ΜΑΘΗΜΑΤΙΚΟ ΚΑΙ ΥΠΟΛΟΓΙΣΜΙΚΟ ΥΠΟΒΑΘΡΟ

ΜΕΡΟΣ Ι: ΘΕΩΡΙΑ ΑΡΙΘΜΩΝ - ΘΕΩΡΙΑ ΟΜΑΔΩΝ - ΠΙΘΑΝΟΤΗΤΕΣ

Η ΑΝΑΓΚΑΙΟΤΗΤΑ ΤΩΝ ΜΑΘΗΜΑΤΙΚΩΝ ΣΤΗΝ ΚΡΥΠΤΟΓΡΑΦΙΑ

Θα παρουσιάσουμε ορισμένα στοιχεία από την Θεωρία Αριθμών, την Θεωρία Ομάδων και την Θεωρία Πιθανοτήτων. Οι έννοιες στις οποίες θα αναφερθούμε παίζουν σημαντικό ρόλο στον ορισμό, την υλοποίηση και την ασφάλεια των σύγχρονων κρυπτοσυστημάτων.

ΘΕΩΡΙΑ ΑΡΙΘΜΩΝ - ΔΙΑΙΡΕΤΟΤΗΤΑ & ΠΡΩΤΟΙ ΑΡΙΘΜΟΙ

- **Διαιρετότητα:** Ορισμός: Ο a διαιρεί τον b ($a|b$) αν $b=ka$ για κάποιο ακέραιο k.
- **Ακέραια Διαιρετότητα (Division Algorithm):** Για $a>0$, κάθε ακέραιος b γράφεται μοναδικά ως $b=qa+r$, όπου $0\leq r<a$ (q είναι το πηλίκο, r το υπόλοιπο).
- **Πρώτοι Αριθμοί:** Ένας ακέραιος $p>1$ είναι πρώτος αν οι μόνοι θετικοί διαιρέτες του είναι το 1 και ο p.
- **Θεμελιώδες Θεώρημα Αριθμητικής:** Κάθε ακέραιος $n>1$ αναλύεται μοναδικά σε γινόμενο πρώτων παραγόντων.

ΜΕΓΙΣΤΟΣ ΚΟΙΝΟΣ ΔΙΑΙΡΕΤΗΣ & ΣΥΝΑΡΤΗΣΗ EULER ϕ(n)

- **Μέγιστος Κοινός Διαιρέτης (ΜΚΔ):** Ορίζεται ως gcd(a,b) ο μεγαλύτερος ακέραιος που διαιρεί τους a και b.
- **Συνάρτηση Euler ϕ(n):** Δίνει το πλήθος των ακεραίων a στο σύνολο {1,2,…,n-1} που είναι πρώτοι προς το n (δηλαδή gcd(a,n)=1).
- **Ιδιότητα ϕ για πρώτο αριθμό p:** $\phi(p)=p-1$.
- **Ιδιότητα ϕ για n=$p_1^{e1}p_2^{e2}\dots p_k^{ek}$:** $\phi(n)=n\prod_{i=1}^{\kappa}(1-1/p_i)$.

ΣΧΕΣΗ ΙΣΟΤΙΜΙΑΣ (CONGRUENCE)

- **Ορισμός:** Δύο ακέραιοι a και b λέγονται ισότιμοι modulo n (σχέση ισοτιμίας) αν n|(a-b), δηλαδή αν a και b έχουν το ίδιο υπόλοιπο στη διαίρεση με το n.
- **Συμβολισμός:** $a \equiv b \pmod{n}$.
- **Ιδιότητες:**
- $a \equiv b \pmod{n} \Rightarrow a+c \equiv b+c \pmod{n}$.
- $a \equiv b \pmod{n} \Rightarrow ac \equiv bc \pmod{n}$.
- $a \equiv b \pmod{n} \Rightarrow a^k \equiv b^k \pmod{n}$

ΠΑΡΑΔΕΙΓΜΑ 1: ΥΠΟΛΟΓΙΣΜΟΣ φ(n) ΚΑΙ ΙΣΟΤΙΜΙΕΣ

- **Ερώτημα 1: Ποια είναι η τιμή της συνάρτησης φ(15);**

Λύση: $15=3\cdot5$.

Άρα: $\phi(15)=15\cdot(1-1/3)\cdot(1-1/5)=15\cdot(2/3)\cdot(4/5)=8$.

Σύνολο: {1,2,4,7,8,11,13,14} (8 αριθμοί)

- **Ερώτημα 2: Ποιο είναι το υπόλοιπο του 2^{100} (mod3);**

Λύση: $2 \equiv -1 \pmod 3$. Άρα, $2^{100} \equiv (-1)^{100} \equiv 1 \pmod 3$.

Επομένως το υπόλοιπο είναι το 1.

