1. Execution trace

Let's execute the handshake protocol with two principals, Alice and Bob. At the beginning of execution, the run $\mathcal{R}$ will be

$\mathcal{R}^0$ = {{Alice, Bob}, {{Alice, **Init**, ⟨Alice, Bob⟩, 1}, {Bob, **Init**, ⟨Bob⟩, 2}}, ⟨ ⟩, { }} .

Note that the *thread_id*s have been chosen arbitrarily; the only condition on them is that they are distinct.

We now execute the protocol step-by-step. The run $\mathcal{R}$ will, after Alice executes the "k := **newnonce**" *action*, be as follows:

$\mathcal{R}^1$ = {{Alice, Bob}, {{Alice, **Init**, ⟨Alice, Bob⟩, 1}, {Bob, **Init**, ⟨Bob⟩, 2}},
⟨
⟨1; k := **newnonce**⟩
⟩,
{⟨⟨1, k⟩, N_1⟩}} ,

where we use N_1 as a meta-variable for some unspecified nonce, the only condition for which is that is "doesn't occur" in run $\mathcal{R}^0$ (the meaning of which is defined in section 4.1).

After Alice's "siga := **sign** ⟨Alice, Bob, !k⟩, sk(Alice)" action, the run looks as follows:

$\mathcal{R}^2$ = {{Alice, Bob}, {{Alice, **Init**, ⟨Alice, Bob⟩, 1}, {Bob, **Init**, ⟨Bob⟩, 2}},
⟨
⟨1; k := **newnonce**⟩,
⟨1; siga := **sign** ⟨Alice, Bob, N_1⟩, sk(Alice)⟩
⟩,
{⟨⟨1, k⟩, N_1⟩, ⟨⟨1, siga⟩, $\left[\!\left[\langle \mathrm{Alice}, \mathrm{Bob}, N_1 \rangle\right]\!\right]_{\mathrm{sk(Alice)}}$⟩}}

Continuing, we obtain the following:

$\mathcal{R}^3$ = {{Alice, Bob}, {{Alice, **Init**, ⟨Alice, Bob⟩, 1}, {Bob, **Init**, ⟨Bob⟩, 2}},
⟨
⟨1; k := **newnonce**⟩,
⟨1; siga := **sign** ⟨Alice, Bob, N_1⟩, sk(Alice)⟩,
⟨1; enca := **enc** $\left[\!\left[\langle \mathrm{Alice}, \mathrm{Bob}, N_1 \rangle\right]\!\right]_{\mathrm{sk(Alice)}}$, pk(Bob)⟩
⟩,
{
⟨⟨1, k⟩, N_1⟩,
⟨⟨1, siga⟩, $\left[\!\left[\langle \mathrm{Alice}, \mathrm{Bob}, N_1 \rangle\right]\!\right]_{\mathrm{sk(Alice)}}$⟩,
⟨⟨1, enca⟩, $\left\{\left[\!\left[\langle \mathrm{Alice}, \mathrm{Bob}, N_1 \rangle\right]\!\right]_{\mathrm{sk(Alice)}}\right\}^{a}_{\mathrm{pk(Bob)}}$⟩
}}

$\mathcal{R}^4$ = {{Alice, Bob}, {{Alice, **Init**, ⟨Alice, Bob⟩, 1}, {Bob, **Init**, ⟨Bob⟩, 2}},
⟨
⟨1; k := **newnonce**⟩,
⟨1; siga := **sign** ⟨Alice, Bob, N_1⟩, sk(Alice)⟩,
⟨1; enca := **enc** $\left[\!\left[\langle \mathrm{Alice}, \mathrm{Bob}, N_1 \rangle\right]\!\right]_{\mathrm{sk(Alice)}}$, pk(Bob)⟩,
⟨1; **send** $\left\{\left[\!\left[\langle \mathrm{Alice}, \mathrm{Bob}, N_1 \rangle\right]\!\right]_{\mathrm{sk(Alice)}}\right\}^{a}_{\mathrm{pk(Bob)}}$⟩
⟩,
{
⟨⟨1, k⟩, N_1⟩,

⟨⟨1, siga⟩, $\left[\!\left|\langle \mathrm{Alice}, \mathrm{Bob}, \mathrm{N}_1 \rangle\right|\!\right]_{\mathrm{sk(Alice)}}$⟩,

⟨⟨1, enca⟩, $\left\{\left[\!\left|\langle \mathrm{Alice}, \mathrm{Bob}, \mathrm{N}_1 \rangle\right|\!\right]_{\mathrm{sk(Alice)}}\right|\}^{\mathrm{a}}_{\mathrm{pk(Bob)}}$⟩

}}

$\mathcal{R}^5$ = {{Alice, Bob}, {{Alice, **Init**, ⟨Alice, Bob⟩, 1}, {Bob, **Init**, ⟨Bob⟩, 2}},

⟨

⟨1; k := **newnonce**⟩,

⟨1; siga := **sign** ⟨Alice, Bob, N_1⟩, sk(Alice)⟩,

⟨1; enca := **enc** $\left[\!\left|\langle \mathrm{Alice}, \mathrm{Bob}, \mathrm{N}_1 \rangle\right|\!\right]_{\mathrm{sk(Alice)}}$, pk(Bob)⟩,

⟨1; **send** $\left\{\left[\!\left|\langle \mathrm{Alice}, \mathrm{Bob}, \mathrm{N}_1 \rangle\right|\!\right]_{\mathrm{sk(Alice)}}\right|\}^{\mathrm{a}}_{\mathrm{pk(Bob)}}$⟩,

⟨2; enca := **receive**⟩

⟩,

{

⟨⟨1, k⟩, N_1⟩,

⟨⟨1, siga⟩, $\left[\!\left|\langle \mathrm{Alice}, \mathrm{Bob}, \mathrm{N}_1 \rangle\right|\!\right]_{\mathrm{sk(Alice)}}$⟩,

⟨⟨1, enca⟩, $\left\{\left[\!\left|\langle \mathrm{Alice}, \mathrm{Bob}, \mathrm{N}_1 \rangle\right|\!\right]_{\mathrm{sk(Alice)}}\right|\}^{\mathrm{a}}_{\mathrm{pk(Bob)}}$⟩,

⟨⟨2, enca⟩, $\left\{\left[\!\left|\langle \mathrm{Alice}, \mathrm{Bob}, \mathrm{N}_1 \rangle\right|\!\right]_{\mathrm{sk(Alice)}}\right|\}^{\mathrm{a}}_{\mathrm{pk(Bob)}}$⟩

}}

$\mathcal{R}^6$ = {{Alice, Bob}, {{Alice, **Init**, ⟨Alice, Bob⟩, 1}, {Bob, **Init**, ⟨Bob⟩, 2}},

⟨

⟨1; k := **newnonce**⟩,

⟨1; siga := **sign** ⟨Alice, Bob, N_1⟩, sk(Alice)⟩,

⟨1; enca := **enc** $\left[\!\left|\langle \mathrm{Alice}, \mathrm{Bob}, \mathrm{N}_1 \rangle\right|\!\right]_{\mathrm{sk(Alice)}}$, pk(Bob)⟩,

⟨1; **send** $\left\{\left[\!\left|\langle \mathrm{Alice}, \mathrm{Bob}, \mathrm{N}_1 \rangle\right|\!\right]_{\mathrm{sk(Alice)}}\right|\}^{\mathrm{a}}_{\mathrm{pk(Bob)}}$⟩,

⟨2; enca := **receive**⟩,

⟨2; siga := **dec** $\left\{\left[\!\left|\langle \mathrm{Alice}, \mathrm{Bob}, \mathrm{N}_1 \rangle\right|\!\right]_{\mathrm{sk(Alice)}}\right|\}^{\mathrm{a}}_{\mathrm{pk(Bob)}}$, dk(Bob)⟩

⟩,

{

⟨⟨1, k⟩, N_1⟩,

⟨⟨1, siga⟩, $\left[\!\left|\langle \mathrm{Alice}, \mathrm{Bob}, \mathrm{N}_1 \rangle\right|\!\right]_{\mathrm{sk(Alice)}}$⟩,

⟨⟨1, enca⟩, $\left\{\left[\!\left|\langle \mathrm{Alice}, \mathrm{Bob}, \mathrm{N}_1 \rangle\right|\!\right]_{\mathrm{sk(Alice)}}\right|\}^{\mathrm{a}}_{\mathrm{pk(Bob)}}$⟩,

⟨⟨2, enca⟩, $\left\{\left[\!\left|\langle \mathrm{Alice}, \mathrm{Bob}, \mathrm{N}_1 \rangle\right|\!\right]_{\mathrm{sk(Alice)}}\right|\}^{\mathrm{a}}_{\mathrm{pk(Bob)}}$⟩,

⟨⟨2, siga⟩, $\left[\!\left|\langle \mathrm{Alice}, \mathrm{Bob}, \mathrm{N}_1 \rangle\right|\!\right]_{\mathrm{sk(Alice)}}$⟩

}}

$\mathcal{R}^7$ = {{Alice, Bob}, {{Alice, **Init**, ⟨Alice, Bob⟩, 1}, {Bob, **Init**, ⟨Bob⟩, 2}},

⟨
⟨1; k := **newnonce**⟩,
⟨1; siga := **sign** ⟨Alice, Bob, N_1⟩, sk(Alice)⟩,
⟨1; enca := **enc** $\left[\left\langle \text{Alice}, \text{Bob}, N_1 \right\rangle\right]_{\text{sk(Alice)}}$, pk(Bob)⟩,
⟨1; **send** $\left\{\left[\left\langle \text{Alice}, \text{Bob}, N_1 \right\rangle\right]_{\text{sk(Alice)}}\right\}^{a}_{\text{pk(Bob)}}$⟩,
⟨2; enca := **receive**⟩,
⟨2; siga := **dec** $\left\{\left[\left\langle \text{Alice}, \text{Bob}, N_1 \right\rangle\right]_{\text{sk(Alice)}}\right\}^{a}_{\text{pk(Bob)}}$, dk(Bob)⟩,
⟨2; texta := **unsign** $\left[\left\langle \text{Alice}, \text{Bob}, N_1 \right\rangle\right]_{\text{sk(Alice)}}$⟩
⟩,
{
⟨⟨1, k⟩, N_1⟩,
⟨⟨1, siga⟩, $\left[\left\langle \text{Alice}, \text{Bob}, N_1 \right\rangle\right]_{\text{sk(Alice)}}$⟩,
⟨⟨1, enca⟩, $\left\{\left[\left\langle \text{Alice}, \text{Bob}, N_1 \right\rangle\right]_{\text{sk(Alice)}}\right\}^{a}_{\text{pk(Bob)}}$⟩,
⟨⟨2, enca⟩, $\left\{\left[\left\langle \text{Alice}, \text{Bob}, N_1 \right\rangle\right]_{\text{sk(Alice)}}\right\}^{a}_{\text{pk(Bob)}}$⟩,
⟨⟨2, siga⟩, $\left[\left\langle \text{Alice}, \text{Bob}, N_1 \right\rangle\right]_{\text{sk(Alice)}}$⟩,
⟨⟨2, texta⟩, ⟨Alice, Bob, N_1⟩⟩
}}

