Ομάδες, Στατιστική Απόσταση & Pedersen

1. Να δείξετε ότι το σύνολο των συμβολοσειρών μήκους 2 bit ("00","10","01","11",), με πράξη το XOR κατά συντεταγμένη, αποτελεί ομάδα.

   Λύση Ελέγχουμε ότι οι ιδιότητες της ομάδας ισχύουν:

   - Έστω ένα ζεύγος συμβολοσειρών "ab", "cd". Το αποτέλεσμα της πράξης μεταξύ τους θα είναι "ef" όπου $e = a$ XOR c και $f = b$ XOR d. Με έλεγχο του πίνακα τιμών της XOR επιβεβαιώνουμε ότι το XOR δύο bits είναι bit, οπότε θα ισχύει ότι το e και το f είναι bits.
   - Η μεταθετικότητα της ομάδας προκύπτει από το ότι το XOR είναι μεταθετικό, και η ιδιότητα διατηρείται κάνοντας πράξεις ανα συντεταγμένη (όπως παραπάνω)
   - Υπάρχει ουδέτερο στοιχείο και είναι το "00", αφού ισχύει ότι a XOR $0 = a$, και η ιδιότητα διατηρείται κάνοντας πράξεις ανα συντεταγμένη (όπως παραπάνω).

2. Να δείξετε ότι η παραπάνω ομάδα είναι μεταθετική αλλά όχι κυκλική.

   Λύση

   - Η μεταθετικότητα της ομάδας προκύπτει από το ότι το XOR είναι μεταθετικό.
   - Η ομάδα δεν είναι κυκλική: για κάθε συμβολοσειρά bits ισχύει ότι το XOR με τον εαυτό της παράγει μηδενικά. Άρα κάθε στοιχείο έχει τάξη το πολύ 2 $neq4$, οπότε δεν υπάρχει στοιχείο που να παράγει την ομάδα.

3. Βρείτε ένα στοιχείο που παράγει την ομάδα $\mathbb{Z}_{11}^*$ με πράξη τον πολλαπλασιασμό

4. Να υπολογίσετε το $123^{2023} \mod 23$.

   Λύση: Στη βάση εργαζόμαστε modulo 23 και, αφού ο p είναι πρώτος, λόγω του ΜΘF στον εκθέτη εργαζόμαστε modulo $23 - 1 = 22$. Άρα έχουμε $123^{2023} \equiv 8^{2023} \equiv 8^{43} \equiv 8^{21} \mod 23$. Συνεχίζουμε γράφοντας $8^{21} \equiv 2^{63} \equiv 2^{19} \equiv 64^3 \cdot 2 \equiv (-5)^3 \cdot 2 \equiv 25 \cdot (-10) \equiv 2 \cdot 13 \equiv 26 \equiv 3 \mod 23$

5. Να υπολογίσετε (προσεγγιστικά) το $\log_{10}(12345678901234567890123456789 0)$ καθώς και το $\log_2(12345678901234567890123456789 0)$. Δίνεται ότι $\log_2(10) \approx 3.3$

   Λύση: Το 12345678901234567890123456789 0 γράφεται: $1{\cdot}10^{29}+2{\cdot}10^{28}+\ldots+9{\cdot}10^1+0 \approx 10^{29}$, άρα ο λογαριθμός του με βάση το 10 είναι περίπου 29. Για το λογάριθμο με βάση το 2 εφαρμόζουμε τον τύπο αλλαγής βάσης όπου $log_b(a) = log_c(a) \cdot log_c(b)$, άρα έχουμε $\log_2(12345678901234567890123456789 0) \approx 29 \cdot 3.3 = 95.7$. (Ο κανονικός υπολογισμός δίνει τιμή περίπου 96.64).

6. Να υπολογίσετε το $\log_2 5 \mod 37$. Χρησιμοποιείστε τον αλγόριθμο Baby step, Giant step, ο οποίος δίνεται παρακάτω.

   Στον αλγόριθμο Baby step, Giant step, θέλουμε να λύσουμε την εξίσωση $g^x = h \mod p$ «σπάζοντας» τον άγνωστο λογάριθμο $0 \leq x < p - 1$ σε $x = b + S \cdot G$, όπου $S = \lceil \sqrt{(p-1)} \rceil$ και $b, G \leq S$.

