Εργασία Κρυπτογραφίας– Μάρτιος 2022

Οδηγίες:

- Όπου απαιτούνται πράξεις, θα πρέπει να εξηγείτε τους υπολογισμούς σας.
- Να απαντάτε στο ζητούμενο με σαφήνεια, και να εξηγείτε τη σκέψη σας.

Άσκηση 1 Με βάση όσα ξέρουμε από το μάθημα, ποιές από τις παρακάτω κατασκευές αποτελούν ομάδες κατάλληλες ως προς τη δομή τους για κρυπτογραφικές κατασκευές που βασίζονται στο DLOG[1] και το DDH, οπως το πρωτόκολο Diffie-Hellman; Αιτιολογήστε σε κάθε περίπτωση τις απαντήσεις σας (κατάλληλες και ακατάλληλες).

- Το σύνολο $\mathbb{Z}_p$ με p πρώτο και πράξη την πρόσθεση modulo p.
- Το σύνολο των συμβολοσειρών από bit μήκους $2k$. Ως πράξη ανάμεσα σε δύο συμβολοσειρές $s = (s_0, s_1, \ldots, s_{2k-1})$ και $t = (t_0, t_1, \ldots, t_{2k-1})$ θεωρούμε το $s * t := (s_0 \cdot t_0, s_1 \oplus t_1, s_2 \cdot t_2, t_3 \oplus s_3, \ldots, s_{2k-2} \cdot t_{2k-2}, s_{2k-1} \oplus t_{2k-1})$. Οπου $\cdot, \oplus$ θεωρήστε τον πολλαπλασιασμό ακεραίων και το XOR αντίστοιχα.

  Θεωρήστε ότι τα $\log(p), k$ είναι σχετικά μεγάλα ως προς την παράμετρο ασφαλείας που μας ενδιαφέρει.

Λύση

- Το Z_p με πράξη την πρόσθεση modulo p πράγματι αποτελεί κυκλική ομάδα με τάξη πρώτο (το p). Όμως, επειδή έχουμε ως πράξη την πρόσθεση, η εύρεση «διακριτού λογαρίθμου» στην ομάδα είναι στην πραγματικότητα «διαίρεση modulo p» στους ακέραιους. Αυτό επειδή όταν γράφουμε $h = g^a$ εννοούμε $h = g \bullet g \bullet g \ldots \bullet g$, όπου το g εμφανίζεται a φορές. Αφού όμως $\bullet = +$, έχουμε ότι $h = g \cdot a \mod p$. Άρα η ομάδα δεν είναι κατάλληλη αφού το DLOG είναι εύκολο.
- Αρχικά εξετάζουμε εάν το σύνολο αυτό όντως αποτελεί ομάδα.
  - Η κλειστότητα και η επιμεριστική ιδιότητα ισχύουν αφού ισχύουν κατά συντεταγμένη.
  - Ως ουδέτερο στοιχείο, παρατηρούμε ότι το $\epsilon := (1, 0, 1, 0, \ldots)$ έχει πράγματι την ιδιότητα $\epsilon * a = a$ για κάθε συμβολοσειρά a, με έλεγχο των πράξεων.
  - Παρατηρούμε ότι ο αντίστροφος δεν υπάρχει πάντα: συγκεκριμμένα, για μια συμβολοσειρά a με τιμή 0 σε θέση με άρτιο δείκτη, δεν υπάρχει συμβολοσειρά b ώστε $a * b$ να έχει αποτέλεσμα ϵ: το ϵ έχει τιμή 1 σε κάθε άρτια θέση, οπότε στην επίμαχη θέση, έστω i θα πρέπει να έχουμε $a_i \cdot b_i = \epsilon_i$, δηλαδή $0 \cdot b_i = 1$.

  Άρα, χωρίς την ύπαρξη αντιστρόφου, το παραπάνω σύνολο δεν αποτελεί ομάδα.

