ΕΙΣΑΓΩΓΗ ΣΤΗΝ ΚΡΥΠΤΟΛΟΓΙΑ
ΣΗΜΕΙΩΣΕΙΣ #10

ΘΕΟΔΟΥΛΟΣ ΓΑΡΕΦΑΛΑΚΗΣ

1. Υπογραφες ElGamal

Στη δημοσίευση του 1985, ο ElGamal μαζί με το σύστημα κρυπτογράφησης πρότεινε και ένα σύστημα ψηφιακών υπογραφών, η ασφάλεια του οποίου βασίζεται στη δυσκολεία επίλυσης του προβλήματος του διακριτού λογάριθμου σε πεπερασμένες αβελιανές ομάδες. Αν και ο ElGamal δεν είχε κάνει χρήση συνάρτησης κατακερματισμού, εμείς θα παρουσιάσουμε το σύστημα κάνοντας χρήση μιας τέτοιας συνάρτησης h. Η συνάρτηση h χρειάζεται για τους ίδιους λόγους ασφάλειας, όπως και στο σύστημα υπογραφών RSA.

Οι παράμετροι του συστήματος υπογραφών είναι ακριβώς οι ίδιες με αυτές του συστήματος κρυπτογράφησης. Δηλαδή, επιλέγουμε μια πεπερασμένη αβελιανή ομάδα G και ένα στοιχείο $g \in G$ τάξης πρώτου q. Μπορούμε να υποθέσουμε ότι ο q είναι πρώτος αριθμός. Τα G, g και q είναι παράμετροι του συστήματος κοινά για όλους τους χρήστες (και φυσικά γνωστά σε όλους).

Κάθε χρήστης, ας πούμε η Αλίκη, επιλέγει ένα ακέραιο a στο διάστημα $[1, q]$ τυχαία. Το a είναι το ιδιωτικό κλειδί της Αλίκης. Ακόμη η Αλίκη υπολογίζει και δημοσιοποιεί το $y = g^a$, που είναι το δημόσιο κλειδί της.

Υποθέτουμε ότι τα μηνύματα είναι ακέραιοι. Τότε η συνάρτηση κατακερματισμού που χρησιμοποιούμε είναι μια συνάρτηση

$$h : \mathbb{Z} \longrightarrow \mathbb{Z}/q\mathbb{Z}$$

που έχει τις τρεις βασικές ιδιότητες που περιγράψαμε στο προηγούμενο μάθημα. Επίσεις χρειαζόμαστε μία 1-1 απεικόνιση

$$f : \langle g \rangle \longrightarrow \mathbb{Z}.$$

Δεν έχουμε καμμία άλλη απαίτηση από την f. Ο λόγος ύπαρξης της, όπως θα φανεί στην περιγραφή του αλγορίθμου, είναι ότι χρειαζόμαστε μια αναπαράσταση (μία γραφή) οποιουδήποτε στοιχείου της υποομάδας $\langle g \rangle$ ως ακεραίου. Αν, για παράδειγμα, η ομάδα G είναι η $\mathbb{F}_p^\times$ για κάποιο πρώτο p, τότε μια επιλογή της f είναι προφανής.

Αλγόριθμος υπογραφής

(1) Επιλέγει $k \in \{1, \ldots, q-1\}$ τυχαία και υπολογίζει το $r = g^k$.
(2) Υπολογίζει το $s = k^{-1}(h(m) + af(r)) \mod q$.
(3) Η υπογραφή στο μήνυμα m είναι το (s, r).

Αλγόριθμος πιστοποίησης

(1) Δεδομένων του μηνύματος m, της υπογραφής (s, r) και του δημόσιου κλειδιού y, υπολογίζει τα $r^s, g^{h(m)}, y^{f(r)}$.
(2) Αν $r^s = g^{h(m)} y^{f(r)}$ απαντά «ΝΑΙ», διαφορετικά απαντά «ΟΧΙ».

Μπορεί κανείς να ελέγξει εύκολα ότι όλες οι υπογραφές που έχουν παραχθεί με γνώση του ιδιωτικού κλειδιού (δηλαδή νόμιμα) πιστοποιούνται από τον αλγόριθμο, αφού από την εξίσωση υπογραφής έχουμε

$$\begin{aligned} sk &\equiv h(m) + af(r) \pmod{q} \iff \\ g^{sk} &= g^{h(m)} g^{af(r)} \iff \\ r^s &= g^{h(m)} y^{f(r)} \end{aligned}$$

