

Υπογραφές, Συναρτήσεις Κατακερματισμού

1. Η Καρολίνα λαμβάνει το παρακάτω μήνυμα, μαζί με μία σωστή ηλεκτρονική υπογραφή ως προς το κλειδί του Λυκούργου PK_Λ «Παραβίασαν τον υπολογιστή μου, παρακαλώ μην εμπιστευέσαι πλέον αυτό το κλειδί, και ειδοποίησε όσους μπορείς». Θα πρέπει να πιστέψει το μήνυμα η Καρολίνα;
2. Εάν μια συνάρτηση κατακερματισμού είναι ανθεκτική σε συγκρούσεις, είναι απαραίτητα και μονόδρομη;
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 ότι η συνάρτηση είναι 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 k 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 $\mathcal{H}^\dagger_i(x) = \text{MSB}(\mathcal{H}_i(x), k/2)$

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

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

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^λ} (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.