$\mathcal{R}^8$ = {{Alice, Bob}, {{Alice, **Init**, ⟨Alice, Bob⟩, 1}, {Bob, **Init**, ⟨Bob⟩, 2}},
⟨
⟨1; k := **newnonce**⟩,
⟨1; siga := **sign** ⟨Alice, Bob, N_1⟩, sk(Alice)⟩,
⟨1; enca := **enc** $\left[\left\langle \text{Alice}, \text{Bob}, N_1 \right\rangle\right]_{\text{sk(Alice)}}$, pk(Bob)⟩,
⟨1; **send** $\left\{\left[\left\langle \text{Alice}, \text{Bob}, N_1 \right\rangle\right]_{\text{sk(Alice)}}\right\}^{a}_{\text{pk(Bob)}}$⟩,
⟨2; enca := **receive**⟩,
⟨2; siga := **dec** $\left\{\left[\left\langle \text{Alice}, \text{Bob}, N_1 \right\rangle\right]_{\text{sk(Alice)}}\right\}^{a}_{\text{pk(Bob)}}$, dk(Bob)⟩,
⟨2; texta := **unsign** $\left[\left\langle \text{Alice}, \text{Bob}, N_1 \right\rangle\right]_{\text{sk(Alice)}}$⟩,
⟨2; idA := π_1 ⟨Alice, Bob, N_1⟩
⟩,
{
⟨⟨1, k⟩, N_1⟩,
⟨⟨1, siga⟩, $\left[\left\langle \text{Alice}, \text{Bob}, N_1 \right\rangle\right]_{\text{sk(Alice)}}$⟩,
⟨⟨1, enca⟩, $\left\{\left[\left\langle \text{Alice}, \text{Bob}, N_1 \right\rangle\right]_{\text{sk(Alice)}}\right\}^{a}_{\text{pk(Bob)}}$⟩,
⟨⟨2, enca⟩, $\left\{\left[\left\langle \text{Alice}, \text{Bob}, N_1 \right\rangle\right]_{\text{sk(Alice)}}\right\}^{a}_{\text{pk(Bob)}}$⟩,

⟨⟨2, siga⟩, $\left[\!\left|\langle \mathrm{Alice}, \mathrm{Bob}, \mathrm{N}_1 \rangle\right|\!\right]_{\mathrm{sk(Alice)}}$⟩,

⟨⟨2, texta⟩, ⟨Alice, Bob, N_1⟩⟩,

⟨⟨2, idA⟩, Alice⟩

}}

$\mathcal{R}^9$ = {{Alice, Bob}, {{Alice, **Init**, ⟨Alice, Bob⟩, 1}, {Bob, **Init**, ⟨Bob⟩, 2}},

⟨

⟨1; k := **newnonce**⟩,

⟨1; siga := **sign** ⟨Alice, Bob, N_1⟩, sk(Alice)⟩,

⟨1; enca := **enc** $\left[\!\left|\langle \mathrm{Alice}, \mathrm{Bob}, \mathrm{N}_1 \rangle\right|\!\right]_{\mathrm{sk(Alice)}}$, pk(Bob)⟩,

⟨1; **send** $\left\{\left[\!\left|\langle \mathrm{Alice}, \mathrm{Bob}, \mathrm{N}_1 \rangle\right|\!\right]_{\mathrm{sk(Alice)}}\right|\}^{\mathrm{a}}_{\mathrm{pk(Bob)}}$⟩,

⟨2; enca := **receive**⟩,

⟨2; siga := **dec** $\left\{\left[\!\left|\langle \mathrm{Alice}, \mathrm{Bob}, \mathrm{N}_1 \rangle\right|\!\right]_{\mathrm{sk(Alice)}}\right|\}^{\mathrm{a}}_{\mathrm{pk(Bob)}}$, dk(Bob)⟩,

⟨2; texta := **unsign** $\left[\!\left|\langle \mathrm{Alice}, \mathrm{Bob}, \mathrm{N}_1 \rangle\right|\!\right]_{\mathrm{sk(Alice)}}$⟩,

⟨2; idA := π_1 ⟨Alice, Bob, N_1⟩,

⟨2; idB := π_2 ⟨Alice, Bob, N_1⟩

⟩,

{

⟨⟨1, k⟩, N_1⟩,

⟨⟨1, siga⟩, $\left[\!\left|\langle \mathrm{Alice}, \mathrm{Bob}, \mathrm{N}_1 \rangle\right|\!\right]_{\mathrm{sk(Alice)}}$⟩,

⟨⟨1, enca⟩, $\left\{\left[\!\left|\langle \mathrm{Alice}, \mathrm{Bob}, \mathrm{N}_1 \rangle\right|\!\right]_{\mathrm{sk(Alice)}}\right|\}^{\mathrm{a}}_{\mathrm{pk(Bob)}}$⟩,

⟨⟨2, enca⟩, $\left\{\left[\!\left|\langle \mathrm{Alice}, \mathrm{Bob}, \mathrm{N}_1 \rangle\right|\!\right]_{\mathrm{sk(Alice)}}\right|\}^{\mathrm{a}}_{\mathrm{pk(Bob)}}$⟩,

⟨⟨2, siga⟩, $\left[\!\left|\langle \mathrm{Alice}, \mathrm{Bob}, \mathrm{N}_1 \rangle\right|\!\right]_{\mathrm{sk(Alice)}}$⟩,

⟨⟨2, texta⟩, ⟨Alice, Bob, N_1⟩⟩,

⟨⟨2, idA⟩, Alice⟩,

⟨⟨2, idB⟩, Bob⟩

}}

$\mathcal{R}^{10}$ = {{Alice, Bob}, {{Alice, **Init**, ⟨Alice, Bob⟩, 1}, {Bob, **Init**, ⟨Bob⟩, 2}},

⟨

⟨1; k := **newnonce**⟩,

⟨1; siga := **sign** ⟨Alice, Bob, N_1⟩, sk(Alice)⟩,

⟨1; enca := **enc** $\left[\!\left|\langle \mathrm{Alice}, \mathrm{Bob}, \mathrm{N}_1 \rangle\right|\!\right]_{\mathrm{sk(Alice)}}$, pk(Bob)⟩,

⟨1; **send** $\left\{\left[\!\left|\langle \mathrm{Alice}, \mathrm{Bob}, \mathrm{N}_1 \rangle\right|\!\right]_{\mathrm{sk(Alice)}}\right|\}^{\mathrm{a}}_{\mathrm{pk(Bob)}}$⟩,

⟨2; enca := **receive**⟩,

⟨2; siga := **dec** $\left\{\left[\!\left|\langle \mathrm{Alice}, \mathrm{Bob}, \mathrm{N}_1 \rangle\right|\!\right]_{\mathrm{sk(Alice)}}\right|\}^{\mathrm{a}}_{\mathrm{pk(Bob)}}$, dk(Bob)⟩,

⟨2; texta := **unsign** $\left[\!\left|\langle \mathrm{Alice}, \mathrm{Bob}, \mathrm{N}_1 \rangle\right|\!\right]_{\mathrm{sk(Alice)}}$⟩,

⟨2; idA := π_1 ⟨Alice, Bob, N_1⟩,

⟨2; idB := π_2 ⟨Alice, Bob, N_1⟩,
⟨2; k := π_3 ⟨Alice, Bob, N_1⟩
⟩,
{
⟨⟨1, k⟩, N_1⟩,
⟨⟨1, siga⟩, $\left[\left|\langle \mathrm{Alice}, \mathrm{Bob}, N_1 \rangle\right|\right]_{\mathrm{sk(Alice)}}$⟩,
⟨⟨1, enca⟩, $\left\{\left[\left|\langle \mathrm{Alice}, \mathrm{Bob}, N_1 \rangle\right|\right]_{\mathrm{sk(Alice)}}\right|\}^{a}_{\mathrm{pk(Bob)}}$⟩,
⟨⟨2, enca⟩, $\left\{\left[\left|\langle \mathrm{Alice}, \mathrm{Bob}, N_1 \rangle\right|\right]_{\mathrm{sk(Alice)}}\right|\}^{a}_{\mathrm{pk(Bob)}}$⟩,
⟨⟨2, siga⟩, $\left[\left|\langle \mathrm{Alice}, \mathrm{Bob}, N_1 \rangle\right|\right]_{\mathrm{sk(Alice)}}$⟩,
⟨⟨2, texta⟩, ⟨Alice, Bob, N_1⟩⟩,
⟨⟨2, idA⟩, Alice⟩,
⟨⟨2, idB⟩, Bob⟩,
⟨⟨2, k⟩, N_1⟩
}}

$\Re^{11}$ = {{Alice, Bob}, {{Alice, **Init**, ⟨Alice, Bob⟩, 1}, {Bob, **Init**, ⟨Bob⟩, 2}},
⟨
⟨1; k := **newnonce**⟩,
⟨1; siga := **sign** ⟨Alice, Bob, N_1⟩, sk(Alice)⟩,
⟨1; enca := **enc** $\left[\left|\langle \mathrm{Alice}, \mathrm{Bob}, N_1 \rangle\right|\right]_{\mathrm{sk(Alice)}}$, pk(Bob)⟩,
⟨1; **send** $\left\{\left[\left|\langle \mathrm{Alice}, \mathrm{Bob}, N_1 \rangle\right|\right]_{\mathrm{sk(Alice)}}\right|\}^{a}_{\mathrm{pk(Bob)}}$⟩,
⟨2; enca := **receive**⟩,
⟨2; siga := **dec** $\left\{\left[\left|\langle \mathrm{Alice}, \mathrm{Bob}, N_1 \rangle\right|\right]_{\mathrm{sk(Alice)}}\right|\}^{a}_{\mathrm{pk(Bob)}}$, dk(Bob)⟩,
⟨2; texta := **unsign** $\left[\left|\langle \mathrm{Alice}, \mathrm{Bob}, N_1 \rangle\right|\right]_{\mathrm{sk(Alice)}}$⟩,
⟨2; idA := π_1 ⟨Alice, Bob, N_1⟩,
⟨2; idB := π_2 ⟨Alice, Bob, N_1⟩,
⟨2; k := π_3 ⟨Alice, Bob, N_1⟩,
⟨2; **verify** $\left[\left|\langle \mathrm{Alice}, \mathrm{Bob}, N_1 \rangle\right|\right]_{\mathrm{sk(Alice)}}$, vk(Alice)⟩
⟩,
{
⟨⟨1, k⟩, N_1⟩,
⟨⟨1, siga⟩, $\left[\left|\langle \mathrm{Alice}, \mathrm{Bob}, N_1 \rangle\right|\right]_{\mathrm{sk(Alice)}}$⟩,
⟨⟨1, enca⟩, $\left\{\left[\left|\langle \mathrm{Alice}, \mathrm{Bob}, N_1 \rangle\right|\right]_{\mathrm{sk(Alice)}}\right|\}^{a}_{\mathrm{pk(Bob)}}$⟩,
⟨⟨2, enca⟩, $\left\{\left[\left|\langle \mathrm{Alice}, \mathrm{Bob}, N_1 \rangle\right|\right]_{\mathrm{sk(Alice)}}\right|\}^{a}_{\mathrm{pk(Bob)}}$⟩,
⟨⟨2, siga⟩, $\left[\left|\langle \mathrm{Alice}, \mathrm{Bob}, N_1 \rangle\right|\right]_{\mathrm{sk(Alice)}}$⟩,
⟨⟨2, texta⟩, ⟨Alice, Bob, N_1⟩⟩,
⟨⟨2, idA⟩, Alice⟩,

