303 - Systems Verification
Assessed Coursework 2

Deadline: 5 March - 14.00

Please submit a zipped file electronically containing a single file called `cw2.smv`. Use the comment environment to report the results to point 3 below, and any further remark you may wish to add. Please use intuitive variable names and comment your code in a way that helps understanding.

The following anonymity protocol is due to Chaum [Cha88].

"Three cryptographers are sitting down to dinner at their favorite three-star restaurant. Their waiter informs them that arrangements have been made with the maitre d'hotel for the bill to be paid anonymously. One of the cryptographers might be paying for dinner, or it might have been NSA (U.S. National Security Agency). The three cryptographers respect each other's right to make an anonymous payment, but they wonder if NSA is paying. They resolve their uncertainty fairly by carrying out the following protocol:

Each cryptographer flips an unbiased coin behind his menu, between him and the cryptographer on his right, so that only the two of them can see the outcome. Each cryptographer then states aloud whether the two coins he can see–the one he flipped and the one his left-hand neighbour flipped–fell on the same side or on different sides. If one of the cryptographers is the payer, he states the opposite of what he sees. An odd number of differences uttered at the table indicates that a cryptographer is paying; an even number indicates that NSA is paying (assuming that dinner was paid for only once). Yet if a cryptographer is paying, neither of the other two learns anything from the utterances about which cryptographer it is."

(Note that TOR is based on a variant of this protocol.)

1. Code the protocol in NuSMV by considering the following points.
   - Assume a random configuration for payers and non-payers with at most one cryptographer to be the payer.
   - Assume a random configuration of coins among the cryptographers.
   - Code the announcements following the coins configurations.
2. Express the specifications for the protocol in terms of temporal formulas either in LTL or CTL.
3. Check the specifications of the point above on your model and comment on the results you obtain.

References

[Cha88] D. Chaum. The dining cryptographers problem: Unconditional sender and recipient untraceability. *Journal of Cryptology*, 1(1):65–75, 1988.