   Για να το κάνουμε αυτό, ξαναγράφουμε την εξίσωση ως $g^{S \cdot B} \equiv h \cdot g^{-b}$, με αγνώστους το B και το b. Έτσι, μπορούμε να εξαντλήσουμε όλες τις περιπτώσεις, με $2S$ υπολογισμούς (και $O(n \log n)$ συγκρίσεις για ταξινόμιση), αντί τους $p - 1 = S^2$ υπολογισμούς της προφανούς λύσης.

   Παρατήρηση. Επειδή το 37 είναι πρώτος και $37 - 1 = 36$, η τάξη της πολλαπλασιαστικής ομάδας του $\mathbb{Z}_{37}^*$ είναι 36. Η τάξη του 2 ξέρουμε ότι διαιρεί το 36 και άρα υπάρχουν πολλές μη τετριμμένες περιπτώσεις για την τάξη του. Σε περίπτωση που η τάξη του 2 δεν είναι 36, τότε δεν παράγει όλη την ομάδα, άρα ενδέχεται το 5 να μην εμφανιστεί ως δυναμή του, και ο ζητούμενος λογάριθμος να μην υπάρχει.

   Λύση:

Παρατήρηση. Εμείς μπορούμε είτε να εξετάσουμε την τάξη του 2 πριν αρχίσουμε τους υπολογισμούς, είτε να τους κάνουμε γνωρίζοντας ότι ενδεχομένως δε θα προκύψει λύση. Για να ελέγξουμε την τάξη μπορούμε να δοκιμάσουμε τους διαιρέτες του 36: 2,3,4,6,9,12,18. Για συντομία, αρκεί να επιβεβαιώσουμε ότι $2^{12} \equiv 100 \equiv 26 \neq 1 \mod 37$ και $2^{18} \equiv -1 \neq 1 \mod 37$. (Οι πράξεις αναλυτικότερα βρίσκονται παρακάτω).

Αφού το 37 είναι πρώτος, η ομάδα μας έχει τάξη 36. Έστω x ο ζητούμενος λογάριθμος, τότε ο x θα γράφεται ως $b + G \cdot 6$ με $b, G \leq 5$. Οπότε θέλουμε να λύσουμε την εξίσωση $2^{b+6G} = 5 \mod 37$, ή ισοδύναμα: $2^b = 5 \cdot 2^{(-6)\cdot G}$.

Ετοιμάζουμε τις δυνάμεις του 2^6.

- Για $G = 0$ έχουμε $2^{6G} \equiv 1 \mod 37$
- Για $G = 1$ έχουμε $2^{6G} \equiv 64 \equiv -10 \equiv 27 \mod 37$ (Αφαιρούμε το $37 \cdot 2 = 74$ για να πάρουμε -10. Ως αποτέλεσμα κρατάμε το 26 που είναι ο αντιπρόσωπος της κλάσσης, αλλά όποτε εξυπηρετεί στις πράξεις το υπολογίζουμε και ως -10).
- Για $G = 2$ έχουμε $2^{6G} \equiv 64^2 \equiv (-10)^2 \equiv 100 \equiv -11 \equiv 26 \mod 37$ (Αρχίζουμε θεωρώντας στο 26 ως -10 για ευκολία στις πράξεις. Μετά αφαιρούμε $3 \cdot 37 = 111$.)
- Για $G = 3$ έχουμε $2^{6G} \equiv -10 \cdot (-11) \equiv 110 \equiv -1 \equiv 36 \mod 37$
- Για $G = 4$ έχουμε $2^{6G} \equiv -10 \cdot -1 \equiv 10 \mod 37$
- Για $G = 5$ έχουμε $2^{6G} \equiv -11 \cdot -1 \equiv 11 \mod 37$

Για να υπολογίσουμε τα πολλαπλάσια του 2^{-1}, πρώτα εκτελούμε την αντιστροφή: είτε υψώνουμε στην 35η είτε χρησιμοποιούμε ευκλείδια διαίρεση. Με την Ευκλείδια διαίρεση, έχουμε:

$$\begin{aligned} 37 &= 18 \cdot 2 + 1 \\ 1 &= 37 + (-18) \cdot 2 \\ 1 &\equiv 0 + (-18) \cdot 2 \mod 37 \end{aligned}$$

Άρα, ο αντίστροφος του 2 είναι ο $-18 \equiv 19$ και συνεχίζουμε με τις δυνάμεις του 19.

