Εθνικό Μετσόβιο Πολυτεχνείο
Σχολή Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών

Υπολογιστική Κρυπτογραφία

(ΣΗΜΜΥ, ΣΕΜΦΕ, ΑΛΜΑ, ΕΜΕ)

4η Σειρά Ασκήσεων

Προθεσμία παράδοσης: 11/02/2023

Άσκηση 1. Δίνονται οι παρακάτω παράμετροι ενός συστήματος υπογραφών:

- n είναι σύνθετος με άγνωστη παραγοντοποίηση.
- $k, s \in \mathbb{Z}_n^*$ τέτοια ώστε $s^2 \equiv -k \pmod{n}$.
- Συνάρτηση σύνοψης $\mathsf{H} : \{0,1\}^* \to \mathbb{Z}_n$.

Το κλειδί επαλήθευσης είναι το $\mathsf{vk} = k$ και το κλειδί υπογραφής είναι το $\mathsf{sk} = s$.
Η υπογραφή για κάποιο μήνυμα $m \in \{0,1\}^*$ είναι $\sigma = (x, y) \in \mathbb{Z}_n^2$.
Ο αλγόριθμος επαλήθευσης Vf είναι: $\mathsf{Vf}(\mathsf{pk}, m, \sigma) =_{\text{def}} x^2 + ky^2 \equiv \mathsf{H}(m) \pmod{n}$.
Ποιός είναι ο αλγόριθμος δημιουργίας υπογραφής Sign;

Άσκηση 2. Υλοποιήστε το σχήμα υπογραφών Schnorr σε γλώσσα προγραμματισμού της επιλογής σας. Η υλοποίηση να βασιστεί στην υποομάδα τάξης q της ομάδας ακέραιων mod (safe) πρώτο $p = 2q + 1$ όπου q: πρώτος. Ο κώδικάς σας θα πρέπει να γεννάει τις παραμέτρους της ομάδας και της υποομάδας, να βρίσκει κάποιον κατάλληλο γεννήτορα εκείνη τη στιγμή, και να υπογράφει με τυχαίο $t \in_R \mathbb{Z}_q^*$ (όπως περιγράφει το πρωτόκολλο) το SHA-512 hash ενός μηνύματος (κατά προτίμηση μεγάλου αρχείου). Επίσης, κατασκευάστε συνάρτηση που θα επαληθεύει την υπογραφή Schnorr (το πρόγραμμά σας δηλαδή θα πρέπει να υπογράφει και να επαληθεύει την υπογραφή του αρχείου). Εργασθείτε με το Fiat-Shamir challenge $c = \mathsf{H}(y||m)$ για το σχήμα υπογραφών Schnorr.

Άσκηση 3. Δίνεται μια ομάδα $\mathbb{G} = \langle g \rangle$ με τάξη q πρώτο, όπου το πρόβλημα απόφασης Diffie - Hellman είναι δύσκολο και $h \in \mathbb{G}$. Έστω το παρακάτω πρωτόκολλο. Οι δημόσιες παράμετροι είναι $\langle \mathbb{G}, g, q \rangle$ και ο prover γνωρίζει ένα x τέτοιο ώστε $g^x = h$.

- Ο prover επιλέγει ομοιόμορφα ένα $t \in \mathbb{Z}_q^*$ και στέλνει στον verifier το $y = g^t$.
- Ο verifier επιλέγει ομοιόμορφα $c \in \mathbb{Z}_q^*$ και το στέλνει στον prover.
- Ο prover υπολογίζει το $s = t + c + x \bmod q$ και το στέλνει στον verifier.

- Ο verifier αποδέχεται αν και μόνο αν $g^s = yg^c h$.

Είναι το παραπάνω πρωτόκολλο Σ-πρωτόκολλο, διαθέτει δηλαδή πληρότητα, ειδική ορθότητα, μηδενική γνώση για τίμιους επαληθευτές;

Άσκηση 4. Δίνεται μια ομάδα $\mathbb{G}$ με τάξη q πρώτο όπου το πρόβλημα απόφασης Diffie - Hellman είναι δύσκολο. Έστω g, h γεννήτορες της $\mathbb{G}$ τέτοιοι ώστε να είναι άγνωστοι οι διακριτοί λογάριθμοι $\log_g h$ και $\log_h g$. Σε αυτή την ομάδα ορίζουμε το σχήμα δέσμευσης του Pedersen με αλγόριθμο δέσμευσης $\mathsf{Commit}(m, r) = c = g^m h^r$ με $m, r \in \mathbb{Z}_q$.
Θεωρήστε το παρακάτω πρωτόκολλο Π με δημόσια είσοδο $\langle \mathbb{G}, g, h, q, c \rangle$ που αποδεικνύει ότι ο prover γνωρίζει m, r ώστε $c = g^m h^r$:

