

Online Wallet [1]

Remark. This protocol uses $A \rightarrow C, S \{ \ell \dots \}$ to indicate that A sends the same message to both C and S .

$$C \rightarrow A \left\{ \begin{array}{l} \textcolor{red}{Login}(\langle \textcolor{brown}{string}, \textcolor{brown}{string} \rangle). A \rightarrow C, S \left\{ \begin{array}{l} \textcolor{red}{Ok}.\mu\textcolor{blue}{t}. S \rightarrow C \left\{ \textcolor{red}{Account}(\langle \textcolor{brown}{balance} : \textcolor{brown}{int}, \textcolor{brown}{overdraft} : \textcolor{brown}{int} \rangle). C \rightarrow S \left\{ \begin{array}{l} \textcolor{red}{Pay}(\langle \textcolor{brown}{string}, \textcolor{brown}{int} \rangle).\textcolor{blue}{t} \\ \textcolor{red}{Quit}.\textcolor{brown}{end} \end{array} \right\} \end{array} \right\} \\ \textcolor{red}{Fail}(\textcolor{brown}{string}).\textcolor{brown}{end} \end{array} \right\} \end{array} \right\}$$

References

- [1] Romyana Neykova, Nobuko Yoshida, and Raymond Hu. SPY: Local Verification of Global Protocols. In David Hutchison, Takeo Kanade, Josef Kittler, Jon M. Kleinberg, Friedemann Mattern, John C. Mitchell, Moni Naor, Oscar Nierstrasz, C. Pandu Rangan, Bernhard Steffen, Madhu Sudan, Demetri Terzopoulos, Doug Tygar, Moshe Y. Vardi, Gerhard Weikum, Axel Legay, and Saddek Bensalem, editors, *Runtime Verification*, volume 8174, pages 358–363. Springer Berlin Heidelberg, Berlin, Heidelberg, 2013.