- Για $b = 0$ έχουμε $19^b \equiv 1 \mod 37$
- Για $b = 1$ έχουμε $19^b \equiv 19 \mod 37$
- Για $b = 2$ έχουμε $19^b \equiv 19 \cdot 19 \equiv 361 \equiv 361 - 370 \equiv -9 \equiv 28 \mod 37$.
- Για $b = 3$ έχουμε $19^b \equiv 19 \cdot (-9) \equiv -171 \equiv 185 - 171 \equiv 14 \mod 37$. (Χρησιμοποιούμε το ότι $37 \cdot 5 = 185$).
- Για $b = 4$ έχουμε $19^b \equiv (-9) \cdot (-9) \equiv 81 \equiv 81 - 74 \equiv 7 \mod 37$.
- Για $b = 5$ έχουμε $19^b \equiv (14) \cdot (-9) \equiv 148 - 126 \equiv 22 \mod 37$. (Χρησιμοποιούμε το ότι $37 \cdot 4 = 148$)

Έπειτα, πολλαπλασιάζουμε τις δυνάμεις του 19 επί 5.

- Για $b = 0$ έχουμε $5 \cdot 19^b \equiv 5 \mod 37$
- Για $b = 1$ έχουμε $5 \cdot 19^b \equiv 5 \cdot 19 \equiv 95 - 74 \equiv 21 \mod 37$
- Για $b = 2$ έχουμε $5 \cdot 19^b \equiv 5 \cdot 28 \equiv 140 - 111 \equiv 29 \mod 37$.
- Για $b = 3$ έχουμε $5 \cdot 19^b \equiv 5 \cdot 14 \equiv 70 - 37 \equiv 33 \mod 37$.
- Για $b = 4$ έχουμε $5 \cdot 19^b \equiv 5 \cdot 7 \equiv 35 \mod 37$.

- Για $b = 5$ έχουμε $5 \cdot 19^b \equiv 5 \cdot 22 \equiv 110 - 74 \equiv 36 \mod 37$.

Συγκρίνοντας τις λίστες, βλέπουμε ότι για $G = 3, b = 5$ έχουμε και στις δύο, την τιμή 36. Δηλαδή:

$$2^{18} \equiv 5 \cdot 2^{-5} \mod 37 \quad \text{οπότε,}$$
$$2^{23} \equiv 5 \mod 37$$

7. 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.

8. 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:

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

   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.

9. Για τους παρακάτω αλγορίθμους, να υπολογιστεί η στατιστική απόσταση της εξόδου τους από την ομοιόμορφη κατανομή U στο $S = \{0, 1, 2, \ldots, A - 1\}$.

Sampler 1. $n := \lceil \log_2 A \rceil$
$x_0, x_1, \ldots, x_{n-1} \leftarrow \{0, 1\}$
$y := \sum_{i=0}^{n-1} 2^i \cdot x_i$
return y

Sampler 2. $x_0, x_1, \ldots, x_{A-1} \leftarrow \{0,1\}$
$y := \sum_{i=0}^{A-1} x_i$
return y

Υπόδειξη: Γνωρίζουμε ότι για τη διωνυμική ο μέσος όρος $E(X)$ είναι $n \cdot p = \frac{A}{2}$, και η διακύμανση $Var[X]$ είναι $n \cdot p \cdot q = \frac{A}{4}$. Επιπλέον, από τις σημειώσεις, ανατρέξτε στην ανισότητα του Chebychev (2.5.2):

$$\Pr[|X - E(X)| \geq t] \leq \frac{Var[X]}{t^2}$$

Sampler 3. $n := \lceil \log_2 A \rceil$
repeat:
$x_0, x_1, \ldots, x_{n-1} \leftarrow \{0,1\}$
$y := \sum_{i=0}^{n-1} 2^i \cdot x_i$
if $y < A$: return y

Υπόδειξη: Αρκεί να υπολογίσουμε ένα φράγμα ώστε να εκτιμήσουμε αν η απόσταση είναι σημαντική ή όχι. Χρησιμοποιήστε την έννοια της δεσμευμένης πιθανότητας.

