Υπογραφές, Συναρτήσεις Κατακερματισμού

1. Η Καρολίνα λαμβάνει το παρακάτω μήνυμα, μαζί με μία σωστή ηλεκτρονικη υπογραφή ως προς το κλειδί του Λυκούργου PK_Λ «Παραβίασαν τον υπολογιστή μου, παρακαλώ μην εμπιστεύεσαι πλέον αυτό το κλειδί, και ειδοποίησε όσους μπορεις». Θα πρέπει να πιστέψει το μήνυμα η Καρολίνα;

   Λύση Ναι. Αν το μήνυμα πράγματι προέρχεται από τον Λυκούργο, θα πρέπει να σταματήσει να εμπιστεύεται 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.

2. Εάν μια συνάρτηση κατακερματισμού είναι ανθεκτική σε συγκρούσεις, είναι απαραίτητα και μονόδρομη;

   Λύση Ναι, υπό συνθήκες. Συγκεκριμένα, πρέπει να ενισχύσουμε την ιδιότητα της συμπίεσης. Αρχικά θα υποθέσουμε ότι η συνάρτηση συμπιέζει κατά τουλάχιστον ένα bit, δηλαδή αντιστοιχίζει $2n$ ορίσματα σε (το πολύ) n διαφορετικές εικόνες. Με αυτή την (ισχυρότερη) υπόθεση, μπορούμε να κάνουμε την εξής παρατήρηση: τουλάχιστον n από τα πιθανά ορίσματα της συνάρτησης δεν έχουν μοναδική εικόνα (δηλαδή «μοιράζονται» την εικόνα τους με τουλάχιστον ένα άλλο στοιχείο). Πράγματι, έστω ότι το παραπάνω δεν ισχύει. Αυτό σημαίνει ότι υπάρχουν τουλάχιστον $2n - n = n$ ορίσματα τα οποία έχουν μοναδική εικόνα. Όμως, το σύνολο των διαφορετικών εικόνων έχει μέγεθος το πολύ n στοιχεία, άρα τα υπόλοιπα στοιχεία του πεδίου ορισμού δεν μπορούν να πάρουν εικόνα, άτοπο.

   Μετά την παραπάνω παρατήρηση, μπορούμε πλέον να δείξουμε ότι αν υπάρχει αντίπαλος $\mathcal{A}$ που αντιστρέφει την συνάρτηση με καλή πιθανότητα έστω a, τότε μπορούμε με αντίστοιχα καλή πιθανότητα να παράξουμε σύγκρουση. Για να παράξουμε σύγκρουση εργαζόμαστε ως εξής: επιλέγουμε ένα τυχαίο στοιχείο x από το D και υπολογίζουμε την εικόνα του y. Δίνουμε το y στον αλγόριθμο $\mathcal{A}$ που μας επιστρέφει x'. Η απαντησή μας είναι x, x'.

   Για να ολοκληρώσουμε την απόδειξη πρέπει να υπολογίσουμε την πιθανότητα επιτυχίας της παραπάνω διαδικασίας. Από την παραπάνω παρατήρηση, με πιθανότητα τουλάχιστον $1/2$ το x είναι στοιχείο τέτοιο όπου το y έχει $n_y \geq 1$ αντίστροφες εικόνες. Οπότε εάν ο $\mathcal{A}$ επιτύχει (με πιθανότητα a), τότε με πιθανότητα $\frac{n_y - 1}{n_y} \geq \frac{1}{2}$ το x' θα είναι πράγματι μια αντίστροφη εικόνα του y διαφορετική από το x. Συνολικά η πιθανότητα επιτυχίας είναι τουλάχιστον $\frac{a}{4}$.

   Η ίδια απόδειξη δουλεύει όσο η διαφορά μεγέθους R_i και D_i είναι σημαντική. Σε ακραίες περιπτώσεις, που δεν εμφανίζονται στην πράξη, (πχ από 2^λ στοιχεία σε $2^\lambda - 1$) είναι δυνατό τα στοιχεία που δεν έχουν μοναδική εικόνα να είναι αμελητέο κλάσμα του R_i και άρα η τελική πιθανότητα επιτυχίας να είναι και αυτή αμελητέα.

3. Εάν γενικεύσουμε το παραπάνω από συναρτήσεις κατακερματισμού σε συναρτήσεις που είναι εύκολες στον υπολογισμό και τη δειγματοληψία, ισχύει ότι η αντοχή σε συγκρούσεις συνεπάγεται οτι η συνάρτηση είναι μονόδρομη;

   Λύση Όχι. Παράδειγμα η ταυτοτική συνάρτηση. Είναι εξ'ορισμού ανθεκτική σε συγκρούσεις αλλά προφανώς όχι μονόδρομη.

