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. 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[1], 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).

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

4. 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.

   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[2] ως προς το μήκος της αναπαράστασης των στοιχείων, η απόσταση είναι αμελητέα.

5. 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[3] 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 $\frac{1}{2}$.

[2] ή απλά υπερ-πολυωνυμική

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

6. 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 $\{0,1\}$;

   Εστω το σύνολο των συμβολοσειρών μήκους λ. Έστω $i \leq lambda$. Ορίζουμε B_0 το υποσύνολο του B του οποίου τα μέλη έχουν ως i ψηφίο το 0, και αντίστοιχα B_1. Είναι σαφές ότι $B = B_0 \cup B_1$ και επιπλέον $B_0 \cap B_1 = \emptyset$.

   Αν X είναι μια τυχαία μεταβλητή που ακολουθεί την S, τότε η μεταβλητή $Y = F(X)$ ακολουθεί την S_i, όπου $F(x) = 1$ όταν $x \in B_1$ και $F(X) = 0$ αλλιώς. Αντίστοιχα αν η U ακολουθεί την ομοιόμορφη στο B, τότε η $V = F(U)$ ακολουθεί την ομοιόμορφη στο $\{0,1\}$

   Υπολογίζουμε την στατιστική Δ απόσταση της Y από την V.

$$
\begin{aligned}
\Delta &= \frac{1}{2}\sum_{j=0}^{1} |\Pr[Y=j] - \Pr[V=j]| \\
&= \frac{1}{2}|\Pr[Y=1] - \Pr[U=1]| + \frac{1}{2}|\Pr[Y=0] - \Pr[V=0]| \\
&= \frac{1}{2}|\Pr[F(X)=1] - \Pr[F(U)=j]| + \frac{1}{2}|\Pr[F(X)=0] - \Pr[F(U)=0]| \\
&= \frac{1}{2}|\Pr[X \in B_1] - \Pr[U \in B_1]| + \frac{1}{2}|\Pr[X \in B_0] - \Pr[U \in B_0]| \\
&= \frac{1}{2}|\sum_{t \in B_1} \Pr[X=t] - \sum_{t \in B_1} \Pr[U=t]| + \frac{1}{2}|\sum_{t \in B_0} \Pr[X=t] - \sum_{t \in B_0} \Pr[U=t]| \\
&= \frac{1}{2}|\sum_{t \in B_1} (\Pr[X=t] - \Pr[U=t])| + \frac{1}{2}|\sum_{t \in B_0} (\Pr[X=t] - \Pr[U=t])| \\
&\leq \frac{1}{2}|\sum_{t \in B_1} |\Pr[X=t] - \Pr[U=t]|| + \frac{1}{2}|\sum_{t \in B_0} |\Pr[X=t] - \Pr[U=t]|| \\
&= \frac{1}{2}\sum_{t \in B_1} |\Pr[X=t] - \Pr[U=t]| + \frac{1}{2}\sum_{t \in B_0} |\Pr[X=t] - \Pr[U=t]| \\
&= \frac{1}{2}\sum_{t \in B} |\Pr[X=t] - \Pr[U=t]| \\
&\leq \delta
\end{aligned}
$$

*. 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.