rhd^{\mathrm{sic2}} \vec{z}$
- Decryptions of adversarial ciphers do not help: If $\mathcal{O}$ is either IND or KDM CCA2, either symmetric or asymmetric, then

$$\mathsf{RandGen}(K) \wedge \hat{\phi}, \vec{x} \rhd^{\mathrm{sic2}} y \wedge \hat{\phi}, \vec{x}, \mathit{sdec}(y, dK) \rhd^{\mathrm{sic2}} z \wedge \forall x R(y = \{\!|x|\!\}^R_{eK} \rightarrow \{\!|x|\!\}^R_{eK} \not\sqsubseteq \hat{\phi}, \vec{x}) \longrightarrow \hat{\phi}, \vec{x} \rhd^{\mathrm{sic2}} z$$

- No telepathy: $\mathsf{fresh}(x; \hat{\phi}) \longrightarrow \hat{\phi} \not\rhd^{\mathcal{O}} x$
- Fresh items do not help to compute: $\mathsf{fresh}(x; \hat{\phi}, \vec{x}, y) \wedge \vec{x}, y \preccurlyeq \hat{\phi} \wedge \hat{\phi}, \vec{x}, x \rhd^{\mathrm{sic2}} y \longrightarrow \hat{\phi}, \vec{x} \rhd^{\mathrm{sic2}} y$

We assume that the encryption is both CCA2 and INT-CTXT secure, and use the combined corruption predicate:

$$\hat{\phi}, \vec{x} \blacktriangleright K \equiv \hat{\phi}, \vec{x} \blacktriangleright^{\mathrm{sic2}} K \wedge \hat{\phi}, \vec{x} \blacktriangleright^{\mathrm{ic}} K$$

For this, the following axioms hold:

- Equal terms are substitutable on the rhs of $\blacktriangleright$.
- Derivability implies corruption: $\hat{\phi}, \vec{x} \rhd^{\mathrm{sic2}} K \longrightarrow \hat{\phi}, \vec{x} \blacktriangleright K$
- Increasing capabilities: $\hat{\phi}, \vec{x} \blacktriangleright K \longrightarrow \hat{\phi}, \vec{x}, x \blacktriangleright K$
- 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: $\hat{\phi}, \vec{x} \rhd^{\mathrm{sic2}} \vec{y} \wedge \hat{\phi}, \vec{x}, \vec{y} \blacktriangleright K \longrightarrow \hat{\phi}, \vec{x} \blacktriangleright K$

- Decryptions of adversarial ciphers do not help:

$$\mathsf{RandGen}(K) \ \wedge \ \mathsf{RandGen}(K') \ \wedge \ \hat{\phi}, \vec{x} \rhd^{\mathrm{sic2}} y \ \wedge \ \hat{\phi}, \vec{x}, \mathit{sdec}(y, dK) \blacktriangleright K' \ \wedge \ \forall x R(y = \{\!|x|\!\}^R_{eK} \rightarrow \{\!|x|\!\}^R_{eK} \not\sqsubseteq \hat{\phi}, \vec{x}) \\ \longrightarrow \ \hat{\phi}, \vec{x} \blacktriangleright K'$$

- Uncorrupted keys securely encrypt:

$$\mathsf{RandGen}(K) \ \wedge \ \mathsf{fresh}(R; \hat{\phi}, \vec{x}, x, y, K) \ \wedge \ \vec{x}, x, y \preccurlyeq \hat{\phi} \ \wedge \ \hat{\phi}, \vec{x}, \{\!|x|\!\}^R_{eK} \rhd^{\mathrm{sic2}} y \ \longrightarrow \ \hat{\phi}, \vec{x}, x \blacktriangleright K \ \vee \ \hat{\phi}, \vec{x} \rhd^{\mathrm{sic2}} y$$

- Uncorrupted key's encryption cannot be faked:

$$\mathsf{RandGen}(K) \ \wedge \ \hat{\phi}, \vec{x} \rhd y \ \wedge \ \mathit{dec}(y, dK) \neq \bot \ \wedge \ \forall x R(y = \{x\}^R_{eK} \rightarrow \{x\}^R_{eK} \not\sqsubseteq \hat{\phi}, \vec{x}) \ \longrightarrow \ \hat{\phi}, \vec{x} \blacktriangleright^{\mathrm{ic}} K$$

- Encryptions with uncorrupted keys do not corrupt

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

- Fresh keys are not corrupted: If the encryption is IND-CCA2 secure and INT-CTXT secure, then $\mathsf{keyfresh}(K; \hat{\phi}) \ \longrightarrow \ \hat{\phi} \not\blacktriangleright K$
- Fresh items do not corrupt: $\mathsf{fresh}(x; \hat{\phi}, \vec{x}, y) \ \wedge \ \vec{x}, y \preccurlyeq \hat{\phi} \ \wedge \ \hat{\phi}, \vec{x}, x \blacktriangleright y \ \longrightarrow \ \hat{\phi}, \vec{x} \blacktriangleright y$

Bla

- Special to c_i, c_r, c_t, d_i, d_r, d_t (Let c be either of them):
  - c does not help the adversary: $\mathsf{RandGen}(N) \wedge \hat{\phi}, \vec{x}, c(\vec{y}) \rhd N \rightarrow \hat{\phi}, \vec{x} \rhd N$
  - c cannot be forged and cannot be subparts of terms:

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

  - c cannot be equal with anything else: If the outermost function symbol of a term T something different from c, then $c(\vec{y}) \neq T$.
- Equations for the function symbols
  - Equations for encryption/decryption:
    - Decryption of an encryption results the plaintext: $\mathit{sdec}(\{\!|x|\!\}^R_K, K) = x$
  - Equations for pairing/projections:
    - First projection: $\pi_1(\langle x, y \rangle) = x$
    - Second projection: $\pi_2(\langle x, y \rangle) = y$
  - Equations for $+1$ and -1 (We write $+1(x)$ as $x + 1$ and $-1(x)$ as $x - 1$):
    - $(x - 1) + 1 = x$
    - $(x + 1) - 1 = x$
    - $x - 1 \neq x$
  - Equations for long-term shared key:
    - Shared key of Q and Q' is the same as that of Q' and Q: $K_{Q'Q} = K_{QQ'}$

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,

$$\mathsf{RandGen}(N) \to \pi_1(N) \neq N$$

Without this, there is an attack.

We further assume that secret keys of agents other than A, B and T are accessible to the adversary. Names are all public. There is only 1 trusted server.

Agreement Proof

a)
We show first that if A, B and T follow their roles honestly, then

$$\begin{aligned}
&c_i\big(A, Q, T, N_2, \pi_1(\pi_2(\pi_2(\mathit{sdec}(h_5, K_{AT}))))\big) \sqsubseteq \hat{\phi} \longrightarrow \\
&\quad \exists K h_4 R_2 \big(c_t\big(\pi_1(h_4),\ \pi_1(\pi_2(h_4)),\ T,\ \pi_2\big(\mathit{dec}\big(\pi_2(\pi_2(\pi_2(h_4))), K_{\pi_1(\pi_2(h_4))T}\big)\big),\ \pi_1(\pi_2(\pi_2(h_4))),\ K\big) \sqsubseteq \hat{\phi} \\
&\wedge\ K = \pi_1(\pi_2(\pi_2(\mathit{sdec}(h_5, K_{AT})))) \ \wedge\ N_2 = \pi_1(\pi_2(\pi_2(h_4))) \ \wedge\ A = \pi_1(h_4) \ \wedge\ Q = \pi_1(\pi_2(h_4)) \\
&\wedge\ \pi_2(\pi_2(\pi_2(\mathit{sdec}(h_5, K_{AT})))) = \big\{\big|K,\ \pi_2\big(\mathit{dec}\big(\pi_2(\pi_2(\pi_2(h_4))), K_{\pi_1(\pi_2(h_4))T}\big)\big),\ \pi_1(h_4)\big|\big\}^{R_2}_{K_{\pi_1(\pi_2(h_4))T}}\big)
\end{aligned}$$

That is, if the initiator A is running a session with Q and trusted party T, and it received what was meant to be the shared key (in step 4. of the protocol above), then he indeed received a real shared key K generated by the trusted party for A and Q. And, moreover, the trusted party and A agree on the nonce N_2 generated by A as well.

Proof of a)
$c_i\big(A, Q, T, N_2, \pi_1(\pi_2(\pi_2(\mathit{sdec}(h_5, K_{AT}))))\big) \sqsubseteq \phi_m$ means by the initiator role that A received an h_5 with $\pi_1(\mathit{sdec}(h_5, K_{AT})) = N_2$ and $\pi_1(\pi_2(\mathit{sdec}(h_5, K_{AT}))) = Q$, and $\hat{\phi}_n \triangleright h_5$. for some $n < m$. Since the long-term key is never sent out, it is uncorrupted, and by the uncorrupted key's encryption cannot be faked axiom, as $\mathit{sdec}(h_5, K_{AT}) \neq \bot$, there is a z and R with $\{\!|z|\!\}^R_{K_{AT}} \sqsubseteq \phi_n$ and $h_5 = \{\!|z|\!\}^R_{K_{AT}}$. The only messages that are sent out encrypted with K_{AT} are among those sent by T, and they look like

$$\{\!|z|\!\}^R_{K_{AT}} \equiv \big\{\big|K,\ \pi_2\big(\mathit{dec}\big(\pi_2(\pi_2(\pi_2(h_4))), K_{\pi_1(\pi_2(h_4))T}\big)\big),\ \pi_1(h_4)\big|\big\}^{R_2}_{K_{\pi_1(\pi_2(h_4))T}}$$

or

$$\{\!|z|\!\}^R_{K_{AT}} \equiv \Big\{\Big|\pi_1(\pi_2(\pi_2(h_4))),\ \pi_1(\pi_2(h_4)),\ K,\ \big\{\big|K,\ \pi_2\big(\mathit{dec}\big(\pi_2(\pi_2(\pi_2(h_4))), K_{\pi_1(\pi_2(h_4))T}\big)\big),\ \pi_1(h_4)\big|\big\}^{R_2}_{K_{\pi_1(\pi_2(h_4))T}}\Big|\Big\}^{R_3}_{K_{\pi_1(h_4)T}}$$

1.) Suppose first that $\{\!|z|\!\}^R_{K_{AT}} \equiv \big\{\big|K,\ \pi_2\big(\mathit{dec}\big(\pi_2(\pi_2(\pi_2(h_4))), K_{\pi_1(\pi_2(h_4))T}\big)\big),\ \pi_1(h_4)\big|\big\}^{R_2}_{K_{\pi_1(\pi_2(h_4))T}}$. In this case, $\pi_1(\mathit{sdec}(h_5, K_{AT})) = K$. But we had earlier that $\pi_1(\mathit{sdec}(h_5, K_{AT})) = N_2$. So $K = N_2$. However, N_2 was generated by B and K was generated by T. Since according to their roles, they always generate new items, they cannot be the same.

