

PhD Subject in Computer Science: Formal Verification of E-voting Protocols

Verimag*

October 23, 2007

Supervisor: P. Lafourcade¹
Contact: Pascal.Lafourcade@imag.fr
Also a master degree subject

1 Context

In the last few years, formal analysis of cryptographic protocols has become classical. Many formal methods exist or are still being designed for automatic verification of security properties such as secrecy or authentication [11, 3, 1, 12, 4, 2], aiming in the end at proving concrete protocols actually are secure. Here, we focus our analysis more specifically on voting protocols [9, 6]. In such protocols, a kind of secrecy and authentication is required to guarantee the secret of one vote and authentication of the voter. But some more complex properties have to be achieved by voting protocols like for instance the property that nobody, except the voter himself, can link one vote to his voter. One usual method developed in voting protocols is to use a homomorphic encryption (see [5] for a survey). A homomorphic encryption scheme has the following property:

$$\prod \{v_i\}_k = \{\sum v_i\}_k$$

The product of encrypted messages with the same key is equal to the encryption of the sum of the messages.

2 Goals

The first goal of this work is to list existing e-voting protocols using homomorphic encryption from the state of the art. From this list, the student should understand which properties are consequences of this homomorphic property.

The second phase of this study is to perform an automatic formal analysis for homomorphic encryptions. We strongly expect that existing methods based on constraints and resolution of equations systems can be extended to analyze this specific property [8].

*<http://www-verimag.imag.fr>

¹<http://www-verimag.imag.fr/~plafourc>

The last phase of this work consists in proposing a first draft of formal definition of these properties for voting protocols. Some recent results have been obtained in this direction [10, 7], but many properties have not been formally analyzed yet.

3 Bibliography

References

- [1] R. Amadio, D. Lugiez, and V. Vanackère. On the symbolic reduction of processes with cryptographic functions. *Theoretical Computer Science*, 290(1):695–740, 2002.
- [2] David Basin, Sebastian Mödersheim, and Luca Viganò. OFMC: A symbolic model checker for security protocols. *International Journal of Information Security*, 4(3):181–208, June 2005. Published online December 2004.
- [3] B. Blanchet and A. Podelski. Verification of cryptographic protocols: Tagging enforces termination. In *Proc. 6th International Conference on Foundations of Software Science and Computation Structures (FOSSACS'03)*, volume 2620 of *Lecture Notes in Computer Science*, pages 136–152, Warsaw, Poland, 2003. Springer-Verlag.
- [4] Liana Bozga, Yassine Lakhnech, and Michael Perin. HERMES: An Automatic Tool for Verification of Secrecy in Security Protocols. In *Computer Aided Verification*, 2003.
- [5] Véronique Cortier, Stéphanie Delaune, and Pascal Lafourcade. A survey of algebraic properties used in cryptographic protocols. *Journal of Computer Security*, 14(1):1–43, 2006.
- [6] R. Cramer, M. K. Franklin, B. Schoenmakers, and M. Yung. Multi-authority secret-ballot elections with linear work. In *Proc. International Conference on the Theory and Application of Cryptographic Techniques (EUROCRYPT'96)*, volume 1070 of *Lecture Notes in Computer Science*, pages 72–83, Zaragoza, Spain, 1996. Springer-Verlag.
- [7] Stéphanie Delaune, Steve Kremer, and Mark D. Ryan. Coercion-resistance and receipt-freeness in electronic voting. In *Proceedings of the 19th IEEE Computer Security Foundations Workshop (CSFW'06)*, pages 28–39, Venice, Italy, July 2006. IEEE Computer Society Press.
- [8] Stéphanie Delaune, Pascal Lafourcade, Denis Lugiez, and Ralf Treinen. Symbolic protocol analysis in presence of a homomorphism operator and *exclusive or*. In *Proceedings of the 33rd International Colloquium on Automata, Languages and Programming (ICALP'06)*, Lecture Notes in Computer Science, pages 132–143, Venice, Italy, jul 2006. Springer.
- [9] Martin Hirt and Kazue Sako. Efficient receipt-free voting based on homomorphic encryption. In *EUROCRYPT*, pages 539–556, 2000.

- [10] Steve Kremer and Mark D. Ryan. Analysis of an electronic voting protocol in the applied pi-calculus. In Mooly Sagiv, editor, *Programming Languages and Systems — Proceedings of the 14th European Symposium on Programming (ESOP'05)*, volume 3444 of *Lecture Notes in Computer Science*, pages 186–200, Edinburgh, U.K., April 2005. Springer.
- [11] M. Rusinowitch and M. Turuani. Protocol insecurity with finite number of sessions is NP-complete. In *Proc. 14th Computer Security Foundations Workshop (CSFW'01)*, pages 174–190, Cape Breton, Canada, 2001. IEEE Comp. Soc. Press.
- [12] Mathieu Turuani. The cl-atse protocol analyser. In *Proceedings of the 17th International Conference on Rewriting Techniques and Applications (RTA'06)*, Lecture Notes in Computer Science, Seattle, USA, August 2006. Springer-Verlag. To appear.