ΘΠ05 Κρυπτογραφία

Σημειώσεις 2023-2024

Κωνσταντίνος Χούσος

Περίληψη

Εισαγωγικά: Στοιχεία θεωρίας πολυπλοκότητας, αλγεβρικών δομών, θεωρίας αριθμών, πιθανοτήτων, αλγεβρικών αλγορίθμων. Έννοια της ασφάλειας, απόκρυψη μυνήματος, κρυπτογραφικά πρωτόκολλα, κρυπτανάλυση και επιθέσεις. Τυχαίες και ψευδο-τυχαίες ακολουθίες ψηφίων. Μονόδρομες (one-way) συναρτήσεις και συναρτήσεις κρυφής εισόδου (trapdoor). Απόκρυψη και επιθέσεις σε πρωτόκολλα κρυφού/ιδιωτικού και δημόσιου κλειδιού (πχ. RSA, Diffie-Hellman, El Gamal). Τεχνικές βασισμένες στη θεωρία κωδίκων, την συνάρτηση διακριτού λογαρίθμου, τη δυσκολία παραγοντοποίησης, τις ελλειπτικές καμπύλες, τη δυσκολία επίλυσης πολυωνυμικών συστημάτων και σε προβλήματα συνδυαστικής βελτιστοποίησης (πχ. Πρόβλημα του σακιδίου). Εφαρμογές: Internet (ssh), ηλεκτρονική υπογραφή, ηλεκτρονικό εμπόριο και χρήμα, διενέργεια εκλογών, κινητές τηλεπικοινωνίες, κλπ.

1 2024-03-13

1.1 Διαδικαστικά

Πολλαπλά σετ ασκήσεων + 3 εργασίες.

Βαθμός = 80% Εξέταση + 30% Εργασίες

Οι ασκήσεις θα λύνονται στα φροντιστήρια τις Τετάρτες. Ωστόσο καλό θα είναι να τις προσπαθούμε πρώτα μόνοι μας.

Υλικό μαθήματος: Σημειώσεις, καθως και τα [1]–[3].

1.2 Εισαγωγή

Η τριάδα μήνυμα-πιστοποιητικό (certificate)-υπογραφή μας δίνει την σιγουριά για το αν ένα μήνυμα στέλνεται όντως από αυτόν που φαίνεται.

Το κάθε πιστοποιητικό *πιστοποιείται* από μία συγκεκριμένη οργάνωση (π.χ. HARICA για την Ελλάδα) η οποία έχει κι αυτή ένα πιστοποιητικό.

Αυτά τα πιστοποιητικά **δεν** μπορούν να πλαστογραφηθούν από τρίτους.

Αλγόριθμος κρυπτογράφησης: $E(M, K) \to C$, όπου M το μήνυμα, K ένα κλειδί και C το κρυπτογραφημένο μήνυμα. Αντίστοιχα, υπάρχει κι ο αλγόριθμος αποκρυπτογράφησης $D(C, K) \to M$.

Για κάθε επικοινωνία μεταξύ δύο ατόμων χρειάζεται ξεχωριστό κλειδί.

$$N \text{ χρήστες} \implies \frac{N(N-1)}{2} \text{ κλειδιά} \simeq \frac{N^2}{2}$$

Για την επικοινωνία μεταξύ των A, B, πρέπει πρώτα να δημιουργηθεί το κλειδί K. Αυτή η διαδικασία συνεννόησης γίνεται δημόσια, με τρόπο όμως που κανείς τρίτος δεν μπορεί να παράξει αυτό το κλειδί ακόμα κι έχοντας όλες τις δημόσιες πληροφορίες.

Πιο ρεαλιστικά, κάθε χρήστης έχει δύο κλειδιά, ένα για να κρυπτογραφεί και ένα για να αποκρυπτογραφεί μηνύματα αντίστοιχα.

$$(EK, DK)$$
$$E(M, EK) = C$$
$$D(C, DK) = M$$

Το EK μπορεί να είναι δημόσιο, καθώς έχοντας αυτό και ένα κρυπτογραφημένο μήνυμα C, δεν μπορούμε να αποκρυπτογραφήσουμε το τελευταίο.

Η παραπάνω διαδικασία ονομάζεται κρυπτογράφηση *ιδιωτικού-δημόσιου κλειδιού*. Ανακαλύφθηκε το 1976.

Ένας αλγόριθμος κρυπτογράφησης κι η αποδοτικότητά του κρίνονται ανά περίπτωση.

Οι τωρινοί αλγόριθμοι κρυπτογράφησης απειλούνται από τους κβαντικούς υπολογιστές.

2 2024-03-15

2.1 Στοιχηματισμός πάνω σε ρίψη κέρματος

Έστω δύο παίκτες A, B που στοιχηματίζουν πάνω στο αποτέλεσμα μιας ρίψης κέρματος, το οποίο γίνεται εξ αποστάσεως. Οι A, B δεν εμπιστεύονται ο ένας τον άλλο. Ο καθένας έχει από ένα κέρμα. Υπάρχει επίσης ένας τρίτος Γ, τον οποίο εμπιστεύονται κι οι δύο παίκτες, ο οποίος δεν έχει όμως κέρμα.

Μια λύση είναι ο κάθε παίκτης να ποντάρει πριν και να γνωστοποιεί το στοίχημά του στον Γ. Έπειτα, οι δύο παίκτες ρίχνουν ταυτόχρονα τα κέρματά τους, και πιστοποιεί τα αποτελέσματά τους ο Γ. Το αποτέλεσμα είναι το $x = a \oplus b$.

Έτσι, $\Pr[x = 0] = \frac{1}{2}$, αρκεί ο ένας παίκτης να παίζει τίμια. Εφόσον ο ένας παίκτης παίζει τίμια, το a είναι ανεξάρτητο από το b.

$$\Pr[a = 0 \cap b = 0] + \Pr[a = 1 \cap b = 1] = \Pr[a = 0] \cdot \Pr[b = 0] + \Pr[a = 1] \cdot \Pr[b = 1] =$$
$$\frac{1}{2} \cdot \Pr[b = 0] + \frac{1}{2} \cdot \Pr[b = 1] = \frac{1}{2}[\Pr[b = 0] + \Pr[b = 1]] = \frac{1}{2}$$

Άρα ανεξάρτητα από τις πράξεις του κακόβουλου παίκτη, το τελικό αποτέλεσμα έχει την κατανομή που θέλουμε. Οπότε ο τίμιος παίκτης είναι *ασφαλής*.

Αυτό είναι ο στόχος της κρυπτογραφίας: Να μην απαιτείται η εμπιστοσύνη των υπόλοιπων μελών, αλλά να εγγυάται η ασφάλεια μέσω του συστήματος.

Επόμενο πρόβλημα αποτελεί το submission των αποτελεσμάτων. Λόγω του $\oplus$, ο δεύτερος παίκτης πάντα θα κερδίσει. Έτσι, πρέπει κάπως να προστατεύσουμε τα αποτελέσματα των ρίψεων.

Έστω τα αποτελέσματα των ρίψεων a, b του κάθε παίκτη A, B αντίστοιχα. Χρειάζεται μία συνάρτηση f για να στέλνουμε τα αποτελέσματα μεταξύ των παικτών. Πρέπει να ισχύουν τα παρακάτω:

1. $f(x) \to x$: δύσκολο
2. Αν $x \neq y \to f(x), y$ δεν επιβεβαιώνεται

Για το 2, χρειάζεται και μία συνάρτηση Ver, η οποία θα παίρνει $Ver(c, x^*, \_)$ και θα επιστρέφει ναι ή όχι.

$$Ver(f(x), x, \_) = \text{Yes}$$
$$Ver(f(x), y, \_) = \text{No}, \quad x \neq y$$

Ο B έχει μία τιμή $z = f(a)$. Μπορεί να δει το αποτέλεσμα της $Ver(z, 0)$ και της $Ver(z, 1)$, οπότε χρειαζόμαστε κάτι παραπάνω.

Χρησιμοποιούμε οπότε κι άλλη μία συνάρτηση $Com(m) \to c, r$ και χρησιμοποιούμε το r για το τρίτο όρισμα της Ver. Άρα τελικά

$$Ver(c_0, x, r_0) = \text{Yes}, \quad c_0, r_0 = Com(x)$$
$$\forall r^* \, , Ver(c, y, r^*) = \text{No}, \quad c, r_0 = Com(x) \text{ και } x \neq y$$

Οπότε ο κανόνας 1 μετατρέπεται σε:

1. $c, r \leftarrow Com(x) \; : \; c \to x$: δύσκολο

Άρα:

$$Com(a) \to c, r \; ; \; B(c) \to \text{guess} \; ; \; \Pr[\text{guess} = a] = \frac{1}{2},$$

το οποίο είναι το κατώτατο όριο πιθανότητας που θα μπορούσαμε να ζητήσουμε.

Ένα πρόβλημα είναι πως ο B μπορεί να δοκιμάσει σειριακά τα

$$Ver(c, 0, r_0)$$
$$Ver(c, 1, r_0)$$
$$Ver(c, 0, r_1)$$
$$Ver(c, 1, r_1)$$
$$\vdots$$

Αν ο B δεν έχει άπειρο χρόνο, τότε υπάρχουν η πιθανότητα να πετύχει ο B το a είναι

$$P(\Delta^+) + P(\Delta^-)\frac{1}{2} = \frac{P(\Delta^+)}{2} + \frac{1}{2}(P(\Delta^-) + P(\Delta^+)) = \frac{P(\Delta^+)}{2} + \frac{1}{2}$$

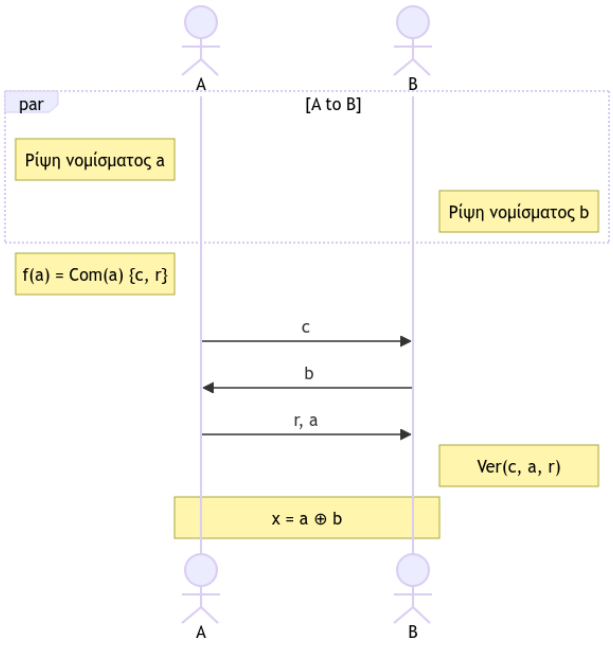
Αυτό δεν λύνεται όσο απαιτούμε η δέσμευση (commitment Pedersen) να είναι τέλεια.

Η όλη διαδικασία επικοινωνίας φαίνεται στο παρακάτω διάγραμμα ακολουθίας.

2.2 Θεωρία ομάδων (Group theory)

Kiayias [4], παρ. 2.1.1.

Παράδειγμα ομάδας $(\mathbb{G}, *)$ είναι η $(\mathbb{Z}, +)$, καθώς ικανοποιεί όλες τις αναγκαίες ιδιότητες. Ουδέτερο στοιχείο της το $e = 0$. Αντίθετος του a το $-a$. Αντιπαράδειγμα είναι το $(\mathbb{N}, +)$.



Εικόνα 1: Επικοινωνία μεταξύ των παικτών A, B.

Δεύτερο αντιπαράδειγμα αποτελεί η $(\mathbb{R}, \cdot)$, καθώς δεν υπάρχει αντίστροφος για το 0, καθώς σε αυτήν την περίπτωση $e = 1$ και η εξίσωση $0 \cdot x = 1$ δεν έχει λύση. Αυτό το πρόβλημα δεν υφίστανται για το $(\mathbb{R}^*, \cdot)$.

Στο μάθημα θα περιοριστούμε στις πεπερασμένες ομάδες, στις οποίες ορίζεται η *τάξη* [4, ορ. 2.1.3].

Τάξη ενός στοιχείου: $\text{ord}(g) = \min i \mid g^i = e$ [4, ορ. 2.1.5]. Αποδεικνύεται ότι **πάντα** υπάρχει τουλάχιστον ένα τέτοιο i (για απόδειξη βλ. 2η ώρα ~25'). Αποδεικνύεται επίσης ότι η τάξη ενός στοιχείου g *διαιρεί* την τάξη της ομάδας $\mathbb{G}$ (η απόδειξη παραλείπεται).

2.3 Ακέραιοι mod n

Παράδειγμα ομάδας που χρησιμοποιείται στην κρυπτογραφία. Αποτελείται από τις τάξεις των υπολοίπων που έχουν οι ακέραιοι όταν τους διαιρούμε με κάποιον αριθμό n.

$$a \equiv b \iff a - b = k \cdot n$$

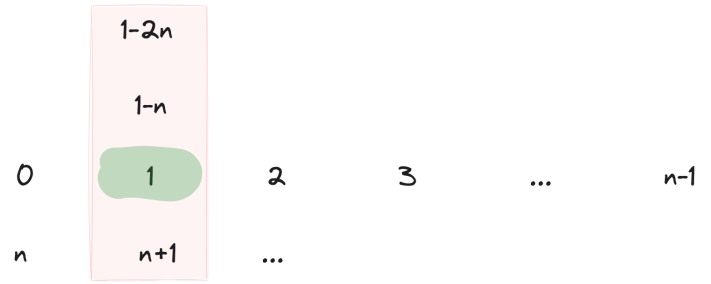
Οι παραπάνω αριθμοί είναι τα στοιχεία της ομάδας. Ακόμα μένει να ορίσουμε την πράξη της ομάδας. Έχοντας υπόψιν ότι θέλουμε το πρόβλημα να είναι υπολογιστικά δύσκολο, επιλέγουμε το πρόβλημα του διακριτού λογαρίθμου.

2.4 Πρόβλημα του διακριτού λογαρίθμου

Kiayias [4], εν. 3.3.

Έστω $\mathbb{G}$ μια ομάδα που είναι μεταθετική ($a * b = b * a$) και κυκλική ($\exists g \mid \langle g \rangle = \mathbb{G}$), με γεννήτορα g και τάξη q. Δεδομένου ενός στοιχείου h, να βρεθεί ένα στοιχείο x τ.ω.

$$g^x = h.$$



Εικόνα 2: Ομαδοποίηση των ακεραίων $\mod n$. Οι αριθμοί στην ίδια στήλη είναι *ισοδύναμοι*. Κάθε στήλη όμως έχει μόνο έναν αριθμό που είναι ανάμεσα στο 0 και το $n-1$. Αυτός ο αριθμός ονομάζεται *αντιπρόσωπος* των αριθμών της στήλης.

Για σωστά δομημένες και μεγάλης τάξης ομάδες, το πρόβλημα αυτό είναι υπολογιστικά απαγορευτικό.

Ένα *κακό* παράδειγμα είναι η ομάδα των ακεραίων $\mod n$ με πράξη την πρόσθεση $(\mathbb{Z}_n, +)$, καθώς

$$h \to x \mid g^x = h \implies \underbrace{g * g * g * \cdots * g}_{x} = h* = +x \cdot g \mod n = h$$

κι άρα ψάχνουμε τον αντίστροφο ως προς τον πολλαπλασιασμό του x, άρα το πρόβλημα γίνεται πρόβλημα πολλαπλασιασμού. Αυτό καθιστά το πρόβλημα απλό, καθώς λύνεται με τον αλγόριθμο του Ευκλείδη. Αν βρούμε τον αντίστροφο του g, μπορούμε να βρούμε το $x = h \cdot g^{-1} \mod n$. Ισχύει ότι

$$g^{\mathrm{ord(g)}} = e \iff g^{\mathrm{ord(g)\cdot k}} = e^k = e \iff g^{\mathrm{ord(G)}} = e.$$

Αν όμως πολλαπλασιάσουμε με τον αντίστροφο g^{-1}, θα έχουμε

$$g^{\mathrm{ord(G)}-1} = g^{-1}.$$

Για να αξιοποιήσουμε το παραπάνω, δεν θα πάρουμε ως πράξη την πρόσθεση, αλλά τον πολλαπλασιασμό. Οπότε τελικά θα προκύψει ότι $h = g^x \mod n$.