Παράδειγμα 1.1. Ας δούμε ένα παράδειγμα, όπου η ομάδα μας είναι η $\mathbb{F}_{47}^{\times}$. Η τάξη της ομάδας είναι $47 - 1 = 2 \cdot 23$. Με δοκιμές βρίσκουμε ότι το στοιχείο $g = 2$ έχει τάξη $q = 23$. Ας υποθέσουμε ότι το ιδιωτικό κλειδί μας είναι το $a = 14$, οπότε υπολογίζουμε το δημόσιο κλειδί μας $y = 2^{14} \mod 47 = 28$. Ας υπογράψουμε το μήνυμα $m = 32$. Επιλέγουμε $k = 8$ και υπολογίζουμε το $r = 2^8 \mod 47 = 21$. Ας υποθέσουμε ακόμα ότι $h(m) = h(32) = 20$. Υπολογίζουμε $s = k^{-1}(h(m) + ar) \mod q = 3 \cdot (20 + 14 \cdot 21) \mod 23 = 22$ Άρα η υπογραφή στο μήνυμα $m = 32$ είναι το ζεύγος $(s, r) = (22, 21)$. Οποιοσδήποτε θέλει να πιστοποιήσει την υπογραφή υπολογίζει τα $r^s = 21^{22} \mod 47 = 9$, $g^{h(m)} = 2^{20} \mod 47 = 6$ και $y^r = 28^{21} \mod 47 = 25$ και να ελέγξει ότι $9 \equiv 6 \cdot 25 \pmod{47}$. Παρατηρήστε ότι μια δεύτερη υπογραφή στο το ίδιο μήνυμα και με το ίδιο ιδιωτικό κλειδί θα είναι με μεγάλη πιθανότητα διαφορετική, καθώς το k επιλέγεται κάθε φορά τυχαία.

2. Υπογραφες Schnorr

Από τη δημοσίευση του ElGamal και μετά έχουν προταθεί διάφορες παραλλαγές του παραπάνω σχήματος. Ένα από τα πιο ενδιαφέροντα είναι αυτό του Schnorr. Οι παράμετροι του συστήματος είναι ίδιες ακριβώς με αυτές του κλασικού ElGamal. Ας θεωρήσουμε, λοιπόν, μια πεπερασμένη αβελιανή ομάδα G, στοιχείο $g \in G$ τάξης q πρώτου αριθμού και ας είναι (a, y) ένα ζεύγος ιδιωτικού,δημόσιου κλειδιού. Θα χρησιμοποιήσουμε μια συνάρτηση κατακερματισμού $h : \mathbb{Z} \times \langle g \rangle \longrightarrow \mathbb{Z}/q\mathbb{Z}$. Όπως είναι φανερό από τον ορισμό της συνάρτησης κατακερματισμού και τον παρακάτω αλγόριθμο υπογραφής, θεωρούμε ότι το μήνυμα είναι ένας ακέραιος.

Αλγόριθμος υπογραφής

(1) Επιλέγει $k \in \{0, \ldots, q-1\}$ τυχαία και υπολογίζει το $r = g^k$.
(2) Υπολογίζει το $e = h(m, r)$.
(3) Υπολογίζει το $s = k + ae \mod q$.

(4) Η υπογραφή στο μήνυμα m είναι το (s, e).

Αλγόριθμος πιστοποίησης

(1) Δεδομένων του μηνύματος m, της υπογραφής (s, e) και του δημόσιου κλειδιού y, υπολογίζει το $r' = g^s y^{-e}$.
(2) Υπολογίζει το $e' = h(m, r')$
(3) Αν $e' = e$ απαντά «ΝΑΙ», διαφορετικά απαντά «ΟΧΙ».

Δεν είναι δύσκολο να δει κανείς ότι κάθε υπογραφή που έχει κατασκευαστεί με χρήση του αλγόριθμου υπογραφής, δηλαδή με γνωση του ιδιωτικού κλειδιού πιστοποιήται επιτυχώς, διότι

$$\begin{aligned} r' &= g^s y^{-e} \\ &= g^{k+ae} g^{-ae} \\ &= g^k \\ &= r \end{aligned}$$

και συνεπώς $e' = h(m, r') = h(m, r) = e$.

Παράδειγμα 2.1. Με τις ίδιες παραμέτρους του προηγούμενου παραδείγματος θα υπογράψουμε το μήνυμα $m = 15$ με το σχήμα του Schnorr. Επιλέγουμε τυχαία $k = 7$ και υπολογίζουμε $r = 2^7 \mod 47 = 34$. Έστω ότι $e = h(15, 34) = 3$. Υπολογίζουμε $s = 7 + 14 \cdot 3 \mod 23 = 3$. Άρα η υπογραφή στο μήνυμα $m = 15$ είναι το ζεύγος $(s, e) = (3, 3)$. Για πιστοποίηση της υπογραφής κανείς υπολογίζει το $r' = 2^3 \cdot 28^{-3} \mod 47 = 34$ και υπολογίζει το $e' = h(m, r') = h(15, 34) = 3$, το οποίο είναι ίσο με το e άρα η υπογραφή πιστοποιήται.

