Chapter 5

The Remark!
Internet-Based Exam

In this chapter, we introduce Remark!, a protocol designed for secure Internet-based exams. Remark! runs fully on computers to execute typical local tasks, such as the generation of questions and automatic marking, as well as remote tasks, such as remote registration and remote notification of candidates. Notably, it supports remote testing, in which distantly located candidates take the exam at their place, which is the distinctive functionality of Internet-based exams.

The goal of Remark! is to guarantee several authentication, privacy, and verifiability requirements without relying on a single trusted authority. The fundamental aim of its design is to distribute the trust among the parties and to get rid of TTP. This design approach is novel in the context of exam protocols because their design has normally been conceived with a TTP. However, the use of computers exposes exams to new threats and requires us to change the well-established procedures used in traditional exams. The conflicting interests that roles typically have in an exam complicate the design of secure exam protocols further. In fact, TTP may be corrupted, as recent scandals confirm [Cop13, Wat14, Lip14].

Remark! distributes the trust across the several servers that compose an exponentiation mixnet. As we shall see later, the mixnet generates the pseudonyms that allow the exam principals to encrypt and sign messages anonymously. Using ProVerif, we prove that Remark! ensures all the authentication and privacy requirements proposed in Chapter 3, with minimal reliance on trusted parties. Additionally, we demonstrate that Remark! provides the verifiability-tests listed in the same chapter, and discuss the necessary assumptions to make Remark! fully verifiable.

Similarly to any other security protocol, Remark! is not designed to withstand every possible threat. For instance, it cannot cope with plagiarism but assumes appropriate invigilation during testing. Principals may still collude and communicate via subliminal channels, for example by using steganography. Although it is hard to rule out completely such a threat, steganalysis techniques can be of some help here. Other countermeasures may be needed against collusion attacks that exploit covert channels. We thus specify seven assumptions...
conveniently for the goals of Remark!. In particular, we assume that:

1. Each principal holds a long-term public/private pair of keys.

2. The candidate holds a smart card in which the personal details of the candidate are visibly engraved. The smart card securely stores the candidate’s private key, namely the private key cannot be extracted from the smart card.

3. The candidate is invigilated during testing to mitigate cheating. Invigilation for remote testing can be guaranteed with online invigilation software, such as ProctorU [Inc15].

4. The model answers are kept secret from the candidates until after testing. The examiners may be provided with the model answers at marking.

5. An authenticated append-only bulletin board that guarantees that everyone can see the same data is available, though write access might be restricted to appropriate entities [BRT13].

6. An implementation of TLS channel that ensures integrity and confidentiality of messages is available.

Outline of the chapter. Section 5.1 reviews a few proposals of secure protocols for Internet-based exams. Section 5.2 details the basics of exponentiation mixnet, the cryptographic scheme on which Remark! is based. Section 5.3 describes Remark! according to the four phases of an exam. Section 5.4 contains the formal analysis in ProVerif of authentication, privacy, and verifiability requirements. Finally, Section 5.5 discusses future work and concludes the chapter.

5.1 Internet-Based Exams

Internet-based exams are probably not the most practised type of exam, but they are becoming more popular in innovative educational test technologies. MOOC companies offer students Internet-based exams that grant them credits for many universities [Lew13]. TOEFL [TOE], which is one of the major English-language tests in the world, has replaced its traditional exams with Internet-based exams. However, to the best of our knowledge, neither the specification nor the security requirements of MOOCs and TOEFL protocols are publicly available. Moreover, their design probably includes a trusted exam authority that is in charge of the critical tasks of the exam. Conversely, Remark! is designed to minimise the reliance on trusted parties. Huszti-Pethő [HP10] advanced an Internet-based exam with a few trust requirements on principals, but in Chapter 3 we have shown that the protocol has several security issues. In contrast, we prove that Remark! ensures all the security requirements.

In the domain of Computer Supported Collaborative Working, Foley and Jacob [FJ95] formalised confidentiality requirements and proposed an exam as a case study. Maffei et al. [MPR13] implemented a course evaluation system that guarantees privacy using anonymous credential schemes without a trusted third party. Similarly, Hohenberger et al. [HMPs14] advanced ANONIZE, a protocol