Δείξαμε ότι η $(\mathbb{Z}_n, +) = \mathbb{Z} \mod n = \{[0], [1], \ldots, [n]\}$, όπου με $[i]$ υποδηλώνουμε τη στήλη του αριθμού i, είναι ομάδα. Δεν αποτελεί ομάδα όμως για την πράξη του πολλαπλασιασμού. Οπότε παίρνουμε την ομάδα $(\mathbb{Z}_n^*, \cdot)$. Αυτό στην πραγματικότητα ισχύει μόνο αν $n = p$ όπου p είναι πρώτος (βλ. 3η ώρα ~17'). Άρα φεύγει η στήλη $[0]$.

Για παράδειγμα, έστω η $\mathbb{Z}_7^*$ και $g = 5$. Ψάχνουμε $5^{-1} = ?$. Έχουμε $\mathrm{ord}(\mathbb{Z}_7^*) = 6$. Άρα

$$5^{-1} = 5^{6-1} = 5^5.$$

Οπότε λύνουμε ως εξής:

$$
\begin{aligned}
5^5 &\mod 7 \\
5 \cdot 5 \cdot 5 \cdot 5 \cdot 5 &\mod 7 \\
25 \cdot 25 \cdot 5 &\mod 7 \\
4 \cdot 4 \cdot 5 &\mod 7 \\
16 \cdot 5 &\mod 7 \\
2 \cdot 5 &\mod 7 \\
3 &\mod 7
\end{aligned}
$$

Αλγόριθμος επίλυσης:

1. Παίρνουμε την τάξη της g, η οποία συνήθως μας δίνεται (q)
2. Αφαιρούμε 1
3. Υψώνουμε το στοιχείο που μας δώσανε σε αυτή τη δύναμη

Σε πολλές περιπτώσεις, το q θα είναι της τάξης του 2^{256}. Σε τέτοιες περιπτώσεις, δεν είναι εφικτό να κάνουμε τους υπολογισμούς.

Έστω η αφηρημένη ομάδα $\mathbb{G}$ και θέλουμε να υπολογίσουμε το g^x, όπου το x είναι τεράστιο. Η πράξη μπορεί να είναι οτιδήποτε. Γράφουμε το x στο δυαδικό σύστημα.

$$x = x_0 + 2x_1 + 4x_2 + \cdots + 2^k x_k$$

Οπότε προκύπτει ότι

$$g^x = g^{x_0} \cdot g^{2x_1} \cdot \ldots \cdot g^{2^k x_k}$$

Μπορούμε να δούμε τα g σαν το g υψωμένο στην αντίστοιχη δύναμη του 2 που ενεργοποιείται από το εκάστοτε bit x_i. Οπότε πολλαπλασιάζουμε *μόνο* τους όρους όπου $x_i = 1$. Δεδομένου ότι κάποιος μας δίνει τα πολλαπλάσια του g, το κόστος είναι το πολύ k, και στην μέση περίπτωση $\frac{k}{2}$.

Εφόσον το x αναπαριστάται από k bits, $k \simeq \log x$. Επίσης, οι δυνάμεις του g μπορούν να υπολογιστούν ως εξής:

$$
\left.
\begin{aligned}
g & \\
g^2 &= g \cdot g \\
g^4 &= g^2 \cdot g^2 \\
g^8 &= g^4 \cdot g^4 \\
&\vdots \\
g^{2^k} &= g^{2^{k-1}} \cdot g^{2^{k-1}}
\end{aligned}
\right\} k \text{ πράξεις}
$$

Άρα υπολογίζονται γραμμικά. Οπότε, όλη η ύψωση στον εκθέτη θέλει $2k$ πράξεις στη χειρότερη περίπτωση, ή $\frac{3}{2}k$ πράξεις σε μία μέση περίπτωση.

Προσοχή

Άρα η ύψωση σε δύναμη έχει γραμμική πολυπλοκότητα ως προς το πλήθος bits του x.

Η παραπάνω διαδικασία εφαρμόζεται σε οποιαδήποτε ομάδα.

Αν η ομάδα μας είναι της μορφής $\mathbb{Z}_p$, μπορούμε να ακολουθήσουμε κι άλλη τακτική. Μπορούμε δηλαδή να κάνουμε αντιστροφή κατευθείαν, βρίσκοντας τον αντίστροφο με ευκλείδια διαίρεση. Για παράδειγμα:

$$\begin{aligned} 7 &= 2 \cdot 5 + 2 \\ 5 &= 2 \cdot 2 + 1 \\ 2 &= 2 \cdot 1 + 0 \end{aligned}$$

οπότε

$$\begin{aligned} 1 &= -2 \cdot 2 + 5 \\ 1 &= -2 \cdot (7 - 5) + 5 \\ 1 &= -2 \cdot 7 + 2 \cdot 5 + 5 \\ 1 &= -2 \cdot 7 + \underbrace{3}_{\alpha} \cdot 5 \end{aligned}$$

2.4.1 Πολυπλοκότητα εύρεσης x

Έστω ότι έχουμε τα $g^x = h, g, q$ και ψάχνουμε το x. Μια απλή προσέγγιση είναι να κάνουμε δοκιμές σειριακά, δηλαδή g, g^2, g^3 .... Αυτό κοστίζει περίπου x.

Έστω ότι $\lambda =$ το πλήθος bits του x. Η παραπάνω προσέγγιση θα απαιτεί περίπου 2^λ δοκιμές, κάτι δηλαδή ανέφικτο.

Μπορούμε να πέσουμε από τις x στις $\sqrt{x}$ δοκιμές, που όμως και πάλι δεν είναι αρκετά αποδοτικό.

$$\begin{aligned} x &= \lambda \text{ bits} \\ x &= 2^\lambda \\ \sqrt{x} &= \sqrt{2^\lambda} = 2^{\frac{\lambda}{2}} \end{aligned}$$

3 2024-03-20 (Φροντιστήριο)

ex_1_2024gr.pdf sol_1_2024gr.pdf

3.1 Άσκηση 1

XOR ανάμεσα στις ρίψεις των δύο κερμάτων.

$$X \oplus Y = Y \oplus X$$

Αποδεικνύεται βρίσκοντας την πιθανότητα $P[Z = 1]$, όπου $Z = X \oplus Y$.

$$\begin{aligned} P[Z = 1] &= P[X = 0 \wedge Y = 1] + P[x = 1 \wedge Y = 0] \\ &= P[x = 0] \cdot P[Y = 1] + P[X = 1] \cdot P[Y = 0] \\ &= (1 - q) \cdot \frac{1}{2} + q \cdot \underbrace{(1 - p)}_{=p=\frac{1}{2}} = \frac{1 - q}{2} + \frac{q}{2} = \frac{1}{2} \end{aligned}$$

3.2 Άσκηση 2

Παραγωγή 1: $\frac{1}{2} + \delta$. Παραγωγή 0: $\frac{1}{2} - \delta$.

Πάλι, κάνουμε XOR.

$$\begin{aligned} P[Z = 1] &= P[X = 0 \wedge Y = 1] + P[X = 1 \wedge Y = 0] \\ &= \left(\frac{1}{2} - \delta\right) \cdot \left(\frac{1}{2} + \delta\right) + \left(\frac{1}{2} + \delta\right) \cdot \left(\frac{1}{2} - \delta\right) \\ &= 2 \cdot \left(\frac{1}{4} - \delta^2\right) = \frac{1}{2} - \delta^2 \end{aligned}$$

Πρέπει να επιβεβαιώσουμε πως το σφάλμα είναι μικρότερο από δ.

$$\delta < \frac{1}{2} \iff \delta^2 < \frac{1}{2}\delta^2 \iff 2\delta^2 < \delta \implies |-2\delta^2| < \delta$$

3.3 Άσκηση 3

Σημείωση

Εφόσον ο Βασίλης μιλάει δεύτερος, δεν είναι ξεκάθαρο γιατί και από τι θέλουμε να τον προστατέψουμε.

Ένα σενάριο είναι ο Βασίλης να στείλει το ίδιο c. Έτσι, θα μπορεί στο επόμενό του βήμα να στέλνει μόνο a, r, όπου σε εκείνο το σημείο θα είναι πλέον γνωστά, και θα είναι η μόνη επιλογή γιατί μόνο με αυτά θα ταιριάζει το c. Έτσι, στο XOR θα βγαίνει πάντα 0 κι άρα θα χάνει συνέχεια η Αλίκη.

3.4 Άσκηση 4

$$123^{2024} \mod 23$$

Το 23 είναι πρώτος, άρα είμαστε σε πολλαπλασιαστική ομάδα. Άρα $x^{22} \mod 23 \equiv 1$.

Παρατηρούμε ότι

$$\begin{aligned} 123^{2024} &\equiv 123^{44} \cdot 123^{1980} && \mod 23 \\ &\equiv 123^{44} \cdot (123^{22})^{90} && \mod 23 \\ &\equiv 123^{44} \cdot \cancel{1^{90}} && \mod 23 \\ &\equiv (123^{22})^2 && \mod 23 \\ &\equiv 1 && \mod 23 \end{aligned}$$

3.5 Άσκηση 5

$$\underbrace{12345678901234567890123456789}_{29\ \psi\eta\phi\acute{\iota}\alpha} \approx 10^{29} \iff$$

$$\log_{10}(12345678901234567890123456789) = 29$$

Ορισμός 3.1

$$\log_c(a) = \log_b(a) \cdot \log_c(b) \implies \log_b(a) = \frac{\log_c(a)}{\log_c(b)}$$

$$\log_2(10^{29}) = \log_{10}(10^{29}) \cdot \log_2(10) \approx 3,3 \cdot 29 = 95,7$$

4 2024-03-22

4.1 Σχήμα δέσμευσης

Kiayias [4], κεφ. 3.

Ορισμός 4.1: Απαιτούνται οι συναρτήσεις:

1. $\text{Param}(1^\lambda) \to ck$
2. $\text{Com}(ck, m) \to c, r$
3. $\text{Ver}(ck, m, c, r) \to \{0, 1\}$

ώστε να ισχύει

$$\Pr[ck \leftarrow \text{Param}(1^\lambda); c, r \leftarrow \text{Com}(ck, m); \text{Ver}(ck, m, c, r) = 1] = 1, \forall \lambda, m \in M$$

λ: Παράμετρος ασφάλειας

Το κλειδί ck επεκτείνει τον ορισμό που είδαμε στο 2ο μάθημα. Αν οι συναρτήσεις με συγκεκριμένο ck έχουν γίνει compromised, μπορούμε απλά να αλλάξουμε το ck.

Επίσης, πρέπει να διασφαλίζεται η ασφάλεια.

A: πιθανός αντίπαλος

4.1.1 Ιδιότητα δέσμευσης

Τσεκάρουμε αν υπάρχουν διφορούμενα commitments, δηλαδή ισχύει το παρακάτω:

$$\Pr\begin{bmatrix} ck \leftarrow \text{Param}(1^\lambda); \\ (c, m, m', r, r') \leftarrow A(ck); \\ \text{Ver}(ck, c, m, r) = 1 \wedge \text{Ver}(ck, c, m', r') = 1 \wedge m \neq m' \end{bmatrix} = 0, \forall \lambda, \quad A \mid \text{PPT}(\lambda)$$

4.1.2 Ιδιότητα απόκρυψης

Το d είναι μια ρίψη κέρματος. Σε αυτό το σενάριο, έχουν μείνει μόνο 2 “passwords” τα οποία ξέρει ο αντίπαλος, δηλαδή του δίνουμε πολύ περισσότερη δύναμη από ό,τι σε ένα ρεαλιστικό σενάριο. Πρέπει $m_0 \neq m_1$.

$$\Pr\left[\begin{array}{c} ck \leftarrow \text{Param}(1^\lambda); \\ m_0, m_1 \leftarrow A(ck); \\ d \leftarrow \{0,1\}; \\ c, r \leftarrow \text{Com}(ck, m_d); \\ d^* \leftarrow A(ck, c) \ : \ d = d^* \end{array}\right] = \frac{1}{2}, \quad \forall \lambda, A \mid \text{PPT}(\lambda)$$

βλ. Kiayias [4] εν. 3.2.

4.1.2.1 Αντίπαλος με άπειρο χρόνο Ένα πρόβλημα που προκύπτει είναι το αν ο αντίπαλος έχει άπειρο χρόνο. Σε αυτή τη περίπτωση, θα πρέπει να ισχύει $M \cap M' = \emptyset$ για τον πρώτο ορισμό, ενώ αυτό αναιρεί τον δεύτερο.

Φεύγουμε από την *τέλεια* δέσμευση και την *τέλεια* απόκρυψη, και προσθέτουμε μια μικρή ποσότητα στις πιθανότητες.

Η πιθανότητα του πρώτου ορισμού θα γίνει από 0 σε ϵ, το οποίο είναι αμελητέο.

Η πιθανότητα του δεύτερου θα γίνει $\frac{1}{2} + \epsilon$.

Αμελητέα είναι μια συνάρτηση f όπου ισχύει $f(x) < \frac{1}{x^k} \iff f(x)x^k < 1, \forall k$.

Οι δύο ιδιότητες μετατρέπονται σε *στατιστική* δέσμευση και απόκρυψη.

4.1.3 Παραλλαγές σχημάτων δέσμευσης

1. Τέλεια
2. Στατιστική
3. Υπολογιστική
4. Με adversarial κλειδιά Το ck το στέλνει ο αντίπαλος μαζί με τα m_0, m_1.

Υπάρχουν κι άλλες, συνολικά είναι 36(!).

4.2 Πρόβλημα διακριτού λογαρίθμου

Kiayias [4], εν 3.3.

$$\forall \mathbb{G}, g, q, A \ : \ \Pr[h \leftarrow \mathbb{G}; x \leftarrow A(h); g^x = h] = \text{negl}$$

Ένα πρόβλημα είναι ο αντίπαλος να έχει μάθει την ομάδα. Η λύση είναι η ομάδα να ορίζεται μέσα στο πείραμα, αφού έχει οριστεί ο αντίπαλος.

Ορίζουμε την παρακάτω συνάρτηση γεννήτρια ομάδων:

$$h \in \mathbb{G} \mid (\mathbb{G}, g, q) \leftarrow \text{GGen}(1^\lambda)$$

Άρα τελικά

$$\forall \lambda, A\text{PPT}(\lambda) \ : \ \Pr[(\mathbb{G}, g, q) \leftarrow \text{GGen}(1^\lambda); h \leftarrow \mathbb{G}; x \leftarrow A(h); g^x = h] = \text{negl}(\lambda)$$

4.3 Σχήμα δέσμευσης του Pedersen

Kiayias [4], εν. 3.4.

- Απόδειξη ιδιότητας δέσμευσης Δεδομένων των c, m, m', r, r' μπορούμε να βρούμε τον διακριτό λογάριθμο του h *ένκολα* μέσω ενός αλγορίθμου B που εκμεταλλεύεται τον αντίπαλο A: **ΆΤΟΠΟ**

5 2024-03-27 (Φροντιστήριο)

ex_1_2024gr.pdf sol_1_2024gr.pdf

5.1 Άσκηση 6

$$\log_2 5 \mod 37$$

Ορισμός 5.1: Αλγόριθμος Baby-step, Giant-step

Στον αλγόριθμο Baby step, Giant step, θέλουμε να λύσουμε την εξίσωση $g^x \equiv h \mod p$ "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.

$g = 2, \mathbb{G} = \mathbb{Z}_{37}^*$. Πρέπει να ισχύει $q = 36$, έτσι ώστε το g να μπορεί να παράγει όλα τα στοιχεία της ομάδας $\mathbb{G}$.

