Context. We develop two protocol verification tools:

- ProVerif ([http://proverif.inria.fr](http://proverif.inria.fr)) is an automatic protocol verifier that works in the symbolic model of cryptography. It has been widely fairly widely used by research teams internationally. It was presented in course 2-30.

- CryptoVerif ([http://cryptoverif.inria.fr](http://cryptoverif.inria.fr)) is a protocol verifier that works in the computational model of cryptography. It aims to mechanize the game-based proofs, usually done manually by cryptographers.

The goal of the internship will be to verify protocols using these tools and possibly to develop them.

Planed work. Several protocols are interesting targets for formal verification:

- A web authentication protocol ([https://w3c.github.io/webauthn/](https://w3c.github.io/webauthn/)), designed to allow single sign-on on various web-sites via major providers such as Google or Microsoft, with multi-factor authentication (using for instance a mobile phone or a USB key). The verification of this protocol will be in collaboration with Harry Halpin, the founder of the working group that merged a previous version of the protocol, named FIDO, with W3C.

- An avionic protocol that is currently being standardized to secure communications between airplanes and ground entities. This work is done in collaboration with Airbus France.

- A blockchain-based key discovery protocol designed for a wide variety of use-cases. The work builds from existing protocols like SDSI and CONIKS ([https://coniks.cs.princeton.edu/](https://coniks.cs.princeton.edu/)), but without a single central server. The verification of this protocol will be in collaboration with George Danezis (University College London) and Harry Halpin.

- A privacy-enhanced version of an authorization protocol ([http://dl.acm.org/citation.cfm?id=2994637&CFID=867988395&CFTOKEN=37351901](http://dl.acm.org/citation.cfm?id=2994637&CFID=867988395&CFTOKEN=37351901)). This protocol is based on OAuth but improves its privacy via the usage of blind signatures. The verification of this protocol will be in collaboration with George Danezis (University College London) and Harry Halpin.
The goal of the internship will be to model and verify one of these protocols using ProVerif and/or CryptoVerif. It may also be an opportunity to develop these tools with new features needed for analyzing the considered protocol. The target protocol will be discussed with the candidate intern.

**Practical information.** The internship will take place at Inria Paris, 2 rue Simone Iff, 75012 Paris (near gare de Lyon). Students that are not already paid will be compensated (within the limits allowed by Inria).

This internship could be a starting point for a PhD on protocol verification within the Prosecco team.

Please contact me early as there is a fairly long hiring delay in our team.

For additional information, please contact Bruno.Blanchet@inria.fr.