



## UvA-DARE (Digital Academic Repository)

### Epistemic modelling and protocol dynamics

Wang, Y.

**Publication date**  
2010

[Link to publication](#)

#### **Citation for published version (APA):**

Wang, Y. (2010). *Epistemic modelling and protocol dynamics*. [Thesis, fully internal, Universiteit van Amsterdam]. Institute for Logic, Language and Computation.

#### **General rights**

It is not permitted to download or to forward/distribute the text or part of it without the consent of the author(s) and/or copyright holder(s), other than for strictly personal, individual use, unless the work is under an open content license (like Creative Commons).

#### **Disclaimer/Complaints regulations**

If you believe that digital publication of certain material infringes any of your rights or (privacy) interests, please let the Library know, stating your reasons. In case of a legitimate complaint, the Library will make the material inaccessible and/or remove it from the website. Please Ask the Library: <https://uba.uva.nl/en/contact>, or a letter to: Library of the University of Amsterdam, Secretariat, P.O. Box 19185, 1000 GD Amsterdam, The Netherlands. You will be contacted as soon as possible.

---

## Bibliography

- [ABV03] R. Accorsi, D. Basin, and L. Vigano. Towards an awareness-based semantics for security protocol analysis. *Electronic Notes in Theoretical Computer Science*, 55(1):5–24, January 2003. Cited on page 143.
- [ABvDS09] T. Ågotnes, P. Balbiani, H. van Ditmarsch, and P. Seban. Group announcement logic. *Journal of Applied Logic*, July 2009. Cited on page 35.
- [AC04] M. Abadi and V. Cortier. Deciding knowledge in security protocols under equational theories. In *Proceedings of ICALP '04*, volume 3142 of LNCS, pages 46–58, 2004. Cited on pages 150 and 151.
- [AF01] M. Abadi and C. Fournet. Mobile values, new names, and secure communication. In *Proceedings of POPL '01*, pages 104–115, 2001. Cited on pages 141 and 150.
- [AHL<sup>+</sup>08] A. Antonik, M. Huth, K. Larsen, U. Nyman, and A. Wasowski. 20 years of mixed and modal specifications. *Bulletin of the European Association for Theoretical Computer Science*, June 2008. Cited on page 104.
- [AHM<sup>+</sup>98] R. Alur, T. A. Henzinger, F. Y. C. Mang, S. Qadeer, S. K. Rajamani, and S. Tasiran. Mocha: Modularity in model checking. In *Proceedings of CAV'98*, pages 521–525, 1998. Cited on page 149.
- [AN95] R. Anderson and R. Needham. Programming satan's computer. In J. Leeuwen, editor, *Computer Science Today*, volume 1000 of LNCS, pages 426–440, Berlin/Heidelberg, 1995. Springer-Verlag. Cited on page 140.
- [AR02] M. Abadi and P. Rogaway. Reconciling two views of cryptography (the computational soundness of formal encryption). In *Proceedings of the International Conference IFIP*, 2002. Cited on page 150.
- [AT91] M. Abadi and M. R. Tuttle. A semantics for a logic of authentication (extended abstract). In *Proceedings of PODC '91*, pages 201–216, New York, NY, USA, 1991. ACM. Cited on page 150.
- [Auc09] G. Aucher. BMS revisited. In *Proceedings of TARK '09*, pages 24–33, 2009. Cited on pages 39 and 56.
- [Aum76] R. J. Aumann. Agreeing to disagree. *The Annals of Statistics*, 4(6):1236–1239, 1976. Cited on page 84.

- [Aum89] R. Aumann. Notes on interactive epistemology. 1989. Cited on page 84.
- [AvC07] R. Alur, P. Černý, and S. Chaudhuri. Model checking on trees with path equivalences. In *Proceedings of TACAS '07*, pages 664–678, 2007. Cited on pages 156 and 157.
- [AvDR09] M. D. Atkinson, H. van Ditmarsch, and S. Roehling. Avoiding bias in cards cryptography. *Australasian Journal of Combinatorics*, 44:3–17, February 2009. Cited on pages 3 and 33.
- [AvZ06] R. Alur, P. Černý, and S. Zdancewic. Preserving secrecy under refinement. In *Automata, Languages and Programming*, pages 107–118, 2006. Cited on page 156.
- [BAN89] M. Burrows, M. Abadi, and R. Needham. A logic of authentication. *Proceedings of the Royal Society of London, Series A, Mathematical and Physical Sciences*, 426(1871):233–271, December 1989. Cited on page 142.
- [BCG87] M. Browne, E. Clarke, and O. Grumberg. Characterizing kripke structures in temporal logic. In *Proceedings of TAPSOFT '87*, pages 256–270, 1987. Cited on page 83.
- [BCL09] I. Boureanu, M. Cohen, and A. Lomuscio. Automatic verification of temporal-epistemic properties of cryptographic protocols. *Journal of Applied Non-Classical Logics*, 19(4):463–487, 2009. Cited on pages 146, 147, 148, and 149.
- [BCM<sup>+</sup>92] J. R. Burch, E. M. Clarke, K. L. McMillan, D. L. Dill, and L. J. Hwang. Symbolic model checking:  $10^{20}$  states and beyond. *Information and Computation*, 98(2):142–170, June 1992. Cited on page 6.
- [BdRV02] P. Blackburn, M. de Rijke, and Y. Venema. *Modal Logic*. Cambridge University Press, November 2002. Cited on pages 13, 88, and 132.
- [BE09] D. Bonnay and P. Égré. Inexact knowledge with introspection. *Journal of Philosophical Logic*, 38(2):179–227, April 2009. Cited on page 40.
- [BG99] G. Bruns and P. Godefroid. Model checking partial state spaces with 3-valued temporal logics. In Nicolas Halbwachs and D. Peled, editors, *Proceedings of CAV '99*, volume 1633 of LNCS, page 684, Berlin, Heidelberg, January 1999. Springer Berlin Heidelberg. Cited on page 103.
- [BG04] G. Bruns and P. Godefroid. Model checking with multi-valued logics. In *Automata, Languages and Programming*, pages 245–273. 2004. Cited on page 108.
- [BHR84] D. Brookes, C. A. R. Hoare, and A. W. Roscoe. A theory of communicating sequential processes. *Journal of the ACM*, 31(3):560–599, 1984. Cited on pages 60 and 143.
- [Bie90] P. Bieber. A logic of communication in hostile environment. In *Proceedings of Computer Security Foundations Workshop III*, pages 14–22, 1990. Cited on page 143.
- [BK85] J. A. Bergstra and J. W. Klop. Algebra of communicating processes with abstraction. *Theoretical Computer Science*, 37(1):77–121, 1985. Cited on page 60.