ΘΕΩΡΗΜΑ EULER ΚΑΙ FERMAT

Θεώρημα Euler: Αν $\gcd(a,n)=1$, τότε $a^{\phi(n)} \equiv 1 \pmod{n}$. •

Μικρό Θεώρημα Fermat: Ειδική περίπτωση του Euler: $a^{p-1} \equiv 1 \pmod{p}$.

Βάση RSA: Το Θεώρημα Euler επιτρέπει την αποκρυπτογράφηση: $M^{ed} \equiv M \pmod{n}$.

ΘΕΩΡΙΑ ΟΜΑΔΩΝ - ΒΑΣΙΚΕΣ ΕΝΝΟΙΕΣ

Ομάδα (Group): Ένα σύνολο G με μια πράξη $*$ που ικανοποιεί: κλειστότητα, προσεταιριστική ιδιότητα, ύπαρξη ουδέτερου στοιχείου, και ύπαρξη αντίστροφου στοιχείου για κάθε μέλος.

Σώμα (Field): Ένας δακτύλιος όπου όλα τα μη-μηδενικά στοιχεία έχουν αντίστροφο. Η σχέση μεταξύ του σώματος (field) και της ομάδας (group) είναι μια σχέση δομικής υπεροχής στην αφηρημένη άλγεβρα. Κάθε σώμα εμπεριέχει δύο ομάδες.

Αβελιανή Ομάδα: Μια ομάδα όπου ισχύει και η αντιμεταθετική ιδιότητα ($a*b=b*a$).

Κυκλική Ομάδα: Μια ομάδα όπου όλα τα στοιχεία μπορούν να παραχθούν από ένα μόνο στοιχείο (γεννήτορα).

Σημασία στην Κρυπτογραφία: Οι ομάδες Z_n (πρόσθεση modulo n) και Z_n^* (πολλαπλασιασμός modulo n με στοιχεία πρώτα προς n) είναι θεμελιώδεις για τα κρυπτοσυστήματα Δημοσίου Κλειδιού (π.χ. RSA, ElGamal). Η $\phi(n)$ είναι η τάξη της πολλαπλασιαστικής ομάδας Z_n^* .

Πεπερασμένα Σώματα GF(p^k)

GF(2^k): Σώματα με 2^k στοιχεία.

Κατασκευή: Χρησιμοποιώντας πολυώνυμα (modn) και κάνοντας πράξεις modulo ένα ανάγωγο πολυώνυμο.

Εφαρμογή: Ο αλγόριθμος AES χρησιμοποιεί το GF(2^8).

ΠΟΛΥΩΝΥΜΑ

Πολυώνυμα πάνω από Σώματα: Πολυώνυμα με συντελεστές από ένα σώμα F (π.χ. Zp , όπου p είναι πρώτος).

Πράξεις: Πρόσθεση, αφαίρεση και πολλαπλασιασμός πολυωνύμων.

Διαίρεση Πολυωνύμων: Αντίστοιχη του αλγορίθμου διαίρεσης ακεραίων, με αποτέλεσμα: $A(x)=Q(x)G(x)+R(x)$, όπου $\deg(R(x))<\deg(G(x))$.

Σώματα Πολυωνύμων: Το σύνολο των πολυωνύμων modulo σε ένα ανάγωγο πολυώνυμο P(x), σχηματίζει ένα σώμα (το σύμβολο F (ή GF για Galois Field) υποδηλώνει ένα πεπερασμένο σώμα).

Κρυπτογραφική Σημασία: Θεμελιώδης για τον αλγόριθμο AES (χρησιμοποιεί $F_{2^8}=256$ στοιχεία ⇒ κάθε στοιχείο ένα byte, π.χ., $(b_7b_6b_5b_4b_3b_2b_1b_0)$ ⇒ αντιστοιχεί στο πολυώνυμο: $(b_7 x^7 + b_6 x^6 + \ldots + b_0 x^0)$.

ΚΙΝΕΖΙΚΟ ΘΕΩΡΗΜΑ ΥΠΟΛΟΙΠΩΝ (CRT)

Πρόβλημα: Επίλυση συστημάτων $x \equiv \alpha_i \pmod{m_i}$ όπου τα m_i είναι ανά δύο πρώτα.

Οφέλη: Επιτρέπει τον διαχωρισμό ενός μεγάλου υπολογισμού σε πολλούς μικρούς.

Σημασία: Χρησιμοποιείται για την αύξηση της ταχύτητας της εκθετικοποίησης (π.χ. στον RSA).

ΤΕΤΡΑΓΩΝΙΚΑ ΥΠΟΛΟΙΠΑ & ΣΥΝΘΕΤΟΙ ΑΡΙΘΜΟΙ

Ορισμός: Το α είναι τετραγωνικό υπόλοιπο (mod n) αν $x^2 \equiv$ α (mod n) έχει λύση.

Σημασία: Όταν το n=pq είναι σύνθετος, η εύρεση της τετραγωνικής ρίζας είναι υπολογιστικά δύσκολη.

Εφαρμογή: Κρυπτοσύστημα Rabin (βασίζεται σε αυτή τη δυσκολία).

