Εργασία Κρυπτογραφίας– Μάιος 2022

Οδηγίες:

- Όπου απαιτούνται πράξεις, θα πρέπει να εξηγείτε τους υπολογισμούς σας.
- Να απαντάτε στο ζητούμενο με σαφήνεια και να εξηγείτε τη σκέψη σας.

Άσκηση 1 Έστω GGen μια συνάρτηση η οποία με είσοδο 1^λ, επιστρέφει ως έξοδο $(\mathbb{G}, g, q)$, τέτοια ώστε η κυκλική ομάδα $\mathbb{G} = \langle g \rangle$ έχει τάξη q, με q πρώτο και $q \approx 2^\lambda$. Επιπλέον, στις ομάδες που παράγει η GGen, το πρόβλημα DDH είναι δύσκολο.

(α΄) Στο σχήμα υπογραφών DSA είναι δυνατό να προσδιορίσουμε το δημόσιο κλειδί από μια υπογραφή $\sigma = (r, s)$ όπου $r, s \neq 0 \mod q$, και ένα μήνυμα m. Για δική σας διευκόλυνση, υποθέστε[1] ότι η συνάρτηση F είναι αντιστρέψιμη και «1-1».

Με αυτή την υπόθεση διατυπώστε έναν αλγόριθμο Retrieve$(param, \sigma, m) \rightarrow h$, με $h \in \mathbb{G}$ ο οποίος για μια υπογραφή υπολογίζει ενα υποψήφιο δημόσιο κλειδί h^*, τέτοιο ώστε αν $\sigma = \mathsf{Sign}(param, sk, m)$ ισχύει ότι $g^{sk} = \text{Retrieve}(param, \sigma, m)$.

(β΄) Στο μάθημα, όπως και στο παραπάνω ερώτημα, είχαμε αναφέρει ότι η F δεν χρειάζεται να έχει τις ιδιότητες ασφάλειας που έχει μια κρυπτογραφική συνάρτηση κατακερματισμού (λ.χ. ανθεκτική σε συγκρούσεις, δύσκολη στην αντιστροφή). Αντίθετα, οι ιδιότητες αυτές χρειάζονται στην H.

Θεωρήστε μια παραλλαγή του ECDSA όπου:

i. Στη θέση της H χρησιμοποιούμε την ταυτοτική συνάρτηση $id(x) = x$,
ii. Αλλάζουμε τον χώρο μηνυμάτων σε $\mathcal{M} := \mathbb{Z}_q$.

Δείξτε ότι μπορούμε να δημιουργήσουμε πλαστογραφίες υπογραφών γνωρίζοντας μόνο τις παραμέτρους $param$ και το δημόσιο κλειδί h. Η επιλογή μηνύματος είναι ελεύθερη. Συγκεκριμμένα, δείξτε ότι παραβιάζεται η ασφάλεια κατα EUF-KOA (δηλαδή χωρίς παροχή μαντείου Sign στον αντίπαλο).

Υπόδειξη: Αντί $r \leftarrow F(g^k)$ δοκιμάστε να χρησιμοποιήσετε $r \leftarrow F(g^k h^\lambda)$.

Λύση

(α΄) Ξεκινάμε από την εξίσωση ελέγχου μιας υπογραφής: $r \stackrel{?}{=} F(g^{w \cdot H(m)} h^{w \cdot r})$. Ισοδύναμα, η έκφραση $g^{w \cdot H(m)} h^{w \cdot r}$ πρέπει να είναι αντίστροφη εικόνα του r μέσω της F, αν και όχι απαραίτητα μοναδική. Με την υπόθεση ότι η F αντιστρέφεται εύκολα, έχουμε, ότι στις υπογραφές που επαληθευονται ισχύει: $F^{-1}(r) = g^{w \cdot H(m)} h^{w \cdot r}$. Θέτουμε[2] $R = F^{-1}(r)$ και έτσι έχουμε:

$$R = g^{w \cdot H(m)} h^{w \cdot r}$$

Ισοδύναμα: $R \cdot g^{-w \cdot H(m)} = h^{w \cdot r}$ και τελικά $h = (R \cdot g^{-w \cdot H(m)})^{1/(w \cdot r)}$.

Στην πράξη η παραπάνω δυνατότητα μας επιτρέπει να εκτελούμε το verification ακόμα και εάν αντί το h έχουμε στη διαθεσή μας μόνο μια συναρτησή του(πχ ένα hash του, $H_1(h)$) με περιορισμένη επίπτωση στην συνολική ασφάλεια (μιας και πρέπει πλέον να θεωρήσουμε ότι υπάρχουν πιθανές πλαστογραφίες μέσω συγκρούσεων στην H_1). Από την άλλη, για υπογραφές *μίας* χρήσης, η παραχάραξη υπογραφών παραμένει δύσκολη ακόμα και για αντιπάλους που μπορούν να υπολογίσουν διακριτούς λογαρίθμους!