⟨⟨2, idB⟩, Bob⟩,
⟨⟨2, k⟩, N_1⟩
}}

$\mathcal{R}^{12}$ = {{Alice, Bob}, {{Alice, **Init**, ⟨Alice, Bob⟩, 1}, {Bob, **Init**, ⟨Bob⟩, 2}},
⟨
⟨1; k := **newnonce**⟩,
⟨1; siga := **sign** ⟨Alice, Bob, N_1⟩, sk(Alice)⟩,
⟨1; enca := **enc** $\left[\left\langle \text{Alice}, \text{Bob}, N_1 \right\rangle\right]_{\text{sk(Alice)}}$, pk(Bob)⟩,
⟨1; **send** $\left\{\left[\left\langle \text{Alice}, \text{Bob}, N_1 \right\rangle\right]_{\text{sk(Alice)}}\right\}^{a}_{\text{pk(Bob)}}$⟩,
⟨2; enca := **receive**⟩,
⟨2; siga := **dec** $\left\{\left[\left\langle \text{Alice}, \text{Bob}, N_1 \right\rangle\right]_{\text{sk(Alice)}}\right\}^{a}_{\text{pk(Bob)}}$, dk(Bob)⟩,
⟨2; texta := **unsign** $\left[\left\langle \text{Alice}, \text{Bob}, N_1 \right\rangle\right]_{\text{sk(Alice)}}$⟩,
⟨2; idA := π_1 ⟨Alice, Bob, N_1⟩,
⟨2; idB := π_2 ⟨Alice, Bob, N_1⟩,
⟨2; k := π_3 ⟨Alice, Bob, N_1⟩,
⟨2; **verify** $\left[\left\langle \text{Alice}, \text{Bob}, N_1 \right\rangle\right]_{\text{sk(Alice)}}$, vk(Alice)⟩,
⟨2; **assert:** Bob=Bob⟩
⟩,
{
⟨⟨1, k⟩, N_1⟩,
⟨⟨1, siga⟩, $\left[\left\langle \text{Alice}, \text{Bob}, N_1 \right\rangle\right]_{\text{sk(Alice)}}$⟩,
⟨⟨1, enca⟩, $\left\{\left[\left\langle \text{Alice}, \text{Bob}, N_1 \right\rangle\right]_{\text{sk(Alice)}}\right\}^{a}_{\text{pk(Bob)}}$⟩,
⟨⟨2, enca⟩, $\left\{\left[\left\langle \text{Alice}, \text{Bob}, N_1 \right\rangle\right]_{\text{sk(Alice)}}\right\}^{a}_{\text{pk(Bob)}}$⟩,
⟨⟨2, siga⟩, $\left[\left\langle \text{Alice}, \text{Bob}, N_1 \right\rangle\right]_{\text{sk(Alice)}}$⟩,
⟨⟨2, texta⟩, ⟨Alice, Bob, N_1⟩⟩,
⟨⟨2, idA⟩, Alice⟩,
⟨⟨2, idB⟩, Bob⟩,
⟨⟨2, k⟩, N_1⟩
}}

$\mathcal{R}^{13}$ = {{Alice, Bob}, {{Alice, **Init**, ⟨Alice, Bob⟩, 1}, {Bob, **Init**, ⟨Bob⟩, 2}},
⟨
⟨1; k := **newnonce**⟩,
⟨1; siga := **sign** ⟨Alice, Bob, N_1⟩, sk(Alice)⟩,
⟨1; enca := **enc** $\left[\left\langle \text{Alice}, \text{Bob}, N_1 \right\rangle\right]_{\text{sk(Alice)}}$, pk(Bob)⟩,
⟨1; **send** $\left\{\left[\left\langle \text{Alice}, \text{Bob}, N_1 \right\rangle\right]_{\text{sk(Alice)}}\right\}^{a}_{\text{pk(Bob)}}$⟩,
⟨2; enca := **receive**⟩,
⟨2; siga := **dec** $\left\{\left[\left\langle \text{Alice}, \text{Bob}, N_1 \right\rangle\right]_{\text{sk(Alice)}}\right\}^{a}_{\text{pk(Bob)}}$, dk(Bob)⟩,

⟨2; texta := **unsign** $\left[\left|\langle \mathrm{Alice}, \mathrm{Bob}, \mathrm{N}_1 \rangle\right|\right]_{\mathrm{sk(Alice)}}$⟩,
⟨2; idA := π_1 ⟨Alice, Bob, N_1⟩,
⟨2; idB := π_2 ⟨Alice, Bob, N_1⟩,
⟨2; k := π_3 ⟨Alice, Bob, N_1⟩,
⟨2; **verify** $\left[\left|\langle \mathrm{Alice}, \mathrm{Bob}, \mathrm{N}_1 \rangle\right|\right]_{\mathrm{sk(Alice)}}$, vk(Alice)⟩,
⟨2; **assert:** Bob=Bob⟩,
⟨2; s := **newnonce**⟩
⟩,
{
⟨⟨1, k⟩, N_1⟩,
⟨⟨1, siga⟩, $\left[\left|\langle \mathrm{Alice}, \mathrm{Bob}, \mathrm{N}_1 \rangle\right|\right]_{\mathrm{sk(Alice)}}$⟩,
⟨⟨1, enca⟩, $\left\{\left[\left|\langle \mathrm{Alice}, \mathrm{Bob}, \mathrm{N}_1 \rangle\right|\right]_{\mathrm{sk(Alice)}}\right|\}^{a}_{\mathrm{pk(Bob)}}$⟩,
⟨⟨2, enca⟩, $\left\{\left[\left|\langle \mathrm{Alice}, \mathrm{Bob}, \mathrm{N}_1 \rangle\right|\right]_{\mathrm{sk(Alice)}}\right|\}^{a}_{\mathrm{pk(Bob)}}$⟩,
⟨⟨2, siga⟩, $\left[\left|\langle \mathrm{Alice}, \mathrm{Bob}, \mathrm{N}_1 \rangle\right|\right]_{\mathrm{sk(Alice)}}$⟩,
⟨⟨2, texta⟩, ⟨Alice, Bob, N_1⟩⟩,
⟨⟨2, idA⟩, Alice⟩,
⟨⟨2, idB⟩, Bob⟩,
⟨⟨2, k⟩, N_1⟩,
⟨⟨2, s⟩, N_2⟩ (Here, N_2 does not occur in $\mathfrak{R}^{12}$.)
}}

$\mathfrak{R}^{14}$ = {{Alice, Bob}, {{Alice, **Init**, ⟨Alice, Bob⟩, 1}, {Bob, **Init**, ⟨Bob⟩, 2}},
⟨
⟨1; k := **newnonce**⟩,
⟨1; siga := **sign** ⟨Alice, Bob, N_1⟩, sk(Alice)⟩,
⟨1; enca := **enc** $\left[\left|\langle \mathrm{Alice}, \mathrm{Bob}, \mathrm{N}_1 \rangle\right|\right]_{\mathrm{sk(Alice)}}$, pk(Bob)⟩,
⟨1; **send** $\left\{\left[\left|\langle \mathrm{Alice}, \mathrm{Bob}, \mathrm{N}_1 \rangle\right|\right]_{\mathrm{sk(Alice)}}\right|\}^{a}_{\mathrm{pk(Bob)}}$⟩,
⟨2; enca := **receive**⟩,
⟨2; siga := **dec** $\left\{\left[\left|\langle \mathrm{Alice}, \mathrm{Bob}, \mathrm{N}_1 \rangle\right|\right]_{\mathrm{sk(Alice)}}\right|\}^{a}_{\mathrm{pk(Bob)}}$, dk(Bob)⟩,
⟨2; texta := **unsign** $\left[\left|\langle \mathrm{Alice}, \mathrm{Bob}, \mathrm{N}_1 \rangle\right|\right]_{\mathrm{sk(Alice)}}$⟩,
⟨2; idA := π_1 ⟨Alice, Bob, N_1⟩,
⟨2; idB := π_2 ⟨Alice, Bob, N_1⟩,
⟨2; k := π_3 ⟨Alice, Bob, N_1⟩,
⟨2; **verify** $\left[\left|\langle \mathrm{Alice}, \mathrm{Bob}, \mathrm{N}_1 \rangle\right|\right]_{\mathrm{sk(Alice)}}$, vk(Alice)⟩,
⟨2; **assert:** Bob=Bob⟩,
⟨2; s := **newnonce**⟩,
⟨2; encb := **se** N_2, N_1⟩
⟩,
{
⟨⟨1, k⟩, N_1⟩,

$\langle\langle 1, \texttt{siga}\rangle, \ \left[\!\left|\langle \text{Alice}, \text{Bob}, N_1\rangle\right|\!\right]_{sk(\text{Alice})}\rangle,$

$\langle\langle 1, \texttt{enca}\rangle, \ \left\{\!\left|\left[\!\left|\langle \text{Alice}, \text{Bob}, N_1\rangle\right|\!\right]_{sk(\text{Alice})}\right|\!\right\}^{a}_{pk(\text{Bob})}\rangle,$

$\langle\langle 2, \texttt{enca}\rangle, \ \left\{\!\left|\left[\!\left|\langle \text{Alice}, \text{Bob}, N_1\rangle\right|\!\right]_{sk(\text{Alice})}\right|\!\right\}^{a}_{pk(\text{Bob})}\rangle,$

$\langle\langle 2, \texttt{siga}\rangle, \ \left[\!\left|\langle \text{Alice}, \text{Bob}, N_1\rangle\right|\!\right]_{sk(\text{Alice})}\rangle,$

$\langle\langle 2, \texttt{texta}\rangle, \langle \text{Alice}, \text{Bob}, N_1\rangle\rangle,$

$\langle\langle 2, \texttt{idA}\rangle, \text{Alice}\rangle,$

$\langle\langle 2, \texttt{idB}\rangle, \text{Bob}\rangle,$

$\langle\langle 2, \texttt{k}\rangle, N_1\rangle,$

$\langle\langle 2, \texttt{s}\rangle, N_2\rangle,$

$\langle\langle 2, \texttt{encb}\rangle, \ \left\{\!\left|N_2\right|\!\right\}^{s}_{N_1}\rangle$

}}

$\Re^{15}$ = {{Alice, Bob}, {{Alice, **Init**, ⟨Alice, Bob⟩, 1}, {Bob, **Init**, ⟨Bob⟩, 2}},

⟨

⟨1; k := **newnonce**⟩,

⟨1; siga := **sign** ⟨Alice, Bob, N_1⟩, sk(Alice)⟩,

⟨1; enca := **enc** $\left[\!\left|\langle \text{Alice}, \text{Bob}, N_1\rangle\right|\!\right]_{sk(\text{Alice})}$, pk(Bob)⟩,

⟨1; **send** $\left\{\!\left|\left[\!\left|\langle \text{Alice}, \text{Bob}, N_1\rangle\right|\!\right]_{sk(\text{Alice})}\right|\!\right\}^{a}_{pk(\text{Bob})}\rangle,$

⟨2; enca := **receive**⟩,

⟨2; siga := **dec** $\left\{\!\left|\left[\!\left|\langle \text{Alice}, \text{Bob}, N_1\rangle\right|\!\right]_{sk(\text{Alice})}\right|\!\right\}^{a}_{pk(\text{Bob})}$, dk(Bob)⟩,

⟨2; texta := **unsign** $\left[\!\left|\langle \text{Alice}, \text{Bob}, N_1\rangle\right|\!\right]_{sk(\text{Alice})}\rangle,$

⟨2; idA := π_1 ⟨Alice, Bob, N_1⟩,

⟨2; idB := π_2 ⟨Alice, Bob, N_1⟩,

⟨2; k := π_3 ⟨Alice, Bob, N_1⟩,

⟨2; **verify** $\left[\!\left|\langle \text{Alice}, \text{Bob}, N_1\rangle\right|\!\right]_{sk(\text{Alice})}$, vk(Alice)⟩,

⟨2; **assert:** Bob=Bob⟩,

⟨2; s := **newnonce**⟩,

⟨2; encb := **se** N_2, N_1⟩,

⟨2; **send** $\left\{\!\left|N_2\right|\!\right\}^{s}_{N_1}\rangle$

⟩,

{

⟨⟨1, k⟩, N_1⟩,

$\langle\langle 1, \texttt{siga}\rangle, \ \left[\!\left|\langle \text{Alice}, \text{Bob}, N_1\rangle\right|\!\right]_{sk(\text{Alice})}\rangle,$

$\langle\langle 1, \texttt{enca}\rangle, \ \left\{\!\left|\left[\!\left|\langle \text{Alice}, \text{Bob}, N_1\rangle\right|\!\right]_{sk(\text{Alice})}\right|\!\right\}^{a}_{pk(\text{Bob})}\rangle,$

$\langle\langle 2, \texttt{enca}\rangle, \ \left\{\!\left|\left[\!\left|\langle \text{Alice}, \text{Bob}, N_1\rangle\right|\!\right]_{sk(\text{Alice})}\right|\!\right\}^{a}_{pk(\text{Bob})}\rangle,$

⟨⟨2, siga⟩, $\left[\!\left|\langle \mathrm{Alice}, \mathrm{Bob}, \mathrm{N}_1 \rangle\right|\!\right]_{\mathrm{sk(Alice)}}$⟩,
⟨⟨2, texta⟩, ⟨Alice, Bob, N_1⟩⟩,
⟨⟨2, idA⟩, Alice⟩,
⟨⟨2, idB⟩, Bob⟩,
⟨⟨2, k⟩, N_1⟩,
⟨⟨2, s⟩, N_2⟩,
⟨⟨2, encb⟩, $\left\{\left|\mathrm{N}_2\right|\right\}^{\mathrm{s}}_{\mathrm{N}_1}$⟩
}}

$\Re^{16}$ = {{Alice, Bob}, {{Alice, **Init**, ⟨Alice, Bob⟩, 1}, {Bob, **Init**, ⟨Bob⟩, 2}},
⟨
⟨1; k := **newnonce**⟩,
⟨1; siga := **sign** ⟨Alice, Bob, N_1⟩, sk(Alice)⟩,
⟨1; enca := **enc** $\left[\!\left|\langle \mathrm{Alice}, \mathrm{Bob}, \mathrm{N}_1 \rangle\right|\!\right]_{\mathrm{sk(Alice)}}$, pk(Bob)⟩,
⟨1; **send** $\left\{\left[\!\left|\langle \mathrm{Alice}, \mathrm{Bob}, \mathrm{N}_1 \rangle\right|\!\right]_{\mathrm{sk(Alice)}}\right\}^{\mathrm{a}}_{\mathrm{pk(Bob)}}$⟩,
⟨2; enca := **receive**⟩,
⟨2; siga := **dec** $\left\{\left[\!\left|\langle \mathrm{Alice}, \mathrm{Bob}, \mathrm{N}_1 \rangle\right|\!\right]_{\mathrm{sk(Alice)}}\right\}^{\mathrm{a}}_{\mathrm{pk(Bob)}}$, dk(Bob)⟩,
⟨2; texta := **unsign** $\left[\!\left|\langle \mathrm{Alice}, \mathrm{Bob}, \mathrm{N}_1 \rangle\right|\!\right]_{\mathrm{sk(Alice)}}$⟩,
⟨2; idA := π_1 ⟨Alice, Bob, N_1⟩,
⟨2; idB := π_2 ⟨Alice, Bob, N_1⟩,
⟨2; k := π_3 ⟨Alice, Bob, N_1⟩,
⟨2; **verify** $\left[\!\left|\langle \mathrm{Alice}, \mathrm{Bob}, \mathrm{N}_1 \rangle\right|\!\right]_{\mathrm{sk(Alice)}}$, vk(Alice)⟩,
⟨2; **assert:** Bob=Bob⟩,
⟨2; s := **newnonce**⟩,
⟨2; encb := **se** N_2, N_1⟩,
⟨2; **send** $\left\{\left|\mathrm{N}_2\right|\right\}^{\mathrm{s}}_{\mathrm{N}_1}$⟩,
⟨1; encb := **receive**⟩
⟩,
{
⟨⟨1, k⟩, N_1⟩,
⟨⟨1, siga⟩, $\left[\!\left|\langle \mathrm{Alice}, \mathrm{Bob}, \mathrm{N}_1 \rangle\right|\!\right]_{\mathrm{sk(Alice)}}$⟩,
⟨⟨1, enca⟩, $\left\{\left[\!\left|\langle \mathrm{Alice}, \mathrm{Bob}, \mathrm{N}_1 \rangle\right|\!\right]_{\mathrm{sk(Alice)}}\right\}^{\mathrm{a}}_{\mathrm{pk(Bob)}}$⟩,
⟨⟨2, enca⟩, $\left\{\left[\!\left|\langle \mathrm{Alice}, \mathrm{Bob}, \mathrm{N}_1 \rangle\right|\!\right]_{\mathrm{sk(Alice)}}\right\}^{\mathrm{a}}_{\mathrm{pk(Bob)}}$⟩,
⟨⟨2, siga⟩, $\left[\!\left|\langle \mathrm{Alice}, \mathrm{Bob}, \mathrm{N}_1 \rangle\right|\!\right]_{\mathrm{sk(Alice)}}$⟩,
⟨⟨2, texta⟩, ⟨Alice, Bob, N_1⟩⟩,
⟨⟨2, idA⟩, Alice⟩,
⟨⟨2, idB⟩, Bob⟩,
⟨⟨2, k⟩, N_1⟩,
⟨⟨2, s⟩, N_2⟩,

⟨⟨2, encb⟩, $\{\!|N_2|\!\}^{s}_{N_1}$ ⟩,

⟨⟨1, encb⟩, $\{\!|N_2|\!\}^{s}_{N_1}$ ⟩

}}

$\Re^{17}$ = {{Alice, Bob}, {{Alice, **Init**, ⟨Alice, Bob⟩, 1}, {Bob, **Init**, ⟨Bob⟩, 2}},

⟨

⟨1; k := **newnonce**⟩,

⟨1; siga := **sign** ⟨Alice, Bob, N_1⟩, sk(Alice)⟩,

⟨1; enca := **enc** $[\![\langle \mathrm{Alice}, \mathrm{Bob}, N_1 \rangle]\!]_{sk(Alice)}$, pk(Bob)⟩,

⟨1; **send** $\{\!|[\![\langle \mathrm{Alice}, \mathrm{Bob}, N_1 \rangle]\!]_{sk(Alice)}|\!\}^{a}_{pk(Bob)}$ ⟩,

⟨2; enca := **receive**⟩,

⟨2; siga := **dec** $\{\!|[\![\langle \mathrm{Alice}, \mathrm{Bob}, N_1 \rangle]\!]_{sk(Alice)}|\!\}^{a}_{pk(Bob)}$, dk(Bob)⟩,

⟨2; texta := **unsign** $[\![\langle \mathrm{Alice}, \mathrm{Bob}, N_1 \rangle]\!]_{sk(Alice)}$⟩,

⟨2; idA := π_1 ⟨Alice, Bob, N_1⟩,

⟨2; idB := π_2 ⟨Alice, Bob, N_1⟩,

⟨2; k := π_3 ⟨Alice, Bob, N_1⟩,

⟨2; **verify** $[\![\langle \mathrm{Alice}, \mathrm{Bob}, N_1 \rangle]\!]_{sk(Alice)}$, vk(Alice)⟩,

⟨2; **assert:** Bob=Bob⟩,

⟨2; s := **newnonce**⟩,

⟨2; encb := **se** N_2, N_1⟩,

⟨2; **send** $\{\!|N_2|\!\}^{s}_{N_1}$ ⟩,

⟨1; encb := **receive**⟩,

⟨1; s := **sd** $\{\!|N_2|\!\}^{s}_{N_1}$, N_1⟩

⟩,

{

⟨⟨1, k⟩, N_1⟩,

⟨⟨1, siga⟩, $[\![\langle \mathrm{Alice}, \mathrm{Bob}, N_1 \rangle]\!]_{sk(Alice)}$⟩,

⟨⟨1, enca⟩, $\{\!|[\![\langle \mathrm{Alice}, \mathrm{Bob}, N_1 \rangle]\!]_{sk(Alice)}|\!\}^{a}_{pk(Bob)}$⟩,

⟨⟨2, enca⟩, $\{\!|[\![\langle \mathrm{Alice}, \mathrm{Bob}, N_1 \rangle]\!]_{sk(Alice)}|\!\}^{a}_{pk(Bob)}$⟩,

⟨⟨2, siga⟩, $[\![\langle \mathrm{Alice}, \mathrm{Bob}, N_1 \rangle]\!]_{sk(Alice)}$⟩,

⟨⟨2, texta⟩, ⟨Alice, Bob, N_1⟩⟩,

⟨⟨2, idA⟩, Alice⟩,

⟨⟨2, idB⟩, Bob⟩,

⟨⟨2, k⟩, N_1⟩,

⟨⟨2, s⟩, N_2⟩,

⟨⟨2, encb⟩, $\{\!|N_2|\!\}^{s}_{N_1}$ ⟩,

$\langle\langle 1, \texttt{encb}\rangle,\ \{\!|N_2|\!\}^{s}_{N_1}\ \rangle,$

$\langle\langle 1, \texttt{s}\rangle, N_2\rangle$

$\}\}$

2. Full proof

Note: We use a notation where list elements can be written using record element notation (list.1, list.2, ...) in addition to projection notation. (Recall that we identify tuples and lists.)

(1) *uses:* **AA0**$_{\textbf{verify}}$

true [**Resp**(T.rpars.1)]$_T$ $\text{siga}^{[T]} = \left[\left|\left[\left|\text{siga}^{[T]}\right|\right]^{-}\right|\right]_{\overline{vk(\text{idA}^{[T]})}}$

Note that here and below, T is a meta-variable, not an abbreviation for a specific thread.

(2) *uses:* **AA0**$_{\textbf{unsign}}$

true [**Resp**(T.rpars.1)]$_T$ $\text{texta}^{[T]} = \left[\left|\text{siga}^{[T]}\right|\right]^{-}$

(3) *uses:* **AA0**$_{\textbf{assert}}$

true [**Resp**(T.rpars.1)]$_T$ $\text{idB}^{[T]} = \text{T.rpars.1}$

(4) *uses:* **AA0**$_{\textbf{assert}}$

true [**Resp**(T.rpars.1)]$_T$ $\text{texta}^{[T]} = \left\langle \text{idA}^{[T]}, \text{idB}^{[T]}, \text{k}^{[T]} \right\rangle$

(5) *uses:* definition of $\bar{k}$

$\overline{vk(\text{idA}^{[T]})} = sk(\text{idA}^{[T]})$

(6) This is **step 1** of the proof in the book chapter.
uses: (1-5), **G1**, **G3**, **G4**

true [**Resp**(T.rpars.1)]$_T$ $\text{siga}^{[T]} = \left|\left\langle \text{idA}^{[T]}, \text{T.rpars.1}, \text{k}^{[T]} \right\rangle\right|_{sk(\text{idA}^{[T]})}$

(7) *uses:* **AA1**$_{\textbf{verify}}$

true [**Resp**(T.rpars.1)]$_T$ $\text{Verify}\left(\text{T}, \text{siga}^{[T]}, vk(\text{idA}^{[T]})\right)$

(8) This is **step 2** of the proof in the book chapter.
uses: (6, 7), **G1**, **G3**

true [**Resp**(T.rpars.1)]$_T$ $\text{Verify}\left(\text{T}, \left[\left|\left\langle \text{idA}^{[T]}, \text{T.rpars.1}, \text{k}^{[T]} \right\rangle\right|\right]_{sk(\text{idA}^{[T]})}, vk(\text{idA}^{[T]})\right)$

(9) *uses:* **VER**

$$\text{Honest}(\text{idA}^{[T]}) \wedge \text{Verify}\left(\text{T}, \left[\left|\left\langle \text{idA}^{[T]}, \text{T.rpars.1}, \text{k}^{[T]} \right\rangle\right|\right]_{sk(\text{idA}^{[T]})}, vk(\text{idA}^{[T]})\right)$$
$$\Rightarrow \exists \text{T}' : \text{T}'.\text{pname} = \text{idA}^{[T]} \wedge \text{Sign}\left(\text{T}', \left\langle \text{idA}^{[T]}, \text{T.rpars.1}, \text{k}^{[T]} \right\rangle, sk(\text{idA}^{[T]})\right)$$

(10) This is **step 3** of the proof in the book chapter.
uses: (8, 9), **G1**, **G3**, **G4**

true [**Resp**(T.rpars.1)]$_T$ $\left(\begin{array}{l}\text{Honest}(\text{idA}^{[T]}) \\ \Rightarrow \exists \text{T}' : \text{T}'.\text{pname} = \text{idA}^{[T]} \wedge \text{Sign}\left(\text{T}', \left\langle \text{idA}^{[T]}, \text{T.rpars.1}, \text{k}^{[T]} \right\rangle, sk(\text{idA}^{[T]})\right)\end{array}\right)$

(11) *uses:* **AA2**$_{\text{Sign}}$

Start(T) [ ]$_T$ $\neg\text{Sign}(\text{T}, \langle \text{X}, \text{Y}, \text{K} \rangle, sk(\text{X}))$

(12) *uses:* (11), **G3**

Start(T) [ ]$_T$ $\left(\begin{array}{l}\text{Sign}\left(\text{T}, \langle \text{X}, \text{Y}, \text{K} \rangle, sk(\text{X})\right) \\ \Rightarrow \text{NewNonce}(\text{T}, \text{K}) \\ \wedge \text{FirstSend}\left(\text{T}, \text{K}, \left\{\left[\left|\langle \text{X}, \text{Y}, \text{K} \rangle\right|\right]_{sk(\text{X})}\right|\right\}_{pk(\text{Y})}^{a}\right)\end{array}\right)$

(13) *uses:* **AA1$_{sign}$**

true [**Init**(T.rpars).bseqs.1]$_T$ $\mathrm{Sign}\left(T,\langle T.pname, T.rpars.2, k^{[T]}\rangle, sk(T.pname)\right)$

Note that T.pname = T.rpars.1.

(14) *uses:* **AN3**

true [k := **newnonce**]$_T$ $\mathrm{Fresh}\left(T,k^{[T]}\right)$

(15) *uses:* **P2.1**

$\mathrm{Fresh}\left(T,k^{[T]}\right)$ [siga := **sign** ⟨T.pname, T.rpars.2, !k⟩, *sk*(T.pname); enca := **enc** !siga, *pk*(T.rpars.2)]$_T$ $\mathrm{Fresh}\left(T,k^{[T]}\right)$

(16) *uses:* **FS1**

$\mathrm{Fresh}\left(T,k^{[T]}\right)$ [**send** $\left\{\left|\left[\left\langle T.pname, T.rpars.2, k\right\rangle\right|\right]_{sk(T.pname)}\right|\right\}^{a}_{pk(T.rpars.2)}$]$_T$

$$\left(\begin{array}{l} k^{[T]} \subset\subset \left\{\left|\left[\left\langle T.pname, T.rpars.2, k^{[T]}\right\rangle\right|\right]_{sk(T.pname)}\right|\right\}^{a}_{pk(T.rpars.2)} \\ \Rightarrow \mathrm{NewNonce}\left(T,k^{[T]}\right) \\ \wedge \mathrm{FirstSend}\left(T,k^{[T]},\left\{\left|\left[\left\langle T.pname, T.rpars.2, k^{[T]}\right\rangle\right|\right]_{sk(T.pname)}\right|\right\}^{a}_{pk(T.rpars.2)}\right) \end{array}\right)$$

(17) *uses:* **IN**

$$k^{[T]} \subset\subset \left\{\left|\left[\left\langle T.pname, T.rpars.2, k^{[T]}\right\rangle\right|\right]_{sk(T.pname)}\right|\right\}^{a}_{pk(T.rpars.2)}$$

(18) *uses:* (14-17), **G1**, **G3**, **G4**, **SEQ**

true [**Init**(T.rpars).bseqs.1]$_T$ $\left(\begin{array}{l} \mathrm{NewNonce}\left(T,k^{[T]}\right) \\ \wedge \mathrm{FirstSend}\left(T,k^{[T]},\left\{\left|\left[\left\langle T.pname, T.rpars.2, k^{[T]}\right\rangle\right|\right]_{sk(T.pname)}\right|\right\}^{a}_{pk(T.rpars.2)}\right) \end{array}\right)$

(19) *uses:* (13, 18), **G1**

true [**Init**(T.rpars).bseqs.1]$_T$ $\left(\begin{array}{l} \mathrm{Sign}\left(T,\langle T.pname, T.rpars.2, k^{[T]}\rangle, sk(T.pname)\right) \\ \wedge \mathrm{NewNonce}\left(T,k^{[T]}\right) \\ \wedge \mathrm{FirstSend}\left(T,k^{[T]},\left\{\left|\left[\left\langle T.pname, T.rpars.2, k^{[T]}\right\rangle\right|\right]_{sk(T.pname)}\right|\right\}^{a}_{pk(T.rpars.2)}\right) \end{array}\right)$

(20) *uses:* (19), **G3**

[**Init**(T.rpars).bseqs.1]$_T$

$$\left(\begin{array}{l} \mathrm{Sign}\left(T,\langle T.pname, T.rpars.2, k^{[T]}\rangle, sk(T.pname)\right) \\ \Rightarrow \mathrm{NewNonce}\left(T,k^{[T]}\right) \\ \wedge \mathrm{FirstSend}\left(T,k^{[T]},\left\{\left|\left[\left\langle T.pname, T.rpars.2, k^{[T]}\right\rangle\right|\right]_{sk(T.pname)}\right|\right\}^{a}_{pk(T.rpars.2)}\right) \end{array}\right)$$

$$\left(\begin{array}{l} \mathrm{Sign}\left(T,\langle T.pname, T.rpars.2, k^{[T]}\rangle, sk(T.pname)\right) \\ \Rightarrow \mathrm{NewNonce}\left(T,k^{[T]}\right) \\ \wedge \mathrm{FirstSend}\left(T,k^{[T]},\left\{\left|\left[\left\langle T.pname, T.rpars.2, k^{[T]}\right\rangle\right|\right]_{sk(T.pname)}\right|\right\}^{a}_{pk(T.r\,p\,a)}\right) \end{array}\right)$$

(21) *uses:* **AA3$_{sign}$**

$\neg\mathrm{Sign}\left(T,\langle X, Y, K\rangle, sk(X)\right)$ [**Init**(T.rpars).bseqs.2]$_T$ $\neg\mathrm{Sign}\left(T,\langle X, Y, K\rangle, sk(X)\right)$

(22) *uses:* (21), **G3**

$\neg\mathrm{Sign}\left(T,\langle X, Y, K\rangle, sk(X)\right)$ [**Init**(T.rpars).bseqs.2]$_T$

$$\left(\begin{array}{l} \mathrm{Sign}\left(T,\langle X, Y, K\rangle, sk(X)\right) \\ \Rightarrow \mathrm{NewNonce}\left(T,K\right) \\ \wedge \mathrm{FirstSend}\left(T,K,\left\{\left|\left[\left\langle X, Y, K\right\rangle\right|\right]_{sk(X)}\right|\right\}^{a}_{pk(Y)}\right) \end{array}\right)$$

(23) *uses:* **P1**

$\mathrm{Sign}\left(T,\langle X, Y, K\rangle, sk(X)\right)$ [**Init**(T.rpars).bseqs.2]$_T$ $\mathrm{Sign}\left(T,\langle X, Y, K\rangle, sk(X)\right)$

(24) *uses:* (23), **G3**

$$[\mathbf{Init}(\mathrm{T.rpars}).\mathrm{bseqs}.2]_{\mathrm{T}} \quad \mathrm{Sign}\left(\mathrm{T},\langle \mathrm{X},\mathrm{Y},\mathrm{K}\rangle, sk(\mathrm{X})\right)$$

$$\left(\begin{array}{l}\mathrm{Sign}\left(\mathrm{T},\langle \mathrm{X},\mathrm{Y},\mathrm{K}\rangle, sk(\mathrm{X})\right)\\ \wedge\ \mathrm{NewNonce}(\mathrm{T},\mathrm{K})\\ \wedge\ \mathrm{FirstSend}\left(\mathrm{T},\mathrm{K},\left\{\left[\langle \mathrm{X},\mathrm{Y},\mathrm{K}\rangle\right]_{sk(\mathrm{X})}\right\}^{a}_{pk(\mathrm{Y})}\right)\end{array}\right)$$

(25) *uses:* **P1**

$$\mathrm{NewNonce}(\mathrm{T},\mathrm{K}) \quad [\mathbf{Init}(\mathrm{T.rpars}).\mathrm{bseqs}.2]_{\mathrm{T}} \quad \mathrm{NewNonce}(\mathrm{T},\mathrm{K})$$

(26) *uses:* (25), **G3**

$$[\mathbf{Init}(\mathrm{T.rpars}).\mathrm{bseqs}.2]_{\mathrm{T}} \quad \mathrm{NewNonce}(\mathrm{T},\mathrm{K})$$

$$\left(\begin{array}{l}\mathrm{Sign}\left(\mathrm{T},\langle \mathrm{X},\mathrm{Y},\mathrm{K}\rangle, sk(\mathrm{X})\right)\\ \wedge\ \mathrm{NewNonce}(\mathrm{T},\mathrm{K})\\ \wedge\ \mathrm{FirstSend}\left(\mathrm{T},\mathrm{K},\left\{\left[\langle \mathrm{X},\mathrm{Y},\mathrm{K}\rangle\right]_{sk(\mathrm{X})}\right\}^{a}_{pk(\mathrm{Y})}\right)\end{array}\right)$$

(27) *uses:* **P1**

$$\mathrm{FirstSend}\left(\mathrm{T},\mathrm{K},\left\{\left[\langle \mathrm{X},\mathrm{Y},\mathrm{K}\rangle\right]_{sk(\mathrm{X})}\right\}^{a}_{pk(\mathrm{Y})}\right) \quad [\mathbf{Init}(\mathrm{T.rpars}).\mathrm{bseqs}.2]_{\mathrm{T}} \quad \mathrm{FirstSend}\left(\mathrm{T},\mathrm{K},\left\{\left[\langle \mathrm{X},\mathrm{Y},\mathrm{K}\rangle\right]_{sk(\mathrm{X})}\right\}^{a}_{pk(\mathrm{Y})}\right)$$

(28) *uses:* (27), **G3**

$$[\mathbf{Init}(\mathrm{T.rpars}).\mathrm{bseqs}.2]_{\mathrm{T}} \quad \mathrm{FirstSend}\left(\mathrm{T},\mathrm{K},\left\{\left[\langle \mathrm{X},\mathrm{Y},\mathrm{K}\rangle\right]_{sk(\mathrm{X})}\right\}^{a}_{pk(\mathrm{Y})}\right)$$

$$\left(\begin{array}{l}\mathrm{Sign}\left(\mathrm{T},\langle \mathrm{X},\mathrm{Y},\mathrm{K}\rangle, sk(\mathrm{X})\right)\\ \wedge\ \mathrm{NewNonce}(\mathrm{T},\mathrm{K})\\ \wedge\ \mathrm{FirstSend}\left(\mathrm{T},\mathrm{K},\left\{\left[\langle \mathrm{X},\mathrm{Y},\mathrm{K}\rangle\right]_{sk(\mathrm{X})}\right\}^{a}_{pk(\mathrm{Y})}\right)\end{array}\right)$$

(29) *uses:* (24, 26, 28), **G1**

$$[\mathbf{Init}(\mathrm{T.rpars}).\mathrm{bseqs}.2]_{\mathrm{T}}$$

$$\left(\begin{array}{l}\mathrm{Sign}\left(\mathrm{T},\langle \mathrm{X},\mathrm{Y},\mathrm{K}\rangle, sk(\mathrm{X})\right)\\ \wedge\ \mathrm{NewNonce}(\mathrm{T},\mathrm{K})\\ \wedge\ \mathrm{FirstSend}\left(\mathrm{T},\mathrm{K},\left\{\left[\langle \mathrm{X},\mathrm{Y},\mathrm{K}\rangle\right]_{sk(\mathrm{X})}\right\}^{a}_{pk(\mathrm{Y})}\right)\end{array}\right) \qquad \left(\begin{array}{l}\mathrm{Sign}\left(\mathrm{T},\langle \mathrm{X},\mathrm{Y},\mathrm{K}\rangle, sk(\mathrm{X})\right)\\ \wedge\ \mathrm{NewNonce}(\mathrm{T},\mathrm{K})\\ \wedge\ \mathrm{FirstSend}\left(\mathrm{T},\mathrm{K},\left\{\left[\langle \mathrm{X},\mathrm{Y},\mathrm{K}\rangle\right]_{sk(\mathrm{X})}\right\}^{a}_{pk(\mathrm{Y})}\right)\end{array}\right)$$

(30) *uses:* (29), **G3**

$$[\mathbf{Init}(\mathrm{T.rpars}).\mathrm{bseqs}.2]_{\mathrm{T}}$$

$$\left(\begin{array}{l}\mathrm{Sign}\left(\mathrm{T},\langle \mathrm{X},\mathrm{Y},\mathrm{K}\rangle, sk(\mathrm{X})\right)\\ \wedge\ \mathrm{NewNonce}(\mathrm{T},\mathrm{K})\\ \wedge\ \mathrm{FirstSend}\left(\mathrm{T},\mathrm{K},\left\{\left[\langle \mathrm{X},\mathrm{Y},\mathrm{K}\rangle\right]_{sk(\mathrm{X})}\right\}^{a}_{pk(\mathrm{Y})}\right)\end{array}\right) \qquad \left(\begin{array}{l}\mathrm{Sign}\left(\mathrm{T},\langle \mathrm{X},\mathrm{Y},\mathrm{K}\rangle, sk(\mathrm{X})\right)\\ \Rightarrow\ \mathrm{NewNonce}(\mathrm{T},\mathrm{K})\\ \wedge\ \mathrm{FirstSend}\left(\mathrm{T},\mathrm{K},\left\{\left[\langle \mathrm{X},\mathrm{Y},\mathrm{K}\rangle\right]_{sk(\mathrm{X})}\right\}^{a}_{pk(\mathrm{Y})}\right)\end{array}\right)$$

(31) *uses:* (22, 30), **G2**

$$[\mathbf{Init}(\mathrm{T.rpars}).\mathrm{bseqs}.2]_{\mathrm{T}}$$

$$\mathrm{Sign}\left(\mathrm{T},\langle \mathrm{X},\mathrm{Y},\mathrm{K}\rangle, sk(\mathrm{X})\right) \Rightarrow \left(\begin{array}{l}\mathrm{Sign}\left(\mathrm{T},\langle \mathrm{X},\mathrm{Y},\mathrm{K}\rangle, sk(\mathrm{X})\right)\\ \wedge\ \mathrm{NewNonce}(\mathrm{T},\mathrm{K})\\ \wedge\ \mathrm{FirstSend}\left(\mathrm{T},\mathrm{K},\left\{\left[\langle \mathrm{X},\mathrm{Y},\mathrm{K}\rangle\right]_{sk(\mathrm{X})}\right\}^{a}_{pk(\mathrm{Y})}\right)\end{array}\right) \qquad \left(\begin{array}{l}\mathrm{Sign}\left(\mathrm{T},\langle \mathrm{X},\mathrm{Y},\mathrm{K}\rangle, sk(\mathrm{X})\right)\\ \Rightarrow\ \mathrm{NewNonce}(\mathrm{T},\mathrm{K})\\ \wedge\ \mathrm{FirstSend}\left(\mathrm{T},\mathrm{K},\left\{\left[\langle \mathrm{X},\mathrm{Y},\mathrm{K}\rangle\right]_{sk(\mathrm{X})}\right\}^{a}_{pk(\mathrm{Y})}\right)\end{array}\right)$$

(32) *uses*: (31), **G3**

$$[\mathbf{Init}(\mathrm{T.rpars}).\mathrm{bseqs}.2]_{\mathrm{T}}$$

$$\left(\begin{array}{l}\mathrm{Sign}\left(\mathrm{T},\langle \mathrm{X},\mathrm{Y},\mathrm{K}\rangle, sk(\mathrm{X})\right)\\ \Rightarrow\ \mathrm{NewNonce}(\mathrm{T},\mathrm{K})\\ \wedge\ \mathrm{FirstSend}\left(\mathrm{T},\mathrm{K},\left\{\left[\langle \mathrm{X},\mathrm{Y},\mathrm{K}\rangle\right]_{sk(\mathrm{X})}\right\}^{a}_{pk(\mathrm{Y})}\right)\end{array}\right) \qquad \left(\begin{array}{l}\mathrm{Sign}\left(\mathrm{T},\langle \mathrm{X},\mathrm{Y},\mathrm{K}\rangle, sk(\mathrm{X})\right)\\ \Rightarrow\ \mathrm{NewNonce}(\mathrm{T},\mathrm{K})\\ \wedge\ \mathrm{FirstSend}\left(\mathrm{T},\mathrm{K},\left\{\left[\langle \mathrm{X},\mathrm{Y},\mathrm{K}\rangle\right]_{sk(\mathrm{X})}\right\}^{a}_{pk(\mathrm{Y})}\right)\end{array}\right)$$

(33) *derivation exactly as for (32)*

$$[\mathbf{Resp}(\mathrm{T.rpars})]_{\mathrm{T}}$$

$$\left(\begin{array}{l}\mathrm{Sign}\left(\mathrm{T},\langle \mathrm{X},\mathrm{Y},\mathrm{K}\rangle, sk(\mathrm{X})\right)\\ \Rightarrow\ \mathrm{NewNonce}(\mathrm{T},\mathrm{K})\\ \wedge\ \mathrm{FirstSend}\left(\mathrm{T},\mathrm{K},\left\{\left[\langle \mathrm{X},\mathrm{Y},\mathrm{K}\rangle\right]_{sk(\mathrm{X})}\right\}^{a}_{pk(\mathrm{Y})}\right)\end{array}\right) \qquad \left(\begin{array}{l}\mathrm{Sign}\left(\mathrm{T},\langle \mathrm{X},\mathrm{Y},\mathrm{K}\rangle, sk(\mathrm{X})\right)\\ \Rightarrow\ \mathrm{NewNonce}(\mathrm{T},\mathrm{K})\\ \wedge\ \mathrm{FirstSend}\left(\mathrm{T},\mathrm{K},\left\{\left[\langle \mathrm{X},\mathrm{Y},\mathrm{K}\rangle\right]_{sk(\mathrm{X})}\right\}^{a}_{pk(\mathrm{Y})}\right)\end{array}\right)$$

(34) *uses:* (12, 20, 32, 33), **HON**

$$\text{Honest}(\text{T.pname}) \Rightarrow \left(\begin{array}{l} \text{Sign}\left(\text{T}, \langle \text{T.pname}, \text{T.rpars.2}, \text{k}^{[\text{T}]} \rangle, sk(\text{T.pname})\right) \\ \Rightarrow \text{NewNonce}\left(\text{T}, \text{k}^{[\text{T}]}\right) \\ \wedge \text{FirstSend}\left(\text{T}, \text{k}^{[\text{T}]}, \left\{ \left| [\![\langle \text{T.pname}, \text{T.rpars.2}, \text{k}^{[\text{T}]} \rangle]\!] \right|_{\text{sk(T.pname)}} \right\}^{\text{a}}_{\text{pk(T.rpars.2)}} \right) \end{array} \right)$$

Note that there is a presupposition (sort-of) here that requires the thread to be executing a role with at least 2 role parameters. If the presupposition fails, one could take either of two stances: (1) Sign(...) is false by default. (2) T.rpars.2 is a symbol. Currently the chapter takes stance #2. Option #1 would make the proof easier of course. In either case we strictly speaking don't have a presupposition failure (ie: we don't use error values in this particular case).

(35) This is **step 4** of the proof in the book chapter.

uses: (34)

$$\text{Honest}(\text{T}_{\text{all}}.\text{pname}) \Rightarrow \left(\begin{array}{l} \text{Sign}\left(\text{T}_{\text{all}}, \langle \text{T}_{\text{all}}.\text{pname}, \text{T}_{\text{all}}.\text{rpars.2}, \text{k}^{[\text{T}_{\text{all}}]} \rangle, sk(\text{T}_{\text{all}}.\text{pname})\right) \\ \Rightarrow \text{NewNonce}\left(\text{T}_{\text{all}}, \text{k}^{[\text{T}_{\text{all}}]}\right) \\ \wedge \text{FirstSend}\left(\text{T}_{\text{all}}, \text{k}^{[\text{T}_{\text{all}}]}, \left\{ \left| [\![\langle \text{T}_{\text{all}}.\text{pname}, \text{T}_{\text{all}}.\text{rpars.2}, \text{k}^{[\text{T}_{\text{all}}]} \rangle]\!] \right|_{sk(\text{T}_{\text{all}}.\text{pname})} \right\}^{\text{a}}_{pk(\text{T}_{\text{all}}.\text{rpars.2})} \right) \end{array} \right)$$

(36) *by inspection of the handshake protocol*

$$\text{Honest}(\text{T}_{\text{all}}.\text{pname}) \Rightarrow \left(\text{Sign}\left(\text{T}_{\text{all}}, \langle \text{X}, \text{Y}, \text{K} \rangle, sk(\text{X})\right) \Rightarrow \text{K} = \text{k}^{[\text{T}_{\text{all}}]}\right)$$

(37) *uses:* (36)

$$\text{Honest}(\text{T}_{\text{all}}.\text{pname}) \Rightarrow \left(\begin{array}{l} \text{Sign}\left(\text{T}_{\text{all}}, \langle \text{T}_{\text{all}}.\text{pname}, \text{T}_{\text{all}}.\text{rpars.2}, \text{K} \rangle, sk(\text{T}_{\text{all}}.\text{pname})\right) \\ \Rightarrow \text{K} = \text{k}^{[\text{T}_{\text{all}}]} \wedge \text{Sign}\left(\text{T}_{\text{all}}, \langle \text{T}_{\text{all}}.\text{pname}, \text{T}_{\text{all}}.\text{rpars.2}, \text{k}^{[\text{T}_{\text{all}}]} \rangle, sk(\text{T}_{\text{all}}.\text{pname})\right) \end{array} \right)$$

The *second* Sign(...) of (37) is unified with the Sign(...) of (35).

(38) *uses:* (35, 37)

$$\text{Honest}(\text{T}_{\text{all}}.\text{pname}) \Rightarrow \left(\begin{array}{l} \text{Sign}\left(\text{T}_{\text{all}}, \langle \text{T}_{\text{all}}.\text{pname}, \text{T}_{\text{all}}.\text{rpars.2}, \text{K} \rangle, sk(\text{T}_{\text{all}}.\text{pname})\right) \\ \Rightarrow \text{K} = \text{k}^{[\text{T}_{\text{all}}]} \wedge \text{NewNonce}\left(\text{T}_{\text{all}}, \text{k}^{[\text{T}_{\text{all}}]}\right) \\ \wedge \text{FirstSend}\left(\text{T}_{\text{all}}, \text{k}^{[\text{T}_{\text{all}}]}, \left\{ \left| [\![\langle \text{T}_{\text{all}}.\text{pname}, \text{T}_{\text{all}}.\text{rpars.2}, \text{k}^{[\text{T}_{\text{all}}]} \rangle]\!] \right|_{sk(\text{T}_{\text{all}}.\text{pname})} \right\}^{\text{a}}_{pk(\text{T}_{\text{all}}.\text{rpars.2})} \right) \end{array} \right)$$

(39) *uses:* (38)

$$\text{Honest}(\text{T}_{\text{all}}.\text{pname}) \Rightarrow \left(\begin{array}{l} \text{Sign}\left(\text{T}_{\text{all}}, \langle \text{T}_{\text{all}}.\text{pname}, \text{T}_{\text{all}}.\text{rpars.2}, \text{K} \rangle, sk(\text{T}_{\text{all}}.\text{pname})\right) \\ \Rightarrow \text{NewNonce}\left(\text{T}_{\text{all}}, \text{K}\right) \\ \wedge \text{FirstSend}\left(\text{T}_{\text{all}}, \text{K}, \left\{ \left| [\![\langle \text{T}_{\text{all}}.\text{pname}, \text{T}_{\text{all}}.\text{rpars.2}, \text{K} \rangle]\!] \right|_{sk(\text{T}_{\text{all}}.\text{pname})} \right\}^{\text{a}}_{pk(\text{T}_{\text{all}}.\text{rpars.2})} \right) \end{array} \right)$$

(40) *uses:* (39), **G4**

$$\textit{true}\ [\mathbf{Resp}(\mathrm{T.rpars.1})]_{\mathrm{T}}\quad \left(\begin{array}{l}\mathrm{Honest}(\mathrm{T_{all}.pname})\\ \Rightarrow \left(\begin{array}{l}\mathrm{Sign}\left(\mathrm{T_{all}},\langle \mathrm{T_{all}.pname}, \mathrm{T_{all}.rpars.2}, \mathrm{K}\rangle, sk(\mathrm{T_{all}.pname})\right)\\ \Rightarrow \mathrm{NewNonce}(\mathrm{T_{all}}, \mathrm{K})\\ \wedge \mathrm{FirstSend}\left(\mathrm{T_{all}}, \mathrm{K}, \left\{\left|\left[\left\langle \mathrm{T_{all}.pname}, \mathrm{T_{all}.rpars.2}, \mathrm{K}\right\rangle\right|\right]_{sk(\mathrm{T_{all}.pname})}\right|\right\}^{\mathrm{a}}_{pk(\mathrm{T_{all}.rpars.2})}\right)\end{array}\right)\end{array}\right)$$

(41) *uses:* (10, 40), **G1**, **G3**

$$\textit{true}\ [\mathbf{Resp}(\mathrm{T.rpars.1})]_{\mathrm{T}}\quad \left(\begin{array}{l}\left(\begin{array}{l}\mathrm{Honest}(\mathrm{idA}^{[\mathrm{T}]})\\ \Rightarrow \exists \mathrm{T'}: \mathrm{T'.pname} = \mathrm{idA}^{[\mathrm{T}]}\\ \wedge \mathrm{Sign}\left(\mathrm{T'}, \left\langle \mathrm{idA}^{[\mathrm{T}]}, \mathrm{T.rpars.1}, \mathrm{k}^{[\mathrm{T}]}\right\rangle, sk(\mathrm{idA}^{[\mathrm{T}]})\right)\end{array}\right)\\ \wedge \left(\begin{array}{l}\mathrm{Honest}(\mathrm{T_{all}.pname})\\ \Rightarrow \left(\begin{array}{l}\mathrm{Sign}\left(\mathrm{T_{all}},\langle \mathrm{T_{all}.pname}, \mathrm{T_{all}.rpars.2}, \mathrm{K}\rangle, sk(\mathrm{T_{all}.pname})\right)\\ \Rightarrow \mathrm{NewNonce}(\mathrm{T_{all}}, \mathrm{K})\\ \wedge \mathrm{FirstSend}\left(\mathrm{T_{all}}, \mathrm{K}, \left\{\left|\left[\left\langle \mathrm{T_{all}.pname}, \mathrm{T_{all}.rpars.2}, \mathrm{K}\right\rangle\right|\right]_{sk(\mathrm{T_{all}.pname})}\right|\right\}^{\mathrm{a}}_{pk(\mathrm{T_{all}.rpars.2})}\right)\end{array}\right)\end{array}\right)\end{array}\right)$$

$\mathrm{T_{all}}$ is instantiated as T' with $\mathrm{T_{all}.rpars} = \langle \mathrm{T_{all}.pname}, \mathrm{T_{all}.rpars.2}\rangle = \langle \mathrm{idA}^{[\mathrm{T}]}, \mathrm{T.rpars.1}\rangle$. K is instantiated as $\mathrm{k}^{[\mathrm{T}]}$.

(42) This is **step 5** of the proof in the book chapter.
uses: (41), **G3**

$$\textit{true}\ [\mathbf{Resp}(\mathrm{T.rpars.1})]_{\mathrm{T}}\quad \left(\begin{array}{l}\mathrm{Honest}(\mathrm{idA}^{[\mathrm{T}]})\\ \Rightarrow \exists \mathrm{T'}: \mathrm{T'.pname} = \mathrm{idA}^{[\mathrm{T}]} \wedge \mathrm{NewNonce}(\mathrm{T'}, \mathrm{k}^{[\mathrm{T}]})\\ \wedge \mathrm{FirstSend}\left(\mathrm{T'}, \mathrm{k}^{[\mathrm{T}]}, \left\{\left|\left[\left\langle \mathrm{idA}^{[\mathrm{T}]}, \mathrm{T.rpars.1}, \mathrm{k}^{[\mathrm{T}]}\right\rangle\right|\right]_{sk(\mathrm{idA}^{[\mathrm{T}]})}\right|\right\}^{\mathrm{a}}_{pk(\mathrm{T.rpars.1})}\right)\end{array}\right)$$

(43) *uses:* $\mathbf{AA1}_{\mathbf{receive}}$

$$\textit{true}\ [\mathbf{Resp}(\mathrm{T.rpars.1})]_{\mathrm{T}}\quad \mathrm{Receive}\left(\mathrm{T}, \mathrm{enca}^{[\mathrm{T}]}\right)$$

(44) *uses:* $\mathbf{AA0}_{\mathbf{dec}}$

$$\textit{true}\ [\mathbf{Resp}(\mathrm{T.rpars.1})]_{\mathrm{T}}\quad \mathrm{enca}^{[\mathrm{T}]} = \left\{\left|\mathrm{siga}^{[\mathrm{T}]}\right|\right\}^{\mathrm{a}}_{\overline{dk(\mathrm{T.rpars.1})}}$$

(45) *uses:* definition of $\overline{k}$

$$\overline{dk(\mathrm{T.rpars.1})} = pk(\mathrm{T.rpars.1})$$

(46) *uses:* (6, 43-45), **G1**, **G3**, **G4**

$$\textit{true}\ [\mathbf{Resp}(\mathrm{T.rpars.1})]_{\mathrm{T}}\quad \mathrm{Receive}\left(\mathrm{T}, \left\{\left|\left[\left\langle \mathrm{idA}^{[\mathrm{T}]}, \mathrm{T.rpars.1}, \mathrm{k}^{[\mathrm{T}]}\right\rangle\right|\right]_{sk(\mathrm{idA}^{[\mathrm{T}]})}\right|\right\}^{\mathrm{a}}_{pk(\mathrm{T.rpars.1})}\right)$$

(47) *uses:* **IN**

$$\mathrm{k}^{[\mathrm{T}]} \subset\subset \left\{\left|\left[\left\langle \mathrm{idA}^{[\mathrm{T}]}, \mathrm{T.rpars.1}, \mathrm{k}^{[\mathrm{T}]}\right\rangle\right|\right]_{sk(\mathrm{idA}^{[\mathrm{T}]})}\right|\right\}^{\mathrm{a}}_{pk(\mathrm{T.rpars.1})}$$

(48) This is **step 6** of the proof in the book chapter.
uses: (46, 47), **G1**, **G4**

$$\textit{true}\ [\mathbf{Resp}(\mathrm{T.rpars.1})]_{\mathrm{T}}\ \left(\begin{array}{l} \mathrm{k}^{[\mathrm{T}]} \subset\subset \left\{\left|\left[\!\left[\left\langle \mathrm{idA}^{[\mathrm{T}]}, \mathrm{T.rpars.1}, \mathrm{k}^{[\mathrm{T}]}\right\rangle\right|\right]_{sk\left(\mathrm{idA}^{[\mathrm{T}]}\right)}\right|\right\}^{\mathrm{a}}_{pk(\mathrm{T.rpars.1})} \\ \wedge\ \mathrm{Receive}\left(\mathrm{T}, \left\{\left|\left[\!\left[\left\langle \mathrm{idA}^{[\mathrm{T}]}, \mathrm{T.rpars.1}, \mathrm{k}^{[\mathrm{T}]}\right\rangle\right|\right]_{sk\left(\mathrm{idA}^{[\mathrm{T}]}\right)}\right|\right\}^{\mathrm{a}}_{pk(\mathrm{T.rpars.1})}\right) \end{array}\right)$$

(49) *uses:* **FS2**

$$\begin{array}{l} \mathrm{NewNonce}\left(\mathrm{T}_1, \mathrm{k}^{[\mathrm{T}]}\right) \wedge \mathrm{FirstSend}\left(\mathrm{T}_1, \mathrm{k}^{[\mathrm{T}]}, \left\{\left|\left[\!\left[\left\langle \mathrm{idA}^{[\mathrm{T}]}, \mathrm{T.rpars.1}, \mathrm{k}^{[\mathrm{T}]}\right\rangle\right|\right]_{sk\left(\mathrm{idA}^{[\mathrm{T}]}\right)}\right|\right\}^{\mathrm{a}}_{pk(\mathrm{T.rpars.1})}\right) \\ \wedge\ \mathrm{T}_1 \neq \mathrm{T} \wedge \mathrm{k}^{[\mathrm{T}]} \subset\subset \left\{\left|\left[\!\left[\left\langle \mathrm{idA}^{[\mathrm{T}]}, \mathrm{T.rpars.1}, \mathrm{k}^{[\mathrm{T}]}\right\rangle\right|\right]_{sk\left(\mathrm{idA}^{[\mathrm{T}]}\right)}\right|\right\}^{\mathrm{a}}_{pk(\mathrm{T.rpars.1})} \\ \wedge\ \mathrm{Receive}\left(\mathrm{T}, \left\{\left|\left[\!\left[\left\langle \mathrm{idA}^{[\mathrm{T}]}, \mathrm{T.rpars.1}, \mathrm{k}^{[\mathrm{T}]}\right\rangle\right|\right]_{sk\left(\mathrm{idA}^{[\mathrm{T}]}\right)}\right|\right\}^{\mathrm{a}}_{pk(\mathrm{T.rpars.1})}\right) \\ \Rightarrow \left(\begin{array}{l} \mathrm{Send}\left(\mathrm{T}_1, \left\{\left|\left[\!\left[\left\langle \mathrm{idA}^{[\mathrm{T}]}, \mathrm{T.rpars.1}, \mathrm{k}^{[\mathrm{T}]}\right\rangle\right|\right]_{sk\left(\mathrm{idA}^{[\mathrm{T}]}\right)}\right|\right\}^{\mathrm{a}}_{pk(\mathrm{T.rpars.1})}\right) \\ \lhd\ \mathrm{Receive}\left(\mathrm{T}, \left\{\left|\left[\!\left[\left\langle \mathrm{idA}^{[\mathrm{T}]}, \mathrm{T.rpars.1}, \mathrm{k}^{[\mathrm{T}]}\right\rangle\right|\right]_{sk\left(\mathrm{idA}^{[\mathrm{T}]}\right)}\right|\right\}^{\mathrm{a}}_{pk(\mathrm{T.rpars.1})}\right) \end{array}\right) \end{array}$$

(50) *uses:* (42, 48, 49), **G1**, **G3**, **G4**

$$\textit{true}\ [\mathbf{Resp}(\mathrm{T.rpars.1})]_{\mathrm{T}}\ \left(\begin{array}{l} \mathrm{Honest}\left(\mathrm{idA}^{[\mathrm{T}]}\right) \Rightarrow \exists \mathrm{T}' : \mathrm{T}'.\mathrm{pname} = \mathrm{idA}^{[\mathrm{T}]} \\ \wedge \left(\begin{array}{l} \mathrm{T}' \neq \mathrm{T} \\ \Rightarrow \left(\begin{array}{l} \mathrm{Send}\left(\mathrm{T}', \left\{\left|\left[\!\left[\left\langle \mathrm{idA}^{[\mathrm{T}]}, \mathrm{T.rpars.1}, \mathrm{k}^{[\mathrm{T}]}\right\rangle\right|\right]_{sk\left(\mathrm{idA}^{[\mathrm{T}]}\right)}\right|\right\}^{\mathrm{a}}_{pk(\mathrm{T.rpars.1})}\right) \\ \lhd\ \mathrm{Receive}\left(\mathrm{T}, \left\{\left|\left[\!\left[\left\langle \mathrm{idA}^{[\mathrm{T}]}, \mathrm{T.rpars.1}, \mathrm{k}^{[\mathrm{T}]}\right\rangle\right|\right]_{sk\left(\mathrm{idA}^{[\mathrm{T}]}\right)}\right|\right\}^{\mathrm{a}}_{pk(\mathrm{T.rpars.1})}\right) \end{array}\right) \end{array}\right) \end{array}\right)$$

(51) This is **step 7** of the proof in the book chapter.
uses: (6, 44, 45, 50), **G1**, **G3**, **G4**

$$\textit{true}\ [\mathbf{Resp}(\mathrm{T.rpars.1})]_{\mathrm{T}}\ \left(\begin{array}{l} \mathrm{Honest}\left(\mathrm{idA}^{[\mathrm{T}]}\right) \Rightarrow \exists \mathrm{T}' : \mathrm{T}'.\mathrm{pname} = \mathrm{idA}^{[\mathrm{T}]} \\ \wedge \left(\begin{array}{l} \mathrm{T}' \neq \mathrm{T} \\ \Rightarrow \mathrm{Send}\left(\mathrm{T}', \mathrm{enca}^{[\mathrm{T}]}\right) \lhd \mathrm{Receive}\left(\mathrm{T}, \mathrm{enca}^{[\mathrm{T}]}\right) \end{array}\right) \end{array}\right)$$

(52) *uses:* **AA4**

$$\textit{true}\ [\mathbf{Resp}(\mathrm{T.rpars.1})]_{\mathrm{T}}\ \ \mathrm{Receive}\left(\mathrm{T}, \mathrm{enca}^{[\mathrm{T}]}\right) \lhd \mathrm{Send}\left(\mathrm{T}, \mathrm{encb}^{[\mathrm{T}]}\right)$$

(53) *uses:* (51, 52), **G1**, **G3**

$$\textit{true}\ [\mathbf{Resp}(\mathrm{T.rpars.1})]_{\mathrm{T}}\ \left(\begin{array}{l} \mathrm{Honest}\left(\mathrm{idA}^{[\mathrm{T}]}\right) \Rightarrow \exists \mathrm{T}' : \mathrm{T}'.\mathrm{pname} = \mathrm{idA}^{[\mathrm{T}]} \\ \wedge \left(\begin{array}{l} \mathrm{T}' \neq \mathrm{T} \\ \Rightarrow \mathrm{Send}\left(\mathrm{T}', \mathrm{enca}^{[\mathrm{T}]}\right) \lhd \mathrm{Receive}\left(\mathrm{T}, \mathrm{enca}^{[\mathrm{T}]}\right) \\ \wedge\ \mathrm{Receive}\left(\mathrm{T}, \mathrm{enca}^{[\mathrm{T}]}\right) \lhd \mathrm{Send}\left(\mathrm{T}, \mathrm{encb}^{[\mathrm{T}]}\right) \end{array}\right) \end{array}\right)$$

(54) This is **step 8** of the proof in the book chapter.

uses: (53), **G3**

$$\mathit{true}\ [\mathbf{Resp}(\mathrm{T.rpars.1})]_{\mathrm{T}}\ \left(\begin{array}{l}\mathrm{Honest}\left(\mathrm{idA}^{[\mathrm{T}]}\right)\wedge \mathrm{idA}^{[\mathrm{T}]}\neq \mathrm{T.pname}\Rightarrow \exists \mathrm{T'}:\\ \left(\begin{array}{l}\mathrm{T'.pname}=\mathrm{idA}^{[\mathrm{T}]}\\ \wedge\ \mathrm{Send}\left(\mathrm{T'},\mathrm{enca}^{[\mathrm{T}]}\right)\lhd \mathrm{Receive}\left(\mathrm{T},\mathrm{enca}^{[\mathrm{T}]}\right)\\ \wedge\ \mathrm{Receive}\left(\mathrm{T},\mathrm{enca}^{[\mathrm{T}]}\right)\lhd \mathrm{Send}\left(\mathrm{T},\mathrm{encb}^{[\mathrm{T}]}\right)\end{array}\right)\end{array}\right)$$