ΠΑΡΑΔΕΙΓΜΑ 2: ΕΚΤΕΤΑΜΕΝΟΣ ΑΛΓΟΡΙΘΜΟΣ ΕΥΚΛΕΙΔΗ

Πρόβλημα: 13x+21y=1 δηλαδή gcd (13 , 21) =1

Λύση: Χρησιμοποιώντας 21=1·13+8,…, βρίσκουμε: 1=5·21−8·13.

Αποτέλεσμα: x=−8,y=5.

Ο Εκτεταμένος Αλγόριθμος Ευκλείδη είναι κρίσιμος στην κρυπτογραφία γιατί δεν βρίσκει μόνο τον ΜΚΔ, αλλά εκφράζει τον ΜΚΔ ως γραμμικό συνδυασμό των αρχικών αριθμών.

ΠΑΡΑΔΕΙΓΜΑ 3: ΥΠΟΛΟΓΙΣΜΟΣ ΑΝΤΙΣΤΡΟΦΟΥ

Πρόβλημα: $7^{-1} \pmod{26}$.

Διαδικασία: Εφαρμογή Εκτεταμένου Ευκλείδη για $7x+26y=1$.

Λύση: $-11 \cdot 7 \equiv 1 \pmod{26}$.

Απάντηση: $x=-11 \equiv 15 \pmod{26}$.

ΑΝΑΛΥΣΗ ΤΗΣ ΣΗΜΑΣΙΑΣ ΤΟΥ ΠΑΡΑΔΕΙΓΜΑΤΟΣ 3

Η σημασία του πολλαπλασιαστικού αντιστρόφου, όπως φαίνεται στο παράδειγμα $7^{-1} \equiv 15 \pmod{26}$, είναι κεντρική σε όλα τα συμμετρικά κρυπτοσυστήματα που βασίζονται σε πράξεις modulo, καθώς και στον RSA:

1. **Δυνατότητα Αποκρυπτογράφησης (Invertibility):** Για να είναι ένα κρυπτοσύστημα χρησιμοποιήσιμο, πρέπει να υπάρχει ένας μοναδικός τρόπος αντιστροφής της διαδικασίας κρυπτογράφησης. Ο αντίστροφος (α^{-1}) είναι αυτός που αντιστρέφει την πράξη του κλειδιού α.

ΑΝΑΛΥΣΗ ΤΗΣ ΣΗΜΑΣΙΑΣ ΤΟΥ ΠΑΡΑΔΕΙΓΜΑΤΟΣ 3

2. Κρυπτοσύστημα Affine: Κρυπτογράφηση: $C=(7x+b) \pmod{26}$.

Αποκρυπτογράφηση: Πρέπει να πολλαπλασιάσουμε με τον αντίστροφο του 7, δηλαδή τον 15, για να απομονώσουμε το x.

Άρα: $15 \cdot C \equiv 15(7x+b) \pmod{26} \Rightarrow 15C \equiv (15 \cdot 7)x+15b \pmod{26} \Rightarrow 15C \equiv 1x+15b \pmod{26}$.

Έτσι, ο αντίστροφος (15) εξουδετερώνει το κλειδί κρυπτογράφησης (7), επιτρέποντας την ανάκτηση του αρχικού μηνύματος x.

3. RSA: Στο κρυπτοσύστημα RSA, το ιδιωτικό κλειδί d είναι ο πολλαπλασιαστικός αντίστροφος του δημόσιου κλειδιού e modulo $\phi(n)$, δηλαδή $e \cdot d \equiv 1 \pmod{\phi(n)}$. Ο d είναι απολύτως απαραίτητος για την αποκρυπτογράφηση.

ΠΑΡΑΔΕΙΓΜΑ 4: ΕΦΑΡΜΟΓΗ ΚΙΝΕΖΙΚΟΥ ΘΕΩΡΗΜΑΤΟΣ ΥΠΟΛΟΙΠΩΝ (CRT)

Πρόβλημα: Επίλυση συστημάτων ισοτιμιών $x \equiv a_i \pmod{m_i}$, όπως π.χ. το $x \equiv 1 \pmod 3$, $x \equiv 2 \pmod 4$, $x \equiv 0 \pmod 5$.

Διαδικασία: Υπολογισμός $M = m_1 m_2 m_3 = 60$ και των y_i.

Λύση: $x = (1 \cdot 20 \cdot 2) + (2 \cdot 15 \cdot 3) + 0 \equiv 130 \pmod{60}$.

Αποτέλεσμα: $x \equiv 10 \pmod{60}$.

ΑΝΑΛΥΣΗ ΤΗΣ ΣΗΜΑΣΙΑΣ ΤΟΥ ΠΑΡΑΔΕΙΓΜΑΤΟΣ 4

Κρυπτογραφική Σημασία του CRT: Η κύρια χρήση του CRT είναι η επιτάχυνση της διαδικασίας αποκρυπτογράφησης και της υπογραφής στον αλγόριθμο RSA.

