Τελική Εξέταση Κρυπτογραφίας – 23 Ιουνίου 2022

Οδηγίες:

- Απαντήστε και τα 3 (τρία) θέματα. Μέγιστη βαθμολογία είναι το 100.
- Για τους μεταπτυχιακούς φοιτητές υπάρχει επιπλέον ερώτημα με κατάλληλη ένδειξη.
- Μαζί με τα στοιχεία σας σημειώστε αν είστε προ/μεταπτυχιακός.
- Όπου απαιτούνται πράξεις, θα πρέπει να εξηγείτε τους υπολογισμούς σας.
- Να απαντάτε στο ζητούμενο με σαφήνεια, και να εξηγείτε τη σκέψη σας.
- Πριν αρχίσετε να λύνετε, διαβάστε όλα τα θέματα.

Θέμα 1 Στις παρακάτω ερωτήσεις επιλέξτε μία από τις υποψήφιες απαντήσεις. Σε περίπτωση που παραπάνω από μία απαντήσεις είναι αληθείς, σωστή είναι μόνο η ισχυρότερη.

(α΄) Στο μοντέλο του τυχαίου μαντείου:

i. Επιλέγεται μια τυχαιοκρατική συνάρτηση, όπου επιτρέπεται σε διαφορετικές κλήσεις με το ίδιο όρισμα να επιστρέψει διαφορετικές τιμές. Κατόπιν δίνεται η περιγραφή της συνάρτησης σε κάθε συμμετέχοντα στο πρωτόκολλο.

ii. Επιλέγεται με τυχαίο τρόπο μια (ντετερμινιστική) συνάρτηση. Κατόπιν δίνεται η περιγραφή της συνάρτησης σε κάθε συμμετέχοντα στο πρωτόκολλο.

iii. Επιλέγεται μια τυχαιοκρατική συνάρτηση, όπου επιτρέπεται σε διαφορετικές κλήσεις με το ίδιο όρισμα να επιστρέψει διαφορετικές τιμές. Σε κάθε συμμετέχοντα στο πρωτόκολλο δίνεται το δικαιωμα να κάνει κλήσεις στη συνάρτηση, αλλα όχι η περιγραφή της.

iv. Επιλέγεται με τυχαίο τρόπο μια (ντετερμινιστική) συνάρτηση. Σε κάθε συμμετέχοντα στο πρωτόκολλο δίνεται το δικαιωμα να κάνει κλήσεις στη συνάρτηση, αλλα όχι η περιγραφή της.

Το τυχαίο μαντείο υλοποιεί μια ντερμινιστική συνάρτηση: αν το ρωτήσουμε δύο φορές με το ίδιο όρισμα, θα πάρουμε την ίδια απάντηση. Η τυχαιότητα έχει να κάνει με την επιλογή της συνάρτησης.

[Μονάδες: 3, Λανθασμένες Απαντήσεις: -1]

(β΄) Πόσα στοιχεία έχει η μεγαλύτερη υποομάδα με τάξη πρώτο του $\mathbb{Z}_{23}^*$.

i. 23
ii. 22
iii. 11
iv. 10

Το $\mathbb{Z}_{23}^*$ έχει 22 στοιχεία, αλλά το 22 δεν είναι πρώτος. Το μεγαλύτερο υποπολλαπλάσιο του 22 που είναι πρώτος είναι το 11.

[Μονάδες: 3, Λανθασμένες Απαντήσεις: -1]

(γ΄) Σε μία ομάδα $\mathbb{G}$, δίνεται ένα στοιχείο g με μεγάλη τάξη. Ποιο από τα παρακάτω είναι το καλύτερο κάτω φράγμα για τους πολλαπλασιασμούς που χρειάζονται για τον υπολογισμο του g^{15}; Θεωρήστε ότι οι τετραγωνισμοί έχουν ίδιο κόστος με τους πολλαπλασιασμούς.

i. 14
ii. 8

iii. 6

iv. 4

Με τετραγωνισμούς υπολογίζουμε: g^2, g^4, g^8 και έπειτα $g \cdot g^2 \cdot g^4 \cdot g^8$, άρα συνολικά 3 τετραγωνισμούς και 3 πολλαπλασιασμούς, οπότε ισοδύναμα 6 πολλαπλασιασμούς. Εναλλακτικά, μπορούμε να υπολογίσουμε: $g^2, g^4, g^5 = g \cdot g^4, g^10, g^15$ οπότε 3 τετραγωνισμούς και 2 πολλαπλασιασμούς, ισοδύναμα 5.

