Σχήματα Δέσμευσης & Diffie Hellman

1. Η Καρολίνα και ο Λυκούργος χρησιμοποιούν το σχήμα δέσμευσης του Pedersen. Η Καρολίνα έχει ορίσει τις παραμέτρους και ο Λυκούργος της έχει στείλει τη δέσμευση c. Πριν γίνει οτιδήποτε άλλο, ο Λυκούργος διαπιστώνει ότι από τυπογραφικό λάθος στις σημειώσεις του, υπολόγισε την τιμή $g^m h^r$ αντί $g^r h^m$. Είναι δυνατό με τις ανάλογες διορθώσεις από τη μεριά της Καρολίνας να συνεχίσουν την επικοινωνία τούς ή πρέπει ο Λυκούργος να δημιουργήσει νέα δέσμευση;

   Λύση Ναι. Ουσιαστικά, πρόκειται για μια παραλλαγή του συστήματος. Μπορούμε να ελέγξουμε ότι οι αποδείξεις και για τις δύο ιδιότητες ασφάλειας (δέσμευση, απόκρυψη) μπορούν να επαναδιατυπωθούν με τυπικές μόνο αλλαγές.

2. Ο Λυκούργος αποφασίζει για καλό και για κακό να δημιουργήσει νέα δέσμευση c' έχοντας διορθώσει το λάθος στον υπολογισμό, αλλά για οικονομία χρόνου επαναχρησιμοποιεί την ίδια τιμή r. Δεδομένου ότι δεσμεύεται στο ίδιο μήνυμα με πριν (άρα και η τιμή m είναι ίδια), είναι σωστή η αποφασή του;

   Λύση Όχι. Θα έχει αποστείλει δύο δεσμεύσεις $c = g^m h^r$ και $c' = g^r h^m$ οι οποίες έχουν συγκεκριμμένη σχέση μεταξύ τους. Αυτό κατά κανόνα πρέπει να αποφεύγεται. Συγκεκριμμένα, στις δεσμεύσεις Pedersen, ο ορισμός του commit προβλέπει ότι το r θα είναι μια «φρέσκια» τιμή από το $\mathbb{Z}_q$ και όχι κάποια τιμή που δεν έχει χρησιμοποιηθεί. Αυτό έχει σαν αποτέλεσμα η απόδειξη της ασφάλειας να μη μας καλύπτει.

   Πέρα από τη θεωρητική διερεύνηση, θα δώσουμε και ένα συγκεκριμμένο υπολογισμό που μπορεί να εκτελέσει η Αλίκη: $q = c/(c'^t)$ όπου $h = g^t$. Το t της είναι γνωστό αφού αυτή έφτιαξε τις παραμέτρους. Άρα έχουμε:

$$
\begin{aligned}
q &= g^m h^r / (h^m g^r) \\
q &= g^m h^r h^{-tm} g^{-tr} \\
q &= g^m g^{tr} g^{-t^2 m} g^{-tr} \\
q &= g^{m+tr-t^2 m-tr} \\
q &= g^{m-t^2 m} \\
q &= g^{m(1-t^2)}
\end{aligned}
$$

   Με βάση το q, και αφού το $1 - t^2$ είναι γνωστό, η Αλίκη είναι σε θέση να ελέγξει αν το c περιέχει κάποια τιμή m^* ή όχι, παραβιάζοντας έτσι την ιδιότητα της απόκρυψης.

3. Χρησιμοποιούμε δεσμεύσεις Pedersen για να υλοποιήσουμε τη ρίψη νομισμάτων. 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).

   Λύση Η αλλαγή καταστρέφει την ασφάλεια του πρωτοκόλου. Ο δεύτερος παίκτης μπορεί να εξαναγκάσει το πρωτόκολο να βγάλει αποτέλεσμα 0. Ο πιο απλός τρόπος είναι απλά να επαναλάβει τη δέσμευση 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 δέσμευση (ειδικά εάν συμβεί παραπάνω από μία φορά). Για το

λόγο αυτό, ο δεύτερος παίκτης μπορεί να πολλαπλασιάσει την αρχική δέσμευση με g^z για τυχαίο z, και οταν ανοίγει την (παραλλαγμένη πλέον) δέσμευση να προσθέσει z στο r που έδωσε ο πρώτος παίκτης ως άνοιγμα.

4. 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.

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

5. 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 περιπτώσεις[2], 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 $2^{\log^2(\lambda)} = \lambda^{\log \lambda}$ έλεγχους οι οποίοι είναι υπερ-πολυωνυμικοί το πλήθος (αφού το $\lambda^{\log \lambda}$).

*. Θεωρήστε την εξής παραλλαγή του σχήματος του Pedersen: αντί $h := g^t, t \leftarrow \mathbb{Z}_q$ κατασκευάζουμε δύο παραμέτρους $h_1, h_2 := g^{t_1}, g^{t_2}, t_i \leftarrow \mathbb{Z}_q$ και υπολογίζουμε (για ζεύγος μηνυμάτων m_1, m_2) την δέσμευση ως $c := g^r {h_1}^{m_1} {h_2}^{m_2}$.

   Να εξετάσετε την ασφάλεια της παραλλαγής σε σχέση με το αρχικό σύστημα, πάντα υπό την υπόθεση ότι το DDH είναι δύσκολο.

[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