Το πρώτο πρόβλημα είναι το αν το $g = 2$ όντως παράγει όλα τα στοιχεία της ομάδας, δηλαδή αν η τάξη του είναι όντως 36.

Παράδειγμα 5.1

Έστω ότι θέλουμε να δούμε αν το 36 μπορεί να παράξει όλα τα στοιχεία της ομάδας $\mathbb{G}$ πιο πάνω.
Το 36 έχει τάξη 2, καθώς $-1 \equiv 36 \mod 37 \iff 1 \equiv 36^2 \mod 37$, όπου το 1 είναι το *ουδέτερο στοιχείο* e της ομάδας. Άρα, με το 36 μπορούμε να παράξουμε μόνο 36 και 1, οπότε δεν είναι γεννήτορας της ομάδας. Πιο απλά, $\text{ord}(36) = 2 < 36 = \text{ord}(\mathbb{Z}_{37}^*)$.

Για να βρούμε την τάξη του 2, θα εκμεταλλευτούμε το θεώρημα του Lagrange:

Θεώρημα 5.1: Lagrange

Έστω μία ομάδα $\mathbb{G}$ και μία υποομάδα της $\mathbb{H} = \langle h \rangle$. Τότε η τάξη $\text{ord}(\mathbb{H}) = \text{ord}(h)$ διαιρεί την τάξη $\text{ord}(\mathbb{G})$.

Οπότε, η τάξη του 2 μπορεί να είναι μία από: 36, 18, 12, 9, 6, 3, 2. Για να αποφύγουμε τον έλεγχο της κάθε μίας περίπτωσης, μπορούμε να ελεγξουμε μόνο για 18 και 12. Αυτό γιατί, αν π.χ. το $12 = 2 \cdot 2 \cdot 3$ δεν βγάζει 1, τότε ούτε τα 2 και 3 θα μπορούσαν να είναι η τάξη.

1. Πρώτος έλεγχος: Ισχύει ότι $2^{12} \equiv 1 \mod 37$; Κάνοντας τις πράξεις, προκύπτει ότι $2^{12} \equiv \cdots \equiv 26 \mod 37$.

2. Δεύτερος έλεγχος: Ισχύει ότι $2^{18} \equiv 1 \mod 37$; Κάνοντας τις πράξεις, προκύπτει ότι $2^{18} \equiv \cdots \equiv 36 \mod 37$.

Άρα κανένα από τα δύο δεν βγάζει 1. Οπότε, όντως η τάξη του 2 είναι 36. Άρα ο ζητούμενος λογάριθμος ορίζεται.

Για να αποφύγουμε τον υπολογισμό και των 36 δυνάμεων του 2 (που σε πραγματικές συνθήκες δεν θα ήταν 36 αλλά πολλές παραπάνω), θα αξιοποιήσουμε τον αλγόριθμο του ορισμού 5.1.

$$2^x \equiv 5 \mod 37, 0 \leq x < 36$$
$$2^{b+6\cdot B} \equiv 5 \mod 37, 0 \leq b, B < 6$$

Τροποιούμε την εξίσωση ως εξής:

$$2^{6B} \equiv 5 \cdot 2^{-b} \mod 37$$

Υπολογίζουμε τις τιμές του κάθε μέλους για κάθε διαφορετική τιμή των b, B. Δηλαδή, κάνουμε συνολικά $6 + 6 = 12$ υπολογισμούς, αντί για τους αρχικούς 36. Προκύπτουν τα ακόλουθα αποτελέσματα, όπου γράφουμε τον *αντιπρόσωπο* σε κάθε κελί. Παρατηρούμε ότι η εξίσωση λύνεται για $B = 3, b = 5$.

b, B	2^{6B}	$5 \cdot 2^{-b}$
0	1	5
1	27	21
2	26	29
3	36	33
4	10	35
5	11	36

Οπότε, η εξίσωση παίρνει την ακόλουθη μορφή:

$$2^{5+6\cdot 3=23} \equiv 5 \mod 37$$

Άρα, $x = 23$.

6 2024-03-29

Οι ομάδες που μπορούμε να χρησιμοποιήσουμε για το σχήμα Pedersen, πρέπει να έχουν p πρώτο και q πρώτο. Εφόσον $q = p - 1$, όπου ο p είναι μονός, δεν γίνεται να έχουμε μη-ζυγό/πρώτο q με τύπο ομάδων $\mathbb{Z}_p^*$. Άρα θα πρέπει να αφαιρούμε κι άλλα στοιχεία.

Παραλλαγή του σχήματος του Pedersen όπου αντί για $g^r \cdot h^m$ η Com παράγει μόνο g^r: Αυτή η παραλλαγή έχει *τέλεια απόκρυψη* αλλά δεν έχει *δέσμευση*. Χρησιμεύει για να αποδείξουμε ότι και η κανονική παραλλαγή έχει *τέλεια απόκρυψη*.

Αυτό θα γίνει ορίζοντας τις δύο περιπτώσεις ως στατιστικές μεταβλητές και αποδεικνύοντας ότι αυτές οι μεταβλητές είναι ίδιες/ίσες. Έτσι, κάποιος που βλέπει το output μιας από των δύο δεν μπορεί να διακρίνει για ποια μεταβλητή πρόκειται.

6.1 Στατιστική απόσταση

Έστω οι μεταβλητές $X \leftarrow D_1, Y \leftarrow D_2$. Έστω ο χώρος πιθανότητας V. Η στατιστική απόσταση των X, Y ορίζεται ως

$$\Delta[X,Y] = \frac{1}{2}\sum_{u\in V}\left|\Pr_{X\sim D_1}[X=u] - \Pr_{Y\sim D_2}[Y=u]\right|$$

![Δύο κατανομές πιθανοτήτων σε διαφορετικά σύνολα υποστήριξης D_1

Παράδειγμα 6.1

Έστω ένα δίκαιο τετράεδρο ζάρι με πιθανοτική μεταβλητή X : $\Pr[1] = \Pr[2] = \Pr[3] = \Pr[4] = \frac{1}{4}$ και ένα δίκαιο εξάεδρο ζάρι με πιθανοτική μεταβλητή Y : $\Pr[1] = \Pr[2] = \Pr[3] = \Pr[4] = \Pr[5] = \Pr[6] = \frac{1}{6}$. Για $u = 1,2,3,4$, τα στοιχεία του αθροίσματος θα είναι $\left|\frac{1}{6} - \frac{1}{4}\right| = \left|\frac{4-6}{24}\right|$ και για $u = 5,6$ θα είναι $\left|\frac{1}{6} - 0\right| = \frac{1}{6}$. Η στατιστική τους απόσταση θα είναι

$$\Delta[X,Y] = \frac{1}{2}\left[\frac{4\cdot 1}{12} + \frac{2\cdot 1}{6}\right] = \frac{1}{2}\left[\frac{1}{3} + \frac{1}{3}\right] = \frac{1}{3}.$$

Παράδειγμα 6.2

Σελίδα 16 [4].
D_1: αριθμός που πέφτει κάπου ανάμεσα στους αριθμούς με 2^n και 2^{n+1} bits. D_2: αριθμός με κανονική κατανομή πάνω στους αριθμούς μέχρι 2^n bits.

6.2 Στατιστικά tests

Kiayias [4], εν. 2.7.

$$\Delta_{\mathcal{A}}[X,Y] = \left|\Pr_{X\leftarrow\mathcal{D}_1}[\mathcal{A}(X)=1] - \Pr_{Y\leftarrow\mathcal{D}_2}[\mathcal{A}(Y)=1]\right|$$

- Ιδιότητες
  1. $\forall A : \Delta_A[X,Y] \le \Delta[X,Y]$
  2. $\exists A : \Delta_A[X,Y] = \Delta[X,Y]$

Αν περιορίσουμε τα A σε πολυωνυμικούς αλγορίθμους, η ανισότητα μπορεί να γίνει γνήσια.

Έστω A_k ο αντίπαλος της δεύτερης ιδιότητας, όπου μαντεύει ολόσωστα. Ισχύει ότι

$$\mathcal{A}_k(a) = \begin{cases} 1, & \Pr_{\mathbf{D}_1}[a] \ge \Pr_{\mathbf{D}_2}[a] \\ 0 \end{cases}$$

6.3 Ιδιότητα απόκρυψης του σχήματος Pedersen

Kiayias [4], εν. 3.4.1.

1. Η στατιστική απόσταση των δύο πειραμάτων είναι 0.

$$\left.\begin{aligned} X &= g^t, & t &\leftarrow \mathbb{Z}_q \\ Y &= g^r \cdot h^m, & r &\leftarrow \mathbb{Z}_q \end{aligned}\right\} \quad \Delta[X,Y] = 0$$

2. Εφόσον η στατιστική απόσταση είναι 0, τα δύο πειράματα είναι ίσα. Δηλαδή, $X = Y$, δηλαδή οι απαντήσεις του αντιπάλου θα ταυτίζονται και στα δύο πειράματα.
3. Η πιθανότητα σωστής απάντησης του αντιπάλου για το X είναι $\frac{1}{2}$, άρα το ίδιο θα ισχύει και για το Y.

Προσοχή

Στο σχήμα Pedersen, τα σύνολα M_0, M_1 της εν. 4.1.2.1 είναι *το ίδιο σύνολο*, άρα **μπορούμε** να έχουμε **τέλεια απόκρυψη**.

7 2024-04-03 (Φροντιστήριο)

ex_2_2024gr.pdf sol_2_2024gr.pdf

7.1 Άσκηση 1

Εφόσον πρόκειται για το σχήμα του Pedersen, $c = g^r \cdot h^a$. Στόχος $\bar{c} \approx g^r \cdot h^a$. Μπορούμε να αλλάξουμε το $r \to r'$. Βλέποντας το c, δεν μπορούμε να υπολογίσουμε το a. Μπορούμε όμως να φτιάξουμε ένα $\bar{c} = c \cdot g = g^r \cdot h^a \cdot g = g^{r+1} \cdot h^a \to \text{Ver}(c \cdot g, a, r+1) == \text{Ver}(g, a, r)$. Γενικεύεται για $\bar{c} = c \cdot g^k, r' = r + k$. Έτσι, γίνεται ο Βασίλης, με διαφορετικό c, μπορεί να αναγκάσει το XOR να βγαίνει πάντα 0.

7.2 Άσκηση 2

Τρέχοντας τις αποδείξεις βλέπουμε ότι δουλεύει κι αυτή η παραλλαγή.

Στην απόδειξη της δέσμευσης, χρειάζεται να δείξουμε ότι $\Delta_r \neq 0$ αντί για $\Delta_m \neq 0$.

Αν $\Delta_r = 0 \to g^{r_1} = g^{r_2} \to h^{m_1} = h^{m_2}$: ΑΤΟΠΟ.

7.3 Άσκηση 3

Η Καρολίνα έχει φτιάξει το h. Έστω $h = g^x$. Τότε, $g^m \cdot h^r = g^{m+rx}$ και $g^r \cdot h^m = g^{r+mx}$.

$$\frac{\bar{c}}{c^x} = \frac{g^{m+rx}}{g^{r+mx}} = g^{m+rx-rx-mxx} = g^{m(1-xx)} = g^{m \cdot z}, \quad z \equiv 1 - x^2 \mod q$$

Άρα με q δοκιμές μπορούμε να βρούμε το m.

8 2024-04-05

8.1 Σχήματα κρυπτογράφησης

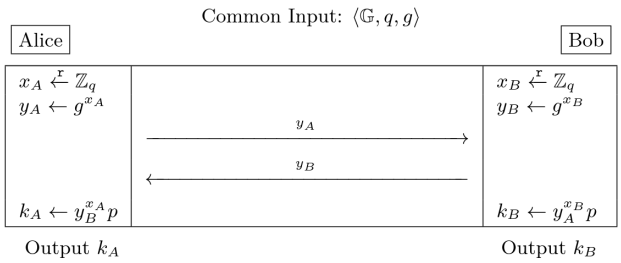
8.1.1 Κρυπτογράφηση συμμετρικού κλειδιού

Kiayias [4], κεφ. 4.

Ζεύγος συναρτήσεων encrypt/decrypt $E(k, m) \to c, D(k, c) \to m$. Χρειαζόμαστε και μία συνάρτηση $G(1^\lambda) \to k$. Θα πρέπει οι παίκτες να γνωρίζουν το k, το οποίο δεν πρέπει να σταλθεί ανάμεσά τους σε περίπτωση που κάποιος τρίτος "ακούει" τη μεταξύ τους επικοινωνία. Αν πρόκειται για πολλούς παίκτες, θα θέλουμε ένα κλειδί για κάθε ζευγάρι παικτών, δηλαδή $\frac{N^2}{2}$.

8.1.2 Πρωτόκολλο ανταλλαγής κλειδιών Diffie-Hellman

Kiayias [4], κεφ. 6.



Εικόνα 3: Το πρωτόκολλο ανταλλαγής κλειδιών Diffie-Hellman, όπου g είναι παραγωγός μιας υποομάδας του $\mathbb{G}$ με τάξη q.

Σκοπός είναι $k_A = k_B$, που ισχύει:

$$B^a = (g^b)^a = g^{b \cdot a}$$
$$=$$
$$A^b = (g^a)^b = g^{a \cdot b}$$

Ισχύει ότι $g^{a \cdot b} \approx g^c$. ...απόδειξη... $\implies$ Η στατιστική απόσταση μεταξύ $g^{a \cdot b}$ και g^c είναι *μικρή*. **Άρα** τα κλειδιά που παράγει το DH έχουν κατανομή σχεδόν ίδια με τυχαία κατανομή.

Όμως, ο αντίπαλος γνωρίζει και τα A, B. Άρα στην πραγματικότητα συγκρίνει τριάδες, όχι μόνο κλειδιά μεταξύ τους.

$$\mathcal{A}(A, B, K_{ab}) \approx \mathcal{A}(A, B, z) \implies g^a, g^b, g^{a \cdot b} \mid g^a, g^b, g^c$$

Τα μέρη με ίδιο χρώμα έχουν μικρή στατιστική απόσταση. **Όμως**, οι τριάδες καθαυτές αποδεικνύεται ότι έχουν *μεγάλη* στατιστική απόσταση. Ο χώρος της δεύτερης τριάδας είναι q^3, ενώ της πρώτης q^2. Έστω οι δύο κατανομές D και R που αντιστοιχούν σε κάθε σκέλος αντίστοιχα.

$$\begin{aligned}
\Delta[D, R] &= \frac{1}{2} \sum_{u \in \mathbb{G}^3} |\Pr[D = u] - \Pr[R = u]| \\
&= \frac{1}{2} \sum_{u \in K} \left| P[D = u] - \frac{1}{q^3} \right| + \frac{1}{2} \sum_{u \in \overline{K}} \left| 0 - \frac{1}{q^2} \right| \\
&= \frac{1}{2} \cdot q^2 \left| \frac{1}{q^2} - \frac{1}{q^3} \right| + \frac{1}{2} \cdot (q^3 - q^2) \cdot \frac{1}{q^3} \\
&= \frac{1}{2} q^2 \frac{q-1}{q^3} + \frac{1}{2} \frac{q-1}{q} \\
&= \frac{1}{2} \cdot \frac{q-1}{q} + \frac{1}{2} \frac{q-1}{q} = \frac{q-1}{q} = 1 - \frac{1}{q}
\end{aligned}$$

Με άπειρο χρόνο ο αντίπαλος μπορεί να βρει το κλειδί. Άρα πρέπει να περιορίζεται *υπολογιστικά*.

8.1.2.1 Υπολογιστικό πρόβλημα Diffie-Hellman (CDH) Kiayias [4], ορ. 6.2.2.

> The computational Diffie-Hellman problem is no harder than the discrete logarithm problem.

8.1.3 Ασφάλεια απέναντι σε αντιπάλους

Kiayias [4], εν. 6.4.