[Προαιρετικά (+2 Μονάδες): Πέρα από την επιλογή σας, δώστε ακριβέστερο φράγμα με εξήγηση μιας πρότασης.]

[Μονάδες: 3, Λανθασμένες Απαντήσεις: -1]

(δ΄) Το σχήμα δέσμευσης του Pedersen:

i. Έχει τέλεια απόκρυψη και υπολογιστική δέσμευση.

ii. Έχει τέλεια δέσμευση και υπολογιστική απόκρυψη.

iii. Έχει τέλεια αποκρυψη και τέλεια δέσμευση.

iv. Έχει υπολογιστική απόκρυψη και υπολογιστική δέσμευση.

Το σχήμα έχει υπολογιστική δέσμευση (δηλ. είναι ασφαλές μόνο για αντίπαλους περιορισμένους υπολογιστικά) και τέλεια απόκρυψη.

[Μονάδες: 3, Λανθασμένες Απαντήσεις: -1]

(ε΄) Πως σχετίζονται τα προβλήματα CDH και DLOG (στη γενική περίπτωση)?

i. Ένας αντίπαλος που μπορεί να λύσει το CDH μπορεί να λύσει και το DLOG.

ii. Ένας αντίπαλος που μπορεί να λύσει το DLOG μπορεί να λύσει και το CDH

iii. Και τα δύο: τα προβλήματα είναι ισοδύναμα.

iv. Τίποτα από τα παραπάνω.

Το δευτερο: λύνοντας το DLOG μπορούμε να πάρουμε τους εκθέτες των στοιχείων και να λύσουμε το CDHμε ένα πολλαπλασιασμό $\mod q$ και μια ύψωση στοιχείου σε δύναμη.

[Μονάδες: 3, Λανθασμένες Απαντήσεις: -1]

(στ΄) Στο RSA χρησιμοποιούμε την ομάδα Z_n^* όπου το $n = p \cdot q$, για p, q πρώτους. Τι ισχύει για τους αριθμούς modulo n (το σύνολο $\mathbb{Z}_n$) και τα p, q;

i. Όλοι οι αριθμοί του Z_n είναι πρώτοι ως προς τα p, q.

ii. Όλοι οι αριθμοί του Z_n είναι πρώτοι ως προς τα p, q, εκτός από ένα σταθερό πλήθος O(1).

iii. Όλοι οι αριθμοί του Z_n είναι πρώτοι ως προς τα p, q, εκτός από ένα αμελητέο μέρος O($\frac{1}{\sqrt{n}}$).

iv. Περίπου οι μισοί αριθμοί του Z_n είναι πρώτοι ως προς τα p, q.

Το Z_n έχει $n = p \cdot q$ στοιχεία. Προβληματικά στοιχεία είναι τα πολλαπλάσια του p (τα οποία είναι q τον αριθμό) και του q τα οποία είναι p τον αριθμό. Στα $p+q$ στοιχεία έχουμε διπλομετρήσει το pq που είναι πολλαπλάσιο και των δύο, άρα τα μη πρώτα στοιχεία είναι ακριβώς $p+q-1 \approx \sqrt{(p \cdot q)}$.

[Μονάδες: 3, Λανθασμένες Απαντήσεις: -1]

(ζ΄) Έστω μια εκτέλεση του σχήματος ανταλλαγής κλειδιών Diffie Hellman στην ομάδα $(\mathbb{G}, g, q)$ όπου το q είναι πρώτος, και στην οποία θεωρούμε ότι το DDH και το Dlog είναι δύσκολα. Θεωρήστε X την τυχαία μεταβλητή που εκφράζει το κοινό στοιχείο στοιχείο g^{ab} στο οποίο καταλήγουν οι αντισυμβαλόμενοι. Έστω Y μια τυχαία μεταβλητή που ακολουθεί την ομοιόμορφη κατανομή στα στοιχεία της $\mathbb{G}$. Τι ισχύει για τις X, Y ;

i. Η στατιστική απόσταση τους είναι μικρή και επίσης δεν υπάρχει καλός πολυωνυμικός διαχωριστής μεταξύ τους.

ii. Η στατιστική απόσταση τους είναι σημαντική και επίσης δεν υπάρχει καλός πολυωνυμικός διαχωριστής μεταξύ τους.

iii. Η στατιστική απόσταση είναι σημαντική και επίσης υπάρχει καλός πολυωνυμικός διαχωριστής μεταξύ τους. Η ασφάλεια προκύπτει από την υπόθεση DDH.

iv. Η στατιστική απόσταση είναι μικρή και επίσης υπάρχει καλός πολυωνυμικός διαχωριστής μεταξύ τους. Η ασφάλεια προκύπτει από τη δυσκολία του DLog.