4. Έστω ότι οι οικογένεια συναρτήσεων κατακερματισμού $\mathcal{F} = \{\mathcal{H}_i\}_{i \in \mathcal{I}}$ με είσοδο συμβολοσειρές $2k$ bits και έξοδο συμβολοσειρές k bits είναι ανθεκτική σε συγκρούσεις. Εξετάστε τις παρακάτω παραλλαγές ως προς την ανθεκτικότητα σε συγκρούσεις:

   (α΄) Η οικογένεια $\mathcal{F}'$ με εισόδους $3k/2$ bits και εξόδους k bits όπου $\mathcal{H'}_i(x) = \mathcal{H}_i(x||0^{k/2})$

   (β΄) Η οικογένεια $\mathcal{F}''$ με εισόδους $2k$ bits και εξόδους $3k/2$ bits όπου $\mathcal{H''}_i(x) = \mathcal{H}_i(x)||0^{k/2}$

   (γ΄) Η οικογένεια $\mathcal{F}^\dagger$ με εισόδους $2k$ bits και εξόδους $k/2$ bits όπου $\mathcal{H}^\dagger{}_i(x) = \mathsf{MSB}(\mathcal{H}_i(x), k/2)$

   (δ΄) Η οικογένεια $\mathcal{F}^\ddagger$ με εισόδους $5k/2$ bits και εξόδους k bits όπου $\mathcal{H}^\ddagger{}_i(x) = \mathcal{H}_i(\mathsf{MSB}(x, 2k))$

Για μια συμβολοσειρά από bits s και ένα φυσικό n, συμβολίζουμε με $\mathsf{MSB}(s, n)$ τα n πρώτα bit της συμβολοσειράς s.

Λύση

(α΄) Είναι ανθεκτική, με αναγωγή στην ανθεκτικότητα της $\mathcal{F}$: έστω ένας αντίπαλος $\mathcal{A}'$ που σε πολυωνυμικό χρόνο βρίσκει συγκρούσεις απέναντι στην $\mathcal{F}'$ με μη αμελητέα πιθανότητα. Κατασκευάζουμε έναν αντίπαλο $\mathcal{B}$ απέναντι στην $\mathcal{F}$: ο $\mathcal{B}$ παίρνει από το πείραμα την παράμετρο i την οποία περνάει στον $\mathcal{A}$. Εάν ο $\mathcal{A}$ επιστρέψει μια σύγκρουση για την $\mathcal{H}'_i$ έστω x, x' είναι ευκολο να δούμε ότι οι συμβολοσειρές $x||0^{k/2}$, $x'||0^{k/2}$ αποτελούν σύγκρουση για την $\mathcal{H}_i$. Συνεπώς, ο $\mathcal{B}$ επιστρέφοντας $x||0^{k/2}$, $x'||0^{k/2}$ έχει πιθανότητα επιτυχίας ίση με αυτήν του $\mathcal{A}$. Επίσης εύκολα ελέγχουμε ότι ο $\mathcal{B}$ τρέχει σε πολυωνυμικό χρόνο.

Αυτό όμως αντικρούει στην υπόθεση ότι η $\mathcal{F}$ είναι ανθεκτική σε συγκρούσεις. Επομένος, δεν είναι δυνατό να υπάρχει αντίπαλος $\mathcal{A}'$ που σε πολυωνυμικό χρόνο βρίσκει συγκρούσεις απέναντι στην $\mathcal{F}'$ με μη αμελητέα πιθανότητα, και άρα η $\mathcal{F}'$ είναι ανθεκτική σε συγκρούσεις.

(β΄) Είναι ανθεκτική: μια σύγκρουση στην $\mathcal{H}''$ δίνει σύγκρουση και στην $\mathcal{H}$, ομοίως με παραπάνω.

(γ΄) Δεν ισχύει, αλληλεπιδρά καταστροφικά με συναρτήσεις όπως η περίπτωση β (με αλλαγή της φοράς).

(δ΄) Δεν ισχύει, οι συμβολοσειρές $0^{5k/2}$ και $0^{5k/2-1}||1$ είναι διαφορετικές και αποτελούν σύγκρουση για κάθε i.

5. Εξετάζουμε μια παραλλαγή του ορισμού EUF-CMA από τις σημειώσεις. Στην παραλλαγή αυτή, αντικαθιστούμε τον έλεγχο $m \notin Q$ με $(m, \sigma) \notin Q$, και θεωρούμε ως Q αντί το σύνολο των μηνυμάτων m στα οποία ζήτησε υπογραφές ο $\mathcal{A}$, το σύνολο των ζευγών (m, σ) από μηνύματα m στα οποία ο $\mathcal{A}$ ζήτησε υπογραφές και σ οι απαντήσεις που πήρε.