Άσκηση 2 Να εκτελέσετε τους παρακάτω υπολογισμούς στους ακέραιους $\mod 7$:

[1] Αφού αλλάζει η πράξη της ομάδας, η δράση που αντιστοιχεί στο DLOG δεν είναι απαραίτητα ο λογάριθμος.

$$
\begin{aligned}
2^3 &\mod 7\\
20^{30} &\mod 7\\
2^{-1} &\mod 7\\
2^{-2} &\mod 7\\
(-2)^{-2} &\mod 7\\
-2^{-2} &\mod 7\\
2^{1/5} &\mod 7\\
(1/5)^2 &\mod 7\\
(1/5)^{-1/5} &\mod 7
\end{aligned}
$$

Υπενθύμιση Όταν γράφουμε $1/a$ εννούμε b τέτοιο ώστε $a \cdot b = 1$. Αντίστοιχα, όταν γράφουμε Όταν γράφουμε $g^{1/a}$ εννούμε h τέτοιο ώστε $h^a = g$.

Λύση.

Αρχικά, παρατηρούμε ότι το 7 είναι πρώτος, άρα το $\mathbb{Z}_7^*$ είναι ομάδα ως προς τον πολλαπλασιασμό, με τάξη 6.

$$
\begin{aligned}
2^3 &\mod 7 =\\
8 &\mod 7 =\\
1 &\mod 7
\end{aligned}
$$

$$
\begin{aligned}
20^{30} &\mod 7 =\\
= 6^{30} &\mod 6 \mod 7 = \text{Αλλάζουμε τη βάση με ισοδύναμο.}\\
= 20^{30} &\mod 6 \mod 7 = \text{ Εφόσον η βάση δεν είναι 0, είναι στοιχείο της ομάδας άρα έχει τάξη που διαιρεί το 6.}\\
= 20^0 &\mod 7 =\\
= 1 &\mod 7
\end{aligned}
$$

Για το $2^{-1} \mod 7$ χρησιμοποιούμε ευκλείδια διαίρεση[2]:

$$
\begin{aligned}
&7 = 3 \cdot 2 + 1\\
&1 = 1 \cdot 7 + (-3) \cdot 2 \quad \text{(Μετακινούμε το τελικό υπόλοιπο στα αριστερά.)}\\
&1 = 0 + (-3) \cdot 2 \mod 7 \quad \text{(Εργαζόμαστε πλέον modulo 7 αντί στους ακέραιους.)}\\
&1 = 4 \cdot 2 \mod 7
\end{aligned}
$$

[2]Μπορούμε επίσης, αφού η τάξη της ομάδας είναι 6 να υψώσουμε στην $5 = -1 \mod 6$.

$$\begin{aligned} 2^{-2} \mod 7 &= \\ (2^{-1})^2 \mod 7 &= \\ 4^2 \mod 7 &= \\ 16 \mod 7 &= \\ 2 \mod 7 &= \end{aligned}$$

Για το $(-2)^{-2} \mod 7$ αρκεί να παρατηρήσουμε ότι $a^2 = (-a)^2$, αλλά θα επιλέξουμε να κάνουμε πράξεις:

$$\begin{aligned} (-2)^{-2} \mod 7 &= \\ (5)^4 \mod 7 &= \quad \text{(Η τάξη της ομάδας είναι 6, άρα στον εκθέτη εργαζόμαστε mod 6.)} \\ 25 \cdot 25 \mod 7 &= \\ 4 \cdot 4 \mod 7 &= \\ 16 \mod 7 &= \\ 2 \mod 7 & \end{aligned}$$

$$\begin{aligned} -2^{-2} \mod 7 &= \\ -2 \mod 7 &= \quad \text{(Από τα προηγούμενα.)} \\ 5 \mod 7 & \end{aligned}$$

Για το $2^{1/5} \mod 7$ θα πρέπει να αντιστρέψουμε το 5 modulo την τάξη της ομάδας[3], 6. Χρησιμοποιούμε ευκλειδια διαίρεση:

$6 = 1 \cdot 5 + 1$, άρα $1 = 6 + (-1) \cdot 5$, άρα αντίστροφος του 5 είναι το $-1 \mod 6$ δηλαδή το 5.

Άρα $2^{1/5} \mod 7 = 2^5 \mod 7 = 32 \mod 7 = 4 \mod 7$.

