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;

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;

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 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).

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 $\lambda^{\log \lambda}$ είναι μεγαλύτερο από οποιοδήποτε πολυώνυμο για μεγάλες τιμές του λ).

6. Στη διάλεξη αναφερθήκαμε στο γεγονός ότι δεδομένης μίας ομάδας $\mathbb{G}$ τάξης q, όπου q πρώτος, παραγόμενη από το g, μια μεταβλητή A που ακολουθεί την κατανομή $K := g^{x \cdot y}$ όπου $x, y \leftarrow \mathbb{Z}_q$ και μια μεταβλητή B που ακουλουθεί την κατανομή $U := g^z$ όπου $z \leftarrow \mathbb{Z}_q$ έχουν μικρή στατιστική απόσταση. Επιβεβαιώστε αυτό τον ισχυρισμό.

[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

Λύση Θα χρησιμοποιήσουμε την στατιστική απόσταση. Για την ομοιόμορφη κατανομή U ξέρουμε ότι η πιθανότητα να πάρει οποιαδήποτε τιμή είναι $\frac{1}{q}$. Για την κατανομή K θα χρειαστεί να κάνουμε μια διερεύνηση, διαχωρίζοντας περιπτώσεις αν $A = g^0$ ή $A = g^t, t \neq 0$.

Για την περίπτωση $A = g^0$, έχουμε ότι $\Pr[A = g^0] = \Pr[x \cdot y = 0 \mod q, \text{όπου } x, y \leftarrow \mathbb{Z}_q]$. Χρησιμοποιώντας τη δεσμευμένη πιθανότητα, παίρνουμε περιπτώσεις για το x και έχουμε:

$$\begin{aligned}
&\Pr[x \cdot y = 0 \mod q, \text{όπου } y \leftarrow \mathbb{Z}_q | x = 0] \cdot Pr[x = 0 \mod q] + \\
&\Pr[x \cdot y = 0 \mod q, \text{όπου } y \leftarrow \mathbb{Z}_q | x \neq 0] \cdot Pr[x \neq 0 \mod q] \\
=&\Pr[x \cdot y = 0 \mod q, \text{όπου } y \leftarrow \mathbb{Z}_q | x = 0] \cdot \frac{1}{q} + \Pr[x \cdot y = 0 \mod q, \text{όπου } y \leftarrow \mathbb{Z}_q | x \neq 0] \cdot \frac{q-1}{q} \\
=&1 \cdot \frac{1}{q} + \Pr[y = 0 \mod q, \text{όπου } y \leftarrow \mathbb{Z}_q] \cdot \frac{q-1}{q} \\
=&\frac{1}{q} + \frac{1}{q} \cdot \frac{q-1}{q} \\
=&\frac{q}{q^2} + \frac{q-1}{q^2} = \frac{2q-1}{q^2}
\end{aligned}$$

Για την περίπτωση $A = g^t$, $t \neq 0 \mod q$ εργαζόμαστε αντίστοιχα: $\Pr[A = g^t] = \Pr[x \cdot y = t \mod q, \text{όπου } x, y \leftarrow \mathbb{Z}_q]$. Χρησιμοποιούμε πάλι δεσμευμένη πιθανότητα στο x για να πάρουμε περιπτώσεις: αν το x είναι 0, η εξίσωση $0 \cdot y = t \mod q$ είναι αδύνατη, αλλιώς έχει λύση (ως προς το y) $y = t \cdot x^1 \mod q$. Άρα έχουμε:

$$\begin{aligned}
&\Pr[x \cdot y = t \mod q, \text{όπου } y \leftarrow \mathbb{Z}_q | x = 0] \cdot Pr[x = 0 \mod q] + \\
&\Pr[x \cdot y = t \mod q, \text{όπου } y \leftarrow \mathbb{Z}_q | x \neq 0] \cdot Pr[x \neq 0 \mod q] \\
&= 0 \cdot \frac{1}{q} + \Pr[y = t \cdot x^{-1} \mod q, \text{όπου } y \leftarrow \mathbb{Z}_q | x \neq 0] \cdot Pr[x \neq 0 \mod q] \\
&= 0 \cdot \frac{1}{q} + \Pr[y = t \cdot x^{-1} \mod q, \text{όπου } y \leftarrow \mathbb{Z}_q | x \neq 0] \cdot \frac{q-1}{q} \\
&= 0 \cdot \frac{1}{q} + \frac{1}{q} \cdot \frac{q-1}{q} \quad \text{η πιθανότητα το y να πετύχει τη σωστή τιμή είναι } 1/q \\
&= \frac{q-1}{q^2}
\end{aligned}$$