Διαχωρισμός Υπολογισμών: Επιτρέπει έναν μεγάλο υπολογισμό εκθετικοποίησης modulo N (όπου $N=p \cdot q$) να αντικατασταθεί από δύο παράλληλους, ταχύτερους υπολογισμούς modulo με τους μικρότερους πρώτους παράγοντες p και q.

Λόγος Ταχύτητας: Ο υπολογισμός $M^d \pmod N$ μπορεί να γίνει *έως και τέσσερις φορές πιο γρήγορα* χρησιμοποιώντας το CRT.

Αντίστροφη Λειτουργία: Αφού πραγματοποιηθούν οι υπολογισμοί modulo p και modulo q, το CRT χρησιμοποιείται για την ανασύνθεση του τελικού αποτελέσματος modulo N.

ΠΙΘΑΝΟΤΗΤΕΣ & ΑΝΤΙΠΑΛΟΣ PPT

Υπολογιστική Ασφάλεια: Η ασφάλεια είναι πιθανοτική (όχι απόλυτη).

Αντίπαλος PPT: Ο αντίπαλος μοντελοποιείται ως αλγόριθμος Probabilistic Polynomial Time (PPT).

Αμελητέα Πιθανότητα: Η πιθανότητα επιτυχίας του αντιπάλου ***πρέπει να είναι αμελητέα.***

ΤΟ ΠΑΡΑΔΟΞΟ ΤΩΝ ΓΕΝΕΘΛΙΩΝ

Φαινόμενο: Η πιθανότητα σύγκρουσης σε σύνολο N είναι υψηλή με k ≈ $\sqrt{N}$ επιλογές.

Birthday Attack: Επίθεση σε Hash Functions με έξοδο *m* bits.

Συνέπεια: Μείωση της ασφάλειας από $O(2^m)$ σε $O(2^{m/2})$.

ΣΤΑΤΙΣΤΙΚΗ ΑΠΟΣΤΑΣΗ & ΑΔΙΑΚΡΙΣΙΑ

Στατιστική Απόσταση: Μέτρο της διαφοράς μεταξύ δύο κατανομών.

Αδιακρισία (Indistinguishability): Ένας κρυπτογραφικός ορισμός ασφάλειας. Δύο κατανομές είναι αδιάκριτες αν η στατιστική τους απόσταση είναι αμελητέα από έναν αντίπαλο PPT.

ΣΥΜΠΕΡΑΣΜΑΤΙΚΗ ΣΥΝΟΨΗ

Βάση: Η Θεωρία Αριθμών και η Θεωρία Ομάδων (π.χ., Z_n^*, φ(n)) παρέχουν τα δομικά υλικά για την κρυπτογραφία.

Πλαίσιο: Η ασφάλεια ορίζεται με όρους πιθανότητας (PPT αντίπαλοι) και βασίζεται στην διαμόρφωση της δυσκολίας προβλημάτων και του χρόνου επίλυσής τους.

ΜΑΘΗΜΑΤΙΚΟ ΚΑΙ ΥΠΟΛΟΓΙΣΜΙΚΟ ΥΠΟΒΑΘΡΟ

ΜΕΡΟΣ ΙΙ: ΣΤΟΙΧΕΙΑ ΘΕΩΡΙΑΣ ΥΠΟΛΟΓΙΣΜΟΥ

ΣΚΟΠΟΣ ΤΗΣ ΘΕΩΡΙΑΣ ΥΠΟΛΟΓΙΣΜΟΥ ΣΤΗΝ ΚΡΥΠΤΟΓΡΑΦΙΑ

Σκοπός: Παρέχει το τυπικό πλαίσιο για την υπολογιστική ασφάλεια.

Μοντέλο Turing: Το θεωρητικό μοντέλο του υπολογιστή (χρόνος/χώρος). Οι σύγχρονοι αλγόριθμοι είναι πλήρεις κατά Turing.

Υπολογιστικός Περιορισμός: Ο αντίπαλος είναι πάντα πολυωνυμικός .

ΚΛΑΣΕΙΣ ΠΟΛΥΠΛΟΚΟΤΗΤΑΣ P ΚΑΙ NP

Κλάση P: Προβλήματα που λύνονται σε πολυωνυμικό χρόνο (αποδοτικά).

Κλάση NP: Προβλήματα που επαληθεύονται αποδοτικά. •

Υπόθεση: Η ασφάλεια βασίζεται στο ότι P ≠ NP, δηλαδή ότι υπάρχουν δύσκολα προβλήματα.

ΤΑ «ΔΥΣΚΟΛΑ» ΚΡΥΠΤΟΓΡΑΦΙΚΑ ΠΡΟΒΛΗΜΑΤΑ

Τα "δύσκολα" κρυπτογραφικά προβλήματα είναι αυτά που μπορούν να επιλυθούν μόνο σε εκθετικό (πολύ αργό) χρόνο, ενώ η κρυπτογράφηση/αποκρυπτογράφηση (με το κλειδί) γίνεται σε πολυωνυμικό (γρήγορο) χρόνο. Αυτή η ασυμμετρία είναι ο πυρήνας της ασφάλειας.

