MSc thesis defense presentation

Παναγι■της Γροντ■ς defends his MSc thesis

Date:	Τετ■ρτη, 07 Μ■ι 2014
■ρα:	14:15-15:15
Location:	Σχολ■ Ηλεκτρολ■γων Μηχανικ■ν και Μηχανικ■ν Υπολογιστ■ν, ΕΜΠ (παλαι■ κτ■ρια), α■θουσα 1.1.29
Thesis title:	Secure Multi Party Computations for Electronic Voting
Committee:	• ■γγελος Κιαγι■ς • Αριστε■δης Παγουρτζ■ς • Ευστ■θιος Ζ■χος

Thesis abstract

In this thesis, we study the problem of electronic voting as a general decision making process that can be implemented using multi party computations, fulfilling strict and often conflicting security requirements. To this end, we review relevant cryptographic techniques and their combinations to form voting protocols. More specifically, we analyze schemes based on homomorphic cryptosystems, mix nets with proofs of shuffles and blind signatures. We analyze how they achieve integrity and privacy in the voting process, while keeping efficiency. We examine the types of social choice functions that can be supported by each protocol. We provide two proof of concept implementations. Moreover, we review ways to thwart stronger adversaries by adding receipt freeness and coercion resistance to voting systems. We build on the latter concept to propose a modification to a well-known protocol. Finally, we study two actual e-Voting implementations namely Helios and Pret a Voter.