Πρωτόκολλα Μηδενικής Γνώσης

1. Εξετάστε τι συμβαίνει αν πολλαπλασιάσουμε κατά συντεταγμένη δύο κρυπτοκείμενα ElGamal ως προς το ίδιο δημόσιο κλειδί.

   Λύση Έστω $c_1 = (g^{r_1}, m_1 h^{r_1})$ και $c_2 = (g^{r_2}, m_2 h^{r_2})$. Το αποτέλεσμα της πράξης $c_1 \odot c_2$ θα είναι $c^* = (g^{r_1+r_2}, m_1 m_2 h^{r_1+r_2})$. Ξαναγράφουμε το $r_1 + r_2$ ως r^* και το $m_1 m_2$ ως m^*. Τελικά έχουμε $c_1 \odot c_2 := c^* = (g^{r^*}, m^* h^{r^*})$, δηλαδή η κρυπτογράφηση του $m^* = m_1 m_2$ με τυχαιότητα $r* = r_1 + r_2$. Άρα, ο πολλαπλασιασμός κατά συντεταγμένη δύο κρυπτοκειμένων ElGamal είναι ομοιομορφισμός (ως προς την πρόσθεση $\mod q$ για τις τυχαίες τιμές και ως προς την πράξη της ομάδας για τα μηνύματα).

2. Δίνονται οι παράμετροι: $g \equiv 2 \mod 23, \mathbb{G} = \mathbb{Z}_{23}^* \cap \langle g \rangle, q = 11$. Ακολουθήστε τη διαδικασία κατασκευής ζευγους κλειδιών και κατασκευάστε ένα ζεύγος x, h. Κρυπτογραφήστε το μήνυμα $m \equiv 6 \mod 23$ με randomness της επιλογής[1] σας, και κατόπιν αποκρυπτογραφήστε το.

   Παράδειγμα

   Δημιουργία κλειδιού. Επιλέγουμε ένα x ως ιδιωτικό κλειδί από το $\mathbb{Z}_q$, πχ $x = 3$. Υπολογίζουμε το δημόσιο κλειδί ως $h = g^x$, οπότε έχουμε $h \equiv 2^3 \equiv 8 \mod 23$.

   Κρυπτογράφηση. Μας έχει δωθεί το μήνυμα $m = 6 \mod 23$ το οποίο είναι στοιχείο της ομάδας. Επιλέγουμε ένα r ως τυχαίο παράγοντα από το $\mathbb{Z}_q$, πχ $r = 7$. Υπολογίζουμε τα U, V ως $U = g^r$ και $V = h^r$.

   Για το U έχουμε: $U \equiv 2^7 \equiv 128 \equiv 128 - 115 \equiv 13 \mod 23$.

   Για το V έχουμε $V \equiv 6 \cdot 8^7 \equiv 6 \cdot 64 \cdot 64 \cdot 64 \cdot 8 \mod 23$. Όμως, $64 \equiv 64 - 69 \equiv -5 \mod 23$. Οπότε $V \equiv 6 \cdot -5 \cdot -5 \cdot -5 \cdot 8 \equiv 6 \cdot 25 \cdot -40 \equiv 6 \cdot 2 \cdot (46 - 40) \equiv 72 \equiv 72 - 69 \equiv 3 \mod 23$.

   Άρα $c = (U, V) = (13, 3)$.

   Αποκρυπτογράφηση. Γνωρίζουμε ότι $x = 3$ και $c = (U, V) = (13, 3)$. Υπολογίζουμε το $\tilde{m} = U^{-x} \cdot V$. Έχουμε: $U^{-x} \cdot V = 13^{-x} \cdot 3 \equiv 13^{-3} \cdot 3 \equiv 13^8 \cdot 3 \mod 23$. Στον εκθέτη το -3 είναι ισοδύναμο με το 8 αφού η τάξη της ομάδας είναι $q = 11$. Επίσης, παρατηρούμε ότι $13 \equiv -10 \mod 23$. Έχουμε λοιπόν $\tilde{m} \equiv (-10)^8 \cdot 3 \equiv 100 \cdot 100 \cdot 100 \cdot 100 \cdot 3 \equiv (100-92) \cdot (100-92) \cdot (100-92) \cdot (100-92) \cdot 3 \equiv 8 \cdot 8 \cdot 8 \cdot 8 \cdot 3 \equiv 64 \cdot 64 \cdot 3 \equiv (-5) \cdot (-5) \cdot 3 \equiv 25 \cdot 3 \equiv 2 \cdot 3 \equiv 6 \mod 23$.

