Εργασία Κρυπτογραφίας– Μάιος 2023

Παράδοση: Τετάρτη 31/5/2023 4:00μμ

Οδηγίες:

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

1. Ποιές από τις παρακάτω ομάδες είναι κατάλληλες για χρήση με το σχήμα κρυπτογράφησης του ElGamal:

   (α□) Η υπο-ομάδα που παράγεται από ένα στοιχείο g μέγιστης τάξης στο Z_n^*, όπου n μεγάλος πρώτος της μορφής $2p+1$, p πρώτος.

   (β□) Η υπο-ομάδα που παράγεται από ένα στοιχείο g^2 όταν το g είναι στοιχείο μέγιστης τάξης στο $\mathbb{Z}_n^*$, με πράξη τον πολλαπλασιασμό $\mod n$ όπου n μεγάλος πρώτος της μορφής $2p+1$, p πρώτος.

   (γ□) Η υπο-ομάδα που παράγεται από το στοιχείο -1 στο $\mathbb{Z}_n^*$, με πράξη τον πολλαπλασιασμό $\mod n$ όπου n μεγάλος πρώτος της μορφής $2p+1$, p πρώτος.

2. Σε μία εμπορική υλοποίηση του σχήματος του Schnorr έχει χρησιμοποιηθεί ο αλγόριθμος [1] του σχήματος 1 ώστε να επιλεγεί ένα τυχαίο στοιχείο στο $\mathbb{Z}_q$. Αυτός ο αλγόριρθμος καλείται από τον prover όσο και από τον verifier για τις τιμές του t, c αντίστοιχα.

```
int getRandomNumber()
{
    return 4;  // chosen by fair dice roll.
               // guaranteed to be random.
}
```

Σχήμα 1: Αλγόριθμος επιλογής τυχαίου στοιχείου στο $\mathbb{Z}_q$.

   (α□) Εργαζόμαστε στην ομάδα τάξης 11 που παράγει το $g = 2 \mod 23$. Παρουσιάστε μια εκτέλεση του πρωτοκόλου, για $h = g^w$, όπου w το τελευταίο ψηφίο του ΑΜ σας (ή 10 εάν αυτό το τελευταίο ψηφίο είναι 0) με τους συμμετέχοντες να χρησιμοποιούν τον παραπάνω αλγόριθμο. Όπως συνήθως, το h είναι δημόσιο αλλά το w το γνωρίζει μόνο ο prover.

   (β□) Περιγράψτε πως μπορεί ένας prover που δεν ξέρει το w ή τον ΑΜ σας να παριστάνει ότι το γνωρίζει, όταν τον ελέγχει ο παραπάνω verifier.

   (γ□) Περιγράψτε πως μπορεί ένας verifier να αποσπάσει το w εάν μπορεί να αλληλεπιδράσει φυσιολογικά[1] με τον υλοποιημένο prover.

3. Εξετάστε **αναλυτικά** τους παρακάτω ισχυρισμούς:

   (α□) Εστω ένα κρυπτομήνυμα $c = (u, v)$ κρυπτογραφήμένο με ElGamal για το οποίο γνωρίζουμε και έχουμε αποθηκεύσει την τιμή r που χρησιμοποιήθηκε κατά την κρυπτογράφηση. Για να δείξουμε ότι το c είναι κρυπτογράφηση του $m = 0$ αρκεί να εκτελέσουμε δύο φορές το πρωτόκολο του Schnorr: μια για να δείξουμε ότι γνωρίζουμε μάρτυρα w_1 ώστε $u = g^{w_1}$, και μια για να δείξουμε ότι γνωρίζουμε μάρτυρα w_2 ώστε $v = g^{w_2}$.

[1] Χωρίς τη δυνατότητα να παγώνει, αποθηκεύει ή να επαναφέρει την εκτέλεση σε προηγούμενο σημείο.

(β□) Εστω ένα κρυπτομήνυμα $c = (u, v)$ κρυπτογραφήμένο με ElGamal για το οποίο γνωρίζουμε και έχουμε αποθηκεύσει την τιμή r που χρησιμοποιήθηκε κατά την κρυπτογράφηση. Εάν καταστεί απαραίτητο, είναι εφικτό να αποκαλύψουμε το μήνυμα m που περιέχεται στο c ακόμα και αν έχουμε ξεχάσει το ίδιο το m;

(γ□) Είναι εφικτό με έναν εμπορικά διαθέσιμο υπολογιστή σημερινής τεχνολογίας να λύσουμε[2] το πρόβλημα του διακριτού λογαρίθμου σε ομάδες με τάξης $q \approx 2^{64}$.

References

[1] Randall Munroe. *Random number*. Feb. 2007. url: `https://xkcd.com/221/`.

[2] Αναφερόμαστε σε τοπικό υπολογισμό στο δικό μας υπολογιστή.