Sampler 1. Ορίζουμε $B = 2^n$, και ελέγχουμε ότι η έξοδος του sampler είναι μια τυχαία μεταβλητή Y που ακολουθεί την ομοιόμορφη κατανομή στο $\{0, 1, 2, \ldots, B-1\}$. Παρατηρούμε επίσης ότι $B \geq A$, άρα το σύνολο τιμών της Y υπερκαλύπτει αυτό της U. Από τον ορισμό της στατιστικης απόστασης έχουμε:

$$\begin{aligned}
\Delta(U,Y) =& \frac{1}{2}\sum_{i=0}^{B} |\Pr(U=1) - \Pr(Y=i)| \\
&= \frac{1}{2}\sum_{i=0}^{A} |\Pr(U=1) - \Pr(Y=i)| + \frac{1}{2}\sum_{i=A}^{B} |\Pr(U=1) - \Pr(Y=i)| \\
&= \frac{1}{2}\sum_{i=0}^{A} \left| \frac{1}{A} - \frac{1}{B} \right| + \frac{1}{2}\sum_{i=A}^{B} \left| 0 - \frac{1}{B} \right| \\
&= \frac{1}{2}A \left| \frac{1}{A} - \frac{1}{B} \right| + \frac{1}{2}(B-A) \left| 0 - \frac{1}{B} \right| \\
&= \frac{1}{2}A \left(\frac{1}{A} - \frac{1}{B} \right) + \frac{1}{2}(B-A)\frac{1}{B} \\
&= \frac{1}{2} \left(\frac{A}{A} - \frac{A}{B} \right) + \frac{1}{2}\frac{B-A}{B} \\
&= \frac{1}{2} \left(1 - \frac{A}{B} + 1 - \frac{A}{B} \right) \\
&= 1 - \frac{A}{B}
\end{aligned}$$

Οπως αναμένουμε, όταν $A = B$ η στατιστική απόσταση είναι μηδενική, ενώ όταν $A = 2^k - 1$ η διαφορά είναι σχεδόν $\frac{1}{2}$. Όταν το A είναι κοντά στο B, παρατηρούμε επίσης ότι η απόσταση είναι αμελητέα ως προς το n.

Sampler 2. Αναγνωρίζουμε ότι η κατανομή Y του sampler είναι η διωνυμική με παραμέτρους $p = q = \frac{1}{2}$ και $n = A$ το πλήθος δοκιμές. Ξέρουμε ότι η κατανομή αυτή έχει σχήμα καμπύλης, άρα πιστεύουμε ότι μακριά από το μέσο όρο, θα εμφανίζει χαμηλή πιθανότητα. Αφού ο μέσος όρος είναι $p \cdot A = \frac{A}{2}$,

επιλέγουμε να εξετάσουμε τις τιμές από το $\frac{3A}{4}$ ως το A. Προφανώς για τη στατιστική απόσταση θα ισχύει ότι:

$$\begin{aligned}
\Delta(U,Y) =& \frac{1}{2}\sum_{i=0}^{A} |\Pr(U=1) - \Pr(Y=i)| \\
\geq& \frac{1}{2}\sum_{i=3A/4}^{A} |\Pr(U=1) - \Pr(Y=i)| \quad \text{(Παραλείπουμε θετικούς όρους, το άθροισμα δεν αυξάνεται)} \\
\geq& \frac{1}{2}\sum_{i=3A/4}^{A} (\Pr(U=1) - \Pr(Y=i)) \quad \text{(Αφαιρούμε απόλυτα, άρα το άθροισμα δεν αυξάνεται)} \\
=& \frac{1}{2}\sum_{i=3A/4}^{A} \Pr(U=1) - \frac{1}{2}\sum_{i=3A/4}^{A} \Pr(Y=i) \\
=& \frac{1}{2}\cdot\frac{1}{4} - \frac{1}{2}\sum_{i=3A/4}^{A} \Pr(Y=i) \\
=& \frac{1}{8} - \frac{1}{2}\sum_{i=3A/4}^{A} \Pr(Y=i)
\end{aligned}$$

Για να έχουμε λοιπόν μια εκτίμηση για την απόσταση, μένει να υπολογίσουμε (προσεγγιστικά) το άθροισμα πιθανοτήτων της Y για τιμές από $3A/4$ ως A, ή ισοδύναμα την πιθανότητα $P[Y >= \frac{3A}{4}]$. Από τις σημειώσεις γνωρίζουμε την ανισότητα του Chebychev:

$$\Pr[|Y - E(Y)| \geq t] \leq \frac{Var[Y]}{t^2}$$

Γνωρίζουμε ότι για τη διωνυμική ο μέσος όρος $E(Y)$ είναι $n \cdot p = \frac{A}{2}$, η διακύμανση $Var[Y]$ είναι $n \cdot p \cdot q = \frac{A}{4}$. Αντικαθιστούμε για $t = \frac{A}{4}$ και έχουμε:

$$\Pr[Y \geq \frac{3A}{4}] = \Pr[Y - \frac{A}{2} \geq \frac{A}{4}] = \Pr[Y - E(Y) \geq t] \leq \Pr[|Y - E(Y)| \geq t] \leq \frac{\frac{A}{8}}{\frac{A}{4}\cdot\frac{A}{4}} = \frac{\frac{1}{2}}{\frac{A}{4}} = \frac{1\cdot 4}{2\cdot A} = \frac{2}{A}$$