2.)
If $\{\!|z|\!\}^R_{K_{AT}} \equiv \Big\{\Big|\pi_1(\pi_2(\pi_2(h_4))),\ \pi_1(\pi_2(h_4)),\ K,\ \big\{\big|K,\ \pi_2\big(\mathit{dec}\big(\pi_2(\pi_2(\pi_2(h_4))), K_{\pi_1(\pi_2(h_4))T}\big)\big),\ \pi_1(h_4)\big|\big\}^{R_2}_{K_{\pi_1(\pi_2(h_4))T}}\Big|\Big\}^{R_3}_{K_{\pi_1(h_4)T}}$,
then

- $A = \pi_1(h_4)$, and
- $N_2 = \pi_1(\mathit{sdec}(h_5, K_{AT})) = \pi_1(\pi_2(\pi_2(h_4)))$, and
- $Q = \pi_1(\pi_2(\mathit{sdec}(h_5, K_{AT}))) = \pi_1(\pi_2(h_4))$, and
- $K = \pi_1(\pi_2(\pi_2(\mathit{sdec}(h_5, K_{AT}))))$, and

- $\pi_2\left(\pi_2\left(\pi_2\left(\mathit{sdec}(h_5, K_{AT})\right)\right)\right) = \left\{\!\middle|K,\ \ \pi_2\left(\mathit{dec}\left(\pi_2\left(\pi_2\left(\pi_2\left(h_4\right)\right)\right), K_{\pi_1(\pi_2(h_4))T}\right)\right),\ \ \pi_1\left(h_4\right)\middle|\!\right\}^{R_2}_{K_{\pi_1(\pi_2(h_4))T}}$

which is exactly what we had to show.

□

b)
Next we show that if A, B and T follow their respective roles, then

$$c_r\big(h_2, B, T, N_1, \pi_1\left(\mathit{sdec}(h_6, K_{BT})\right)\big) \sqsubseteq \hat{\phi} \longrightarrow$$
$$\exists K h_4 \big(c_t\big(\pi_1\left(h_4\right),\ \ \pi_1\left(\pi_2\left(h_4\right)\right),\ \ T,\ \ \pi_2\left(\mathit{dec}\left(\pi_2\left(\pi_2\left(\pi_2\left(h_4\right)\right)\right), K_{\pi_1(\pi_2(h_4))T}\right)\right),\ \ \pi_1\left(\pi_2\left(\pi_2\left(h_4\right)\right)\right),\ \ K\big) \sqsubseteq \hat{\phi}$$
$$\wedge\ B = \pi_1\left(\pi_2\left(h_4\right)\right)\ \wedge\ N_1 = \pi_2\left(\mathit{dec}\left(\pi_2\left(\pi_2\left(\pi_2\left(h_4\right)\right)\right), K_{\pi_1(\pi_2(h_4))T}\right)\right)\ \wedge\ h_2 = \pi_1\left(h_4\right)\ \wedge\ K = \pi_1\left(\mathit{sdec}(h_6, K_{BT})\right)\big)$$

Proof of b)
$c_r\big(h_2, B, T, N_1, \pi_1\left(\mathit{sdec}(h_6, K_{BT})\right)\big) \sqsubseteq \phi_m$ means by the role of B, that B received an h_6 for which $\pi_1\left(\pi_2\left(\mathit{sdec}(h_6, K_{BT})\right)\right) = N_1$ and $\pi_2\left(\pi_2\left(\mathit{sdec}(h_6, K_{BT})\right)\right) = h_2$, and $\phi_m \rhd h$. Since the long-term key is never sent out, it is uncorrupted, and by the uncorrupted key's encryption cannot be faked axiom, as $\mathit{sdec}(h_6, K_{BT}) \neq \bot$, there is a z and R with $\{\!|z|\!\}^R_{K_{AT}} \sqsubseteq \phi_n$ and $h_6 = \{\!|z|\!\}^R_{K_{BT}}$. The only messages that are sent out encrypted with K_{BT} are among those sent by B or T.

1.) Suppose first that B sent it. Then it has the form

$$\{\!|z|\!\}^R_{K_{BT}} \equiv \{\!|h'_2, N'_1|\!\}^{R'_1}_{K_{BT}}.$$

That is, $\pi_2\left(\mathit{sdec}(h_6, K_{BT})\right) = N'_1$. But we had $\pi_1\left(\pi_2\left(\mathit{sdec}(h_6, K_{BT})\right)\right) = N_1$ and $\pi_2\left(\pi_2\left(\mathit{sdec}(h_6, K_{BT})\right)\right) = h_2$ by the role of B, so $\pi_1\left(N'_1\right) = N_1$. But then $N'_1 \neq N_1$ is not possible because at the point when they are both fresh, let's say at the beginning, $\phi_1, N'_1 \rhd^{\mathrm{sic2}} N_1$, which contradicts the no telepathy axiom together with the fresh items don't help axiom. So $N'_1 = N_1$, but then $\pi_1\left(N_1\right) = N_1$ contradicts our additional assumption.

2.) Suppose T sent it. Then it looks like

$$\left\{\!\middle|\pi_1\left(\pi_2\left(\pi_2\left(h_4\right)\right)\right),\ \ \pi_1\left(\pi_2\left(h_4\right)\right),\ \ K',\ \ \left\{\!\middle|K',\ \ \pi_2\left(\mathit{dec}\left(\pi_2\left(\pi_2\left(\pi_2\left(h_4\right)\right)\right), K_{\pi_1(\pi_2(h_4))T}\right)\right),\ \ \pi_1\left(h_4\right)\middle|\!\right\}^{R_2}_{K_{\pi_1(\pi_2(h_4))T}}\middle|\!\right\}^{R_3}_{K_{\pi_1(h_4)T}}$$

for some h_4, R_1 and R_2. Since T sent this message, it succeeded the checks before, so we have

- $W(\pi_1\left(h_4\right))$ that is, $\pi_1\left(h_4\right)$ is a name, let's call it Q_1
- $W(\pi_1\left(\pi_2\left(h_4\right)\right))$ that is, $\pi_1\left(\pi_2\left(h_4\right)\right)$ is also a name, let it be Q_2
- $\pi_1\left(\mathit{sdec}(\pi_2\left(\pi_2\left(\pi_2\left(h_4\right)\right)\right), K_{\pi_1(\pi_2(h_4))T})\right) = \pi_1\left(h_4\right) = Q_1$

Let us also denote

$$n_1 \equiv \pi_2\left(\mathit{dec}\left(\pi_2\left(\pi_2\left(\pi_2\left(h_4\right)\right)\right), K_{\pi_1(\pi_2(h_4))T}\right)\right)$$

and

$$n_2 \equiv \pi_1\left(\pi_2\left(\pi_2\left(h_4\right)\right)\right)$$

with these, the message looks like

$$\left\{\!\middle|n_2,\ \ Q_2\ \ K,\ \ \{\!|K,\ \ n_1,\ \ Q_1|\!\}^{R_2}_{K_{Q_2T}}\middle|\!\right\}^{R_3}_{K_{Q_1T}}$$

So either

$$\{\!|z|\!\}^R_{K_{BT}} \equiv \{\!|K,\ \ n_1,\ \ Q_1|\!\}^{R_2}_{K_{Q_2T}}$$

or

$$\{\!|z|\!\}^R_{K_{BT}} \equiv \left\{\!\middle|n_2,\ \ Q_2\ \ K,\ \ \{\!|K,\ \ n_1,\ \ Q_1|\!\}^{R_2}_{K_{Q_2T}}\middle|\!\right\}^{R_3}_{K_{Q_1T}}.$$

2.1.) If $\{\!|z|\!\}^{R}_{K_{BT}} \equiv \{\!|n_2,\ Q_2\ K,\ \{\!|K,\ n_1,\ Q_1|\!\}^{R_2}_{K_{Q_2T}}|\!\}^{R_3}_{K_{Q_1T}}$, then $Q_1 \equiv B$ and

$$\mathit{sdec}(h_6, K_{BT}) = \langle n_2,\ Q_2\ K,\ \{\!|K,\ n_1,\ Q_1|\!\}^{R_2}_{K_{Q_2T}}\rangle. \tag{1}$$

From this, and the preceeding,

$$N_1 = \pi_1\left(\pi_2\left(\mathit{sdec}(h_6, K_{BT})\right)\right) = Q_2$$

and

$$h_2 = \pi_2\left(\pi_2\left(\mathit{sdec}(h_6, K_{BT})\right)\right) = \langle K,\ \{\!|K,\ n_1,\ Q_1|\!\}^{R_2}_{K_{Q_2T}}\rangle.$$

Hence, $\pi_1\left(h_2\right) = K_2$. Now, h_2 is the agent name with which B is communicating in the session in which N_1 is generated. By the role of B, h_2 must exist already by the time N_2 was generated.

