

# MSc thesis defense presentation

## Panagiotis Kalogeropoulos defends his MSc thesis

<b>Date:</b>	Wednesday, 08 Nov 2017
<b>Time:</b>	16:00
<b>Location:</b>	School of Electrical and Computer Engineering (old buildings), 1.1.31 <a href="#">Ηλεκτρονικ</a> <a href="#">Ψηφοφο</a> <a href="#">Ανθεκτικ</a> σε <a href="#">Εκβιασμο</a>
<b>Thesis title:</b>	<a href="#">Dimitris Fotakis</a> <a href="#">Aggelos Kiayias</a> <a href="#">Aristeidis T.</a> <a href="#">Pagourtzis</a>
<b>Committee:</b>	

---

### Thesis abstract

Η ασφάλεια και η μυστικότητα της ψήφου στην πλειοψηφία των εκλογικών πρωτοκόλλων βασίζεται στην αδυναμία του αντιπάλου να σπείσει τα κρυπτογραφικά εργαλεία. Δεδομένου ότι η υπολογιστική ισχύς αυξάνεται συνεχώς και η αποθήκευση για μελλοντική χρήση κάθε δημόσιας πληροφορίας έχει πλέον αμελητέο κόστος, τι θα συμβεβήκε μετ' απ' μερικά χρόνια τα κρυπτογραφικά εργαλεία σπείσουν; Στην παρούσα διπλωματική εργασία ασχολομαστέ με πρωτόκολλα που παρέχουν “Everlasting Privacy” καθώς και “Coercion Resistance”. Ιδιότητες που εξασφαλίζουν την μυστικότητα της ψήφου ακόμη κι απέναντι σε αντιπάλους με απεριόριστη υπολογιστική ισχύ και χρόνο καθώς και την δυνατότητα στον ψηφοφόρο να αποφύγει κάθε πιθανό εκβιασμό. Στην εργασία παρουσιάζονται δύο εκλογικά πρωτόκολλα που παρέχουν τριτογενούς ασφάλεια καθώς και τα επιμέρους κρυπτογραφικά εργαλεία που χρησιμοποιούν. Ως επίλογο αφενούμε την προσπείθεια μας για να τριτο εκλογικό πρωτόκολλο με ανάλογες ιδιότητες.

Download date: 2024-09-11, 12:27.