Εθνικό Μετσόβιο Πολυτεχνείο

Σχολή Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών

Προχωρημένα Θέματα Κρυπτογραφίας 2024-25

(ΣΗΜΜΥ, ΑΛΜΑ, ΕΜΕ)

Διδάσκοντες: Α. Παγουρτζής, Ν. Λεονάρδος, Π. Γροντάς

2η Σειρά Ασκήσεων

Bitcoin & Byzantine Agreement

Άσκηση 1. Έστω ένας αντίπαλος που έχει το $1/3$ της συνολικής υπολογιστικής ισχύος, αλλά έχει την δυνατότητα διαμέρισης του δικτύου (δηλ. να χωρίσει τους τίμιους παίκτες σε σύνολα A και B ώστε να μην φθάνουν καθόλου μηνύματα από το A στο B και αντίστροφα). Δείξτε ότι οι ιδιότητες common prefix and chain quality δεν ισχύουν με μη-αμελητέα πιθανότητα για τέτοιο αντίπαλο.

Άσκηση 2. Δώστε απόδειξη ότι η επίθεση του Bahack επιτυγχάνει με μη-αμελητέα πιθανότητα όταν χρησιμοποιείται «naive target recalculation.»

Άσκηση 3. Δείξτε πως ένα πρωτόκολλο για το broadcast (την εκδοχή όπου ένας παίκτης ορίζεται ως αποστολέας) μπορεί να χρησιμοποιηθεί για την επίλυση του consensus.

Άσκηση 4. Δείξτε, ορίζοντας αντίπαλο, ότι ο αλγόριθμος EIG δεν λύνει το πρόβλημα consensus για $t = 1$ και $n = 3$ σε δύο γύρους.

Άσκηση 5. Δείξτε, ορίζοντας αντίπαλο για κάποιο $t < n$, ότι ο αλγόριθμος των Dolev και Strong δεν λύνει το πρόβλημα broadcast αν οι παίκτες σταματήσουν έναν γύρο νωρίτερα.

Προθεσμία υποβολής και οδηγίες. (α) προσπαθήστε μόνοι σας, (β) συζητήστε με συμφοιτητές σας, (γ) αναζητήστε ιδέες στο διαδίκτυο, με αυτή τη σειρά και αφού αφιερώσετε αρκετό χρόνο σε κάθε στάδιο! Οι απαντήσεις θα πρέπει να υποβληθούν έως 10/06/2025, σε ηλεκτρονική μορφή με αναφορά σε όποιες πηγές έχουν χρησιμοποιηθεί.