Formal verification with algebraic techniques and its application

Abstract

Formal verification has been extensively used to analyze various kinds of systems, such as verifying cryptographic protocols with security properties and mutual exclusion protocols with mutex properties. It is known as a unique approach in guaranteeing the absence of bugs (undesirable properties) in such systems. This approach formally describes the system under verification as a mathematical model using a dedicated language. The obtained result is called the formal specification of the system. Once the desired properties are specified with respect to the specification, formal verification that the system satisfies the properties can be conducted. There are two complementary approaches in formal verification: model checking and theorem proving. The former can be automatically conducted but cannot be used for systems that have an infinite number of states (infinite-state systems) in general due to the state explosion problem. The latter can deal with infinite-state systems but it requires human creativity, especially in lemma conjecture.

This thesis presents a formal verification approach with the employment of an algebraic specification language, namely CafeOBJ, equipped with an interactive theorem proving system, applied to verify the requirement properties of systems. We propose an approach and implement a supporting tool, namely IPSG, that can automatically generate formal proofs, the so-called proof scores, for formal verification of invariant properties. The algebraic specification language CafeOBJ is equipped with a rich specification syntax and many useful features for formal specifications of even complex systems, such as concurrent systems and distributed systems. It can be used as a powerful interactive theorem proving system, where humans can write a proof score to verify a desired property. However, writing proof scores is time- and effort-consuming, especially with complicated systems or specifications, and proof scores manually written are subject to human errors because they are user-defined, while CafeOBJ does not check their correctness. That is the reason motivating us to automate the proof score writing process and implement the tool. To demonstrate the efficiency and the practicability of the tool, experiments with various systems/protocols are conducted, ranging from a classical key distribution protocol to authentication protocols, from a real-time system to mutual exclusion protocols, and from a distributed protocol to real cryptographic protocols currently in use.

In recent years, advanced research in the field of quantum computing and quantum information theory has brought a credible threat to cryptosystems currently in use. The most popular public-key (or asymmetric) primitives used today will no longer be secure under sufficient strong quantum computers because they can be efficiently broken by Shor's algorithm. That motivates cryptographers and security researchers to construct a new class of cryptographic protocols that are resistant to quantum attacks, called post-quantum cryptographic protocols (PQCPs), and verify the security of those PQCPs. Therefore, it would be very useful and meaningful to apply formal verification techniques to PQCP security analysis. This thesis presents two security verification case studies with: (1) the Hybrid Post-Quantum Transport Layer Security Protocol (PQ TLS) and (2) the Hybrid Post-Quantum Secure Shell Transport Layer Protocol (PQ SSH). PQ TLS has been proposed by Amazon Web Services (AWS) as a quantum-resistant version of the TLS 1.2 protocol, which is one of the most crucial and extensively used cryptographic protocols. PQ SSH has been proposed as a quantum-resistant version of the SSH Transport Layer protocol, where AWS is also one of the authors. We formally verify that the two protocols enjoy the desired security properties claimed in their design specifications, such as *session key secrecy* and *forward secrecy*, by using IPSG to generate their proof scores. The formal verifications are achieved under a threat model with the presence of an active attacker who can control the network, with respect to an unbounded number of protocol participants and protocol executions. The attacker can break the security of classical key exchange algorithms presuming by utilizing the power of large quantum computers. Moreover, the threat model also assumes the compromises of all secret types, such as ephemeral secret keys and long-term private keys of honest principals.

In the PQ SSH verification case study, in addition to the formal verification of three properties, we point out a counterexample showing that the protocol does not enjoy the *authentication* property, although what we found does not affect the confidentiality of session keys shared between honest participants. We then propose to slightly revise the protocol by adding the identifiers of the client and the server into the exchange hash. After revising the CafeOBJ formal specification accordingly, we can formally verify that the improved protocol enjoys the *authentication* property as well as the three other properties.

Keywords: formal verification, proof scores, post-quantum cryptographic protocols, algebraic language, IPSG.