Εθνικό Μετσόβιο Πολυτεχνείο

Σχολή Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών

Προχωρημένα Θέματα Κρυπτογραφίας 2023-24

(ΣΗΜΜΥ, ΑΛΜΑ, ΕΜΕ)

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

1η Σειρά Ασκήσεων

Blockchain, Consensus

Μέρος 1: Consensus (n είναι ο συνολικός αριθμός παικτών και t ο αριθμός των παικτών που ελέγχει ο αντίπαλος.)

Άσκηση 1. Δώστε στρατηγική του αντιπάλου, για την οποία ο αλγόριθμος EIG δεν ικανοποιεί τουλάχιστον μία ιδιότητα του consensus για $t = 1$ και $n = 3$.

Άσκηση 2. Με δεδομένο ότι το consensus δεν λύνεται για $t = 1$ και $n = 3$, αποδείξτε ότι δεν λύνεται για $n = 3t$ για όλα τα $t \geq 1$.

Μέρος 2: Bitcoin backbone ($\{0,1\}^\kappa$ είναι το πεδίο τιμών της συνάρτησης κατακερματισμού, $p = T/2^\kappa$, n και t όπως παραπάνω.)

Άσκηση 3. Δώστε πλήρη απόδειξη ότι η επίθεση του Bahack's επιτυγχάνει με μη-αμελητέα πιθανότητα όταν χρησιμοποιείται "naive target recalculation."

Άσκηση 4. Επιλέξτε τιμές για τα p και n ώστε ακόμα και ένας αντίπαλος με μηδενική υπολογιστική ισχύ να μπορεί να δημιουργήσει fork μήκους k στο Bitcoin backbone με πιθανότητα μη-αμελητέα στο k. (Τα p και n μπορούν να εξαρτώνται από το k.)

Άσκηση 5. Θεωρείστε το bounded-delay μοντέλο στο οποίο ο αντίπαλος μπορεί να καθυστερήσει κάθε μήνυμα μέχρι Δ γύρους. Επιλέξτε τιμή για το Δ ώστε ακόμα και ένας αντίπαλος με μηδενική υπολογιστική ισχύ να μπορεί να δημιουργήσει fork μήκους k στο Bitcoin backbone με πιθανότητα μη-αμελητέα στο k. (Τα p και n είναι ανεξάρτητα από το k, ενώ το Δ μπορεί να οριστεί ως συνάρτηση του k.)

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 την Παρασκευή 14/06/2024, σε ηλεκτρονική μορφή με αναφορά σε όποιες πηγές έχουν χρησιμοποιηθεί.