NSL Verification and Attacks Agents Playing Both Roles

Pedro Adão Gergei Bana

Abstract

Background: [2] and eprint version: [1]

1 The Axioms

- **Equality is a Congruence.** The first axiom says that the equality is a congruence relation:
  - $x = x$, and the substitutability (congruence) property of equal terms holds for predicates.
- **Axioms for the Derivability Predicate.**
  - 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 (if interpretations of function symbols are PT): $\hat{\phi}, \vec{x} \rhd f(\vec{x})$
- **Axioms for Randomly Generated Items.**
  - No telepathy (if fresh items are not guessable non-negligibly): $\mathsf{fresh}(x; \hat{\phi}) \longrightarrow \hat{\phi} \not\rhd x$
  - Fresh items are independent and hence contain no information about other items:

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

- **Equations for the fixed function symbols**:
  - $dec(\{x\}^R_{eK}, dK) = x$;
  - $\pi_1(\langle x, y\rangle) = x; \quad \pi_2(\langle x, y\rangle) = y;$
  - $\tau_1(\langle x, y, z\rangle) = x; \quad \tau_2(\langle x, y, z\rangle) = y; \quad \tau_3(\langle x, y, z\rangle) = z;$
- **Special to IND-CCA2 Encryption.** Let $x_1, ..., x_n \preccurlyeq \hat{\phi} \equiv x_1 \preccurlyeq \hat{\phi} \wedge ... \wedge x_n \preccurlyeq \hat{\phi}$. If encryption is IND-CCA2 secure:

– **Secrecy of CCA2 Encryption.** If the encryption scheme is IND-CCA2, then the following formula is computationally sound.

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

– **Non-Malleability of CCA2 Encryption.** Let us now consider the case of non-malleability and suppose that we have pairing as before. Let $f_1, ..., f_n$ be the rest of the non-0-arity function symbols not in $\mathcal{F}_c \cup \mathcal{F}_d$. Let $\mathsf{MayCor}_{\mathrm{CCA2}}(u; \hat{\phi}, \vec{x})$ be a constraint meaning that u is a term that is paired-together all terms which occur in $\phi, \vec{x}$ not guarded by an honest encryption, and immediately under one of the functions $f_1, \ldots, f_n$ or immediately under an honest decryption. (Note, that since in different parts of the computational execution, the number of such terms may differ, it is not possible to replace u with a list in the formula.)

If the encryption scheme is IND-CCA2, then the following formula is computationally sound.

$$\exists u(\mathsf{MayCor}_{\mathrm{CCA2}}(u; \hat{\phi}, \vec{x}) \wedge \hat{\phi}, \vec{x}, u \not\rhd N) \ \wedge \ \mathsf{RandGen}(N) \ \wedge \ \mathsf{RandGen}(K) \\ \wedge \ \hat{\phi} \rhd eK \ \wedge \ \vec{x} \preccurlyeq \hat{\phi} \ \wedge \ N \sqsubseteq \hat{\phi}, \vec{x} \ \wedge \ \hat{\phi}, \vec{x} \rhd y \ \wedge \ \hat{\phi}, \vec{x}, \mathit{dec}(y, dK) \rhd N \\ \longrightarrow \ \exists K'(\mathsf{RandGen}(K') \wedge dK' \sqsubseteq_{\mathit{d}} \hat{\phi}, \vec{x}) \ \vee \ \exists x R(y = \{x\}^R_{eK} \wedge \{x\}^R_{eK} \sqsubseteq \hat{\phi}, \vec{x})$$

- Special to c_i, c_r. These axioms are trivial as c_i, c_r are just ideal functions introduced for convenience to represent the agents' view of a session. (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 subpart of a term:
    $\hat{\phi}, \vec{x} \rhd c(x, y, z, w) \longrightarrow c(x, y, z, w) \sqsubseteq \hat{\phi} \vee x_1 = c(x, y, z, w) \vee \ldots \vee x_l = c(x, y, z, w)$
  - c cannot be equal to anything else: If the outermost function symbol of a term T is something different from c, then $c(x, y, z, w) \neq T$.

2 NSL Protocol Definition

We define the roles of principals as follows: the initiator, communicating with intended party Q, does the following sequence of steps in session i (denoted by $Init^{A}_{NSL}[i, A, Q, N_1, h_1, h_3, R_1, R_3]$):

1. Receives handle h_1 that triggers the start of the session with intended party Q;
2. A generates nonce N_1;
3. A sends $\{N_1, A\}^{R_1}_{eK_Q}$;
4. A receives h_3, and checks:
   - $\tau_1\left(dec(h_3, dK_A)\right) = N_1$
   - $\tau_3\left(dec(h_3, dK_A)\right) = Q$;
5. A sends $\{\tau_2\left(dec(h_3, dK_A)\right)\}^{R_3}_{eK_Q}$;
6. A sends $c_i\big(A, Q, N_1, \tau_2\left(dec(h_3, dK_A)\right)\big)$.

For verification purposes, let c_i be a special function symbol, that takes as arguments A, Q, N_1, n_2, respectively who commits for whom and the corresponding nonces. $c_i(A, Q, N_1, n_2)$ is sent immediately after $\{N_1, n_2, B\}^{R_3}_{eK_A}$. For the responder, there is a similar commitment: at the end of the protocol, B emits (as a last message) $c_r(Q, B, n_1, N_2)$.

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

1. B receives some h_2 from the adversary and checks:
   - $\exists Q\,.\,\left(W(Q) \;\wedge\; Q = \pi_2\left(dec(h_2, dK_B)\right)\right)$ (W is a constraint for constants that are agent names);
2. B generates nonce N_2;
3. B sends $\{\pi_1\left(dec(h_2, dK_B)\right), N_2, B\}^{R_2}_{eK_Q}$;
4. B receives h_4, and checks if $dec(h_4, dK_B) = N_2$;
5. B sends $c_r(\pi_2\left(dec(h_2, dK_B)\right), B, \pi_1\left(dec(h_2, dK_B)\right), N_2)$.

We assume that the names and keys of honest names are assigned honestly at the beginning. That is, this proof does not account for e.g. assigned name attacks. This is not a limitation of the technique, the proof would just be longer without this assumption.

3 Auxiliary Propositions

Proposition 3.1 *For all i, if $\phi_m, \vec{x}, \pi_i(x) \rhd y$ then $\phi_m, \vec{x}, x \rhd y$.*

Proposition 3.2 *For all i, if $\phi_m, \vec{x}, \tau_i(x) \rhd y$ then $\phi_m, \vec{x}, x \rhd y$.*

Proposition 3.3 *For all i, if $\phi_m, \vec{x}, \pi_i(h) \rhd y$ and $\phi_m, \vec{x} \rhd h$, then $\phi_m, \vec{x} \rhd y$.*

Proposition 3.4 *For all i, if $\phi_m, \vec{x}, \tau_i(h) \rhd y$ and $\phi_m, \vec{x} \rhd h$, then $\phi_m, \vec{x} \rhd y$.*

4 Secrecy (Both Roles)

The aim of the secrecy proof is to show that nonces N generated and sent between honest agents remain secret. Throughout this section we will denote honest agents by $X, Y, X', Y', \ldots$ and arbitrary agents by $Q, Q', \ldots$. We will denote by $\mathcal{H}$ the set of all honest agents. The fact that N is a nonce generated and sent by an honest initiator X to an honest responder Y in the NSL protocol can be expressed as

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

and that a nonce N is generated and sent by an honest responder X to an honest initiator Y can be expressed as

$$\exists hR\,.\,\big(\{\pi_1\left(dec(h, dK_X)\right), N, X\}^R_{eK_Y} \sqsubseteq \hat{\phi}\big).$$

Such nonces can be characterized by the condition

$$\begin{aligned} C_{X,Y}[N] \stackrel{def}{\equiv} \mathsf{RandGen}(N) \wedge \big(&\exists R\,.\,\{N, X\}^R_{eK_Y} \sqsubseteq \hat{\phi} \\ &\vee \left(\exists hR\,.\,\{\pi_1\left(dec(h, dK_Y)\right), N, Y\}^R_{eK_X} \sqsubseteq \hat{\phi}\right)\big) \end{aligned}$$

where $X, Y \in \mathcal{H}$. We write $C[N]$ when X, Y are clear from the context.

The secrecy property we aim at is $\forall N\big(C[N] \longrightarrow \hat{\phi} \not\rhd N\big)$, meaning that such nonces cannot be derived by the adversary. It is equivalent to show that its negation,

$$\exists N\big(C[N] \wedge \hat{\phi} \rhd N\big) \tag{1}$$

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

Suppose that the symbolic trace in question was generated by the exchange of n messages. At the end of the trace, the frame ϕ contains n terms. Let us denote the frames at each node of this trace by $\phi_0, \phi_1, \phi_2, \ldots, \phi_n$ where each frame contains one more term than the previous one.

Satisfaction of $C_{X,Y}[N]$ by this trace means that either $\{N, X\}^R_{eK_Y}$ or $\{\pi_1\left(dec(h, dK_Y)\right), N, Y\}^R_{eK_X}$ appears in frame ϕ_n for some handle h and randomness R. Let us fix such N.

Notice that honest participants may generate other nonces. Let $\vec{x} \equiv N_1, \ldots, N_l$ be the list of all nonces generated by either X or Y that are different from N (possibly intended to each other, or possibly intended for other possibly malicious agents). These nonces satisfy the following condition:

$$\begin{aligned} &C'_{X,Y}[N_1, \ldots, N_l, N] \stackrel{def}{\equiv} \\ &\stackrel{def}{\equiv} \bigwedge_{i=1}^{l} \left(\begin{array}{l} \mathsf{RandGen}(N_i) \ \wedge \ N \neq N_i \wedge \\ \big(\exists QR.\{N_i, X\}^R_{eK_Q} \sqsubseteq \hat{\phi} \ \vee \exists QhR.\{\pi_1\left(dec(h, dK_Y)\right), N_i, Y\}^R_{eK_Q} \sqsubseteq \hat{\phi}\big) \end{array} \right) \end{aligned}$$

We will carry out an inductive proof on the length of ϕ_n. In order to avoid loops in the proof, instead of $\exists N\big(C[N] \wedge \hat{\phi} \rhd N\big)$, one will prove that

$$\exists N \exists \vec{x}\big(C[N] \wedge C'[\vec{x}, N] \wedge \hat{\phi}, \vec{x} \rhd N\big) \tag{2}$$

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

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

is inconsistent with the axioms and agent checks.

Namely, we show that having fixed N such that $C[N]$ holds, if for some $m < n$, $\exists\vec{x}\big(C'[\vec{x}, N] \wedge \phi_m, \vec{x} \rhd N\big)$ holds together with the axioms and agent checks, then

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

also holds. Then, as at $m = 0$ the formula contradicts no-telepathy axiom, our result follows. This is what the following theorem says. Notice that within C and C', $\hat{\phi}$ is always ϕ_n and not ϕ_m.

Proposition 4.1 *Let $\phi_0, \phi_1, \phi_2, \ldots, \phi_n$ be an execution of NSL protocol, N be such that $C[N]$ is satisfied, and let $m < n$ (consequently all agent checks up to step n are satisfied).*

If for all $\vec{x}$ such that $C'[\vec{x}, N]$ and $\phi_{m+1}, \vec{x} \rhd N$ holds, then the axioms together with the protocol roles imply (by FOL deduction rules) that $\phi_m, \vec{x}' \rhd N$ holds for all $\vec{x}'$ satisfying $C'[\vec{x}', N]$. + some additional conditions to prevent attacks

Proof: Consider first $\exists u(\mathsf{MayCor}_{\mathrm{CCA2}}(u; \hat{\phi}, \vec{x}) \wedge \hat{\phi}, \vec{x}, u \not\rhd N)$ in the non-malleability axiom. Since there are no other function symbols in case of the NSL protocol, we only have to look inside of the decryption function. However, in the NSL protocol, the decryption function is only applied to handles, which came from the adversary, and can be computed from the frame. Hence, for any u satisfying $\mathsf{MayCor}_{\mathrm{CCA2}}(u; \hat{\phi}, \vec{x})$, u is just a list of handles. Since handles are all derivable from the frames, we have $\hat{\phi}, \vec{x} \rhd u$, and hence, by transitivity, $\hat{\phi}, \vec{x}, u \not\rhd N$ is equivalent with $\hat{\phi}, \vec{x} \not\rhd N$. Moreover, decryption keys are never sent out. Hence, for the NSL protocol, the non-malleability axiom can be replaced by:

$$\begin{aligned}
&\mathsf{RandGen}(N) \ \wedge \ \mathsf{RandGen}(K) \\
&\wedge \ eK \sqsubseteq \hat{\phi} \ \wedge \ \vec{x} \preccurlyeq \hat{\phi} \ \wedge \ N \sqsubseteq \hat{\phi}, \vec{x} \wedge \hat{\phi}, \vec{x}, x \rhd \ \wedge \hat{\phi}, \vec{x} \rhd y \ \wedge \ \hat{\phi}, \vec{x}, \mathit{dec}(y, dK) \rhd N \\
&\longrightarrow \ \exists x R(y = \{x\}^R_{eK} \wedge \{x\}^R_{eK} \sqsubseteq \hat{\phi}, \vec{x}) \ \vee \ \hat{\phi}, \vec{x} \rhd N
\end{aligned}$$

Let us assume that there is a finite list of nonces $\vec{x}^\star \equiv N^\star_1, \ldots, N^\star_l$ such that $C'[\vec{x}^\star, N]$ and

$$\phi_{m+1}, N^\star_1, \ldots, N^\star_l \rhd N$$

is satisfied in some model. We will show that this, together with the honest agent checks and the axioms, imply that there exists nonces $\vec{x}^\dagger \equiv N^\dagger_1, \ldots, N^\dagger_{l'}$ with $C'[\vec{x}^\dagger, N]$ and

$$\phi_m, N^\dagger_1, \ldots, N^\dagger_{l'} \rhd N.$$

Let t be the last term in ϕ_{m+1}, that is, $\phi_{m+1} \equiv \phi_m, t$, and so by our assumption $\phi_m, t, \vec{x}^\star \rhd N$. By commutativity, we get

$$\phi_m, \vec{x}^\star, t \rhd N. \tag{3}$$

Since t is in frame ϕ_{m+1} it was necessarily sent by an honest agent that can be either an initiator or a responder. We have then that either for some (honest) initiator X

1. $t \equiv \{N_1, X\}^{R_1}_{eK_Q}$ with an arbitrary agent Q, freshly generated nonce N_1, and freshly generated randomness R_1; or

2. $t \equiv \{\tau_2\left(dec(h_3, dK_X)\right)\}^{R_3}_{eK_Q}$ for some handle h_3, arbitrary agent Q, freshly generated nonce N_1, and freshly generated randomness R_3 such that $\phi_m \rhd h_3$, $N_1 = \tau_1\left(dec(h_3, dK_X)\right)$, and $Q = \tau_3\left(dec(h_3, dK_X)\right)$; or
3. $t \equiv c_i\left(X, Q, N_1, \tau_2\left(dec(h_3, dK_X)\right)\right)$ for some handle h_3, freshly generated nonce N_1, and arbitrary agent Q, such that $\phi_m \rhd h_3$, $N_1 = \tau_1\left(dec(h_3, dK_X)\right)$, and $Q = \tau_3\left(dec(h_3, dK_X)\right)$;

or for some (honest) responder X

4. $t \equiv \{\pi_1\left(dec(h_2, dK_X)\right), N_2, X\}^{R_2}_{eK_Q}$ for some handle h_2 with $\phi_m \rhd h_2$, agent Q such that $Q = \pi_2\left(dec(h_2, dK_X)\right)$, freshly generated nonce N_2, and freshly generated randomness R_2; or
5. $t \equiv c_r(\pi_2\left(dec(h_2, dK_X)\right), X, \pi_1\left(dec(h_2, dK_X)\right), N_2)$ for some handle h_2 with $\phi_m \rhd h_2$ and $W(\pi_2\left(dec(h_2, dK_X)\right))$, and freshly generated nonce N_2.

Remark: *We will always use the same notation as in the definition of the protocol. However, since we may have different instances of the protocol running at the same time, we will use superscripts to distinguish those runs, for example, N_1 is generated by honest initiator X and we will use $N_1', N_1'', \ldots$ for the nonces generated by honest initiators $X', X'', \ldots$.*

Let us analyze all possible 5 cases.

1.) An initiator X sends $t \equiv \{N_1, X\}^{R_1}_{eK_Q}$ with an arbitrary agent Q, generated nonce N_1, and freshly generated randomness R_1.[1]

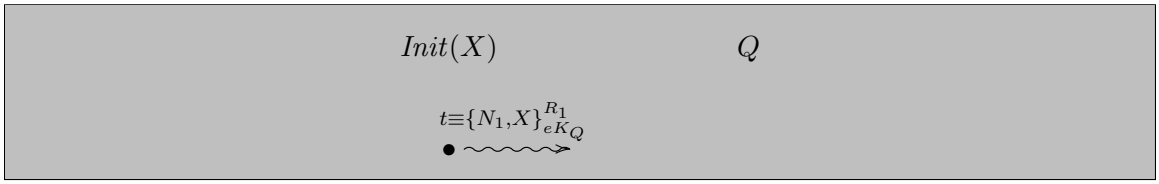

Figure 1: Case 1.) $t \equiv \{N_1, X\}^{R_1}_{eK_Q}$ is the first message sent by the Initiator X.

Let us consider two cases:

1.1.) $Q \in \mathcal{H}$. Applying the secrecy axiom with $\phi_m, \vec{x}^\star, \{N_1, X\}^{R_1}_{eK_Q} \rhd N$ and $dK_Q \not\sqsubseteq_{\mathit{d}} \phi_m, \vec{x}^\star, N_1, X$ one gets the intended result $\phi_m, \vec{x}^\star \rhd N$.

1.2.) $Q \notin \mathcal{H}$. Notice that $N_1 \not\equiv N$, as N was generated in a session between two honest users (it satisfies $C[N]$) and N_1 was generated in a session with $Q \notin \mathcal{H}$. In this case, $N_1 \neq N$, otherwise as $\phi_0, N \rhd N$ holds by self derivability, $\phi_0, N_1 \rhd N$ also holds by the congruence of $=$, and then

[1] We will illustrate our cases with diagrams. Solid arrows represent messages that were sent or received by the honest agents. Dotted arrows correspond to exchanged messages or messages sent by an attacker.