Οι κατανομές έχουν μικρή απόσταση: με υπολογισμούς μπορούμε να δούμε ότι η στατιστική απόσταση είναι $\frac{1}{q}$ άρα αμελητέα. Από τη θεωρία γνωρίζουμε ότι αν η στατιστική απόσταση είναι μικρή, δεν υπάρχει καλός πολυωνυμικός διαχωριστής [η υπολογιστική απόσταση είναι ισχυρότερη από την υπολογιστική] .

[Μονάδες: 3, Λανθασμένες Απαντήσεις: -1]

(η΄) Έστω μια εκτέλεση του σχήματος ανταλλαγής κλειδιών Diffie Hellman στην ομάδα $(\mathbb{G}, g, q)$ όπου το q είναι πρώτος, και στην οποία θεωρούμε ότι το DDH και το Dlog είναι δύσκολα. Θεωρήστε V την τυχαία μεταβλητή που εκφράζει την τριάδα (g^a, g^b, g^{ab}) από τα επιμέρους στοιχεία που στέλνει κάθε αντισυμβαλόμενος το κοινό στοιχείο στοιχείο στο οποίο καταλήγουν οι αντισυμβαλόμενοι. Έστω W μια τυχαία μεταβλητή (g_1, g_2, g_3) που ακολουθεί την ομοιόμορφη κατανομή στις τριάδες στοιχείων του $\mathbb{G}$. Τι ισχύει για τις V, W ;

i. Η στατιστική απόσταση τους είναι μικρή και επίσης δεν υπάρχει καλός πολυωνυμικός διαχωριστής μεταξύ τους.

ii. Η στατιστική απόσταση τους είναι σημαντική και επίσης δεν υπάρχει καλός πολυωνυμικός διαχωριστής μεταξύ τους.

iii. Η στατιστική απόσταση είναι σημαντική και επίσης υπάρχει καλός πολυωνυμικός διαχωριστής μεταξύ τους. Η ασφάλεια προκύπτει από την υπόθεση DDH.

iv. Η στατιστική απόσταση είναι μικρή και επίσης υπάρχει καλός πολυωνυμικός διαχωριστής μεταξύ τους. Η ασφάλεια προκύπτει από τη δυσκολία του DLog.

Η στατιστική απόσταση είναι μεγάλη: η ομοιόμορφη κατανομή δίνει πιθανότητα $1/q^3$ σε q^3 διαφορετικές τριάδες, ενώ οι DDH τριάδες είναι q^2 το πλήθος.

Άρα, η στατιστική απόσταση είναι μεγάλη μια και στα πιο πολλά $(q^3 - q^2)$ στοιχεία η μία κατανομή δίνει πιθανότητα $1/q^3$ και η άλλη 0. Καλός πολυωνυμικός διαχωριστής δεν υπάρχει: αυτό είναι το αντικείμενο της υπόθεσης DDH. Παρατήρηση: αν η απόσταση ήταν μικρή, δε θα χρειαζόμασταν την υπόθεση. Αν υπήρχε πολυωνυμικός διαχωριστής, η υπόθεση δε θα είχε νόημα, θα ξέραμε από πριν ότι είναι ψευδής.

[Μονάδες: 3, Λανθασμένες Απαντήσεις: -1]

(θ΄) Έστω μια εκτέλεση του σχήματος ανταλλαγής κλειδιών Diffie Hellman στην ομάδα $(\mathbb{G}, g, q)$ όπου το q είναι πρώτος, και στην οποία θεωρούμε ότι το DDH και το Dlog είναι δύσκολα. Θεωρήστε (g^a, g^b) τα επιμέρους στοιχεία που στέλνει κάθε αντισυμβαλόμενος. Η Εύα κατάφερε να υποκλέψει και τα δύο. Τι ισχύει για τις τιμές $g^{a+b}, g^{a \cdot b}$;

i. Υπάρχουν πολυωνυμικοί αλγόριθμοι για τον υπολογισμό των $g^{a+b}, g^{a \cdot b}$.

ii. Υπάρχει πολυωνυμικός αλγόριθμος για το g^{a+b} και εκθετικός για το $g^{a \cdot b}$.

iii. Υπάρχει πολυωνυμικός αλγόριθμος για το $g^{a \cdot b}$ και εκθετικός για το g^{a+b}.

iv. Δεν υπάρχει αλγόριθμος υπολογισμού του $g^{a \cdot b}$.