- [BKR09] V. Bárány, Łukasz K. ser, and A. Rabinovich. Cardinality quantifiers in MLO over trees. In *Proceedings of CSL 09*, pages 117–131, 2009. Cited on page 85.
- [BM96] J. Barwise and L. Moss. *Vicious Circles*. (Center for the Study of Language and Information, August 1996. Cited on page 83.
- [BM04] A. Baltag and L. Moss. Logics for epistemic programs. *Synthese*, 139(2):165–224, March 2004. Cited on pages 22, 39, 49, and 117.
- [BMS98] A. Baltag, L. Moss, and S Solecki. The logic of public announcements, common knowledge, and private suspicions. In *Proceedings of TARK '98*, pages 43–56. Morgan Kaufmann Publishers Inc., 1998. Cited on pages 3, 15, and 51.
- [BP05] M. Bhargava and C. Palamidessi. Probabilistic anonymity. In *Proceedings of CONCUR'05*, volume 3653 of LNCS, pages 171–185, 2005. Cited on page 144.
- [BRS07] A. Baskar, R. Ramanujam, and S. P. Suresh. Knowledge-based modelling of voting protocols. In *Proceedings of TARK '07*, pages 62–71, New York, NY, USA, 2007. ACM. Cited on pages 141, 142, 145, 150, 151, 153, and 157.
- [Brz64] J. A. Brzowski. Derivatives of regular expressions. *Journal of the ACM*, 11(4):481–494, October 1964. Cited on page 40.
- [BS97] J. Barwise and J. Seligman. *Information flow: the logic of distributed systems*. Cambridge University Press, New York, NY, USA, 1997. Cited on page 3.
- [BS06] J. Bradfield and C. Stirling. Modal  $\mu$ -calculi. In *Handbook of Modal Logic*, volume 3, pages 722–756. Elsevier Science Inc., New York, NY, USA, 2006. Cited on page 84.
- [BS08a] A. Baltag and S. Smets. Probabilistic dynamic belief revision. *Synthese*, 165(2):179–202, 2008. Cited on pages 56 and 143.
- [BS08b] Mario Benevides and L. Schechter. A propositional dynamic logic for CCS programs. pages 83–97, 2008. Cited on page 39.
- [CBRZ01] E. Clarke, A. Biere, R. Raimi, and Y. Zhu. Bounded model checking using satisfiability solving. *Formal Methods in System Design*, 19(1):7–34, July 2001. Cited on page 6.
- [CC77] P. Cousot and R. Cousot. Abstract interpretation: a unified lattice model for static analysis of programs by construction or approximation of fixpoints. In *Proceedings of POPL '77*, pages 238–252, New York, NY, USA, 1977. ACM. Cited on page 6.
- [CCD88] D. Chaum, C. Crépeau, and I. Damgard. Multiparty unconditionally secure protocols. In *Proceedings of STOC '88*, pages 11–19, New York, NY, USA, 1988. ACM. Cited on page 155.
- [CD05a] M. Cohen and M. Dam. A completeness result for BAN logic. In *Proceedings of Methods for Modalities '05*, 2005. Cited on page 150.
- [CD05b] M. Cohen and M. Dam. Logical omniscience in the semantics of BAN logic. In *Proceedings of FCS '05*, 2005. Cited on page 143.
- [CD07] M. Cohen and M. Dam. A complete axiomatization of knowledge and cryptography. In *Proceedings of LiCS '07*, pages 77–88. IEEE Computer Society, 2007. Cited on pages 143, 150, and 151.

- [CDGLV02] D. Calvanese, G. De Giacomo, M. Lenzerinia, and M. Y. Vardi. Rewriting of regular expressions and regular path queries. *Journal of Computer and System Sciences*, 64(3):443–465, May 2002. Cited on pages **121**, **123**, and **125**.
- [CDK09a] R. Chadha, S. Delaune, and S. Kremer. Epistemic logic for the applied pi calculus. In *Proceedings of FMOODS '09/FORTE '09*, pages 182–197, Berlin, Heidelberg, 2009. Springer-Verlag. Cited on page **150**.
- [CDK09b] S. Ciobăcă, S. Delaune, and S. Kremer. Computing knowledge in security protocols under convergent equational theories. In *Proceedings of CADE*, pages 355–370, 2009. Cited on page **150**.
- [CDLR09] M. Cohen, M. Dam, A. Lomuscio, and F. Russo. Abstraction in model checking multi-agent systems. In *Proceedings of AAMAS '09*, 2009. Cited on pages **6**, **104**, and **158**.
- [CEFJ96] E. M. Clarke, R. Enders, T. Filkorn, and S. Jha. Exploiting symmetry in temporal logic model checking. *Formal Methods in System Design*, 9(1-2):77–104, 1996. Cited on page **6**.
- [CGJ+03] E. Clarke, O. Grumberg, S. Jha, Y. Lu, and H. Veith. Counterexample-guided abstraction refinement for symbolic model checking. *Journal of the ACM*, 50(5):752–794, September 2003. Cited on pages **6** and **117**.
- [CGL94] E. M. Clarke, O. Grumberg, and D. E. Long. Model checking and abstraction. *ACM Transactions on Programming Languages and Systems*, 16(5):1512–1542, September 1994. Cited on page **6**.
- [CGP99] E. M. Clarke, O. Grumberg, and D. A. Peled. *Model Checking*. The MIT Press, January 1999. Cited on pages **5**, **125**, and **143**.
- [Cha88] D. Chaum. The dining cryptographers problem: unconditional sender and receiver untraceability. *Journal of Cryptology*, 1:65–75, 1988. Cited on page **149**.
- [CJM98] E. M. Clarke, S. Jha, and W. R. Marrero. Using state space exploration and a natural deduction style message derivation engine to verify security protocols. In *Proceedings of PROCOMET '98*, pages 87–106, London, UK, UK, 1998. Chapman & Hall, Ltd. Cited on page **144**.
- [CLDQ09] M. Cohen, A. Lomuscio, M. Dam, and H. Qu. A symmetry reduction technique for model checking temporal epistemic logic. In *Proceedings of IJCAI '09*, 2009. Cited on pages **6**, **80**, **104**, and **158**.
- [Con71] J. H. Conway. *Regular Algebra and Finite Machines*. Chapman and Hall, September 1971. Cited on pages **40** and **126**.
- [Cre06] C. J. F. Cremers. *Scyther - Semantics and Verification of Security Protocols*. Ph.D. dissertation, Eindhoven University of Technology, 2006. Cited on page **146**.
- [CvdPW08] T. Chen, J. van de Pol, and Y. Wang. Pdl over accelerated labeled transition systems. In *Proceedings of TASE '09*, pages 193–200, Los Alamitos, CA, USA, 2008. IEEE Computer Society. Cited on pages **8** and **136**.
- [DETW09] F. Dechesne, D. J. N. Eijck, W. Teepe, and Y. Wang. What is protocol analysis? In D. J. N. van Eijck and R. Verbrugge, editors, *Discourses on Social Software*, volume 5 of *Texts in Logic and Games*. Amsterdam University Press, January 2009. Cited on page **8**.

