References

[1] M. Abadi and Cédric Fournet. Mobile values, new names, and secure communication. In *Proceedings of the 28th ACM Symposium on Principles of Programming Languages (POPL'01)*, pages 104–115, January 2001.

[2] Hubert Comon-Lundh, Véronique Cortier, and Eugen Zlinescu. Deciding security properties of cryptographic protocols. application to key cycles. *Transaction on Computational Logic*, 2009. To appear. A preminary verion is available at `http://arxiv.org/abs/0708.3564`.

[3] D. Dolev, S. Even, and R. M. Karp. On the security of ping-pong protocols. *Information and Control*, 55:57–68, 1982.

[4] Gavin Lowe. An attack on the needham-schroeder public-key authentication protocol. *Information Processing Letters*, 56(3):131–133, 1996.

[5] Gavin Lowe. Breaking and fixing the needham-schroeder public-key protocol using fdr. In Margaria and Steffen, editors, *Tools and Algorithms for the Construction and Analysis of Systems (TACAS)*, volume 1055 of *Lecture Notes in Computer Science*, pages 147–166, 1996.

[6] Olivier Pereira and Jean-Jacques Quisquater. On the Perfect Encryption Assumption. In P. Degano, editor, *Proceedings of the Workshop on Issues in the Theory of Security (WITS 2000)*, pages 42–45, 2000.

[7] Victor Shoup. Sequences of games: A tool for taming complexity in security proofs, January 2004.

[8] Bogdan Warinschi. A computational analysis of the needham-schröeder-(lowe) protocol. In *IEEE Computer Security Foundations Workshop*, 2003.