9 2024-04-12

9.1 Επαλήθευση ασφάλειας Diffie-Hellman

DDH: $\Delta_A[(g^a, g^b, g^{ab}), (g^a, g^b, g^c)] = \text{negl}$.

Ορισμός 9.1

$$\Pr_{\tau \leftarrow \text{trans}_{A,B}(1^\lambda)}[\mathcal{A}(\tau) = V(key(\tau))] \leq \max\{\delta, 1-\delta\} + \text{negl}(\lambda)$$

Security model 3 [4, σσ. 37–40].

Για να το αποδείξουμε αυτό, θέλουμε να δείξουμε ότι δεν υπάρχει αντίπαλος A που να τρέχει σε πολυωνυμικό χρόνο και να σπάει τον παραπάνω ορισμό. Αυτό οδηγείται σε άτοπο εφόσον τότε θα υπήρχε και αντίπαλος B που παραβιάζει την υπόθεση DDH.

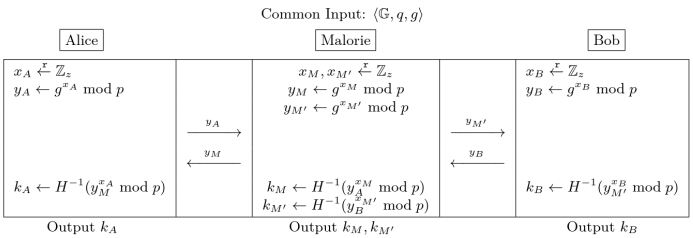
Σημαντικό για τη συμπεριφορά του B σε τυχαίες τριάδες: Εφόσον οι μεταβλητές είναι ανεξάρτητες, και τα $A(a,b), V(c)$ είναι ανεξάρτητες.

9.2 Pedersen με ομάδα μη-πρώτου q

Kiayias [4], παρ. 6.5.

9.3 Man-in-the-middle επίθεση

Kiayias [4], παρ. 6.7.



Εικόνα 4: Η επίθεση "man-in-the-middle" στο πρωτόκολλο ανταλλαγής κλειδιού Diffie-Hellman.

10 2024-04-17 (Φροντιστήριο)

ex_2_2024gr.pdf sol_2_2024gr.pdf

10.1 Άσκηση 5

10.1.1 Sampler 1

y: ομοιόμορφα επιλεγμένος αριθμός n bits

$x \in [0, A), y \in [0.B)$ όπου $B = 2^n$.

10.1.2 Sampler 2

Προσοχή

Όταν λέμε ότι κάτι είναι τυχαίο, παίζει ρόλο κι η τιμή που ακολουθεί, όχι μόνο ο χώρος τιμών.

Ο Sampler 2 ακολουθεί τη διωνυμική κατανομή. Υποψιαζόμαστε ότι η στατιστική απόσταση θα είναι μεγάλη.

10.1.3 Sampler 3

Αν $y \geq A$, goto start. Ενώ παίρνει τιμές στο $[0, B)$ επιστρέφει μόνο τιμές από το $[0, A)$.

11 2024-04-19

Προσοχή

Μπορούμε να πούμε ότι για μια τυχαία συνάρτηση h δεν ξέρουμε π.χ. πόσο κάνει το $h(x_5)$. Όταν μάθουμε, θα ξέρουμε μόνο αυτή τη τιμή. Δεν μαθαίνουμε τίποτα για π.χ. το $h(x_6)$.

11.1 Ψηφιακές υπογραφές

Kiayias [4], κεφ. 7.

Η κρυπτογράφηση ενός μηνύματος εγγυάται την *απόκρυψη*, όχι την ακεραιότητα ενός σταλμένου μηνύματος. Με τη χρήση ψηφιακών υπογραφών, εγγυόμαστε όσον αφορά τον αποστολέα και το περιεχόμενο του μηνύματος.

Ένα *σχήμα ψηφιακών υπογραφών* απαιτεί 3 συναρτήσεις [4, ορ. 7.0.1]:

1. $\text{Gen}(1^\lambda) \to (vk, sk)$
2. $\text{Sign}(sk, M) \to \sigma$
3. $\text{Verify}(vk, M, \sigma) \to \{0, 1\}$

Επίσης, πρέπει να τηρεί 2 ιδιότητες:

1. Ορθότητα

$$\forall \lambda, m \in \mathscr{M}_\Lambda, \Pr[vk, sk \leftarrow \text{Gen}(1^\lambda); \sigma \leftarrow \text{Sign}(sk, m); \text{Ver}(vk, m, \sigma) = 1] = 1$$

2. Αδυναμία παραποίησης (unforgeability)

Μπορούμε ως ορισμό να χρησιμοποιήσουμε αυτό που θέλουμε να αποφύγουμε, ως εξής:

$$\Pr[(vk, sk) \leftarrow \text{Gen}; sk \leftarrow \mathscr{A}(vk)] = \text{negl}$$

Όμως, αυτό δεν εγγυάται την ακεραιότητα και την ασφάλεια του συστήματός μας, καθώς ο αντίπαλος δεν χρειάζεται απαραίτητα το κλειδί για να πλαστογραφήσει ένα μήνυμα. **Αυτό** είναι στην ουσία αυτό που θέλουμε να αποφύγουμε.

Διαφορετικοί πιθανοί ορισμοί: Βλέπε πρώτη ώρα. Με μικρά βήματα, καταλήγουμε σε 19 πιθανούς ορισμούς μέχρι να φτάσουμε στον πιο ισχυρό. Κάποιες αξιόλογες παραλλαγές:

1. Universal unforgeability (UUF) Δεν υπάρχει αντίπαλος που μπορεί να πλαστογραφήσει οποιοδήποτε μήνυμα του δοθεί.
2. Selective unforgeability (SEL) Δεν υπάρχει αντίπαλος που μπορεί να πλαστογραφήσει κάποιο μήνυμα που αποφασίζει εκείνος. Δεν έχει δει ακόμη το δημόσιο κλειδί.
3. Existential unforgeability (EUF) Δεν υπάρχει αντίπαλος που μπορεί να πλαστογραφήσει *ένα* από τα πιθανά μηνύματα με βάση το δημόσιο κλειδί.

Βοήθεια

Όσο πιο αργά στη διαδικασία αποφασίζεται το μήνυμα m, τόσο περισσότερη δύναμη δίνουμε στον αντίπαλο.

Σε περίπτωση που ο αντίπαλος έχει κάποια εικόνα για το πώς είναι οι υπογραφές, δηλαδή να έχει δει παλιές υπογραφές, ανοίγουν κι οι παρακάτω περιπτώσεις.

1. Key only attack (KOA) Ο αντίπαλος γνωρίζει μόνο το δημόσιο κλειδί.
2. Known message attack (KMA) Γνωρίζει κάποιους valid συνδυασμούς μηνυμάτων και υπογραφών.
3. Chosen message attack (CMA) Ο αντίπαλος έχει πρόσβαση σε ένα "API"/oracle στο οποίο μπορεί να ζητάει υπογραφές για μηνύματα που επιλέγει.

   Το oracle του αντιπάλου μπορούμε να πούμε ότι είναι μία συνάρτηση $\mathrm{Sig}(m)$ που εκτελείται στο "cloud", με ορισμό:

$$\begin{aligned}&\mathrm{Sig}(m)\ :\\ &\quad \sigma \leftarrow \mathrm{Sign}(sk, m)\\ &\quad Q = Q \cup (m, \sigma)\\ &\quad \texttt{return}\ \sigma\end{aligned}$$

Για να καλύψουμε τη περίπτωση του CMA, που κανονικά ο αντίπαλος θα μπορεί να πλαστογραφήσει οποιοδήποτε μήνυμα, εισάγουμε την έννοια του Q. Στην περίπτωση του KMA, είναι ένα σύνολο από τα μηνύματα και τις υπογραφές που έχει δει, ενώ στη περίπτωση του CMA, ένα σύνολο από τα μηνύματα για τα οποία έχει ζητήσει υπογραφή και έχει λάβει την αντίστοιχη υπογραφή.

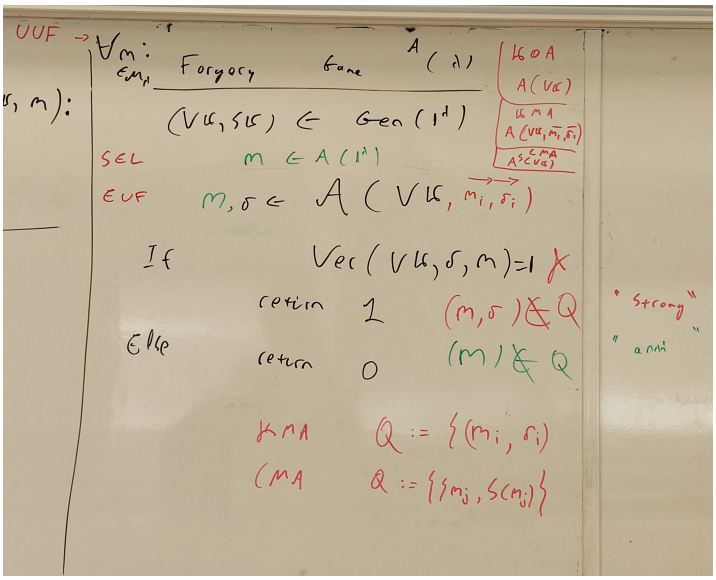
Αυτή τη στιγμή έχουμε 10 ορισμούς. 1 αρχικό, 3 που έχουν να κάνουν με τον *στόχο* του αντιπάλου και 3 που έχουν να κάνουν με τα *εφόδιά* του, οι οποίοι συνδυάζονται μεταξύ τους κι άρα καταλήγουν σε $3 \cdot 3 = 9$.

Το επόμενο βήμα είναι να εξετάσουμε τις δύο περιπτώσεις που φαίνονται και στην παρακάτω εικόνα όσον αφορά τον έλεγχο στο Q:

$$(m, \sigma) \notin Q \vee m \notin Q.$$

Εάν απαγορεύσουμε να χρησιμοποιήσει ένα ζευγάρι, τότε έχουμε τον "ισχυρό" ορισμό, Αν απαγορεύσουμε να χρησιμοποιήσει μόνο το μήνυμα, έχουμε τον "απλό" ορισμό.

Οπότε καταλήγουμε σε $1 + (3 \cdot 3) \cdot 2 = 19$ ορισμούς.



Εικόνα 5: Οι 19 πιθανοί ορισμοί, συνοπτικά. Οι επιθέσεις βρίσκονται σε δύο άξονες. Ο ένας έχει να κάνει με το forgeability και το κατά πόσο μπορεί να πλαστογραφήσει υπογραφές ο αντίπαλος και για ποια μηνύματα, πάει UUF->SEL->EUF. Ο άλλος έχει να κάνει με το κατά πόσο ο αντίπαλος έχει πρόσβαση σε κλειδιά: KOA->KMA->CMA.

11.1.1 Βασικό ζητούμενο ψηφιακών υπογραφών

> Το να πάρουμε από ένα μήνυμα την υπογραφή είναι δύσκολο, ενώ το να επιβεβαιώσουμε μια υπογραφή είναι εύκολο.

Για την παραγωγή ασφαλών υπογραφών, χρειαζόμαστε ουσιαστικά μία υπό συνθήκη αντιστρέψιμη συνάρτηση f [4, κεφ. 7.4], τέτοια ώστε

$$\text{δύσκολο} : m \xrightarrow{f_e^{-1}} \sigma$$
$$\text{εύκολο} : m \xleftarrow{f_e} \sigma.$$

όπου το e πρόκειται για το δημόσιο κλειδί. Αυτή η τάξη συναρτήσεων ονομάζεται *trapdoor one-way functions* [4, κεφ. 7.1]. Το *κλειδί* του *trapdoor* θα είναι το z. Ένα παράδειγμα σχήματος υπογραφών που χρησιμοποιεί τέτοια συνάρτηση είναι το **σύστημα υπογραφών RSA**.

11.1.2 Σύστημα ψηφιακών υπογραφών RSA

Στο πρόβλημα του διακριτού λογαρίθμου, μπορούμε από το g^a να βρούμε το g υψώνοντάς το στο a^{-1}. Δηλαδή, λέμε ότι $b = a^{-1} \mod q \to (g^a)^{1/a} = (g^a)^b = g$. Αυτό είναι ένα παράδειγμα αντιστροφής συνάρτησης υπό συνθήκη, καθώς δεν μπορούμε να κάνουμε αυτή τη διαδικασία αντιστροφής αν **δεν ξέρουμε το** q.

11.1.2.1 Συνάρτηση RSA

Kiayias [4], κεφ. 7.5.

Οι ομάδες πλέον είναι τύπου $\mathbb{Z}_n^*$, όπου $n = p \cdot q$, p, q πρώτοι. Έχουμε δείξει ότι σε μία ομάδα $(\mathbb{Z}_p^*, \cdot)$, πρέπει να διώξουμε οποιοδήποτε στοιχείο έχει κοινό παράγοντα το p, έτσι ώστε να συνεχίσουν να ισχύουν οι ιδιότητες των ομάδων (συγκεκριμένα, δεν θα έχει αντίστροφο). Άρα σε αυτή τη περίπτωση, θα διώξουμε τα p, q και όλα τα πολλαπλάσιά τους.

$$\begin{aligned}\mathbb{Z}_n^* &= \{\dots, \cancel{p}, \dots, \cancel{q}, \dots, \cancel{2p}, \dots, \cancel{2q}, \dots, n-1\} \\ |\mathbb{Z}_n^*| &= p \cdot q - p - q + 1 = \underbrace{(p-1)(q-1)}_{\phi(n)}\end{aligned}$$

με $\phi(n)$ τη συνάρτηση του Euler, που ορίζεται ως

$$\phi(m) = \begin{cases} m-1, & m \text{ πρώτος} \\ (p-1)p^{k-1}, & m = p^k, \quad p \text{ πρώτος} \\ \phi(p) \cdot \phi(q), & m = p \cdot q, \quad p, q \text{ πρώτοι} \end{cases}$$

Στη γενική περίπτωση, μία ομάδα $\mathbb{Z}_n^*$ θα έχει $\phi(n)$ στοιχεία.

11.1.2.1.1 Πρόβλημα Παραγοντοποίησης Εάν έχουμε τα $n, \phi(n)$, τότε μπορούμε να βρούμε τα p, q, δηλαδή έχουμε παραγοντοποιήσει το n.

$$\left.\begin{aligned} n &= p \cdot q \\ \phi(n) &= p \cdot q - p - q + 1 \end{aligned}\right\} A = p \cdot q, B = p + q$$

Εάν θεωρήσουμε ότι η παραγοντοποίηση ακεραίων τάξης n, όπου είναι γινόμενο μεγάλων πρώτων παρόμοιας τάξης, τότε και η εύρεση της τάξης της ομάδας θα είναι δύσκολη.

Εάν δεν έχουμε φτιάξει εμείς την ομάδα, είναι δύσκολο να βρούμε το n και την τάξη της. Εξακολουθούμε όμως να μπορούμε να κάνουμε πράξεις πάνω σε αυτήν(!).

Σε αυτή τη περίπτωση, η τάξη της ομάδας είναι το z — ή το trapdoor — του δημιουργού της.

11.1.2.2 Ψηφιακές υπογραφές RSA

Kiayias [4], κεφ. 7.6.

Textbook RSA (χρήσιμο μόνο για εκμάθηση, **όχι ασφαλές/επικίνδυνο**):

- $\text{Gen}(1^\lambda)$

$$\begin{aligned} &p, q \leftarrow \text{primes}(\lambda); n = pq \\ &e \leftarrow \mathbb{Z}_{\phi(n)}^* \\ &d = e^{-1} \mod \phi(n) \\ &vk = (n, e), \quad sk = (vk, d) \end{aligned}$$

- $\text{Sign}(sk, n)$

$$\sigma \leftarrow m^d \mod \phi(n)$$

- $\text{Ver}(vk, m, \sigma)$

$$m^* \leftarrow \sigma^e \mod \phi(n), \text{return } m^* == m$$

Ορισμός 11.1: Υπόθεση RSA

Ο καλύτερος τρόπος για να υπολογίζουμε ρίζες στην ομάδα $\mathbb{Z}_n^*$ είναι να βρούμε την τάξη της ομάδας.

