

Key Exchange, ElGamal

1. Δίνεται το παρακάτω σχήμα ανταλλαγής κλειδιού¹:

(α') Η Αλίκη επιλέγει τυχαία $k, r \leftarrow \{0, 1\}^n$ και στέλνει στο Βασίλη την τιμή $s := k \oplus r$.

(β') Ο Βασίλης επιλέγει τυχαίο $t \leftarrow \{0, 1\}^n$ και στέλνει στην Αλίκη $u := s \oplus t$.

(γ') Η Αλίκη υπολογίζει την τιμή $w := u \oplus r$ και τη στέλνει στο Βασίλη.

(δ') Η Αλίκη χρησιμοποιεί την τιμή k και ο Βασίλης την τιμή $w \oplus t$.

Να εξετάσετε το παραπάνω σχήμα ως προς την ορθότητα και την ασφάλεια.

Λύση Η ορθότητα ισχύει με έλεγχο των πράξεων. Δεν είναι όμως ασφαλές. Υπολογίστε το $s \oplus u \oplus w$.

2. [Λύθηκε στην τάξη] Εξετάστε τι συμβαίνει αν πολλαπλασιάσουμε κατά συντεταγμένη δύο κρυπτοκειμένα 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).

3. Δίνεται ένα κρυπτομήνυμα ElGamal $c = (U, V) \in \mathbb{G}^2$, οι παράμετροι (\mathbb{G}, g, q) της αντίστοιχης ομάδας, και ένα δημόσιο κλειδί $h := g^x$ (το x καθαυτό δεν δίνεται). Περιγράψτε πως μπορούμε να κατακευάσουμε ένα κρυπτομήνυμα $c' \neq c$ με την ιδιότητα $\text{Dec}_x c' = \text{Dec}_x c$.

Λύση

Έστω $c = (u, v)$. Από την παραπάνω άσκηση, αρκεί να πολλαπλασιάσουμε κατά συντεταγμένη το c με ένα κρυπτομήνυμα το οποίο περιέχει οποιοδήποτε στοιχείο εκτός από το ουδέτερο. Π.χ. έστω $c^* = (g^0, h^0 g)$, το οποίο είναι κρυπτογράφηση του $m = g$ με $r = 0$. Τότε, το $c' = c \cdot c^*$ έχει σίγουρα διαφορετική αποκρυπτογράφηση από το c .

4. Δίνονται οι παράμετροι: $g \equiv 2 \pmod{23}$, $\mathbb{G} = \mathbb{Z}_{23}^* \cap \langle g \rangle$, $q = 11$. Ακολουθήστε τη διαδικασία κατασκευής ζευγους κλειδιών και κατασκευάστε ένα ζεύγος x, h . Κρυπτογραφήστε το μήνυμα $m \equiv 6 \pmod{23}$ με randomness της επιλογής² σας, και κατόπιν αποκρυπτογραφήστε το.

Παράδειγμα

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

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

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

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

Άρα $c = (U, V) = (13, 3)$.

¹Άσκηση 9.3 (1η έκδοση)/ 10.4 (2η έκδοση) από το Katz & Lindell

²Τετριμμένες επιλογές ανατρούν το νόημα της άσκησης.

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

5. Τι συμβαίνει αν στο κρυπτοσύστημα ElGamal επιλέξουμε ως \mathbb{G} ομάδα σύνθετης τάξης, συγκεκριμένα 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. Συγκεκριμένα, 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 ποιο από τα δύο κρυπτογραφήθηκε.

6. Έστω ένα σχήμα κρυπτογράφησης (Kgen, Enc, Dec), με χώρο μηνυμάτων \mathcal{M} , ασφαλές ως προς IND-CPA. Κατασκευάστε ένα σχήμα κρυπτογράφησης με χώρο μηνυμάτων $\mathcal{M}' := \mathcal{M}^2$. Μπορείτε να είστε σύντομοι στην κατασκευή και την ορθότητα, περιγράψτε όμως αναλυτικά την απόδειξη της ασφαλείας του.

Λύση

Για ευκολία, και αποφυγή διπλών δεικτών, συμβολίζουμε τα στοιχεία του νέου χώρου μηνυμάτων \mathcal{M}^2 ως $(m, k) \in \mathcal{M}^2$ δηλαδή $m, k \in \mathcal{M}$. Η κατασκευή είναι απλή, κατασκευάζουμε το νέο σύστημα ως εξής:

$\text{Kgen}_2 \rightarrow (pk, sk)$: Όπως η Kgen.