2.1.1.) If K was created after N_1, then it was also created after h_2. That means by the freshness axiom that at the point when K is still fresh, but after h_2 was received by B, we have $\phi, h_2 \not\vdash K$. But this contradicts to $\pi_1\left(h_2\right) = K_2$ and function application.

2.1.2.) If K was created before N_1, then Q_2 must also have existed and been public before N_1. At that point, $\phi \not\vdash N_1$ because of freshness, but Q_2 is already public, so $\phi \not\vdash Q_2$. But as we have $N_1 = Q_2$, this is a contradiction.

2.2.) If $\{\!|z|\!\}^{R}_{K_{BT}} \equiv \{\!|K,\ n_1,\ Q_1|\!\}^{R_2}_{K_{Q_2T}}$ then $\pi_1\left(\pi_2\left(h_4\right)\right) = Q_2 = B$, and

$$N_1 = \pi_1\left(\pi_2\left(\mathit{sdec}(h_6, K_{BT})\right)\right) = n_1 \equiv \pi_2\left(\mathit{dec}\left(\pi_2\left(\pi_2\left(\pi_2\left(h_4\right)\right)\right), K_{\pi_1(\pi_2(h_4))T}\right)\right)$$

and

$$h_2 = \pi_2\left(\pi_2\left(\mathit{sdec}(h_6, K_{BT})\right)\right) = Q_1 = \pi_1\left(h_4\right)$$

and

$$K = \pi_1\left(\mathit{sdec}(h_6, K_{BT})\right).$$

□

c)
Let us introduce the condition

$$C[K] \equiv \tag{2}$$

$$\mathsf{RandGen}(K)\ \wedge\ \exists h_4 R_2 R_3\Big(\Big\{\!\Big|\pi_1\left(\pi_2\left(\pi_2\left(h_4\right)\right)\right),\ B,\ K,\ \{\!|K,\ \pi_2\left(\mathit{dec}\left(\pi_2\left(\pi_2\left(\pi_2\left(h_4\right)\right)\right), K_{BT}\right)\right),\ A|\!\}^{R_2}_{K_{BT}}\Big|\!\Big\}^{R_3}_{K_{AT}} \sqsubseteq \hat{\phi}\Big) \tag{3}$$

that is, K was generated by the trusted party and meant for A and B. And let

$$C'[M_1, ..., M_n, K] \equiv \tag{4}$$

$$\bigwedge_{i=1}^{n}\Big(K \neq M_i\ \wedge\ \mathsf{RandGen}(M_i)\ \wedge\ \exists h_2 h_4 h_6 R_1 R_2 R_3 R_4\Big(\{\!|h_2, M_i|\!\}^{R_1}_{K_{BT}} \sqsubseteq \hat{\phi}\ \vee\ \{\!|M_i|\!\}^{R_4}_{\pi_1(\mathit{sdec}(h_6, K_{BT}))} \sqsubseteq \hat{\phi} \tag{5}$$

$$\Big\{\!\Big|\pi_1\left(\pi_2\left(\pi_2\left(h_4\right)\right)\right),\ \pi_1\left(\pi_2\left(h_4\right)\right),\ M_i,\ \{\!|M_i,\ \pi_2\left(\mathit{dec}\left(\pi_2\left(\pi_2\left(\pi_2\left(h_4\right)\right)\right), K_{\pi_1(\pi_2(h_4))T}\right)\right),\ \pi_1\left(h_4\right)|\!\}^{R_2}_{K_{\pi_1(\pi_2(h_4))T}}\Big|\!\Big\}^{R_3}_{K_{\pi_1(h_4)T}} \sqsubseteq \hat{\phi}\Big)\Big)$$

which means that M_i were generated either by either B or T and are not the same as K.

We will carry out an inductive proof on the length of ϕ. As it turns out, in order to avoid loops in the proof, we prove

$$\forall \vec{M} K\Big(C[K]\ \wedge\ C'[\vec{M}, K]\ \wedge\ \hat{\phi}, \vec{M} \blacktriangleright K\Big) \tag{6}$$

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

$$\forall \vec{M} K\Big(C_l[K] \ \wedge \ C'_l[\vec{M}, K] \ \wedge \ \phi_l, \vec{M} \blacktriangleright K\Big)$$

is inconsistent with the axioms and agent checks. As C and C' is always taken at l, we leave that index.

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

$$\exists \vec{M}\Big(C[K] \ \wedge \ C'[\vec{M}, K] \ \wedge \ \phi_m, \vec{M} \blacktriangleright K\Big)$$

is inconsistent with the axioms and agent checks, then

$$\exists \vec{M}\Big(C[K] \ \wedge \ C'[\vec{M}, K] \ \wedge \ \phi_{m+1}, \vec{M} \blacktriangleright K\Big)$$

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

Proposition 1.1 *In the above execution of symmetric NS protocol, let K be such that $C[K]$ is satisfied, and let $m < l$. If for all $\vec{M}$ such that $C'[\vec{M}, K]$ holds, the axioms and agent checks imply (by FOL deduction rules) that $\phi_m, \vec{M} \not\blacktriangleright K$, then for all $\vec{M}$ such that $C'[\vec{M}, K]$ holds, the axioms and agent checks imply (by FOL deduction rules) that $\phi_{m+1}, \vec{M} \not\blacktriangleright K$ holds.*

Proof. Suppose the claim is not true. That is, let us assume that there is a finite set $\vec{M} \equiv M_1, ...M_l$ such that $C'[\vec{M}, K]$ and

$$\phi_{m+1}, M_1, ..., M_l \blacktriangleright K$$

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

$$\phi_m, M'_1, ..., M'_{l'} \blacktriangleright K$$

is satisfied. But, as according to our assumption, this was inconsistent, we get a contradiction and hence $\phi_{m+1}, M_1, ..., M_l \blacktriangleright K$ must also have been inconsistent.

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

$$\phi_m, t, M_1, ..., M_l \blacktriangleright K$$

holds. That is the same as

$$\phi_m, M_1, ..., M_l, t \blacktriangleright K$$

by the commutativity axiom.

1.) Assume that t was sent by T. Since T follows his trusted server role, t must look like

$$\Big\{\Big|\pi_1\left(\pi_2\left(\pi_2\left(h\right)\right)\right), \ \ \pi_1\left(\pi_2\left(h\right)\right), \ \ K', \ \ \Big\{\Big|K', \ \ \pi_2\left(dec\Big(\pi_2\left(\pi_2\left(\pi_2\left(h\right)\right)\right), K_{\pi_1(\pi_2(h))T}\Big)\right), \ \ \pi_1\left(h\right)\Big|\Big\}^{R_2}_{K_{\pi_1(\pi_2(h))T}}\Big|\Big\}^{R_3}_{K_{\pi_1(h)T}}$$

for some h, R_1 and R_2. Since T sent this message, it succeeded the checks before, so we have

- $W(\pi_1\left(h\right))$ that is, $\pi_1\left(h\right)$ is a name, let's call it Q_1
- $W(\pi_1\left(\pi_2\left(h\right)\right))$ that is, $\pi_1\left(\pi_2\left(h\right)\right)$ is also a name, let it be Q_2
- $\pi_1\left(sdec(\pi_2\left(\pi_2\left(\pi_2\left(h\right)\right)\right), K_{\pi_1(\pi_2(h))T}\right)\right) = \pi_1\left(h\right) = Q_1$

Let us also denote

$$n_1 \equiv \pi_2\left(dec\left(\pi_2\left(\pi_2\left(\pi_2\left(h\right)\right)\right), K_{\pi_1(\pi_2(h))T}\right)\right)$$

and

$$n_2 \equiv \pi_1\left(\pi_2\left(\pi_2\left(h\right)\right)\right)$$

with these,

$$t = \left\{\left|n_2,\ \ Q_2\ \ K',\ \ \left\{\left|K',\ \ n_1,\ \ Q_1\right|\right\}_{K_{Q_2T}}^{R_2}\right|\right\}_{K_{Q_1T}}^{R_3}$$

So let

$$\phi_m, \vec{M}, \not\blacktriangleright K$$

1.1.) If Q_1 is one of A, B and T, then K_{Q_1T} was never sent around and is honestly generated, hence by the encryptions with uncorrupted keys do not corrupt axiom (as long term keys are keyfresh)

$$\phi_m, \vec{M}, \left\{\left|n_2,\ \ Q_2\ \ K',\ \ \left\{\left|K',\ \ n_1,\ \ Q_1\right|\right\}_{K_{Q_2T}}^{R_2}\right|\right\}_{K_{Q_1T}}^{R_3} \not\blacktriangleright K,$$

that is,

$$\phi_m, \vec{M}, t \not\blacktriangleright K.$$

1.2.) Suppose now Q_1 is not one of A, B and T, then K_{Q_1T}.

1.2.1.) Suppose that Q_2 is not one of A, B or T either. Then $C[K']$ surely does not hold, as K' was not sent out encrypted by K_{AT} and K_{BT} as $C[K']$ would require (if it were sent out that way too, it would have had to be in another session, but there a new key was generated). So we also have

$$K' \neq K$$

as we assumed $C[K]$.