[Μονάδες: 3, Λανθασμένες Απαντήσεις: -1]

Για το g^{a+b} μπορούμε απλά να εφαρμώσουμε την πράξη της ομάδας στα g^a, g^b. Για το $g^{a \cdot b}$ δεν ξέρουμε αποδοτικό αλγόριθμο (αλλιώς το DDH θα ήταν εύκολο). Αν είχαμε όμως εκθετικό χρόνο στη διαθεσή μας, θα μπορούσαμε να κάνουμε π.χ. brute force τον λογάριθμο του g^a ώστε να μάθουμε το a και έπειτα θα υψώναμε το g^b στην a.

(ι΄) Έστω ένα σχήμα υπογραφών ασφαλές ως προς EUF-CMA. Έστω λ η παράμετρος ασφαλειας. Για κάθε τιμή του λ ορίζουμε: $\mathcal{M}$ το σύνολο όλων των μηνυμάτων που δέχεται η Sign, και $\mathcal{S}$ το σύνολο όλων των ιδιωτικών κλειδιών που προκύπτουν από την Gen. Για ένα $sk \in \mathcal{S}$ ορίζουμε το σύνολο Σ_{sk} των δυνατών υπογραφών του ως $\Sigma_{sk} := \{\sigma : \sigma = \mathsf{Sign}(sk, m) | m \in \mathcal{M}\}$.

i. Για κάθε $\sigma \in \Sigma_{sk}$ υπάρχει μοναδικό $m \in \mathcal{M}$ τέτοιο ώστε $\sigma = \mathsf{Sign}(sk, m)$.
ii. Για κάθε $m \in \mathcal{M}$ υπάρχει μοναδικό $\sigma \in \Sigma_{sk}$ τέτοιο ώστε $\sigma = \mathsf{Sign}(sk, m)$.
iii. Και τα δύο από τα παραπάνω.
iv. Κανένα από τα παραπάνω.

Κανένα από τα δύο. Δεδομένου ότι συχνά χρησιμοποιούμε συναρτήσεις κατακερματισμού σε ένα σχήμα υπογραφών (πχ στο RSA-FDH), είναι αναμενόμενο ότι δύο μηνύματα με το ίδιο hash θα είχαν την ίδια υπογραφή. Ούτε είναι αλήθεια ότι οι υπογραφή κάθε μηνύματος πρέπει να είναι μοναδική: πχ οι υπογραφές Shnorr.

[Μονάδες: 3, Λανθασμένες Απαντήσεις: -1]

(ια΄) Θεωρήστε μια παραλλαγή του σχήματος δέσμευσης του Pedersen όπου ο χώρος των μηνυμάτων αλλάζει και είναι $\mathcal{M} = \mathbb{G}$. Σε αυτή την παραλλαγή, μια δέσμευση c σε ένα μήνυμα m υπολογίζεται ως: $r \leftarrow \mathbb{Z}_q; c \leftarrow m \cdot h^r$. Η επιβεβαίωση υπολογίζεται ως $\mathsf{Ver}(c, m, r)$: if $(c = m \cdot g^r)$ return 1 else return 0. Εργαζόμενοι σε μια ομάδα $\mathbb{G}, g, q$ όπου q πρώτος και το DLog είναι δύσκολο:

i. Η παραλλαγή διατηρεί την ιδιότητα της απόκρυψης (υπολογιστικά, στατιστικά είτε τέλεια).
ii. Η παραλλαγή διατηρεί την ιδιότητα της δέσμευσης (υπολογιστικά, στατιστικά είτε τέλεια).
iii. Η παραλλαγή διατηρεί και τις δύο ιδιότητες.
iv. Η παραλλαγή διατηρεί δεν διατηρεί καμία από τις δύο ιδιότητες.

