

Véronique Cortier

23, avenue du Général Leclerc
75014 Paris, France
tél. : +(33) 1 43 21 38 49
e-mail : *cortier@lsv.ens-cachan.fr*

born the 31th march 1978
French nationality

Research Subject

Cryptographic protocols describe a sequence of messages exchange. They may have several goals like secrecy of a data, authentication, anonymity... But even if we assume perfect encryption (an intruder may open a message only if he has the corresponding key), then there is no algorithm in general to decide if a protocol preserves secrecy.

I study decidable classes of protocols for secrecy, with possibly some equationnal theories in order to model the algebraic properties of the cryptographic primitives like xor or exponential. I have also developed some proof methods for secrecy (in J. Millen and H. Rueß model and in the spi-calculus model) and one of them has been implemented.

Studies

2000-2002 : PhD thesis in Computer Science at **École Normale Supérieure de Cachan**, defended on Thursday, March 20th 2003. Subject : **Automated verification of cryptographic protocols**. PhD Advisor : Hubert Comon-Lundh.

1997-2001 : Student at **ENS Cachan**.

Agrégation de mathématiques, option calcul scientifique. Rank : **52th**.

Master of Mathematics and Computer Science at ENS Cachan and University Paris 7, **major of the master**.

Foreign Experiences

May-June 2001 Fellowship (7 weeks) at Stanford University, California, in John Mitchell's team. This work has been published in [5].

November 2000 Fellowship (5 weeks) at **SRI Computer Science Laboratory**, California. Supervised by Jon Millen. Work on PVS proofs for cryptographic protocols. This work has been published in [6].

July 1998 Research initiation at **Max-Planck Institut Laboratory** in H. Ganziger's team. This work has been published in [8].

Publications

Journals

- [1] V. Cortier. *About the decision of reachability for register machines*. Theoretical Informatics and Applications (**ITA**), 2003. To appear.
- [2] H. Comon-Lundh and V. Cortier. *Tree automata with one memory, set constraints and cryptographic protocols*. Theoretical Computer Science (**TCS**), 2003. To appear.

Conferences

- [3] H. Comon-Lundh and V. Cortier. *New decidability results for fragments of first-order logic and application to cryptographic protocols*. Accepted to Rewriting Techniques and Applications, LNCS, to appear.
- [4] H. Comon-Lundh and V. Cortier. *Security properties : two agents are sufficient*. In Proc. European Symposium On Programming (**ESOP'03**), April 2003. To appear.
- [5] H. Comon, V. Cortier and J. Mitchell. *Tree automata with one memory, set constraints and ping-pong protocols*. In Proc. 28th Int. Coll. Automata, Languages, and Programming (**ICALP'01**), Crete, Greece, July 2001. Springer, 2001.
- [6] V. Cortier, J. Millen and Harald Rueß. *Proving Secrecy is easy enough*. In Proc. 14th IEEE Computer Security Foundations Workshop (**CSFW'01**), pages 97-108, 2001.
- [7] H. Comon and V. Cortier. *Flatness is not a weakness*. In Proc. 14th Int. Workshop Computer Science Logic (**CSL'2000**), Fischbachau, Germany, Aug. 2000. Volume 1862 of Lecture Notes in Computer Science, pp. 262-276. Springer, 2000.
- [8] V. Cortier, H. Ganzinger, F. Jacquemard, and M. Veanes. *Decidable fragments of simultaneous rigid reachability*. In Proc. 26th Int. Coll. Automata, Languages, and Programming (**ICALP'99**), Prague, Czech Republic, July 1999. Volume 1644 of Lecture Notes in Computer Science, pages 250-260. Springer, 1999.

Tool

Securify : verification tool for cryptographic protocols. May be used on the following web page : <http://www.lsv.ens-cachan.fr/~cortier/EVA/eva-comp.php#table>

Teaching

Assistant for the course *Calculability and Complexity* for undergraduate students at ENS Cachan.

Assistant for C++ course for undergraduate students at ENS Cachan.