   - Εξηγήστε σε φυσική γλώσσα την διαφορά της παραπάνω παραλλαγής από τον αρχικό ορισμό.
   - Περιγράψτε συνοπτικά γιατί ο αλγόριθμος RSA-FDH που εξετάσαμε στις διαλέξεις μας ασφαλής με τον παραπάνω ορισμό.
   - Δώστε μια σύντομη παραλλαγή του παραπάνω αλγορίθμου ώστε να είναι ασφαλής κατά τον αρχικό ορισμό, αλλά όχι από την παραλλαγή. Η παραλλαγή σας δε χρειάζεται να είναι χρήσιμη στην πράξη.

6. Στον αλγόριθμο υπογραφών RSA-FDH, θεωρούμε ότι η συνάρτηση κατακερματισμού H έχει σύνολο τιμών το $\mathbb{Z}_N^*$. Η Αλίκη, προτείνει για ευκολία να χρησιμοποιήσουμε συνάρτηση κατακερματισμού H' με σύνολο τιμών το $\mathbb{Z}_{2^\lambda}$ (συμβολοσειρές λ bits, θεωρούμενες ως ακέραιους). Υποθέτωντας ότι $|\mathbb{Z}_N^*| = \Omega(2^{2\lambda})$, εξετάστε εάν η απόδειξη ασφάλειας που έχουμε δώσει ισχύει ως έχει.

   Λύση

   - Στον αρχικό ορισμό δεν θεωρείται πρόβλημα ασφαλείας εάν ο αντίπαλος μπορεί να παράξει μια νέα, έγκυρη υπογραφή, σε κάποιο μήνυμα που έχει «δει» (ζητήσει) στο παρελθόν. Στην παραλλαγή, θεωρείται παραβίαση της ασφάλειας, άρα ο ορισμός είναι αυστηρότερος.

     Σε καμία από τις δύο περιπτώσεις δεν θεωρείται πρόβλημα το να παρουσιάσει ο αντίπαλος απαράλακτο ένα ζεύγος μηνύματος-υπογραφής που έχει δει.

   - Όχι. Η απόδειξη παρουσιάζει μια τεχνική δυσκολία: όταν ο αντίπαλος ζητά από την αναγωγή μας να «υπογράψει» ένα μήνυμα, εμείς επιλέγουμε ένα τυχαίο σ θέτουμε $y = f_e(\sigma)$ και προγραμματίζουμε το μαντείο ώστε $H(m) = y$. Επειδή όμως το σύνολο τιμών της H είναι περιορισμένο, είναι πολύ πιθανό το y να μην ανήκει σε αυτό.

     Σε πρώτη ανάλυση οι επιλογές μας είναι είτε να επιστρέψουμε ένα y εκτός του πεδίου τιμών, το οποίο όμως μπορεί να «χαλάσει» την συμπεριφορά του αντιπάλου, αφού πλέον τρέχει «εκτός

προδιαγραφών» είτε να δοκιμάσουμε διαφορετικά σ μέχρι να βρούμε ένα y στο πεδίο τιμών την H. Χωρίς όμως κάποια άλλη υπόθεση, η πιθανότητα να γίνει αυτό είναι σε κάθε προσπάθεια είναι $\frac{2^\lambda}{2^{2\lambda}} = 2^{-\lambda}$, και το πλήθος των προσπαθειών που θα χρειαστεί να κάνουμε είναι κατά μέσο όρο εκθετικό. Δυστυχώς, μια αναγωγή που τρέχει σε εκθετικό χρόνο δεν μας είναι χρήσιμη εδώ. Θα αποδεικνύαμε ότι "εάν υπάρχει πολυωνυμικός αντίπαλος για το σχήμα υπογραφών RSA-FDH, υπάρχει εκθετικός αντίπαλος που λύνει το RSA problem". Αυτό όμως είναι τετριμμένο: σε εκθετικό χρόνο μπορούμε πράγματι να παραγωγίσουμε το N και να λύσουμε το RSA problem υπολογίζοντας το d που αντιστοιχεί στο e. Πιο συγκεκριμμένα, η υποθεσή μας είναι ότι δεν υπάρχει πολυωνυμικός αντίπαλος για το RSA problem και άρα ο εκθετικός αντίπαλος που κατασκευάσαμε (ή ο εκθετικός αντίπαλος που παραγωγίζει) δεν προκαλούν αντίφαση.