Η απόκρυψη διατηρείται: μπορούμε όπως στις σημειώσεις να δείξουμε ότι η κατανομή των c είναι η ομοιόμορφη. Η δέσμευση δεν ισχύει. Για οποιαδήποτε m, r εύκολα ελέγχουμε ότι τα m, r και $m \cdot h, r - 1$ αποτελούν σύγκρουση.

[Μονάδες: 3, Λανθασμένες Απαντήσεις: -1]

Θέμα 2 (α΄) Εξηγήστε (1) τυπικά και (2) σε φυσική γλώσσα τις έννοιες της εγκυρότητας (soundness) και της ειδικής εγκυρότητας (special soundness) για ένα πρωτόκολλο 3 κινήσεων. Επιπλέον, (3) δώστε ένα παράδειγμα εφαρμογής στην οποία η διαφορά μεταξύ των δύο εννοιών είναι σημαντική.

Σημειώσεις. Η διαφορά ανάμεσα στις δύο έννοιες εμφανίζεται πχ σε μια απόδειξη ότι $h = g^x$ για σταθερό g και κάποιο $h \in \mathbb{G}$ και μάρτυρα το x. Σε μια κυκλική ομάδα, κάθε h γράφεται ως δύναμη του g. Συνεπώς, δεν υπάρχει h για το οποίο δεν υπάρχει μάρτυρας, οπότε η εγκυρότητα δεν συνεπάγεται τίποτα. Αντίθετα, με την ειδική εγκυρότητα και την εγκυρότητα γνώσης εξασφαλίζουμε ότι ο μάρτυρας τον γνωρίζει (ή έστω μπορεί με κάποιο τρόπο να τον ανακαλέσει).

[Μονάδες: 15]

(β΄) Μία εταιρία φορητών συσκευών θέλει να υλοποιήσει κρυπτογράφηση ElGamal για την ασφαλή αποστολή μετρήσεων ανάμεσα στις συσκευές της. Οι μετρήσεις στέλνονται με συχνότητα περίπου 1 ανα ώρα. Δυστυχώς, λόγω περιορισμών στο κόστος δεν υπάρχει διαθέσιμη κάποια κατάλληλη γενήτρια τυχαίων αριθμών στην πλατφόρμα. Οι μηχανικοί τις εταιρίας έχουν προτείνει τις παρακάτω λύσεις, τις οποίες καλείστε να σχολιάσετε συνοπτικά, καθώς και να προτείνετε τη δική σας. Η κάθε συσκευή είναι εφοδιασμένη με ένα ζεύγος κλειδιών pk, sk μοναδικό για κάθε συσκευή.

- Για την παραγωγή του r θα χρησιμοποιείται μια συνάρτηση κατακερματισμού μήκους 32 bit $H_{32} : \{0,1\}^* \to \{0,1\}^{32}$ ως εξής: $r := H_{32}(m, t)$
- Για την παραγωγή του r θα χρησιμοποιείται μια συνάρτηση κατακερματισμού μήκους q bit $H_q : \{0,1\}^* \to \mathbb{Z}_q$ ως εξής: $r := H_q(pk_r, m)$
- Για την παραγωγή του r θα χρησιμοποιείται μια συνάρτηση κατακερματισμού μήκους q bit $H_q : \{0,1\}^* \to \mathbb{Z}_q$ ως εξής: $r := H_q(t, pk_s)$

Όπου m το μήνυμα (μέτρηση) που θα κρυπτογραφηθεί, pk_r το δημόσιο κλειδί του παραλήπτη, pk_s το δημόσιο κλειδί του αποστολέα, t η ώρα εκπεφρασμένη σε unix format (δευτερόλεπτα από τις 00:00 UTC 1/1/1970 –θεωρήστε ότι το ρολόι της συσκευής είναι ακριβές).

i. Για κάθε υποψήφια λύση στο σχολιασμό σας να αναφερθείτε κατ'ελάχιστο στην ασφάλεια ως προς IND-CPA εκτιμώντας εάν πλήττεται άμεσα ή όχι.