Ασφάλεια: Η δυσκολία τους μεγαλώνει εκθετικά με το μέγεθος του κλειδιού.

ΤΑ «ΔΥΣΚΟΛΑ» ΚΡΥΠΤΟΓΡΑΦΙΚΑ ΠΡΟΒΛΗΜΑΤΑ

1. Παραγονοποίηση (Factoring): Είναι η βάση του RSA.

Πρόβλημα Παραγοντοποίησης: Δίνονται δύο πολύ μεγάλοι πρώτοι αριθμοί, p και q, και υπολογίζεται το γινόμενό τους $N=p \cdot q$. Το πρόβλημα είναι: Αν δίνεται το N, να βρεθούν οι αρχικοί παράγοντες p και q.

Δυσκολία: Η εύρεση του N από τα p , q είναι γρήγορη (πολυωνυμικός χρόνος). Η εύρεση των p , q από το N είναι αργή (εκθετικός χρόνος, ή υπο-εκθετικός). Στον RSA, το N είναι το δημόσιο κλειδί. Αν ένας εισβολέας βρει τους p και q από το N, μπορεί να υπολογίσει το φ(N) και άρα το ιδιωτικό κλειδί.

Σημασία: Η ασφάλεια του RSA βασίζεται στην υπόθεση ότι δεν υπάρχει αποδοτικός αλγόριθμος για την παραγοντοποίηση μεγάλων αριθμών (π.χ. των 2048-bit).

Παράδειγμα: Έστω $N=3127$. Είναι εύκολο να βρεθεί ότι $N=47 \times 67$. Αλλά όταν το N έχει 600 ψηφία, είναι πρακτικά αδύνατο να παραγοντοποιηθεί σε γινόμενο πρώτων αριθμών!

ΤΑ «ΔΥΣΚΟΛΑ» ΚΡΥΠΤΟΓΡΑΦΙΚΑ ΠΡΟΒΛΗΜΑΤΑ

2. Διακριτός Λογάριθμος (Discrete Logarithm Problem – DLOG ή DLP): Βάση των Diffie-Hellman & ElGamal.

Πρόβλημα DLOG: Δίνεται μία ομάδα G (συνήθως η Z_p^*) και ένας γεννήτορας g. Δίνονται επίσης το g και το h, όπου $h = g^x \pmod p$. Το πρόβλημα είναι να βρεθεί ο εκθέτης x.

Δυσκολία: Ο υπολογισμός του h από τα g και x είναι γρήγορος (γρήγορη εκθετικοποίηση). Ο υπολογισμός του x από τα g και h είναι αργός (δεν υπάρχει αποδοτικός αλγόριθμος). Το x είναι το ιδιωτικό κλειδί του χρήστη. Ο αλγόριθμος DH επιτρέπει σε δύο χρήστες να συμφωνήσουν σε ένα κοινό μυστικό κλειδί, χωρίς να αποκαλύψουν τα ιδιωτικά τους κλειδιά x.

Σημασία: Η ασφάλεια των αλγορίθμων Diffie-Hellman και ElGamal βασίζεται στη δυσκολία επίλυσης του DLOG.

Παράδειγμα: Στην ομάδα Z_{17}^*, g=3. Αν h=10, ποιο είναι το x; ($3^x \equiv 10 \pmod{17}$). Η απάντηση είναι x=13, γιατί $3^{13} \equiv 10 \pmod{17}$. Όταν οι αριθμοί είναι μεγάλοι, η επίλυση είναι εξαιρετικά δύσκολη.

ΤΑ «ΔΥΣΚΟΛΑ» ΚΡΥΠΤΟΓΡΑΦΙΚΑ ΠΡΟΒΛΗΜΑΤΑ

3. CDH (Computational Diffie-Hellman): Υπολογιστικό πρόβλημα συχνά δυσκολότερο από το DLOG. .

Πρόβλημα CDH : Το πρόβλημα CDH ορίζεται ως εξής:

Δεδομένα: Δίνεται μια κυκλική ομάδα G (συνήθως η πολλαπλασιαστική ομάδα Z_p^* ή μια ομάδα σημείων ελλειπτικής καμπύλης) με γεννήτορα g. Σας δίνονται τα στοιχεία g^a και g^b .

Ζητούμενο: Να υπολογίσετε το στοιχείο g^{ab}.

1. Σύνδεση με το Key Exchange

Ο εισβολέας (Εύα) παρακολουθεί τις δημόσιες τιμές g^a και g^b και προσπαθεί να υπολογίσει το κοινό μυστικό κλειδί g^{ab}. Η ικανότητα της Εύας να το επιτύχει αυτό εξαρτάται ακριβώς από την ικανότητά της να λύσει το πρόβλημα CDH. Επομένως, το πρωτόκολλο DH είναι ασφαλές εάν και μόνο εάν το πρόβλημα CDH είναι υπολογιστικά δύσκολο.

