

# MSc thesis defense presentation

Παναγιώτης Καλογερόπουλος

## defends his MSc thesis

<b>Date:</b>	Τετάρτη, 08 Νοβ 2017
<b>Ώρα:</b>	16:00
<b>Location:</b>	Σχολή Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών, ΕΜΠ (παλαιό κτίριο), 1.1.31 <a href="#">Ηλεκτρονικός</a> <a href="#">Ψηφοφορίες</a> <a href="#">Ανθεκτικός σε</a> <a href="#">Εκβιασμούς</a>
<b>Thesis title:</b>	<a href="#">Δημιτρής</a> <a href="#">Φωτκής</a>
<b>Committee:</b>	<ul style="list-style-type: none"><li><a href="#">Γγέλος Κιαγής</a></li><li><a href="#">Αριστείδης</a> <a href="#">Παγουρτζής</a></li></ul>

---

## Thesis abstract

Η ασφάλεια και η μυστικότητα της ψήφου στην πλειοψηφία των εκλογικών πρωτοκόλλων βασίζεται στην αδυναμία του αντιπάλου να σπείρει 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 συμβεβήταν μετά από μερικά χρόνια τα κρυπτογραφικά εργαλεία σπύσουν; 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 έπαιλο αφήνουμε την προοπτική μας για ένα τρίτο εκλογικό πρωτόκολλο με ανώλογες ιδιότητες.