Semantics of Cryptographic Proofs.

Bridging Parametric and Polynomial Security

David Baelde
ENS Rennes

Adrien Koutsos
Inria Paris

Guillaume Scerri
UVSQ

September 22, 2021

Location Ideally, the internship will take place at Inria Paris (close to Gare de Lyon), in the Prosecco team. If necessary, the internship could also take place at UVSQ in the PETRUS team, or at IRISA (Rennes) in the Spicy team.

Contact information:

- David Baelde: baelde@lsv.fr
- Adrien Koutsos: adrien.koutsos@inria.fr
- Guillaume Scerri: guillaume.scerri@uvsq.fr

Expected abilities of the student The student will need a strong background in logics and proof theory. While knowledge in security and cryptography is a plus, it is *not* required: the necessary background will be acquired by the student during the internship when needed.

General Presentation Security protocols are small concurrent programs that rely on cryptographic primitives to achieve various security and privacy goals, e.g. secrecy, authentication, or untraceability. To formally establish the security of a protocol P, cryptographers show that the probability that an attacker $\mathcal{A}$ breaks the protocol's security is negligible[1] in the length η of the keys, where the attacker is an arbitrary probabilistic polynomial-time Turing machine (PPTM).

$$\forall \mathcal{A} \text{ PPTM}, \quad \Pr(\mathcal{A} \text{ breaks } P) = \text{negl}(\eta)$$

This approach is usually referred to as the computational model, and several logics and tools have been proposed to mechanize such proofs, e.g., by game transformations in CryptoVerif [Bla06], or using a Hoare logic in Easycrypt [Bar+11].

More recently, Bana and Comon have proposed in [BC14] a new approach to prove the security of cryptographic protocol. It is a first-order logic for the indistinguishability of bitstring distributions, which allows to reduce the security of a protocol to the unsatisfiability

[1] Formally, a function $f(\eta)$ is negligible if $f(\eta)$ is asymptotically smaller, when $\eta \to +\infty$, than the inverse of any polynomial.

of a (recursive) set of first-order formulas. This approach is different from the ones provided by the above-mentioned tools in the computational model: it completely hides probabilities from the user, reasons directly on protocol traces, ... Very recently, this framework has been extended [Bae+21] and implemented in a proof assistant called Squirrel [Bae+20].

Goal of the internship There is a subtle gap between the security guarantees in the BC and computational model. It has been shown ([BC14; Bae+21]) that if a protocol P is secure in the BC framework, then, for any PPTM adversary $\mathcal{A}$, and for *any number of sessions* N, the execution of N sessions of the protocol P against $\mathcal{A}$ is secure:

$$\forall \mathcal{A} \text{ PPTM}, \forall N \in \mathbb{N}, \;\; \Pr\left(\mathcal{A} \text{ breaks } N \text{ sessions of } P\right) = \text{negl}(\eta)$$

In the computational model, one actually expects a stronger guarantee, where the attacker may interact with an arbitrary (polynomial) number of sessions of the protocol, but his probability of success is negligible regardless of this number of sessions:

$$\forall \mathcal{A} \text{ PPTM}, \;\; \Pr\left(\mathcal{A} \text{ breaks } P\right) = \text{negl}(\eta)$$

We call the former definition parametric security, and the latter one polynomial security. In polynomial security, the attacker can interact with the protocol using any (polynomial) number of sessions. Polynomial security captures attacks relying on a number of sessions that grows with η, but parametric security does not[2].

The intern will work on finding sufficient conditions for bridging this gap.

- Currently, the Bana-Comon approach relies on proof systems which are shown to be sound w.r.t. parametric semantics. In order to obtain polynomial security guarantees, a natural idea is to move to a more precise semantics: instead of showing that proof rules preserve negligibility, the intern will have to analyze for each rule how the probability of breaking the conclusion is bounded by an expression depending on the probabilities of breaking the premises. Combining this throughout the derivation, one will obtain from a proof a *first bound* on the probability of breaking a security property (concretely, it will be a formal expression depending on the unknown probability of breaking cryptographic assumptions).

- Unfortunately, we foresee that this bound will often not be good enough: it will often depend on the number of sessions, in a way that does not allow to conclude that the probability of an attack is negligible regardless of that number. To obtain a better bound, the intern will use *proof rewriting* techniques to transform a proof into a new

[2] To be more precise, we need to expand the definition of negligible: then the BC security notion (parametric security) is of the form

$$\forall N, \forall \mathcal{A}, \forall k \in \mathbb{N}, \exists \eta_0, \forall \eta > \eta_0, \;\; \Pr\left(\mathcal{A} \text{ breaks } N \text{ sessions of } P\right) < \eta^{-k}$$

but the expected (polynomial) security guarantee is

$$\forall \mathcal{A}, \forall k \in \mathbb{N}, \exists \eta_0, \forall \eta > \eta_0, \forall N, \;\; \Pr\left(\mathcal{A} \text{ breaks } N \text{ sessions of } P\right) < \eta^{-k}.$$

one which will yield an *improved bound*. To this end, the intern will design new inference rules with tighter probability bounds, find proof rewritings which are beneficial w.r.t. these probability bounds, and identify proof fragments for which there exists proof rewriting strategies which systematically allow to reduce the size of the derivations to a polynomial size. In this task, it may be useful to work at the *meta-logic* level of [Bae+21] rather than the *base logic* level of [BC14].

This internship can lead to a PhD.

References

[Bae+21] David Baelde, Stéphanie Delaune, Charlie Jacomme, Adrien Koutsos, and S. Moreau. "An Interactive Prover for Protocol Verification in the Computational Model". In: *IEEE Symposium on Security and Privacy*. San Fransisco / Virtual, United States: IEEE, May 2021, pp. 537–554.

[Bae+20] David Baelde, Stéphanie Delaune, Charlie Jacomme, Adrien Koutsos, and Solène Moreau. *The Squirrel Prover (paper and source code for anonymous submission)*. 2020. URL: https://github.com/squirrel-submission-sp21/squirrel-prover.

[BC14] Gergei Bana and Hubert Comon-Lundh. "A Computationally Complete Symbolic Attacker for Equivalence Properties". In: *ACM Conference on Computer and Communications Security*. ACM, 2014, pp. 609–620.

[Bar+11] Gilles Barthe, Benjamin Grégoire, Sylvain Heraud, and Santiago Zanella Béguelin. "Computer-Aided Security Proofs for the Working Cryptographer". In: *CRYPTO*. Vol. 6841. Lecture Notes in Computer Science. Springer, 2011, pp. 71–90.

[Bla06] Bruno Blanchet. "A Computationally Sound Mechanized Prover for Security Protocols". In: *IEEE Symposium on Security and Privacy*. IEEE Computer Society, 2006, pp. 140–154.