ΤΑ «ΔΥΣΚΟΛΑ» ΚΡΥΠΤΟΓΡΑΦΙΚΑ ΠΡΟΒΛΗΜΑΤΑ

2. Σχέση με το Διακριτό Λογάριθμο (DLP)

Το πρόβλημα CDH συνδέεται στενά με το βασικότερο πρόβλημα της ασύμμετρης κρυπτογραφίας: το Discrete Logarithm Problem (DLP).

Πρόβλημα Διακριτού Λογαρίθμου (DLP)

Δεδομένα: Δίνεται η βάση g και το στοιχείο g^x.

Ζητούμενο: Να υπολογιστεί ο εκθέτης x.

Ισχύς των Προβλημάτων

Ισχύει η ακόλουθη σχέση δυσκολίας: $DLP \Longrightarrow CDH$

Αυτό σημαίνει: Αν μπορείτε να λύσετε το DLP, μπορείτε να λύσετε και το CDH.

Ωστόσο, το αντίστροφο δεν έχει αποδειχθεί: $CDH \not\Rightarrow DLP$

Συμπέρασμα: Το πρόβλημα CDH είναι λογικά ασθενέστερο (ή τουλάχιστον όχι ισοδύναμο) από το DLP, αλλά είναι η ακριβής απαίτηση ασφάλειας για το πρωτόκολλο DH-Key Exchange.

PPT ΚΑΙ ΨΕΥΔΟΤΥΧΑΙΟΤΗΤΑ

Κρυπτογραφία & ασφάλεια: λέμε ότι ένα σύστημα είναι ασφαλές αν κανένας PPT αντίπαλος (δηλαδή, κανένας αλγόριθμος πολυωνυμικού χρόνου, ακόμα και πιθανοτικός) δεν μπορεί να το «σπάσει» με μη-αμελητέα πιθανότητα (non-negligible probability).

Η ψευδοτυχαιότητα απαντά στην ερώτηση: Μπορούμε να δημιουργήσουμε μεγάλες τυχαίες ακολουθίες από μια μικρή τυχαία είσοδο, έτσι ώστε κανένας αποδοτικός υπολογιστής να μην μπορεί να τις διακρίνει από μια αληθινά τυχαία ακολουθία;

Ο κεντρικός ορισμός είναι: Ψευδοτυχαία Γεννήτρια (Pseudorandom Generator - PRG)

PPT ΚΑΙ ΨΕΥΔΟΤΥΧΑΙΟΤΗΤΑ

Η σχέση μεταξύ PPT και Ψευδοτυχαιότητας είναι θεμελιώδης για τη μοντέρνα κρυπτογραφία:

α) Η Υπόθεση Δυσκολίας: Η ύπαρξη Κρυπτογραφικά Ασφαλών PRGs (CSPRNGs) βασίζεται στην υπόθεση ότι υπάρχουν προβλήματα που είναι υπολογιστικά δύσκολα (π.χ., το πρόβλημα της παραγοντοποίησης ή του διακριτού λογαρίθμου).

Θεώρημα: Η ύπαρξη μιας PRG είναι ισοδύναμη με την ύπαρξη μιας συνάρτησης μονής κατεύθυνσης (One-Way Function - OVF).

OVF: Μια συνάρτηση f που είναι εύκολο να υπολογιστεί, αλλά δύσκολο να αντιστραφεί από έναν PPT αλγόριθμο.

PPT ΚΑΙ ΨΕΥΔΟΤΥΧΑΙΟΤΗΤΑ

β) Ο Ρόλος του P και BPP (Derandomization): Η θεωρία της ψευδοτυχαιότητας συνδέεται άμεσα με την ερώτηση «Μπορεί η τυχαιότητα να εξαλειφθεί από τους αποδοτικούς αλγορίθμους;» (Derandomization)

Συλλογισμός: Αν μια PRG μπορούσε να κατασκευαστεί με βάση μια ντετερμινιστική υπόθεση δυσκολίας (π.χ. EXP ≠ BPP), τότε αυτή η PRG θα μπορούσε να αντικαταστήσει τα αληθινά τυχαία bits σε κάθε BPP αλγόριθμο.

.

PPT ΚΑΙ ΨΕΥΔΟΤΥΧΑΙΟΤΗΤΑ

Θεώρημα Impagliazzo–Wigderson (IW98): Αν υπάρχουν προβλήματα στην EXP που είναι υπολογιστικά δύσκολα (από την BPP), τότε BPP=P.

Ερμηνεία: Αν έχουμε κρυπτογραφική σκληρότητα (δηλαδή, υπάρχει μια δύσκολη συνάρτηση, την οποία δεν μπορεί να σπάσει ένας PPT), τότε η τυχαιότητα δεν είναι απαραίτητη για τους αποδοτικούς αλγορίθμους.