- Ο prover επιλέγει ομοιόμορφα ένα $t_1, t_2 \in \mathbb{Z}_q^*$ και στέλνει στον verifier το $t = g^{t_1} h^{t_2}$.
- Ο verifier επιλέγει ομοιόμορφα $e \in \mathbb{Z}_q^*$ και το στέλνει στον prover.
- Ο prover υπολογίζει το $s_1 = t_1 + em \bmod q$, $s_2 = t_2 + er \bmod q$ και τα στέλνει στον verifier.
- Ο verifier αποδέχεται αν και μόνο αν $g^{s_1} h^{s_2} = tc^e$.

1. Είναι το Π Σ-πρωτόκολλο, διαθέτει δηλαδή πληρότητα, ειδική ορθότητα, μηδενική γνώση για τίμιους επαληθευτές;
2. Είναι το Π witness indistinguishable; Δηλαδή με δεδομένο έναν τίμιο prover και κοινή δημόσια είσοδο $\langle \mathbb{G}, g, h, q, c \rangle$ τι συμπεράσματα μπορεί να βγάλει ένας κακόβουλος επαληθευτής, από τις συζητήσεις (t, e, s_1, s_2) για witness (m, r) και (t', e', s_1', s_2') για witness (m', r') με $m \neq m'$ και $r \neq r'$.
3. Αλλάζουμε το Π σε Π′, έτσι ώστε στο πρώτο βήμα ο prover υπολογίζει και στέλνει αντί για $t = g^{t_1} h^{t_2}$ τις τιμές $a = g^{t_1}$ και $b = h^{t_2}$. Ποια είναι η σχέση που πρέπει να ελέγξει ο verifier για να πειστεί ότι ο prover γνωρίζει m, r; Είναι το Π′ Σ-πρωτόκολλο;

Άσκηση 5. Μία συνάρτηση σύνοψης $\mathsf{H} : \{0,1\}^* \to \{0,1\}^n$ είναι ασφαλής για χρήση σε συστήματα proof of work (PoW) αν για κάθε είσοδο x είναι δύσκολο να βρεθεί λύση r ώστε να ισχύει $\mathsf{H}(x||r) \in Y$, 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 H' που είναι collision resistant, αλλά όχι ασφαλής για PoW, επεκτείνοντας μια συνάρτηση H που είναι collision resistant και ασφαλής για PoW.
2. Να δείξετε ότι η συνάρτηση $\mathsf{G}(z) = \mathsf{H}(z)||LSB(z)$, όπου $LSB(z)$ είναι το λιγότερο σημαντικό bit του z, είναι ασφαλής για PoW αλλά δεν έχει αντίσταση πρώτου ορίσματος.

Άσκηση 6.

1. Στο άρθρο Bitcoin: A Peer-to-Peer Electronic Cash System περιγράφεται το επιχείρημα του Satoshi Nakamoto για την ασφάλεια του πρωτοκόλλου Bitcoin απέναντι στην επίθεση double spending. Εξηγήστε συνοπτικά το επιχείρημά του.

2. Θεωρήστε το σενάριο στο οποίο υπάρχει μη αμελητέα καθυστέρηση στον χρόνο παράδοσης των block στο δίκτυο και αυξάνουμε τον ρυθμό παραγωγής των block ή το άνω φράγμα στο μέγεθος των block ώστε να υποστηρίζονται περισσότερες συναλλαγές το δευτερόλεπτο. Θα είναι τότε 50% το άνω φράγμα για το ποσοστό της υπολογιστικής ισχύος που μπορεί να κατέχουν οι κακόβουλοι χρήστες και ταυτόχρονα να αποφεύγεται η επίθεση double spending, ή θα μπορούσε ένας αντίπαλος με λιγότερο από 50% της συνολικής υπολογιστικής ισχύος να πετύχει στην επίθεση;

   Υπόδειξη: Μπορείτε να συμβουλευτείτε το άρθρο Secure High-Rate Transaction Processing in Bitcoin

Σε όλες τις ασκήσεις με "$\oplus$" συμβολίζουμε το XOR και με "||" την παράθεση.

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*.