[Μονάδες: 12]

Καμία λύση δεν είναι ασφαλής, αφού ένας αντίπαλος μπορεί πάντα να υπολογίσει το r αν υποψιάζεται ότι ξέρει το μήνυμα m. Επιπλέον, στην πρώτη λύση το r παίρνει λίγες τιμές οπότε μπορούμε εξαντλητικά να βρούμε το λογάριθμο του g^r και κατόπιν να εξάγουμε το μήνυμα από το $m \cdot h^r$. Στη δεύτερη λύση υπάρχει επιπλέον η κακή ιδιότητα ότι ίδιες μετρήσεις σε άλλες ημερομηνίες παράγουν το ίδιο κρυπτομήνυμα. Στην τρίτη λύση, το r είναι ανεξάρτητο από τη μέτρηση, οπότε είναι εφικτό να υπολογιστεί και το ίδιο το r αλλά και τα g^r, h^r ως προς κάποιο t που αντιστοιχεί στην ώρα που θα γίνει η μέτρηση. Αυτή η ιδιότητα μπορεί να έχει αντικείμενο σε συσκευές με περιορισμένη αυτονομία ή/και υπολογιστικούς πόρους.

ii. Προτείνετε τη δική σας λύση για το παραπάνω με βάση τις απαιτήσεις και τα δεδομένα της εκφώνησης. Μπορείτε να χρησιμοποιήσετε παραπάνω πόρους (σε χρόνο, χώρο σε μνήμη, χώρο αποθήκευσης) από ότι οι υποψήφιες λύσεις αλλα θα πρέπει να το αιτιολογήσετε.
Κατ'ελάχιστο θέλουμε στο hash να συμμετέχει το ιδιωτικό κλειδί του αποστολέα(!) ώστε να μην είναι εφικτό να υπολογιστεί το r από κάποιον άλλο. Επιπλέον, δεν πρέπει το μήκος του hash να είναι περιορισμένο όπως στο πρώτο παράδειγμα..

[Μονάδες: 7]

Θέμα 3 **Απρόβλεπτη συνάρτηση με έλεγχο**. Η Αλίκη και ο Βασίλης θέλουν να επιλέξουν ένα στοιχείο στην ομάδα $(\mathbb{G}, g, q)$ με τρόπο που η επιλογή του στοιχείου να μην είναι στον έλεγχο κανενός από τους δύο. Ο Ντίνος, εμπνευσμένος από τις επαληθεύσιμες απρόβλεπτες συναρτήσεις (Verifiable Unpredictable function – VUF) τους προτείνει την παρακάτω κατασκευή:

$Gen(1^\lambda)$: $(\mathbb{G}, g, q) \leftarrow \text{GGen}(1^\lambda); ek \leftarrow \mathbb{Z}_q; vk \leftarrow g^{ek}; return(ek, vk, (\mathbb{G}, g, q))$. Τα $(\mathbb{G}, g, q)$ και vk δημοσιεύονται.

$Eval(x, ek)$: Για ένα $x \in \mathbb{G}$ επιστρέφει $y \leftarrow x^{ek}$.

$Prove(g, vk, x, y, ek)$ Επιστρέφει μια μη διαδραστική απόδειξη μηδενικής γνώσης π ότι γνωρίζουμε μάρτυρα w τέτοιο ώστε $w = \log_g vk = \log_x y = w$. Ο Ντίνος προτείνει η απόδειξη να γίνει με χρήση λογικής σύζευξης στο πρωτόκολλο του Schnorr (δηλ. την κατασκευή των Chaum και Pedersen).

$Ver(vk, x, y, \pi)$ Επιστρέφει 1 εάν η απόδειξη π είναι αποδεκτή για την πρόταση g, vk, x, y και 0 αλλιώς.

Μια απρόβλεπτη συνάρτηση πρέπει (μεταξύ άλλων) να έχει τις παρακάτω ιδιότητες:

- Για κάθε πολυωνυμικό αντίπαλο $\mathcal{A}$, η παρακάτω πιθανότητα είναι αμελητέα στο λ:

$$P[(ek, vk, (\mathbb{G}, g, q) \leftarrow Gen(1^\lambda); (x, y, y', \pi, \pi') \leftarrow \mathcal{A}((\mathbb{G}, g, q), ek, vk) : \\ y \neq y' \wedge Ver(vk, x, y, \pi) = Ver(vk, x, y', \pi') = 1]$$

- Για κάθε πολυωνυμικό αντίπαλο $\mathcal{A}$, η παρακάτω πιθανότητα είναι αμελητέα στο λ:

$$P[(ek, vk, (\mathbb{G}, g, q) \leftarrow Gen(1^\lambda); (x, y) \leftarrow \mathcal{A}((\mathbb{G}, g, q), vk, x); y_0 \leftarrow Eval(x, ek) : y_0 = y]$$

Θεωρήστε ως δεδομένο ότι το σύστημα αποδείξεων που χρησιμοποιείται είναι πλήρες, (ειδικά) έγκυρο και έχει την ιδιότητα της μηδενικής γνώσης. Επίσης θεωρήστε ότι στις ομάδες που κατασκευάζει η GGen είναι δύσκολα το Dlog, το DDH και το CDH.