Για το $(1/5)^2 \mod 7$ εκτελούμε πρώτα ευκλείδια διαίρεση:

$$\begin{aligned} 7 &= 1 \cdot 5 + 2 \\ 5 &= 2 \cdot 2 + 1 \\ 1 &= 5 - 2 \cdot 2 \\ 1 &= 5 - 2 \cdot (7 - 5) \\ 1 &= 3 \cdot 5 + (-2) \cdot 7 \\ 1 &= 3 \cdot 5 + 0 \mod 7 \\ 1/5 &= 3 \mod 7 \end{aligned}$$

Άρα $(1/5)^2 \mod 7 = 3^2 \mod 7 = 2 \mod 7$. Εναλακτικά, μπορούμε να υπολογίσουμε το $5^{-2} = 5^4 \mod 7$.

[3] Από τα προηγούμενα μπορούμε να παρατηρήσουμε ότι το στοιχείο 2 έχει τάξη 3, οπότε οι πράξεις θα ήταν λίγο απλούστερες

$$
\begin{aligned}
(1/5)^{-1/5} &\mod 7 \\
3^{-5} &\mod 7 \text{Γνωρίζουμε τους αντίστροφους από τα προηγούμενα} \\
3^{6-5} &\mod 7 \text{Στον εκθέτη εργαζόμαστε modulo 6} \\
3 &\mod 7
\end{aligned}
$$

Άσκηση 3 Έστω μία συνάρτηση $\text{GGen}(1^\lambda)$ με έξοδο $(\mathbb{G}, g, q)$, όπου $\mathbb{G}$ μία κυκλική ομάδα $\mathbb{G} = \langle g \rangle$ με τάξη q: πρώτο και στην οποία θεωρούμε ότι το πρόβλημα DDH είναι δύσκολο. Εξετάζουμε μία παραλλαγή του σχήματος δέσμευσης του Pedersen $(\text{Param}, \text{Commit}, \text{Verify})$, με χώρο μηνυμάτων $\mathcal{M} := \mathbb{Z}_q^2$.

Στην παραλλαγή αυτή, ένα μήνυμα είναι ένα ζευγάρι τιμών $m, n \mod q$.

- $\text{Param}(1^\lambda) : (\mathbb{G}, g, q) \leftarrow \text{GGen}(1^\lambda); t \leftarrow \mathbb{Z}_q; z \leftarrow \mathbb{Z}_q; h_1 \leftarrow g^t; h_2 \leftarrow g^z;$ return $(b := (\mathbb{G}, g, q, h_1, h_2)$.
- $\text{Commit}(b, (m, n)) : r \leftarrow \mathbb{Z}_q; c \leftarrow g^r h_1^m h_2^n;$ return (r, c)
- $\text{Verify}(b, (m, n), c, r) : c^* \leftarrow g^r h_1^m h_2^n;$ return $(c == c^*)$

(α) Εξετάστε αν η ιδιότητα της δέσμευησης ισχύει υπολογιστικά, στατιστικά ή τέλεια.
Υπόδειξη: Δεν είναι απαραίτητο μια αναγωγή να «πετυχαίνει» με πιθανότητα ακριβώς 1. Είναι αρκετό να πετυχαίνει με μη αμελητέα πιθανότητα.

(β) Εξετάστε εάν η ιδιότητα της δέσμευσης πλήττεται εάν το b ορίζεται από τον παίκτη που δημιουργεί τη δέσμευση.

(γ) Εξετάστε εάν η παραπάνω κατασκευή ικανοποιεί την ιδιότητα της απόκρυψης (με χρήση στατιστικής απόστασης, αναγωγής ή επίθεσης) όταν το b ορίζεται από τον παίκτη που δέχεται τη δέσμευση.

Λύση.

- Η δέσμευση ισχύει με παρόμοιο τρόπο με το αρχικό σχήμα, αλλά η αναγωγή είναι λίγο πιο περίπλοκη. Μια πρώτη παρατήρηση είναι ότι ενώ στο DLOG μας δίνονται 2 στοιχεία, g, h εμείς πρέπει να δώσουμε στον αντίπαλο μέσω του b μια τριάδα g, h_1, h_2.