- [dJ09] T. de Jager. *Awareness, Attention, Assumption*. PhD thesis, October 2009. Cited on page 81.
- [DKR06] S. Delaune, S. Kremer, and M. Ryan. Coercion-resistance and receipt-freeness in electronic voting. In *Proceedings of CSFW '06*, pages 28–42. IEEE Computer Society, 2006. Cited on page 142.
- [DKR07] S. Delaune, S. Kremer, and M. Ryan. Verifying privacy-type properties of electronic voting protocols. *Journal of Computer Security*, 2007. Cited on pages 139 and 142.
- [DLMS99] N. A. Durgin, P. D. Lincoln, J. C. Mitchell, and A. Scedrov. Undecidability of bounded security protocols. In *Proceedings of the Workshop on Formal Methods and Security Protocols (FMSP)*, 1999. Cited on page 157.
- [DMO07] F. Dechesne, M. R. Mousavi, and S. Orzan. Operational and epistemic approaches to protocol analysis: Bridging the gap. In *Proceedings of LPAR '07*, pages 226–241, 2007. Cited on page 148.
- [DN05] D. Dams and K. S. Namjoshi. Automata as abstractions. In *Proceedings of VMCAI '05*, pages 216–232, 2005. Cited on page 86.
- [DOW08] F. Dechesne, S. Orzan, and Y. Wang. Refinement of kripke models for dynamics. In *Proceedings of ICTAC '08*, pages 111–125, 2008. Cited on pages 6, 8, 117, and 158.
- [DvETW09] F. Dechesne, J. van Eijck, W. Teepe, and Y. Wang. Dynamic epistemic logic for protocol analysis. In D. J. N. van Eijck and R. Verbrugge, editors, *Discourses on Social Software*, volume 5 of *Texts in Logic and Games*. Amsterdam University Press, January 2009. Cited on page 8.
- [DvEW10] H. Ditmarsch, J. van Eijck, and W. Wu. One hundred prisoners and a lightbulb – logic and computation. In *Proceedings of KR '10*. AAAI, 2010. Cited on page 3.
- [DW07] F. Dechesne and Y. Wang. Dynamic epistemic verification of security protocols: framework and case study. In *A Meeting of the minds: Proceedings of LORI-I workshop*, Texts in Computer Science, pages 129–144, 2007. Cited on pages 6, 8, 23, 59, 117, and 148.
- [DW10] F. Dechesne and Y. Wang. To know or not to know: Epistemic approaches to security protocol verification. *To appear in Synthese, special section of Knowledge, Rationality and Action*, 2010. Cited on page 8.
- [DY83] D. Dolev and A. Yao. On the security of public key protocols. *IEEE Transactions on Information Theory*, 29(2):198–208, 1983. Cited on page 146.
- [EGvdM07] K. Engelhardt, P. Gammie, and R. van der Meyden. Model checking knowledge and linear time: Pspace cases. In *Proceedings of LFCS '07*, pages 195–211, 2007. Cited on page 157.
- [Eme87] E. Allen Emerson. Uniform inevitability is tree automaton ineffable. *Information Processing Letters.*, 24(2):77–79, 1987. Cited on page 156.
- [ES96] E. A. Emerson and A. Prasad Sistla. Symmetry and model checking. *Formal Methods in System Design*, 9(1-2):105–131, 1996. Cited on page 6.