$\phi_0 \rhd N$ by freshly generated items, but that contradicts the no-telepathy axiom. Then,

i. $\phi_m, \vec{x}^\star, \{N_1, X\}^{R_1}_{eK_Q} \rhd N$ by (3)

ii. $\phi_m, \vec{x}^\star, \{N_1, X\}^{R_1}_{eK_Q}, N_1, X, eK_Q, R_1 \rhd N$ by IC (i).

iii. $\phi_m, \vec{x}^\star, N_1, X, eK_Q, R_1 \rhd \{N_1, X\}^{R_1}_{eK_Q}$ by $\{\cdot\}$-FD

iv. $\phi_m, \vec{x}^\star, N_1, X, eK_Q, R_1 \rhd N$ by T(iii,ii)

v. $\phi_m, \vec{x}^\star, N_1, eK_Q, R_1 \rhd N$ X public in ϕ_0 (iv)

vi. $\phi_m, \vec{x}^\star, N_1, R_1 \rhd N$ eK_Q public in ϕ_0 (v)

vii. $\phi_m, \vec{x}^\star, N_1 \rhd N$ by freshness of R_1(vi)

viii. $\phi_m, \vec{x}^\star \rhd N$ by freshness of N_1(vii) and $N_1 \neq N$

2.) An initiator X sends $t \equiv \{\tau_2\,(dec(h_3, dK_X))\}^{R_3}_{eK_Q}$ for some handle h_3 with $\phi_m \rhd h_3$, $N_1 = \tau_1\,(dec(h_3, dK_X))$, and $Q = \tau_3\,(dec(h_3, dK_X))$, and freshly generated randomness R_3.

Remark: *Note that from the equalities above one might be wrongly led to claim that for some R and n we have some $t' = \langle N_1, n, Q\rangle$ and $h_3 = \{t'\}^R_{eK_X}$. This is however not true as the decrypted term may not have been created as a proper encryption, and the projected "triple" may not have been originally a triple. If they are the correct encryption and triple, then these equalities hold, otherwise they do not. In fact, we do not have any axioms that allow such a conclusion from the foregoing. Our only possible conclusion is that whatever t' was received, it returns N_1 and Q whenever one applies respectively $\tau_1\,(t')$ and $\tau_3\,(t')$.*

In order to simplify notation we will use $t' = \langle\!\langle x, y, z\rangle\!\rangle$ to express that t' *looks like* the triple $\langle x, y, z\rangle$; t' is not necessarily the triple but parses like it, that is, $x = \tau_1\,(t')$, $y = \tau_2\,(t')$, and $z = \tau_3\,(t')$. Similarly for pairs. Furthermore, if we omit the random input of an encryption, that will mean something that decrypts to the plaintext. Accordingly, let us introduce the following abbreviations:

$$u = \langle\!\langle x, y, z\rangle\!\rangle \stackrel{def}{\equiv} x = \tau_1\,(u) \wedge y = \tau_2\,(u) \wedge z = \tau_3\,(u)$$

$$u = \langle\!\langle x, y\rangle\!\rangle \stackrel{def}{\equiv} x = \pi_1\,(u) \wedge y = \pi_2\,(u)$$

$$u = \{x\}_{eK_X} \stackrel{def}{\equiv} dec(u, dK_X) = x$$

In our case, and for $n \stackrel{def}{\equiv} \tau_2\,(dec(h_3, dK_X))$, we have that $t' = \langle\!\langle N_1, n, Q\rangle\!\rangle$.
Case $Q \in \mathcal{H}$ is similar to case 1.1. Let us then consider the case $Q \notin \mathcal{H}$.

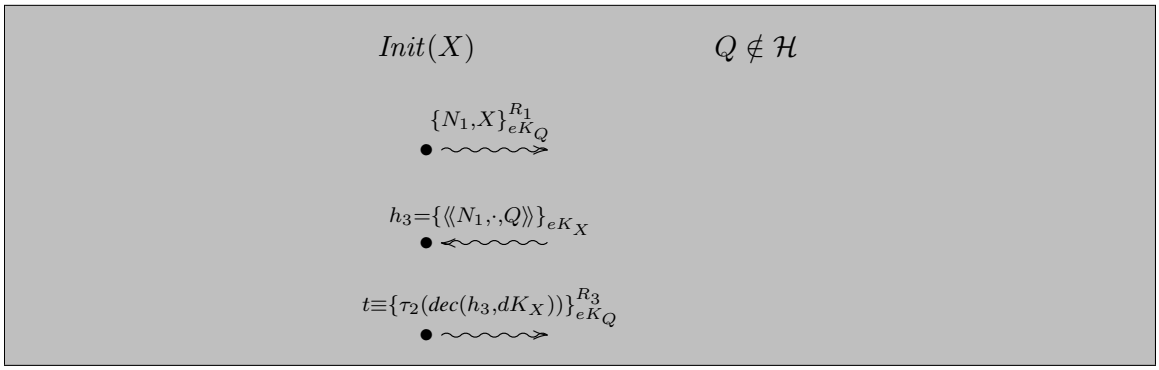

Figure 2: Case 2.) $t \equiv \{\tau_2\left(dec(h_3, dK_X)\right)\}^{R_3}_{eK_Q}$ is the last message sent by the Initiator X.

i.	$\phi_m, \vec{x}^\star, \{\tau_2\left(dec(h_3, dK_X)\right)\}^{R_3}_{eK_Q} \rhd N$	by (3)
ii.	$\phi_m, \vec{x}^\star, \{\tau_2\left(dec(h_3, dK_X)\right)\}^{R_3}_{eK_Q}, \tau_2\left(dec(h_3, dK_X)\right), eK_Q, R_3 \rhd N$	by IC(i)
iii.	$\phi_m, \vec{x}^\star, \tau_2\left(dec(h_3, dK_X)\right), eK_Q, R_3 \rhd \{\tau_2\left(dec(h_3, dK_X)\right)\}^{R_3}_{eK_Q}$	by $\{\cdot\}$-FD
iv.	$\phi_m, \vec{x}^\star, \tau_2\left(dec(h_3, dK_X)\right), eK_Q, R_3 \rhd N$	by T(iii,ii)
v.	$\phi_m, \vec{x}^\star, \tau_2\left(dec(h_3, dK_X)\right), R_3 \rhd N$	eK_Q public in ϕ_0 (iv)
vi.	$\phi_m, \vec{x}^\star, \tau_2\left(dec(h_3, dK_X)\right) \rhd N$	by freshness of R_3(v)
vii.	$\phi_m, \vec{x}^\star, dec(h_3, dK_X) \rhd N$	by Proposition 3.2 applied to (vi)
viii.	$\phi_m \rhd h_3$	by hypothesis
ix.	$\phi_m, \vec{x}^\star \rhd h_3$	by IC(viii)
x.	$\phi_m, \vec{x}^\star \rhd N$ or $\exists x' R'.\left(h_3 = \{x'\}^{R'}_{eK_X} \wedge \{x'\}^{R'}_{eK_X} \sqsubseteq \phi_m, \vec{x}^\star\right)$	by NM(ix,vii)

The first immediately implies the result so let us consider the second. Notice also that since $\vec{x}^\star$ is a list of nonces, one can omit it and equivalently obtain

$$\exists x' R'.\left(h_3 = \{x'\}^{R'}_{eK_X} \wedge \{x'\}^{R'}_{eK_X} \sqsubseteq \phi_m\right)$$

Remark: *Note that only at this point we do know that h_3 is an honest encryption. Before, we only knew how h_3 was decrypted, but we did not know if it was created as an honest encryption.*

By hypothesis 2.) and the derivation above it follows that for $n \stackrel{def}{=} \tau_2\left(dec(h_3, dK_X)\right)$,

$$x' = dec(h_3, dK_X) \stackrel{2.}{=} \langle\langle N_1, n, Q\rangle\rangle \qquad \text{and} \qquad \phi_m, \vec{x}^\star, x' \rhd N. \tag{4}$$

Let us analyze who could have sent $\{x'\}^{R'}_{eK_X}$ as it is in the frame ϕ_m.

Remark: *Note that at this stage we do know that h_3 was created as an honest encryption but we still do not know if $\{x'\}^{R'}_{eK_X}$ was indeed (correctly) sent as a response to the first message of X, or if it was sent at some other stage. For that, we consider the two dotted messages in Figure 3.*

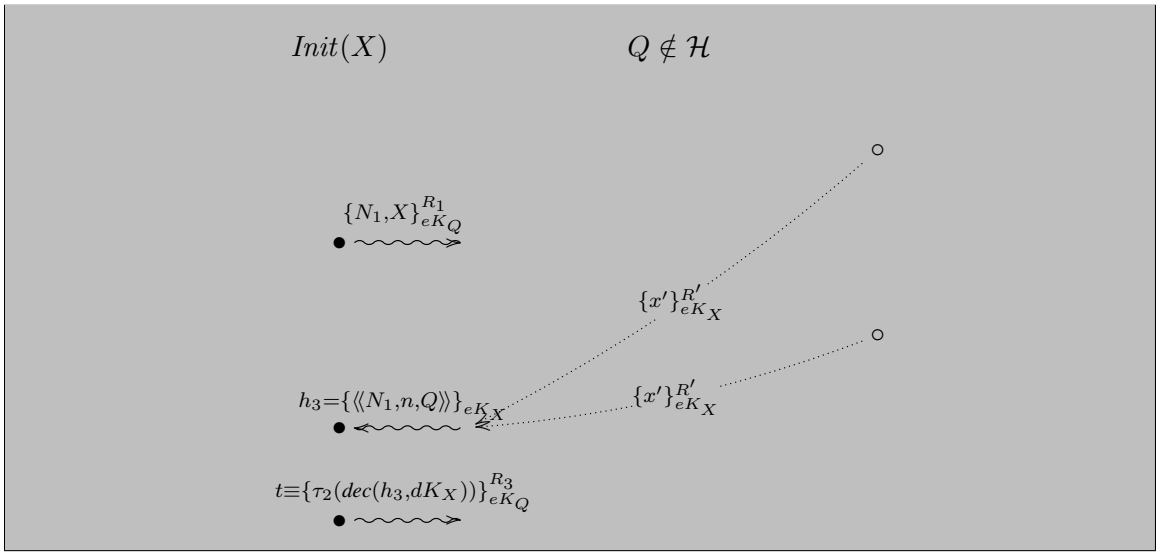

Figure 3: Case 2.x.) Who sent the $\{x'\}^{R'}_{eK_X}$ that matches the h_3 received by the Initiator X.

There are again 5 possible cases for $\{x'\}^{R'}_{eK_X}$: it was sent by some (honest) initiator X'

2.1. $\{x'\}^{R'}_{eK_X} \equiv \{N'_1, X'\}^{R'_1}_{eK_{Q'}}$ with an some agent Q', freshly generated nonce N'_1, and freshly generated randomness R'_1; or

2.2. $\{x'\}^{R'}_{eK_X} \equiv \{\tau_2\left(dec(h'_3, dK_{X'})\right)\}^{R'_3}_{eK_{Q'}}$ for some handle h'_3, freshly generated nonce N'_1, arbitrary agent Q', and freshly generated randomness R'_3 such that $\phi_m \rhd h'_3$, $N'_1 = \tau_1\left(dec(h'_3, dK_{X'})\right)$, and $Q' = \tau_3\left(dec(h'_3, dK_{X'})\right)$; or

2.3. $\{x'\}^{R'}_{eK_X} \equiv c_i\left(X', Q', N'_1, \tau_2\left(dec(h'_3, dK_{X'})\right)\right)$ for some handle h'_3, freshly generated nonce N'_1, and arbitrary agent Q', such that $\phi_m \rhd h'_3$, $N'_1 = \tau_1\left(dec(h'_3, dK_{X'})\right)$, and $Q' = \tau_3\left(dec(h'_3, dK_{X'})\right)$;

or by some (honest) responder X'

2.4. $\{x'\}^{R'}_{eK_X} \equiv \{\pi_1\left(dec(h'_2, dK_{X'})\right), N'_2, X'\}^{R'_2}_{eK_{Q'}}$ for some handle h'_2 with $\phi_m \rhd h'_2$, agent Q' such that $Q' = \pi_2\left(dec(h'_2, dK_{X'})\right)$, freshly generated nonce N'_2, and freshly generated randomness R'_2; or

2.5. $\{x'\}^{R'}_{eK_X} \equiv c_r(\pi_2\left(dec(h'_2, dK_{X'})\right), X', \pi_1\left(dec(h'_2, dK_{X'})\right), N'_2)$ for some handle h'_2 with $\phi_m \rhd h'_2$ and $W(\pi_2\left(dec(h'_2, dK_{X'})\right))$, and freshly generated nonce N'_2.

2.1.) In this case $\langle N'_1, X'\rangle \equiv x' \stackrel{(4)}{=} \langle\!\langle N_1, n, Q\rangle\!\rangle$ and so $\phi_0, N'_1, X' \rhd N_1$ and $\phi_0, N'_1 \rhd N_1$ as X' is public.

If $N'_1 \not\equiv N_1$ then one applies the freshness axiom and obtains $\phi_0 \rhd N_1$ contradicting the no-telepathy axiom. So we necessarily have that $N'_1 \equiv N_1$.

Since N_1 was generated and sent in a single session we necessarily have $\{N_1, X\}^{R_1}_{eK_Q} \equiv \{N'_1, X'\}^{R'_1}_{eK_{Q'}} \stackrel{2.1.}{\equiv} \{x'\}^{R'}_{eK_X}$ that implies $X \equiv Q \notin \mathcal{H}$ that is a contradiction.

2.2.) This is a non-trivial case and we address it after the others.

2.3.) $c_i(\cdot)$ can never match the encryption $\{x'\}^{R'}_{eK_X}$ as c_i is (syntactically) not the encryption function symbol.

2.4.) In this case $\langle \pi_1\left(dec(h'_2, dK_{X'})\right), N'_2, X'\rangle \equiv x' \overset{(4)}{=} \langle\!\langle N_1, n, Q\rangle\!\rangle$ which implies that $X' = \tau_3\left(x'\right) = Q \notin \mathcal{H}$ that is a contradiction.

2.5.) Same as 2.3.

2.2.—Recap) Let us now analyze this case, that is, $\{x'\}^{R'}_{eK_X} \overset{2.2.}{\equiv} \{\tau_2\left(dec(h'_3, dK_{X'})\right)\}^{R'_3}_{eK_{Q'}}$ for some h'_3, N'_1, Q', R'_3, such that $\phi_m \rhd h'_3$, and $N'_1 = \tau_1\left(dec(h'_3, dK_{X'})\right)$, and $Q' = \tau_3\left(dec(h'_3, dK_{X'})\right)$. It follows then that $Q' \equiv X$ and $R'_3 \equiv R'$.

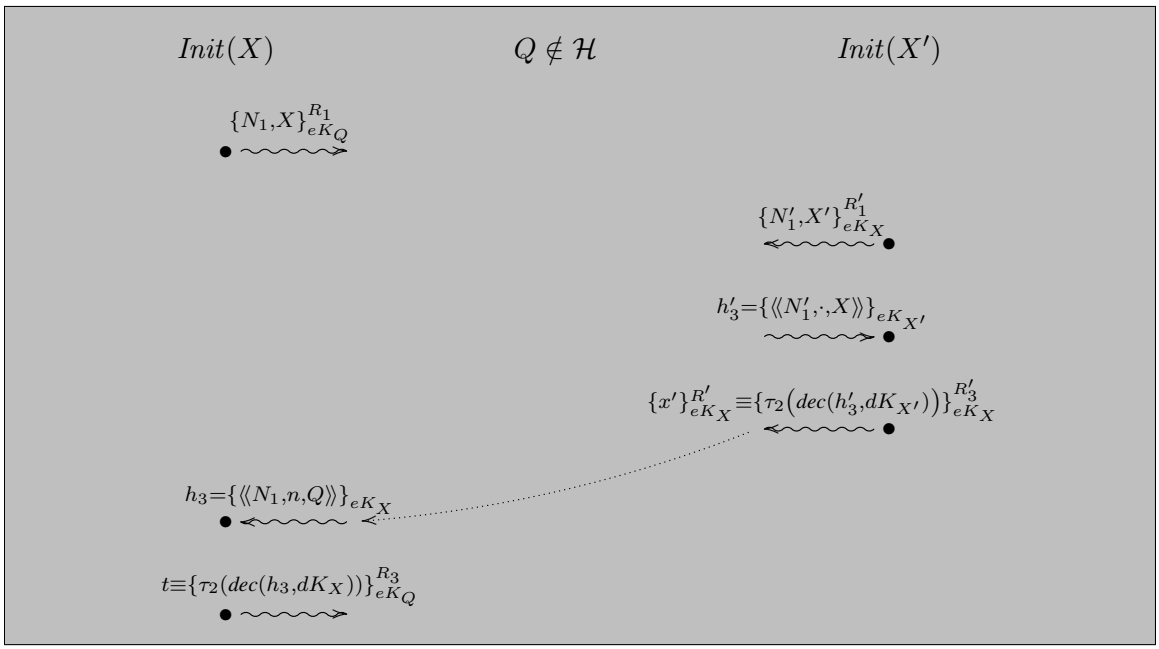

Figure 4: Case 2.2.) where $\{x'\}^{R'}_{eK_X}$ is the last message sent by the Initiator X'.

i. $\phi_m, \vec{x}^\star, x' \rhd N$ — by (4)

ii. $\phi_m, \vec{x}^\star, \tau_2\left(dec(h'_3, dK_{X'})\right) \rhd N$ — by congruence of $\equiv$ applied to (i) and 2.2.

iii. $\phi_m, \vec{x}^\star, dec(h'_3, dK_{X'}) \rhd N$ — by Proposition 3.2 applied to (ii)

iv. $\phi_m \rhd h'_3$ — by hypothesis

v. $\phi_m, \vec{x}^\star \rhd h'_3$ — by IC(iv)

vi. $\phi_m, \vec{x}^\star \rhd N$ or $\exists x'' R''.\left(h'_3 = \{x''\}^{R''}_{eK_{X'}} \wedge \{x''\}^{R''}_{eK_{X'}} \sqsubseteq \phi_m, \vec{x}^\star\right)$ — by NM(v,iii)

The first immediately implies the result so let us consider the second. Notice also that since $\vec{x}^\star$ is a list of nonces, one can omit it and equivalently obtain

$$\exists x'' R''.\left(h'_3 = \{x''\}^{R''}_{eK_{X'}} \wedge \{x''\}^{R''}_{eK_{X'}} \sqsubseteq \phi_m\right)$$

By the derivation above and since we obtained earlier that $Q' \equiv X$, it follows that for $n' \stackrel{def}{=} \tau_2\left(dec(h'_3, dK_{X'})\right) \stackrel{2.2.}{\equiv} x' \stackrel{(4)}{=} \langle\langle N_1, n, Q\rangle\rangle$,

$$x'' = dec(h'_3, dK_{X'}) \stackrel{2.2.}{=} \langle\langle N'_1, n', Q'\rangle\rangle = \langle\langle N'_1, n', X\rangle\rangle \qquad \text{and} \qquad \phi_m, \vec{x}^\star, x'' \rhd N. \tag{5}$$

The second formula follows from Step (iii) of the previous derivation.