$\text{Enc}_2(pk, m, k) \rightarrow (c_m, c_k)$: Return ($\text{Enc}(pk, m), \text{Enc}(pk, k)$)

$\text{Dec}_2(sk, c_m, c_k) \rightarrow (m, k)$: Return ($\text{Dec}(sk, c_m), \text{Dec}(sk, c_k)$)

Η ορθότητα του $(\text{Kgen}_2, \text{Enc}_2, \text{Dec}_2)$ προκύπτει μετά από έλεγχο της κατασκευής, αφού το σχήμα $(\text{Kgen}, \text{Enc}, \text{Dec})$ είναι ορθό.

Για την ασφάλεια του συστήματος ως προς IND-CPA ουσιαστικά πρέπει, ακολουθώντας τον ορισμό να δείξουμε ότι ένα ζεύγος $(\text{Enc}(pk, m_0), \text{Enc}(pk, k_0))$ είναι όμοια για τον αντίπαλο με ένα ζεύγος $(\text{Enc}(pk, m_1), \text{Enc}(pk, k_1))$. Η τεχνική δυσκολία είναι ότι δεν έχουμε άμεσο τρόπο να καταλήξουμε σε άτοπο εάν κάποιος αντίπαλος τα ξεχωρίσει. Διαισθητικά, η ασφάλεια IND-CPA του $(\text{Kgen}, \text{Enc}, \text{Dec})$, μας εγγυάται ότι το μεμονωμένο $\text{Enc}(pk, m_0)$ είναι όμοιο με το $\text{Enc}(pk, m_1)$, και αντίστοιχα το $\text{Enc}(pk, k_0)$ με το $\text{Enc}(pk, k_1)$, αλλά δεν μας δίνει πληροφορία για τα ζευγάρια που μας ενδιαφέρουν.

Θα πρέπει λοιπόν να «χτίσουμε» ένα συλλογισμό που χρησιμοποιεί την ομοιότητα των επιμέρους στοιχείων για να αποδείξουμε την ομοιότητα των ζευγαριών. Η τεχνική αυτή μοιάζει με την τριγωνική ανισότητα, και στη βιβλιογραφία είναι γνωστή ως «Υβριδικό επιχείρημα» (Hybrid Argument). Θα δείξουμε λοιπόν ότι είναι δύσκολο για κάποιον αντίπαλο να ξεχωρίσει (1) το ζευγάρι $(\text{Enc}(pk, m_0), \text{Enc}(pk, k_0))$ από το $(\text{Enc}(pk, m_0), \text{Enc}(pk, k_1))$ και (2) το $(\text{Enc}(pk, m_0), \text{Enc}(pk, k_1))$ από το $(\text{Enc}(pk, m_1), \text{Enc}(pk, k_1))$. Και στα δύο βήματα του συλλογισμού, το ένα ζεύγος από το άλλο διαφέρει μόνο σε μία συντεταγμένη, άρα είναι εύκολο να στηρίζουμε το συλλογισμό μας στην IND-CPA ασφάλεια του $(\text{Kgen}, \text{Enc}, \text{Dec})$. Αναλυτικά, η απόδειξη δίνεται παρακάτω:

Βάση Από τον ορισμό της ασφάλειας IND-CPA, μας ενδιαφέρει η πιθανότητα $P_0 = \text{Prob}[\text{Game}_{\text{IND-CPA}}^A(1^\lambda)]$ να είναι το πολύ $\frac{1}{2} + \epsilon$ για κάποιο ϵ αμελητέο.

Δεύτερο Βήμα Ορίζουμε $P_1 = \text{Prob}[\text{Game}_{\text{IND-CPA}^*}^A(1^\lambda)]$, όπου στο παιχνίδι IND-CPA^* αντί τα ζεύγη $(\text{Enc}(pk, m_0), \text{Enc}(pk, k_0))$ και $(\text{Enc}(pk, m_1), \text{Enc}(pk, k_1))$, δίνουμε στον αντίπαλο $(\text{Enc}(pk, m_0), \text{Enc}(pk, k_0))$ όταν $b = 0$ και $(\text{Enc}(pk, m_0), \text{Enc}(pk, k_1))$ όταν $b = 1$. Θέτουμε $\epsilon_1 = |P_0 - P_1|$. Γράφουμε ως \mathcal{A}_2 το 2ο στάδιο του \mathcal{A} , και για συντομία γράφουμε το $(\text{Enc}(pk, m_i), \text{Enc}(pk, k_j))$ ως C_{ij} . Έχουμε:

$$P_0 = \frac{1}{2}P[\mathcal{A}_2(C_{00}) = 0] + \frac{1}{2}P[\mathcal{A}_2(C_{11}) = 1] \quad (1)$$