- [EvdMM98] K. Engelhardt, R. van der Meyden, and Y. Moses. Knowledge and the logic of local propositions. In *Proceedings of TARK '98*, pages 29–41, San Francisco, CA, USA, 1998. Morgan Kaufmann Publishers Inc. Cited on page 69.
- [EVDMS02] K. Engelhardt, R. Van Der Meyden, and K. Su. Modal logics with a linear hierarchy of local propositional quantifiers. In *Proceedings of AiML '02*, volume 9, 2002. Cited on page 158.
- [EvdP06] M. Espada and J. van de Pol. Accelerated modal abstractions of labelled transition systems. In M. J.son and Varmo Vene, editors, *Proceedings of AMAST '06*, volume 4019, pages 338–352, Berlin, Heidelberg, 2006. Springer Berlin Heidelberg. Cited on pages 120, 121, 128, and 136.
- [FGM04] R. Focardi, R. Gorrieri, and F. Martinelli. *Classification of Security Properties (Part II: Network Security)*, volume 2946 of LNCS, pages 139–185. Springer Berlin / Heidelberg, 2004. Cited on page 141.
- [FHMV95] R. Fagin, J. Halpern, Y. Moses, and M. Vardi. *Reasoning about knowledge*. MIT Press, Cambridge, MA, USA, 1995. Cited on pages 2, 4, 15, 59, 117, 143, and 149.
- [FHMV97] R. Fagin, J. Y. Halpern, Y. Moses, and M. Y. Vardi. Knowledge-based programs. *Distributed Computing*, 10(4):199–225, July 1997. Cited on pages 2, 4, 24, and 153.
- [Fit91] M. Fitting. Many-valued modal logics. *Fundamenta Informaticae*, 15(3-4):235–254, 1991. Cited on page 104.
- [Fit92] M. Fitting. Many-valued modal logics II. *Fundamenta Informaticae*, 17(1-2):55–73, 1992. Cited on page 104.
- [FL79] M. J. Fischer and R. E. Ladner. Propositional dynamic logic of regular programs. *Journal of Computer and System Sciences*, 18(2):194–211, 1979. Cited on page 13.
- [FW96] M. J. Fischer and Rebecca N. Wright. Bounds on secret key exchange using a random deal of cards. *Journal of Cryptology*, Springer Verlag, 9:71–99, 1996. Cited on page 155.
- [Gab02] D. M. Gabbay. A theory of hypermodal logics: Mode shifting in modal logic. *Journal of Philosophical Logic*, 31(3):211–243, June 2002. Cited on pages 39 and 40.
- [GG97] J. Gerbrandy and W. Groeneveld. Reasoning about information change. *Journal of Logic, Language and Information*, 6(2):147–169, April 1997. Cited on pages 3, 15, 17, and 105.
- [GHJ01] P. Godefroid, M. Huth, and R. Jagadeesan. Abstraction-based model checking using modal transition systems. In K. G. Larsen and Mogens Nielsen, editors, *Proceedings of CONCUR '01*, volume 2154 of LNCS, pages 426–440, Berlin, Heidelberg, August 2001. Springer Berlin Heidelberg. Cited on pages 6 and 103.
- [GHPvR05] F. D. Garcia, I. Hasuo, W. Pieters, and P. van R. um. Provable anonymity. In *Proceedings of FMSE '05*, pages 63–72, New York, NY, USA, 2005. ACM. Cited on page 150.

- [GJ02] P. Godefroid and R. Jagadeesan. Automatic abstraction using generalized model checking. In *Proceedings of CAV '02*, pages 137–150, London, UK, 2002. Springer-Verlag. Cited on page 105.
- [GJ03] P. Godefroid and R. Jagadeesan. On the expressiveness of 3-valued models. In *Proceedings of VMCAI '03*, pages 206–222, 2003. Cited on page 107.
- [GK03] E. Grädel and S. Kreutzer. Will deflation lead to depletion? on non-monotone fixed point inductions. In *Proceedings of LiCS '03*, pages 158–178, Washington, DC, USA, 2003. IEEE Computer Society. Cited on page 34.
- [GM99] D. Giammarresi and R. Montalbano. Deterministic generalized automata. *Theoretical Computer Science*, 215(1-2):191–208, 1999. Cited on page 121.
- [GNY90] L. Gong, R. Needham, and R. Yahalom. Reasoning about belief in cryptographic protocols. In *Research in Security and Privacy*, 1990. Cited on page 143.
- [GO06] V. Goranko and M. Otto. Model theory of modal logic. In *Handbook of Modal Logic*, volume 3, pages 249–329. Elsevier Science Inc., New York, NY, USA, 2006. Cited on page 88.
- [GP94] J. F. Groote and A. Ponse. The syntax and semantics of  $\mu$ CRL. In *Algebra of Communicating Processes, Workshops in Computing*, pages 26–62. 1994. Cited on page 60.
- [GPS96] P. Godefroid, D. Peled, and M. Staskauskas. Using partial-order methods in the formal validation of industrial concurrent programs. In *Proceedings of ISSTA '96*, pages 261–269, New York, NY, USA, 1996. ACM. Cited on page 6.
- [GvdM04] P. Gammie and R. van der Meyden. MCK: Model checking the logic of knowledge. In *Proceedings of CAV '04*, pages 256–259, 2004. Cited on page 149.
- [Hal87] J. Y. Halpern. A little knowledge goes a long way: simple knowledge-based derivations and correctness proofs for a family of protocols. In *Proceedings of PODC '87*, pages 269–280, New York, NY, USA, 1987. ACM. Cited on page 3.
- [Hal00] J. Y. Halpern. A note on knowledge-based programs and specifications. *Distributed Computing*, 13(3):145–153, July 2000. Cited on page 3.
- [Har96] S. Hart. “knowing whether”, “knowing that”, and the cardinality of state spaces. *Journal of Economic Theory*, 70(1):249–256, July 1996. Cited on pages 84 and 85.
- [HD07] A. Hunter and J. P. Delgrande. Belief change and cryptographic protocol verification. In *Proceedings of AAI '07*, pages 427–433, 2007. Cited on page 143.
- [HF89] J. Y. Halpern and R. Fagin. Modelling knowledge and action in distributed systems. *Distributed Computing*, 3(4):159–177, 1989. Cited on pages 2, 3, 37, and 153.
- [Hin62] J. Hintikka. *Knowledge and Belief: An Introduction to the Logic of the Two Notions*. Cornell University Press, Ithaca N.Y., 1962. Cited on page 143.