Let us analyze who could have sent $\{x''\}^{R''}_{eK_{X'}}$ as it is in the frame ϕ_m.

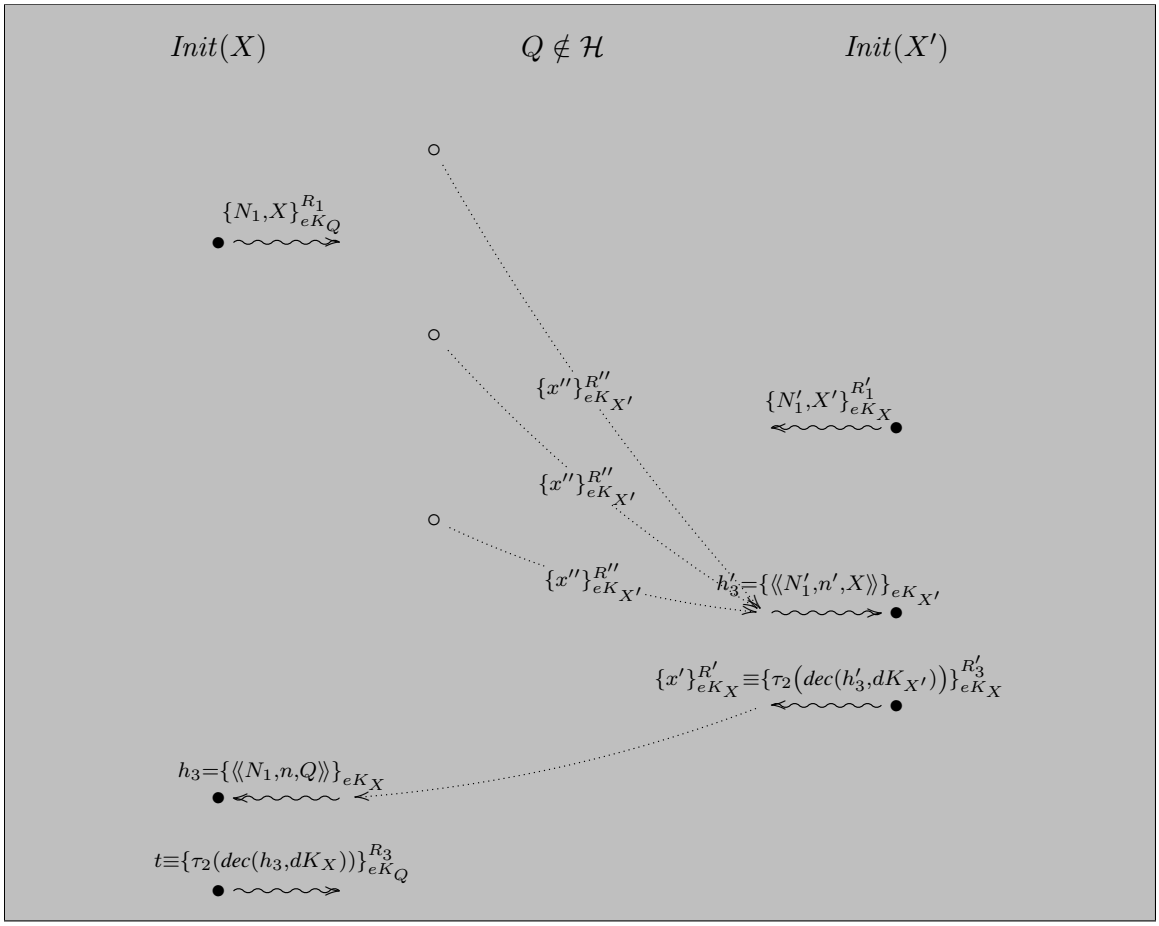

Figure 5: Case 2.2.x.) Who sent $\{x''\}^{R''}_{eK_{X'}}$ that matches the h'_3 received by the Initiator X'.

Remark: *Note again that at this stage we do not know if $\{x''\}^{R''}_{eK_{X'}}$ was indeed (correctly) sent as a response to the first message of X', or if it was sent at some other stage. For that, we consider the three dotted messages in Figure 5.*

There are again 5 possible cases for $\{x''\}^{R''}_{eK_{X'}}$: it was sent by some (honest) initiator X''

2.2.1. $\{x''\}^{R''}_{eK_{X'}} \equiv \{N''_1, X''\}^{R''_1}_{eK_{Q''}}$ with an arbitrary agent Q'', freshly generated nonce N''_1, and freshly generated randomness R''_1; or

2.2.2. $\{x''\}^{R''}_{eK_{X'}} \equiv \{\tau_2\,(dec(h''_3, dK_{X''}))\}^{R''_3}_{eK_{Q''}}$ for some handle h''_3, freshly generated nonce N''_1, arbitrary agent Q'', and freshly generated randomness R''_3 such that $\phi_m \rhd h''_3$, $N''_1 = \tau_1\,(dec(h''_3, dK_{X''}))$, and $Q'' = \tau_3\,(dec(h''_3, dK_{X''}))$; or

2.2.3. $\{x''\}^{R''}_{eK_{X'}} \equiv c_i\,(X'', Q'', N''_1, \tau_2\,(dec(h''_3, dK_{X''})))$ for some handle h''_3, freshly generated nonce N''_1, and arbitrary agent Q'', such that $\phi_m \rhd h''_3$, $N''_1 = \tau_1\,(dec(h''_3, dK_{X''}))$, and $Q'' = \tau_3\,(dec(h''_3, dK_{X''}))$;

or by some (honest) responder X''

2.2.4. $\{x''\}^{R''}_{eK_{X'}} \equiv \{\pi_1\,(dec(h''_2, dK_{X''}))\,, N''_2, X''\}^{R''_2}_{eK_{Q''}}$ for some handle h''_2 with $\phi_m \rhd h''_2$, agent Q'' such that $Q'' = \pi_2\,(dec(h''_2, dK_{X''}))$, freshly generated nonce N''_2, and freshly generated randomness R''_2; or

2.2.5. $\{x''\}^{R''}_{eK_{X'}} \equiv c_r(\pi_2\,(dec(h''_2, dK_{X''}))\,, X'', \pi_1\,(dec(h''_2, dK_{X''}))\,, N''_2)$ for some handle h''_2 with $\phi_m \rhd h''_2$ and $W(\pi_2\,(dec(h''_2, dK_{X''})))$, and freshly generated nonce N''_2.

2.2.1.) In this case $\langle N''_1, X''\rangle \equiv x'' \overset{(5)}{=} \langle\!\langle N'_1, n', X\rangle\!\rangle$ and since $n' = \langle\!\langle N_1, n, Q\rangle\!\rangle$ it follows that $\phi_0, N''_1, X'' \rhd N_1$ and $\phi_0, N''_1 \rhd N_1$ as X'' is public.

If $N''_1 \not\equiv N_1$ then one applies the freshness axiom and obtains $\phi_0 \rhd N_1$ contradicting the no-telepathy axiom. So we necessarily have again that $N''_1 \equiv N_1$.

Since N_1 was generated and sent in a single session we necessarily have $\{N_1, X\}^{R_1}_{eK_Q} \equiv \{N''_1, X''\}^{R''_1}_{eK_{Q''}} \overset{2.2.1.}{\equiv} \{x''\}^{R''}_{eK_{X'}}$ that implies $X' \equiv Q \notin \mathcal{H}$ that is a contradiction.

2.2.2.) This is again a non-trivial case and we address it after the others.

2.2.3.) Same as 2.3.

2.2.4.) In this case $\langle \pi_1\,(dec(h''_2, dK_{X''}))\,, N''_2, X''\rangle \equiv x'' \overset{(5)}{=} \langle\!\langle N'_1, n', X\rangle\!\rangle$ that implies that $N''_2 = \tau_2\,(x'') = \tau_2\,(\langle\!\langle N'_1, n', X\rangle\!\rangle) = n' \overset{(4)}{=} \langle\!\langle N_1, n, Q\rangle\!\rangle$ and consequently $\phi_0, N''_2 \rhd N_1$.

Similarly to case 2.2.1. we necessarily have that $N''_2 \equiv N_1$ which is a contradiction as N_1 was generated in an initiator's session whereas N''_2 was generated in a responder's session.

2.2.5.) Same as 2.3.

2.2.2.—Recap) Let us now analyze this case, that is, $\{x''\}^{R''}_{eK_{X'}} \overset{2.2.2.}{\equiv} \{\tau_2\,(dec(h''_3, dK_{X''}))\}^{R''_3}_{eK_{Q''}}$ for some h''_3, N''_1, Q'', R''_3, such that $\phi_m \rhd h''_3$, and $N''_1 = \tau_1\,(dec(h''_3, dK_{X''}))$, and $Q'' = \tau_3\,(dec(h''_3, dK_{X''}))$. It follows then that $Q'' \equiv X'$ and $R''_3 \equiv R''$.

i. $\phi_m, \vec{x}^\star, x'' \rhd N$ — by (5)

ii. $\phi_m, \vec{x}^\star, \tau_2\,(dec(h''_3, dK_{X''})) \rhd N$ — by congruence of $\equiv$ applied to (i) and 2.2.2.

iii. $\phi_m, \vec{x}^\star, dec(h''_3, dK_{X''}) \rhd N$ — by Proposition 3.2 applied to (ii)

iv. $\phi_m \rhd h''_3$ — by hypothesis

v. $\phi_m, \vec{x}^\star \rhd h''_3$ — by IC(iv)

vi. $\phi_m, \vec{x}^\star \rhd N$ or $\exists x'''R'''.\left(h''_3 = \{x'''\}^{R'''}_{eK_{X''}} \wedge \{x'''\}^{R'''}_{eK_{X''}} \sqsubseteq \phi_m, \vec{x}^\star\right)$ — by NM(v,iii)

The first immediately implies the result so let us consider the second. Notice also that since $\vec{x}^\star$ is a

list of nonces, one can omit it and equivalently obtain

$$\exists x''' R'''. \left(h_3'' = \{x'''\}^{R'''}_{eK_{X''}} \wedge \{x'''\}^{R'''}_{eK_{X''}} \sqsubseteq \phi_m \right)$$

By the derivation above and since we obtained earlier that $Q'' \equiv X'$, it follows that for $n'' \equiv \tau_2\left(dec(h_3'', dK_{X''})\right) \overset{2.2.2}{\equiv} x'' \overset{(5)}{=} \langle\langle N_1', n', X \rangle\rangle$,

$$x''' = dec(h_3'', dK_{X''}) \overset{2.2.2}{=} \langle\langle N_1'', n'', Q'' \rangle\rangle = \langle\langle N_1'', n'', X' \rangle\rangle \qquad \text{and} \qquad \phi_m, \vec{x}^\star, x''' \rhd N. \quad (6)$$

The second formula follows from Step (iii) of the previous derivation.

Let us analyze who could have sent $\{x'''\}^{R'''}_{eK_{X''}}$ as it is in the frame ϕ_m.

Remark: *Note again that at this stage we do not know if $\{x'''\}^{R'''}_{eK_{X''}}$ was indeed (correctly) sent as a response to the first message of X'', or if it was sent at some other stage.*

There are again 5 possible cases for $\{x'''\}^{R'''}_{eK_{X''}}$: it was sent by some (honest) initiator X'''

2.2.2.1. $\{x'''\}^{R'''}_{eK_{X''}} \equiv \{N_1''', X'''\}^{R_1'''}_{eK_{Q'''}}$ with an arbitrary agent Q''', freshly generated nonce N_1''', and freshly generated randomness R_1'''; or

2.2.2.2. $\{x'''\}^{R'''}_{eK_{X''}} \equiv \{\tau_2\left(dec(h_3''', dK_{X'''})\right)\}^{R_3'''}_{eK_{Q'''}}$ for some handle h_3''', freshly generated nonce N_1''', arbitrary agent Q''', and freshly generated randomness R_3''' such that $\phi_m \rhd h_3'''$, $N_1''' = \tau_1\left(dec(h_3''', dK_{X'''})\right)$, and $Q''' = \tau_3\left(dec(h_3''', dK_{X'''})\right)$; or

2.2.2.3. $\{x'''\}^{R'''}_{eK_{X''}} \equiv c_i\left(X''', Q''', N_1''', \tau_2\left(dec(h_3''', dK_{X'''})\right)\right)$ for some handle h_3''', freshly generated nonce N_1''', and arbitrary agent Q''', such that $\phi_m \rhd h_3'''$, $N_1''' = \tau_1\left(dec(h_3''', dK_{X'''})\right)$, and $Q''' = \tau_3\left(dec(h_3''', dK_{X'''})\right)$;

or by some (honest) responder X'''

2.2.2.4. $\{x'''\}^{R'''}_{eK_{X''}} \equiv \{\pi_1\left(dec(h_2''', dK_{X'''})\right), N_2''', X'''\}^{R_2'''}_{eK_{Q'''}}$ for some handle h_2''' with $\phi_m \rhd h_2'''$, agent Q''' such that $Q''' = \pi_2\left(dec(h_2''', dK_{X'''})\right)$, freshly generated nonce N_2''', and freshly generated randomness R_2'''; or

2.2.2.5. $\{x'''\}^{R'''}_{eK_{X''}} \equiv c_r(\pi_2\left(dec(h_2''', dK_{X'''})\right), X''', \pi_1\left(dec(h_2''', dK_{X'''})\right), N_2''')$ for some handle h_2''' with $\phi_m \rhd h_2'''$ and $W(\pi_2\left(dec(h_2''', dK_{X'''})\right))$, and freshly generated nonce N_2'''.

2.2.2.1.) In this case $\langle N_1''', X''' \rangle \equiv x''' \overset{(6)}{=} \langle\langle N_1'', n'', X' \rangle\rangle$ and since $n'' \overset{(6)}{=} \langle\langle N_1', n', X \rangle\rangle$ and $n' \overset{(5)}{=} \langle\langle N_1, n, Q \rangle\rangle$ it follows that $\phi_0, N_1''', X''' \rhd N_1$ and $\phi_0, N_1''' \rhd N_1$ as X''' is public.

If $N_1''' \not\equiv N_1$ then one applies the freshness axiom and obtains $\phi_0 \rhd N_1$ contradicting the no-telepathy axiom. So we necessarily have again that $N_1''' \equiv N_1$.

Since N_1 was generated and sent in a single session we necessarily have $\{N_1, X\}^{R_1}_{eK_Q} \equiv \{N_1''', X'''\}^{R_1'''}_{eK_{Q'''}} \overset{2.2.2.1.}{\equiv} \{x'''\}^{R'''}_{eK_{X''}}$ that implies $X'' \equiv Q \notin \mathcal{H}$ that is a contradiction.

2.2.2.2.) This is again a non-trivial case and we address it after the others.

2.2.2.3.) Same as 2.3.

2.2.2.4.) In this case $\langle \pi_1\left(dec(h_2''', dK_{X'''})\right), N_2''', X''' \rangle \equiv x''' \overset{(6)}{=} \langle\langle N_1'', n'', X' \rangle\rangle$ implies that $N_2''' = \tau_2\left(x'''\right) = n'' \overset{(6)}{=} \langle\langle N_1', n', X \rangle\rangle$ and $n' \overset{(5)}{=} \langle\langle N_1, n, Q \rangle\rangle$ and consequently $\phi_0, N_2''' \rhd N_1$.

Similarly to case 2.2.2.1. we necessarily have that $N_2''' \equiv N_1$ which is a contradiction as N_1 was generated in an initiator's session whereas N_2''' was generated in a responder's session.

2.2.2.5.) Same as 2.3.

2.2.2.2.—Recap) Let us now analyze this case, that is, $\{x'''\}^{R'''}_{eK_{X''}} \overset{2.2.2.2.}{\equiv} \{\tau_2\left(dec(h_3''', dK_{X'''})\right)\}^{R'''_3}_{eK_{Q'''}}$ for some $h_3''', N_1''', Q''', R_3'''$, such that $\phi_m \rhd h_3'''$, and $N_1''' = \tau_1\left(dec(h_3''', dK_{X'''})\right)$, and $Q''' = \tau_3\left(dec(h_3''', dK_{X'''})\right)$. It follows then that $Q''' \equiv X''$ and $R_3''' \equiv R'''$.

i. $\phi_m, \vec{x}^\star, x''' \rhd N$ by (6)

ii. $\phi_m, \vec{x}^\star, \tau_2\left(dec(h_3''', dK_{X'''})\right) \rhd N$ by congruence of $\equiv$ applied to (i) and 2.2.2.2.

iii. $\phi_m, \vec{x}^\star, dec(h_3''', dK_{X'''}) \rhd N$ by Proposition 3.2 applied to (ii)

iv. $\phi_m \rhd h_3'''$ by hypothesis

v. $\phi_m, \vec{x}^\star \rhd h_3'''$ by IC(iv)

vi. $\phi_m, \vec{x}^\star \rhd N$ or $\exists x^{\text{iv}} R^{\text{iv}}.\left(h_3''' = \{x^{\text{iv}}\}^{R^{\text{iv}}}_{eK_{X'''}} \wedge \{x^{\text{iv}}\}^{R^{\text{iv}}}_{eK_{X'''}} \sqsubseteq \phi_m, \vec{x}^\star\right)$ by NM(v,iii)

The first immediately implies the result so let us consider the second. Notice also that since $\vec{x}^\star$ is a list of nonces, one can omit it and equivalently obtain

$$\exists x^{\text{iv}} R^{\text{iv}}.\left(h_3''' = \{x^{\text{iv}}\}^{R^{\text{iv}}}_{eK_{X'''}} \wedge \{x^{\text{iv}}\}^{R^{\text{iv}}}_{eK_{X'''}} \sqsubseteq \phi_m\right)$$

By the derivation above and since we obtained earlier that $Q''' \equiv X''$, it follows that for $n''' \equiv \tau_2\left(dec(h_3''', dK_{X'''})\right) \overset{2.2.2.2}{\equiv} x''' \overset{(6)}{=} \langle\langle N_1'', n'', X'\rangle\rangle$,

$$x^{\text{iv}} = dec(h_3''', dK_{X'''}) \overset{2.2.2.2}{=} \langle\langle N_1''', n''', Q'''\rangle\rangle = \langle\langle N_1''', n''', X''\rangle\rangle \qquad \text{and} \qquad \phi_m, \vec{x}^\star, x^{\text{iv}} \rhd N. \tag{7}$$

The second formula follows from Step (iii) of the previous derivation.

