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.

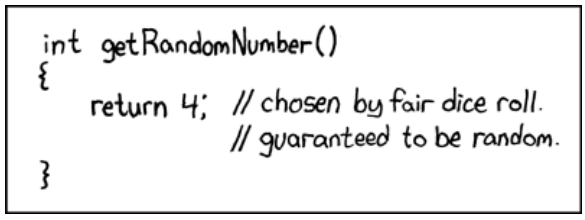
   (γ□) Η υπο-ομάδα που παράγεται από το στοιχείο -1 στο $\mathbb{Z}_n^*$, με πράξη τον πολλαπλασιασμό $\mod n$ όπου n μεγάλος πρώτος της μορφής $2p+1$, p πρώτος.

   (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. Σε αυτή την περίπτωση, σύμφωνα με όσα ξέρουμε το g, και κατά συνέπεια η παραγόμενη ομάδα $\mathbb{G} := \langle g \rangle$ που θα κατασκευάσουμε θα έχει τάξη $\phi(n) = n - 1 = 2p$. Αφού ο $2p$ είναι σύνθετος, από προηγούμενες αναλύσεις που έχουμε κάνει στο μάθημα μπορούμε να κατασκευάσουμε επιθέσεις στο κρυπτοσύστημα ElGamal, ή ισογύναμα να δείξουμε ότι το DDH δεν είναι δύσκολο (σκιαγράφηση: αν (A,B,C) είναι μια υποψήφια τριάδα, το C^p έχει πολύ διαφορετική κατανομή ανάλογα με το αν η τριάδα είναι DDH ή όχι).

   (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. Σε αυτή την περίπτωση, σύμφωνα με όσα ξέρουμε το g, θα έχει τάξη $\phi(n) = n - 1 = 2p$, άρα το g^2 θα έχει τάξη p, οπου p πρώτος. Στην κατασκευή αυτή λοιπόν έχουμε ομάδα με τάξη πρώτο, και σύμφωνα με όσα έχουμε δει στις σημειώσεις θεωρούμε ότι σε τέτοιες υποομάδες του $\mathbb{Z}_n^*$, το DLOG και το DDH είναι δύσκολα.

   (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. Σε αυτή την περίπτωση, η ομάδα μας έχει τάξη 2, αφού ισχύει ότι $(-1)^2 = 1 \mod n$. Αυτό κάνει την ομάδα μας υπερβολικά μικρή για οποιαδήποτε πρακτική εφαρμογή, αφού ο υπολογισμός π.χ. του DLOG λύνεται με έλεγχο αν το στοιχείο είναι -1 (με λογάριθμο 1) ή 1 (με λογάριθμο 0).

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.



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.

(α□) Θεωρούμε ότι $w = 10$, άρα $h = 2^{10} = 32 \cdot 32 \mod 23 = 81 \mod 23 = 12$.Ο prover αρχικά υπολογίζει $t \leftarrow 4$ (από υπόθεση) και $a \leftarrow 2^4 \mod 23$. Άρα $a = 16$. Από υπόθεση ο verifier στέλνει $c \leftarrow 4$, και τελικά ο prover θα υπολογίσει $s \leftarrow c \cdot w + t$ άρα $s = 4 \cdot 10 + 4 \mod 11 = 0$.

(β□) Ένας τέτοιος prover μπορεί να επιχειρήσει να προσομοιώσει την εκτέλεση αφού έχει την εξασφάλιση ότι ο verifier θα επιλέξει $c = 4$. Άρα, διαλέγει ένα τυχαίο $\tilde{s} \leftarrow \mathbb{Z}_q$, και υπολογίζει πόσο χρειάζεται να είναι η τιμή του $\tilde{a}$ ώστε ο έλεγχος του verifier να είναι επιτυχής. Δηλαδή: $2^{\tilde{s}} = 12^4 \cdot a$ ή ισοδύναμα: $a = 2^{\tilde{s}} \cdot 12^{-4}$. Επιλέγοντας π.χ. $\tilde{s} = 5$ έχουμε ότι το a θα είναι: $32/(144^2) = 9/6^2 = 9/36 = 1/4 = 6$.

(γ□) Από τη στιγμή που ο prover εχει χρησιμοποιήσει $t = 4$, ο verifier μπορεί να χρησιμοποιήσει τη δομή που έχει το $s = c \cdot w + t$ ώστε να υπολογίσει $w = (s - t)/c$. Στην περίπτωση π.χ. του πρώτου ερωτήματος θα υπολόγιζε $w = (0 - 4)/4 = -1 = 10 \mod 11$.

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 $m = 0$ (δηλ. του ουδέτερου στοιχείου) 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 $v = g^{w_2}$.

(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 $q \approx 2^{64}$.

