Εθνικό Μετσόβιο Πολυτεχνείο

Σχολή Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών

Προχωρημένα Θέματα Κρυπτογραφίας 2020-21

(ΣΗΜΜΥ, ΑΛΜΑ, ΕΜΕ)

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

1η Σειρά Ασκήσεων

(Byzantine Fault Tolerance - Consensus - Blockchain)

Άσκηση 1. Θεωρήστε το πρωτόκολλο BGP'89 [P. Berman, J.A. Garay and K.J. Perry, "Towards Optimal Distributed Consensus," Proc. 30th FOCS, pp. 410-415, 1989] που συζητήσαμε στο μάθημα.

(α) Αν επιχειρήσουμε να εκτελέσουμε το πρωτόκολλο με $n = 2t+1$ σε ποια σημεία μπορεί να αποτύχει (όπου n το πλήθος των παικτών και t το πλήθος των διεφθαρμένων παικτών); Κατασκευάστε ένα απλό παράδειγμα.

(β) Μπορείτε να χρησιμοποιήσετε randomization για επιτάχυνση κατά την επιλογή του βασιλιά; Πώς ακριβώς μπορεί να γίνει αυτό; Εξηγήστε.

Ποια θα είναι η αναμενόμενη πολυπλοκότητα γύρων (round complexity);

Άσκηση 2. Στην εργασία [Brian A. Coan, "A communication-efficient canonical form for fault-tolerant distributed protocols", Proc. 5th ACM PODC, pp. 63–72, 1986] στην Ενότητα 4 ορίζεται το πρόβλημα Avalanche Agreement και προτείνεται ένα πρωτόκολλο (Protocol 2) που επιτυγχάνει το ζητούμενο αν $n \geq 3t+1$. Σε κάποιο σημείο της σελ. 66 αναφέρεται ότι η παραλλαγή όπου το Consensus Condition απαιτεί συμφωνία σε έναν γύρο αντί για δύο μπορεί να λυθεί εύκολα αν $n \geq 4t+1$ με κατάλληλη προσαρμογή του παραπάνω πρωτοκόλλου (Protocol 2). Βρείτε και περιγράψτε την παραλλαγή αυτή και εξηγήστε την ορθότητά της.

Άσκηση 3. [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 (σελ. 19 στις διαφάνειες) 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 $k = 30$;

Προθεσμία υποβολής και οδηγίες. Οι απαντήσεις θα πρέπει να υποβληθούν έως τις 7/5/2021, σε ηλεκτρονική μορφή. Για απορίες / διευκρινίσεις: επικοινωνήστε με τους διδάσκοντες: `atc2021@corelab.ntua.gr`