This thesis sets as goal the study and development of cryptographic multi-party protocols offering the properties of verifiability and privacy. The verifiability property guarantees the protocols participants and/or observers that the result of the execution of the protocol is exactly what is expected from a honest execution of the protocol. On the other hand, the privacy property ensures the participants that their private information is not leaked by executing the protocol. The thesis targets real-world applications as well as any multi-party function.

The first part of the work focus on cryptographic voting systems. In this case, the function to evaluate is rather simple – e.g. a sum of yes/no votes – and, we show how we conciliate the verifiability with the privacy to obtain a cryptographic voting system that offers a perfectly private audit trail of its execution. A perfectly private audit trail means that it contains no information about the voters' votes whatsoever. In addition, the trail computationally guarantees the observers that the tally of the votes is correct.

Next, we extend our study to encompass more complex functions. We work on combinatorial problems such as graph problems. In this part, following the traditional approach of secure multi-party computation, we investigate potential sources of privacy leakages that appear when turning the unsecured version of an algorithm into its secure version.

In the last part of the thesis, we follow a different approach where we rely on a third party (worker) entrusted with the privacy of the protocol participants' inputs. We show that several important gains can be made in this setting. Our solution is generic and non-interactive. It also offers the worker the possibility to use his own algorithms.

Membres du jury :

Prof. Olivier Pereira (UCL), promoteur
Prof. David Bol (UCL), président
Prof. François-Xavier Standaert (UCL), secrétaire
Prof. Gildas Avoine (UCL)
Dr. Steve Kremer (Inria Nancy -Grand Est & LORIA, France)
Prof. Olivier Markowitch (ULB)