Επιστρέφοντας στο φράγμα για τη στασιστική απόσταση έχουμε ότι:

$$\begin{aligned}
\Delta(U,Y) =& \frac{1}{2}\sum_{i=0}^{A} |\Pr(U=1) - \Pr(Y=i)| \\
\geq& \frac{1}{8} - \frac{1}{2}\sum_{i=3A/4}^{A} \Pr(Y=i) \\
\geq& \frac{1}{8} - \frac{1}{2}\frac{2}{A} \\
=& \frac{1}{8} - \frac{1}{A}
\end{aligned}$$

Άρα για μεγάλες τιμές του Α, η στατιστική απόσταση είναι σημαντική, και αυξάνεται όσο μεγαλώνει το Α.

Παρατήρηση: Σε τρία σημεία της λύσης μπορούμε επικαλούμενοι τη συμμετρία να πάρουμε σημαντικά καλύτερες τιμές για τα φράγματα (περίπου 3 διπλασιασμούς). Πρώτα: μπορούμε να εξετάσουμε και το διάστημα από 0 έως $\frac{A}{4}$. Μετά: μπορούμε να ισχυριστούμε ότι αφού οι πιθανότητες και των δύο κατανομών αθροίζονται στο 1, η διαφορά που έχουν στο διάστημα $[0, A]$ θα είναι συνολικά 0, άρα η διαφορά στο κεντρικο διάστημα (χωρίς απόλυτη τιμή) θα είναι η αντίθετη της διαφοράς στα άκρα (οπότε εφαρμόζοντας την απόλυτη τιμή διπλασιάζουμε τη διαφορά που είχαμε). Τέλος, στην ανισότητα Chebychev φράξαμε την πιθανότητα να ξεπεράσουμε τα 3/4 με την πιθανότητα να απομακρυνθούμε από το 1/2 κατά 1/4 ή παραπάνω, η οποία λόγω συμμετρίας θα είναι περίπου διπλάσια.

Sampler 3. Θα κάνουμε χρήση της δεσμευμένης πιθανότητας. Οι τιμές του y επιλέγονται ομοιόμορφα από το $\{0, 1, 2, \ldots, B-1\}$ αλλά επιστρέφονται μόνο εάν ισχύει $y < A$. Ονομάζουμε Z την τυχαία μεταβλητή της εξόδου του sampler, και θεωρούμε την Y όπως στον πρώτο sampler. Από την κατασκευή του προγράμματος έχουμε ότι: $\Pr(Z = x) = \Pr(Y = x | Y < A)$. Από τον ορισμό της δεσμευμένης πιθανότητας:

$$\Pr(Y = x | Y < A) = \Pr(Y = x | x < A) = \frac{\Pr\left((Y = x) \cap (x < A)\right)}{\Pr(Y < A)}$$

Όταν $x >= A$ η παραπάνω πιθανότητα είναι μηδενική. Στη μη τετριμμένη περίπτωση όπου $x < A$, έχουμε:

$$\frac{\Pr(Y = x)}{\Pr(Y < A)} = \frac{\frac{1}{B}}{\frac{A}{B}} = \frac{1}{B} \cdot \frac{B}{A} = \frac{1}{A}$$

.

Άρα, για $x >= A$, $\Pr(Z = x) = 0$ και για $x < A$, $\Pr(Z = x) = \frac{1}{A}$, και η στατιστική απόσταση είναι προφανώς 0. Παρατηρούμε όμως ότι ο χρόνος εκτέλεσης δεν είναι σταθερός.

10. 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.

    Γνωρίζοντας από την προηγούμενη εβδομάδα ότι αυτή η παραλλαγή είναι ευπαθής σε replay attacks, εάν ο δεύτερος παίκτης απλώς επαναλάβει τη δέσμευση του πρώτου, θεωρούμε ότι χάνει χωρίς να υπολογίσουμε το XOR.

    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, άρα και μπορεί να «απαγορευτεί» όπως περιγράφουμε.

    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.