Δημήτριος Κυριακίδης
el17077

Κρυπτογραφία
4η Φυλλάδιο Ασκήσεων

Άσκηση 2:

Τα χαρακτηριστικά που συνθέτουν μία απόδειξη μηδενικής γνώσης (ZPK) είναι τα εξής:

- πληρότητα: ο prover μπορεί να πείσει τον verifier, με υψηλή πιθανότητα, ότι πρόκειται για αληθή πρόταση.
- ορθότητα: ο verifier απορρίπτει τις λανθασμένες προτάσεις με υψηλή πιθανότητα.
- μηδενική γνώση: αυτά που έχει μάθει ο verifier μετά την επικοινωνία με τον prover, θα μπορούσε να τα είχε υπολογίσει χωρίς να λάβει μέρος σε αυτήν.

Οι πρώτες δύο ιδιότητες προφανώς ικανοποιούνται από το δοθέν πρωτόκολλο: εάν ο prover πράγματι γνωρίζει το *x*, τότε μπορεί να πείσει τον verifier για αυτό, και αν όχι, είναι απίθανο να το καταφέρει (η πιθανότητα είναι αμελητέα).

Η βασική ιδέα για την απόδειξη της μηδενικής γνώσης είναι ότι οι μοναδικές πληροφορίες που διακινούνται σε κάθε γύρο της συναλλαγής-επικοινωνίας μεταξύ των παικτών είναι οι τυχαίοι αριθμοί $y = g^t \ mod \ p, t \in \mathbb{Z}_m^*$ και $c \in \mathbb{Z}_m^*$, και το άθροισμα *s*. Ένας προσομοιωτής, λοιπόν, που παράγει τυχαίους αριθμούς από τον $\mathbb{Z}_m^*$, δίνει ένα πρακτικό επικοινωνίας το οποίο είναι υπολογιστικά μη διαχωρίσιμο από την επικοινωνία prover και verifier.

Άσκηση 3:

Εάν ένα σχήμα δέσμευσης (commitment) χαρακτηρίζεται από τέλεια δέσμευση (binding), τότε είναι απολύτως αδύνατον ο αποστολέας να αλλάξει την τιμή του ύστερα από την αποστολή. Για να αληθεύει αυτό, θα πρέπει η τιμή της συνάρτησης commit που έχει αποστείλει να αντιστοιχεί σε μοναδικό στοιχείο του πεδίου ορισμού της, ώστε ο αποστολέας να μην μπορεί να αλλάξει την τιμή στην οποία έχει δεσμευθεί χωρίς επίπτωση στο $c = commit(m, r) = g^m h^r \ mod \ p$. Αν, όμως, ισχύει αυτό, τότε από την πλευρά του παραλήπτη η υποκλοπή του μηνύματος ανάγεται σε λύση του DLP, η οποία είναι υπολογιστικώς δύσκολη μεν, όχι εντελώς ανέφικτη δε, και συνεπώς δεν υπάρχει τέλεια απόκρυψη (hiding).

Άσκηση 6:

Το σενάριο αυτό μπορεί να εμφανισθεί αν, κατά σύμπτωση, οι δύο miners ανακαλύψουν επόμενο block για την αλυσίδα ταυτοχρόνως, και συνεχίζουν να εργάζονται ο καθένας συνεχίζοντας το block αυτό που «εξόρυξε». Επειδή η εξόρυξη νέων blocks απαιτεί την εύρεση μιας λύσης σε πρόβλημα proof-of-work (στο $SHA256^2$), είναι, δηλαδή, υπολογιστικώς δύσκολη, είναι εξαιρετικά απίθανο οι δύο miners να συνεχίσουν να εξορύσσουν blocks με τον ίδιο ρυθμό για μεγάλο διάστημα. Κάποια στιγμή ο ένας από τους δύο θα έχει κατασκευάσει αλυσίδα μεγαλύτερου μήκους, και τότε το πρωτόκολλο του Bitcoin θα επιλέξει την μεγαλύτερη αλυσίδα ως την μοναδική έγκυρη.