

Key Exchange, Diffie Hellman & Pedersen

1. Δίνεται το παρακάτω σχήμα ανταλλαγής κλειδιού¹:

(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.

Λύση Η ορθότητα ισχύει με έλεγχο των πράξεων. Δεν είναι όμως ασφαλές. Υπολογίστε το $s \oplus u \oplus w$.

2. Στον πρώτο υποψήφιο ορισμό ασφαλείας για σχήματα ανταλλαγής κλειδιών, αναφέραμε ότι ένα σχήμα που είναι ασφαλές σύμφωνα με τον ορισμό, μπορεί στην πράξη να αποκαλύπτει όλο το κλειδί εκτός από $\log^2(\lambda)$ bits. Εξηγήστε από που προκύπτει το όριο (κατ'ελάχιστο, εξηγήστε γιατί δεν θα μπορούσαμε να αλλάξουμε το όριο σε $\log \lambda$).

Λύση Ας υποθέσουμε ότι ένα τέτοιο σχήμα αποκάλυπτε όλο το κλειδί εκτός από τα $\log n$ τελευταία bit. Θα μπορούσαμε να ψάξουμε για το πλήρες κλειδί με εξαντλητικό έλεγχο σε αυτά τα bit. Συνολικά θα πρέπει να εξετάσουμε $2^{\log \lambda}$ bits δηλαδή λ περιπτώσεις², δηλαδή πολυωνυμικές το πλήθος περιπτώσεις. Οπότε, αν κάθε μία δοκιμή μας παίρνει πολυωνυμικό χρόνο, θα μπορούσαμε να κάνουμε όλες τις απαραίτητες δοκιμές σε πολυωνυμικό χρόνο. Άρα υπολογίζουμε όλο το κλειδί.

Αντίθετα, αν υπολείπονται $\log^2(\lambda)$ bits, ο εξαντλητικός έλεγχος περιλαμβάνει $2^{\log^2(\lambda)} = \lambda^{\log \lambda}$ ελέγχους οι οποίοι είναι υπερ-πολυωνυμικοί το πλήθος (αφού το $\lambda^{\log \lambda}$ είναι μεγαλύτερο από οποιοδήποτε πολυώνυμο για μεγάλες τιμές του λ).

3. 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 δεσμευση, την οποία ανοίγει αφού φανερώσει την τιμή του ο δεύτερος παίκτης.

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

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

Λύση Η αλλαγή καταστρέφει την ασφάλεια του πρωτοκόλλου. Ο δεύτερος παίκτης μπορεί να εξαναγκάσει το πρωτόκολλο να βγάλει αποτέλεσμα 0. Ο πιο απλός τρόπος είναι απλά να επαναλάβει τη δεσμευση που έλαβε από τον πρώτο παίκτη, και να επαναλάβει το άνοιγμα που θα κάνει ο πρώτος παίκτης στο επόμενο βήμα. Αφού οι τιμές θα είναι ίδιες, το αποτέλεσμα της αποκλειστικής διάζευξης (XOR) θα είναι 0.

Η παραπάνω «επίθεση» γίνεται όμως εύκολα αντιληπτή. Ο πρώτος παίκτης θα θεωρήσει απίθανο να παράξει ο δεύτερος την ίδια ακριβώς δεσμευση (ειδικά εάν συμβεί παραπάνω από μία φορά). Για το λόγο αυτό, ο δεύτερος παίκτης μπορεί να πολλαπλασιάσει την αρχική δεσμευση με g^z για τυχαίο z , και όταν ανοίγει την (παραλλαγμένη πλέον) δεσμευση να προσθέσει z στο r που έδωσε ο πρώτος παίκτης ως άνοιγμα.

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

² Αν ο λογάριθμος δεν είναι με βάση το 2 πολλαπλασιάζουμε με κατάλληλη σταθερά