At this stage it is clear that we can iterate the process, going backwards, each time adding a comma everywhere. We notice that while in this process all 2.2.2.x branches were ruled out except for branch 2.2.2.2. that needed us to go backwards once more. But as the trace is finite, we cannot go backwards indefinitely and, at a certain point, there will be no more encryptions $\{x^n\}^{R^n}_{eK_{X^n}} \sqsubseteq \phi_m$ that could match the decryption. When this happens, we arrive at a contradiction and can rule out this branch too.

3.) An initiator X sends $t \equiv c_i\left(X, Q, N_1, \tau_2\left(dec(h_3, dK_X)\right)\right)$ for some handle h_3 with $\phi_m \rhd h_3$, $N_1 = \tau_1\left(dec(h_3, dK_X)\right)$, and $Q = \tau_3\left(dec(h_3, dK_X)\right)$.

Then $\phi_m, \vec{x}^\star \rhd N$ immediately follows as by the axioms for c one has that $\mathsf{RandGen}(N) \wedge \phi_m, \vec{x}^\star, c(\cdot) \rhd N$ implies $\phi_m, \vec{x}^\star \rhd N$.

4.) A responder X sends $t \equiv \{\pi_1\left(dec(h_2, dK_X)\right), N_2, X\}^{R_2}_{eK_Q}$ for some handle h_2 with $\phi_m \rhd h_2$, agent Q such that $Q = \pi_2\left(dec(h_2, dK_X)\right)$, freshly generated nonce N_2, and freshly generated randomness R_2.

If $Q \in \mathcal{H}$ then it is similar to case 1.1 and the result follows by secrecy. Let us then consider the case $Q \notin \mathcal{H}$. In this case $N_2 \not\equiv N$ as by hypothesis N was generated in a session between two honest users (it satisfies $C[N]$) and N_2 was generated in a session with $Q \notin \mathcal{H}$.

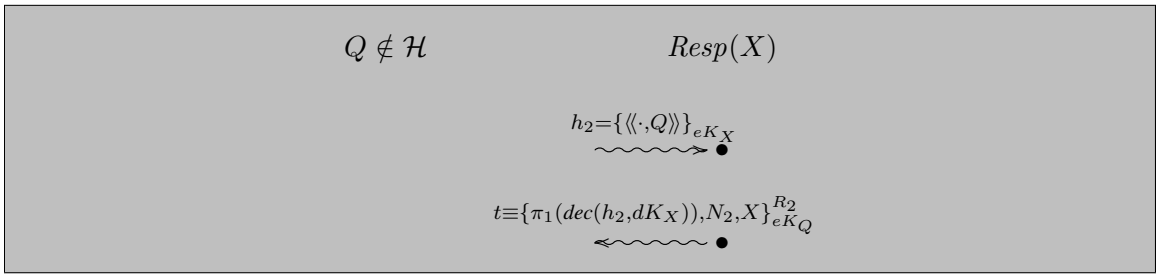

Figure 6: Case 4.) $t \equiv \{\pi_1\left(dec(h_2, dK_X)\right), N_2, X\}^{R_2}_{eK_Q}$ is the message sent by the Responder X.

i. $\phi_m, \vec{x}^\star, \{\pi_1\left(dec(h_2, dK_X)\right), N_2, X\}^{R_2}_{eK_Q} \rhd N$ by (3)

ii. $\phi_m, \vec{x}^\star, \{\pi_1\left(dec(h_2, dK_X)\right), N_2, X\}^{R_2}_{eK_Q}, \pi_1\left(dec(h_2, dK_X)\right), N_2, X, eK_Q, R_2 \rhd N$ by IC(i)

iii. $\phi_m, \vec{x}^\star, \pi_1\left(dec(h_2, dK_X)\right), N_2, X, eK_Q, R_2 \rhd \{\pi_1\left(dec(h_2, dK_X)\right), N_2, X\}^{R_2}_{eK_Q}$ by $\{\cdot\}$-FD

iv. $\phi_m, \vec{x}^\star, \pi_1\left(dec(h_2, dK_X)\right), N_2, X, eK_Q, R_2 \rhd N$ by T(iii,ii)

v. $\phi_m, \vec{x}^\star, \pi_1\left(dec(h_2, dK_X)\right), N_2, eK_Q, R_2 \rhd N$ X public in ϕ_0 (iv)

vi. $\phi_m, \vec{x}^\star, \pi_1\left(dec(h_2, dK_X)\right), N_2, R_2 \rhd N$ eK_Q public in ϕ_0 (v)

vii. $\phi_m, \vec{x}^\star, \pi_1\left(dec(h_2, dK_X)\right), N_2 \rhd N$ by freshness of R_2(vi)

viii. $\phi_m, \vec{x}^\star, \pi_1\left(dec(h_2, dK_X)\right) \rhd N$ by freshness of N_2(vii) and $N_2 \neq N$

ix. $\phi_m, \vec{x}^\star, dec(h_2, dK_X) \rhd N$ Proposition 3.1 applied to (vii)

x. $\phi_m \rhd h_2$ by hypothesis

xi. $\phi_m, \vec{x}^\star \rhd h_2$ by IC(x)

xii. $\phi_m, \vec{x}^\star \rhd N$ or $\exists x' R'.\left(h_2 = \{x'\}^{R'}_{eK_X} \wedge \{x'\}^{R'}_{eK_X} \sqsubseteq \phi_m, \vec{x}^\star\right)$ by NM(xi,ix)

The first immediately implies the result so let us consider the second. Notice also that since $\vec{x}^\star$ is a list of nonces, one can omit it and equivalently obtain

$$\exists x' R'.\left(h_2 = \{x'\}^{R'}_{eK_X} \wedge \{x'\}^{R'}_{eK_X} \sqsubseteq \phi_m\right)$$

By hypothesis 4. and the derivation above it follows that for $n \stackrel{def}{\equiv} \pi_1\left(dec(h_2, dK_X)\right)$

$$x' = dec(h_2, dK_X) \stackrel{4.}{=} \langle\!\langle n, Q \rangle\!\rangle \qquad \text{and} \qquad \phi_m, \vec{x}^\star, x' \rhd N. \tag{8}$$

Let us analyze who could have sent $\{x'\}^{R'}_{eK_X}$ as it is in the frame ϕ_m.
There are again 5 possible cases for $\{x'\}^{R'}_{eK_X}$: it was sent by some (honest) initiator X'

4.1. $\{x'\}^{R'}_{eK_X} \equiv \{N'_1, X'\}^{R'_1}_{eK_{Q'}}$ with an arbitrary agent Q', freshly generated nonce N'_1, and freshly generated randomness R'_1; or

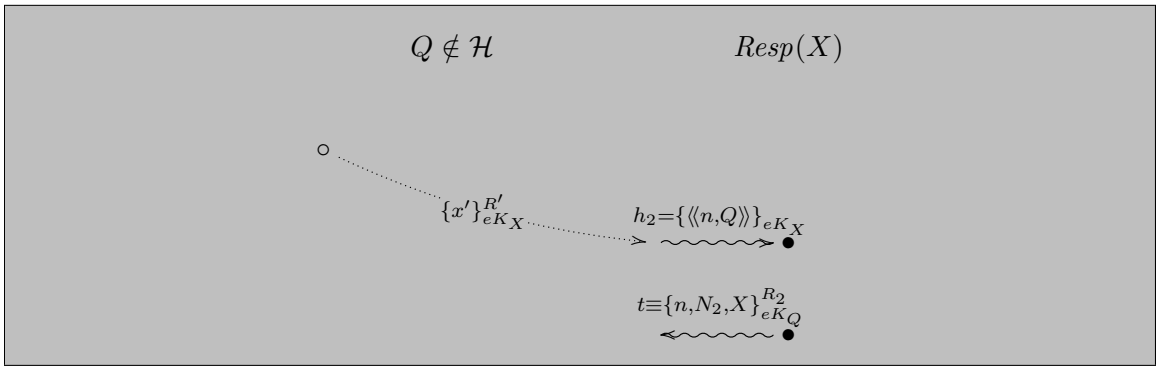

Figure 7: Case 4.x.) Who sent $\{x'\}^{R'}_{eK_X}$ that matches the h_2 received by the Responder X.

4.2. $\{x'\}^{R'}_{eK_X} \equiv \{\tau_2\left(dec(h'_3, dK_{X'})\right)\}^{R'_3}_{eK_{Q'}}$ for some handle h'_3, freshly generated nonce N'_1, arbitrary agent Q', and freshly generated randomness R'_3 such that $\phi_m \triangleright h'_3$, $N'_1 = \tau_1\left(dec(h'_3, dK_{X'})\right)$, and $Q' = \tau_3\left(dec(h'_3, dK_{X'})\right)$; or

4.3. $\{x'\}^{R'}_{eK_X} \equiv c_i\left(X', Q', N'_1, \tau_2\left(dec(h'_3, dK_{X'})\right)\right)$ for some handle h'_3, freshly generated nonce N'_1, and arbitrary agent Q', such that $\phi_m \triangleright h'_3$, $N'_1 = \tau_1\left(dec(h'_3, dK_{X'})\right)$, and $Q' = \tau_3\left(dec(h'_3, dK_{X'})\right)$;

or by some (honest) responder X'

4.4. $\{x'\}^{R'}_{eK_X} \equiv \{\pi_1\left(dec(h'_2, dK_{X'})\right), N'_2, X'\}^{R'_2}_{eK_{Q'}}$ for some handle h'_2 with $\phi_m \triangleright h'_2$, agent Q' such that $Q' = \pi_2\left(dec(h'_2, dK_{X'})\right)$, freshly generated nonce N'_2, and freshly generated randomness R'_2; or

4.5. $\{x'\}^{R'}_{eK_X} \equiv c_r(\pi_2\left(dec(h'_2, dK_{X'})\right), X', \pi_1\left(dec(h'_2, dK_{X'})\right), N'_2)$ for some handle h'_2 with $\phi_m \triangleright h'_2$ and $W(\pi_2\left(dec(h'_2, dK_{X'})\right))$, and freshly generated nonce N'_2.

4.1.) In this case $\langle N'_1, X'\rangle \equiv x' \overset{(8)}{=} \langle\!\langle n, Q\rangle\!\rangle$ and consequently $X' = Q \notin \mathcal{H}$ that is a contradiction.

4.2.) This is again a non-trivial case and we address it after the others.

4.3.) Same as 2.3.

4.4.) In this case, and together with (8) we get

$$\langle \pi_1\left(dec(h'_2, dK_{X'})\right), N'_2, X'\rangle \overset{4.4.}{\equiv} x' \overset{(8)}{=} \langle\!\langle n, Q\rangle\!\rangle$$

and $Q' \equiv X = \pi_2\left(dec(h'_2, dK_{X'})\right)$.

Attack: *From Figures 8 (and 9) and 10 we can see that some extra condition is needed in this case, otherwise there is an attack. Namely, if (with non-negligible probability) for honestly generated nonce N_2', bit string n', and honest agent name X', there is a name Q of a dishonest agent, and a bit string n such that $\langle n', N_2', X' \rangle = \langle\langle n, Q \rangle\rangle$ (that is, parsed as a pair, see definition on page 7), then* ***we may exploit this fact to create an attack*** *that allows one to recover a nonce generated in a session between X and (supposedly) X'.*

The attack is as follows (Figure 8): a malicious agent Q, acting as X, sends $\{n', X\}_{eK_{X'}}$ to X' starting this way a new session with X'. Let $Resp(X')$ be the associated responder session of X'. Upon receiving this message, X' responds according to his role generating a new nonce N_2' and sending $\{n', N_2', X'\}_{eK_X}$ back to Q that is pretending to be X.

Then Q starts a new session with X by forwarding the received message $\{n', N_2', X'\}_{eK_X}$, which is understood by X as $\{n, Q\}_{eK_X}$. This n may hold information about N_2'. According to his role, X responds by sending $\{n, N_2, X\}_{eK_Q}$, for some freshly generated nonce N_2, that can be now decrypted by Q.

So Q is able to retrieve the value of n and possibly compute $\langle n', N_2', X' \rangle$ from n and Q.

If $\langle N', N_2', X' \rangle = \langle\langle n, Q \rangle\rangle$ may hold non-negligibly for honestly generated nonce N', then it is not even needed to initiate the protocol maliciously. X may have initiated a legitimate session with message $\{N', X\}_{eK_{X'}}$, and then even this N' will be compromised as shown in Figure 9.

To provide a **concrete model** *in which this attack is possible, suppose that Q is just the last few bits of X. In that case, $\langle N', N_2', X' \rangle = \langle\langle n, Q \rangle\rangle$ is possible, and n will be N' and N_2' together, plus the first few bits of X. When Q retrieves n, it can compute both N' and N_2'.*

Both these attacks can easily be ruled out if, for example, X checks the length of n.

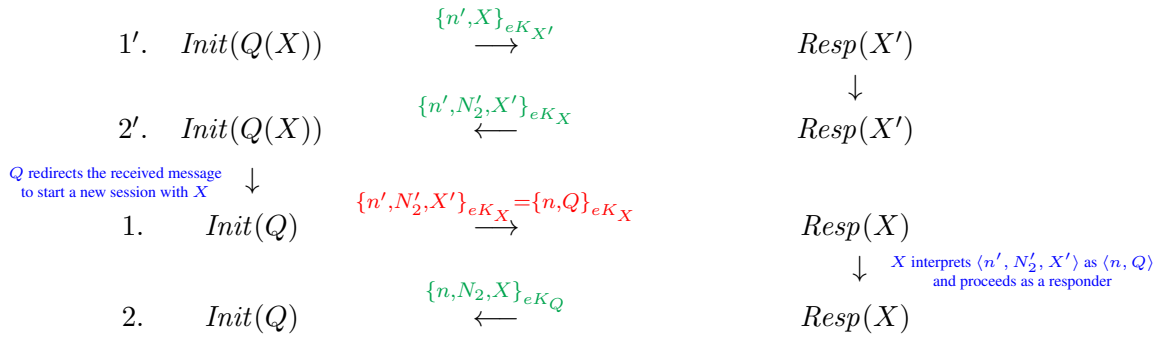

Figure 8: Attack 1 on the NSL Protocol

Consider the following condition: let $X \in \mathcal{H}$ be the abbreviation for $X = A \vee X = B$.

$$\mathsf{RandGen}(N) \wedge X \in \mathcal{H} \Rightarrow (\neg W(\pi_2(\langle n, N, X \rangle)) \vee \pi_2(\langle n, N, X \rangle) \in \mathcal{H}).$$

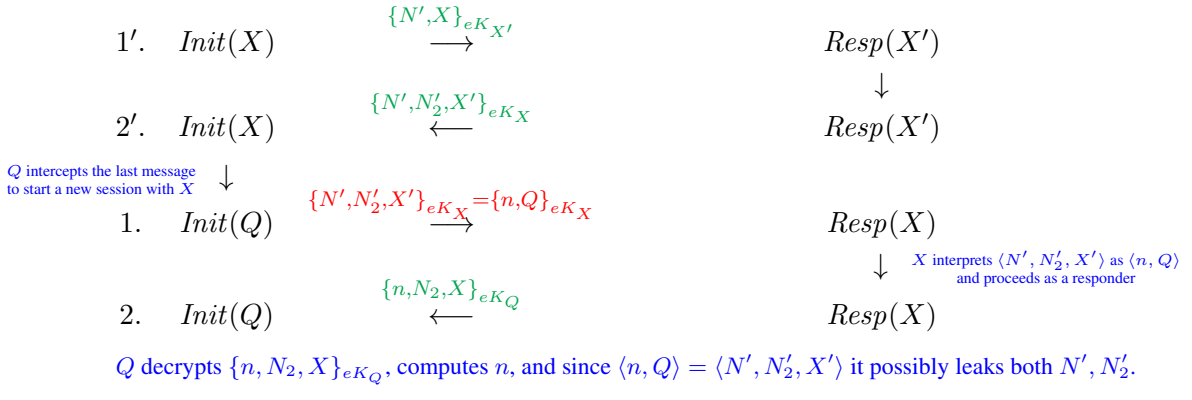

Figure 9: Attack 1.5 on the NSL Protocol

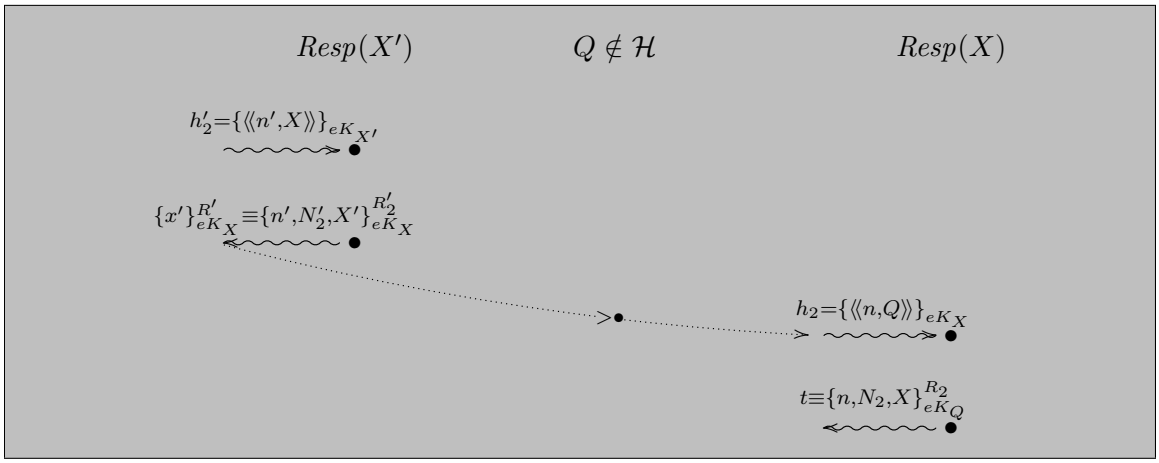

Figure 10: Case 4.4.) Attack when $\{x'\}^{R'}_{eK_X}$ is the message sent by the Responder X' that is used to initialize a new session with Responder X.

