

MSc thesis defense presentation

Παναγιώτης Καλογερόπουλος

defends his MSc thesis

Date:	Τετάρτη, 08 Νοβ 2017
Ώρα:	16:00
Location:	Σχολή Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών, ΕΜΠ (παλαιό κτίριο), 1.1.31 Ηλεκτρονικός Ψηφοφορίες Ανθεκτικός σε Εκβιασμό
Thesis title:	Δημιτρής Φωτικής
Committee:	<ul style="list-style-type: none">Γγελος ΚιαγίληςΑριστείδης Παγουρτζής

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 επίλογο αφενούμε την προσέθετα μας για να τριτο εκλογικό πρωτόκολλο με ανάλογες ιδιότητες.