Έχουμε αποδείξει ότι αν βρούμε την τάξη, σπάει η ομάδα. Δεν έχουμε αποδείξει το αντίθετο.

Το ότι η παραγοντοποίηση ακεραίων είναι δύσκολη δεν εγγυάται ότι και το σύστημά μας είναι ασφαλές.

Ορισμός 11.2: RSA problem

Έστω αντίπαλος $\mathscr{B}$. Δεδομένου ενός y, ο αντίπαλος κερδίζει αν βρει τη ρίζα $\sqrt[e]{y}$ mod n.

$$
\begin{aligned}
&p, q \leftarrow \text{primes}(\lambda)\\
&n \leftarrow pq\\
&e \leftarrow \mathbb{Z}^*_{\phi(n)}\\
&d = e^{-1} \mod \phi(n)\\
&x \leftarrow \mathbb{Z}^*_n; y \leftarrow x^e \iff x = y^d\\
&x^* \leftarrow \mathscr{B}(n, e, y)\\
&\texttt{return } x == x^*
\end{aligned}
$$

Για την ώρα, θέλουμε να αποδείξουμε ότι ο textbook RSA είναι ασφαλής απέναντι στον πιο αδύναμο αντίπαλο, δηλαδή αντίπαλο της *απλής* ($m \notin Q$) μορφής UUF-KOA.

Έστω ότι υπάρχει αντίπαλος $\mathscr{A}$ που παραβιάζει τη καθολική μη-πλαστογράφηση του RSA, γνωρίζοντας μόνο τα κλειδιά, δηλαδή σπάει το σύστημα υπογραφών RSA. Τότε υπάρχει αντίπαλος $\mathscr{B}$ που λύνει το πρόβλημα RSA (11.2): **ΆΤΟΠΟ**.

Απόδειξη

Έστω ο παρακάτω αντίπαλος $\mathscr{B}$:

$$
\begin{aligned}
&\mathscr{B}(n, e, y)\ :\\
&\qquad \sigma \leftarrow A(vk = (n, e), m = y)\\
&\qquad x^* = \sigma\\
&\qquad \texttt{return } x^*
\end{aligned}
$$

Ο $\mathscr{B}$ κερδίζει όταν $(x^*)^e = y$[a]. Επίσης, ο $\mathscr{A}$ κερδίζει όταν

$$\text{Ver}(vk, m, \sigma) = 1 \iff \sigma^e == m \iff (x^*)^e = y.$$

Άρα αν ο $\mathscr{A}$ κερδίζει με μη-αμελητέα πιθανότητα, με ίδια πιθανότητα ο $\mathscr{B}$ σπάει το RSA problem, το οποίο είναι άτοπο.

□

[a] η x^e είναι 1-1.

Έστω τώρα ότι ο αντίπαλος $\mathscr{A}$ έγκειται στην περίπτωση SEL. Τότε, δεν μπορούμε να του πούμε σε ποιο μήνυμα θα υπογράψει. Πλέον παύει να υφίστανται η παραπάνω απόδειξη.

$$\mathcal{B}(n, e, y) :$$
$$m \leftarrow A(1^\lambda)$$
$$\sigma \leftarrow A(vk = (n, e))$$
$$x^* = \sigma$$
$$\texttt{return } x^*$$

Αντίστοιχα σε περίπτωση που πρόκειται για τη περίπτωση του EUF.

$$\mathcal{B}(n, e, y) :$$
$$m, \sigma \leftarrow A(vk = (n, e))$$
$$x^* = \sigma$$
$$\texttt{return } x^*$$

Αυτό όχι απλά χαλάει την υπόθεση, αλλά δίνει την δυνατότητα στον $\mathcal{A}$ να **κερδίσει**.

Είπαμε ότι είναι εύκολο να πάμε από το σ στο m αλλά δύσκολο το ανάποδο. Όμως, όταν επιλέγουμε ένα ζευγάρι, δεν χρειάζεται να επιλέξουμε πρώτα το m.

Έχουμε τον ακόλουθο $\mathcal{A}$:

$$\mathcal{A}(n, e) :$$
$$\sigma^* \leftarrow \mathbb{Z}_n^*$$
$$m^* \leftarrow (\sigma^*)^e$$
$$\texttt{return } m, \sigma$$

Ανεξάρτητα του περιεχόμενου του m, αυτός ο αντίπαλος θα περάσει το verification και πλέον σπάει τον ορισμό.

Τώρα, θα ελέγξουμε τον άλλον άξονα, αυτόν των κλειδιών. Έστω ένας αντίπαλος $\mathcal{A}$ UUF-KMA. Εφόσον δεν έχουμε το d, δεν μπορούμε να φτιάξουμε υπογραφές για να δώσουμε στον αντίπαλο. Μπορούμε βέβαια να κάνουμε το ίδιο με τον παραπάνω αντίπαλο, και να παράγουμε τυχαία ζευγάρια μηνυμάτων και υπογραφών. Άρα η ασφάλεια είναι λίγο αμφίβολη.

Έστω τώρα ένας αντίπαλος $\mathcal{A}$ UUF-CMA. Όντας ο $\mathcal{B}$, πρέπει εμείς δρούμε ως το oracle S, κάτι που όμως δεν μπορούμε καθώς δεν μπορούμε να παράξουμε υπογραφές για δεδομένα μηνύματα $m \to \sigma$. Μπορούμε αντ'αυτού να δράσουμε ως *τυχαίο μαντείο* [4, κεφ. 7.3]. Η μόνη μας υποχρέωση είναι οι απαντήσεις μας να μην απέχουν στατιστικά σε μεγάλο βαθμό από ό,τι θα απάνταγε το πραγματικό μαντείο (oracle).

Για να "αποδείξουμε" σε αυτή τη περίπτωση την ικανότητα του $\mathcal{B}$ να σπάει το RSA problem, θα πρέπει να προσθέσουμε στο σχήμα ψηφιακών υπογραφών RSA και μία συνάρτηση κατακερματισμού [4, κεφ. 7.2] $H : \{0,1\}^* \to \{0,1\}^*$, η οποία είναι μονόδρομη (δύσκολο το $H(x) \to x$) και είναι ανθεκτική σε συγκρούσεις (δύσκολο ο αντίπαλος να βρει δύο στοιχεία x_1, x_2 τέτοια ώστε $H(x_1) = H(x_2)$). Άρα:

$$\mathcal{A}(H(x)) \not\to \overline{x} \mid H(x) = H(\overline{x})$$

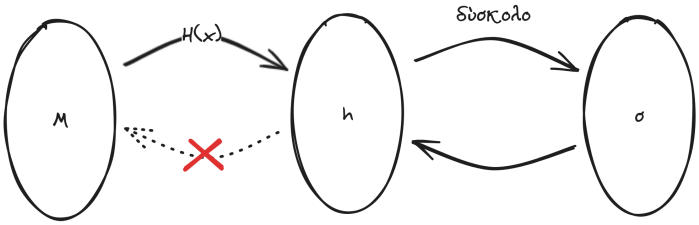
Άρα μετατρέπουμε το σχήμα ως εξής:

- $\text{Sign}(sk, n)$
$$\sigma \leftarrow H(m)^d \mod q(n)$$

- $\text{Ver}(vk, m, \sigma)$

$$H(m^*) \leftarrow \sigma^e \mod q(n), \text{return } m^* == m$$

Πλέον, τα μηνύματα κι οι υπογραφές έχουν την παρακάτω σχέση:



Εικόνα 6: ΘΠ05 Κρυπτογραφία 2024-04-21 21.37.30.excalidraw

Όταν μπούμε ως $\mathscr{B}$ στη μέση και δρούμε ως τυχαίο μαντείο, θα παρεμβάλουμε στον χώρο ανάμεσα στα μηνύματα και το hash-άρισμά τους. Έτσι, όταν ο $\mathscr{A}$ μας ρωτάει για το hash του m, εμείς θα του δίνουμε το y.

Το σημείο που χρήζει προσοχής εδώ είναι να μην μας καταλάβει ο αντίπαλος, π.χ. αν δίνουμε σε κάθε τιμή το y. Μια προσέγγιση είναι από τις T φορές που θα μας ρωτήσει ο $\mathscr{A}$, εμείς να "φυτέψουμε" το y την μία. Έτσι, αν ο $\mathscr{A}$ κερδίζει με πιθανότητα a, εμείς θα κερδίσουμε με πιθανότητα $a \cdot \frac{1}{T}$. Στην πραγματικότητα, η πιθανότητα αυτή είναι μικρότερη, γιατί ο αντίπαλος μπορεί να "τζογάρει" και να κάνει πλαστογραφία για ένα m που δεν ρώτησε για αυτό ποτέ το μαντείο. Αυτή η πλαστογραφία δεν είναι πιθανό να δουλέψει. Άρα θα κερδίζουμε με πιθανότητα $(a - \epsilon) \cdot \frac{1}{T}$.

12 2024-04-24 (Φροντιστήριο)

ex_3_2024gr.pdf sol_3_2024gr.pdf

12.1 Άσκηση 1

12.1.1 Ορθότητα

$$k = w \oplus t = u \oplus r \oplus t = s \oplus \not{t} \oplus r \oplus \not{t} = k \oplus \not{r} \oplus \not{r} = k$$

12.1.2 Ασφάλεια

Δημόσιες τιμές: s, u, w. Κρυφές τιμές: k, r, t.

$$w \oplus u \oplus s = \not{u} \oplus r \oplus \not{u} \oplus s = r \oplus s = \not{r} \oplus \not{r} \oplus k = k$$

12.2 Άσκηση 2

12.2.1 Ερώτημα (α')

Καταρχάς βρίσκουμε την τάξη του 4.

Το $\mathbb{Z}_{23}^*$ έχει 22 στοιχεία, καθώς 23 πρώτος. Πιθανοί διαιρέτες του 22: 22, 11, 2. Άρα η τάξη του 4 θα είναι ένα από αυτά τα τρία νούμερα.

Αποκλείουμε το 2 καθώς $4 \cdot 4 \equiv 16 \neq 1 \mod 23$.

Ύστερα, παρατηρούμε ότι $4 \equiv 2^2$ κι άρα ψάχνουμε την τάξη του 2, η οποία είναι είτε 11 είτε 22 (όχι 2 καθώς $2^2 \equiv 4 \neq 1 \mod 23$). Αν η τάξη του 2 είναι 11, τότε $\text{ord}(2^2) = 11$. Αν η τάξη του 2 είναι 22, τότε $(2^2)^{11} \equiv 1$, άρα η τάξη του 2^2 είναι ≤ 11. Άρα $\text{ord}(4) = 11$.

Εναλλακτικά, μπορούμε απλά να υπολογίσουμε το εξής: ισχύει $4^{11} \mod 23 = 1$;

$$\begin{aligned}
(16 \cdot 16 \cdot 4)^2 \cdot 4 &\mod 23 \\
(32 \cdot 32)^2 \cdot 4 &\mod 23 \\
(9 \cdot 9)^2 \cdot 4 &\mod 23 \\
(3 \cdot 27)^2 \cdot 4 &\mod 23 \\
12^2 \cdot 4 &\mod 23 \\
24 \cdot 24 &\mod 23 \\
1 \cdot 1 &\mod 23
\end{aligned}$$

12.2.2 Ερώτημα (β')

Η Αλίκη στέλνει $g^3 \equiv 4^3 \equiv \cdots \equiv 18$, ενώ ο Βασίλης $g^5 \equiv \cdots \equiv 12$.

Η Αλίκη υπολογίζει το $12^a = 12^3 \mod 23$.

$$\begin{aligned}
12 \cdot 12 \cdot 12 &\mod 23 \\
12 \cdot 2 \cdot 12 \cdot 2 \cdot 3 &\mod 23 \\
24 \cdot 24 \cdot 3 &\mod 23 \\
1 \cdot 1 \cdot 3 &\mod 23
\end{aligned}$$

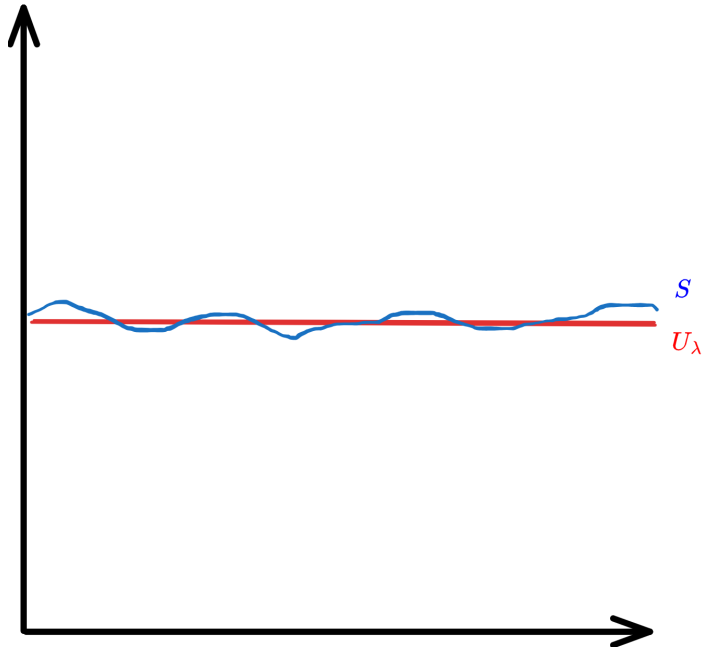
ενώ ο Βασίλης υπολογίζει το $18^b = 18^5 \mod 23$.

$$\begin{aligned}
2^5 \cdot 9 \cdot 9 \cdot 9 \cdot 9 \cdot 9 &\mod 23 \\
9 \cdot 2^5 \cdot 3 \cdot 27 \cdot 3 \cdot 27 &\mod 23 \\
9 \cdot 2^3 \cdot \underbrace{2 \cdot 3 \cdot 4}_{=24 \equiv 1} \cdot \underbrace{2 \cdot 3 \cdot 4}_{=24 \equiv 1} &\mod 23 \\
9 \cdot 4 \cdot 2 &\mod 23 \\
3 \cdot 3 \cdot 4 \cdot 2 &\mod 23 \\
3 &\mod 23
\end{aligned}$$

12.3 Άσκηση 6

Συμβολοσειρές s από λ bits από κατανομή S όπου $\Delta(S, U_\lambda) \leq \delta$. Ζητείται να αποδείξουμε ότι για το εκάστοτε bit μιας συμβολοσειράς s ισχύει $\Delta(s_i, U_1) \leq \delta$.

Έστω $B = \{0,1\}^\lambda$. $B_1 = \{s \in B \mid S_i = 1\}$ κι αντίστοιχα το B_0. Εμείς θέλουμε να βρούμε το $\Delta(S_i, U_1)$. Αυτή η απόσταση θα ισούται με το πλήθος των συμβολοσειρών που έχουν στο i 1 μείον $\frac{1}{2}$ από την ομοιόμορφη κατανομή συν το πλήθος των συμβολοσειρών που έχουν στο i 0 μείον $\frac{1}{2}$.



