Thesis advisor: prof. Jerzy Jaworski

Łukasz Nitschke

Security of protocols in an untrusted environment

Abstract

The dissertation is devoted to the problem of providing security of computation in an untrusted environment. It introduces modifications to well known protocols like mix networks or key establishment protocols (interactive key generation). Based on these solutions new e-voting and e-exams protocols are presented. Special attention is paid to mix networks and to methods of augmenting their abilities. One of the proposed remote electronic voting protocols uses innovative computing mix networks which are able to perform modulo addition (on encrypted numbers) in a distributed way. The mentioned protocol and electronic exam protocols employ a modified mix network integrity verification procedure that allows for allows for using the same mix network twice. The analysis of the impact the partial checking procedures have on the level of anonymity of the mixing process is a substantial part of the work. For the presented mathematical model describing mix network anonymity a process of an observer information decline is presented and discussed in relation to the number of mix servers and messages sent.