This condition prevents the above attack and we can complete the proof of 4.4. as $\langle \pi_1 \left(dec(h_2', dK_{X'})\right), N_2', X' \rangle = \langle\!\langle n, Q \rangle\!\rangle$ together with our new condition imply that $\neg W(Q) \vee Q \in \mathcal{H}$ which contradicts our assumptions about Q.

4.5.) Same as 2.5.

4.2.—Recap) Let us now analyze this case. Together with (8) we have

$$\tau_2 \left(dec(h_3', dK_{X'})\right) \overset{4.2.}{\equiv} x' \overset{(8)}{=} \langle\!\langle n, Q \rangle\!\rangle$$

with $\phi_m \rhd h_3'$, and $N_1' = \tau_1 \left(dec(h_3', dK_{X'})\right)$, and $Q' = \tau_3 \left(dec(h_3', dK_{X'})\right)$, and $Q' \equiv X$ and $R_3' \equiv R'$.

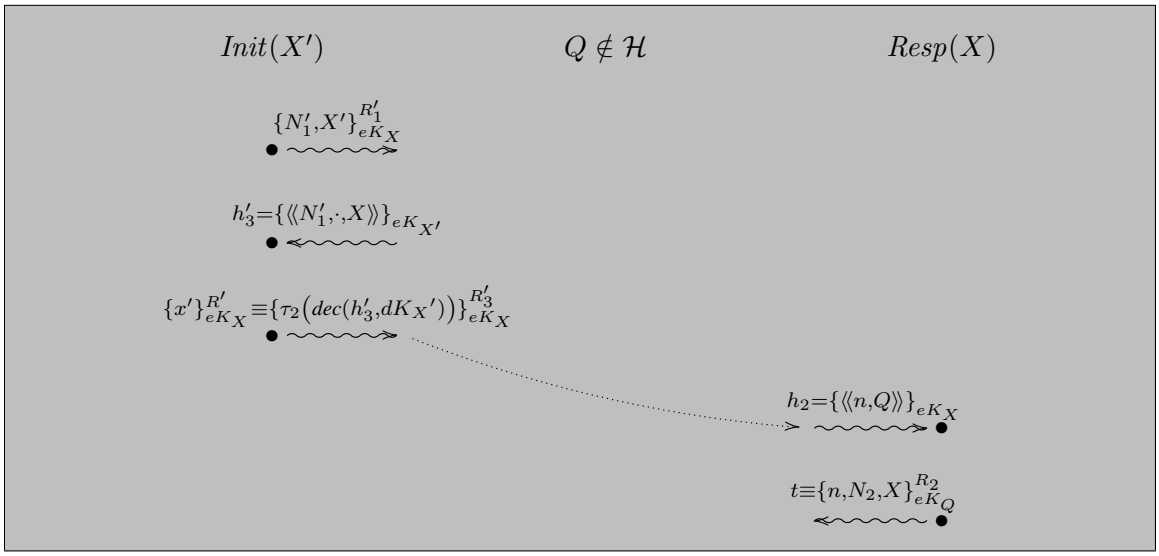

Figure 11: Case 4.2.) where $\{x'\}^{R'}_{eK_X}$ is the last message sent by the Initiator X'.

i. $\phi_m, \vec{x}^\star, x' \rhd N$ by (8)

ii. $\phi_m, \vec{x}^\star, \tau_2\left(dec(h_3', dK_{X'})\right) \rhd N$ by congruence of $\equiv$ applied to (i) and 4.2.

iii. $\phi_m, \vec{x}^\star, dec(h_3', dK_{X'}) \rhd N$ by Proposition 3.2 applied to (ii)

iv. $\phi_m \rhd h_3'$ by hypothesis

v. $\phi_m, \vec{x}^\star \rhd h_3'$ by IC(iv)

vi. $\phi_m, \vec{x}^\star \rhd N$ or $\exists x'' R''.\left(h_3' = \{x''\}^{R''}_{eK_{X'}} \wedge \{x''\}^{R''}_{eK_{X'}} \sqsubseteq \phi_m, \vec{x}^\star\right)$ by NM(v,iii)

The first immediately implies the result so let us consider the second. Notice also that since $\vec{x}^\star$ is a list of nonces, one can omit it and equivalently obtain

$$\exists x'' R''.\left(h_3' = \{x''\}^{R''}_{eK_{X'}} \wedge \{x''\}^{R''}_{eK_{X'}} \sqsubseteq \phi_m\right)$$

By the derivation above it follows that for $n' \equiv \tau_2\left(dec(h_3', dK_{X'})\right) \overset{4.2.}{\equiv} x' \overset{(8)}{=} \langle\!\langle n, Q \rangle\!\rangle$

$$x'' = dec(h_3', dK_{X'}) \overset{4.2.}{=} \langle\!\langle N_1', n', Q' \rangle\!\rangle = \langle\!\langle N_1', n', X \rangle\!\rangle \qquad \text{and} \qquad \phi_m, \vec{x}^\star, x'' \rhd N. \tag{9}$$

Let us analyze who could have sent $\{x''\}^{R''}_{eK_{X'}}$ as it is in the frame ϕ_m. There are again 5 possible cases for $\{x''\}^{R''}_{eK_{X'}}$: it was sent by some (honest) initiator X''

4.2.1. $\{x''\}^{R''}_{eK_{X'}} \equiv \{N_1'', X''\}^{R_1''}_{eK_{Q''}}$ with an arbitrary agent Q'', freshly generated nonce N_1'', and freshly generated randomness R_1''; or

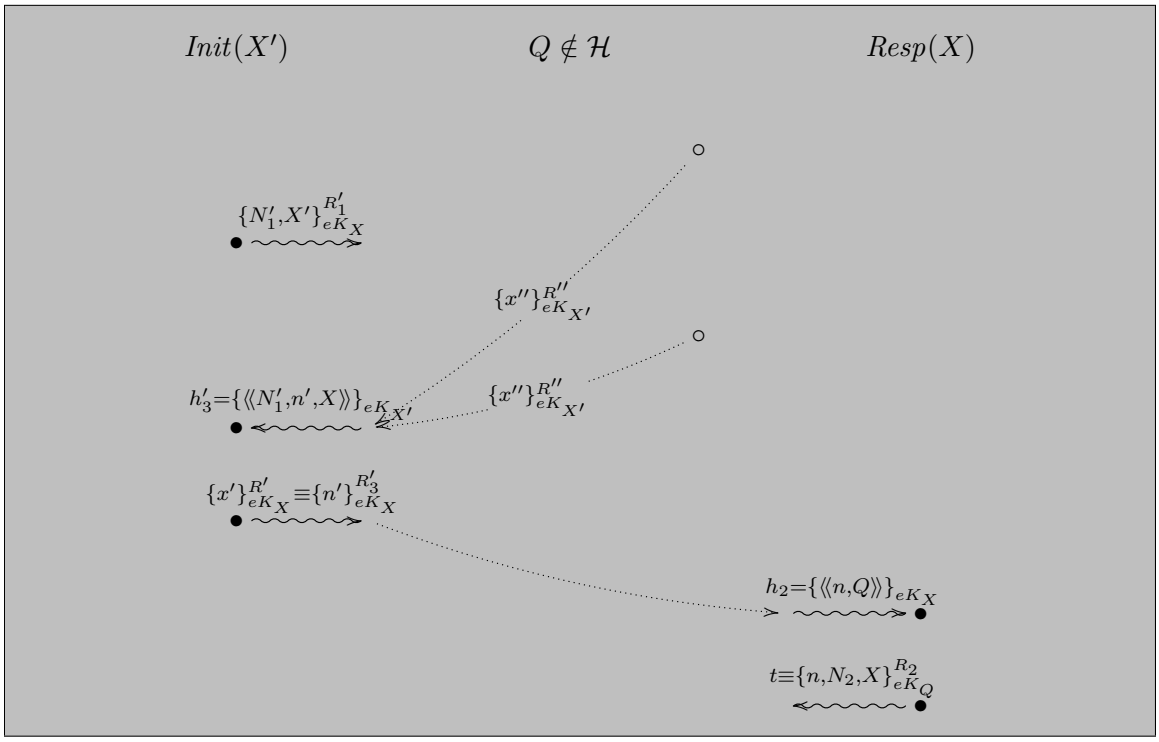

Figure 12: Case 4.2.x.) Who sent $\{x''\}^{R''}_{eK_{X'}}$ that matches the h_3' received by the Initiator X'.

4.2.2. $\{x''\}^{R''}_{eK_{X'}} \equiv \{\tau_2\left(dec(h_3'', dK_{X''})\right)\}^{R_3''}_{eK_{Q''}}$ for some handle h_3'', freshly generated nonce N_1'', arbitrary agent Q'', and freshly generated randomness R_3'' such that $\phi_m \rhd h_3''$, $N_1'' = \tau_1\left(dec(h_3'', dK_{X''})\right)$, and $Q'' = \tau_3\left(dec(h_3'', dK_{X''})\right)$; or

4.2.3. $\{x''\}^{R''}_{eK_{X'}} \equiv c_i\left(X'', Q'', N_1'', \tau_2\left(dec(h_3'', dK_{X''})\right)\right)$ for some handle h_3'', freshly generated nonce N_1'', and arbitrary agent Q'', such that $\phi_m \rhd h_3''$, $N_1'' = \tau_1\left(dec(h_3'', dK_{X''})\right)$, and $Q'' = \tau_3\left(dec(h_3'', dK_{X''})\right)$;

or by some (honest) responder X''

4.2.4. $\{x''\}^{R''}_{eK_{X'}} \equiv \{\pi_1\left(dec(h_2'', dK_{X''})\right), N_2'', X''\}^{R_2''}_{eK_{Q''}}$ for some handle h_2'' with $\phi_m \rhd h_2''$, agent Q'' such that $Q'' = \pi_2\left(dec(h_2'', dK_{X''})\right)$, freshly generated nonce N_2'', and freshly generated randomness R_2''; or

4.2.5. $\{x''\}^{R''}_{eK_{X'}} \equiv c_r(\pi_2\left(dec(h_2'', dK_{X''})\right), X'', \pi_1\left(dec(h_2'', dK_{X''})\right), N_2'')$ for some handle h_2'' with $\phi_m \rhd h_2''$ and $W(\pi_2\left(dec(h_2'', dK_{X''})\right))$, and freshly generated nonce N_2''.

4.2.1.) In this case $\langle N_1'', X''\rangle \equiv x'' \overset{(9)}{=} \langle\!\langle N_1', n', X\rangle\!\rangle$ and it follows that $\phi_0, N_1'', X'' \rhd N_1'$ and $\phi_0, N_1'' \rhd N_1'$ as X'' is public. If $N_1'' \not\equiv N_1'$ then one applies the freshness axiom and obtains $\phi_0 \rhd N_1'$ contradicting the no-telepathy axiom. So we necessarily have that $N_1'' \equiv N_1'$.

Since N_1' was generated and sent in a single session we necessarily have $\{N_1', X'\}^{R_1'}_{eK_X} \equiv \{N_1'', X''\}^{R_1''}_{eK_{Q''}} \overset{4.2.1.}{\equiv} \{x''\}^{R''}_{eK_{X'}}$ that implies $X' \equiv X''$ and $X \equiv Q''$ by the first equivalence, and $Q'' \equiv X'$ by the second. Putting all these together we get $X \equiv Q'' \equiv X' \equiv X''$.

Attack: *In this case we also need an extra condition as in the particular case that $N \equiv N_1'' \equiv N_1'$ one may create the* ***attack sketched in Figure 13 and presented in detail in Figure 14****. Notice that in this case $N \equiv N_1'$ is generated in a session between X and himself as $X' \equiv X$.*

This attack relies on the fact that for an honestly generated nonce N and honest name X, $\pi_2(\tau_2(\langle N, X\rangle))$ (that is $\pi_2(n')$ in our example) is the name of a malicious agent.

Let $Init(X)$, the protocol on the left hand-side of Figure 14, be the initiator process in a protocol run between an honest initiator X and himself, and where he generates nonce N. Suppose that adversary Q intercepts the first message and sends it back to X fooling him as being the responder's answer.

Let $Resp(X)$ be the responder process in a protocol run between adversary Q and X that is initialized by Q by forwarding to X the message $\{n'\}_{eK_X}$ that he captured from the network, which X parses as $\{n, Q\}_{eK_X}$.

In this case, by decrypting the last message, the adversary Q is able to retrieve n, and as in the previous attack, may be able to compute n' as $\langle n, Q\rangle$. With n' and X he may now retrieve part of the message $\langle N, X\rangle$. In particular, if $\langle N, X\rangle = \langle N, N, X\rangle$, then $n' = N$. Of course in typical implementations this would not hold but, as we have not assumed anything about the way pairs and triples are related, $\langle N, X\rangle = \langle N, N, X\rangle$ is actually possible in some implementations.

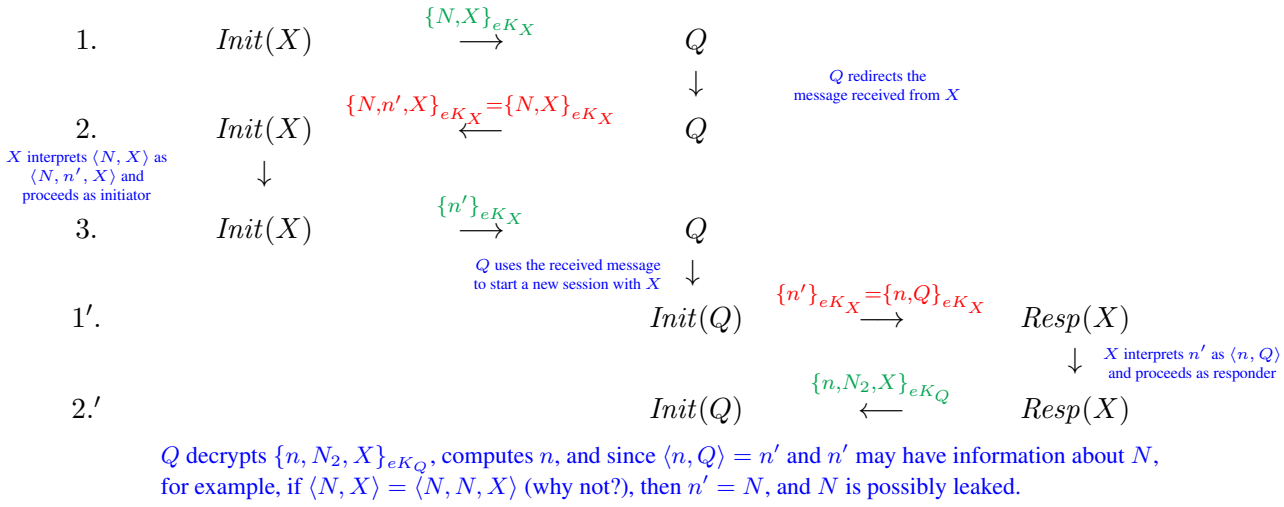

Figure 13: Attack 2 on the NSL Protocol

Consider the following condition:

$$\mathsf{RandGen}(N) \wedge X \in \mathcal{H} \Rightarrow (\tau_1(\langle N, X\rangle) \neq N \ \vee \ \tau_3(\langle N, X\rangle) \neq X).$$

This condition, although stricter than needed, clearly prevents the above attack.
4.2.2.) This is again a non-trivial case and we address it after the others.
4.2.3.) Same as 2.3.

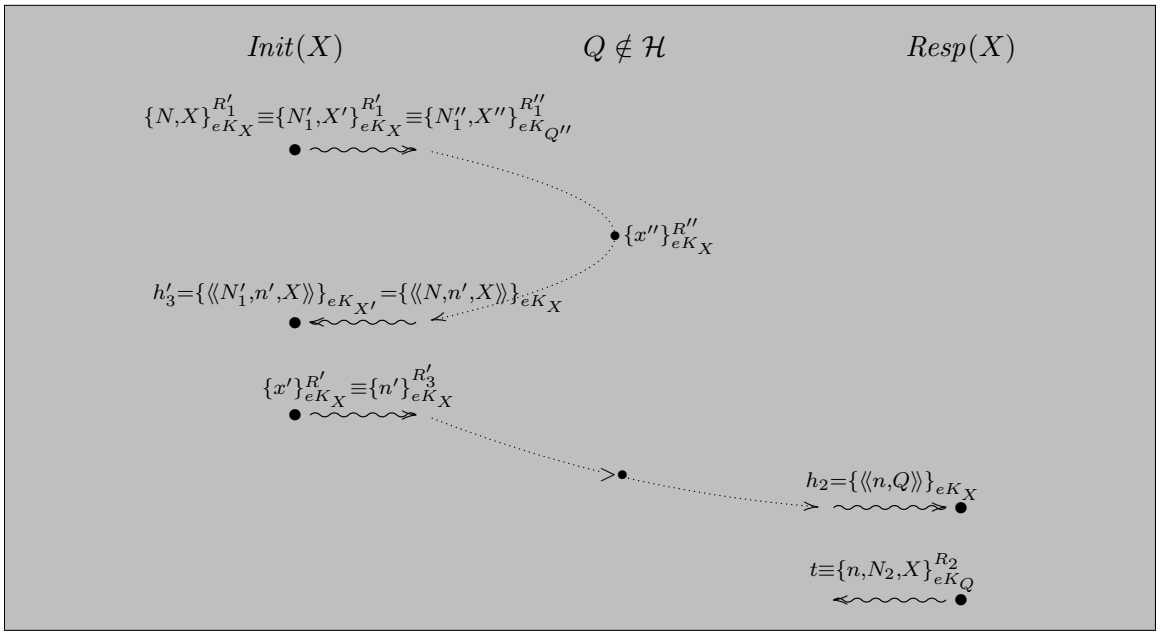

Figure 14: Case 4.2.1.) Attack when the message $\{x''\}^{R''}_{eK_{X'}}$ sent by the Initiator X when it generates the nonce N is re-used as the response message by the receiver.

4.2.4.) In this case, and together with (9) we get that for $n'' \equiv \pi_1\left(dec(h''_2, dK_{X''})\right)$

$$\langle n'', N''_2, X'' \rangle \overset{4.2.4.}{\equiv} x'' \overset{(9)}{=} \langle\!\langle N'_1, n', X \rangle\!\rangle$$

for some honest responder X'', handle h''_2 with $\phi_m \triangleright h''_2$, agent Q'' such that $Q'' = \pi_2\left(dec(h''_2, dK_{X''})\right)$, freshly generated nonce N''_2, and freshly generated randomness R''_2. Moreover, $Q'' \equiv X'$ and $N''_2 = \tau_2\left(x''\right) = n' \overset{(9)}{=} \langle\!\langle n, Q \rangle\!\rangle$.