Εικόνα 7: Στατιστική απόσταση S, U_λ

$$\Delta = \frac{1}{2}\sum_{j=0}^{1} |\Pr[Y = j] - \Pr[V = j]|$$

$$= \frac{1}{2}|\Pr[Y = 1] - \Pr[U = 1]| + \frac{1}{2}|\Pr[Y = 0] - \Pr[V = 0]|$$

$$= \frac{1}{2}|\Pr[F(X) = 1] - \Pr[F(U) = j]| + \frac{1}{2}|\Pr[F(X) = 0] - \Pr[F(U) = 0]|$$

$$= \frac{1}{2}|\Pr[X \in B_1] - \Pr[U \in B_1]| + \frac{1}{2}|\Pr[X \in B_0] - \Pr[U \in B_0]|$$

$$= \frac{1}{2}|\Pr[X = t] - \sum_{t\in B_1}\Pr[U = t]| + \frac{1}{2}|\sum_{t\in B_0}\Pr[X = t] - \sum_{t\in B_0}\Pr[U = t]|$$

$$= \frac{1}{2}|\sum_{t\in B_1}|\Pr[X = t] - \Pr[U = t]|| + \frac{1}{2}|\sum_{t\in B_0}|\Pr[X = t] - \Pr[U = t]||$$

$$\leq \frac{1}{2}|\sum_{t\in B_1}|\Pr[X = t] - \Pr[U = t]|| + \frac{1}{2}|\sum_{t\in B_0}|\Pr[X = t] - \Pr[U = t]||$$

$$= \frac{1}{2}\sum_{t\in B_1}|\Pr[X = t] - \Pr[U = t]| + \frac{1}{2}\sum_{t\in B_0}|\Pr[X = t] - \Pr[U = t]|$$

$$= \frac{1}{2}\sum_{t\in B_1}|\Pr[X = t] - \Pr[U = t]|$$ [25]

$$\leq \delta$$

13 2024-04-26

13.1 Λύσεις εργασίας 1

- Άσκηση 2: Η 2 ρίψεις του ίδιου ζαριού και μία ρίψη δύο ζαριών **δεν είναι ίδιο πείραμα**.

13.2 Ψηφιακές υπογραφές RSA

Συνέχεια της εν. 11.1.2.2. Η απόδειξη βρίσκεται στο [4, κεφ. 7.4] για trapdoor functions, που εφαρμόζεται όμοια και στο σύστημα RSA.

Πλέον το Sign γίνεται ως $\text{Sign}(m) = h(m)^d \mod \phi(n)$ και το Ver ως $\text{Ver}(vk, m, d) = \sigma^e == h(m) \mod \phi(n)$.

Η τακτική που ακολουθούμε για την απόδειξη με αντιπάλους $\mathscr{A}, \mathscr{B}$ είναι η εξής: Για κάποιο από τα μηνύματα που ο A θα ρωτήσει το τυχαίο μαντείο, εμείς θα ορίσουμε το a. Έτσι δεν θα έχει σημασία αν ο αντίπαλος A είναι συνεργάσιμος ή όχι. Σημείωση: ελέγχουμε το EUF.

Ανά τις εκτελέσεις, ο αντίπαλος θα ρωτάει το hash διαφόρων μηνυμάτων. Εμείς ως το τυχαίο μαντείο θα απαντάμε με κάποια τυχαία τιμή $r_i \in \mathbb{Z}_n^*$. Για κάποιο $j^* \in \{1, \dots, q_H\}$ (όπου q_H το πλήθος ερωτήσεων), το hash του m_{j^*} θα απαντήσουμε ότι είναι το a του οποίου θέλουμε ο αντίπαλος να υπολογίσει τη ρίζα. Άρα σε όλες πέρα από μια ερώτηση απαντάμε κανονικά, έτσι δεν κινούμε την υποψία του αντιπάλου.

Για κάποιο από αυτά τα μηνύματα ο αντίπαλος θα παράξει μία πλαστογραφία, όπου εφόσον είναι καλός, θα έχει πιθανότητα να κάνει verify α μη-αμελητέα. Η πιθανότητα ο αντίπαλος να επιλέξει το m_{j^*} είναι $\frac{1}{q_H}$, *εφόσον όμως επιλέξει* m *το οποίο έχει ρωτήσει*. Άρα με πιθανότητα $\frac{\alpha}{q_h}$, καταφέραμε να πάρουμε τη ρίζα του a κι άρα "νικήσαμε" ως $\mathscr{B}$.

Τι γίνεται αν ο $\mathscr{A}$ ποντάρει σε ένα m που δεν έχει ρωτήσει; Η πιο απλή προσέγγιση είναι η εξής: Για κάθε αντίπαλο $\mathscr{A}$ υπάρχει ένας $\mathscr{A}'$ που *ρωτάει* για το m, άρα ουσιαστικά δεν υφίστανται στη γενική περίπτωση ο αντίπαλος να φτιάξει πλαστογραφία για άγνωστο m.

> Για κάθε αντίπαλο A που δεν ρωτάει, υπάρχει στο διπλανό κτίριο αντίπαλος που ρωτάει για το m.

Εναλλακτικά, σκεφτόμαστε το εξής: "Εφόσον ο αντίπαλος δεν ρώτησε για το m, ποια είναι η πιθανότητα η πλαστογραφία να πετύχει;". Η πιθανότητα να κερδίσει ο αντίπαλος από ένα m για το οποίο δεν έχει ρωτήσει, είναι ίση με $\Pr[z_0 = h(m)] = \frac{1}{|\mathbb{Z}_q^*|} \approx \frac{1}{2^\lambda} = \text{negl}$.

Στην παραπάνω απόδειξη, έχουμε αντίπαλο που μπορεί να υπογράψει ό,τι θέλει, αλλά δεν έχει πρόσβαση σε έτοιμες υπογραφές. Μετατρέποντας το πρόβλημα σε CMA, αναλαμβάνουμε εμείς την ευθύνη να παράγουμε αυτές τις υπογραφές. Μπορούμε να ξεγελάσουμε τον αντίπαλο ως εξής: Όταν λειτουργούμε ως τυχαίο μαντείο για hashes μηνυμάτων, αντί να επιλέγουμε ένα τυχαίο r_i, θα επιλέγουμε μια τυχαία υπογραφή $\sigma_i \in \mathbb{Z}_n^*$ κι άρα το r_i θα ισούται με σ_i^e. Οπότε, πλέον θα μπορούμε να υπογράψουμε το m_i, εάν μας το ζητήσει ο αντίπαλος. Αυτό γίνεται για κάθε m_i εκτός του m_{j^*}, καθώς αν το έστελνε στο τυχαίο μαντείο, δεν θα μπορούσε να το πλαστογραφήσει μετά.

Η πιθανότητα επιτυχίας $\frac{\alpha}{q_H}$ είναι κι αυτή μη-αμελητέα, καθώς είναι μη-αμελητέα ποσότητα προς πολυωνυμική ποσότητα.

Το τελευταίο εμπόδιο είναι το εξής: Η προσομοίωση που έχουμε κάνει στο τυχαίο μαντείο θα πρέπει να μην έχει γίνει αντιληπτή από τον αντίπαλο. Αυτό έχει σημασία γιατί η πιθανότητα

a υφίστανται όταν χρησιμοποιείται *κανονικό* τυχαίο μαντείο. Άρα πρέπει να αποδείξουμε ότι η προσομοίωσή μας έχει ίδια κατανομή με ένα πραγματικό τυχαίο μαντείο. Έχουν ίδια καθώς και στα δύο οι τιμές είναι τυχαίες από το $\mathbb{Z}_n^*$, το a δεν αλλάζει ουσιαστικά την κατανομή, καθώς δεν διαφέρει από μια τυχαία τιμή. Αυτό δεν ισχύει εάν συμπεριλάβουμε το a παραπάνω από μία φορές, δηλαδή για διαφορετικά m_i.

Βέβαια, μπορούμε να "μασκαρέψουμε" το a με κάποιο τρόπο (π.χ πολλαπλασιασμό με κάποιο τυχαίο r) σε άλλη θέση χωρίς να αλλάζει η κατανομή. Αυτή η μέθοδος όμως αποτυγχάνει, γιατί ο αντίπαλος μπορεί να μας ζητήσει υπογραφή για ένα από τα δύο a, ενώ εμείς δεν μπορούμε να υπογράψουμε κανένα από τα δύο.

Μέχρι τώρα μιλάμε για RSA full-domain hash. Όταν ο χώρος του H είναι πολύ μικρότερος από το $\mathbb{Z}_N^*$, τότε η απόδειξη χαλάει (βλ. διάλεξη μέρος 3 ~26').

14 2024-05-15 (Φροντιστήριο)

Πρώτα 40': επανάληψη αξόνων ορισμών UUF->SEL->EUF και KOA->KMA->CMA.

ex_4_2024gr.pdf sol_4_2024gr.pdf

14.1 Άσκηση 1

Είτε το έχει στείλει όντως ο Λυκούργος, είτε το έχει στείλει κάποιος κακόβουλος τρίτος, η Καρολίνα δεν θα πρέπει να εμπιστεύεται πλέον το συγκεκριμένο κλειδί.

> Αν το μήνυμα πράγματι προέρχεται από τον Λυκούργο, θα πρέπει να σταματήσει να εμπι στεύεται το αντίστοιχο κλειδί. Εάν το μήνυμα προέρχεται από κάποιο τρίτο χρήστη, αυτό σημαίνει ότι είτε το ιδιωτικό κλειδί του Λυκούργου διέρευσε (άρα πρέπει να μην εμπιστευόμαστε το αντίστοιχο δημόσιο) ή ότι υπάρχει μια γενικότερη επίθεση στο σχήμα υπογραφών.

14.2 Άσκηση 2

Αντίπαλος που σπάει την ανθεκτικότητα σε συγκρούσεις:

$$h \leftarrow H; x_0, x_1 \leftarrow A(h) \mid h(x_0) = h(x_1)$$

Αντίπαλος που σπάει την αντιστροφή:

$$h \leftarrow H; x \leftarrow X; y \leftarrow h(x); x^* \leftarrow A(h, y) \mid h(x^*) = y$$

Έστω ο A μπορεί να αντιστρέψει την h. Τότε, θα δείξουμε ότι μπορούμε να παράγουμε σύγκρουση.

1. Παίρνουμε $x \leftarrow X$ και την εικόνα του $y \leftarrow h(y)$
2. Δίνουμε το y στον αντίπαλο A και εκείνος μας επιστρέφει με πιθανότητα $\frac{1}{2}$ το x' που επίσης έχει εικόνα το y (γενικεύεται για πολλά x με ίδια εικόνα y)
3. Αν $x \neq x'$ και $h(x') = y$, "κερδίζουμε"

Το παραπάνω προϋποθέτει ότι το x **δεν έχει μοναδική εικόνα**. Για να "κερδίσουμε", πρέπει να δείξουμε ότι αυτό συμβαίνει "αρκετά συχνά" (έστω πιθανότητα p). Για να ισχύει κάτι τέτοιο, πρέπει το πεδίο ορισμού να είναι *σημαντικά μεγαλύτερο* από το πεδίο τιμών.

Αυτό δεν είναι τόσο δύσκολο. Αν π.χ. το πεδίο ορισμού αποτελείται από ένα παραπάνω bit, τότε θα έχουν μέγεθος $2N$ και N αντίστοιχα. Στην καλύτερη περίπτωση, τα $N-1$ στοιχεία του πεδίου τιμών θα είναι μοναδικές εικόνες και το 1 θα αναλαμβάνει όλες τις συγκρούσεις. Άρα από τα $2N$ στοιχεία του πεδίου ορισμού, τα $N-1$ έχουν μοναδική εικόνα. Αυτό σημαίνει ότι τα $2N-(N-1)=N+1$ στοιχεία **δεν** θα έχουν μοναδική εικόνα. Τότε, η πιθανότητα p παίρνει τιμή $\geq \frac{1}{2}$.

Συμπεραίνουμε ότι σε περιπτώσεις όπου η συνάρτηση κατακερματισμού συμπιέζει σημαντικά, η ανθεκτικότητα σε συγκρούσεις είναι *πιο ισχυρή έννοια* από τη δυσκολία αντιστροφής.

15 2024-05-17

Kiayias [4], κεφ. 4.

Ασφάλεια σε επικοινωνία μεταξύ A, B: απόκρυψη κι ακεραιότητα. Το δεύτερο το διασφαλίζουν οι ψηφιακές υπογραφές. Το αντικείμενο προς μελέτη πλέον είναι ο E που βλέπει την μεταξύ επικοινωνία να μην μπορεί να δει το μήνυμα m. Άρα το κρυπτογραφούμε στο κρυπτο-μήνυμα c, το οποίο θα πάρει ο B.

15.1 Κρυπτογράφηση ιδιωτικού κλειδιού

$$c = E(k, m)$$
$$m = D(k, c)$$

- Bottom notation: αποτυχία (υπολογισμού) $\triangleq \perp$.

Το πρόβλημα αυτού του σχήματος είναι ότι πρέπει να έχει προσυμφωνηθεί το κλειδί.

15.2 One-time pad

15.3 Κρυπτογράφηση δημοσίου κλειδιού

15.3.1 Σύνταξη

$$(pk, sk) \leftarrow \text{Gen}(1^\lambda)$$
$$c \leftarrow E(pk, m)$$
$$m \leftarrow D(sk, c)$$

15.3.2 Ιδιότητες

Σημείωση

Οι παραπάνω συναρτήσεις πρέπει να εκτελούν πολυωνυμικούς αλγορίθμους.

1. Ορθότητα (all-or-nothing chosen-plaintext attack/AON-CPA)

   $$\forall \lambda, m \leftarrow \mathcal{M}_\lambda \ : \ \Pr[(pk, sk) \leftarrow \text{Gen}(1^\lambda); c \leftarrow E(pk, m); m^* \leftarrow D(sk, c); m == m^*] = 1$$

2. Ασφάλεια

   $$\Pr[(pk, sk) \leftarrow \text{Gen}(1^\lambda); m \leftarrow \mathcal{M}_\lambda; c \leftarrow E(pk, m); m^* \leftarrow \mathcal{A}(c, pk); m^* == m] = \text{negl}(\lambda)$$

   ή

   $$\Pr[(pk, sk) \leftarrow \text{Gen}(1^\lambda); m \leftarrow \mathcal{M}_\lambda; c \leftarrow E(pk, m); sk^* \leftarrow \mathcal{A}(pk); sk^* \approx sk] = \text{negl}(\lambda),$$

όπου το *περίπου ίσο* για τα ιδιωτικά κλειδιά σημαίνει ότι το ένα κλειδί μπορεί να κάνει decrypt μηνύματα που μπορεί να κάνει και το άλλο, δηλαδή $\forall c, D(sk, c) = D(sk^*, c)$.

Ο πρώτος ορισμός είναι πιο ισχυρός, γιατί ένας αντίπαλος $\mathscr{A}$ που σπάει τον δεύτερο σίγουρα σπάει τον πρώτο, αλλά το αντίστροφο δεν ισχύει.

Στον πρώτο ορισμό, θεωρούμε ότι ο αντίπαλος δεν θα βρει *ολόκληρο* το μήνυμα, όμως δέχεται περιπτώσεις όπου γίνεται leak πληροφορία. Όμως, δεν σημαίνει ότι ο ορισμός δέχεται και το να αποκρύβεται μόνο το τελευταίο bit, γιατί η πιθανότητα να βρει το τελευταίο δεν είναι negligible. Ο ορισμός ικανοποιείται όσο το κρυφό μέρος του μηνύματος έχει τουλάχιστον 2^x bits, όπου το x είναι κάτι μεγαλύτερο από $\log(\lambda)$.

Εναλλακτικός ορισμός: **IND-CPA**. Παρακάτω, ο αντίπαλος είναι stateful ανάμεσα στις δύο κλήσεις του. Από τον ορισμό του IND-CPA, η E πρέπει να είναι τυχαία/μη-ντετερμινιστική. Αυτό γιατί στην αντίθετη περίπτωση, ο αντίπαλος μπορεί απλά να συγκρίνει τα encryptions των δύο μηνυμάτων. Θα πρέπει ο αντίπαλος στην παρακάτω επίθεση να έχει πιθανότητα επιτυχίας $\frac{1}{2} + \epsilon$.

$$
\begin{aligned}
(pk, sk) &\leftarrow \text{Gen}(1^\lambda) \\
m_0, m_1 &\leftarrow \mathscr{A}(pk) \\
b &\leftarrow \{0, 1\} \\
c^* &\leftarrow E(pk, m_b) \\
b^* &\leftarrow \mathscr{A}(c^*) \\
&\texttt{If } b == b^* \texttt{ return 1, else return 0.}
\end{aligned}
$$

15.3.3 (Απο)κρυπτογράφηση με RSA

- $\text{Gen}(1^\lambda) : p, q \leftarrow \text{Primes}(1^\lambda); N \leftarrow pq; e \leftarrow \mathbb{Z}_{\phi(N)}; d = e^{-1} \mod \phi(N)$
- $pk : (N, e)$
- $sk : d$
- $E(pk, m) : m^e$
- $D(sk, c) : c^d$

Η E σε αυτό το σχήμα είναι ντετερμινιστική. Άρα απαιτεί διόρθωση. Αυτή η παραλλαγή ονομάζεται RSA-OAEP:

> $E'(pk, m) : F(m)^e$, όπου η F είναι κάποια pseudo-random function.