Η θεωρία της ψευδοτυχαιότητας, λοιπόν, αποτελεί τη γέφυρα μεταξύ της υπολογιστικής πολυπλοκότητας (PPT) και των απαιτήσεων ασφάλειας της κρυπτογραφίας, ορίζοντας την ασφάλεια ως μη-διακριτότητα από έναν PPT αντίπαλο.

ΑΝΑΛΥΣΗ ΤΗΣ ΚΛΑΣΗΣ ΠΟΛΥΠΛΟΚΟΤΗΤΑΣ: ΔΙΑΛΟΓΙΚΗ ΑΠΟΔΕΙΞΗ (IP)

Η Διαλογική Απόδειξη (Interactive Proof - IP) σηματοδοτεί μια σημαντική στροφή στη Θεωρία Πολυπλοκότητας. Αντί να ορίζει προβλήματα με βάση το χρόνο ή τον χώρο που απαιτεί μια ενιαία μηχανή (όπως τα P, BPP, EXP), η κλάση IP ορίζεται με βάση την αλληλεπίδραση μεταξύ δύο μερών (διάλογος).

1. Ο Ορισμός της Κλάσης IP

Η κλάση IP περιλαμβάνει όλα τα προβλήματα απόφασης για τα οποία υπάρχει ένα Διαλογικό Πρωτόκολλο μεταξύ δύο οντοτήτων.

Του Αποδεικνύοντα (Prover - P): Ένας αλγόριθμος που είναι απεριόριστος σε υπολογιστική ισχύ (μπορεί να είναι η EXP ή και παραπάνω). Ο ρόλος του είναι να πείσει το V για την απάντηση.

ΑΝΑΛΥΣΗ ΤΗΣ ΚΛΑΣΗΣ ΠΟΛΥΠΛΟΚΟΤΗΤΑΣ: ΔΙΑΛΟΓΙΚΗ ΑΠΟΔΕΙΞΗ (IP)

Του Επαληθευτή (Verifier - V): Ένας αλγόριθμος Πιθανοτικού Πολυωνυμικού Χρόνου (PPT) (δηλαδή, $V \in BPP$). Ο ρόλος του είναι να επαληθεύσει την απάντηση, αλλά περιορίζεται σε γρήγορους υπολογισμούς. Ο Verifier V επιλύει το πρόβλημα (δίνει την απάντηση ΝΑΙ/ΟΧΙ) μετά από πολυωνυμικού μήκους ανταλλαγή μηνυμάτων με τον Prover P.

2. Η Θέση της IP στην Ιεραρχία: Το πιο εκπληκτικό και σημαντικό αποτέλεσμα σχετικά με αυτή την κλάση είναι το Θεώρημα Shamir (1990):

$$IP = PSPACE$$

ΑΝΑΛΥΣΗ ΤΗΣ ΚΛΑΣΗΣ ΠΟΛΥΠΛΟΚΟΤΗΤΑΣ: ΔΙΑΛΟΓΙΚΗ ΑΠΟΔΕΙΞΗ (IP)

Η αλληλεπίδραση προσφέρει τεράστια ισχύ: Το παραπάνω αποτέλεσμα δείχνει ότι η διαλογική αλληλεπίδραση (με χρήση τυχαιότητας από τον Verifier) δίνει στον Verifier την ικανότητα να λύσει όλα τα προβλήματα που μπορούν να λυθούν με πολυωνυμικό χώρο μνήμης (PSPACE).

Πολυπλοκότητα Χρόνου έναντι Χώρου: Τα προβλήματα PSPACE (που απαιτούν πολυωνυμική μνήμη) είναι πολύ πιο δύσκολα από τα προβλήματα NP (που απαιτούν πολυωνυμικό χρόνο για επαλήθευση). Το γεγονός ότι η κλάση IP καλύπτει όλα τα προβλήματα PSPACE σημαίνει ότι η αλληλεπίδραση, η τυχαιότητα και ο χρόνος του V μπορούν να αντικαταστήσουν την τεράστια μνήμη που απαιτείται για μια απλή ντετερμινιστική επίλυση.

ΣΥΜΠΕΡΑΣΜΑΤΙΚΗ ΣΥΝΟΨΗ

Η θεωρία υπολογισμού εισάγει τις κλάσεις πολυπλοκότητας (P,NP) στην κρυπτογραφική μεθοδολογία και ορίζει την υπολογιστική δυσκολία (Factoring, DLOG) ως βάση της ασφάλειας σε αυτήν.