- [HJS01] M. Huth, R. Jagadeesan, and D. Schmidt. Modal transition systems: A foundation for three-valued program analysis. In D. Sands, editor, *Programming Languages and Systems*, volume 2028, pages 155–169, Berlin, Heidelberg, March 2001. Springer Berlin Heidelberg. Cited on pages **103**, **105**, and **107**.
- [HKP82] D. Harel, D. Kozen, and R. Parikh. Process logic: Expressiveness, decidability, completeness. *Journal of Computer and System Sciences*, 25(2):144–170, 1982. Cited on page **39**.
- [HKT00] D. Harel, D. Kozen, and J. Tiuryn. *Dynamic Logic (Foundations of Computing)*. The MIT Press, 1st edition, October 2000. Cited on pages **50** and **135**.
- [HM90] J. Y. Halpern and Y. Moses. Knowledge and common knowledge in a distributed environment. *Journal of the ACM*, 37(3):549–587, 1990. Cited on page **15**.
- [HMY94] J. Y. Halpern, Y. Moses, and M. Y. Vardi. Algorithmic knowledge. In *Proceedings of TARK '94*, pages 255–266, San Francisco, CA, USA, 1994. Morgan Kaufmann Publishers Inc. Cited on page **143**.
- [HMY05] A. Hommersom, J.-Jules Meyer, and E. Vink. Update semantics of security protocols. In *Information, Interaction and Agency*, pages 289–327, Berlin/Heidelberg, 2005. Springer-Verlag. Cited on page **148**.
- [HO02] J. Halpern and K. O’Neill. Secrecy in multiagent systems. In *Proceedings of CSFW '02*, pages 32–46, 2002. Cited on page **144**.
- [HO05] J. Halpern and K. O’Neill. Anonymity and information hiding in multiagent systems. *Journal of Computer Security*, 13(3):483–514, May 2005. Cited on pages **142** and **144**.
- [Hoa85] C. A. R. Hoare. *Communicating Sequential Processes*. Prentice/Hall International, April 1985. Cited on page **5**.
- [Hos09] T. Hoshi. *Epistemic Dynamics and Protocol Information*. PhD thesis, Stanford, 2009. Cited on pages **3**, **21**, **37**, and **39**.
- [Hos10] T. Hoshi. Merging DEL and ETL. *Journal of Logic, Language and Information*, January 2010. Cited on pages **3** and **154**.
- [HP03] J. Y. Halpern and R. Pucella. Modeling adversaries in a logic for security protocol analysis. In *Formal Aspects of Security*, pages 87–100, 2003. Cited on pages **141**, **143**, **144**, **145**, and **146**.
- [HP10a] J. Y. Halpern and R. Pucella. Dealing with logical omniscience: Expressiveness and pragmatics. *Artificial Intelligence*, April 2010. To appear. Cited on page **143**.
- [HP10b] T. Hoshi and E. Pacuit. A dynamic logic of knowledge and access. *Synthese*, 2010. forthcoming. Cited on pages **3** and **37**.
- [HV86] J. Y. Halpern and M. Y. Vardi. The complexity of reasoning about knowledge and time. In *Proceedings of STOC '86*, pages 304–315, New York, NY, USA, 1986. ACM. Cited on page **157**.
- [HW05] Y-S Han and D. Wood. The generalization of generalized automata: Expression automata. In *Implementation and Application of Automata*, pages 156–166, 2005. Cited on page **121**.

- [HY09] T. Hoshi and A. Yap. Dynamic epistemic logic with branching temporal structures. *Synthese*, 169(2):259–281, July 2009. Cited on pages 3, 21, 37, 39, and 154.
- [ID96] C. N. Ip and D. L. Dill. Better verification through symmetry. *Formal Methods in System Design*, 9(1-2):41–75, 1996. Cited on page 6.
- [Jac02] D. Jackson. Alloy: a lightweight object modelling notation. *ACM Transactions on Software Engineering and Methodology*, 11(2):256–290, April 2002. Cited on page 32.
- [JdV06] H. L. Jonker and E. P. de Vink. Formalising Receipt-Freeness. In Sokratis K. Katsikas, Javier Lopez, M. Backes, Stefanos Gritzalis, and Bart Preneel, editors, *Information Security*, volume 4176 of *LNCS*, pages 476–488, August 2006. Cited on page 142.
- [JP06] H. Jonker and W. Pieters. Receipt-freeness as a special case of anonymity in epistemic logic. In *IAVoSS Workshop On Trustworthy Elections*, June 2006. Cited on pages 142 and 150.
- [JW95] D. Janin and I. Walukiewicz. Automata for the modal  $\mu$ -calculus and related results. In *Proceedings of MFCS '95*, pages 552–562, 1995. Cited on pages 84, 86, and 87.
- [Kle50] S. C. Kleene. *Introduction to Metamathematics*. D. Van Nostrand, Princeton, NJ, 1950. Cited on page 107.
- [KNN<sup>+</sup>08] M. Kacprzak, W. Nabi lek, A. Niewiadomski, W. Penczek, Agata P trola, Maciej Szreter, Bożena Woźna, and Andrzej Zbrzezny. Verics 2007 - a model checker for knowledge and real-time. *Fundamenta Informaticae*, 85(1):313–328, January 2008. Cited on page 149.
- [Koz83] D. Kozen. Results on the propositional  $\mu$ -calculus. *Theoretical Computer Science*, 27(3):333–354, 1983. Cited on page 84.
- [Koz91] D. Kozen. A completeness theorem for kleene algebras and the algebra of regular events. In *Proceedings of LiCS '91*, pages 214–225, 1991. Cited on pages 40, 121, 131, and 132.
- [Koz01] D. Kozen. Automata on guarded strings and applications. Technical report, Ithaca, NY, USA, 2001. Cited on pages 43, 46, and 47.
- [Kra07] S. Kramer. *Logical concepts in cryptography*. PhD thesis, EPFL, 2007. Cited on pages 140 and 141.
- [KvB04] B. Kooi and J. van Benthem. Reduction axioms for epistemic actions. In R. Schmidt, I. Pratt-Hartmann, M. Reynolds, and H. Wansing, editors, *Preliminary Proceedings of AiML-2004*, pages 197–211. Department of Computer Science, University of Manchester, 2004. Cited on pages 39, 49, 51, 52, and 53.
- [Lan06] M. Lange. Model checking propositional dynamic logic with all extras. *Journal of Applied Logic*, 4(1):39–49, March 2006. Cited on pages 120 and 125.
- [Lar90] K. Larsen. Modal specifications. In *Automatic Verification Methods for Finite State Systems*, pages 232–246, 1990. Cited on page 110.