Attack: *In this case we also need an extra condition as in the particular case that $X'' \equiv X$ one may create an **attack as shown in Figure 15 and detailed in Figure 16**. Notice that this attack is performed after a correctly executed session between X' and X.*

Let an honest Initiator X' execute the protocol with an honest Responder X, and suppose that the adversary Q intercepts the last message $\{N''_2\}^{R'_3}_{eK_X}$ and uses it to initiate a new session with Responder X fooling him as the message being of the form $\{n, Q\}_{eK_X}$.

In this case, by decrypting the last message, similarly to the previous attacks, the adversary Q is able to retrieve n, and may be able to compute N''_2 if $N''_2 = \langle\!\langle n, Q \rangle\!\rangle$. It may actually be true that $N''_2 = \langle n, Q \rangle$.

Consider the following condition:

$$\mathsf{RandGen}(N) \rightarrow \left(\neg W(\pi_2\left(N\right)) \vee \pi_2\left(N\right) \in \mathcal{H}\right).$$

This condition, although stricter than needed, prevents the above attack.

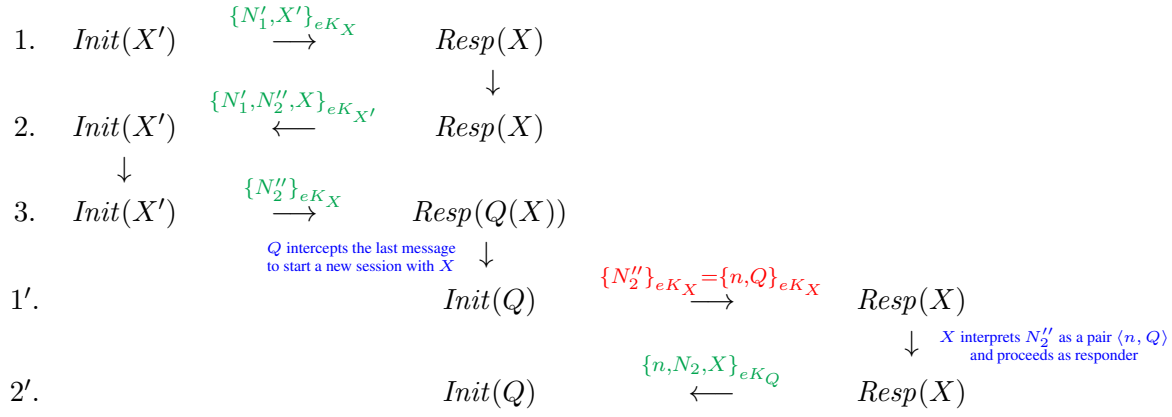

Figure 15: Attack 3 on the NSL Protocol

4.2.5.) Same as 2.3.

4.2.2.—Recap) Let us now analyze this case. Together with (9) we get

$$\tau_2\left(dec(h_3'', dK_{X''})\right) \overset{4.2.2.}{\equiv} x'' \overset{(9)}{=} \langle\langle N_1', n', X\rangle\rangle$$

such that $\phi_m \rhd h_3''$, $N_1'' = \tau_1\left(dec(h_3'', dK_{X''})\right)$, and $Q'' = \tau_3\left(dec(h_3'', dK_{X''})\right)$. Moreover, $Q'' \equiv X'$ and $R_3'' \equiv R''$. Then,

i. $\phi_m, \vec{x}^\star, x'' \rhd N$ by (9)

ii. $\phi_m, \vec{x}^\star, \tau_2\left(dec(h_3'', dK_{X''})\right) \rhd N$ by congruence of $\equiv$ applied to (i) and 4.2.2.

iii. $\phi_m, \vec{x}^\star, dec(h_3'', dK_{X''}) \rhd N$ by Proposition 3.2 applied to (ii)

iv. $\phi_m \rhd h_3''$ by hypothesis

v. $\phi_m, \vec{x}^\star \rhd h_3''$ by IC(iv)

vi. $\phi_m, \vec{x}^\star \rhd N$ or $\exists x''' R'''.\left(h_3'' = \{x'''\}^{R'''}_{eK_{X''}} \wedge \{x'''\}^{R'''}_{eK_{X''}} \sqsubseteq \phi_m, \vec{x}^\star\right)$ by NM(v,iii)

The first immediately implies the result so let us consider the second. Notice also that since $\vec{x}^\star$ is a list of nonces, one can omit it and equivalently obtain

$$\exists x''' R'''.\left(h_3'' = \{x'''\}^{R'''}_{eK_{X''}} \wedge \{x'''\}^{R'''}_{eK_{X''}} \sqsubseteq \phi_m\right)$$

By the derivation above it follows that for $n'' \equiv \tau_2\left(dec(h_3'', dK_{X''})\right) \overset{4.2.2.}{\equiv} x'' \overset{(9)}{=} \langle\langle N_1', n', X\rangle\rangle$

$$x''' = dec(h_3'', dK_{X''}) \overset{4.2.2}{=} \langle\langle N_1'', n'', Q''\rangle\rangle = \langle\langle N_1'', n'', X'\rangle\rangle \qquad \text{and} \qquad \phi_m, \vec{x}^\star, x''' \rhd N. \quad (10)$$

Let us analyze who could have sent $\{x'''\}^{R'''}_{eK_{X''}}$ as it is in the frame ϕ_m. There are again 5 possible cases:

4.2.2.1.) In this case $\langle N_1''', X'''\rangle \equiv x''' \overset{(10)}{=} \langle\langle N_1'', n'', X'\rangle\rangle$ and it follows that $\phi_0, N_1''', X''' \rhd N_1''$ and $\phi_0, N_1''' \rhd N_1''$ as X''' is public. If $N_1''' \not\equiv N_1''$ then one applies the freshness axiom and

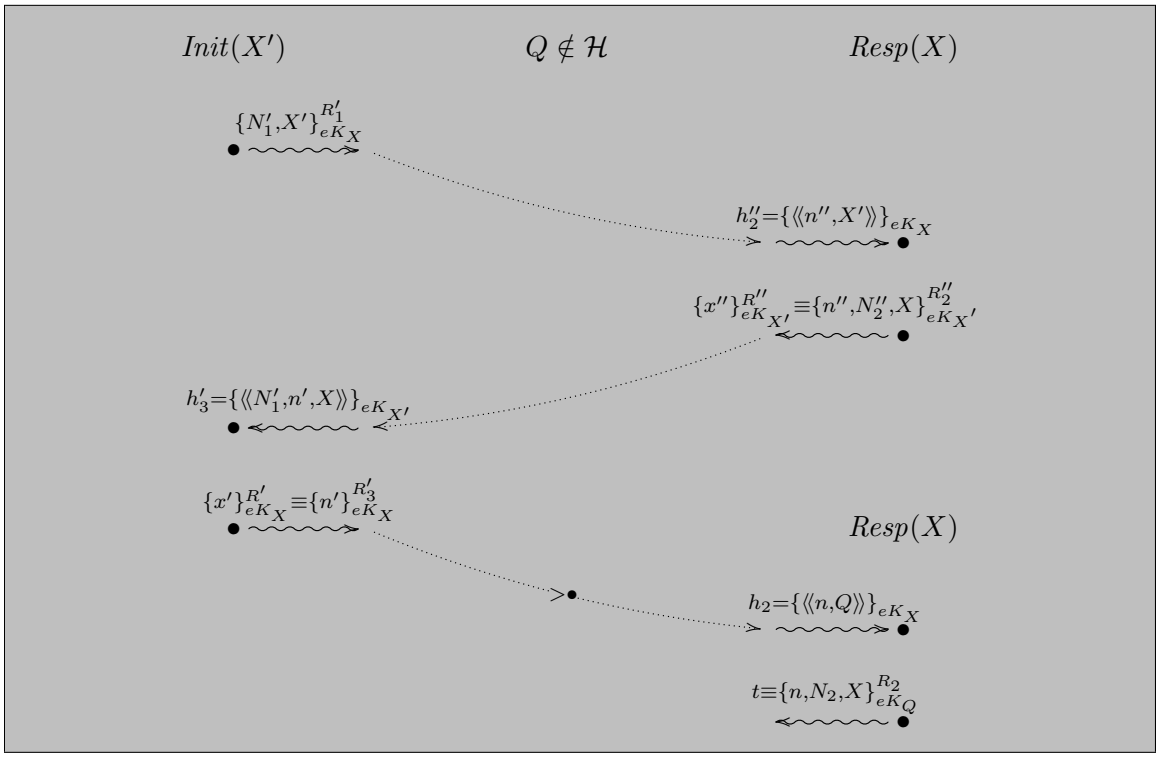

Figure 16: Case 4.2.4.) Attack when the last message of a correctly executed protocol between X' and $X'' \equiv X$ is used to initiate a protocol with Responder X.

obtains $\phi_0 \rhd N_1''$ contradicting the no-telepathy axiom. So we necessarily have that $N_1''' \equiv N_1''$, and since N_1'' was generated and sent in a single session we necessarily have that $X''' \equiv X''$. Hence $\langle N_1'', X''\rangle \equiv \langle N_1''', X'''\rangle \overset{4.2.2.1.}{=} x''' \overset{(10)}{=} \langle\langle N_1'', n'', X'\rangle\rangle$ and since $n'' \overset{(10)}{=} \langle\langle N_1', n', X\rangle\rangle$ it follows that $\phi_0, N_1'', X'' \rhd N_1'$ and $\phi_0, N_1'' \rhd N_1'$ as X'' is public.

If $N_1'' \not\equiv N_1'$ then one applies the freshness axiom and obtains $\phi_0 \rhd N_1'$ contradicting the no-telepathy axiom. So we necessarily have that $N_1'' \equiv N_1'$. This is the same as saying that the two sessions run by X' and X'' in Figure 17 are the same which is a contradiction as the session on the right ends before the session on the left.

4.2.2.2.) In this case $\{x'''\}^{R'''}_{eK_{X''}} \equiv \{\tau_2\,(dec(h_3''', dK_{X'''}))\}^{R_3'''}_{eK_{Q'''}}$ for some handle h_3''', freshly generated nonce N_1''', arbitrary agent Q''', and freshly generated randomness R_3''' such that $\phi_m \rhd h_3'''$, $N_1''' = \tau_1\,(dec(h_3''', dK_{X'''}))$, and $Q''' = \tau_3\,(dec(h_3''', dK_{X'''}))$. Hence,

$$\tau_2\left(dec(h_3''', dK_{X'''})\right) \overset{4.2.2.2.}{\equiv} x''' \overset{(10)}{=} \langle\langle N_1'', n'', X'\rangle\rangle$$

and $Q''' \equiv X''$ and $R_3''' \equiv R'''$.

Similarly to the case 4.2.2. one can derive that for $n''' \equiv \tau_2\,(dec(h_3''', dK_{X'''})) \overset{4.2.2.2.}{\equiv} x''' \overset{(10)}{=} \langle\langle N_1'', n'', X'\rangle\rangle$

$$x^{\text{iv}} = dec(h_3''', dK_{X'''}) \overset{4.2.2.2.}{=} \langle\langle N_1''', n''', Q'''\rangle\rangle = \langle\langle N_1''', n''', X''\rangle\rangle \qquad \text{and} \qquad \phi_m, \vec{x}^{\star}, x^{\text{iv}} \rhd N. \tag{11}$$

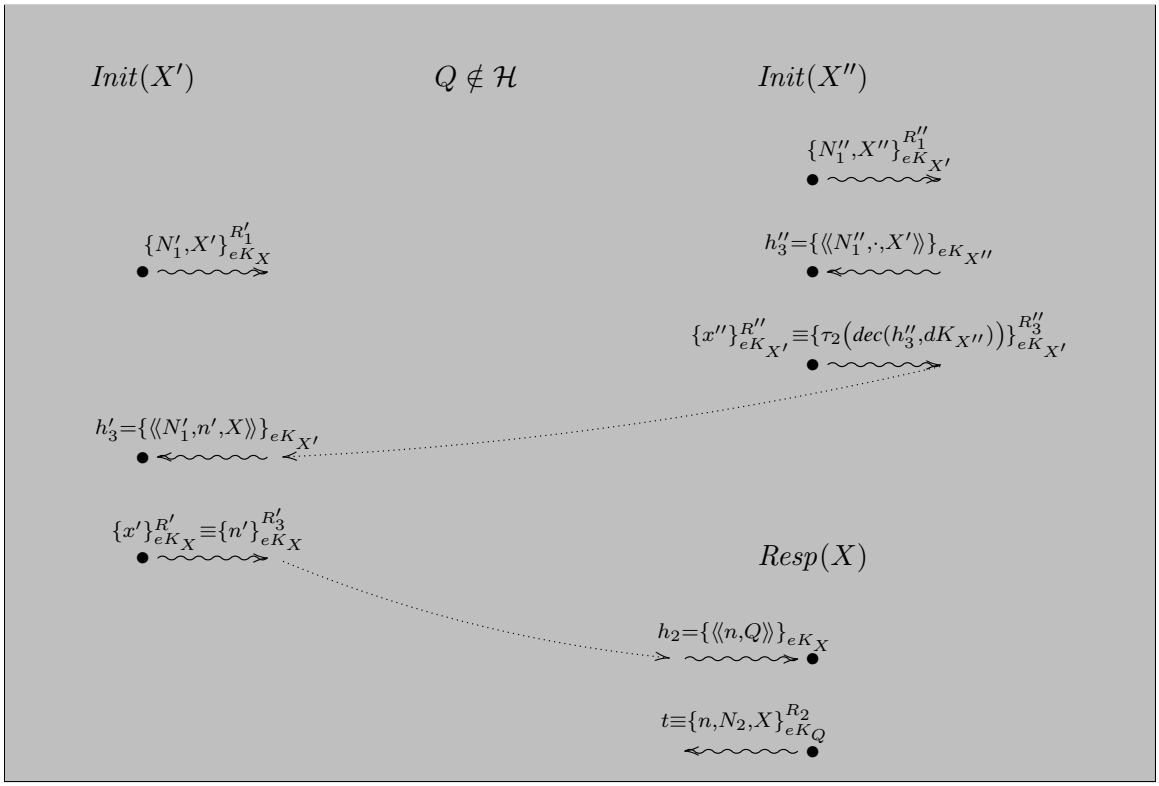

Figure 17: Case 4.2.2.) where $\{x''\}^{R''}_{eK_{X'}}$ is the last message sent by the Initiator X''.

Splitting 4.2.2.2. in 5 sub-cases 4.2.2.2.x. will be the same as when we divided 4.2.2 into 4.2.2.x. as now we have $x^{\text{iv}} \overset{(11)}{=} \langle\langle N_1''', n''', X''\rangle\rangle$ with $n''' \overset{(11)}{=} \langle\langle N_1'', n'', X'\rangle\rangle$, whereas before we had $x''' \overset{(10)}{=} \langle\langle N_1'', n'', X'\rangle\rangle$ with $n'' \overset{(10)}{=} \langle\langle N_1', n', X\rangle\rangle$, with both N_1''', N_1'' generated in honest initiator's sessions by X''' and X'' respectively.

We can then apply the same reasoning as in 4.2.2 and be sure that it stops as the number of previously sent messages is finite.

4.2.2.3.) Same as 2.3.

4.2.2.4.) In this case $\langle \pi_1 (dec(h_2''', dK_{X'''})), N_2''', X'''\rangle \equiv x''' \overset{(10)}{=} \langle\langle N_1'', n'', X'\rangle\rangle$ that implies $N_2''' = n'' \overset{(10)}{=} \langle\langle N_1', n', X\rangle\rangle$ and consequently $\phi_0, N_2''' \rhd N_1'$. Since N_2''' was generated in a responder session by X''' and N_1' in an initiator's session by X' one necessarily has that $N_2''' \not\equiv N_1'$, and consequently $\phi_0 \rhd N_1'$ contradicting the no-telepathy axiom.

4.2.2.5.) Same as 2.3.

4.5.) Same as 2.3.

5.) A responder X sends $t \equiv c_r(\pi_2 (dec(h_2, dK_X)), X, \pi_1 (dec(h_2, dK_X)), N_2)$ for some handle h_2 with $\phi_m \rhd h_2$ and $W(\pi_2 (dec(h_2, dK_X)))$, and freshly generated nonce N_2.

Then $\phi_m, \vec{x}^\star \rhd N$ immediately follows as by the axioms for c one has that $\mathsf{RandGen}(N) \wedge \phi_m, \vec{x}^\star, c(\cdot) \rhd N$ implies $\phi_m, \vec{x}^\star \rhd N$. QED

We still have to prove that the property initially holds, that is, $\exists N \exists \vec{x} \big(C[N] \wedge C'[\vec{x}, N] \wedge \phi_0, \vec{x} \rhd N \big)$ is inconsistent with the axioms. Let $C[N]$ and $C'[\vec{x}, N]$ hold for N and $\vec{x} \equiv \vec{x}^\star$. At step 0, N, $N_1, \ldots, N_l$ are still fresh (remember, we assumed for simplicity that everything was generated upfront, and clearly, these nonces have not been sent), so by the no telepathy axiom, $\phi_0 \not\rhd N$, and then by the independence of fresh items, $\phi_0, N_1 \not\rhd N$. Then again by the independence of fresh items, $\phi_0, N_1, N_2 \not\rhd N$, etc. So

$$\phi_0, \vec{x}^\star \not\rhd N$$

holds, meaning that $\exists N \exists \vec{x} \big(C[N] \wedge C'[\vec{x}, N] \wedge \phi_0, \vec{x} \rhd N \big)$ is indeed inconsistent. Then the induction step in Proposition 4.1 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 an arbitrary number of possible dishonest participants and two honest participants A, B that only execute either of the NSL roles in each of their sessions.*

Our axioms together with the agent checks and the conditions we introduced to avoid attacks imply that for any $n \in \mathbb{N}$ and for any nonce N that was either generated by A and sent to B, or vice versa, $\phi_n \not\rhd N$.

The above Theorem states that secrecy of nonces satisfying $C[N]$ is never broken. That is, nonces that were generated by A or B and intended to be sent between each other, remain secret. In particular, taking $\vec{x}$ to be the empty list, the formula $\exists N \big(C[N] \wedge \hat{\phi} \rhd N \big)$, together with the axioms and the agent checks, and the conditions we introduced to avoid attacks are inconsistent on any symbolic trace.