  Μια απλή πρόταση θα ήταν να θέσουμε $h_1 = h_2 = h$. Αυτό, αν και δεν απαγορεύεται από το σχήμα δέσμευσης σημαίνει ότι δεν δίνουμε στον $\mathcal{A}$ την ίδια κατανομή με το κανονικό σχήμα, και άρα η συμπεριφορά του ενδέχεται να αποκλίνει, ειδικά ως προς το ποσοστό επιτυχίας.

  Μια δεύτερη πρόταση είναι να θέσουμε $h_1 = h, h_2 = h^s$ για τυχαίο s. Έτσι, πετυχαίνουμε μια κατανομή στο b ίδια με αυτή που αναμένει ο $\mathcal{A}$. Όμως, υπάρχει και πάλι ένα ενδεχόμενο πρόβλημα: έστω μια σύγκρουση της μορφής $(r, m, n), (r, m', r')$, όπου δηλαδή το r είναι κοινό και για τα δύο ανοίγματα.

  Αυτό μας δίνει ότι:

$$g^r h_1^m h_2^n = g^r h_1^{m'} h_2^{n'} \tag{1}$$

$$h_1^{m-m'} = h_2^{n'-n} \tag{2}$$

$$h_2 = h_1^{\frac{m-m'}{n'-n}} \tag{3}$$

  Το οποίο όμως δε μας είναι χρήσιμο, και μας ήταν ήδη γνωστό αφού $h_2 = h_1^s$ από κατασκευή.

Μια τρίτη σκέψη, είναι να θέσουμε $h_1 = h, h_2 = g^s$ για τυχαίο s. Τότε, στο παραπάνω ενδεχόμενο, θα μπορούμε πράγματι να αντλήσουμε πληροφορία για τη σχέση των g, h. Όμως, ανακύπτει πρόβλημα στα ανοίγματα της μορφής $(r, m, n), (r', m, r')$.

Για να ολοκληρώσουμε την αρχική διερεύνηση, χρειάζεται μια παρατήρηση για να ανοίγματα που μας στέλνει ο αντίπαλος: πρέπει να έχουν μη-μηδενικές διαφορές σε τουλάχιστο δύο συντεταγμένες. Σε μηδέν συντεταγμένες απαγορεύεται από τον ορισμό της δέσμευσης, οπότε εξετάζουμε την περίπτωση να υπάρχει διαφορά σε μόνο μία συντεταγμένη. Τότε, απλοποιώντας, θα πάρουμε μια σχέση της μορφής:

$$f^v = f^v$$

όπου $f \in g, h_1, h_2$ και $v \neq v \mod q$. Όμως, το f έχει τάξη q, άρα το παραπάνω είναι αδύνατο, αφού θα είχαμε $f^{|v-v'|} = f^0$ με $0 < |v - v'| < q$.

Άρα:

- Όποτε ο $\mathcal{A}$ κερδίζει, θα πρέπει να παράγει ανοίγματα με μη-μηδενικές διαφορές σε τουλάχιστο δύο συντεταγμένες.
- Δεν έχουμε τρόπο να εξαναγκάσουμε την επιλογή των συντεταγμένων που θέλουμε.
- Εάν ο αντίπαλος ανοίξει μόνο συντεταγμένες που είναι συνάρτηση ενός μόνο από τα ζητούμενα, π.χ. g, g^s, δεν μπορούμε να προχωρήσουμε.

Άρα, η αναγωγή μας πρέπει να δουλεύει τυχαιοκρατικά, "μαντεύοντας΄΄ ποιές συντεταγμένες θα ανοίξει ο $\mathcal{A}$ ενώ παράλληλα θα εξασφαλίζει ότι η είσοδος του $\mathcal{A}$ –δηλαδή το b είναι ανεξάρτητο της "μαντεψιάς". Το τελευταίο ζητούμενο ευτυχώς υπερκαλύπτεται από την απαίτηση το b της αναγωγής να έχει κατανομή ίδια με το πείραμα.

