Εργασία Κρυπτογραφίας– Απρίλιος 2023

Παράδοση: Παρασκευή 28/4/2023 1:00μμ

Οδηγίες:

- Όπου απαιτούνται πράξεις, θα πρέπει να εξηγείτε τους υπολογισμούς σας.
- Να απαντάτε στο ζητούμενο με σαφήνεια, και να εξηγείτε τη σκέψη σας.

1. Εξετάστε τις παρακάτω παραλλαγές για το σχήμα του Pedersen. Για κάθε μία ελέγξτε εάν διατηρούνται οι ιδιότητες της δέσμευσης και της απόκρυψης.

   (α□) Αλλάζουμε το χώρο μηνυμάτων $\mathcal{M}$ ώστε να γίνονται δεκτά μόνο $m \in \{0, 1\}$.

   (β□) Αλλάζουμε την επιλογή της τυχαίας τιμής r στην Com ώστε να έχουμε $r \leftarrow \{0, 1\}$.

   (γ□) Στις παραμέτρους, θέτουμε $h \leftarrow g$.

2. Μία παρέα φοιτητών θέλει να παίξει ένα επιτραπέζιο παιχνίδι, αλλά ανακαλύπτει ότι δεν έχει στη διάθεσή της εξάπλευρα ζάρια.

   Η Μαρία προτείνει να χρησιμοποιήσουν κέρματα ως εξής: αντί για ένα ζάρι θα ρίχνονται 3 ανεξάρτητα και αμερόληπτα κέρματα, όπου κάθε πλευρά με όψη «κεφάλι» θα ισοδυναμεί με 0 και κάθε πλευρά με όψη «γράμματα» θα ισοδυναμεί με 1. Το αποτέλεσμα θα είναι το άθροισμα των όψεων συν 2.

   Η Στέλλα, προτείνει να χρησιμοποιήσουν 5 κέρματα συν 1 (με τις ίδιες αξίες ανα όψη).

   (α□) Υπολογίστε τη μέση τιμή κάθε κατανομής: ζάρι, 3 κέρματα +2, 5 κέρματα +1.

   (β□) Με τη βοήθεια της στατιστικής απόστασης, υπολογίστε ποιά πρόταση είναι καλύτερη.

3. Στον ορισμό της απόκρυψης για σχήματα δέσμευσης (¶3.2 σελ 21) ζητάμε ο αντίπαλος να μην μπορεί να "μαντέψει" την τιμή του b Με πιθανότητα σημαντικά καλύτερη από $\frac{1}{2}$. Μπορούμε να περιγράψουμε την ιδιότητα της απόκρυψης με έναν εναλλακτικό τρόπο: ζητάμε κανένας (πολυωνυμικός) αντίπαλος να μην αλλάζει τη συμπεριφορά του ανάλογα με την τιμή του b. Για να το περιγράψουμε και τυπικά, ορίζουμε την παραλλαγή $hiddingattack_x^B$ ως το παιχνίδι $hiddingattack^B$ αλλά στη γραμμή 3 θέτουμε $d \leftarrow x$. Επίσης, ορίζουμε $out_{\mathcal{A}}(hiddingattack_b^B(1^\lambda))$ να είναι η τελευταία έξοδος του $\mathcal{A}$ σε αυτό το παιχνίδι.

   Τότε πλέον ορίζουμε την ιδιότητα απόκρυψη* ως εξής:

   $$|\text{Prob}[out_{\mathcal{A}}(hiddingattack_0^B(1^\lambda)) = 1] - \text{Prob}[out_{\mathcal{A}}(hiddingattack_1^B(1^\lambda)) = 1]| = \text{negl}(1^\lambda)$$

   (α□) Δείξτε ότι ο νέος ορισμός είναι ισοδύναμος με τον αρχικό.

4. Συχνά, οι κρυπτογραφικοί ορισμοί επιτρέπουν μια μικρή πιθανότητα ο αντίπαλος να λύσει κάποιο υπολογιστικό πρόβλημα. Δε δίνουν όμως εγγυήσεις για την κατανομή αυτής της πιθανότητας. Πχ μπορεί ένας αντίπαλος να λύνει κάθε εκδοχή του προβλήματος με πιθανότητα p ενώ ένας άλλος, να λύνει ένα κλάσμα $1/p$ των εκδοχών του προβλήματος με πιθανότητα 1. Δείξτε ότι στο πρόβλημα του διακριτού λογαρίθμου, αυτό το ζήτημα ουσιαστικά δεν υπάρχει.

   (α□) (Μόνο προπτυχιακοί). Έστω ένας πολυωνυμικός αλγόριθμος $\mathcal{E}$ ο οποίος υπολογίζει διακριτούς λογάριθμους με μη αμελητέα πιθανότητα p οταν ο διακριτός λογάριθμος του στοιχείου που δίνεται είναι άρτιος και με πιθανότητα 0 όταν είναι περιττός. Περιγράψτε έναν πολυωνυμικός αλγόριθμος που υπολογίζει διακριτούς λογαρίθμους με μη αμελητέα πιθανότητα για κάθε στοιχείο.

   (β□) Δείξτε τη γενική περίπτωση του παραπάνω: δηλαδή αν ισχύει[1] ότι $\text{Prob}[h \leftarrow \mathbb{G}; E(\mathbb{G}, g, q, h) = x : g^x = h] = p$, οπου p μη αμελητέο τότε μπορούμε να φτιάξουμε αλγόριθμο D ώστε $min_{h \in \mathbb{G}}(\text{Prob}[h \leftarrow \mathbb{G}; D(\mathbb{G}, g, q, h) = x : g^x = h]) = p'$, οπου p' μη αμελητέο.

[1] Για ευκολία έχουμε σταθεροποιήσει την επιλογή της ομάδας.