But taking $\vec{M}' \equiv \vec{M}, K'$, it is easy to see that $C'[\vec{M}', K]$ is satisfied so by the induction hypothesis,

$$\phi_m, \vec{M}, K' \not\blacktriangleright K$$

Since there h was received earlier, $\phi_{m-x} \rhd h$ for some positive x and by the weakening property of derivability, $\phi_m, \vec{M}, K' \rhd h$. By the transitivity property and commutativity, $\phi_m, \vec{M}, K' \rhd h \wedge \phi_m, \vec{M}, h, K' \blacktriangleright K \rightarrow \phi_m, \vec{M}, K' \blacktriangleright K$, so we have

$$\phi_m, \vec{M}, h, K' \not\blacktriangleright K$$

applying the function symbols of projections, we receive

$$\phi_m, \vec{M}, h, \pi_1\left(\pi_2\left(\pi_2\left(h\right)\right)\right), K' \not\blacktriangleright K$$

Since $K_{\pi_1(h)T} = K_{Q_2T}$ is also owned by the adversary,

$$\phi_m, \vec{M}, h, K_{\pi_1(h)T}, \pi_1\left(\pi_2\left(\pi_2\left(h\right)\right)\right), K' \not\blacktriangleright K,$$

employing functions again,

$$\phi_m, \vec{M}, \pi_2\left(dec\left(\pi_2\left(\pi_2\left(\pi_2\left(h\right)\right)\right), K_{\pi_1(\pi_2(h))T}\right)\right), \pi_1\left(\pi_2\left(\pi_2\left(h\right)\right)\right), K' \not\blacktriangleright K,$$

which is the same as

$$\phi_m, \vec{M}, n_1, n_2, K' \not\blacktriangleright K,$$

Since the names Q_1 and Q_2 are public,

$$\phi_m, \vec{M}, Q_1, Q_2, n_1, n_2, K' \not\blacktriangleright K$$

As neither Q_1 nor Q_2 are any of A, B and T, we have as earlier that K_{Q_2T} and K_{Q_1T} are available to the adversary,

$$\phi_m, \vec{M}, Q_1, Q_2, n_1, n_2, K', K_{Q_1T}, K_{Q_2T} \not\vdash K$$

As R_1 and R_2 were freshly generated, by the fresh items do not corrupt axiom,

$$\phi_m, \vec{M}, Q_1, Q_2, n_1, n_2, K', K_{Q_1T}, K_{Q_2T}, R_1, R_2 \not\vdash K$$

Finally, again by function application

$$\phi_m, \vec{M}, \{|n_2,\ \ Q_2\ \ K',\ \ \{|K',\ \ n_1,\ \ Q_1|\}^{R_2}_{K_{Q_2T}}|\}^{R_3}_{K_{Q_1T}} \not\vdash K,$$

that is,

$$\phi_m, \vec{M}, t \not\vdash K.$$

1.2.) Let now Q_2' be one of A, B, T. Just as in 1.1.), we have

$$\phi_m, \vec{M}, h, \not\vdash K$$

and

$$\phi_m, \vec{M}, n_2, \not\vdash K.$$

Since Q_2' be one of A, B, T, the secret key K_{Q_2T} has never been sent out, and so by the uncorrupted keys securely encrypt axiom we have

$$\phi_m, \vec{M}, n_2, \{|K', n_1, Q_1|\}^{R_2}_{K_{Q_2'T}}, \not\vdash K.$$

As we assumed that Q_1 is not one of A, B or T, we have $Q_1 \neq A$. Then just as earlier as the trusted party follows its role, this implies that $C[K']$ does not hold and therefore $K' \neq K$, and again $C'[\vec{M}', K]$ is satisfied with $\vec{M}, K'$. Since in the above, $\vec{M}$ can be anything satisfying $C'[\vec{M}, K]$, it can also be taken to be $\vec{M}'$, so we have

$$\phi_m, \vec{M}', n_2, \{|K', n_1, Q_1|\}^{R_2}_{K_{Q_2'T}}, \not\vdash K,$$

that is,

$$\phi_m, \vec{M}, K', n_2, \{|K', n_1, Q_1|\}^{R_2}_{K_{Q_2'T}}, \not\vdash K.$$

Again, Q_2 is public, so by transitivity,

$$\phi_m, \vec{M}, K', n_2, Q_2, \{|K', n_1, Q_1|\}^{R_2}_{K_{Q_2'T}}, \not\vdash K$$

and K_{Q_1T} is known to the adversary and R_3 is fresh so by transitivity again,

$$\phi_m, \vec{M}, K', n_2, Q_2, \{|K', n_1, Q_1|\}^{R_2}_{K_{Q_2'T}}, K_{Q_1T}, R_3 \not\vdash K,$$

and by function application,

$$\phi_m, \vec{M}, \{|n_2,\ \ Q_2\ \ K',\ \ \{|K',\ \ n_1,\ \ Q_1|\}^{R_2}_{K_{Q_2T}}|\}^{R_3}_{K_{Q_1T}} \not\vdash K,$$

that is,

$$\phi_m, \vec{M}, t \not\vdash K.$$

2.) If t was sent by B then the role of B implies that t is either of the form (note that this is now a new h) $t \equiv \{|h, N_1|\}^{R_1}_{K_{BT}}$ or of the form $t \equiv \{|N_3|\}^{R_4}_{\pi_1(sdec(h', K_{BT}))}$.

2.1.) If $t \equiv \{\!|h, N_1|\!\}^{R_1}_{K_{BT}}$, then the encryption is secure as K_{BT} has never been sent around, so by the encryptions with uncorrupted key does not corrupt axiom

$$\phi_m, \vec{M}, \{\!|h, N_1|\!\}^{R_1}_{K_{BT}} \not\triangleright K$$

and so

$$\phi_m, \vec{M}, t \not\triangleright K$$

follows.

2.2.) If $t \equiv \{\!|N_3|\!\}^{R_4}_{\pi_1(sdec(h', K_{BT}))}$, then by **b)** for some K' honest key generated by T, we have $K' = \pi_1\left(sdec(h', K_{BT})\right)$.

2.2.1.) Suppose $K' = K$. Since N_3 was generated by B, and $N_3 \neq K$ we have for $\vec{M'} \equiv \vec{M}, N_3$ that $C'[M', K]$ is satisfied, so,

$$\phi_m, \vec{M}, N_3 \not\triangleright K.$$

By again the encryptions with uncorrupted keys do not corrupt axiom, since we had $\phi_m, M, N_3 \not\triangleright K$, we also have

$$\phi_m, \vec{M}, \{\!|N_3|\!\}^{R_4}_{K'} \not\triangleright K.$$

2.2.2.) Suppose now that $K' \neq K$. Then with $\vec{M'} \equiv M, N_3, K', C'[\vec{M'}, K]$ is satisfied, and by the induction hypothesis,

$$\phi_m, \vec{M}, N_3, K' \not\triangleright K.$$

As R_4 is freshly generated, by the fresh items do not help we get

$$\phi_m, \vec{M}, N_3, K', R_4 \not\triangleright K,$$

and by function application,

$$\phi_m, \vec{M}, \{\!|N_3|\!\}^{R_4}_{K'} \not\triangleright K.$$

3.) If t was sent by A, then by the role of A, this mean that there are four possibilities:

3.1.) If $t \equiv A$, then clearly, $\phi_m, \vec{M}, \not\triangleright K$ implies $\phi_m, \vec{M}, A \not\triangleright K$ as names are public.

3.2.) If $t \equiv \langle A, B, N_2, h_3\rangle$, as N_2 is fresh, $\phi_m, \vec{M}, \not\triangleright K$ implies $\phi_m, \vec{M}, N_2 \not\triangleright K$. Then, A, B are public, so we have $\phi_m, \vec{M}, N_2, A, B \not\triangleright K$, and as $\phi_m \rhd h_3$, we have $\phi_m, \vec{M}, N_2, A, B, h_3 \not\triangleright K$ by transitivity. By commutativity and function application,

$$\phi_m, \vec{M}, \langle A, B, N_2, h_3\rangle \not\triangleright K.$$

3.3.) If $t \equiv \pi_2\left(\pi_2\left(\pi_2\left(sdec(h_5, K_{AT})\right)\right)\right)$, then A also sent $c_i\big(A, Q, T, N_2, \pi_1\left(\pi_2\left(\pi_2\left(sdec(h_5, K_{AT})\right)\right)\right)\big)$. By **a.)**

$$\begin{aligned}
&\exists K' h_4\big(c_t\big(\pi_1\left(h_4\right),\ \pi_1\left(\pi_2\left(h_4\right)\right),\ T,\ \pi_2\left(dec\big(\pi_2\left(\pi_2\left(\pi_2\left(h_4\right)\right)\right), K_{\pi_1(\pi_2(h_4))T}\big)\right),\ \pi_1\left(\pi_2\left(\pi_2\left(h_4\right)\right)\right),\ K\big) \sqsubseteq \hat{\phi}\\
\wedge\ & K' = \pi_1\left(\pi_2\left(\pi_2\left(sdec(h_5, K_{AT})\right)\right)\right) \wedge N_2 = \pi_1\left(\pi_2\left(\pi_2\left(h_4\right)\right)\right) \wedge A = \pi_1\left(h_4\right) \wedge Q = \pi_1\left(\pi_2\left(h_4\right)\right)\\
\wedge\ & \pi_2\left(\pi_2\left(\pi_2\left(sdec(h_5, K_{AT})\right)\right)\right) = \big\{\!\big|K',\ \pi_2\left(dec\big(\pi_2\left(\pi_2\left(\pi_2\left(h_4\right)\right)\right), K_{\pi_1(\pi_2(h_4))T}\big)\right),\ \pi_1\left(h_4\right)\big|\!\big\}^{R_2}_{K_{\pi_1(\pi_2(h_4))T}}\big)
\end{aligned}$$

So in this case,

$$t = \big\{\!\big|K',\ \pi_2\left(dec\big(\pi_2\left(\pi_2\left(\pi_2\left(h_4\right)\right)\right), K_{QT}\big)\right),\ \pi_1\left(h_4\right)\big|\!\big\}^{R_2}_{K_{QT}}.$$

And Note that $Q \neq T$ because T is not allowed to communicate with itself.