Η αναγωγή με πιθανότητα $\frac{1}{3}$ επιλέγει για τα g, h_1, h_2 του b:

- $(g, g^s, h), s \leftarrow \mathbb{Z}_q$ –Πετυχαίνει όταν η τρίτη συντεταγμένη έχει μη-μηδενική διαφορά.
- $(g, h, g^s), s \leftarrow \mathbb{Z}_q$ –Πετυχαίνει όταν η δευτερη συντεταγμένη έχει μη-μηδενική διαφορά.
- $(h, g, g^s), s \leftarrow \mathbb{Z}_q$ –Πετυχαίνει όταν η πρώτη συντεταγμένη έχει μη-μηδενική διαφορά.

Οπότε, εάν σε μία εκτέλεση ο αντίπαλος ανοίξει οποιεσδήποτε δύο θέσεις, έχουμε για κάθε μία από τις δύο θέσεις πιθανότητα $\frac{1}{3}$ *ανεξάρτητη* με την είσοδο και έξοδο του αντιπάλου να έχουμε χρησιμοποιήσει επιλογή που μας δίνει τρόπο υπολογισμού για τον διακριτό λογάριθμο του h.

Τελικά, αν ο αντίπαλος έχει πιθανότητα επιτυχίας a μη αμελητέα, η αναγωγή μας πετυχαίνει πιθανότητα $\frac{2a}{3}$.

- Η δέσμευση δεν ισχύει όταν ο παίκτης που θέτει τις παραμέτρους δημιουργεί τις δεσμεύσεις. Μια δέσμευση στο (m, n) θα είναι της μορφής $c = g^r h_1^m h_2^n$, ή ισοδύναμα $c = g^{r+t\cdot m+z\cdot n}$. Έστω $x = r + t \cdot m + z \cdot n$.

  Γνωρίζοντας τα t, z μπορεί να επιλέξει οποιοδήποτε μηνύμα $(m', n') \neq (m, n)$ και να υπολογίσει $r' := x - t \cdot m' + z \cdot n'$. Από κατασκευή, το $(m', n'), r'$ είναι ένα δεύτερο άνοιγμα της δέσμευσης c για μήνυμα (m', n') διαφορετικό από το (m, n).

  Η παραπάνω επίθεση δεν "παραβιάζει" την απόδειξη που δώσαμε παραπάνω. Η απόδειξη προϋποθέτει ότι ο έλεγχος των παραμέτρων είναι πέρα από τον αντίπαλλο $\mathcal{A}$, ενώ η επίθεση προυποθέτει το αντίθετο.

- Η απόκρυψη ισχύει τέλεια, ανεξάρτητα από το ποιός παράγει το b, όπως και στο αρχικό σύστημα. Έστω $b := (\mathbb{G}, g, q, h_1, h_2)$. Θέτω $t = \log_g h_1$ και $z = \log_g h_1$. Έστω ένα οποιοδήποτε μήνυμα (m, n). Τότε μια δέσμευση στο (m, n) θα είναι της μορφής $c = g^r h_1^m h_2^n$ για $r \leftarrow \mathbb{Z}_q$.

  Ξαναγράφοντας το c έχουμε $c = g^{r+t\cdot m+z\cdot n}$ ή $c = g^{\theta+r}$, όπου $\theta = t \cdot m + z \cdot n$ σταθερά. Με χρήση της στατιστικής απόστασης, βλέπουμε ότι η κατανομή του $c = g^{\theta+r}$ ταυτίζεται με την ομοιόμορφη στο $\mathbb{G}$.

Άρα, η κατανομή του c όταν $(m, n) = (m_0, n_0)$ είναι ίδια με αυτήν όταν $(m, n) = (m_1, n_1)$. Άρα, στο πείραμα της απόκρυψης μπορούμε να ισχυριστούμε ότι η είσοδος του αντίπαλου είναι ουσιαστικά ανεξάρτητη του d, αφού έχει την ίδια κατανομή είτε $d = 0$ είτε $d = 1$. Οπότε, ανεξάρτητη θα είναι και η έξοδος του $d*$, και άρα η πιθανότητα επιτυχίας του θα είναι ακριβώς $\frac{1}{2}$.