(α΄) Να εξηγήσετε σε φυσική γλώσσα τι σημαίνει κάθε μία από τις δύο ιδιότητες.

Στην πρώτη ιδιότητα, ένας πολυωνυμικός αντίπαλος δεν μπορεί να αποδείξει ότι το ίδιο x κάνει eval σε δύο διαφορετικά y, y' ακόμα και αν μπορεί να διαλέξει τα x, y, y' ο ίδιος. Στη δεύτερη, ένας πολυωνυμικός αντίπαλος δεν μπορεί να «μαντέψει» το y το οποίο αντιστοιχεί σε ένα x, ακόμα και αν το x το επιλέγει ο ίδιος.

[Μονάδες: 11 (Μεταπτυχιακοί: 8)]

(β΄) Εξετάστε εάν η πρώτη ιδιότητα ισχύει για το πρωτόκολλο του Ντίνου.

Επιγραμματικά: Έστω ένας αντίπαλος ο οποίος επιτυγχάνει στο να παραβιάσει την πρώτη ιδιότητα με μη αμελητέα πιθανότητα έστω p. Αφού $y \neq y'$ τουλάχιστον ένα από τα δύο θα είναι διάφορο του x^{ek}, άρα τουλάχιστον μια από τις αποδείξεις αποδεικνύει μια ψευδή πρόταση. Επιλέγοντας τυχαία μια από τις δύο προτάσεις, έχουμε έναν αλγόριθμο που σε πολυωνυμικό χρόνο παραράγει αποδείξεις ψευδών προτάσεων με πιθανότητα $p/2$ που αντιβαίνει στην εγκυρότητα του Chaum-Pedersen.

[Μονάδες: 11 (Μεταπτυχιακοί: 8)]

(γ΄) Εξετάστε εάν η δεύτερη ιδιότητα ισχύει για το πρωτόκολλο του Ντίνου. Ισχύει: από την ειδική εγκυρότητα

Δεν ισχύει: αν ο αντίπαλος μπορεί να επιλέξει το x, επιλέγει $x = g^r$ και υπολογίζει $y = vk^r$. Αφού $vk = g^{ek}$ έχουμε $y = g^{ek \cdot r} = (g^r)^{ek} = x^{ek}$.

[Μονάδες: 11 (Μεταπτυχιακοί: 8)]

(δ΄) **[Μόνο Μεταπτυχιακοί]** Είναι δυνατό ένας πολυωνυμικός αντίπαλος με είσοδο μια ομάδα $(\mathbb{G}, g, q)$, ένα vk και ένα τυχαίο $x \in \mathbb{G}$ να φτιάξει ένα σωστό ζεύγος (y, π) χωρίς πρόσβαση στην $Eval$ ή την $Prove$;

Επιγραμματικά: Από τη διερεύνηση που κάναμε για την πρώτη ιδιότητα, η πιθανότητα επιτυχίας του αντιπάλου για κάποιο y διαφορετικό από το $x^e k$ είναι αμελητέα (αφού η απόδειξη θα είναι αποδεκτή μόνο με αμελητέα πιθανότητα). Άρα ένας αντίπαλος $\mathcal{A}$ που φτιάχνει αποδεκτά ζεύγη (y, π) με σημαντική πιθανότητα πρέπει να είναι σε θέση να επιστρέφει $y = x^e k$ με σημαντική πιθανότητα. Όμως, με έναν τέτοιο αντίπαλο $\mathcal{A}$ θα ήταν ευκολο να κατασκευάσουμε αντίπαλο $\mathcal{B}$ ο οποίος να λύνει με σημαντική πιθανότητα το CDH (θα του δίναμε $vk = g^a, x = g^b$ και θα έπρεπε να υπολογίσει $y = g^{ab}$), άρα άτοπο. .

[Μονάδες: (**Μόνο Μεταπτυχιακοί**): 9]