Σημείωση

Όλα τα σχήματα κρυπτογράφησης αποτελούν σχήματα δέσμευσης κι έχουν τέλεια δέσμευση.

15.4 Κρυπτογράφηση ElGamal

Kiayias [4], εν. 9.3.

Η E περιέχει τυχαιότητα μέσω της τιμής r, άρα λύνεται το παραπάνω πρόβλημα.

15.5 Απόδειξη ασφάλειας

Έχουμε τα g, g^r, g^x και θέλουμε ο αντίπαλος να μην μπορεί να βρει το g^{rx}/να μην μπορεί να το ξεχωρίσει από οποιοδήποτε άλλο. Βλ. απόδειξη από σημειώσεις.

Προσοχή

Προσοχή στην απόδειξη θέλει το να δείξεις ότι με την αλλαγή μεταβλητών/εισόδου στον αντίπαλο A που λύνει το ElGamal, ότι δεν αλλάζει το πείραμα. Δηλαδή, ότι οι τιμές έχουν ίδια κατανομή κι ότι στέκουν στο σύστημα κρυπτογράφησης.

Παρόμοια με το RSA και το σχήμα του Pedersen, το σύστημα ElGamal έχει ομοιομορφικά μηνύματα, άρα μπορούμε να κάνουμε πράξεις πάνω σε αυτά. Π.χ.:

$$E(m_1)E(m_2) = E(m_1m_2) \iff (g^r, h^r, m_1)(g^{\bar{r}}, h^{\bar{r}}, m_2) = (g^{r+\bar{r}}, h^{r+\bar{r}}, m_1m_2)$$

Εάν ο αντίπαλος $\mathscr{A}$ έχει πρόσβαση σε ένα *ODec* (oracle D) και μπορεί να κάνει decrypt σε πράγματα που δεν έχει κάνει encrypt ο ίδιος (πέρα από το c^*, δηλαδή $\text{ODec}(c^*) = \perp$), λόγω της παραπάνω ιδιότητας θα μπορεί να κάνει κάποια πράξη στο c^*, π.χ. $c^*(g, h)$, και να στείλει αυτή τη τιμή στο ODec. Η παραλλαγή του ορισμού που λαμβάνει κι αυτό υπόψιν λέγεται IND-CCA (indecidability-chosen ciphertext attack). Συγκεκριμένα, πρόκειται για την παραλλαγή IND-CCA 2, όπου η πρόσβαση στο ODec δίνεται *αφού* ο A έχει δει το c^*.

16 2024-05-24

16.1 Zero-knowledge proofs

Kiayias [4], κεφ. 8.

> We have two parties, the prover $\mathscr{P}$and the verifier $\mathscr{V}$. $\mathscr{P}$must convince $\mathscr{V}$that she has some knowledge of a statement x without explicitly stating what she knows. We call this knowledge a witness w. Both parties are aware of a predicate R that will attest to $w$being a valid witness to x.

Παράδειγμα 16.1

Βλέπε παραδείγματα από σημειώσεις, κυρίως το "Η Μαγική Πόρτα" και "Ισομορφισμός Γραφημάτων" [4]. 7_zk_handout_gr.pdf

16.1.1 Ιδιότητες

Άτυποι ορισμοί. Για τους τυπικούς βλέπε σημειώσεις.

- **Πληρότητα**: Ο V πάντα αποδέχεται αληθείς προτάσεις αν η απόδειξη γίνει σωστά από τον P.
- **Εγκυρότητα**: Ο V δεν αποδέχεται ψευδείς προτάσεις (ακόμα και αν ο P προσπαθήσει να τον ξεγελάσει).
- **Μηδενική Γνώση**: Ο V δεν αποκομίζει τίποτα από την απόδειξη, πέρα από την ορθότητα της πρότασης.

Όσον αφορά τον τυπικό ορισμό της μηδενικής γνώσης, εάν ο αντίπαλος A τρέχει σε πολυωνυμικό χρόνο, έχουμε υπολογιστική μηδενική γνώση, ενώ αν δεν τρέχει απαραίτητα σε PPT, τότε έχουμε στατιστική ή τέλεια μηδενική γνώση.

Πιο χαλαρός ορισμός της μηδενικής γνώσης είναι η Honest Verifier Zero Knowledge (HVZK): Όταν ο verifier είναι *έντιμος*. Σε αυτή τη περίπτωση, $V^* \equiv V$.

16.2 Πρωτόκολλο του Schnorr

Kiayias [4], εν. 8.3.

Ο P αποδεικνύει ότι γνωρίζει το w διακριτό λογάριθμο $g^w = h$ χωρίς να αποκαλύψει το w.

Παραλλαγή πρωτοκόλλου v0.5

Αντί να γίνονται τρεις κινήσεις, ο P μπορεί μόνος του να

- επιλέγει $t \leftarrow \mathbb{Z}_q$
- βρίσκει το $a = g^t$
- θέτει $S = t + w$

κι έπειτα να στείλει τα S, a στον V ο οποίος μπορεί να κάνει την επαλήθευση ως $g^S = h \cdot a$.

Σε αυτή την εκδοχή, μπορούμε να κλέψουμε εάν θέσουμε

$$S = r, \quad a = h^{-1} g^r$$

άρα η επαλήθευση θα είναι "ορθή", αφού

$$g^r = h \cdot h^{-1} \cdot g^r$$

Εδώ φαίνεται η αναγκαιότητα της συμμετοχής του V μέσω του challenge e.

Όσον αφορά την εγκυρότητα, **δεν** υπάρχουν h ώστε να μην υπάρχει w ώστε $g^w = h$. Άρα ο P δεν μπορεί να πει ψέματα, πάντα θα υπάρχει μάρτυρας. Άρα το θέμα είναι αν ο P τον ξέρει ή όχι.

Στο πρωτόκολλο του Schnorr έχουμε *ειδική εγκυρότητα.*

16.3 Ειδική εγκυρότητα (special soundness)

Ορισμός 16.1: Ειδική εγκυρότητα

Ένα πρωτόκολλο 3 κινήσεων (με πρώτη κίνηση από τον P) είναι *ειδικά έγκυρο* αν υπάρχει PTM E τέτοια ώστε για οποιαδήποτε πρόταση x και οποιεσδήποτε 2 αποδεκτές συνομιλίες της μορφής $(a, c, s), (a, c', s')$ όπου $c \neq c'$, το $w \leftarrow E(x, a, c, c', s, s')$ αποτελεί μάρτυρα για το x, δηλαδή $R(x, w) = 1$.

Η ειδική εγκυρότητα είναι ισχυρότερη από την εγκυρότητα.

Ο εξαγωγέας E μας δίνει άρα μάρτυρα w ίσο με

$$\begin{aligned} g^S &= h^e a \\ g^{\tilde{S}} &= h^{\tilde{e}} a \end{aligned} \overset{e \neq \tilde{e}}{\Longrightarrow} g^{\frac{S - \tilde{S}}{e - \tilde{e}}} = h$$

17 2024-05-29 (Φροντιστήριο)

ex_4_2024gr.pdf sol_4_2024gr.pdf

17.1 Άσκηση 3

Αντιπαράδειγμα αποτελεί η ταυτοτική συνάρτηση.

17.2 Άσκηση 4

- Υποερώτημα (α')

  Αν έχουμε σύγκρουση, $\mathscr{H}'(x_0) = \mathscr{H}'(x_1) \iff \mathscr{H}(x_0 \,||\, 0000\ldots) = \mathscr{H}(x_0 \,||\, 0000\ldots)$. Άρα προκύπτει σύγκρουση και στην αρχική $\mathscr{H}$, άρα **άτοπο**.

- Υποερώτημα (β')

  Παρομοίως, η αρχική ανεκτικότητα σε συγκρούσεις δεν χαλάει.

- Υποερώτημα (γ')

  Αν η $\mathscr{H}_i$ ήταν παρόμοια με την $\mathscr{H}_i''$, αλλά με τα μηδενικά στην αρχή, τότε δεν θα ίσχυε ανθεκτικότητα στις συγκρούσεις.

  Σημείωση

  Πρακτικά, εάν κόψουμε το $\frac{1}{8}$ των bits, θα χάσουμε περίπου το $\frac{1}{8}$ της ασφάλειας, μπορεί να θεωρηθεί σχετικά ασφαλή κατασκευή, αν και δεν είναι ασυμπτωτικά ασφαλή.

- Υποερώτημα (δ')

  Ίδιο σκεπτικό με το (γ').

18 2024-05-31

Kiayias [4], κεφ. 8.3.

18.1 Εγκυρότητα πρωτοκόλλου Schnorr

Schnorr Protocol = Σ-protocol.

Ορισμός 18.1: Ειδική Εγκυρότητα

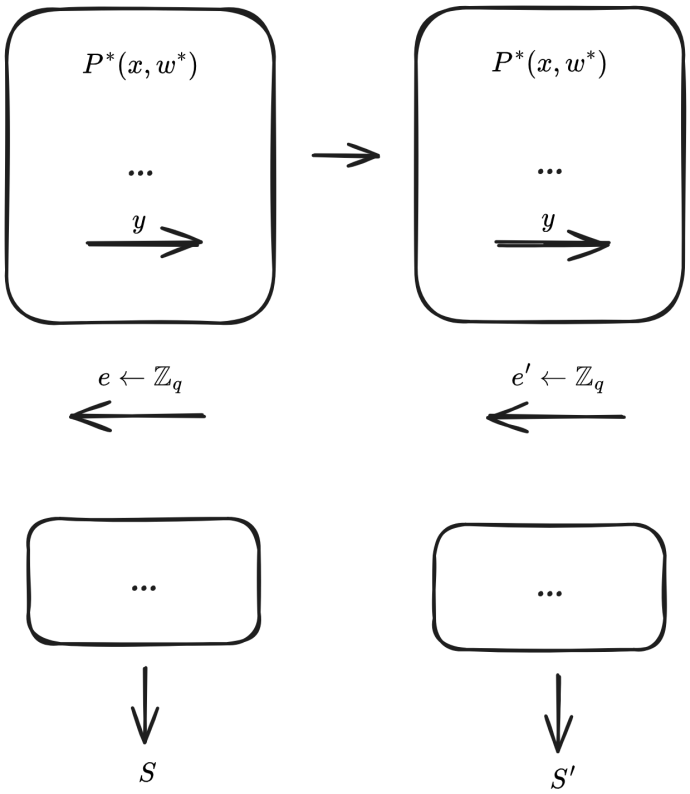
Αν έχουμε δύο πλειάδες της μορφής (y, e, S) και (y, e', S') — δεδομένου του ίδιου x — με $e \neq e'$ και ο Verifier επιστρέφει και για τα δύο 1, τότε υπάρχει Extractor $E(y, e, e', S, S') \to w$ όπου $R(x, w) = 1$.

Άρα σε περίπτωση όπου ισχύει η ειδική εγκυρότητα, μπορούμε να πάρουμε τον μάρτυρα.

Από την ειδική εγκυρότητα, προκύπτει οτι

$$w = \frac{S - S'}{e - e'} \mod m.$$

Είναι σχεδόν απίθανο να προκύψουν φυσικά ζεύγη πλειάδων με ίδιο y. Κάτι τέτοιο γίνεται μέσω του εξαγωγέα γνώσης K όπου μπορεί να παγώσει τον Prover και να τον ξανατρέξει για ίδιο y.



Εικόνα 8: Εκτέλεση του K. Με κάποια πιθανότητα p και p', θα ισχύει ότι $g^S = h^e y$ και $g^{S'} = h^{e'} y$ αντίστοιχα.

Στην παραπάνω διαδικασία, δεν είμαστε σίγουροι για το δεύτερο σκέλος, δηλαδή ότι $g^{S'} = h^{e'} y$, καθώς αυτό το "run" του πρωτοκόλλου εξαρτάται από το ίδιο y με πριν. Άρα μπορεί να προκύψουν καλά και κακά e, όπου η ισότητα ισχύει και δεν ισχύει αντίστοιχα. Αν ο αντίπαλος έχει φροντίσει έτσι ώστε για κάθε y να μην υπάρχουν πολλά καλά e, πιθανώς δεν θα βρούμε άλλο καλό e. Αυτό δεν γίνεται χωρίς η πιθανότητα του P^* να επιτύχει να γίνεται αμελητέα. Βλέπε απόδειξη "heavy rows".

Η εγκυρότητα καθαυτή δείξαμε στο προηγούμενη μάθημα ότι είναι τετριμμένη, καθώς $h \in \langle g \rangle$ άρα υπάρχει κατάλληλο DLog. Για αυτό, θα απαιτήσουμε εγκυρότητα γνώσης, δηλαδή να αποδειχθεί ότι ο P όντως *ξέρει* έναν μάρτυρα w. Άρα, στην απόδειξή μας εξετάζουμε έναν P^* που μπλοφάρει. Βλέπε [4, εν. 8.3] για απόδειξη.

Πόρισμα της απόδειξης είναι ότι *ειδική εγκυρότητα* $\iff$ *εγκυρότητα γνώσης* (για Σ-πρωτόκολλα).

18.2 Απόδειξη heavy rows

Έστω ένας πίνακας $X \times Y$ και σύνολο A μεγέθους $|A| = |X| \cdot |Y| \cdot a$ τα "καλά" στοιχεία (έστω τα κελιά που έχουν 1), όπου a μη-αμελητέο. Ψάχνουμε την εξής πιθανότητα:

$$\Pr\left[(i,j) = 1 \wedge (i,k) = 1 \mid i \xleftarrow{\$} X, j, k \xleftarrow{\$} Y\right]$$

δηλαδή δύο σημεία στην ίδια γραμμή όπου είναι και τα δύο άσοι.

Θα λέμε ότι μία γραμμή είναι "βαριά" όταν $\#(i,m) \mid (i,m) = 1 \geq \frac{a}{2}|Y|$.

Πλέον καλούμαστε να απαντήσουμε στο εξής ερώτημα:

> Πόσοι άσοι βρίσκονται σε ελαφριές γραμμές;

Έστω η παραπάνω τιμή Z. Μια ελαφριά γραμμή έχουν πλήθος από $1 < \frac{a}{2}|Y|$. Όλες οι γραμμές είναι $|X|$. Έστω όλες ελαφριές. Τότε,

$$Z \leq |X|\frac{a}{2}|Y|$$

Αυτό δείχνει ότι το πολύ οι μισοί άσοι ζούνε σε ελαφριές γραμμές, άρα τουλάχιστον οι μισοί άσοι ζούνε σε βαριές γραμμές.

Καταλήγουμε στο ότι σε ένα κελί έχουμε τις εξής πιθανότητες:

- Με πιθανότητα $1 - a$, έχουμε 0
- Με πιθανότητα $\frac{a}{2}+$ θα έχουμε 1 σε βαριά γραμμή
- Με πιθανότητα $\frac{a}{2}-$ θα έχουμε 1 σε ελαφριά γραμμή

Σημείωση

Για τη συνέχεια, δες απόδειξη εγκυρότητας Schnorr από σημειώσεις. Το ζητούμενο είναι στις εκτελέσεις του K να πετύχουμε βαριά γραμμή.

