Εθνικό Μετσόβιο Πολυτεχνείο
Σχολή Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών

Υπολογιστική Κρυπτογραφία

(ΣΗΜΜΥ, ΣΕΜΦΕ, ΑΛΜΑ, ΕΜΕ)

4η Σειρά Ασκήσεων

Προθεσμία παράδοσης: ημέρα εξέτασης

Άσκηση 1. Έστω το παρακάτω πρωτόκολλο μηδενικής γνώσης. Οι δημόσιες παράμετροι είναι $\langle p, m, g, h\rangle$ και ο prover γνωρίζει ένα x τέτοιο ώστε $g^x = h \mod p$.

- Ο prover επιλέγει τυχαία ένα $t \in \mathbb{Z}_m^*$ και στέλνει στον verifier το $y = g^t \mod p$.
- Ο verifier επιλέγει τυχαία $c \in \mathbb{Z}_m^*$ και το στέλνει στον prover.
- Ο prover υπολογίζει το $s = t + c + x$ και το στέλνει στον verifier.
- Ο verifier αποδέχεται αν και μόνο αν $g^s = yg^ch \mod p$.

Εξετάστε αν το παραπάνω πρωτόκολλο είναι μηδενικής γνώσης για τίμιους επαληθευτές.

Άσκηση 2. Να αποδείξετε ότι ένα σχήμα δέσμευσης δεν μπορεί να διαθέτει ταυτόχρονα τις ιδιότητες τέλειας δέσμευσης και τέλειας απόκρυψης.

Άσκηση 3. Υλοποιήστε το σχήμα υπογραφών Schnorr σε γλώσσα προγραμματισμού της επιλογής σας. Μπορείτε να επιλέξετε είτε η υλοποίηση να βασιστεί σε ομάδα ελλειπτικών καμπυλών είτε σε ομάδα ακέραιων mod κάποιον πρώτο, ανάλογα με τις διαθέσιμες βιβλιοθήκες για την γλώσσα προγραμματισμού της επιλογής σας.

Άσκηση 4. Να δώσετε τις μη-διαλογικές αποδείξεις χρησιμοποιώντας την τεχνική Fiat-Shamir για τις παρακάτω περιπτώσεις της διαλέξης για τις ηλεκτρονικές ψηφοφορίες (18.12.2018):

- Ορθή αποκρυπτογράφηση στο πρωτόκολλο CGS97 (βλ. διαφάνεια 21)
- Εγκυρότητα αρνητικής ψήφου στο πρωτόκολλο CGS97 (βλ. διαφάνεια 22)

Άσκηση 5. Μία συνάρτηση σύνοψης $\mathcal{H} : \{0,1\}^* \to \{0,1\}^n$ είναι ασφαλής για χρήση σε συστήματα proof of work (PoW) αν για καθε είσοδο x είναι δύσκολο να βρεθεί λύση r ώστε να ισχύει $\mathcal{H}(x||r) \in Y$, όπου Y κάποιο σημαντικά μικρό υποσύνολο του $\{0,1\}^n$.

1. Να αποδείξετε ότι μία συνάρτηση σύνοψης που έχει την ιδιότητα collision resistance δεν είναι απαραίτητα ασφαλής για PoW.

Υπόδειξη: Να κατασκευάσετε ένα αντιπαράδειγμα, δηλαδή μια συνάρτηση $\mathcal{H}'$ που είναι collision resistant, αλλά όχι ασφαλής για PoW, επεκτείνοντας μια συνάρτηση $\mathcal{H}$ που είναι collision resistant και ασφαλής για PoW.

2. Να δείξετε ότι η συνάρτηση $\mathcal{G}(z) = \mathcal{H}(z)||LSB(z)$, όπου $LSB(z)$ είναι το λιγότερο σημαντικό bit του z είναι ασφαλής για PoW αλλά δεν έχει αντισταση πρώτου ορίσματος.

Άσκηση 6.

1. Περιγράψτε ένα σενάριο στο οποίο δύο miners στο bitcoin δίκτυο ενώ ακολουθούν το πρωτόκολλο πιστά δημιουργούν δύο διαφορετικές αλυσίδες τις οποίες και ακολουθούν.

2. Να επιχειρηματολογήσετε ότι το παραπάνω σενάριο που περιγράψατε συμβαίνει με μικρή πιθανότητα.

3. Η Μίνα, μια κακόβουλη miner, σε κάθε block που βλέπει αλλάζει το coinbase transaction ώστε να πληρώνεται η ίδια πριν το κάνει relay στο δίκτυο. Γιατί η Μίνα δεν βγάζει επιπλέον κέρδη;