Stage de MIM 1

Logique épistémique en COQ

Lieu du stage: LIP, ENS de Lyon
Maitre de stage: Pierre LESCANNE

Contexte du stage: Il se déroule dans l'équipe PLUME du laboratoire LIP de l'ENS de Lyon. Le stagiaire participera au développement de la logique épistémique dans un assistant de preuve ; l'objectif à terme est de l'appliquer à la sécurité des systèmes informatiques.

Sujet du stage: La logique épistémique est aussi appelée logique de la connaissance, c'est la logique qui gère les concepts fondamentaux comme «je sais que», «je sais qu'il sait que», «je crois que» etc. Ses applications sont multiples, notamment à l'intelligence artificielle, aux systèmes d'information (systèmes à base de connaissance), aux systèmes distribués et multi-agents, aux protocoles cryptographiques etc. C'est cette dernière application à la sécurité qui nous intéresse le plus. La logique de la connaissance sert en particulier dans l'authentification où il faut savoir avec à certitude avec qui l'on est en train d'effectuer une transaction.

J'ai développé des modules de preuves automatisées en COQ avec lesquels j'ai déjà moi-même traité des problèmes expérimentaux, mais je souhaiterais qu'un collaborateur mette au point dans ce cadre de nouveaux exemples: parmi ceux-ci, un problème d'école, celui du «jeu des as et huit» et un problème de sécurité celui de la correction du protocole d'authentification de Needham-Schroeder.

Connaissances requises : Les connaissances requises sont celles enseignées dans le module de logique du MIM complétées par la lecture des chapitres qui nous concernent des livres cités dans la bibliographie.

Références

[1] Bruno Barras, Samuel Boutin, Cristina Cornes, Judicaël Courant, Yann Coscoy, David Delahaye, Daniel de Rauglaudre, Jean-Christophe Filliâtre, Eduardo Giménez, Hugo Herbelin, Gérard Huet, Henri Laulhère, César Muñoz, Chetan Murthy, Catherine Parent-Vigouroux, Patrick Loiseleur, Christine Paulin-Mohring, Amokrane Saïbi, and Benjamin Werner. *The* COQ *Proof Assistant Reference Manual.* INRIA, version 6.3.11 edition, May 2000.

[2] Ronald Fagin, Joseph Y. Halpern, Yoram Moses, and Moshe Y. Vardi. *Reasoning about Knowledge.* The MIT Press, 1995.

[3] Pierre Lescanne. Epistemic Logic in Higher Order Logic, an experiment with COQ. note, February 2001.

[4] John-Jules Ch. Meyer and Wiebe van der Hoek. *Epistemic Logic for Computer Science and Artificial Intelligence*, volume 41 of *Cambridge Tracts in Theoretical Computer Science.* Cambridge University Press, 1995.