Key Exchange, Diffie Hellman & Pedersen

1. Δίνεται το παρακάτω σχήμα ανταλλαγής κλειδιού[1]:

   (α΄) Η Αλίκη επιλέγει τυχαία $k, r \leftarrow \{0,1\}^n$ και στέλνει στο Βασίλη την τιμή $s := k \oplus r$.

   (β΄) Ο Βασίλης επιλέγει τυχαίο $t \leftarrow \{0,1\}^n$ και στέλνει στην Αλίκη $u := s \oplus t$.

   (γ΄) Η Αλίκη υπολογίζει την τιμή $w := u \oplus r$ και τη στέλνει στο Βασίλη.

   (δ΄) Η Αλίκη χρησιμοποιεί την τιμή k και ο Βασίλης την τιμή $w \oplus t$.

   Να εξετάσετε το παραπάνω σχήμα ως προς την ορθότητα και την ασφάλεια.

2. Χρησιμοποιούμε δεσμεύσεις Pedersen για να υλοποιήσουμε τη ρίψη νομισμάτων. Στη συνηθισμένη εφαρμογή των δεσμεύσεων, ο πρώτος παίκτης αντί να φανερώσει το κέρμα του φανερώνει μια δέσμευση, την οποία ανοίγει αφού φανερώσει την τιμή του ο δεύτερος παίκτης.

   Κάποιος προτείνει να αλλάξουμε το πρωτόκολο ως εξής για μεγαλύτερη ασφάλεια: ο δεύτερος παίκτης, αντί να αποκαλύψει άμεσα την τιμή b, θα δώσει μία δέσμευση σε αυτήν. Κατόπιν, ο πρώτος παίκτης ανοίγει τη δεσμευσή του, μετά ο δεύτερος τη δική του και το πρωτόκολο τερματίζει κατά τα γνωστά. Οι παράμετροι για το σχήμα του Pedersen υποθέτουμε εδώ ότι προήλθαν από έμπιστο τρίτο πρόσωπο.

   Εξετάστε την επίπτωση της παραπάνω αλλαγής στο πρωτόκολο (πέρα από την ανάγκη για την ύπαρξη του τρίτου προσώπου).

[1] Άσκηση 9.3 (1η έκδοση)/ 10.4 (2η έκδοση) από το Katz & Lindell