- [LC03] C. H. Lundh and V. Cortier. Security properties: two agents are sufficient. In *Proceedings of ESOP '03*, volume 2618 of *LNCS*, pages 99–113, 2003. Cited on page **146**.
- [Liu08] F. Liu. *Changing for the better*. PhD thesis, University of Amsterdam, 2008. Cited on page **56**.
- [Lod95] K. Lodaya. A logical study of distributed transition systems. *Information and Computation*, 119(1):91–118, May 1995. Cited on page **121**.
- [Low96] G. Lowe. Breaking and fixing the needham-schroeder public-key protocol using FDR. In *Proceedings of TACAS '96*, pages 147–166, London, UK, 1996. Springer-Verlag. Cited on pages **140** and **143**.
- [LP85] O. Lichtenstein and A. Pnueli. Checking that finite state concurrent programs satisfy their linear specification. In *Proceedings of POPL '85*, pages 97–107, New York, NY, USA, 1985. ACM. Cited on page **129**.
- [LP07] A. Lomuscio and W. Penczek. Symbolic model checking for temporal-epistemic logics. *SIGACT News*, 38(3):77–99, 2007. Cited on page **149**.
- [LQR09] A. Lomuscio, H. Qu, and F. Raimondi. MCMAS: A model checker for the verification of multi-agent systems. In *Proceedings of CAV '09*, pages 682–688, 2009. Cited on page **149**.
- [LR06a] A. Lomuscio and F. Raimondi. The complexity of model checking concurrent programs against CTLK specifications. In *Proceedings of AAMAS '06*, pages 548–550, New York, NY, USA, 2006. ACM. Cited on page **158**.
- [LR06b] A. Lomuscio and F. Raimondi. MCMAS: A model checker for multi-agent systems. In *Proceedings of TACAS '06*, volume 3920 of *LNCS*, pages 450–454. Springer, 2006. Cited on page **149**.
- [LS87] H. Läuchli and C. Savioz. Monadic second order definable relations on the binary tree. *The Journal of Symbolic Logic*, 52(1):219–226, 1987. Cited on page **156**.
- [LS07] M. Leucker and C. Sánchez. Regular linear temporal logic. In Cliff B. J.es, Zhiming Liu, and Jim Woodcock, editors, *Proceedings of ICTAC '07*, volume 4711 of *LNCS*, pages 291–305, Berlin, Heidelberg, 2007. Springer Berlin Heidelberg. Cited on page **121**.
- [LT88] K. G. Larsen and B. Thomsen. A modal process logic. In *Proceedings of LiCS '88*, pages 203–210, July 1988. Cited on page **104**.
- [Lut06] Carsten Lutz. Complexity and succinctness of public announcement logic. In *Proceedings of AAMAS '06*, pages 137–143, New York, NY, USA, 2006. ACM. Cited on page **56**.
- [Mat03] R. Mateescu. Efficient on-the-fly model-checking for regular alternation-free mu-calculus. *Science of Computer Programming*, 46(3):255–281, March 2003. Cited on page **121**.
- [McM02] K. McMillan. Applying sat methods in unbounded symbolic model checking. In *Proceedings of CAV'02*, pages 250–264, London, UK, 2002. Springer-Verlag. Cited on page **6**.

- [MDH86] Y. Moses, D. Dolev, and J. Y. Halpern. Cheating husbands and other stories: A case study of knowledge, action, and communication. *Distributed Computing*, 1(3):167–176, September 1986. Cited on page 3.
- [Mey87] J. J. Meyer. A different approach to deontic logic: deontic logic viewed as a variant of dynamic logic. *Notre Dame Journal of Formal Logic*, 29(1):109–136, 1987. Cited on page 39.
- [Mil82] R. Milner. *A Calculus of Communicating Systems*. Springer-Verlag New York, Inc., Secaucus, NJ, USA, 1982. Cited on page 60.
- [MM05] J. Miller and L. Moss. The undecidability of iterated modal relativization. *Studia Logica*, 79, April 2005. Cited on page 23.
- [Niw91] D. Niwiński. On the cardinality of sets of infinite trees recognizable by finite automata. In *Proceedings of MFCS '91*, pages 367–376, 1991. Cited on pages 84, 85, 89, 95, 96, 98, and 99.
- [NS78] R. M. Needham and M. D. Schroeder. Using encryption for authentication in large networks of computers. *Communications of the ACM*, 21(12):993–999, December 1978. Cited on page 140.
- [Orz05] S. Orzan. LYS: a knowledge analysis toolset, 2005. Available at <http://www.mobanet.nl/simona/lys/>. Cited on page 149.
- [Par78] R. Parikh. The completeness of propositional dynamic logic. In *Proceedings of MFCS '78*, pages 403–415, 1978. Cited on page 14.
- [Par02] R. Parikh. Social software. *Synthese*, 132:187–211, 2002. Cited on page 55.
- [Par03] R. Parikh. Levels of knowledge, games, and group action. *Research in Economics*, 57(3):267–281, September 2003. Cited on pages 84 and 85.
- [Pau97] L. C. Paulson. Proving properties of security protocols by induction. In *Proceedings of CSFW '97*, pages 70–83. IEEE Computer Society Press, 1997. Cited on page 144.
- [Pau98] L. C. Paulson. The inductive approach to verifying cryptographic protocols. *Journal of Computer Security*, 6:85–128, 1998. Cited on page 144.
- [Pel87] D. Peleg. Concurrent dynamic logic. *Journal of the ACM*, 34(2):450–479, 1987. Cited on page 60.
- [Pel93] D. Peled. All from one, one for all: on model checking using representatives. In *Proceedings of CAV '93*, pages 409–423, London, UK, 1993. Springer-Verlag. Cited on page 6.
- [PK92] R. Parikh and P. Krasucki. Levels of knowledge in distributed systems. *Sadhana*, 17(1):167–191, March 1992. Cited on pages 84 and 85.
- [Pla89] J. A. Plaza. Logics of public communications. In M. L. Emrich, M. S. Pfeifer, M. Hadzikadic, and Z. W. Ras, editors, *Proceedings of the 4th International Symposium on Methodologies for Intelligent Systems*, pages 201–216, 1989. Cited on pages 3, 15, 17, and 105.
- [PP07] S. Petride and R. Pucella. Perfect cryptography, s5 knowledge, and algorithmic knowledge. In *Proceedings of TARK '07*, pages 239–247, New York, NY, USA, 2007. ACM. Cited on page 151.