Είναι δυνατή η πλαστογράφηση υπογραφών Schnorr; Η απάντηση είναι *όχι*. Αποδεικνύεται ότι είναι υπολογιστικά ανέφικτη η υπαρκτή πλαστογραφία με επιθέσεις επιλεγόμενων μηνυμάτων εφόσον ο υπολογισμός διακριτών λογαρίθμων είναι δύσκολος στην ομάδα G και με την επιπλέον υπόθεση ότι η συνάρτηση κατακερματισμού δίνει ομοιόμορφη κατανομή. Η τελευταία υπόθεση είναι γνωστή και ως *Random Oracle Model*.

3. Υπογραφες με ανακτηση μηνυματος

Εκτός από τα κλασικά σχήματα υπογραφών που έχουμε δει ως τώρα, υπάρχουν σχήματα υπογραφών με διάφορες επιπλέον ιδιότητες. Ένα τέτοιο σχήμα είναι αυτό των Nyberg και Rueppel, που προσφέρει ανάκτηση μηνύματος. Στο σχήμα αυτό, δηλαδή, ο υπογράφων αποστέλει μόνο την υπογραφή (και όχι το μήνυμα). Οποιοσδήποτε μπορεί να πιστοποιήσει την υπογραφή και να ανακτήσει το μήνυμα. Όπως και τα προηγούμενα σχήματα, είναι μια παραλλαγή υπογραφών ElGamal στην ομάδα $G = \mathbb{F}_p^\times$, οπότε οι παράμετροι και τα κειδιά δημιουργούνται με τον ίδιο τρόπο όπως στο βασικό σχήμα ElGamal.

Εφόσον θέλουμε να ανακτήσουμε το μήνυμα από την υπογραφή, δε μπορούμε πλέον να χρησιμοποιήσουμε συνάρτηση κατακερματισμού, ώστε να απεικονίσουμε το μήνυμα m σε ένα κατάλληλα μικρό ακέραιο $h(m)$ και στη συνέχεια να υπογράψουμε το $h(m)$. Πρέπει κατ' ανάγκη να κόψουμε το μήνυμα σε τμήματα

και να υπογράψουμε κάθε τμήμα χωριστά. Ας υποθέσουμε ότι δουλευουμε με ένα $g \in G$, τάξης πρώτου q. Για λόγους που θα φανούν αμέσως, θα πρέπει κάθε τμήμα του μηνύματος να έχει μέγεθος (ας πουμε αριθμό δυαδικών ψηφίων) $n/2$, όπου $2^n < q$, δηλαδή $n < \log_2 q$ και n άρτιος. Επιπλέον θα χρησιμοποιήσουμε τη συνάρτηση

$$\begin{aligned} R : \{0,1\}^{n/2} &\longrightarrow \{0,1\} \\ m &\mapsto m \parallel m, \end{aligned}$$

όπου $m \parallel m$ είναι η «συγκόλληση» των δυαδικών αναπαραστάσεων του m. Μπορούμε να εκφράσουμε το ίδιο πράγμα αλγεβρικά ορίζοντας

$$\begin{aligned} R : \{m \in \mathbb{Z} | 0 \leq m < 2^{n/2}\} &\longrightarrow \{m \in \mathbb{Z} | 0 \leq m < 2^n\} \\ m &\mapsto m + 2^{n/2} m. \end{aligned}$$

Οι δύο βασικές ιδιότητες της R είναι ότι αντιστρέφεται εύκολα (κανείς υπολογίζει εύκολα προεικόνες) και ότι αν κανείς επιλέξει κάποιο στοιχείο στο πεδίο τιμών τυχαία (με ομοιόμορφη κατανομή), η πιθανότητα να είναι εικόνα κάποιου στοιχείου του πεδίου ορισμού είναι $2^{-n/2}$, δηλαδή αμελητaία για μεγάλο n.

Αλγόριθμος υπογραφής

(1) Επιλέγει $k \in \{0, \ldots, q-1\}$ τυχαία και υπολογίζει το $r = g^k$.
(2) Υπολογίζει το $e = r \cdot R(m) \mod p$.
(3) Υπολογίζει το $s = k + ae \mod q$.
(4) Η υπογραφή στο μήνυμα m είναι το (s, e).

Αλγόριθμος πιστοποίησης/ανάκτησης μηνύματος

(1) Δεδομένης της υπογραφής (s, r) και του δημόσιου κλειδιού y, υπολογίζει το $u = g^s y^{-e} \mod p$.
(2) Υπολογίζει το $v = e \cdot u^{-1} \mod p$.
(3) Αν το v είναι εικόνα κάποιου $0 \leq m < 2^{n/2}$ μέσω της R απαντά «ΝΑΙ», διαφορετικά απαντά «ΟΧΙ».
(4) Αν η απάντηση στο προηγούμενο βήμα ήταν «ΝΑΙ», προχωρεί σε ανάκτηση του μηνύματος υπολογίζοντας την προεικόνα του v. Υπολογίζει, δηλαδή τον ακέραιο $m = v/(1 + 2^{n/2})$.