(α□) Ένα κρυπτομήνυμα $c = (u, v)$ που περιέχει το ουδέτερο στοιχείο είναι αναγκαστικά της μορφής (g^r, h^r). Αρχικά, δεν είναι εφικτό να δείξουμε ότι η δευτερη συνιστώσα είναι της μορφής $v = g^{w_2}$. Για να το κάνουμε αυτό, θα έπρεπε να γνωρίζουμε $w_1 = r$ και $w_2 = r * cdotx$, όπου x το ιδιωτικό κλειδί που αντιστοιχεί στο h. Αυτό δεν είναι κάτι που έχουμε στη διαθεσή μας. Θα μπορούσαμε να αλλάξουμε τη δεύτερη πρόταση ώστε να δείξουμε ότι γνωρίζουμε μάρτυρα w_2 ώστε $v = h^{w_2}$, αλλά ούτε αυτό είναι απόδειξη για το ζητούμενο: ένας υπολογιστικά ισχυρός Prover μπορεί να βρει κατάλληλο w_2 ακόμα και όταν το v είναι της μορφής $h^r \cdot m$ για μη τετριμμένο m. Αυτό που πρέπει να αποδείξουμε είναι ότι: «γνωρίζουμε μάρτυρα w_1 ώστε $u = g^{w_1}$, και γνωρίζουμε μάρτυρα w_2 ώστε $v = h^{w_2}$ και επιπλέον $w_1 = w_2$», ή ισοδύναμα «γνωρίζουμε μάρτυρα w ώστε $u = g^w$, και $v = h^w$».

(β□) Ναι. Μπορούμε να δημοσιοποιήσουμε το r. Κάποιος που θέλει να αποκρυπτογραφήσει το κρυπτομήνυμα $c = (u, v)$ λειτουργεί ως εξής: πρώτα ελέγχει ότι το r είναι σωστό, δηλαδή εάν $g^r == u$

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

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

(αν όχι, απορρίπτει το r και σταματά). Έπειτα, αφού ισχύει ότι $u = g^r$ θα ισχύει λόγω του αλγορίθμου κρυπτογράφησης ότι $v = h^r \cdot m$. Άρα, υπολογίζει το v/h^r το οποίο είναι και η αποκρυπτογράφηση του μηνύματος m.

Ένας πιο περίπλοκος τρόπος είναι να μη φανερώσουμε το r, αλλά μόνο το m και να αποδείξουμε ότι το $c' = (u, v/m)$ περιέχει το ουδέτερο στοιχείο. Αυτό μας επιτρέπει να κρατήσουμε το r ώστε να μην μπορεί[3] κάποιος που πείσθηκε από εμάς ότι το c περιέχει το m να πείσει και άλλους.

(γ□) Γενικά, ναι. Οι σύγχρονοι υπολογιστές λειτουργούν σε συχνότητες της τάξης των 4Ghz (χοντρικά 2^{32} «χτύποι» το δευτερόλεπτο). Μία ώρα έχει 3600 δευτερόλεπτα, και μία μέρα 86.400 (χοντρικά 2^{16}). Οπότε, σαν μια τάξη μεγέθους έχουμε περίπου 2^{48} «χτύπους» ανα μέρα[4].

Από την άλλη μεριά, γνωρίζουμε ότι ο υπολογισμός ενός διακριτού λογαρίθμου με απλά μέσα (δηλ. με το baby-step giant-step) χρειάζεται περίπου $2 \cdot 2^{32}$ πράξεις ομάδας (αφού χρειαζόμαστε μια μεγάλη σειρά στοιχείων της μορφής $a, a^2, \ldots, a^n$ αρκεί να κάνουμε $n-1$ πολλαπλασιασμούς αντί $n-1$ υψώσεις), δύο ταξινομήσεις πινάκων μεγέθους 2^{32} και μερικές ακόμα ενέργειες με μικρότερο κόστος. Οι ταξινομήσεις n στοιχείων κοστίζουν χοντρικά $n\,logn$, οπότε μπορούμε να θεωρήσουμε ότι το κόστος θα είναι περίπου $2^{32} \cdot (2M + 32C)$, οπου M το κόστος μιας πράξης ομάδας και C το κόστος μιας σύγκριστης.

Συνδυάζοντας τα παραπάνω, συμπεραίνουμε ότι αν σε 2^{16} προλαβαίνουμε να κάνουμε 2 πράξεις και 32 συγκρίσεις, ο παραπάνω υπολογισμός εκτελείται σε λιγότερο από μια μέρα. Οι συγκρίσεις είναι βέβαιο ότι είναι εύκολο να γίνουν χωρίς ιδιαίτερη διερεύνηση. Για τις πράξεις ομάδας η διερεύνηση είναι πιο πολύπλοκή και ξεφεύγει από το στενό πλαίσιο της ύλης που έχουμε καλύψει σε συνδιασμό με γενικές γνώσεις. Στην (εξαιρετικά απλή) περίπτωση που τα στοιχεία της ομάδας είναι αριθμοί $\mod n$ για $n < 64$ μπορούμε να υποθέσουμε ότι οι πολλαπλασιασμοί γίνονται σε ένα κύκλο και το υπόλοιπο $\mod n$ σε μικρό αριθμό κύκλων. Στη γενικότερη περίπτωση, τα στοιχεία της ομάδας έχουν αναπαραστάσεις μεγαλύτερες από μία θέση μνήμης, και ο υπολογισμός μιας πράξης δεν περιορίζεται σε έναν πολλαπλασιασμό ακεραίων.

References

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

[3] Εάν το πρωτόκολο εκτελέσθηκε διαδραστικά.

[4] Ανά πυρήνα, αλλά ο αντίστοιχος συντελεστής είναι μικρός.