Εθνικό Μετσόβιο Πολυτεχνείο
Σχολή Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών

Προχωρημένα Θέματα Κρυπτογραφίας 2022-23
(ΣΗΜΜΥ, ΑΛΜΑ, ΕΜΕ)

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

2η Σειρά Ασκήσεων
Blockchain - Consensus - BA - Voting

Άσκηση 1. [Από το μάθημα 'COMS 6998-006:Foundations of Blockchains' του Tim Roughgarden https://timroughgarden.github.io/fob21/]
Στο πρόβλημα Byzantine Broadcast υποθέτουμε ότι η ιδιωτική είσοδος του αποστολέα είναι είτε 0 είτε 1 και $n \geq 3$. Έστω ότι το παρακάτω πρωτόκολλο εκτελείται από όλους τους honest nodes:

- Γύρος 0: Ο αποστολέας στέλνει το ιδιωτικό του bit (μαζί με την υπογραφή του) σε όλους τους άλλους κόμβους. Στη συνέχεια ο αποστολέας εξάγει ως αποτέλεσμα το δικό του ιδιωτικό bit και τερματίζει.
- Γύρος 1: Κάθε μη-αποστολέας κόμβος i υπογράφει και αποστέλλει ό,τι άκουσε από τον αποστολέα σε όλους τους άλλους μη-αποστολείς κόμβους.
- Γύρος 2: Κάθε μη-αποστολέας κόμβος συλλέγει όλες τις ψήφους που έλαβε (μέχρι $n-1$ ψήφους, με το πολύ μία από τον αρχικό αποστολέα στο γύρο 0 και το πολύ μία από κάθε κόμβο μη-αποστολέα από τον γύρο 1) και επιλέγει ως αποτέλεσμα την τιμή που πλειοψηφεί. (Εάν υπάρχει ίσος αριθμός ψήφων και για το 0 και για το 1, βγάζει 0). Εάν ένας κόμβος υποβάλει πολλαπλές ψήφους για διαφορετικές τιμές, όλες οι ψήφοι από αυτόν τον κόμβο αγνοούνται.

Για καθένα από παρακάτω ερωτήματα δώστε είτε απόδειξη (αν ισχύει), είτε ένα αντιπαράδειγμα:

1. Έστω $t = 1$ (δηλαδή, το πολύ ένας κόμβος είναι διεφθαρμένος, και όλοι οι υπόλοιποι είναι τίμιοι). Ικανοποιεί το πρωτόκολλο αυτό την ιδιότητα της συμφωνίας (agreement);
2. Έστω $t = 1$. Ικανοποιεί το πρωτόκολλο αυτό την ιδιότητα της εγκυρότητας (validity);
3. Έστω $t = 2$. Ικανοποιεί το πρωτόκολλο αυτό την ιδιότητα της συμφωνίας;
4. Έστω $t = 2$. Ικανοποιεί το πρωτόκολλο αυτό την ιδιότητα της εγκυρότητας;
5. Δείτε το πρωτόκολλο Dolev-Strong στη διάλεξη 2 του COMS 6998-006. Αν σταματήσουμε το πρωτόκολλο ένα γύρο νωρίτερα - χωρίς καμία άλλη αλλαγή - εξακολουθεί να ικανοποιεί την ιδιότητα της συμφωνίας;
6. Ισχύει το ίδιο και για την ιδιότητα της εγκυρότητας (για το πρωτόκολλο του προηγούμενου ερωτήματος);

Άσκηση 2. Δείξτε, ορίζοντας τον κατάλληλο αντίπαλο, ότι ο αλγόριθμος EIG δεν λύνει το πρόβλημα του consensus για $t = 1$ και $n = 3$ (n είναι το σύνολο των παικτών).

Άσκηση 3. Έστω ένας αντίπαλος που έχει το $1/3$ της συνολικής υπολογιστικής ισχύος για $n = 2t$ τίμιους παίκτες, αλλά έχει την επιπλέον 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 για τέτοιο αντίπαλο.

