An important aspect of Internet security is the security of cryptographic protocols that it deploys. We need to make sure that such protocols achieve their goals, whether in isolation or in composition, i.e., security protocols must not suffer from any aw that enables hostile intruders to break their security. Among others, tools like OFMC [MV09b] and Proverif [Bla01] are quite efficient for the automatic formal verification of a large class of protocols. These tools use different approaches such as symbolic model checking or static analysis. Either approach has its own pros and cons, and therefore, we need to combine their strengths. Moreover, we need to ensure that the protocol implementation coincides with the formal model that we verify using such tools.

This thesis shows that we can simplify the formal verification of protocols in several ways. First, we introduce an Alice and Bob style language called SPS (Security Protocol Specification) language, that enables users, without requiring deep expertise in formal models from them, to specify a wide range of real-world protocols in a simple and intuitive way. Thus, SPS allows users to verify their protocols using different tools, and generate robust implementations in different languages. Moreover, SPS has the “ultimate” formal semantics for Alice and Bob notation in the presence of an arbitrary set of cryptographic operators and their algebraic theory. Despite its generality, this semantics is mathematically simpler than any previous attempt.

Second, we introduce two types of relative soundness results that reduce complex verification problems into simpler ones. The first kind is typing results showing that if a security protocol, that fulfills a number of sufficient conditions, has an attack then it has a well-typed attack. The second kind considers the parallel composition of protocols, showing that if the parallel composition of two protocols, that fulfill a number of sufficient conditions, allows for an attack then one of the protocols, at least, has an attack in isolation. In fact, we unify and generalize over prior relative soundness results. The most important generalization is the support for all security properties of the geometric fragment proposed by [Gut14].