- [PR85] R. Parikh and R. Ramanujam. Distributed processes and the logic of knowledge. In *Proceedings of Conference on Logic of Programs*, pages 256–268, London, UK, 1985. Springer-Verlag. Cited on pages 3 and 15.
- [PR03] R. Parikh and R. Ramanujam. A knowledge based semantics of messages. *Journal of Logic, Language and Information*, 12(4), 2003. Cited on pages 3, 21, 37, 38, and 39.
- [Pra76] V. R. Pratt. Semantical considerations on floyd-hoare logic. Technical report, Cambridge, MA, USA, 1976. Cited on page 13.
- [Pra79] V. R. Pratt. Process logic. In *Proceedings of POPL '79*, pages 93–100, New York, NY, USA, 1979. ACM. Cited on page 39.
- [Pra80] V. R. Pratt. A near-optimal method for reasoning about action. *Journal of Computer and System Sciences*, 20(2):231–254, 1980. Cited on page 5.
- [PRS09] S. Paul, R. Ramanujam, and S. Simon. Stability under strategy switching. In Klaus Ambos-Spies, Benedikt Löwe, and Wolfgang Merkle, editors, *Mathematical Theory and Computational Practice*, volume 5635, chapter 40, pages 389–398. Springer Berlin Heidelberg, Berlin, Heidelberg, 2009. Cited on page 39.
- [PS10] E. Pacuit and S. Simon. Reasoning with protocols under imperfect information. 2010. Extended abstract presented at Advances in Modal Logic 10. Cited on page 38.
- [Puc06] R. Pucella. Deductive algorithmic knowledge. *Journal of Logic and Computation*, 16(2):287–309, April 2006. Cited on page 143.
- [RR98] M. K. Reiter and A. D. Rubin. Crowds: Anonymity for web transactions. *ACM Transactions on Information and System Security*, 1:66–92, 1998. Cited on page 144.
- [RS01] P. Ryan and S. Schneider. *Modelling and analysis of security protocols*. Addison Wesley, 2001. Cited on pages 139 and 141.
- [RS05a] R. Ramanujam and S. P. Suresh. Decidability of context-explicit security protocols. *Journal of Computer Security*, 13(1):135–165, 2005. Cited on page 157.
- [RS05b] R. Ramanujam and S. P. Suresh. Deciding knowledge properties of security protocols. In *Proceedings of TARK '05*, pages 219–235. Morgan Kaufmann, 2005. Cited on pages 141, 145, 146, and 147.
- [San91] Beverly Sanders. A predicate transformer approach to knowledge and knowledge-based protocols (extended abstract). In *Proceedings of PODC '91*, pages 217–230, New York, NY, USA, 1991. ACM. Cited on page 3.
- [SE89] R. S. Streett and A. E. Emerson. An automata theoretic decision procedure for the propositional mu-calculus. *Information and Computation*, 81(3):249–264, June 1989. Cited on page 5.
- [Seg82] K. Segerberg. A completeness theorem in the modal logic of programs. In T. Traczyk, editor, *Universal Algebra*, volume 9, pages 31–46. Banach Centre Publications, 1982. Cited on page 14.

- [SG02] N. V. Shilov and N. O. Garanina. Model checking knowledge and fixpoints. In Zoltán Ésik, Anna Ingólfssdóttir, Zoltán Ésik, and Anna Ingólfssdóttir, editors, *Proceedings of FICS '02*, volume NS-02-2 of *BRICS Notes Series*, pages 25–39. University of Aarhus, 2002. Cited on pages **104**, **148**, and **157**.
- [SG04] A. P. Sistla and P. Godefroid. Symmetry and reduced symmetry in model checking. *ACM Transactions on Programming Languages and Systems*, 26(4):702–734, 2004. Cited on page **6**.
- [SG08] S. Shoham and O. Grumberg. 3-valued abstraction: More precision at less cost. *Information and Computation*, 206(11):1313–1333, November 2008. Cited on page **6**.
- [Shm04] V. Shmatikov. Probabilistic model checking of an anonymity system. *Journal of Computer Security*, 12(3/4):355–377, 2004. Cited on page **144**.
- [SS99] P. F. Syverson and S. G. Stubblebine. Group principals and the formalization of anonymity. In *Proceedings of World Congress on Formal Methods '09*, volume 1708 of *LNCS*, pages 814–833. Springer, 1999. Cited on pages **142** and **144**.
- [Su04] K. Su. Model checking temporal logics of knowledge in distributed systems. In Deborah L. McGuinness, George Ferguson, Deborah L. McGuinness, and George Ferguson, editors, *Proceedings of AAI '04*, pages 98–103. AAAI Press / The MIT Press, 2004. Cited on page **149**.
- [Syv92] P. F. Syverson. Knowledge, belief, and semantics in the analysis of cryptographic protocols. *Journal of Computer Security*, 1(3-4):317–334, 1992. Cited on page **143**.
- [TDW08] M. T. Dashti and Y. Wang. Risk balance in exchange protocols. In *Proceedings of ASIAN '07*, pages 70–77, 2008. Cited on page **8**.
- [Tee06] W. Teepe. BAN logic is not ‘sound’, constructing epistemic logics for security is difficult. In Rineke, editor, *Proceedings of FEMAS'06*, pages 79–91, 2006. Cited on page **143**.
- [vB98] J. van Benthem. Dynamic odds and ends. Technical report, ILLC, 1998. Cited on page **83**.
- [vB09] J. van Benthem. The great art of modeling. Technical report, ILLC, 2009. Cited on pages **5** and **59**.
- [vBGHP09] J. van Benthem, J. Gerbrandy, T. Hoshi, and E Pacuit. Merging frameworks for interaction. *Journal of Philosophical Logic*, 38(5):491–526, October 2009. Cited on pages **3**, **21**, **37**, **39**, **152**, and **154**.
- [vBI08] J. van Benthem and D. Ikegami. Modal fixed-point logic and changing models. In *Pillars of Computer Science*, pages 146–165, 2008. Cited on page **84**.
- [vBL07] J. van Benthem and F. Liu. Dynamic logic of preference upgrade. *Journal of Applied Non-Classical Logics*, 17(2):157–182, 2007. Cited on page **56**.
- [vBvEK06] J. van Benthem, J. van Eijck, and B. Kooi. Logics of communication and change. *Information and Computation*, 204(11):1620–1662, November 2006. Cited on pages **15**, **17**, **34**, and **39**.

