Logics of Knowledge and Belief for Cryptographic Protocol Analysis

30 hours

Dean Rosenzweig

Logics of knowledge and belief: Modalities, Kripke structures and frames, correspondence. The logic of objective knowledge: individual, shared, distributed and common knowledge. Knowledge of agents in distributed computations. Knowledge and time. Knowledge–based programming. Knowledge and rational belief. Dogmatic belief.

Abstract encryption and protocol models: Dolev–Yao model. Protocols and attacks. Formal models: multiset–rewriting and strand spaces. Formal criteria for security.

Proposed logics for protocol analysis: Logics of Burrows–Abadi–Needham (BAN), Abadi–Tuttle (AT), Gong–Needham–Yahalom (GNY), Syverson–Oorschot (SVO), . . . —notation, rules, examples, semantics, limitations.

An object model of abstract encryption: Abstract notions of secrecy, indistinguishability, plaintext–awareness. Abstract state machines and Asml. Asml–based models of protocols. Logics of knowledge and belief over Asml.

Familiarity with the contents of courses *Introduction to Modal Logic* (2001/2002), and *Cryptographic Protocols* (2000/2001), while not a formal prerequisite, is warmly recommended—topics discussed there will not be rediscussed in detail.

Essential References

R. Fagin, J.Y. Halpern, Y. Moses, M.Y. Vardi, *Reasoning About Knowledge*, MIT Press 1995, http://www.cs.rice.edu/vardi/papers/index.html/

M. Abadi, M. Tuttle, *A semantics for a logic of authentication*, in 10th Annual ACM Symposium on Principles of Distributed Computing, ACM Press 1991, pp. 201–216, http://www.crl.research.digital.com/who/people/tuttle/bib.htm

M. Burrows, M. Abadi, R. Needham, *A logic of authentication*, TR 39, DEC SRC 1989
http://gatekeeper.dec.com/pub/DEC/SRC/research-reports/abstracts/src-rr-039.html

I. Cervesato, N. Durgin, P. Lincoln, J. Mitchell, A. Scedrov, *Relating Strands and Multiset Rewriting for Security Protocol Analysis*, in CSFW00, IEEE 2000, pp. 35–51
http://chacs.nrl.navy.mil/publications/CHACS/CRYPTOindex.html

L. Gong, R. Needham, R. Yahalom, *Reasoning About Belief in Cryptographic Protocols*, in 1990 IEEE Symposium on Research in Security and Privacy, IEEE 1991, http://citeseer.nj.nec.com/gong90reasoning.html

P. Syverson,P.C. van Oorschot, *On Unifying Some Cryptographic Protocol Logics*, in 1994 IEEE Computer Society Symposium on Research in Security and Privacy, IEEE 1994, pp. 14–28,
http://chacs.nrl.navy.mil/publications/CHACS/CRYPTOindex.html

P. Syverson, *Towards a Strand Semantics for Authentication Logics*, in Electronic Notes in Theoretical Computer Science 20, 2000
http://chacs.nrl.navy.mil/publications/CHACS/CRYPTOindex.html

http://www.research.microsoft.com/foundations/AsmL/

Recommended References

http://theory.lcs.mit.edu/rivest/crypto-security.html

http://www.di.ens.fr/ monniaux/biblio/protocols.html

http://www.eecs.umich.edu/gasm/

P. Blackburn, M. de Riejke, Y. Venema, *Modal Logic*, 1999,
http://www.illc.uva.nl/mdr/Publications/modal-logic.html

J. Clark, J. Jacob, *A Survey of Authentication Protocol Literature*, 1997,
http://www-users.cs.york.ac.uk/jac/papers/drareviewps.ps

C. Meadows, *Open Issues in Formal Methods for Cryptographic Protocol Analysis*, in DISCEX2000, IEEE 2000, pp. 237–250
http://chacs.nrl.navy.mil/publications/CHACS/CRYPTOindex.html

D. Stinson, *Cryptography: Theory and Practice*, CRC Press 1997,
http://www.cacr.math.uwaterloo.ca/dstinson/CTAP.html