3.3.1.) If $Q \neq B \wedge Q \neq A$, then K' does not satisfy C, so $K \neq K'$. But T generated K', so $\vec{M'} \equiv \vec{M}, K'$ satisfies $C'[\vec{M'}, K]$, and therefore, $\phi_m, \vec{M}, K' \not\triangleright K$. R_2 is fresh, so $\phi_m, \vec{M}, K', R_2 \not\triangleright K$. Since $\phi_m \rhd K_{QT}$, and also $\phi_4 \rhd h_4$, by transitivity, we get

$$\phi_m, \vec{M}, K', R_2, h_4, K_{QT} \not\triangleright K.$$

By function application, we arrive at

$$\phi_m, \vec{M}, \big\{\!\big|K',\ \pi_2\left(dec\big(\pi_2\left(\pi_2\left(\pi_2\left(h_4\right)\right)\right), K_{QT}\big)\right),\ \pi_1\left(h_4\right)\big|\!\big\}^{R_2}_{K_{QT}} \not\triangleright K.$$

3.3.2.) If $Q = A \ \vee \ Q = B$, then the encryption is safe, and we again have

$$\phi_m, \vec{M}, \{\!|K', \ \ \pi_2\left(dec\big(\pi_2\left(\pi_2\left(\pi_2\left(h_4\right)\right)\right), K_{QT}\big)\right), \ \ \pi_1\left(h_4\right)|\!\}^{R_2}_{K_{QT}} \not\blacktriangleright K.$$

3.4.) If $t \equiv \{\!|sdec(h_7, \pi_1\left(\pi_2\left(\pi_2\left(sdec(h_5, K_{AT}\right)\right)\right)\right) - 1|\!\}^{R_5}_{\pi_1(\pi_2(\pi_2(sdec(h_5,K_{AT}))))}$, then and by **a.)** again, there is a K' generated by T with $K' = \pi_1\left(\pi_2\left(\pi_2\left(sdec(h_5, K_{AT}\right)\right)\right)\right)$. So

$$t = \{\!|sdec(h_7, K') - 1|\!\}^{R_5}_{K'}$$

3.4.1.) Assume $K' = K$.

3.4.1.1.) If $\phi_m, \vec{M}, sdec(h_7, K') - 1 \not\blacktriangleright K'$, then, as we also had $\phi_m, \vec{M} \not\blacktriangleright K'$ by the encryption with uncorrupted key does not corrupt axiom, $\phi_m, \vec{M}, \{\!|sdec(h_7, K') - 1|\!\}^{R_5}_{K'} \not\blacktriangleright K'$

3.4.1.2.) If $\phi_m, \vec{M}, sdec(h_7, K') - 1 \blacktriangleright K'$, then also $\phi_m, \vec{M}, sdec(h_7, K') \blacktriangleright K'$. However, we assumed $\phi_m, \vec{M} \not\blacktriangleright K'$. Since $\phi_m \rhd h_7$, we can apply the decryptions do not help axiom to receive that $h_7 = \{\!|z|\!\}^R_{K'}$ for some z and R, and $\{\!|z|\!\}^R_{K'} \sqsubseteq \phi_m$.

3.4.1.2.1.) T could not have created $\{\!|z|\!\}^R_{K'} \sqsubseteq \phi_m$ because he never encrypts with session key.

3.4.1.2.2.) If it was created by A, then

$$\{\!|z|\!\}^R_{K'} = \{\!|sdec(h'_7, K') - 1|\!\}^R_{K'}.$$

Let us denote the rhs by t'. Clearly, t' was sent earlier than t, and it must be in a different session of A, as such a message is not sent twice in one session (t was the same kind). Let's denote the first nonce generated by A in the session belonging to t by N_2. And the one generated in the session belonging to t' by N'_2. They are different, because they were generated in different sessions. Applying **a.)** to the session when t was generated, we get that $N_2 = \pi_1\left(\pi_2\left(\pi_2\left(h_4\right)\right)\right)$, where h_4 is the message T received in the session when K' was generated. However, if we apply **a.)** to the session when t' was generated, we get that $N'_2 = \pi_1\left(\pi_2\left(\pi_2\left(h_4\right)\right)\right)$, a contradiction. So $\{\!|z|\!\}^R_{K'} \sqsubseteq \phi_m$ could not have been created by A.

3.4.1.2.3.) If B created t', then

$$\{\!|z|\!\}^R_{K'} = \{\!|N_3|\!\}^R_{K'}.$$

In this case, $sdec(h_7, K') = N_3$. As N_3 was generated by B, for $\vec{M}' \equiv \vec{M}, N_3$, $C'(\vec{M}', K)$ is satisfied. Therefore, by our induction hypothesis, $\phi_m, \vec{M}, N_3 \not\blacktriangleright K$, but that is the same as $\phi_m, \vec{M}, N_3 \not\blacktriangleright K'$, and that implies $\phi_m, \vec{M}, N_3 - 1 \not\blacktriangleright K'$. Hence, by the encryption with uncorrupted keys do not corrupt axiom,

$$\phi_m, \vec{M}, \{\!|N_3 - 1|\!\}^R_{K'} \not\blacktriangleright K.$$

3.4.2.) Assume $K' \neq K$. In this case, $\vec{M}' \equiv \vec{M}, K'$ satisfies $C'(\vec{M}', K)$, and so by the induction hypothesis,

$$\phi_m, \vec{M}, K' \not\blacktriangleright K. \tag{7}$$

3.4.2.1.) If $\phi_m, \vec{M}, K', sdec(h_7, K') - 1 \not\blacktriangleright K$, then for fresh R_5, $\phi_m, \vec{M}, K', sdec(h_7, K') - 1 \not\blacktriangleright K$ also holds, and by function application,

$$\phi_m, \vec{M}, \{\!|sdec(h_7, K') - 1|\!\}^{R_5}_{K'} \not\blacktriangleright K$$

3.4.2.2.) If $\phi_m, \vec{M}, sdec(h_7, K') - 1 \blacktriangleright K$, then, $\phi_m, \vec{M}, sdec(h_7, K') \blacktriangleright K$. However, we assumed $\phi_m, \vec{M} \not\blacktriangleright K$. Since $\phi_m \rhd h_7$, we can apply the decryptions do not help axiom to receive that $h_7 = \{\!|z|\!\}^R_{K'}$ for some z and R, and $\{\!|z|\!\}^R_{K'} \sqsubseteq \phi_m$. The same exact way as in 3.4.1.2, we get that $\{\!|z|\!\}^R_{K'}$ was created by B and it is $\{\!|N_3|\!\}^R_{K'}$. Then $sdec(h_7, K') = N_3$, and the same way again $\phi_m, \vec{M}, \{\!|N_3 - 1|\!\}^R_{K'} \not\blacktriangleright K$.

□

d)
Secrecy proof for the nonce is entirely analogous to the key usability proof. Let

$$C_e[N] \equiv \mathsf{RandGen}(K) \wedge \tag{8}$$

$$\exists_{h_4 R_2 R_3 K R_5}\Big(\Big\{\Big|\pi_1\left(\pi_2\left(\pi_2\left(h_4\right)\right)\right),\ B,\ K,\ \{\!|K,\ \pi_2\left(dec\big(\pi_2\left(\pi_2\left(\pi_2\left(h_4\right)\right)\right), K_{BT}\big)\right),\ A|\!\}^{R_2}_{K_{BT}}\Big|\Big\}^{R_3}_{K_{AT}} \sqsubseteq \hat{\phi} \ \wedge\ \{\!|N|\!\}^{R_5}_{K} \sqsubseteq \hat{\phi}\Big) \tag{9}$$

that is, N was encrypted by K that was generated by the trusted party and meant for A and B. And let

$$C'_e[M_1, ..., M_n, N] \equiv \tag{10}$$

$$\bigwedge_{i=1}^{n}\Big(N \neq M_i \ \wedge\ \mathsf{RandGen}(M_i) \ \wedge\ \exists h_2 h_4 h_6 R_1 R_2 R_3 R_4\Big(\{\!|h_2, M_i|\!\}^{R_1}_{K_{BT}} \sqsubseteq \hat{\phi} \ \vee\ \{\!|M_i|\!\}^{R_4}_{\pi_1(sdec(h_6, K_{BT}))} \sqsubseteq \hat{\phi} \tag{11}$$

$$\Big\{\Big|\pi_1\left(\pi_2\left(\pi_2\left(h_4\right)\right)\right),\ \pi_1\left(\pi_2\left(h_4\right)\right),\ M_i,\ \{\!|M_i,\ \pi_2\left(dec\big(\pi_2\left(\pi_2\left(\pi_2\left(h_4\right)\right)\right), K_{\pi_1(\pi_2(h_4))T}\big)\right),\ \pi_1\left(h_4\right)|\!\}^{R_2}_{K_{\pi_1(\pi_2(h_4))T}}\Big|\Big\}^{R_3}_{K_{\pi_1(h_4)T}} \sqsubseteq \hat{\phi}\Big)\Big)$$

which means that M_i were generated either by either B or T and are not the same as N.

We will carry out again an inductive proof on the length of ϕ. As it turns out, in order to avoid loops in the proof, we prove

$$\forall \vec{M} K\Big(C_e[N] \ \wedge\ C'_e[\vec{M}, N] \ \wedge\ \hat{\phi}, \vec{M} \rhd^{\mathrm{sic2}} N\Big) \tag{12}$$

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

$$\forall \vec{M} K\Big(C_{e,l}[N] \ \wedge\ C'_{e,l}[\vec{M}, N] \ \wedge\ \phi_l, \vec{N} \rhd^{\mathrm{sic2}} N\Big)$$

is inconsistent with the axioms and agent checks. As C_e and C'_e is always taken at l, we leave that index.