3. Τι συμβαίνει αν στο κρυπτοσύστημα ElGamal επιλέξουμε ως $\mathbb{G}$ ομάδα σύνθετης τάξης, συγκεκριμμένα το $\mathbb{Z}_p^*$. Δώστε παράδειγμα με βάση το $\mathbb{Z}_{23}^*$, $g \equiv 5, q = 22$.

   Σκιαγράφηση Έχουμε συναντήσει αντίστοιχα παραδείγματα τόσο στο σύστημα του Pedersen όσο και στο Diffie-Hellman. Επειδή η τάξη της ομάδας είναι σύνθετος αριθμός ($22 = 2 \cdot 11$) μπορούμε να υψώσουμε στοιχεία της ομάδας στην 11η ώστε να προκύψουν στοιχεία τάξης το πολύ 2. Συγκεκριμμένα, για οποιοδήποτε $a \in \mathbb{G}$ και $b = a^{11}$ έχουμε $(b)^2 \equiv 1$. Με έλεγχο μπορούμε να δούμε ότι $b \equiv \pm 1$. Οπότε, μπορούμε να ορίσουμε ένα «πρόσημο» για κάθε στοιχείο ανάλογα με το αν υψωμένο στην 11 είναι $+1$ ή -1. Σαν συνέπεια, αν στο πείραμα της ασφάλειας IND-CPA δώσουμε m_0, m_1 με διαφορετικό «πρόσημο», είμαστε τελικά σε θέση να ξεχωρίσουμε ποιό από τα δύο κρυπτογραφήθηκε.

4. Η Μάρτζερι και η Εύα εκτελούν ένα Σ-πρωτόκολλο (δηλ. ένα πρωτόκολλο 3 κινήσεων (έστω a, c, s) με πληρότητα, ειδική εγκυρότητα και HVZK). Η Εύα είναι ο Verifier. Κατά το τέλος τη εκτέλεσης η Εύα ισχυρίζεται ότι ο υπολογιστής της λόγω διακοπής ρεύματος έσβυσε, χάνοντας τα μηνύματα c, s, οπότε ζητάει από την Μάρτζερι να συνεχίσουν την εκτέλεση από αυτό το σημείο. Έχοντας χάσει την

[1] Τετριμμένες επιλογές αναιρούν το νόημα της άσκησης.

τιμή του c, θα στείλει νέα τιμή c'. Η Μάρτζερι προτείνει, για οικονομία, να στείλει εκείνη στην Εύα την χαμένη τιμή του c μαζί με την απάντηση s. Ποιά από τις αντισυμβαλλόμενες έχει δίκιο;

Λύση Δυστυχώς, και οι δύο προτάσεις είναι πιθανώς επικίνδυνες.

Εάν η Εύα λέει ψέματα και έχει κρατήσει τα c, s, τότε στέλνοντας νέο c', το οποίο θα επιλέξει να είναι διαφορετικό του c, θα πάρει μια απάντηση s'. Τότε, λόγω της ειδικής εγκυρότητας, και έχοντας δύο τριάδες (a, c, s), (a, c', s') με $c' \neq c$, θα μπορεί να εξάγει τον μάρτυρα.

