# ΟΜΙΛΙΑ

## "Electronic Voting with Coercion Resistance and Everlasting Privacy"

***Παναγιώτης Γροντάς***

*Ερευνητής*

*ΕΜΠ & Ερευνητική μονάδα 'Αρχιμήδης', Ερευνητικό Κέντρο Αθηνά*

## ΠΕΡΙΛΗΨΗ – ABSTRACT

Η ομιλία αρχικά θα κάνει μια σύντομη εισαγωγή στα χαρακτηριστικά και τις απαιτήσεις ασφάλειας των ηλεκτρονικών ψηφοφοριών καθώς και τον ρόλο της κρυπτογραφίας σε αυτές.

Στην συνέχεια θα παρουσιαστεί ένα νέο σχήμα συνδεδέσιμης υπογραφής δακτυλίου (linkable ring signature) το οποίο διαθέτει τέλεια ανωνυμία, μαζί με ένα πρωτόκολλο ψηφοφορίας που το αξιοποιεί για την επίτευξη αντίστασης στον εξαναγκασμό (coercion resistance) και αέναης ιδιωτικότητας (everlasting privacy). Στο προτεινόμενο σύστημα, οι ψηφοφόροι δημιουργούν διαπιστευτήρια και δημοσιεύουν τα κάποια τμήματα τους. Για να ψηφίσουν, δημιουργούν ένα δακτύλιο (σύνολο ανωνυμίας) που αποτελείται από δημόσια διαπιστευτήρια, μαζί με μια απόδειξη γνώσης του κρυφού τους διαπιστευτηρίου χρησιμοποιώντας την προτεινόμενη υπογραφή. Η τέλεια ανωνυμία του εμποδίζει έναν επιτιθέμενο, ανεξάρτητα από την ισχύ του, να συμπεράνει την ταυτότητα του ψηφοφόρου, επιτυγχάνοντας έτσι αέναη ιδιωτικότητα. Επιπλέον, το προτεινόμενο πρωτόκολλο παρέχει αντίσταση στον εξαναγκασμό στο πλαίσιο JCJ. Όταν ένας αντίπαλος προσπαθεί να εκβιάζει έναν ψηφοφόρο, η επίθεση μπορεί να αποφευχθεί με τη δημιουργία μιας υπογραφής με ένα ψεύτικο αλλά μη διακρίσιμο διαπιστευτήριο. Κατά τη διάρκεια μιας στιγμής ιδιωτικότητας, ο ψηφοφόρος θα υποβάλει την πραγματική του ψήφο. Το σχήμα μας παρέχει επίσης επαληθευσιμότητα και μυστικότητα της ψήφου.

Η ομιλία βασίζεται στην εργασία Voting with coercion resistance and everlasting privacy using linkable ring signatures (https://eprint.iacr.org/2025/002) που αποτελεί δουλειά που έχει εκπονηθεί μαζί με την ΥΔ ΕΜΠ κ. Μαριάννα Σπυράκου και τον Καθηγητή ΕΜΠ κ. Αριστείδη Παγουρτζή.

***Short Bio:*** *Ο Δρ. Παναγιώτης Γροντάς έλαβε το διδακτορικό του στην Κρυπτογραφία από το Τμήμα Ηλεκτρολόγων Μηχανικών και Επιστήμης Υπολογιστών του Εθνικού Μετσόβιου Πολυτεχνείου (ΕΜΠ). Επιπλέον, διαθέτει μεταπτυχιακό στην Λογική, τους Αλγόριθμους και τη Θεωρία Υπολογισμού από το Πανεπιστήμιο Αθηνών, μεταπτυχιακό στα Πληροφοριακά Συστήματα από το Οικονομικό Πανεπιστήμιο Αθηνών και πτυχίο στην Πληροφορική από το Πανεπιστήμιο Πειραιά. Η έρευνά του επικεντρώνεται σε κρυπτογραφικά ασφαλή και επαληθεύσιμα πρωτόκολλα για εφαρμογές με απαιτήσεις ιδιωτικότητας. Έχει δημοσιεύσει άρθρα σε διεθνή συνέδρια και περιοδικά. Έχει συγγράψει κεφάλαια του ηλεκτρονικού βιβλίου "Υπολογιστική Κρυπτογραφία". Αυτή την περίοδο συνεργάζεται με το ΕΜΠ και με την ερευνητική μονάδα 'Αρχιμήδης' του*

*ερευνητικού κέντρου Αθηνά σε θέματα κρυπτογραφίας. Έχει επίσης (συν)διδάξει μαθήματα σχετικά με Κρυπτογραφία (τόσο σε βασικό όσο και σε προχωρημένο επίπεδο), Αλγόριθμους και Πολυπλοκότητα στο Τμήμα Ηλεκτρολόγων Μηχανικών και Επιστήμης Υπολογιστών του ΕΜΠ και στο μεταπτυχιακό πρόγραμμα ΑΛΜΑ.*

*Εκτός από τις ακαδημαϊκές του δραστηριότητες, ο Παναγιώτης Γροντάς έχει εργαστεί ως μηχανικός λογισμικού στον ιδιωτικό και τον δημόσιο τομέα, καθώς και ως καθηγητής πληροφορικής.*

**ΔΕΥΤΕΡΑ 15 ΙΟΥΝΙΟΥ 2026**
**13:30-14:30**
**ΑΙΘΟΥΣΑ ΣΕΜΙΝΑΡΙΩΝ**