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

$$\exists \vec{M}\Big(C_e[N] \ \wedge\ C'_e[\vec{M}, N] \ \wedge\ \phi_m, \vec{M} \rhd^{\mathrm{sic2}} N\Big)$$

is inconsistent with the axioms and agent checks, then

$$\exists \vec{M}\Big(C_e[N] \ \wedge\ C'_e[\vec{M}, N] \ \wedge\ \phi_{m+1}, \vec{M} \rhd^{\mathrm{sic2}} N\Big)$$

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

Proposition 1.2 *In the above execution of symmetric NS protocol, let N be such that $C_e[N]$ is satisfied, and let $m < l$. If for all $\vec{M}$ such that $C'_e[\vec{M}, N]$ holds, the axioms and agent checks imply (by FOL deduction rules) that $\phi_m, \vec{M} \not\rhd^{\mathrm{sic2}} N$, then for all $\vec{M}$ such that $C'_e[\vec{M}, N]$ holds, the axioms and agent checks imply (by FOL deduction rules) that $\phi_{m+1}, \vec{M} \not\rhd^{\mathrm{sic2}} N$ holds.*

Proof. Suppose the claim is not true. That is, let us assume that there is a finite set $\vec{M} \equiv M_1, ...M_l$ such that $C'_e[\vec{M}, N]$ and

$$\phi_{m+1}, M_1, ..., M_l \rhd^{\mathrm{sic2}} N$$

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

$$\phi_m, M'_1, ..., M'_{l'} \rhd^{\mathrm{sic2}} N$$

is satisfied. But, as according to our assumption, this was inconsistent, we get a contradiction and hence $\phi_{m+1}, M_1, ..., M_l \rhd^{\text{sic2}} N$ must also have been inconsistent.

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

$$\phi_m, t, M_1, ..., M_l \rhd^{\text{sic2}} N$$

holds. That is the same as

$$\phi_m, M_1, ..., M_l, t \rhd^{\text{sic2}} N$$

by the commutativity axiom.

1.) Assume that t was sent by T. Since T follows his trusted server role, t must look like

$$\left\{\left|\pi_1\left(\pi_2\left(\pi_2\left(h\right)\right)\right),\ \ \pi_1\left(\pi_2\left(h\right)\right),\ \ K',\ \ \left\{\left|K',\ \ \pi_2\left(\mathit{dec}\left(\pi_2\left(\pi_2\left(\pi_2\left(h\right)\right)\right), K_{\pi_1(\pi_2(h))T}\right)\right),\ \ \pi_1\left(h\right)\right|\right\}^{R_2}_{K_{\pi_1(\pi_2(h))T}}\right|\right\}^{R_3}_{K_{\pi_1(h)T}}$$

for some h, R_1 and R_2. Since T sent this message, it succeeded the checks before, so we have

- $W(\pi_1\left(h\right))$ that is, $\pi_1\left(h\right)$ is a name, let's call it Q_1
- $W(\pi_1\left(\pi_2\left(h\right)\right))$ that is, $\pi_1\left(\pi_2\left(h\right)\right)$ is also a name, let it be Q_2
- $\pi_1\left(\mathit{sdec}(\pi_2\left(\pi_2\left(\pi_2\left(h\right)\right)\right), K_{\pi_1(\pi_2(h))T})\right) = \pi_1\left(h\right) = Q_1$

Let us also denote

$$n_1 \equiv \pi_2\left(\mathit{dec}\left(\pi_2\left(\pi_2\left(\pi_2\left(h\right)\right)\right), K_{\pi_1(\pi_2(h))T}\right)\right)$$

and

$$n_2 \equiv \pi_1\left(\pi_2\left(\pi_2\left(h\right)\right)\right)$$

with these,

$$t = \left\{\left|n_2,\ \ Q_2\ \ K',\ \ \left\{\left|K',\ \ n_1,\ \ Q_1\right|\right\}^{R_2}_{K_{Q_2T}}\right|\right\}^{R_3}_{K_{Q_1T}}$$

So let

$$\phi_m, \vec{M}, \not\rhd^{\text{sic2}} N$$

1.1.) If Q_1 is one of A, B and T, then K_{Q_1T} was never sent around and is honestly generated, hence by the uncorrupted keys securely encrypt axiom (as long term keys are keyfresh)

$$\phi_m, \vec{M}, \left\{\left|n_2,\ \ Q_2\ \ K',\ \ \left\{\left|K',\ \ n_1,\ \ Q_1\right|\right\}^{R_2}_{K_{Q_2T}}\right|\right\}^{R_3}_{K_{Q_1T}} \not\rhd^{\text{sic2}} N,$$

that is,

$$\phi_m, \vec{M}, t \not\rhd^{\text{sic2}} N.$$

1.2.) Suppose now Q_1 is not one of A, B and T, then K_{Q_1T}.

1.2.1.) Suppose that Q_2 is not one of A, B or T either.Taking $\vec{M'} \equiv \vec{M}, K'$, it is easy to see that $C'_e[\vec{M'}, N]$ is satisfied so by the induction hypothesis,

$$\phi_m, \vec{M}, K' \not\rhd^{\text{sic2}} N$$

Since there h was received earlier, $\phi_{m-x} \rhd h$ for some positive x and by the weakening property of derivability, $\phi_m, \vec{M}, K' \rhd h$. By the transitivity property and commutativity, $\phi_m, \vec{M}, K' \rhd h \wedge \phi_m, \vec{M}, h, K' \rhd^{\text{sic2}} N \rightarrow \phi_m, \vec{M}, K' \rhd^{\text{sic2}} N$, so we have

$$\phi_m, \vec{M}, h, K' \not\rhd^{\text{sic2}} N$$

applying the function symbols of projections, we receive

$$\phi_m, \vec{M}, h, \pi_1\left(\pi_2\left(\pi_2\left(h\right)\right)\right), K' \not\rhd^{\text{sic2}} N$$

Since $K_{\pi_1(h)T} = K_{Q_2T}$ is also owned by the adversary,

$$\phi_m, \vec{M}, h, K_{\pi_1(h)T}, \pi_1\left(\pi_2\left(\pi_2\left(h\right)\right)\right), K' \not\vdash^{\mathrm{sic2}} N,$$

employing functions again,

$$\phi_m, \vec{M}, \pi_2\left(dec\big(\pi_2\left(\pi_2\left(\pi_2\left(h\right)\right)\right), K_{\pi_1(\pi_2(h))T}\big)\right), \pi_1\left(\pi_2\left(\pi_2\left(h\right)\right)\right), K' \not\vdash^{\mathrm{sic2}} N,$$

which is the same as

$$\phi_m, \vec{M}, n_1, n_2, K' \not\vdash^{\mathrm{sic2}} N,$$

Since the names Q_1 and Q_2 are public,

$$\phi_m, \vec{M}, Q_1, Q_2, n_1, n_2, K' \not\vdash^{\mathrm{sic2}} N$$

As neither Q_1 nor Q_2 are any of A, B and T, we have as earlier that K_{Q_2T} and K_{Q_1T} are available to the adversary,

$$\phi_m, \vec{M}, Q_1, Q_2, n_1, n_2, K', K_{Q_1T}, K_{Q_2T} \not\vdash^{\mathrm{sic2}} N$$

As R_1 and R_2 were freshly generated, by the fresh items do not corrupt axiom,

$$\phi_m, \vec{M}, Q_1, Q_2, n_1, n_2, K', K_{Q_1T}, K_{Q_2T}, R_1, R_2 \not\vdash^{\mathrm{sic2}} N$$

Finally, again by function application

$$\phi_m, \vec{M}, \left\{\left|n_2,\ \ Q_2\ \ K',\ \ \left\{\left|K',\ \ n_1,\ \ Q_1\right|\right\}^{R_2}_{K_{Q_2T}}\right|\right\}^{R_3}_{K_{Q_1T}} \not\vdash^{\mathrm{sic2}} N,$$

that is,

$$\phi_m, \vec{M}, t \not\vdash^{\mathrm{sic2}} N.$$

1.2.) Let now Q_2' be one of A, B, T. Just as in 1.1.), we have

$$\phi_m, \vec{M}, h, \not\vdash^{\mathrm{sic2}} N$$

and

$$\phi_m, \vec{M}, n_2, \not\vdash^{\mathrm{sic2}} N.$$

Since Q_2' be one of A, B, T, the secret key K_{Q_2T} has never been sent out, and so by the uncorrupted key securely encrypts axiom we have

$$\phi_m, \vec{M}, n_2, \{|K', n_1, Q_1|\}^{R_2}_{K_{Q_2'T}}, \not\vdash N.$$

Again $C_e'[\vec{M'}, N]$ is satisfied with $\vec{M'} \equiv \vec{M}, K'$. Since in the above, $\vec{M}$ can be anything satisfying $C_e'[\vec{M}, N]$, it can also be taken to be $\vec{M'}$, so we have

$$\phi_m, \vec{M'}, n_2, \{|K', n_1, Q_1|\}^{R_2}_{K_{Q_2'T}}, \not\vdash^{\mathrm{sic2}} N,$$

that is,

$$\phi_m, \vec{M}, K', n_2, \{|K', n_1, Q_1|\}^{R_2}_{K_{Q_2'T}}, \not\vdash^{\mathrm{sic2}} N.$$

Again, Q_2 is public, so by transitivity,

$$\phi_m, \vec{M}, K', n_2, Q_2, \{|K', n_1, Q_1|\}^{R_2}_{K_{Q_2'T}}, \not\vdash^{\mathrm{sic2}} N$$

and K_{Q_1T} is known to the adversary and R_3 is fresh so by transitivity again,

$$\phi_m, \vec{M}, K', n_2, Q_2, \{|K', n_1, Q_1|\}^{R_2}_{K_{Q_2'T}}, K_{Q_1T}, R_3 \not\vdash^{\mathrm{sic2}} N,$$

and by function application,

$$\phi_m, \vec{M}, \{\!|n_2,\ Q_2\ K',\ \{\!|K',\ n_1,\ Q_1|\!\}^{R_2}_{K_{Q_2T}}|\!\}^{R_3}_{K_{Q_1T}} \not\vdash^{\mathrm{sic2}} N,$$

that is,

$$\phi_m, \vec{M}, t \not\vdash^{\mathrm{sic2}} N.$$

2.) If t was sent by B then the role of B implies that t is either of the form (note that this is now a new h) $t \equiv \{\!|h, N_1|\!\}^{R_1}_{K_{BT}}$ or of the form $t \equiv \{\!|N_3|\!\}^{R_4}_{\pi_1(\mathit{sdec}(h', K_{BT}))}$.