Εάν η Εύα λέει αλήθεια, και έχει χάσει τα c, s, τότε η Μάρτζερι είναι σε θέση να την εξαπατήσει: ενδεχομένως να είχε ξεκινήσει το πρωτόκολο χωρίς να γνωρίζει κατάλληλο μάρτυρα, ελπίζοντας σε κάποια ευνοϊκή συγκυρία. Σε μια τέτοια περίπτωση το πιθανότερο είναι ότι θα είχε τρέξει ένα simulator για να παράγει μια αποδεκτή τριάδα (a, c^*, s). Το πιθανότερο βέβαια, είναι ότι το c που θα διάλεγε η Εύα δε θα ήταν ίσο με το c^*, οπότε το πρωτόκολο θα αποτύγχανε, αλλά εαν η Εύα επιτρέψει στην Μάρτζερι να στείλει τη «χαμένη» τιμή του c, η Μάρτζερι θα επιλέξει να στείλει το c^* αντ'αυτού.

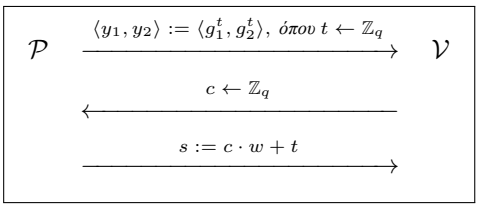
Η μόνη λύση που εξασφαλίζει και τα δύο μέρη είναι να ξαναρχίσει το πρωτόκολο από την πρώτη κίνηση.

5. Βασιζόμενοι στο πρωτόκολλο του Schnorr, διατυπώστε ένα Σ-πρωτόκολλο που αποδεικνύει την ισότητα δύο διακριτών λογαρίθμων (δηλ. ο λογάριθμός του h_1 ως προς το g_1 είναι ίδιος με το λογάριθμο του h_2 ως προς το g_2). Επιβεβαιώστε ότι είναι πλήρες, ειδικά έγκυρο και HVZK.

Λύση Από τις σημειώσεις γνωρίζουμε ότι είναι εφικτό να κατασκευάσουμε πρωτόκολο που να δείχνει την γνώση δύο διαφορετικών διακριτών λογαρίθμων (ως προς διαφορετικές ενδεχομένως βάσεις) με τη χρήση της λογικής σύζευξης στο πρωτόκολο του Schnorr. Το ζητούμενο είναι, επι πλέον, να δείξουμε ότι οι δύο αυτοί διακριτοί λογάριθμοι είναι ίσοι. Η αρχική σκέψη μας είναι να μελετήσουμε την εξαγωγή μαρτύρων μέσω της ειδικής εγκυρότητας ώστε στη συνέχεια να προχωρήσουμε σε κατάλληλες αλλαγές που θα συνεπάγονται την ισότητα των μαρτύρων.

Ας θεωρήσουμε δύο εκτελέσεις του πρωτοκόλου για τα h_1, g_1, h_2, g_2 την πρώτη φορά με μηνύματα $\langle y_1, y_2\rangle, c, \langle s_1, s_2\rangle$ και τη δεύτερη με $\langle y_1, y_2\rangle, c', \langle s'_1, s'_2\rangle$. Από την ειδική εγκυρότητα θα πάρουμε ότι $w_1 = (s_1 - s'_1)/(c - c') \mod q$ και $w_2 = (s_2 - s'_2)/(c - c') \mod q$, όπου w_i ο λογάριθμος του h_i ως προς το g_i, και q η (κοινή) τάξη των g_i. Η συνθήκη που θέλουμε να προσθέσουμε είναι $w_1 = w_2 \mod q$.

Ισοδύναμα, θέλουμε να ισχύει $s_1 - s'_1 = s_2 - s'_2$ ή σε μία πιο χρήσιμη μορφή $s_1 - s_2 = s'_1 - s'_2$. Στην πρώτη μορφή έχουμε μια ισότητα ανάμεσα σε διαφορές τιμών που ανήκουν σε διαφορετικές εκτελέσεις του πρωτοκόλου, οπότε δεν είναι προφανές τι αλλαγές χρειάζεται να κάνουμε. Στη δεύτερη, το ζητούμενο είναι η διαφορά των s_i στην μία εκτέλεση να είναι ίση με τη διαφορά τους στη δεύτερη. Ένας απλός τρόπος[2] να το επιτύχουμε αυτό είναι να ζητήσουμε η διαφορά αυτή σε κάθε εκτέλεση να είναι μηδενική, δηλαδή $s_1 = s_2 = s$. Επειδη γνωρίζουμε ότι στο πρωτόκολο του Schnorr ισχύει $s = c \cdot w + t$, η αλλαγή που κάναμε στα s_i, συνεπάγεται ότι θα πρέπει να χρησιμοποιούμε και ίδια t_i δηλαδή $t_1 = t_2 = t$ και άρα $y_1 = g_1^t, y_2 = g_2^t$. Το πρωτόκολο που προκύπτει, παρουσιάστηκε από τους Chaum και Pedersen το 1992 στο άρθρο "Wallet Databases with Observers" (CRYPTO '92) και δίνεται παρακάτω.