Remark: *Note that all the above attacks can be avoided if nonces have fixed length, pairing and tripling are length regular, and the agents check the lengths of bit-strings that are supposed to be nonces (to cover this symbolically, a new type can be introduced and the conditions to avoid the attacks weakened with an additional disjunct).*

Theorem 4.3 (Agreement and Authentication from Responder's View) *Consider a symbolic execution of the NSL protocol, with an arbitrary number of possible dishonest participants, and an arbitrary number of honest participants that execute both initiator and responder roles (and nothing else) in each of their bounded number of sessions.*

Let us fix honest responder B. For any $X \in \mathcal{H}$, our axioms together with the agent checks and the conditions we introduced to avoid attacks are inconsistent with the negation of the formula

$$c_r(\pi_2(dec(h_2, dK_B)), B, \pi_1(dec(h_2, dK_B)), N_2) \sqsubseteq \hat{\phi} \ \wedge \ X = \pi_2(dec(h_2, dK_B))$$
$$\longrightarrow \ \exists N_1 h_3. \left(\begin{array}{l} c_i(X, B, N_1, \tau_2(dec(h_3, dK_X))) \sqsubseteq \hat{\phi} \wedge \\ N_2 = \tau_2(dec(h_3, dK_X)) \ \wedge \ N_1 = \pi_1(dec(h_2, dK_B)) \end{array} \right)$$

Proof: Suppose that for some $m \in \mathbb{N}$, we have

$$c_r(\pi_2(dec(h_2, dK_B)), B, \pi_1(dec(h_2, dK_B)), N_2) \sqsubseteq \phi_m \ \wedge \ X = \pi_2(dec(h_2, dK_B)).$$

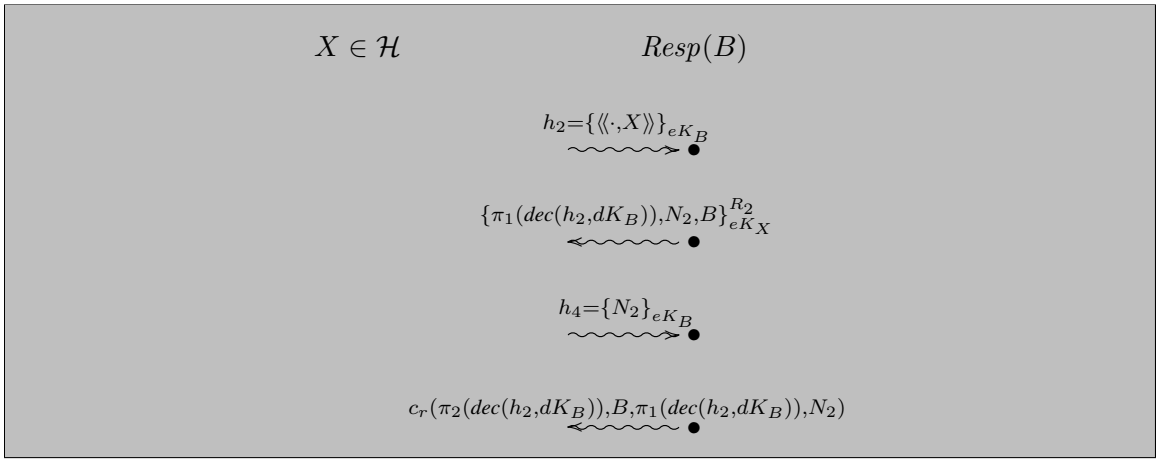

Figure 18: Responder B terminates the protocol.

From the responder's role, and since $X \in \mathcal{H}$, one has that $C[N_2]$, and from the Secrecy Theorem that $\phi_m \not\vdash N_2$. It also follows from the role that for the last message h_4 accepted by B, the condition $dec(h_4, dK_B) = N_2$ was satisfied. Hence by the NM axiom,

$$\exists x' R'. \left(h_4 = \{x'\}^{R'}_{eK_B} \wedge \{x'\}^{R'}_{eK_B} \sqsubseteq \phi_m \right)$$

and

$$x' = dec(h_4, dK_B) = N_2. \tag{12}$$

There are 5 possible cases for $\{x'\}^{R'}_{eK_B}$: it was sent by some (honest) initiator X'

1. $\{x'\}^{R'}_{eK_B} \equiv \{N'_1, X'\}^{R'_1}_{eK_{Q'}}$ with an arbitrary agent Q', freshly generated nonce N'_1, and freshly generated randomness R'_1; or

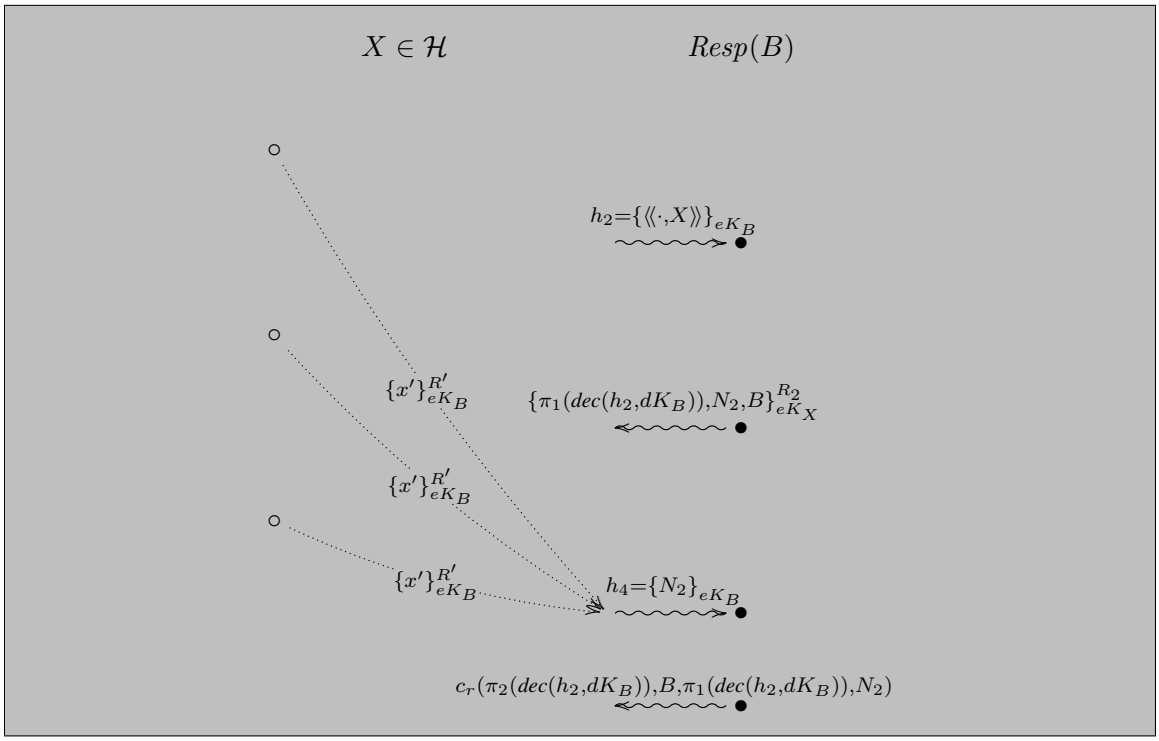

Figure 19: Who sent the $\{x'\}^{R'}_{eK_B}$ that matches the h_4 received by the Responder B.

2. $\{x'\}^{R'}_{eK_B} \equiv \{\tau_2\left(dec(h'_3, dK_{X'})\right)\}^{R'_3}_{eK_{Q'}}$ for some handle h'_3, arbitrary agent Q', freshly generated nonce N'_1, and freshly generated randomness R'_3 such that $\phi_m \rhd h'_3$, $N'_1 = \tau_1\left(dec(h'_3, dK_{X'})\right)$, and $Q' = \tau_3\left(dec(h'_3, dK_{X'})\right)$; or
3. $\{x'\}^{R'}_{eK_B} \equiv c_i\left(X', Q', N'_1, \tau_2\left(dec(h'_3, dK_{X'})\right)\right)$ for some handle h'_3, freshly generated nonce N'_1, and arbitrary agent Q', such that $\phi_m \rhd h'_3$, $N'_1 = \tau_1\left(dec(h'_3, dK_{X'})\right)$, and $Q' = \tau_3\left(dec(h'_3, dK_{X'})\right)$;

or by some (honest) responder X'

4. $\{x'\}^{R'}_{eK_B} \equiv \{\pi_1\left(dec(h'_2, dK_{X'})\right), N'_2, X'\}^{R'_2}_{eK_{Q'}}$ for some handle h'_2 with $\phi_m \rhd h'_2$, agent Q' such that $Q' = \pi_2\left(dec(h'_2, dK_{X'})\right)$, freshly generated nonce N'_2, and freshly generated randomness R'_2; or
5. $\{x'\}^{R'}_{eK_B} \equiv c_r(\pi_2\left(dec(h'_2, dK_{X'})\right), X', \pi_1\left(dec(h'_2, dK_{X'})\right), N'_2)$ for some handle h'_2 with $\phi_m \rhd h'_2$ and $W(\pi_2\left(dec(h'_2, dK_{X'})\right))$, and freshly generated nonce N'_2.

1.) In this case $\langle N'_1, X' \rangle \equiv x' \overset{(12)}{=} N_2$ and so $\phi_0, N'_1, X' \rhd N_2$ and $\phi_0, N'_1 \rhd N_2$ as X' is public.

The case $N'_1 \equiv N_2$ is not possible as N_2 was generated in a responder's session while N'_1 was generated in an initiator's session. On the other hand, if $N'_1 \not\equiv N_2$ then one applies the freshness axiom and obtains that $\phi_0 \rhd N_2$ contradicting the no-telepathy axiom. Case 1.) is not possible.

2.) This is the expected behaviour, so we skip it for now and come back to it later.

3.) $c_i(\cdot)$ can never match the encryption $\{x'\}^{R'}_{eK_B}$ as c_i is (syntactically) not the encryption

function symbol.

4.) In this case $\langle \pi_1 \left(dec(h_2', dK_{X'}) \right), N_2', X' \rangle \equiv x' \overset{(12)}{=} N_2$, and $Q' \equiv B$. Now, if $N_2' \neq N_2$, and since $\phi_0, N_2 \rhd N_2'$, one has by freshness that $\phi_0 \rhd N_2'$ contradicting the no-telepathy axiom.

Attack: *But when $N_2' = N_2$, then there is an attack (Figure4): Dishonest agent Q acting as initiator B sends a message $\{n, B\}_{eK_B}$ to honest agent B. B, in the responder role, thinks he communicates with himself, the initiator B (which is impersonated by Q), and responds with $\{\pi_1 \left(dec(h_2', dK_B) \right), N_2, B\}^{R_2'}_{eK_B}$. This message may be re-directed to B by Q, and B accepts it as the response. Note it is necessary that $\pi_1 \left(dec(h_2', dK_B) \right)$ be also malicious, because if it is a correct nonce N_1' generated by initiator B, then $\phi_0, N_2 \rhd N_1'$, which is impossible because of the usual reasoning as N_1' and N_2 are necessarily generated in different sessions and they cannot be derived from each other.*

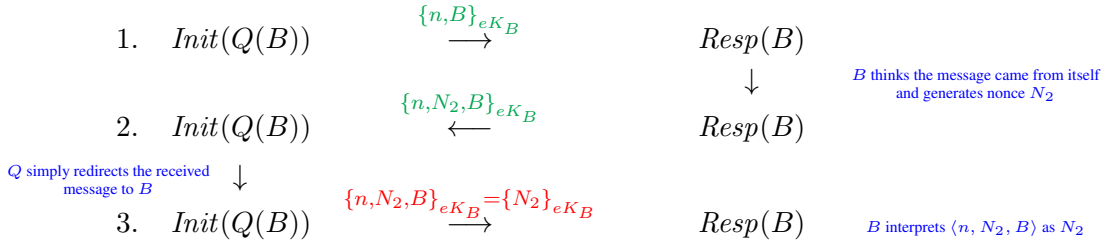

Figure 20: Attack 4 on the NSL Protocol

Assuming

$$\mathsf{RandGen}(N) \rightarrow \tau_2 \left(N \right) \neq N \vee \neg W(\tau_3 \left(N \right))$$

the attack becomes impossible: In this case $\langle \pi_1 \left(dec(h_2', dK_{X'}) \right), N_2', X' \rangle \neq N_2$, so 4. cannot happen.

5.) Same as 2.3.

2.—Recap) Let's get back to case 2. In this case,

$$\tau_2 \left(dec(h_3', dK_{X'}) \right) \equiv x' \overset{(12)}{=} N_2 \text{ and } Q' \equiv B. \tag{13}$$

That is, in this case we have that there was an honest initiator X' that sent out the message $\{\tau_2 \left(dec(h_3', dK_{X'}) \right)\}^{R_3'}_{eK_B} = \{N_2\}^{R_3'}_{eK_B}$ for some handle h_3'. As a consequence, we have that there exists a freshly generated nonce N_1' such that

$$c_i(X', B, N_1', \tau_2 \left(dec(h_3', dK_{X'}) \right)) \sqsubseteq \phi_m \ \wedge \ N_2 = \tau_2 \left(dec(h_3', dK_{X'}) \right).$$

It remains to show that

$$X' = X \text{ and } N_1 = \pi_1 \left(dec(h_2, dK_B) \right). \tag{14}$$

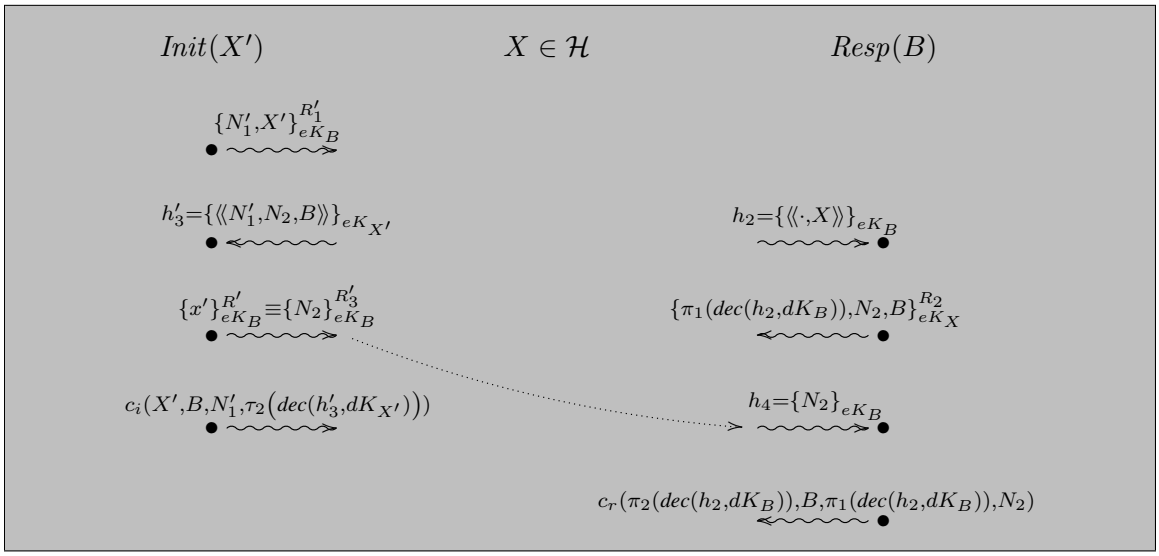

Figure 21: Case 2.) where $\{x'\}^{R'}_{eK_B}$ is the last message sent by the Initiator X'.

What we do know from the initiator's role of the honest agent X' is that he received h_3 (let's switch to h_3 and N_1 instead of h_3' and N_1'), and consequently

$$\tau_1\left(dec(h_3, dK_{X'})\right) = N_1 \quad \text{and} \quad \tau_3\left(dec(h_3, dK_{X'})\right) = Q' = B. \tag{15}$$

This means that N_1 is a nonce generated in an initiator's session of X' with responder B. Hence $C[N_1]$ holds. We can now use again the NM axiom applied either to N_1 or N_2 to get that

$$\exists x'' R''. \left(h_3 = \{x''\}^{R''}_{eK_{X'}} \wedge \{x''\}^{R''}_{eK_{X'}} \sqsubseteq \phi_m\right)$$

From the foregoing, we also have that

$$x'' = dec(h_3, dK_{X'}) \overset{(15)+(13)}{=} \langle\!\langle N_1, N_2, B \rangle\!\rangle \tag{16}$$

There are again 5 possible cases for $\{x''\}^{R''}_{eK_{X'}}$: it was sent by some (honest) initiator X''

2.1. $\{x''\}^{R''}_{eK_{X'}} \equiv \{N_1'', X''\}^{R_1''}_{eK_{Q''}}$ with an arbitrary agent Q'', freshly generated nonce N_1'', and freshly generated randomness R_1''; or

2.2. $\{x''\}^{R''}_{eK_{X'}} \equiv \{\tau_2\left(dec(h_3'', dK_{X''})\right)\}^{R_3''}_{eK_{Q''}}$ for some handle h_3'', freshly generated nonce N_1'', arbitrary agent Q'', and freshly generated randomness R_3'' such that $\phi_m \triangleright h_3''$, $N_1'' = \tau_1\left(dec(h_3'', dK_{X''})\right)$, and $Q'' = \tau_3\left(dec(h_3'', dK_{X''})\right)$; or

2.3. $\{x''\}^{R''}_{eK_{X'}} \equiv c_i\left(X'', Q'', N_1'', \tau_2\left(dec(h_3'', dK_{X''})\right)\right)$ for some handle h_3'', arbitrary agent Q'', freshly generated nonce N_1'', and such that $\phi_m \triangleright h_3''$, $N_1'' = \tau_1\left(dec(h_3'', dK_{X''})\right)$, and $Q'' = \tau_3\left(dec(h_3'', dK_{X''})\right)$;

or by some (honest) responder X''

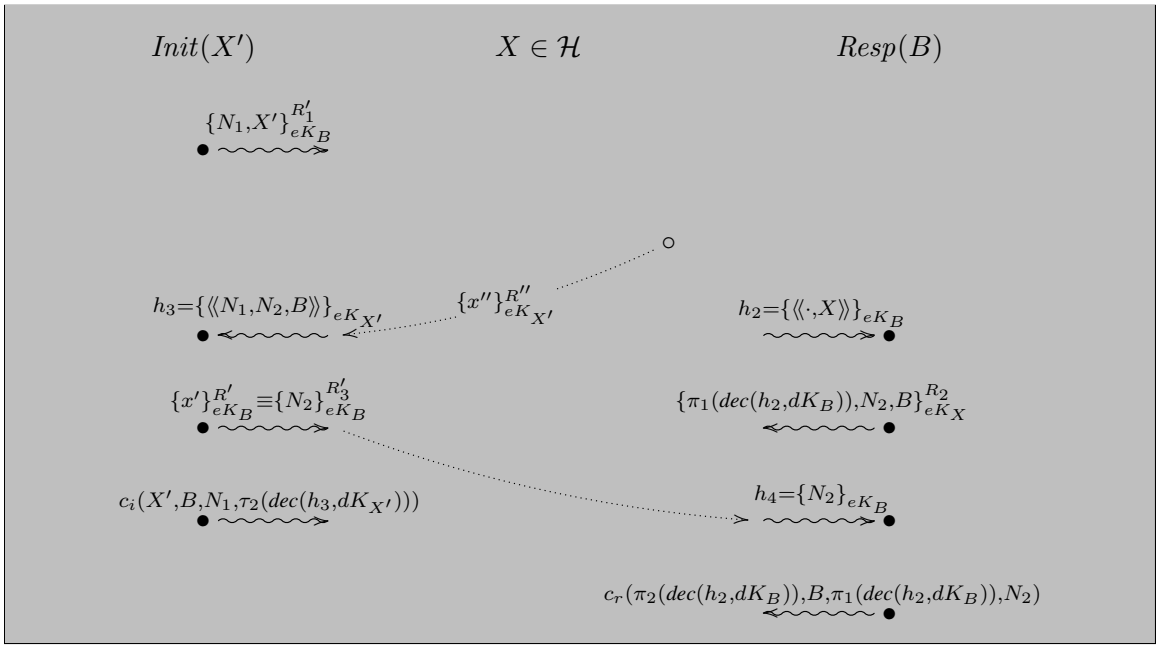

Figure 22: Who sent the $\{x''\}^{R''}_{eK_{X'}}$ that matches the h_3 received by the Initiator X'.