- [vBVQ09] J. van Benthem and F. Velázquez-Quesada. Inference, promotion, and the dynamics of awareness. Technical report, ILLC, Amsterdam, 2009. Cited on page **81**.
- [vD02] H. van Ditmarsch. Descriptions of game actions. *Journal of Logic Language and Information*, 11(3):349–365, 2002. Cited on pages **5**, **22**, and **84**.
- [vD03] H. van Ditmarsch. The Russian Cards Problem. *Studia Logica*, pages 31–62, October 2003. Cited on pages **3**, **4**, **5**, **22**, **26**, **31**, **149**, and **155**.
- [vD08] H. van Ditmarsch. Unconditionally secure protocols with card deals, September 2008. Presented at the Lorentz Center workshop Logic and Information Security, available at <http://www.cs.otago.ac.nz/staffpriv/hans/lorentz/niaslorentz.pdf>. Cited on pages **3** and **155**.
- [vDF09] H. van Ditmarsch and T. French. Simulation and information: Quantifying over epistemic events. In J.-Jules C. Meyer and J. Broersen, editors, *Proceedings of KR '09*, volume 5605, pages 51–65, Berlin, Heidelberg, 2009. Springer Berlin Heidelberg. Cited on pages **64**, **80**, and **81**.
- [vdHW02] W. van der Hoek and M. Wooldridge. Tractable multiagent planning for epistemic goals. In *Proceedings of AAMAS '02*, pages 1167–1174, New York, NY, USA, 2002. ACM. Cited on page **157**.
- [vDK06] H. van Ditmarsch and B. Kooi. The secret of my success. *Synthese*, 153(2):339, November 2006. Cited on page **28**.
- [vDK08] H. van Ditmarsch and B. Kooi. Semantic results for ontic and epistemic change. In G. Bonanno, W. van der Hoek, and M. Wooldridge, editors, *Proceedings of LOFT 7*, pages 87–117, October 2008. Cited on page **34**.
- [vdMS99] R. van der Meyden and N. Shilov. Model checking knowledge and time in systems with perfect recall. In *Proceedings of FSTTCS*, pages 432–445, 1999. Cited on pages **104** and **157**.
- [vdMS04] R. van der Meyden and K. Su. Symbolic model checking the knowledge of the dining cryptographers. In *Proceedings of CSFW 2004*, pages 280–291. IEEE, 2004. Cited on pages **104**, **146**, and **149**.
- [vdMW07] R. van der Meyden and T. Wilke. Preservation of epistemic properties in security protocol implementations. In *Proceedings of TARK '07*, pages 212–221, 2007. Cited on page **143**.
- [vdPE04] J. van de Pol and M. V. Espada. Modal abstractions in  $\mu$ -CRL. In *Proceedings of AMAST '04*, pages 61–64, 2004. Cited on pages **104** and **109**.
- [vDRV05] H. van Ditmarsch, J. Ruan, and L. C. Verbrugge. Model checking sum and product. In Shichao Zhang and R. Jarvis, editors, *Proceedings of AI 2005*, volume 3809 of LNCS, pages 790–795, 2005. Cited on page **5**.
- [vDvdHK03a] H. van Ditmarsch, W. van der Hoek, and B. Kooi. *Descriptions of game states*, volume 161 of *CSLI Lecture Notes*. CSLI Publications, 2003. Cited on pages **5** and **84**.
- [vDvdHK03b] H. van Ditmarsch, W. van der Hoek, B. Kooi, and 105–143. Concurrent dynamic epistemic logic. In V. F. Hendricks, K. F. Jørgensen, and S. A. Pedersen, editors, *Knowledge Contributors*, Synthese Library Series, pages 105–143. Kluwer Academic Publishers, 2003. Cited on page **60**.

- [vDvdHK03c] H. P. van Ditmarsch, W. van der Hoek, and B. P. Kooi. Concurrent dynamic epistemic logic for mas. In *Proceedings of AAMAS '03*, pages 201–208, New York, NY, USA, 2003. ACM. Cited on pages 22 and 60.
- [vDvdHK07] H. van Ditmarsch, W. van der Hoek, and B. Kooi. *Dynamic Epistemic Logic*. (Synthese Library). Springer, 1st edition, November 2007. Cited on pages 3, 4, 21, 22, 23, 60, and 105.
- [vDvdHvdMR06] H. van Ditmarsch, W. van der Hoek, R. van der Meyden, and J. Ruan. Model checking Russian cards. *Electronic Notes Theoretical Computer Science*, 149(2):105–123, 2006. Cited on pages 22 and 149.
- [vE07] J. van Eijck. DEMO — a demo of epistemic modelling. In J. Benthem, Dov Gabbay, and Benedikt Löwe, editors, *Interactive Logic – Proceedings of the 7th Augustus de Morgan Workshop*, number 1 in Texts in Logic and Games. Amsterdam University Press, 2007. Available at <http://www.cwi.nl/~jve/demo/>. Cited on pages 5, 59, and 149.
- [vEW08] J. van Eijck and Y. Wang. Propositional dynamic logic as a logic of belief revision. In *Proceedings of WOLLIC '08*, pages 136–148, 2008. Cited on page 8.
- [vEWS10] J. van Eijck, Y. Wang, and F. Sietsma. Composing models. In *Proceedings of LOFT '10*, 2010. Cited on pages 8 and 80.
- [VO07] J. Vaneijck and S. Orzan. Epistemic verification of anonymity. *Electronic Notes in Theoretical Computer Science*, 168:159–174, February 2007. Cited on pages 3 and 148.
- [VW51] G. H. Von Wright. *An Essay in Modal Logic*. North Holland, Amsterdam, 1951. Cited on page 143.
- [Wal00] I. Walukiewicz. Completeness of kozen’s axiomatisation of the propositional -calculus. *Information and Computation*, 157(1-2):142–182, February 2000. Cited on page 84.
- [Wan06] Y. Wang. Indexed semantics and its application in modelling interactive unawareness. Master’s thesis, University of Amsterdam, 2006. Cited on pages 39 and 40.
- [WKvE09] Y. Wang, L. Kuppusamy, and J. van Eijck. Verifying epistemic protocols under common knowledge. In *Proceedings of TARK '09*, pages 257–266, New York, NY, USA, 2009. ACM. Cited on pages 8, 34, and 39.
- [WSvE10] Y. Wang, F. Sietsma, and J. van Eijck. Logic of information flow on communication channels (extended abstract). In van der Hoek, Kaminka, Lespérance, Luck, and Sen, editors, *Proceedings of AAMAS '10*, 2010. Cited on pages 8, 55, and 154.