Εθνικό Μετσόβιο Πολυτεχνείο
Σχολή Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών

Υπολογιστική Κρυπτογραφία

(ΣΗΜΜΥ, ΣΕΜΦΕ, ΑΛΜΑ, ΕΜΕ)

4η Σειρά Ασκήσεων

Προθεσμία παράδοσης 29/1/2020

Άσκηση 1.

Σταθερό σημείο ενός κρυπτοσυστήματος ονομάζουμε ένα μήνυμα που το κρυπτοκείμενό του είναι το ίδιο το μήνυμα, δηλαδή $enc(m) = m$. Επομένως, στην περίπτωση του RSA, αν το δημόσιο κλειδί είναι το (N, e), τότε για ένα σταθερό σημείο ισχύει $m^e \equiv m \pmod{N}$. Αποδείξτε ότι το πλήθος των σταθερών σημείων στο RSA είναι $[\gcd(e-1, p-1) + 1][\gcd(e-1, q-1) + 1]$.

Άσκηση 2.

΄Εστω το παρακάτω σχήμα υπογραφών όπου για τις παραμέτρους ισχύει ό,τι και στο σχήμα υπογραφών ElGamal. Κάθε χρήστης έχει ιδιωτικό κλειδί x και δημόσιο $y = g^x \bmod p$. Η υπογραφή λειτουργεί ως εξής:

i. Ο υπογράφων αρχικά επιλέγει $h \in \{0, \ldots, p-2\}$ ώστε: $\mathcal{H}(m) + x + h \equiv 0 \pmod{p-1}$, όπου $\mathcal{H}$ collision resistant συνάρτηση σύνοψης.

ii. Η υπογραφή είναι η τριάδα: $sign(x, m) = (m, (x + h) \bmod p - 1, g^h \bmod p)$.

iii. Για την επαλήθευση ότι μια τριάδα (m, a, b) είναι έγκυρη υπογραφή ελέγχεται εάν:

- $yb \equiv g^a \pmod{p}$ και
- $g^{\mathcal{H}(m)} yb \equiv 1 \pmod{p}$.

Να δείξετε ότι το σχήμα αυτό δεν προστατεύει από επίθεση καθολικής πλαστογράφησης.

Άσκηση 3.

Δίνεται το παρακάτω πρωτόκολλο μεταξύ ενός prover $\mathcal{P}$ και ενός verifier $\mathcal{V}$ το οποίο έχει στόχο την απόδειξη γνώσης του μηνύματος που αντιστοιχεί σε ένα δεδομένο κρυπτοκείμενο RSA με δημόσιο κλειδί (e, n), δηλαδή $m \in \mathbb{Z}_n^*$ τέτοιο ώστε $y = m^e \bmod n$. Επιπλέον θεωρήστε ότι e πρώτος.

- Ο $\mathcal{P}$ επιλέγει τυχαία ένα $t \in \mathbb{Z}_n^*$ και στέλνει στον $\mathcal{V}$ το $h = t^e \bmod n$.
- Ο $\mathcal{V}$ επιλέγει ένα τυχαίο c, $c \in \{0, \ldots, e-1\}$, και το στέλνει στον $\mathcal{P}$.
- Ο $\mathcal{P}$ υπολογίζει το $r = tm^c \bmod n$ και το στέλνει στον $\mathcal{V}$.
- Ο $\mathcal{V}$ αποδέχεται αν και μόνο αν $r^e \equiv hy^c \pmod{n}$.

Να αποδείξετε ότι το παραπάνω είναι Σ-πρωτόκολλο. Για την ιδιότητα HVZK η απόδειξη πρέπει να είναι στο επίπεδο ανάλυσης που ακολουθήθηκε στις διαφάνειες, αλλά να φαίνονται αναλυτικά τα transcripts του πρωτοκόλλου και η πιθανότητα εμφάνισής τους.

Άσκηση 4.

Να υλοποιήσετε σε γλώσσα προγραμματισμού της επιλογής σας την επίθεση αποκρυπτογράφησης ενός κρυπτοκειμένου c σε RSA που χρησιμοποιεί ένα oracle το οποίο μπορεί να αποφανθεί αν το μήνυμα που αντιστοιχεί στο κρυπτοκείμενο είναι στο 'πάνω' ή στο 'κάτω' μισό του $\mathbb{Z}_n$ (δηλ. συνάρτηση loc - βλ. διάλεξη RSA - διαφάνειες 36–40).

Συγκεκριμένα πρέπει να υλοποιήσετε 2 προγράμματα:
(1) Το πρώτο θα 'προσομοιώνει' το oracle, αποκρυπτογραφώντας (κανονικά με το ιδιωτικό κλειδί) το c και υπολογίζοντας την loc.
(2) Το δεύτερο θα υλοποιεί την επίθεση ρωτώντας επαναληπτικά το oracle κατάλληλες ερωτήσεις για την loc.

Για την επικοινωνία των προγραμμάτων μπορείτε να χρησιμοποιήσετε οποιαδήποτε μορφή interprocess communication (RPC) γνωρίζετε, ή ακόμα και απλούστερη επικοινωνία μέσω ενός αρχείου ή στην χειρότερη περίπτωση θα γίνεται εσωτερικά στο πρόγραμμα με κατάλληλη κλήση συνάρτησης. Η παραγωγή των κλειδιών και η αρχική κρυπτογράφηση μπορεί να γίνει από δικό σας κώδικα ή χρησιμοποιώντας ένα έτοιμο εργαλείο όπως το Openssl.

Άσκηση 5. 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 $g^s = yg^c h \mod p$.

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

Άσκηση 6. Να αποδείξετε ότι ένα σχήμα δέσμευσης δεν μπορεί να διαθέτει ταυτόχρονα τις ιδιότητες τέλειας δέσμευσης και τέλειας απόκρυψης.

Άσκηση 7. 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 8. Να δώσετε τις μη-διαλογικές αποδείξεις χρησιμοποιώντας την τεχνική Fiat-Shamir για τις παρακάτω ιδιότητες του πρωτοκόλλου ηλεκτρονικών ψηφοφοριών CGS97 που παρουσιάζεται στις διαφάνειες της ενότητας "Αποδείξεις Μηδενικής Γνώσης και Εφαρμογές":

- Ορθή αποκρυπτογράφηση (βλ. διαφάνεια 57)
- Εγκυρότητα αρνητικής ψήφου (βλ. διαφάνεια 58)

Άσκηση 9. Μία συνάρτηση σύνοψης $\mathcal{H} : \{0,1\}^* \rightarrow \{0,1\}^n$ 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 10.

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;

Σύντομες 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! Σε κάθε περίπτωση οι απαντήσεις πρέπει να είναι *αυστηρά ατομικές*.