2.4. $\{x''\}^{R''}_{eK_{X'}} \equiv \{\pi_1(dec(h''_2, dK_{X''})), N''_2, X''\}^{R''_2}_{eK_{Q''}}$ for some handle h''_2 with $\phi_m \rhd h''_2$, agent Q'' such that $Q'' = \pi_2(dec(h''_2, dK_{X''}))$, freshly generated nonce N''_2, and freshly generated randomness R''_2; or

2.5. $\{x''\}^{R''}_{eK_{X'}} \equiv c_r(\pi_2(dec(h''_2, dK_{X''})), X'', \pi_1(dec(h''_2, dK_{X''})), N''_2)$ for some handle h''_2 with $\phi_m \rhd h''_2$ and $W(\pi_2(dec(h''_2, dK_{X''})))$, and freshly generated nonce N''_2.

2.1.) In this case $\langle N''_1, X''\rangle \equiv x'' \overset{(16)}{=} \langle\langle N_1, N_2, B\rangle\rangle$ and so $\phi_0, N''_1, X'' \rhd N_2$ and $\phi_0, N''_1 \rhd N_2$ as X'' is public.

If $N''_1 \not\equiv N_2$ then one applies the freshness axiom to obtain $\phi_0 \rhd N_2$ contradicting the no-telepathy axiom. So we necessarily have that $N''_1 \equiv N_2$. But N''_1 was generated in an initiator's session, while N_2 was generated in a responder's session, so case 2.1. is not possible.

2.2.) In this case $\{x''\}^{R''}_{eK_{X'}} \equiv \{\tau_2(dec(h''_3, dK_{X''}))\}^{R''_3}_{eK_{Q''}}$ for some h''_3, N''_1, Q'', R''_3, such that $\phi_m \rhd h''_3$, and $N''_1 = \tau_1(dec(h''_3, dK_{X''}))$, and $Q'' = \tau_3(dec(h''_3, dK_{X''}))$. It follows then that $Q'' \equiv X'$ and $R''_3 \equiv R''$. Now, for N either N_1 or N_2, we have that

i. $\phi_m, x'' \rhd N$ — by (16)

ii. $\phi_m, \tau_2(dec(h''_3, dK_{X''})) \rhd N$ — by congruence of $\equiv$ applied to (i) and 2.2.

iii. $\phi_m, dec(h''_3, dK_{X''}) \rhd N$ — by Proposition 3.2 applied to (ii)

iv. $\phi_m \rhd h''_3$ — by hypothesis

v. $\phi_m \rhd N$ or $\exists x'''R'''.\left(h''_3 = \{x'''\}^{R'''}_{eK_{X''}} \wedge \{x'''\}^{R'''}_{eK_{X''}} \sqsubseteq \phi_m\right)$ — by NM(iv,iii)

But $\phi_m \rhd N$ is not possible because of the Secrecy Theorem as $C[N]$ holds.

By the derivation above and since we obtained earlier that $Q'' \equiv X'$, it follows that for

$$n'' \stackrel{def}{\equiv} \tau_2\left(dec(h_3'', dK_{X''})\right) \stackrel{2.2.}{\equiv} x'' \stackrel{(16)}{=} \langle\langle N_1, N_2, B\rangle\rangle \tag{17}$$

we have

$$x''' = dec(h_3'', dK_{X''}) \stackrel{2.2.+(17)}{=} \langle\langle N_1'', n'', Q''\rangle\rangle = \langle\langle N_1'', n'', X'\rangle\rangle \qquad \text{and} \qquad \phi_m, x'' \rhd N. \tag{18}$$

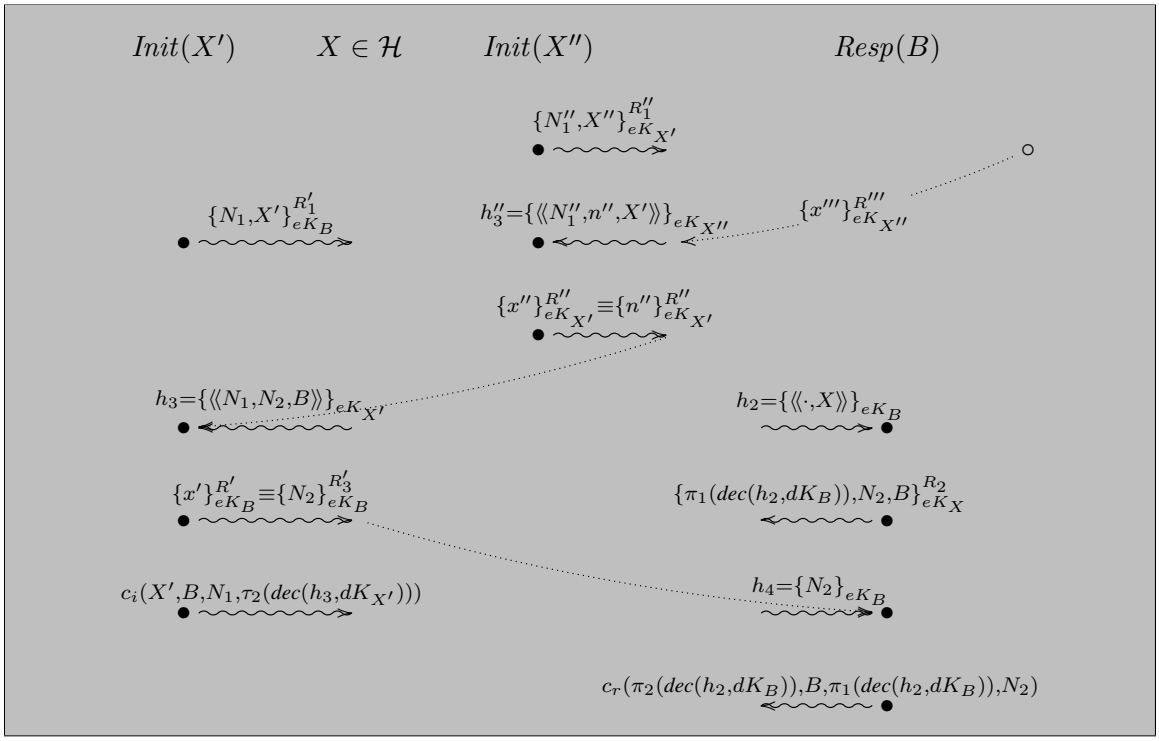

Figure 23: Who sent the $\{x'''\}^{R'''}_{eK_{X''}}$ that matches the h_3'' received by the Initiator X''.

There are again 5 possible cases for $\{x'''\}^{R'''}_{eK_{X''}}$: it was sent by some (honest) initiator X'''

2.2.1. $\{x'''\}^{R'''}_{eK_{X''}} \equiv \{N_1''', X'''\}^{R_1'''}_{eK_{Q'''}}$ with an arbitrary agent Q''', freshly generated nonce N_1''', and freshly generated randomness R_1'''; or

2.2.2. $\{x'''\}^{R'''}_{eK_{X''}} \equiv \{\tau_2\left(dec(h_3''', dK_{X'''})\right)\}^{R_3'''}_{eK_{Q'''}}$ for some handle h_3''', arbitrary agent Q''', freshly generated nonce N_1''', and freshly generated randomness R_3''' such that $\phi_m \rhd h_3'''$, $N_1''' = \tau_1\left(dec(h_3''', dK_{X'''})\right)$, and $Q''' = \tau_3\left(dec(h_3''', dK_{X'''})\right)$; or

2.2.3. $\{x'''\}^{R'''}_{eK_{X''}} \equiv c_i\left(X''', Q''', N_1''', \tau_2\left(dec(h_3''', dK_{X'''})\right)\right)$ for some handle h_3''', freshly generated nonce N_1''', and arbitrary agent Q''', such that $\phi_m \rhd h_3'''$, $N_1''' = \tau_1\left(dec(h_3''', dK_{X'''})\right)$, and $Q''' = \tau_3\left(dec(h_3''', dK_{X'''})\right)$;

or by some (honest) responder X'''

2.2.4. $\{x'''\}^{R'''}_{eK_{X''}} \equiv \{\pi_1\left(dec(h_2''', dK_{X'''})\right), N_2''', X'''\}^{R_2'''}_{eK_{Q'''}}$ for some handle h_2''' with $\phi_m \rhd h_2'''$, agent Q''' such that $Q''' = \pi_2\left(dec(h_2''', dK_{X'''})\right)$, freshly generated nonce N_2''', and freshly generated randomness R_2'''; or

2.2.5. $\{x'''\}^{R'''}_{eK_{X''}} \equiv c_r(\pi_2\left(dec(h_2''', dK_{X'''})\right), X''', \pi_1\left(dec(h_2''', dK_{X'''})\right), N_2''')$ for some handle h_2''' with $\phi_m \rhd h_2'''$ and $W(\pi_2\left(dec(h_2''', dK_{X'''})\right))$, and freshly generated nonce N_2'''.

2.2.1.) In this case $\langle N_1''', X'''\rangle \equiv x''' \overset{(18)}{=} \langle\!\langle N_1'', n'', X'\rangle\!\rangle$. Since $n'' \overset{(17)}{=} \langle\!\langle N_1, N_2, B\rangle\!\rangle$, we have that $\phi_0, n'' \rhd N_2$. So by transitivity $\phi_0, N_1''', X''' \rhd N_2$, and $\phi_0, N_1''' \rhd N_2$ as X''' is public. But this is not possible by the usual freshness+no-telepathy argument as N_1''' was generated in an initiator's session whereas N_2 was generated in a responder's session.

2.2.2.) In this case $\{x'''\}^{R'''}_{eK_{X''}} \equiv \{\tau_2\left(dec(h_3''', dK_{X'''})\right)\}^{R_3'''}_{eK_{Q'''}}$ for some $h_3''', N_1''', Q''', R_3'''$, such that $\phi_m \rhd h_3'''$, and $N_1''' = \tau_1\left(dec(h_3''', dK_{X'''})\right)$, and $Q''' = \tau_3\left(dec(h_3''', dK_{X'''})\right)$. It follows then that $Q''' \equiv X''$ and $R_3''' \equiv R'''$. For N either N_1 or N_2, we have again

i. $\phi_m, x''' \rhd N$ — by (17) and (18)

ii. $\phi_m, \tau_2\left(dec(h_3''', dK_{X'''})\right) \rhd N$ — by congruence of $\equiv$ applied to (i) and 2.2.2.

iii. $\phi_m, dec(h_3''', dK_{X'''}) \rhd N$ — by Proposition 3.2 applied to (ii)

iv. $\phi_m \rhd h_3'''$ — by hypothesis

v. $\phi_m \rhd N$ or $\exists x^{\text{iv}} R^{\text{iv}}.\left(h_3''' = \{x^{\text{iv}}\}^{R^{\text{iv}}}_{eK_{X'''}} \wedge \{x^{\text{iv}}\}^{R^{\text{iv}}}_{eK_{X'''}} \sqsubseteq \phi_m\right)$ — by NM(iv,iii)

But $\phi_m \rhd N$ is not possible because of the Secrecy Theorem as $C[N]$ holds.

By the derivation above and since we obtained earlier that $Q''' \equiv X''$, it follows that for

$$n''' \overset{def}{\equiv} \tau_2\left(dec(h_3''', dK_{X'''})\right) \overset{2.2.2.}{\equiv} x''' \overset{(18)}{=} \langle\!\langle N_1'', n'', X'\rangle\!\rangle \tag{19}$$

one has

$$x^{\text{iv}} = dec(h_3''', dK_{X'''}) \overset{2.2.2.+(19)}{=} \langle\!\langle N_1''', n''', Q'''\rangle\!\rangle = \langle\!\langle N_1''', n''', X''\rangle\!\rangle \qquad \text{and} \qquad \phi_m, x''' \rhd N. \tag{20}$$

Moreover, we also have $\phi_m, n''' \rhd N$ and $\phi_m, x^{\text{iv}} \rhd N$ transitively from (19) and (20).

There are again 5 possible cases for $\{x^{\text{iv}}\}^{R^{\text{iv}}}_{eK_{X'''}}$. However, we are now back in the situation of 2.2., except that we have one more prime everywhere. So we can generate the rest of the argument by adding one more prime. 2.2.2.2.... will keep increasing but, as the protocol has only a finite past, it has to end somewhere, and there will be no further $x'^{\cdots}$ to go back. At that point, we end up with a contradiction.

2.2.3.) $c_i(\cdot)$ can never match the encryption $\{x'''\}^{R'''}_{eK_{X''}}$ as c_i is (syntactically) not the encryption function symbol.

2.2.4.) In this case $Q''' \equiv X''$, and $\langle \pi_1\left(dec(h_2''', dK_{X'''})\right), N_2''', X'''\rangle \equiv x''' \overset{(18)}{=} \langle\!\langle N_1'', n'', X'\rangle\!\rangle$, which implies that $\pi_1\left(dec(h_2''', dK_{X'''})\right) = \tau_1\left(x'''\right) = N_1'$, and $N_2''' = \tau_2\left(x'''\right) = n''$, and $X''' = \tau_3\left(x'''\right) = X'$. As $n'' \overset{(17)}{=} \langle\!\langle N_1, N_2, B\rangle\!\rangle$, we have that $\phi_0, n'' \rhd N_1$, and since $n'' = N_2'''$, it follows that $\phi_0, N_2''' \rhd N_1$. Since N_2''' was generated in a responder's session and N_1 was generated in an initiator's session, this is not possible by the usual freshness+no-telepathy argument.

2.2.5.) Same as 2.2.3.

2.3.) $c_i(\cdot)$ can never match the encryption $\{x''\}^{R''}_{eK_{X'}}$ as c_i is (syntactically) not the encryption function symbol.

2.4.) In this case $Q'' \equiv X'$, and $\langle \pi_1 (dec(h''_2, dK_{X''})), N''_2, X'' \rangle \equiv x'' \overset{(16)}{=} \langle\!\langle N_1, N_2, B \rangle\!\rangle$, that implies $\pi_1 (dec(h''_2, dK_{X''})) = \tau_1 (x'') = N_1$, and $N''_2 = \tau_2 (x'') = N_2$, and $X'' = \tau_3 (x'') = B$.

Recall from (14) that it was left to show that $X' = X$ and $N_1 = \pi_1 (dec(h_2, dK_B))$ that is proved if one shows that $X = X'$ and $h''_2 \equiv h_2$.

To show the latter, consider that since X'' is a constant of an agent name, $X'' \equiv B$, and $N''_2 \equiv N_2$ similarly as before (as $N''_2 = N_2$ according to the foregoing and the same argument as in 1.2. of the secrecy proof where we showed that $N_1 \not\equiv N$ implies $N_1 \neq N$). Hence

$$\{\pi_1 \left(dec(h''_2, dK_{X''})\right), N''_2, X''\}^{R''_2}_{eK_{Q''}} \equiv \{\pi_1 \left(dec(h''_2, dK_B)\right), N_2, B\}^{R''_2}_{eK_{X'}}$$

However, as N_2 cannot be generated in two separate sessions, h''_2 represents the message received by B in the session when he generated N_2, so $h''_2 \equiv h_2$.

In order to show that $X = X'$, remember that we do know from the initiator role of the honest agent X' that he received h_3 (recall that we switched the notation from h'_3 to h_3), and from (15)

$$\tau_1 (dec(h_3, dK_{X'})) = N_1 \quad \text{and} \quad \tau_3 (dec(h_3, dK_{X'})) = B.$$

We also had from the NM axiom and our assumption 2.4. that this h_3 was produced by X'', which in turn is B. Namely, B sent a message of the form

$$\{\pi_1 (dec(h_2, dK_B)), N_2, B\}^{R_2}_{eK_{X'}}$$

(we replaced the notation of R''_2 with R_2 as that is the one sent when h_2 is received). But we know that N_2 was generated by B in a session that was for communicating with X. Hence $X' \equiv X$.

2.5.) Same as 2.3.

QED

Remark: *Note that all the above attacks can be avoided if nonces have fixed length, pairing and tripling are length regular, and the agents check the lengths of bit-strings that are supposed to be nonces (to cover this symbolically, a new type can be introduced and the conditions to avoid the attacks weakened with an additional disjunct).*

References

[1] G. Bana, P. Adão, and H. Sakurada. Computationally complete symbolic attacker in action. Available at IACR ePrint Archive, Report 2012/316.

[2] Gergei Bana, Pedro Adão, and Hideki Sakurada. Computationally Complete Symbolic Attacker in Action. In Deepak D'Souza, Telikepalli Kavitha, and Jaikumar Radhakrishnan, editors, *IARCS Annual Conference on Foundations of Software Technology and Theoretical Computer Science (FSTTCS 2012)*, volume 18 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 546–560, Dagstuhl, Germany, 2012. Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik.