FMSP: Solution Attempt for exam 2021-09

Pizzaiolo

June 28, 2022

Preamble

Feel free to edit it to add more examples, fix mistakes, etc. If you do so, please update both the .tex and .pdf files. And obviously no guarantee for anything.

Problem 1

(a)

$$
\begin{aligned}
P &= (\nu k_1 \colon SymK^{HH}[HH])(\nu k_2 \colon SigK^{HH}[LH, LL])A|B \\
A &= (\nu m \colon LL)(\nu n \colon HH)\overline{c}\langle[\{|n|\}^s_{k_1}, m]\rangle.0 \\
B &= c(x).\ \text{case } x \text{ of } [y, m\prime]_{vk(k_2)} \text{ in } \ \text{case } y \text{ of } \{|n\prime|\}^s_{k_1} \text{ in } 0
\end{aligned}
$$

(b)

We will let $\Gamma = \{c \colon LL\}$.

Restrictions and parallel .

$$
\dfrac{\dfrac{\dfrac{(1)}{\Gamma, k_1 \colon SymK^{HH}[HH], k_2 \colon SigK^{HH}[LH, LL] \vdash A} \quad \dfrac{(2)}{\Gamma, k_1 \colon SymK^{HH}[HH], k_2 \colon SigK^{HH}[LH, LL] \vdash B}\ \text{PAR}}{\Gamma, k_1 \colon SymK^{HH}[HH], k_2 \colon SigK^{HH}[LH, LL] \vdash A|B}\ \text{RES}}{\Gamma, k_1 \colon SymK^{HH}[HH] \vdash (\nu k_2 \colon SigK^{HH}[LH, LL])A|B}\ \text{RES}}{\Gamma \vdash (\nu k_1 \colon SymK^{HH}[HH])(\nu k_2 \colon SigK^{HH}[LH, LL])A|B}\ \text{RES}
$$

.
For simplicity, let

$$\Gamma_1 = \Gamma, k_1 \colon SymK^{HH}[HH], k_2 \colon SigK^{HH}[LH, LL]$$

Proving A .

With

$$\Gamma_2 = \Gamma_1, m \colon LL, n \colon HH$$

$$\dfrac{\dfrac{\dfrac{(2)}{\Gamma_2 \vdash [\{|n|\}^s_{k_1}, m]_{k_2} : LL} \quad \dfrac{\dfrac{(0.2)}{\Gamma_2 \vdash \diamond}}{\Gamma_2 \vdash 0}\ \text{STOP} \quad \dfrac{(4)}{\Gamma_2 \vdash c : C^{LL}[LL]}}{\Gamma_1, m : LL, n : HH \vdash \overline{c}\langle[\{|n|\}^s_{k_1}, m]\rangle.0}\ \text{OUT}}{\Gamma_1, m : LL \vdash (\nu n : HH)\overline{c}\langle[\{|n|\}^s_{k_1}, m]\rangle.0}\ \text{RES}}{\Gamma_1 \vdash (\nu m : LL)(\nu n : HH)\overline{c}\langle[\{|n|\}^s_{k_1}, m]\rangle.0}\ \text{RES}}{(1)}$$

.

$$\dfrac{\dfrac{(0.2)}{\Gamma_2 \vdash \diamond} \quad c : LL \text{ in } \Gamma_2}{\Gamma_2 \vdash c : LL}\ \text{ATOM} \qquad LL \leq C^{LL}[LL]}{\Gamma_2 \vdash c : C^{LL}[LL]}\ \text{SUBSUMPTION}}{(4)}$$

Doing the signature .

$$\dfrac{\dfrac{\dfrac{(0.2)}{\Gamma_2 \vdash \diamond} \quad k_2 : SigK^{HH}[LH, LL] \text{ in } \Gamma_2}{\Gamma_2 \vdash k_2 : SigK^{HH}[LH, LL]}\ \text{ATOM} \quad \dfrac{(5)}{\Gamma_2 \vdash [\{|n|\}^s_{k_1}, m] : [LH, LL]} \quad L = \ldots}{\Gamma_2 \vdash [\{|n|\}^s_{k_1}, m]_{k_2} : LH}\ \text{DigSig} \qquad LH \leq LL}{\Gamma_2 \vdash [\{|n|\}^s_{k_1}, m]_{k_2} : LL}\ \text{SUBSUMPTION}}{(2)}$$

Doing the encryption .

$$\dfrac{\dfrac{\dfrac{\dfrac{(0.2)}{\Gamma_2 \vdash \diamond} \quad k_1 : SymK^{HH}[HH] \text{ in } \Gamma_2}{\Gamma_2 \vdash k_1 : SymK^{HH}[HH]}\ \text{ATOM} \quad \dfrac{\dfrac{(0.2)}{\Gamma_2 \vdash \diamond} \quad n : HH \text{ in } \Gamma_2}{\Gamma_2 \vdash n : HH}\ \text{ATOM}}{\Gamma_2 \vdash \{|n|\}^s_{k_1} : LH}\ \text{SymEnc} \quad \dfrac{\dfrac{(0.2)}{\Gamma_2 \vdash \diamond} \quad m : LL \text{ in } \Gamma_2}{\Gamma_2 \vdash m : LL}\ \text{ATOM}}{\Gamma_2 \vdash [\{|n|\}^s_{k_1}, m] : [LH, LL]}\ \text{LIST}}{(5)}$$

Proving B .

For simplicity we let

$$Q = \text{ case } y \text{ of } \{|n\prime|\}^s_{k_1} \text{ in } 0$$

$$\dfrac{\dfrac{(6)}{\Gamma_1, x\colon LL \vdash \text{ case } x \text{ of } [y, m\prime]_{vk(k_2)} \text{ in } Q} \quad \dfrac{\dfrac{\dfrac{(0.1)}{\Gamma_1 \vdash \diamond}}{\text{similar to (4)}}}{\Gamma_1 \vdash c\colon C^{LL}[LL]}\ \text{IN}}{\dfrac{\Gamma_1 \vdash c(x).\ \text{case } x \text{ of } [y, m\prime]_{vk(k_2)} \text{ in } Q}{\dfrac{\Gamma, k_1\colon SymK^{HH}[HH], k_2\colon SigK^{HH}[LH, LL] \vdash B}{(2)}}}$$

.

$$\dfrac{\dfrac{(7)}{\Gamma_1, x\colon LL \vdash x\colon LL} \quad \dfrac{(8)}{\Gamma_1, x\colon LL \vdash vk(k_2)\colon VerK^{LH}[LH, LL]} \quad \dfrac{(9)}{\Gamma_1, x\colon LL, y\colon LH, m\prime\colon LL \vdash Q} \quad \mathcal{L}_C(LL) = H \implies H = H\ \text{SignCheck}}{\dfrac{\Gamma_1, x\colon LL \vdash \text{ case } x \text{ of } [y, m\prime]_{vk(k_2)} \text{ in } Q}{(6)}}$$

.

$$\dfrac{\dfrac{(0.1)}{\Gamma_1 \vdash \diamond} \quad x\colon LL \text{ in } \Gamma_1, x\colon LL}{\dfrac{\Gamma_1, x\colon LL \vdash x\colon LL}{(7)}}\ \text{ATOM}$$

.

$$\dfrac{\dfrac{\dfrac{\text{similar to (0.1)}}{\Gamma_1, x\colon LL \vdash \diamond} \quad k_2\colon SigK^{HH}[LH, LL] \text{ in } \Gamma_1, x\colon LL}{\Gamma_1, x\colon LL \vdash k_2\colon SigK^{HH}[LH, LL]}\ \text{ATOM}}{\dfrac{\Gamma_1, x\colon LL \vdash vk(k_2)\colon VerK^{LH}[LH, LL]}{(8)}}\ \text{VerKey}$$

Proving the decryption .

For simplicity let

$$\Gamma_3 = \Gamma_1, x\colon LL, y\colon LH, m\prime\colon LL$$

$$\dfrac{\dfrac{\dfrac{(0.3)}{\Gamma_3 \vdash \diamond} \quad y\colon LH \text{ in } \Gamma_3}{\Gamma_3 \vdash y\colon LH}\ \text{ATOM} \quad \dfrac{\dfrac{(0.3)}{\Gamma_3 \vdash \diamond} \quad k_1\colon SymK^{HH}[HH] \text{ in } \Gamma_3}{\Gamma_3 \vdash k_1\colon SymK^{HH}[HH]}\ \text{ATOM} \quad \dfrac{\dfrac{\text{similar to (0.3)}}{\Gamma_3, n\prime\colon HH \vdash \diamond}}{\Gamma_3, n\prime\colon HH \vdash 0}\ \text{STOP}}{\dfrac{\Gamma_3 \vdash \text{ case } y \text{ of } \{|n\prime|\}^s_{k_1} \text{ in } 0}{\dfrac{\Gamma_1, x\colon LL, y\colon LH, m\prime\colon LL \vdash Q}{(9)}}}\ \text{SymDec}$$

Proving the wellformedness The $\Gamma_1 \vdash \diamond$, $\Gamma_2 \vdash \diamond$ and $\Gamma_3 \vdash \diamond$ hold, because all channels and keys in it are of type HH.

Conclusion If I didn't forget about any branch, this should be finished and typechecks. We have $img(\Gamma) = LL$, thus it preserves secrecy and integrity ☺