Με πιθανότητα $\frac{a^2}{4} - \frac{1}{q}$ ο K παράγει δύο συζητήσεις $(y,e,s),(y,e',s')$ με $e \neq e'$.

18.3 Μηδενική γνώση πρωτοκόλλου Schnorr

Η λογική είναι να βρούμε τριάδες που δέχεται ο V χωρίς όμως να ξέρουμε κάποιον μάρτυρα και κανονικές τριάδες, και να δείξουμε ότι αυτές έχουν ίδια πιθανοτική κατανομή.

19 2024-06-05 (Φροντιστήριο)

ex_5_2024gr.pdf sol_5_2024gr.pdf

19.1 Άσκηση 1

$$E = (g^{r_1+r_2}, h^{r_1+r_2} \cdot m_1 \cdot m_2) = (g^{r'}, h^{r'} \cdot m')$$

Εμμέσως κάνουμε πράξεις με τα μηνύματα m_1, m_2.

19.2 Άσκηση 2

Παίρνουμε τυχαίο $x \leftarrow \mathbb{Z}_{11}$, καθώς $q = 11$. Έστω $x = 3$. Τότε $h = g^x = 8$ $(2^3 \mod 23)$.

$m = 6$. Χρειαζόμαστε μία τιμή για το r. Έστω $r = 7$. $g^r = 2^7 = 13 \mod 23, h^r = 8^7 = 12 \mod 23 \implies h^r m = 3 \mod 23$. Άρα

$$E = (\underset{u}{13}, \underset{v}{3}).$$

Για να το αποκρυπτογραφήσουμε, παίρνουμε:

$$m^d = \frac{v}{u^x} = \frac{3}{13^3} = \frac{3}{12} = 3 \cdot (12^{-1}) = 3 \cdot 2 \mod 23 = 6 \mod 23$$

19.3 Άσκηση 3 (SOS)

$$\mathbb{Z}_p^* = \phi(p) = p - 1 = 2k, k \in \mathbb{N}$$

Άρα η ομάδα έχει πλέον τάξη σύνθετη, όχι πρώτη.

Προσοχή

Πλέον το DDH **παύει να είναι δύσκολο**.
Αυτό γιατί από τη στιγμή που η τάξη της ομάδας έχει παράγοντα το 2, ένα στοιχείο $f^{2k} \equiv 1$. Το f^k κάνει είτε 1 είτε όχι, που όμως αυτό στο τετράγωνο θα κάνει 1, άρα το f^k στην πραγματικότητα θα είναι -1.
Εφόσον $f^k \equiv 1$, $f = g^{2\lambda}$. Αν $f^k \not\equiv 1$, $f = g^{2\lambda+1}$. Άρα, τα στοιχεία που μας δίνουν 1 έχουν άρτιο εκθέτη ενώ τα υπόλοιπα περιττό, δηλαδή περίπου μισά-μισά. Τώρα, όσον αφορά το πρόβλημα DDH, θα μπορούμε πλέον να πάρουμε περιπτώσεις για τα a, b. Για τριάδες DDH, το ab θα είναι περιττό μόνο αν και τα δύο a, b είναι περιττά. Πέρα από αυτό, λόγω των περιπτώσεων, σε τριάδες DDH θα έχουμε 4 πιθανά σενάρια, όμως σε τυχαίες τριάδες θα έχουμε **8**. Εάν η τριάδα που έχουμε πέφτει στις περιπτώσεις που δεν καλύπτουν οι τριάδες DDH, π.χ. 'άρτιος-άρτιος-περιττός', θα ξέρουμε ότι πρόκειται για τυχαία τριάδα.

Με παρόμοιο τρόπο "σπάει" και το ElGamal. Εάν αντικαταστήσουμε τα a, b με g^r, h, ένας αντίπαλος θα μπορεί να τεστάρει την αρτιότητά τους, άρα βρίσκει και την αρτιότητα του h^r, όπου θα έχει πιθανότητα $\frac{3}{4}$ να είναι άρτιος.

Εφόσον ξέρει την αρτιότητα του h^r, μπορεί να στείλει m_0 άρτιο και m_1 περιττό κι ύστερα να βρει ποιο από τα δύο έχει κρυπτογραφηθεί.

19.4 Παραλλαγή άσκησης 5

Επέκταση πρωτοκόλλου Schnorr: Απόδειξη γνώσης ανοίγματος σχήματος Pedersen.

20 2024-06-07

20.1 Μη-διαδραστικές αποδείξεις μηδενικής γνώσης

Kiayias [4], κεφ. 8.4.

Αντικαθιστούμε το e με το $H(h, A)$, όπου H μια hash function/τυχαίο μαντείο.

Όταν ο Prover έχει μη-αμελητέα πιθανότητα να παράγει σωστές αποδείξεις, συνεπάγεται ότι χρησιμοποιεί το μαντείο για τα e και δεν τα βγάζει ο ίδιος από το $\mathbb{Z}_q$. Αντίστοιχα για όταν δεν παράγει σωστές αποδείξεις.

Όσο δίνουμε τα ίδια e_i στον P, δεν καταλαβαίνει ότι έχει κλωνοποιηθεί.

20.2 Ηλεκτρονικές εκλογές

Έστω έμπιστος διοργανωτής εκλογών A. Στην πιο απλή περίπτωση, κάθε ψηφοφόρος θα έλεγε στον A την ψήφο του $\in \{0, 1\}$ και ο A θα ανακοίνωνε το αποτέλεσμα.

Έστω ένας πίνακας ανακοινώσεων BB (bullet board). Ο κάθε ψηφοφόρος καρφιτσώνει την ψήφο του σε αυτόν τον πίνακα. Κάθε ψήφος είναι κρυπτογραφημένη.

Διαφορετικές εκδοχές:

1. Κάθε ψηφοφόρος ετοιμάζει ψηφοδέλτιο Ψ και το στέλνει μαζί με την ταυτότητά του και την υπογραφή του σ.
2. Τη κάθε ψήφο να την υπογράφει ένα TTP (εκδοχή τυφλών υπογραφών). Το TTP δεν θα πρέπει να γνωρίζει την κάθε ψήφο.
3. Χρήση Mixnet: Ένας πράκτορας M παίρνει τις ψήφους, τις ανακατεύει και τις κρυπτογραφεί. Αυτό λέγεται *επανατυχαιοποίηση*. Κρατώντας το ανακάτεμα κρυφό, αποκρύβουμε τη σχέση ψηφοφόρου–ψήφου. Αυτό το σύστημα είναι ευάλωτο ανάμεσα σε κακόβουλους M. Αυτό λύνεται με συγκεκριμένα πρωτόκολλα. Επίσης χρησιμοποιούνται πολλοί M σειριακά.
4. Μπορούμε να πάρουμε ένα $\Psi_\sum$ που θα είναι το άθροισμα/γινόμενο όλων των ψηφοδελτίων. Κάθε ψηφοφόρος στέλνει ένα κρυπτογραφημένο μήνυμα $\Psi_i = E(g^{V_i}), V_i \in \{0, 1\}$. Άρα παίρνουμε ένα μεγάλο ψηφοδέλτιο $g^{r_\Sigma}, h^{r_\Sigma} \cdot g^{\sum V_i}$. Ο εκθέτης του τελευταίου είναι το αποτέλεσμα των εκλογών. Το αποτέλεσμα σε αυτήν την περίπτωση μπορούμε να κάνουμε bruteforce τον εκθέτη, καθώς η τιμή φράζεται από το πλήθος των ψηφοφόρων. Εδώ υπάρχει πρόβλημα όσον αφορά αυτόν που αποκρυπτογραφεί τελικά το αποτέλεσμα. Εδώ κολλάει το πρωτόκολλο του Schnorr. Όμως, ο έφορος μπορεί να αποκρυπτογραφήσει την ψήφο κάποιου, κι άρα να παραβιάσει το απόρρητό του. Αυτό λύνεται έχοντας πολλούς εφόρους. Το κλειδί του ElGamal θα είναι

   $$h = h_1 \cdot h_2 \cdot \ldots$$

   όπου κάθε κλειδί θα αντιστοιχεί σε κάθε έφορο. Ευάλωτο σε κακόβουλους ψηφοφόρους, π.χ. να ψηφίσει 2, που θα γίνεται εφόσον στέλνει την κρυπτογράφηση $E(g^{V=2})$. Χρειαζόμαστε ένα πρωτόκολλο που θα εγγυάται ότι η ψήφος είναι αποδεκτή. Αυτό γίνεται με το να ελέγχεται αν η κρυπτογράφηση είναι τύπου $E(g^0)$ ή $E(g^1)$. Μορφή $E(g^0)$ θα έχει όταν η ψήφος είναι g^r, h^r. Το point όμως είναι να μην ξέρουμε ποια από τις 2 μορφές έχει, μόνο το ότι έχει κάποια από αυτές τις 2. Αυτό γίνεται με παραλλαγή του Schnorr όπου στέλνονται A_0, A_1, επιστρέφεται **ένα** e και στέλνονται e_0, e_1, S_0, S_1 όπου $e_0 + e_1 = e$. Εφόσον μόνο η μία περίπτωση είναι αληθής, στην μία περίπτωση τρέχουμε τον Prover και στην άλλη τον $\text{Sim}(A_0, e_0^*, S_0)$.

21 2024-06-14

Πληροφορία

Ένας αλγόριθμος $\mathscr{A}$ που σπάει το ElGamal μπορεί να χρησιμοποιηθεί από αντίπαλο $\mathscr{B}$ για να σπάσει και το DDH.

- ElGamal:
$$E(m_0) \cdot E(m_1) = E(m_0 * m_1),$$
όπου $m_{0,1} \leftarrow \mathbb{G}$.
- Pedersen:
$$C(m_0) \cdot C(m_1) = C(m_0 + m_1),$$
όπου $m_{0,1} \leftarrow \mathbb{Z}_q$.

Σύνολα των πρωτοκόλλων

ElGamal: $\mathscr{M} : \mathbb{G}, \mathscr{C} : \mathbb{G}^2, \mathscr{R} : \mathbb{Z}_q, \mathscr{PK} : \mathbb{G}$.

Pedersen: $\mathscr{M} : \mathbb{Z}_q, \mathscr{C} : \mathbb{G}, \mathscr{R} : \mathbb{Z}_q, \mathscr{CK} : \mathbb{G}$.

Κάποιος που μπορεί να λύσει το DLog λύνει και το DDH, **όχι το αντίστροφο**.

Η υπολογιστική δυσκολία του DDH μπορεί να εκφραστεί ως ο αντίπαλος να μη μπορεί να ξεχωρίσει

- $(U, V) = E(m)$ και
- $(U, V) = (X, Y)$ τυχαία στο $\mathbb{G}^2$

21.1 Υπογραφές

Uni_Defs-beta1.pdf

1. Textbook RSA
2. RSA full hash

21.1.1 Υπογραφές Schnorr

Ίδιο πρωτόκολλο, μόνο που $h = g^w, m$ και το m εμπεριέχεται στο encryption ως $e = \mathscr{H}(\mathbb{G}, h, m, A)$. Αποδεικνύεται από τη $\pi = (A, e, S)$. Στην ουσία, απλά το μήνυμα είναι μέρος του hash.

Blueprint απόδειξης unforgeability: Εάν ο αντίπαλος μπορεί να υπογράφει, θα πάρουμε το w. Θα τον κάνουμε να υπογράψει το ίδιο πράγμα δύο φορές, καθώς ελέγχουμε το τυχαίο μαντείο, δίνοντάς του δύο διαφορετικά e.

Blueprint ασφάλειας CMA: Υπογράφουμε χωρίς να ξέρουμε το w. Αυτό γίνεται μέσω simulation. Αυτό είναι εφικτό καθώς ελέγχουμε το τυχαίο μαντείο.

Ο αντίπαλος A μας ζητάει υπογραφή στο m_0. Εμείς ξέρουμε $h, \mathbb{G}, g, q$. Καλούμαστε άρα να υπολογίσουμε τα

$$e = \mathscr{H}(\mathbb{G}, h, m_0, A), A = g^t, t \leftarrow \mathbb{Z}_q$$
$$g^s = h^e A$$

Χρησιμοποιούμε simulator. Έτσι:

$$S \leftarrow \mathbb{Z}_q$$
$$e \leftarrow \mathbb{Z}_q$$
$$A = g^S h^{-e}$$
$$\mathscr{H}(\mathbb{G}, h, m, A) \leftarrow e$$

21.2 Θέματα Ιουνίου 2021

21.2.1 Θέμα Α

21.2.1.1 Α1

- Η αλλαγή με $r \leftarrow \mathscr{H}(m)$ είναι ευάλωτη σε replay attacks. Επίσης, από υποθέσεις για το μήνυμα μπορούμε να μαντέψουμε το άνοιγμα.
- Ουσιαστικά το ίδιο πρωτόκολλο, απλά χωρισμένο σε offline και online, έχοντας κάνει από πριν τις δύσκολες πράξεις. Σαν να κάνουμε cache τις ακριβές τιμές.
- Εάν γίνει compromised κάποιο r, ύστερα μπορούμε να σπάσουμε οποιοδήποτε cipher. Δηλαδή το επόμενο μήνυμα θα είναι $u \cdot g, \tilde{v} \cdot h \cdot m_2$. Κάθε μεμονωμένη εκτέλεση όμως **δεν** παραβιάζει το IND-CPA (όπως τον έχουμε ορίσει στις σημειώσεις).

21.2.1.2 Α2

Έλεγχος κλειστότητας και ύπαρξη ουδέτερου και αντίστροφου.

21.2.2 Θέμα Β

21.2.2.1 Β1

Ίδιο με της εργασίας 2.

21.2.2.2 Β2

Υπογραφές: ίδιο με εργασίας 2.

Κρυπτογράφηση: Είναι ασφαλές εφόσον δεν παραβιάζει το IND-CPA, καθώς η κρυπτογράφηση του 0 και του 1 δεν θα είναι ίδιες ανάμεσα στις διαφορετικές εμφανίσεις τους.

21.2.3 Θέμα Γ

- Η ύψωση σε δύναμη γίνεται με square multiply, η διαίρεση είναι οκ και ο έλεγχος $m \in \mathbb{G}_k$ είναι γραμμικός ως προς το λ.
- Ίδια απόκρυψη με τον Pedersen.
- $h^{r'} m' = h^r m$. Εφόσον έχουμε μόνο λ περιπτώσεις, μπορούμε να αντικαταστήσουμε τα m, m' με δυνάμεις του g. Άρα μετά με πράξεις θα μπορούμε να λύσουμε το DLog του h ως προς το g.

21.2.4 Θέμα Δ

21.2.4.1 Δ1

- $S \leftarrow \mathbb{Z}_q, y = g^s \cdot h^{-e}$
- $S = w + a, y = g^a$
- $S = w, y = e$

21.2.4.2 Δ2

Το πρώτο από τα 3 έχει μηδενική γνώση κι είναι πλήρης. Ο prover αποτελεί και simulator. Δουλεύει για οποιονδήποτε verifier.

Αναφορές

[1] J. Katz και Y. Lindell, *Introduction to Modern Cryptography* (Chapman & Hall/CRC Cryptography and Network Security Series), Third edition. Boca Raton London New York: CRC Press Taylor & Francis Group, 2021, 626 **pagetotals**, ISBN: 978-0-8153-5436-9.

[2] S. D. Galbraith, *Mathematics of Public Key Cryptography*, 2η έκδοση. Cambridge University Press, 31 Οκτ. 2018. διεύθν.: https://www.math.auckland.ac.nz/~sgal018/crypto-book/crypto-book.html.

[3] V. Shoup, *A Computational Introduction to Number Theory and Algebra*. Cambridge university press, 2009. διεύθν.: https://shoup.net/ntb/.

[4] A. Kiayias, *Cryptography, Primitives and Protocols*, Draft. 18 Μαρ. 2022, 108 **pagetotals**. διεύθν.: https://crypto.di.uoa.gr/class/Kryptographia/Semeioseis_files/Cryptograph_Primitives_and_Protocols-20220318.pdf.