[1] Στην πραγματικότητα υπάρχουν συγκρούσεις, αλλά η αντιστροφή με εξαντλητικές δοκιμές είναι εφικτή.
[2] Όταν δεν έχουμε μοναδική αντίστροφη εικόνα, εξετάζουμε όλες τις περιπτώσεις.

(β΄) Ξεκινάμε και πάλι από την εξίσωση ελεγχου, και χρησιμοποιούμε την υπόδειξη για την επιλογή του r. Έστω τυχαία k, λ, s, οπότε και θέτουμε $w = s^{-1}$. Θα πρέπει να ισχύει:

$$F(g^k h^\lambda) \stackrel{?}{=} F(g^{w \cdot H(m)} h^{w \cdot r})$$

Για το οποίο αρκεί να έχουμε:

$$g^k h^\lambda \stackrel{?}{=} g^{w \cdot H(m)} h^{w \cdot r}$$

Μας αρκεί να ισχύει: $k = wcdotH(m)$ και $\lambda = w \cdot r$. Για το δεύτερο, μπορούμε να θέσουμε $r \leftarrow \lambda / w$ και για το πρώτο, επιλέγουμε κατάλληλο m ώστε $H(m) = k/w$, το οποίο είναι εύκολο όταν η H είναι η ταυτοτική αλλά δύσκολο όταν (ως συνήθως) είναι μονόδρομη.

Άσκηση 2 Θέλουμε να κατασκευάσουμε μια παραλλαγή του πρωτοκόλλου του Schnorr ως εξής:

i. Ο prover στέλνει ως αρχικό μήνυμα ένα στοιχείο a της ομάδας της επιλογής του.

ii. Ο verifier επιλέγει τυχαία εάν θέλει να μαθει είτε τον λογάριθμο του a ως προς το g, είτε το λογάριθμο του h ως προς το a.

Όπως στο αρχικό πρωτόκολλο, η πρόταση $h = g^w$ είναι γνωστή και στους δύο συμμετέχοντες, ενώ ο μάρτυρας w μόνο στον prover.

(α΄) Διατυπώστε ένα πρωτόκολλο σύμφωνα με την παραπάνω περιγραφή και αποδείξτε ότι είναι πλήρες.

(β΄) Αποδείξτε ότι έχει την ιδιότητα της ειδικής εγκυρότητας (special soundness).

(γ΄) Αποδείξτε ότι έχει την ιδιότητα της Μηδενικής Γνώσης Τίμιου Επαληθευτή (HVZK).

(δ΄) **Μεταπτυχιακοί μόνο.** Αποδείξτε ότι έχει την ιδιότητητα της Μηδενικής Γνώσης (ZK).

(α΄) Το πρωτόκολλο μπορεί να λειτουργήσει ως εξής:

- Ο Prover υπολογίζει $t \leftarrow \mathbb{Z}_q^*; a \leftarrow g^t$, και στέλνει το a στον Verifier.
- Ο Verifier επιλέγει τυχαία $c \leftarrow \{0, 1\}$.
- Ο Prover στέλνει $s \leftarrow t$ εάν $(c = 0)$ ή διαφορετικά $s \leftarrow w \cdot t^{-1}$.
  Εάν $c = 0$, ο Verifier ελέγχει εάν $g^s = a$ αλλιώς ελέγχει αν $a^s = h$.

Από κατασκευής, το παραπάνω πρωτόκολλο αντιστοιχεί στην περιγραφή της εκφώνησης. Μπορούμε να επιβεβαιώσουμε την πληρότητα παίρνοντας περιπτώσεις για το c. Επίσης, παρατηρούμε ότι αφού $t \leftarrow \mathbb{Z}_q^*$, δεν υπάρχει ζήτημα κατά την αντιστροφή του t.

(β΄) Για την ειδική εγκυρότητα, αρκεί να δείξουμε ότι υπάρχει αλγόριθμος, όπου για δύο τριάδες αποδεκτών συζητήσεων (a, c, s), (a, c', s') όπου $c \; neq c'$ μπορεί να εξάγει μάρτυρα για το x.

Αρχικά, χωρίς βλάβη, οι τριάδες θα είναι της μορφής $(a, 0, s)$, $(a, 1, s')$. Οπότε, από τον έλεγχο του Verifier θα πρέπει να ισχύει: $g^s = a$ και $a^{s'} = h$. Τότε όμως θα έχουμε για το $g^{s \cdot s'}$ ότι:$g^{s \cdot s'} = (g^s)^{s'} = a^{s'} = h$. Οπότε, το $w' = s \cdot s'$ είναι ένας μάρτυρας ο οποίος εξάγεται εύκολα από δύο κατάλληλες συζητήσεις.