[2] Αυτός δεν είναι ο μόνος τρόπος να πετύχουμε τη σταθερή διαφορά που χρειαζόμαστε, αλλά είναι μάλλον ο απλούστερος.

Ο τελικός έλεγχος του Verifier είναι εάν $g_1^s = h_1^c \cdot y_1$ και $g_2^s = h_2^c \cdot y_2$.

Ο έλεγχος για την ορθότητα, εγκυρότητα και HVZK αφήνεται ως άσκηση.

6. Αξιολογήστε την εγκυρότητα (όχι την ειδική εγκυρότητα) του παραπάνω πρωτοκόλου σε σχέση με αυτό του Schnorr.

   Λύση Η (μη ειδική) εγκυρότητα του Schnorr είναι τετριμμένη στις πιο πολλές περιπτώσεις, αφού για κάθε στοιχείο της ομάδας που παράγει ένα g έχει εξ ορισμού διακριτό λογάριθμο ως προς αυτό. Το μη-τετριμμένο δεν είναι η ύπαρξη του διακριτού λογαρίθμου αλλά η γνώση του. Στην περίπτωση του παραπάνω πρωτοκόλου (Chaum-Pedersen), ακόμα και η απλή εγκυρότητα έχει νόημα αφού δεν είναι προφανές ότι οι διακριτοί λογάριθμοι διαφορετικών στοιχείων ως προς διαφορετικές βάσεις είναι αναγκαστικά ίσοι.

7. Εξηγήστε πως μπορούμε να δείξουμε ότι ένα κρυπτογραφημένο μήνυμα $c = \langle u, v\rangle$ με ElGamal περιέχει ως μήνυμα είτε την τιμή m_1 είτε την τιμή m_2, χωρίς να δώσουμε άλλη πληροφορία για αυτό.

   Λύση Θα αναπτύξουμε ένα τέτοιο πρωτόκολο σε 3 βήματα.

   (α΄) Ένα πρωτόκολο για να αποδείξουμε ότι ένα κρυπτογραφημένο μήνυμα $c = \langle u, v\rangle$ με ElGamal περιέχει ως μήνυμα το ουδέτερο στοιχείο g^0. Η λύση είναι το πρωτόκολο των Chaum και Pedersen από το προηγούμενο ερώτημα. Για ένα τέτοιο μήνυμα ισχύει ότι $u = g^r, v = h^r$, άρα ο ΔΛ του u ως προς g είναι ίσος με αυτόν του v ως προς το δημόσιο κλειδί h. Για να τρέξουμε το πρωτόκολο ο prover αρκεί να ξέρει το r, αφού το ιδιωτικό κλειδί δεν συμμετέχει.

   (β΄) Ένα πρωτόκολο για να αποδείξουμε ότι ένα κρυπτογραφημένο μήνυμα $c = \langle u, v\rangle$ με ElGamal περιέχει ως μήνυμα ένα συγκεκριμένο στοιχείο m. Αν το $c = \langle u, v\rangle$ περιέχει το m, τότε το $c' = \langle u, v/m\rangle$ περιέχει το ουδέτερο στοιχείο, και άρα χρησιμοποιούμε το προηγούμενο υποερώτημα.

   (γ΄) Για να δείξουμε το ζητούμενο, χρησιμοποιούμε την λογική διάζευξη δύο Σ-πρωτοκόλων από τις σημειώσεις μας.