2.1.) If $t \equiv \{\!|h, N_1|\!\}^{R_1}_{K_{BT}}$, then the encryption is secure as K_{BT} has never been sent around, so by the uncorrupted keys securely encrypt axiom

$$\phi_m, \vec{M}, \{\!|h, N_1|\!\}^{R_1}_{K_{BT}} \not\vdash^{\mathrm{sic2}} N$$

and so

$$\phi_m, \vec{M}, t \not\vdash^{\mathrm{sic2}} N$$

follows.

2.2.) If $t \equiv \{\!|N_3|\!\}^{R_4}_{\pi_1(\mathit{sdec}(h', K_{BT}))}$, then by **b)** for some K' honest key generated by T, we have $K' = \pi_1\left(\mathit{sdec}(h', K_{BT})\right)$.

2.2.1.) Suppose $N_3 = N$. Since N_3 was generated by B, and $N_3 \neq K$ we have from **c.)** that

$$\phi_m, \vec{M}, N_3 \not\vdash K.$$

By again the uncorrupted keys securely encrypt axiom, since we had $\phi_m, M \not\vdash^{\mathrm{sic2}} N$, we also have

$$\phi_m, \vec{M}, \{\!|N_3|\!\}^{R_4}_{K'} \not\vdash^{\mathrm{sic2}} N.$$

2.2.2.) Suppose now that $N_3 \neq N$. Then with $\vec{M'} \equiv M, N_3, K', C'_e[\vec{M'}, N]$ is satisfied, and by the induction hypothesis,

$$\phi_m, \vec{M}, N_3, K' \not\vdash^{\mathrm{sic2}} N.$$

As R_4 is freshly generated, by the fresh items do not help we get

$$\phi_m, \vec{M}, N_3, K', R_4 \not\vdash^{\mathrm{sic2}} N,$$

and by function application,

$$\phi_m, \vec{M}, \{\!|N_3|\!\}^{R_4}_{K'} \not\vdash^{\mathrm{sic2}} N.$$

3.) If t was sent by A, then by the role of A, this mean that there are four possibilities:

3.1.) If $t \equiv A$, then clearly, $\phi_m, \vec{M}, \not\vdash^{\mathrm{sic2}} N$ implies $\phi_m, \vec{M}, A \not\vdash^{\mathrm{sic2}} N$ as names are public.

3.2.) If $t \equiv \langle A, B, N_2, h_3\rangle$, as N_2 is fresh, $\phi_m, \vec{M}, \not\vdash^{\mathrm{sic2}} N$ implies $\phi_m, \vec{M}, N_2 \not\vdash^{\mathrm{sic2}} N$. Then, A, B are public, so we have $\phi_m, \vec{M}, N_2, A, B \not\vdash^{\mathrm{sic2}} N$, and as $\phi_m \rhd h_3$, we have $\phi_m, \vec{M}, N_2, A, B, h_3 \not\vdash^{\mathrm{sic2}} N$ by transitivity. By commutativity and function application,

$$\phi_m, \vec{M}, \langle A, B, N_2, h_3\rangle \not\vdash^{\mathrm{sic2}} N.$$

3.3.) If $t \equiv \pi_2\left(\pi_2\left(\pi_2\left(\mathit{sdec}(h_5, K_{AT})\right)\right)\right)$, then A also sent $c_i\big(A, Q, T, N_2, \pi_1\left(\pi_2\left(\pi_2\left(\mathit{sdec}(h_5, K_{AT})\right)\right)\right)\big)$. By **a.)**

$$\begin{aligned}
&\exists K' h_4 \big(c_t\big(\pi_1\left(h_4\right),\ \pi_1\left(\pi_2\left(h_4\right)\right),\ T,\ \pi_2\left(\mathit{dec}\big(\pi_2\left(\pi_2\left(\pi_2\left(h_4\right)\right)\right), K_{\pi_1(\pi_2(h_4))T}\big)\right),\ \pi_1\left(\pi_2\left(\pi_2\left(h_4\right)\right)\right),\ K\big) \sqsubseteq \hat{\phi}\\
\wedge\ & K' = \pi_1\left(\pi_2\left(\pi_2\left(\mathit{sdec}(h_5, K_{AT})\right)\right)\right) \wedge\ N_2 = \pi_1\left(\pi_2\left(\pi_2\left(h_4\right)\right)\right) \wedge\ A = \pi_1\left(h_4\right) \wedge\ Q = \pi_1\left(\pi_2\left(h_4\right)\right)\\
\wedge\ & \pi_2\left(\pi_2\left(\pi_2\left(\mathit{sdec}(h_5, K_{AT})\right)\right)\right) = \big\{\!\big|K',\ \pi_2\left(\mathit{dec}\big(\pi_2\left(\pi_2\left(\pi_2\left(h_4\right)\right)\right), K_{\pi_1(\pi_2(h_4))T}\big)\right),\ \pi_1\left(h_4\right)\big|\!\big\}^{R_2}_{K_{\pi_1(\pi_2(h_4))T}}\big)
\end{aligned}$$

So in this case,

$$t = \big\{\!\big|K',\ \pi_2\left(\mathit{dec}\big(\pi_2\left(\pi_2\left(\pi_2\left(h_4\right)\right)\right), K_{QT}\big)\right),\ \pi_1\left(h_4\right)\big|\!\big\}^{R_2}_{K_{QT}}.$$

And Note that $Q \neq T$ because T is not allowed to communicate with itself.

3.3.1.) If $Q \neq B \ \wedge \ Q \neq A$, then $\vec{M}' \equiv \vec{M}, K'$ satisfies $C'_e[\vec{M}', N]$, and therefore, $\phi_m, \vec{M}, K' \not\rhd^{\text{sic2}} N$. R_2 is fresh, so $\phi_m, \vec{M}, K', R_2 \not\rhd^{\text{sic2}} N$. Since $\phi_m \rhd K_{QT}$, and also $\phi_4 \rhd h_4$, by transitivity, we get

$$\phi_m, \vec{M}, K', R_2, h_4, K_{QT} \not\rhd^{\text{sic2}} N.$$

By function application, we arrive at

$$\phi_m, \vec{M}, \{\!|K', \ \pi_2\left(\mathit{dec}\big(\pi_2\left(\pi_2\left(\pi_2\left(h_4\right)\right)\right), K_{QT}\big)\right), \ \pi_1\left(h_4\right)|\!\}^{R_2}_{K_{QT}} \not\rhd^{\text{sic2}} N.$$

3.3.2.) If $Q = A \ \vee \ Q = B$, then the encryption is safe, and we again have

$$\phi_m, \vec{M}, \{\!|K', \ \pi_2\left(\mathit{dec}\big(\pi_2\left(\pi_2\left(\pi_2\left(h_4\right)\right)\right), K_{QT}\big)\right), \ \pi_1\left(h_4\right)|\!\}^{R_2}_{K_{QT}} \not\rhd^{\text{sic2}} N.$$

3.4.) If $t \equiv \{\!|\mathit{sdec}(h_7, \pi_1\left(\pi_2\left(\pi_2\left(\mathit{sdec}(h_5, K_{AT}\right)\right)\right)\right) - 1|\!\}^{R_5}_{\pi_1(\pi_2(\pi_2(\mathit{sdec}(h_5, K_{AT}))))}$, then and by **a.)** again, there is a K' generated by T with $K' = \pi_1\left(\pi_2\left(\pi_2\left(\mathit{sdec}(h_5, K_{AT}\right)\right)\right)\right)$. So

$$t = \{\!|\mathit{sdec}(h_7, K') - 1|\!\}^{R_5}_{K'}$$

3.4.1.) If $\phi_m, \vec{M}, K', \mathit{sdec}(h_7, K') - 1 \not\rhd^{\text{sic2}} N$, then for fresh R_5, $\phi_m, \vec{M}, K', \mathit{sdec}(h_7, K') - 1 \not\rhd^{\text{sic2}} N$ also holds, and by function application,

$$\phi_m, \vec{M}, \{\!|\mathit{sdec}(h_7, K') - 1|\!\}^{R_5}_{K'} \not\rhd^{\text{sic2}} K$$

3.4.2.) If $\phi_m, \vec{M}, K', \mathit{sdec}(h_7, K') - 1 \rhd^{\text{sic2}} N$, then also $\phi_m, \vec{M}, K', \mathit{sdec}(h_7, K') \rhd^{\text{sic2}} N$. However, we assumed $\phi_m, \vec{M}, K' \not\rhd^{\text{sic2}} N$, as $\vec{M}' \equiv \vec{M}, K$ satisfies $C_e(\vec{M}', K)$. Since $\phi_m \rhd h_7$, we can apply the decryptions do not help axiom to receive that $h_7 = \{\!|z|\!\}^R_{K'}$ for some z and R, and $\{\!|z|\!\}^R_{K'} \sqsubseteq \phi_m$.

3.4.2.1.) T could not have created $\{\!|z|\!\}^R_{K'} \sqsubseteq \phi_m$ because he never encrypts with session key.

