PhD Thesis proposal
Formal verification of e-voting protocols in a post quantum world

Véronique Cortier
veronique.cortier@inria.fr
members.loria.fr/VCortier/

Charlie Jacomme
charlie.jacomme@inria.fr
charlie.jacomme.fr

City and country Nancy, France.

Research team Team PESTO at LORIA lab (Inria Nancy, CNRS and Université de Lorraine).

Thesis subject In recent years, e-voting protocols are used more and more in sensitive contexts, such as unions and political parties elections, and even state level elections in some countries. Given those high-risk situations, we must endeavour to provide guarantees as strong as possible on the underlying cryptographic protocols. One way to do this is to rely on mechanized provers to carry out the security proofs, where a computer tells us that the proof is indeed correct. However, such high assurance proofs remain scarce in the context of e-voting. We believe that the Squirrel Prover [1] (`squirrel-prover.github.io`), a mechanized prover we are co-developing, bears the promise of enabling such proofs at a larger scale. This thesis will thus focus on using the Squirrel prover to develop proofs of increasingly complex e-voting protocols.

As such proofs for e-voting protocols have never been done in Squirrel, the thesis may include the development of novel extensions to its underlying logic or the tool itself.

Finally, with the threat of quantum computers breaking the classical cryptography in the current decades, this thesis would strive to verify the so-called ever lasting privacy for ballots. We note that Squirrel already gives us guarantees against quantum attackers and is thus suited for this specific use case.

Working environment The thesis will take place in the Pesto team at LORIA. The team has a strong experience in e-voting, having studied numerous systems in France or abroad (Geneva's canton system, Scytl), as well as worked on theoretical aspects (choosing/designing the right security definitions, uncovering leaks). More generally, the pesto Team focuses on developing formal methods for proving the security of protocols, and has participated in the development of many tools for this, such as ProVerif, Tamarin, Jasmin, DeepSec, Sapic+, and of course, the Squirrel Prover.

Expected ability The student should either have a strong background in theoretical computer science (notably familiarity with logic) or provable cryptography. Some experience in using a mechanized prover (Rocq, Isabelle, . . .) is a bonus.

References

[1] David Baelde, Stéphanie Delaune, Charlie Jacomme, Adrien Koutsos, and Solène Moreau. An Interactive Prover for Protocol Verification in the Computational Model. In *2021 IEEE Symposium on Security and Privacy (SP)*, pages 537–554, May 2021. ISSN: 2375-1207.