Άσκηση 4. Δείξτε ότι υπάρχουν τιμές για το T και το n έτσι ώστε να μην ισχύει το common prefix lemma ακόμα και για έναν αντίπαλο χωρίς hashing power. *Υπόδειξη: Να χρησιμοποιηθεί η δύναμη του αντιπάλου για τη διάταξη των μηνυμάτων στην ουρά των τίμιων παικτών.*

Άσκηση 5. [Από το μάθημα "Ασφάλεια Υπολογιστικών Συστημάτων: Introduction to Blockchain Science and Engineering" του ΕΚΠΑ (συντελεστές: Α. Κιαγιάς, Δ. Ζήνδρος, Χ. Νασίκας)]
Να απαντήσετε στα ακόλουθα ερωτήματα στο μοντέλο του Bitcoin Backbone:

1. Δείξτε γιατί δεν ισχύει το Common-Prefix Lemma όταν $n = t$ (δηλαδή, όταν ο αντίπαλος έχει την ίδια ισχύ με τους τίμιους παίκτες).
2. Εξηγήστε γιατί η ιδιότητα Chain Growth είναι βέλτιστη.
3. Θεωρήστε ότι το mining target είναι $T = 2^{\kappa-1}$ όπου κ είναι η παράμετρος ασφάλειας και θυμηθείτε ότι το Random Oracle παράγει έξοδο κ bits. Έστω ότι στο παιχνίδι έχουμε $n = 10$ τίμιους παίκτες και $t = 5$ που ελέγχονται από τον αντίπαλο (δηλαδή ο αντίπαλος έχει το 33% της υπολογιστικής ισχύος). Περιγράψτε στρατηγική του αντιπάλου που σπάει τις ιδιότητες Common Prefix και Chain Quality. Εκτιμήστε την πιθανότητα επιτυχίας της στρατηγικής και δείξτε ότι είναι μη αμελητέα.
4. Έστω ότι στο παραπάνω σενάριο $t = 0$ και $n = 22$ (δηλαδή ο αντίπαλος δεν έχει καθόλου υπολογιστική ισχύ, αλλά μπορεί να αλλάζει τη σειρά στα μηνύματα των παικτών). Είναι η πιθανότητα ενός *επιτυχημένου* γύρου ποιοτικά κοντά στην πιθανότητα ενός *μοναδικά επιτυχημένου* γύρου; Θα παραβιαστεί η ιδιότητα του Common Prefix για $k = 30$;

Άσκηση 6. Οι μη-αλληλεπιδραστικές αποδείξεις μηδενικής γνώσης για το Plaintext Equivalence Test (PET) χρησιμοποιούν τον μετασχηματισμό Fiat-Shamir. Με δεδομένο ότι γίνεται χρήση της weak μορφής του, να προσπαθήσετε να επιτεθείτε στο πρωτόκολλο με στόχο να κατασκευάσετε **μία** *ψευδή* απόδειξη ότι δύο κρυπτοκείμενα αντιστοιχούν στο ίδιο μήνυμα (ενώ κάτι τέτοιο δεν ισχύει) ή ότι δύο κρυπτοκείμενα δεν αντιστοιχούν στο ίδιο μήνυμα (ενώ στην πραγματικότητα είναι ισοδύναμα). Κάποιες από τις παρακάτω υποθέσεις μπορούν να σας βοηθήσουν στην επίθεσή σας.

- όλοι οι παίκτες που συμμετέχουν στο πρωτόκολλο PET συνεργάζονται ή
- ότι γνωρίζουν την τυχαιότητα που χρησιμοποιήθηκε για την κατασκευή των μηνυμάτων (είτε πλήρως είτε τμηματικά) ή
- μπορούν να κατασκευάσουν το ένα από τα δύο κρυπτοκείμενα κατά βούληση.

Μπορείτε ενδεχομένως να κάνετε και οποιαδήποτε άλλη υπόθεση θεωρείτε αναγκαία.

Άσκηση 7. Στην εργασία VoteAgain: A scalable coercion-resistant voting system προτείνεται μεταξύ άλλων μια επέκταση του μοντέλου BPRIV για την ιδιότητα Coercion Resistance. Να την συγκρίνετε με το μοντέλο ασφάλειας του JCJ (σύγκριση ιδανικού - πραγματικού παίγνιου) που παρουσιάστηκε στη 2η διάλεξη για τις ηλ. ψηφοφορίες.

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 τις 01/06/2023, σε ηλεκτρονική μορφή με αναφορά σε όποιες πηγές έχουν χρησιμοποιηθεί.