(γ΄) Ακολουθούμε ένα παρόμοιο σκεπτικό με τον simulator του schnorr: επιλέγουμε τυχαίο $s \leftarrow \mathbb{Z}_q^*$, και τυχαίο $c \leftarrow \{0, 1\}$. Τέλος, παρατηρούμε ότι για συγκεκριμμένη επιλογή c, s το a για το οποίο ο έλεγχος του verifier πετυχαίνει είναι μοναδικό. Μένει να δείξουμε ότι οι συζητήσεις που παράγονται από τον simulator έχουν την ίδια κατανομή για τις κανονικές. Όταν $c = 0$ αυτό είναι τετριμμένο, αφού και στις δύο περιπτώσεις το s είναι ομοιόμορφα κατανεμημένο στο $\mathbb{Z}_q^*$.

Όταν $c = 1$, οι κατανομές του s διαφέρουν ελαφρώς: στις προσομοιώσεις το s είναι πάντα ομοιόμορφο στο $\mathbb{Z}_q^*$, ενώ στις αληθινές συζητήσεις είναι όντως ομοιόμορφο όταν $w \neq 0$, αλλά σταθερά

μηδενικό όταν $w = 0$. Η στατιστική απόσταση ανάμεσα στις δύο κατανομές δεν είναι μεγάλη, αφού διαφωνούν κατά $O(q^{-2})$ σε $q - 1$ στοιχεία και κατά $O(q^{-1})$ σε ένα, οπότε η συνολική διαφορά είναι $O(q^{-1})$ άρα αμελητέα όταν το q έχει μήκος bits όσο η παράμετρος ασφαλείας μας.

Εναλλακτικά, ο simulator μπορεί να ελέγχει εάν $w = 0$ στην αρχή της εκτέλεσης, και αν ναι, εκτελεί το πρωτόκολλο γνωρίζοντας πλέον τον μάρτυρα και άρα η προσομοίωση είναι τέλεια.

(δ΄) Αντίθετα με το πρωτόκολλο του Schnorr, λόγω του περιορισμένου εύρους του c, η μηδενική γνώση για οποιονδήποτε επαληθευτή είναι εφικτή. Εργαζόμαστε όπως παραπάνω με ένα επιπλέον βήμα: αφού έχουμε δημιουργήσει μια τριάδα (a, c, s) τρέχουμε τον (πιθανώς κακόβουλο) επαληθευτή V^* με είσοδο το a. Εάν απαντήσει $c^* = c$, κρατάμε την τριάδα ως έξοδο και τερματίζουμε. Αλλιώς, ξαναδοκιμάζουμε από την αρχή.

Μένει να δείξουμε ότι (1) ο νέος αλγόριθμος τερματίζει με συντριπτική πιθανότητα σε πολυωνυμικό χρόνο και (2) η κατανομή των τριάδων είναι σωστή. Και για τα δύο σημεία, παρατηρούμε ότι η κατανομή των a στις αρχικές τριάδες του simulator είναι ίδια όταν[3] $w \neq 0$, ανεξάρτητα από την τιμή του c. Άρα, η απάντηση του V^* είναι ανεξάρτηση του c και συνεπώς $P[c = c^*] = \frac{1}{2}$.

Οπότε ο αλγοριθμός μας έχει πιθανότητα εκθετικά μικρή στο k να κάνει πάνω από k απόπειρες χωρίς να έχει τερματίσει.

Για την κατανομή των συζητήσεων που ο simulator επιλέγει ως έξοδο, παρατηρούμε ότι τα a του simulator έχουν την ίδια κατανομή με τα πραγματικά, άρα και τα c^* αφού προέρχονται από τον V^* (προϋπόθεση για να κρατήσουμε μια τριάδα είναι να συμφωνούν c και c^*). Τέλος, ελέγχοντας ότι το s είναι μοναδικό ως συνάρτηση των a, c έχουμε το ζητούμενο.

Η σημαντική διαφορά με το πρωτόκολλο του schnorr είναι ο χώρος των c. Με 2 πιθανές επιλογές, έχουμε σημαντική πιθανότητα να κρατήσουμε μια τριάδα όταν τη «διασταυρώσουμε» με τον V^*. Με q επιλογές όμως, η πιθανότητα αυτή είναι αμελητέα και δεν έχουμε καλό φράγμα, έστω και στατιστικά, για τον αριθμό των δοκιμών πριν τον τερματισμό.

[3] Όταν $w = 0$ τα πράγματα είναι εύκολα.