Verification of security protocols
– application to e-voting –

Laboratory, institution and university. Univ Rennes, CNRS, IRISA, France. The internship will be located at IRISA, Rennes.

Team or project of the Lab. EMSEC team at IRISA.

Name and email address of the advisor.
Stéphanie Delaune, `stephanie.delaune@irisa.fr`, and Joseph Lallemand, `joseph.lallemand@inf.ethz.ch`

Indemnisation. The internship is supported by the European grant POPSTAR (ERC Starting Grant) and the ANR grant TECAP.

Context. Security protocols are distributed programs that aim at securing all kinds of communications, by using cryptography to ensure security properties, such as confidentiality, authentication or anonymity. Such protocols are widely deployed, *e.g.* for electronic commerce on the Internet, in banking networks, mobile phones and more recently online elections (e-voting systems). As the goal is to provide security guarantees even when communicating over an untrusted network – typically the Internet – it turns out that these protocols are extremely difficult to get right. Formal methods have proved to be a very useful tool to detect errors, and verify the correctness of security protocols. Traditionally two approaches have been used: the *computational* one, which captures strong notions of security and offers guarantees against all probabilistic polynomial-time attackers, and the *symbolic* one in which things are modelled more abstractly and which is more amenable to automation.

Different properties have been proposed to characterise the security guarantees an electronic voting protocol should provide. We consider here *vote privacy*. This property can informally be described as the guarantee that votes remain secret – no one should know who I voted for. Several definitions formalising this idea have already been proposed, both in the computational model and in the symbolic one. Vote privacy is typically formalised as an *indistinguishability property* between two scenarios, *e.g.* one where Alice votes for v_0 whereas Bob votes for v_1, and one where their votes

are exchanged (Alice votes for v_1 and Bob for v_0) – the intuition being that an attacker can learn that the votes are $\{v_0, v_1\}$ as a set, but must not be able to determine who voted for which candidate. Other formalisations, expressing different flavours of vote privacy, have been proposed in the literature. These definitions may notably consider different trust assumptions regarding the authorities (ballot box, talliers, *etc.*).

Regarding verification, even though indistinguishability properties have received a lot of attention, they are still difficult to check for several reasons. In particular, voting systems need to be secure for any arbitrary number of malicious voters. However, existing tools (*e.g.* ProVerif, Tamarin) allowing one to consider arbitrarily many sessions have some limitations that can make them difficult to use to analyse vote privacy. One way to tackle this problem is to develop a reduction result allowing one to get rid of this source of unboundedness. The idea is to identify a class of protocols for which only a small number of voters needs to be considered, essentially proving that, if there exists an attack against vote privacy with some arbitrary number of voters, then it can be adapted to already break vote privacy with a small – fixed – number of voters. It is then sufficient to verify the protocol with this fixed number of voters. Such a reduction result has been developed in [ACK16] for a specific definition of vote-privacy based on swapping, similar to the one sketched above, and several case studies have been performed relying on existing verification tools.

Objectives of the internship. Recently, a new notion of vote privacy has been proposed [BCG+15] with the aim to avoid several shortcomings of the other existing definitions. This definition, called BPRIV (short for *ballot privacy*), has then been extended to consider the case of a malicious ballot box [CLW20], *i.e.* an attacker who is able to modify or remove ballots before they are tallied. All these definitions have originally been proposed in the computational model. Having symbolic counterparts to these computational properties would allow us to use automated tools to analyse them, making verification of voting systems easier. Some first attempts at symbolic versions have been sketched in [Rakar].

The goal of this internship will be to propose general symbolic counterparts of these definitions, and then, getting some inspiration from the reduction result established in [ACK16] to design conditions under which a similar result can be proved regarding this BPRIV definition.

Expected skills. We are looking for candidates with good skills in Foundations of Computer Science (logic, automated deduction, concurrency theory...). Some knowledge in security is an asset but is not mandatory. The candidate will assimilate this knowledge during the internship.

This internship may also lead to a PhD thesis on similar topics.

References

[ACK16] Myrto Arapinis, Véronique Cortier, and Steve Kremer. When are three voters enough for privacy properties? In *Proceedings of the 21st European Symposium on Research in Computer Security (ESORICS'16)*, LNCS. Springer, September 2016.

[BCG+15] David Bernhard, Veronique Cortier, David Galindo, Olivier Pereira, and Bogdan Warinschi. A comprehensive analysis of game-based ballot privacy definitions. In *Proceedings of the 36th IEEE Symposium on Security and Privacy (S&P'15)*, San Jose, CA, USA, May 2015. IEEE Computer Society Press.

[CLW20] Véronique Cortier, Joseph Lallemand, and Bogdan Warinschi. Fifty shades of ballot privacy: Privacy against a malicious board. In *33rd IEEE Computer Security Foundations Symposium (CSF'20)*, Boston, USA, June 2020.

[Rakar] Itsaka Rakotonirina. *Efficient verification of observational equivalences of cryptographic processes: theory and practice*. PhD thesis, Université de Lorraine, To appear.