MSc thesis defense presentation

Παναγι■της Καλογερ■πουλος
defends his MSc thesis

Date:	Τετ■ρτη, 08 Νο■ 2017
■ρα:	16:00
Location:	Σχολ■ Ηλεκτρολ■γων Μηχανικ■ν και Μηχανικ■ν Υπολογιστ■ν, ΕΜΠ (παλαι■ κτ■ρια), 1.1.31
Thesis title:	Ηλεκτρονικ■ς Ψηφοφορ■ες Ανθεκτικ■ς σε Εκβιασμο■ς
Committee:	• Δημ■τρης Φωτ■κης • ■γγελος Κιαγι■ς • Αριστε■δης Παγουρτζ■ς

Thesis abstract

Η ασφ■λεια και η μυστικ■τητα της ψ■φου στην πλειοψηφ■α των εκλογικ■ν πρωτοκ■λλων βασ■ζεται στην αδυναμ■α του αντιπ■λου να σπ■σει τα κρυπτογραφικ■ εργαλε■α. Δεδομ■νου ■τι η υπολογιστικ■ ισχ■ς αυξ■νεται συνεχ■ς και η αποθ■κευση για μελλοντικ■ χρ■ση κ■θε δημ■σιας πληροφορ■ας ■χει πλ■ον αμελητ■ο κ■στος, τι θα συμβε■ ■ταν μετ■ απ■ μερικ■ χρ■νια τα κρυπτογραφικ■ εργαλε■α σπ■σουν; Στην παρο■σα διπλωματικ■ εργασ■α ασχολο■μαστε με πρωτ■κολλα που παρ■χουν “Everlasting Privacy” καθ■ς και “Coercion Resistance”. Ιδι■τητες που εξασφαλ■ζουν την μυστικ■τητα της ψ■φου ακ■μη κι απ■ναντι σε αντιπ■λους με απερι■ριστη υπολογιστικ■ ισχ■ και χρ■νο καθ■ς και την δυνατ■τητα στον ψηφοφ■ρο να αποφ■γει κ■θε πιθαν■ εκβιασμ■. Στην εργασ■α παρουσι■ζονται δ■ο εκλογικ■ πρωτ■κολλα που παρ■χουν τ■τοιου ε■δους ασφ■λεια καθ■ς και τα επιμ■ρους κρυπτογραφικ■ εργαλε■α που χρησιμοποιο■ν. Ως επ■λογο αφ■νουμε την προσπ■θεια μας για ■να τρ■το εκλογικ■ πρωτ■κολλο με αν■λογες ιδι■τητες.