# Mechanized Security Proofs for Security Protocols

A security protocol refers to a sequence of actions and/or message exchanges between communicating parties in a network to establish certain security targets, such as authentication of the parties involved, exchanges of secrets, commitment of a transaction, etc. Security protocols are an essential part of any secure communication systems and infrastructures and are used pervasively today for all sorts of applications, ranging from internet commerce, electronic voting, healthcare, and defence. Reasoning about the correctness of a protocol design is an extremely error prone task and involves subtle reasoning steps that often elude even seasoned researchers. A classic example of this is the Needham-Schroeder public key authentication protocol, which involves only seven message exchanges between three parties, but was only found to be insecure more than a decade after it was published. Figure 1 shows the Needham-Schroeder public key authentication protocol, and Figure 2 shows an attack found by Gavin Lowe. In the figures, we use the notation $\{M\}_k$ to denote the encryption of message $M$ with (public) key $K$, and *Pub(X)* to denote the public key of the participant $X$ in a protocol. The attacker in Figure 2 is represented by $I$ (the intruder representing itself) or *I(X)* (the intruder masquerading as a legitimate participant $X$). The attacker launches two parallel sessions, one between itself and Alice (A), and the other between itself and Bob (B), acting as a "man-in-the-middle" intercepting and modifying messages between the other participants. One notable aspect of the attack is that it does not make any assumptions on the strength of the cryptographic primitives (public key encryption in this case); the attack works even assuming the encryption is unbreakable.

The kind of attacks shown in Figure 2 demonstrates another dimension of security analysis: it is not enough to analyse the encryption functions in isolation, one needs to take into account the dynamics of interactions between agents in a protocol to discover flaws or to prove security. This project focuses on the latter aspect. One difficulty in this reasoning task is that a protocol designer needs to anticipate all potential interactions between attackers and the honest participants, of which there are many (sometimes infinitely many), so a (semi) automated approach to such a reasoning task will help alleviate some complexity of the task.

In this project, we aim to develop techniques and tools for reasoning about observational equivalence of security protocols. Observational equivalence has been shown to be a versatile framework to formalise and analyse a wide range of security properties, especially privacy-type properties. Notable examples include anonymity and unlinkability properties, that are difficult to capture using existing, more mature, techniques that are based on reachability analysis. Mechanized reasoning for observational equivalence is at the frontier of research in symbolic approaches to protocol analysis, and there have been so far only a handful of tools and limited techniques available. We also aim to develop techniques and tools that allow the production of independently checkable formal proofs of security, something that few existing tools have been able to do. The requirement that an (automated) protocol verifier produces independently checkable proofs, we believe, is one that will find useful applications, in particular in the areas of certification of correctness of protocols designs and their implementations. Such formal proofs of correctness are a requirement for certification of hardware and software systems at the Evaluation Assurance Level 7 (EAL 7) of the Common Criteria for Information Technology Evaluation (CC) [40], an internationally accepted standard for IT security evaluation.

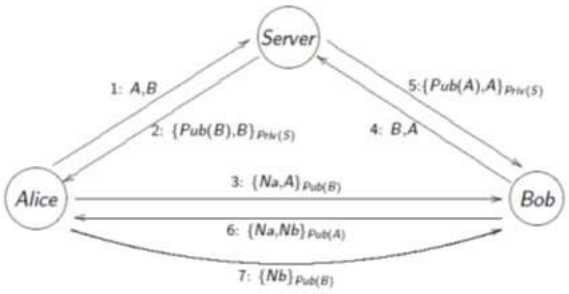


**Figure 1.** The Needham-Schroeder Public Key Authentication Protocol

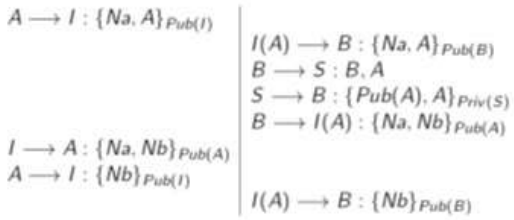


**Figure 2.** Lowe's attack on the Needham-Schroeder Public Key Authentication Protocol.

| | |
|---|---|
| **Principal Investigator** | Asst. Prof. Alwen Fernanto Tiu *(SCSE)* |
| **Researcher** | Dr. Ross Horne<br>Dr. Ki Yung Ahn<br>Mr. Nguyen Thanh Nam |
| **Student** | Ms Jiao Jiao |
| **School / Department** | School of Computer Science and Engineering |
| **Source of Funding** | Ministry of Education – Tier 2 |