ΕΡΩΤΗΣΕΙΣ ΓΙΑ ΣΥΖΗΤΗΣΗ

ΕΡΩΤΗΣΕΙΣ ΣΥΝΤΟΜΗΣ ΑΝΑΠΤΥΞΗΣ – ΑΣΚΗΣΕΙΣ ΜΑΘΗΜΑΤΙΚΗΣ ΠΡΟΠΟΝΗΣΗΣ

ΕΡΩΤΗΣΕΙΣ ΜΕ ΣΥΝΤΟΜΕΣ ΑΠΑΝΤΗΣΕΙΣ

1. Ποια είναι η σχέση P και NP;
2. Πώς επηρεάζει το Birthday Paradox την ασφάλεια των Hash Functions;
3. Τι ρόλο παίζει η φ(n) στον RSA;
4. Τι είναι το CDH και πού εφαρμόζεται;

ΕΡΩΤΗΣΕΙΣ ΓΙΑ ΣΥΖΗΤΗΣΗ

1. P vs. BPP: Το Αίνιγμα της Τυχαιότητας

Ποια είναι η κεντρική διαφορά στην πρακτική εφαρμογή ενός αλγορίθμου P (ντετερμινιστικού) και ενός BPP (πιθανοτικού); Εάν αποδεικνυόταν ότι P=BPP, τι θα σήμαινε αυτό για την αποδοτικότητα των πιθανοτικών αλγορίθμων (όπως το Miller-Rabin) και γιατί η απόδειξη αυτή δεν θα τους καθιστούσε άχρηστους στην πράξη;

ΕΡΩΤΗΣΕΙΣ ΓΙΑ ΣΥΖΗΤΗΣΗ

2. PRG και η Ουσία της Ασφάλειας

Ο κρυπτογραφικός ορισμός της ασφάλειας για μια Ψευδοτυχαία Γεννήτρια (PRG) βασίζεται στην υπολογιστική μη-διακριτότητα από έναν PPT αντίπαλο. Εξηγήστε πώς αυτό διαφέρει από την στατιστική τυχαιότητα και γιατί η ασφάλεια της PRG είναι ισοδύναμη με την ύπαρξη συναρτήσεων μονής κατεύθυνσης (One-Way Functions).

ΕΡΩΤΗΣΕΙΣ ΓΙΑ ΣΥΖΗΤΗΣΗ

3. Η Απίστευτη Δύναμη του IP

Το Θεώρημα Shamir αποδεικνύει ότι IP=PSPACE. Γιατί αυτό το αποτέλεσμα θεωρείται τόσο εκπληκτικό; Πώς καταφέρνει ο PPT Επαληθευτής (V) να επαληθεύσει, με τη χρήση τυχαιότητας και αλληλεπίδρασης, μια δήλωση που απαιτεί υπολογιστική ισχύ ίση με πολυωνυμικό χώρο (PSPACE);

ΕΡΩΤΗΣΕΙΣ ΓΙΑ ΣΥΖΗΤΗΣΗ

4. Η Σημασία του EXP στην Κρυπτογραφία

Η ιεραρχία PSPACE⊆EXP δείχνει ότι ο εκθετικός χρόνος είναι οριοθέτης. Γιατί είναι κρίσιμο για την ασφάλεια των σύγχρονων κρυπτοσυστημάτων (όπως το RSA) το αντίστοιχο πρόβλημα παραβίασης (π.χ., η παραγοντοποίηση) να παραμένει εκτός της κλάσης P (ή BPP), αλλά εντός της EXP (ή NP);

ΕΡΩΤΗΣΕΙΣ ΓΙΑ ΣΥΖΗΤΗΣΗ

5. Ο Κρυπτογραφικός Αντίπαλος

Στην κρυπτογραφική ασφάλεια, ο αντίπαλος ορίζεται πάντα ως PPT (Probabilistic Polynomial Time). Γιατί δεν ορίζουμε την ασφάλεια έναντι ενός αντιπάλου με ισχύ EXP ή απεριόριστη ισχύ (όπως ο Prover στην IP); Τι θα σήμαινε αυτό για την πρακτική αξία και τη δυνατότητα κατασκευής κρυπτοσυστημάτων;

ΕΡΩΤΗΣΕΙΣ ΓΙΑ ΣΥΖΗΤΗΣΗ

6. Σώματα και Ισοδυναμία (Modular Arithmetic)

Στην Υπολογιστική Θεωρία Αριθμών, σχεδόν όλοι οι υπολογισμοί γίνονται σε πεπερασμένα σώματα (F_q). Γιατί είναι κρίσιμη η ιδιότητα του πολλαπλασιαστικού αντιστρόφου (ένα αξίωμα του σώματος) για την αποτελεσματική λειτουργία κρυπτογραφικών αλγορίθμων που βασίζονται στην αριθμητική modulo;

ΕΞΑΣΚΗΣΗ ΣΤΑ ΜΑΘΗΜΑΤΙΚΑ

1. Βρείτε τον $28^{-1} (\mathrm{mod} 51)$.
2. Λύστε το σύστημα $x \equiv 5 \pmod 7$ και $x \equiv 1 \pmod{11}$.
3. Υπολογίστε $28^{27.200.000.023} \pmod{35}$.
4. Σε ποια κλάση ανήκει ένας αλγόριθμος $O(n^2 \log n)$;