Πλέον είμαστε σε θέση να υπολογίσουμε τη στατιστική απόσταση, η οποία θα είναι:

$$\begin{aligned}
\Delta =&\frac{1}{2} \cdot \sum_{0}^{q-1} \left| \Pr[A = g^i] - \Pr[B = g^i] \right| \\
=&\frac{1}{2} \cdot \left| \frac{2q-1}{q^2} - \frac{q}{q^2} \right| + \frac{1}{2} \cdot \sum_{1}^{q-1} \left| \Pr[A = g^i] - \Pr[B = g^i] \right| \\
=&\frac{1}{2} \cdot \frac{q-1}{q^2} + \frac{1}{2} \cdot (q-1) \cdot \left| \frac{q-1}{q^2} - \frac{q}{q^2}] \right| \\
=&\frac{1}{2} \cdot \frac{q-1}{q^2} + \frac{1}{2} \cdot (q-1) \cdot \frac{1}{q^2} \\
=&\frac{q-1}{q^2} \approx \frac{1}{q}
\end{aligned}$$

Άρα, για τις συνηθισμένες περιπτώσεις όπου η τάξη της ομάδας είναι εκθετική[3] ως προς το μήκος της

[3] ή απλά υπερ-πολυωνυμική

αναπαράστασης των στοιχείων, η απόσταση είναι αμελητέα.

7. Κατά τη διαδικασία ανταλλαγής κλειδιού, είναι πιθανό να καταλήξουμε σε ένα κλειδί διαφορετικής μορφής από αυτό που θα θέλαμε να χρησιμοποιήσουμε. Σε ένα παράδειγμα από τις σημειώσεις, η διαδικασία ανταλλαγής κλειδιού μας δίνει ένα τυχαίο στοιχείο του $\mathbb{Z}_q$, ενώ εμείς θα επιθυμούσαμε μια συμβολοσειρά από bits. Διατυπώστε ένα απλό αλγόριθμο για να μετατρέψουμε τον ένα ακέραιο από το 0 ως το $q-1$ σε μια συμβολοσειρά από bits με το μέγιστο δυνατό[4] μήκος. Κατόπιν υπολογίστε τη στατιστική απόσταση των συμβολοσειρών που παράγονται σε σχέση με την ομοιόμορφη κατανομή για το ίδιο μήκος.

   Λύση Η απλούστερη μέθοδος είναι να θεωρήσουμε απλά τα ψηφία του αριθμού στο δυαδικό. Αυτά θα είναι $n = \lceil \log q \rceil$ το πλήθος. Θα συγκρίνουμε λοιπόν την κατανομή που έχουν τα ψηφία από αυτο τον αλγόριθμο, με την ομοιόμορφη κατανομή στο $[0, \ldots, B-1]$, όπου $B = 2^n$.

   Η πιθανότητα να πάρει μια μεταβλητή A που ακολουθει την κατανομή του αλγορίθμου είναι:

$$Pr[A = t] = \begin{cases} \frac{1}{q}, \text{ αν } t < q \\ 0, \text{ αλλιώς} \end{cases}$$

   Οπότε εύκολα υπολογίσουμε τη στατιστική απόσταση από μια μεταβλητή Y που ακολουθεί την ομοιόμορφη στο $[0, \ldots, B-1]$:

$$\begin{aligned} \Delta =& \frac{1}{2} \sum_{0}^{B-1} |Pr[A = t] - Pr[Y = t]| \\ =& \frac{1}{2} \sum_{0}^{q-1} |Pr[A = t] - Pr[Y = t]| + \frac{1}{2} \sum_{q}^{B-1} |Pr[A = t] - Pr[Y = t]| \\ =& \frac{q}{2} \cdot (\frac{1}{q} - \frac{1}{B}) + \frac{B-q}{2} \cdot (\frac{1}{B} - 0) \\ =& \frac{1}{2} \left(1 - \frac{q}{B} + 1 - \frac{q}{B}\right) = 1 - \frac{q}{B} \end{aligned}$$

   Άρα η στατιστική απόσταση είναι μικρή μόνο όταν το q είναι κοντά στην επόμενη μεγαλύτερη δύναμη του 2. Διαφορετικά, η απόσταση μπορεί να είναι έως και $\frac{1}{2}$.

