

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

Verimag\*

October 23, 2007

**Supervisor:** P. Lafourcade<sup>1</sup>  
**Contact:** Pascal.Lafourcade@imag.fr  
**Also a master degree subject**

## 1 Context

Nowadays, providing electronic facilities has become quite essential for companies, for they reduce considerably the cost of services and ease communication between clients and suppliers. A high stress is put on the development of well-available, mobile information services called "e-everything", like e-government, e-money, e-banking and e-auctions. There are many electronic services in the e-commerce, one of them is electronic auctions. For instance the auction websites, such as eBay, are so popular that their number of users is skyrocketting. For a few years, various e-auction protocols have been designed [7, 5, 6, 12]. Auction schemes can be divided into four groups:

- English auction schemes [5], of which eBay is an instance, are the most widespread. During the auction, the users bid the price for a given good. The prices increase till the end of the auction. Hence the winner is the bidder who proposed the highest price.
- Another way of proceeding is to follow a 1st Price Sealed-Bid auction scheme [6, 7]. In this case, the users independently define the price for a given good. The price a bidder defines cannot be changed, it is given once and for all. The user who declares the highest price wins the good and has to pay the announced price.
- The Vickrey auction [11], alternatively called 2nd Price Sealed-Bid, is very similar to the previous scheme. The winner is also the bidder that has declared the highest price, but this time he only has to pay the second highest price announced.
- The Dutch auction [12] starts with the highest possible price and the bidders decrease the price until one bidder decides to pay the current value. The winning bidder pays the price on which the auction is stopped.

---

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

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

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 properties like secrecy or authentication [9, 3, 1, 10, 4, 2]. This area of research is very active and it aims at eventually prove security of concrete protocols used in modern communications.

Unfortunately, protocol conceivers and verification tool designers do not really communicate, and recently in [8], we have found and corrected a flaw on an existing e-auction protocol using OFMC [2] automatic tool dedicated to formal analysis of cryptographic protocols.

## 2 Goals

The first goal of this work is to classify existing e-auction protocols from the state of the art according to the kind of encryption schemes they use and the security properties they achieve. Afterwards, we will be able to find common properties that e-auction protocols have to satisfy. These properties seem to be close to properties of e-voting protocols and at the same time quite different. A comparison between these two fields will help us to obtain a better understanding of properties that e-auctions protocols need to achieve.

The second phase of this work consists in proposing a first draft of formal definitions of these properties. In the end, a more ambitious goal would be to try and analyze some actual e-auction protocols with respect to some chosen important properties, probably adapting and extending existing techniques.

## 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] Esther David, Rina Azoulay-Schwartz, and Sarit Kraus. Tan english auction protocol for multi-attribute items. In *Workshop on Agent Mediated*

*Electronic Commerce on Agent-Mediated Electronic Commerce IV, Designing Mechanisms and Systems*, volume 2531 of *lncs*, pages 52–68. Springer-Verlag, 2002.

- [6] A. Juels and M. Szydło. A two-server, sealed - poverties auction protocol. In *roceedings of the 6th Annual Conference Financial Cryptography (FC)*, volume 2357 of *lncs*, pages 72–86. Springer-Verlag, 2002.
- [7] B. Księżopolski and Z. Kotulski. Cryptographic protocol for electronic auctions with extended requirements. *Annales UMCS Informatica*, 2:391–400, 2004.
- [8] Bogdan Księżopolski and Pascal Lafourcade. Attack and revision of an electronic auction protocol using OFMC. Technical Report 549, Department of Computer Science, ETH Zurich, Switzerland, February 2007. 13 pages.
- [9] 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.
- [10] 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.
- [11] W. Vickrey. Counter speculation, auctions, and competitive sealed tenders. *Journal of Finance*, 16(1):8–37, 1961.
- [12] E. Wolfstetter. Auctions: An introduction. *Journal of Economic Surveys*, pages 367–420, 1996.