3.4.2.2.) If it was created by A, then

$$\{\!|z|\!\}^R_{K'} = \{\!|\mathit{sdec}(h'_7, K') - 1|\!\}^R_{K'}.$$

Let us denote the rhs by t'. Clearly, t' was sent earlier than t, and it must be in a different session of A, as such a message is not sent twice in one session (t was the same kind). Let's denote the first nonce generated by A in the session belonging to t by N_2. And the one generated in the session belonging to t' by N'_2. They are different, because they were generated in different sessions. Applying **a.)** to the session when t was generated, we get that $N_2 = \pi_1\left(\pi_2\left(\pi_2\left(h_4\right)\right)\right)$, where h_4 is the message T received in the session when K' was generated. However, if we apply **a.)** to the session when t' was generated, we get that $N'_2 = \pi_1\left(\pi_2\left(\pi_2\left(h_4\right)\right)\right)$, a contradiction. So $\{\!|z|\!\}^R_{K'} \sqsubseteq \phi_m$ could not have been created by A.

3.4.2.3.) If B created t', then

$$\{\!|z|\!\}^R_{K'} = \{\!|N_3|\!\}^R_{K'}.$$

In this case, $\mathit{sdec}(h_7, K') = N_3$.

3.4.2.3.1.) If $N_3 \neq N$, then, as N_3 was generated by B, for $\vec{M}' \equiv \vec{M}, N_3, K'$, $C'_e(\vec{M}', N)$ is satisfied. Therefore, by our induction hypothesis, $\phi_m, \vec{M}, N_3, K' \not\rhd^{\text{sic2}} N$, but that is the same as $\phi_m, \vec{M}, N_3, K' \not\rhd^{\text{sic2}} N$, and that implies $\phi_m, \vec{M}, N_3 - 1, K' \not\rhd^{\text{sic2}} N$. R is fresh, so by the fresh items do not help axiom we get $\phi_m, \vec{M}, N_3 - 1, K', R \not\rhd^{\text{sic2}} N$, and by function application,

$$\phi_m, \vec{M}, \{\!|N_3 - 1|\!\}^R_{K'} \not\rhd^{\text{sic2}} N.$$

3.4.2.3.1.) If $N_3 = N$, then, the condition $C_e[N]$ obviously implies $C[K']$ from section **c)**. Moreover, as $\vec{M} \equiv \vec{M}, N_3$ satisfies $C[\vec{M}, K']$, we have by **c)** that $\phi_m, \vec{M}, N_3 \not\vdash K'$ and

$$\phi_m, \vec{M}, N_3 - 1 \not\vdash K'.$$

So finally, by the uncorrupted key encrypts securely axiom, as we had $\phi_m, \vec{M}, \not\rhd^{\text{sic2}} N$,

$$\phi_m, \vec{M}, \{\!|N_3 - 1|\!\}^R_{K'} \not\rhd^{\text{sic2}} N.$$

□

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

$$d_r\big(h_2, B, T, N_1, \pi_1\left(\mathit{sdec}(h_6, K_{BT})\right), N_3\big) \sqsubseteq \hat{\phi} \wedge h_2 = A \longrightarrow$$
$$\exists K h_4 h_5 \Big(c_t\big(\pi_1\left(h_4\right),\ \pi_1\left(\pi_2\left(h_4\right)\right),\ T,\ \pi_2\left(\mathit{dec}\big(\pi_2\left(\pi_2\left(\pi_2\left(h_4\right)\right)\right), K_{\pi_1(\pi_2(h_4))T}\big)\right),\ \pi_1\left(\pi_2\left(\pi_2\left(h_4\right)\right)\right),\ K\big) \sqsubseteq \hat{\phi}$$
$$\wedge\, d_i\big(A, Q, T, N_2, \pi_1\left(\pi_2\left(\pi_2\left(\mathit{sdec}(h_5, K_{AT})\right)\right)\right), \mathit{sdec}(h_7, \pi_1\left(\pi_2\left(\pi_2\left(\mathit{sdec}(h_5, K_{AT})\right)\right)\right))\big) \sqsubseteq \hat{\phi}$$
$$\wedge\ \pi_1\left(\mathit{sdec}(h_6, K_{BT})\right) = \pi_1\left(\pi_2\left(\pi_2\left(\mathit{sdec}(h_5, K_{AT})\right)\right)\right) = K$$
$$\wedge\ \pi_1\left(h_4\right) = A \wedge \pi_1\left(\pi_2\left(h_4\right)\right) = B \wedge \pi_2\left(\mathit{dec}\big(\pi_2\left(\pi_2\left(\pi_2\left(h_4\right)\right)\right), K_{\pi_1(\pi_2(h_4))T}\big)\right) = N_1 \wedge \pi_1\left(\pi_2\left(\pi_2\left(h_4\right)\right)\right) = N_2 \Big)$$

Proof of e.)
By the role of B, earlier $c_r\big(h_2, B, T, N_1, \pi_1\left(\mathit{sdec}(h_6, K_{BT})\right)\big)$ was sent. So by **b)**, we have

$$\exists K h_4 \Big(c_t\big(\pi_1\left(h_4\right),\ \pi_1\left(\pi_2\left(h_4\right)\right),\ T,\ \pi_2\left(\mathit{dec}\big(\pi_2\left(\pi_2\left(\pi_2\left(h_4\right)\right)\right), K_{\pi_1(\pi_2(h_4))T}\big)\right),\ \pi_1\left(\pi_2\left(\pi_2\left(h_4\right)\right)\right),\ K\big) \sqsubseteq \phi$$

With

$$\pi_1\left(h_4\right) = A \wedge \pi_1\left(\pi_2\left(h_4\right)\right) = B \wedge \pi_2\left(\mathit{dec}\big(\pi_2\left(\pi_2\left(\pi_2\left(h_4\right)\right)\right), K_{\pi_1(\pi_2(h_4))T}\big)\right) = N_1 \wedge \pi_1\left(\mathit{sdec}(h_6, K_{BT})\right) = K$$

Also, K satisfies C of **c.)**. Hence, the result of **c.)** implies $\phi_m \not\blacktriangleright K$. Moreover, as $h_2 = A$, N_3 satisfies $C_e(N_3)$, and hence it remains secret $\phi_m \not\blacktriangleright^{\mathrm{sic2}} N_3$. However, as $\mathit{sdec}(h_8, \pi_1\left(\mathit{sdec}(h_6, K_{BT})\right))+1 = N_3$, we have that $\phi_m, \mathit{sdec}(h_8, \pi_1\left(\mathit{sdec}(h_6, K_{BT})\right)) \triangleright^{\mathrm{sic2}} N_3$, and by the decryptions do not help axiom, there is a $\{\!|z|\!\}_K^R \sqsubseteq \phi_m$ with $\{\!|z|\!\}_K^R = h_8$.

1.) $\{\!|z|\!\}_K^R$ could not have been sent by T as T never encrypts with session key by his role.

2.) If $\{\!|z|\!\}_K^R$ came from B, then $\{\!|z|\!\}_K^R \equiv \{\!|N_3'|\!\}_K^{R_5'}$ and as $\mathit{sdec}(h_8, \pi_1\left(\mathit{sdec}(h_6, K_{BT})\right)) + 1 = N_3$ by the checks of B, we have

$$N_3' + 1 = N_3.$$

This however is not possible if $N_3' = N_3$ because of the axioms for freshly generated items applied at the point when they were both fresh. It is also not possible if $N_3 = N_3$ because of the properties of addition/subtraction.

3.) If $\{\!|z|\!\}_K^R$ was sent by A, then

$$\{\!|z|\!\}_K^R \equiv \{\!|\mathit{sdec}(h_7, \pi_1\left(\pi_2\left(\pi_2\left(\mathit{sdec}(h_5, K_{AT})\right)\right)\right)) - 1|\!\}_{\pi_1(\pi_2(\pi_2(\mathit{sdec}(h_5, K_{AT}))))}^{R_5}.$$

So

$$K = \pi_1\left(\pi_2\left(\pi_2\left(\mathit{sdec}(h_5, K_{AT})\right)\right)\right).$$

As $\mathit{sdec}(h_8, \pi_1\left(\mathit{sdec}(h_6, K_{BT})\right)) + 1 = N_3$, we have

$$\mathit{sdec}(h_7, \pi_1\left(\pi_2\left(\pi_2\left(\mathit{sdec}(h_5, K_{AT})\right)\right)\right)) = N_3.$$

By the roles of A, we also must have

$$d_i\big(A, Q, T, N_2, \pi_1\left(\pi_2\left(\pi_2\left(\mathit{sdec}(h_5, K_{AT})\right)\right)\right), \mathit{sdec}(h_7, \pi_1\left(\pi_2\left(\pi_2\left(\mathit{sdec}(h_5, K_{AT})\right)\right)\right))\big) \sqsubseteq \phi$$

and

$$c_i\big(A, Q, T, N_2, \pi_1\left(\pi_2\left(\pi_2\left(\mathit{sdec}(h_5, K_{AT})\right)\right)\right)\big) \sqsubseteq \phi.$$

It remains to be proven that $Q = B$.

By **a.)**, we have that

$$\exists h_4' \Big(c_t\big(\pi_1\left(h_4'\right),\ \pi_1\left(\pi_2\left(h_4'\right)\right),\ T,\ \pi_2\left(dec\big(\pi_2\left(\pi_2\left(h_4'\right)\right), K_{\pi_1\left(\pi_2\left(h_4'\right)\right)T}\big)\right),\ \pi_1\left(\pi_2\left(\pi_2\left(h_4'\right)\right)\right),\ K\big) \sqsubseteq \hat{\phi} \Big),$$

where $\pi_1\left(\pi_2\left(h_4'\right)\right) = Q$. However, as K cannot agree in two sessions of T, this must be the same session when h_4 was received. So $h_4' = h_4$, and

$$B = \pi_1\left(\pi_2\left(h_4\right)\right) = Q$$

and that is what we wanted.

□