8. Σε συνέχεια της προηγούμενης άσκησης, έστω ότι έχουμε κατασκευάσει μία διαδικασία που παράγει συμβολοσειρές s bits μήκους λ σύμφωνα με μια κατανομή S που είναι δ-κοντά στην ομοιόμορφη στο $\{0,1\}^\lambda$. Να δείξετε ότι για ένα οποιοδήποτε ψηφίο s_i $(0 \leq i < \lambda)$ αυτών των συμβολοσειρών, ισχύει ότι η κατανομή που ακολουθεί το ψηφίο, έστω S_i είναι δ-κοντα στην ομοιόμορφη κατανομή στο $\{0,1\}$;

*. 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.

   Σκιαγράφηση Αν το DDH είναι δύσκολο, τότε είναι δύσκολο και το DLog. Για την ιδιότητα της απόκρυψης, η απόδειξη των σημειώσεων ισχύει με τυπικές μόνο αλλαγές. Ουσιαστικά το g^r «αναγκάζει» τα c να έχουν την ομοιόμορφη κατανομή. Για την ιδιότητα της δέσμευσης, η απόδειξη χρειάζεται ουσιαστικές αλλαγές. Τις σημειώνουμε περιληπτικά. Η βασικότερη αλλαγή έχει να κάνει με την αναγωγή

[4] Δεν μας ενδιαφέρει να προσθέσουμε τετριμμένα bits που θα είναι σταθερά 0 ή 1

στο DLog: Ο αντίπαλος $\mathcal{B}$ που θα κατασκευάσουμε για το Dlog θα είναι υποχρεωμένος να δεχθεί ένα ζευγος g, h και να δώσει με καλή πιθανότητα το $\log_g h$. Στην αρχική απόδειξη τα ίδια g, h τα χρησιμοποιούσαμε αυτούσια ως παραμμέτρους για το σχήμα δέσμευσης. Τώρα όμως πρέπει να προσθέσουμε ένα δευτερο h' το οποίο θα κατασκευάσουμε ως $h' = g^{t'}$ για τυχαίο t'. Άρα η πρώτη μας σκέψη είναι να χρησιμοποιήσουμε ως παραμέτρους τα g, h, h'.

Δυστυχώς, αυτό δεν αρκεί. Όταν ο αντίπαλος $\mathcal{A}$ δημιουργεί συγκρούσεις, μπορεί να επιλέξει να αγνοήσει τη συνιστώσα του h και να δώσει διαφορετικές τιμές μόνο σε αυτές των g, h' δηλαδή: m_a, m, r_a και m_b, m, r_b. Όταν κάνουμε υπολογισμούς, αυτό θα μας δώσει απλώς το λογάριθμο του h' ως προς το g τον οποίο ήδη ξέρουμε, και ο οποίος δε μας βοηθά στον υπολογισμό μας. Ευτυχώς, η λύση είναι απλή: με πιθανότητα $1/2$ δίνουμε ως παραμέτρους τα g, h, h' και με την ίδια πιθανότητα g, h', h. Αυτό το κάνουμε ελπίζοντας ότι ακόμα και ένας αντίπαλος που αγνοεί μια συνιστώσα θα επιλέξει τη συνιστώσα που μας εξυπηρετεί με πιθανότητα $1/2$. Το μόνο που μένει, είναι να δείξουμε ότι κανένας αντίπαλος δεν είναι δυνατό να μεταβάλει τη συμπεριφορά του ανάλογα με το αν βλέπει το g, h, h' ή το g, h, h' (ώστε να επιλέγει να αγνοήσει κάθε φορά άλλη συνιστώσα ανάλογα με την επιλογή μας). Αυτό δείχνεται απλά με τον υπολογισμό της στατιστικής απόστασης των δύο κατανομών η οποία είναι 0 από κατασκευή (τόσο το h όσο και το h' υπολογιζονται ως g^t για ανεξαρτητα $t \leftarrow \mathbb{Z}_q$).