$$P_1 = \frac{1}{2}P[\mathcal{A}_2(C_{00}) = 0] + \frac{1}{2}P[\mathcal{A}_2(C_{01}) = 1] \quad (2)$$

$$\epsilon_1 = \frac{1}{2}P[\mathcal{A}_2(C_{11}) = 1] - \frac{1}{2}P[\mathcal{A}_2(C_{01}) = 1] \quad (3)$$

$$\epsilon_1 = \frac{1}{2}P[\mathcal{A}_2(C_{11}) = 1] + \frac{1}{2}P[\mathcal{A}_2(C_{01}) = 0] - \frac{1}{2} \quad (4)$$

Απόδειξη πρώτου βήματος Ισχυριζόμαστε ότι το $|\epsilon_1|$ πρέπει να είναι αμελητέο. Αν όχι, μπορούμε να κατασκευάσουμε αντίπαλο \mathcal{B} απέναντι στην IND-CPA ασφάλεια του αρχικού σχήματος. Ο \mathcal{B} παίρνει ένα δημόσιο κλειδί pk και κατόπιν καλεί τον \mathcal{A} και του στέλνει το pk . Ο \mathcal{A} απαντά με δύο ζευγάρια m_0, k_0, m_1, k_1 . Ο \mathcal{B} στέλνει στο πείραμα τα m_0, m_1 , λαμβάνει το $c_b = \text{Enc}(pk, m_b)$, και προωθεί στον \mathcal{A} το κρυπτομήνυμα $(c_b, \text{Enc}(pk, k_1))$. Ο \mathcal{A} απαντά με b^* το οποίο ο \mathcal{B} προωθεί στο πείραμα του. Έστω P' η πιθανότητα επιτυχίας του \mathcal{B} . Παρατηρούμε ότι ο \mathcal{B} επιτυγχάνει στο πείραμα σε δύο περιπτώσεις: όταν δώσει στον \mathcal{A} είσοδο $(c_1, \text{Enc}(pk, k_1))$ και ο \mathcal{A} επιστρέψει 1, ή όταν δώσει είσοδο $(c_0, \text{Enc}(pk, k_1))$ και ο \mathcal{A} επιστρέψει 0. Δηλαδή, για την πιθανότητα επιτυχίας του \mathcal{B} έχουμε:

$$P' = \frac{1}{2}P[\mathcal{A}_2(C_{11}) = 1] + \frac{1}{2}P[\mathcal{A}_2(C_{01}) = 0] \quad (5)$$

$$P' = \frac{1}{2} + \epsilon_1 \quad \text{—Αντικαθιστούμε από την (4)} \quad (6)$$

Άρα, είτε ο \mathcal{B} παραβιάζει την IND-CPA ασφάλεια του αρχικού σχήματος, είτε το ϵ_1 είναι αμελητέο.

Δεύτερο Βήμα Ορίζουμε $P_2 = \text{Prob}[\text{Game}_{\text{IND-CPA}^{**}}^A(1^\lambda)]$, όπου στο παιχνίδι IND-CPA^{**} αντί τα ζεύγη $(\text{Enc}(pk, m_0), \text{Enc}(pk, k_0))$ και $(\text{Enc}(pk, m_1), \text{Enc}(pk, k_1))$, δίνουμε στον αντίπαλο $(\text{Enc}(pk, m_0), \text{Enc}(pk, k_0))$ όταν $b = 0$ και $(\text{Enc}(pk, m_0), \text{Enc}(pk, k_0))$ όταν $b = 1$. Θέτουμε $\epsilon_2 = |P_1 - P_2|$. Γράφουμε ως \mathcal{A}_2 το 2ο στάδιο του \mathcal{A} , και για συντομία γράφουμε το $(\text{Enc}(pk, m_i), \text{Enc}(pk, k_j))$ ως C_{ij} . Έχουμε:

$$P_1 = \frac{1}{2}P[\mathcal{A}_2(C_{00}) = 0] + \frac{1}{2}P[\mathcal{A}_2(C_{01}) = 1] \quad (7)$$

$$P_2 = \frac{1}{2}P[\mathcal{A}_2(C_{00}) = 0] + \frac{1}{2}P[\mathcal{A}_2(C_{00}) = 1] \quad (8)$$

$$\epsilon_2 = \frac{1}{2}P[\mathcal{A}_2(C_{01}) = 1] - \frac{1}{2}P[\mathcal{A}_2(C_{00}) = 1] \quad (9)$$

$$\epsilon_2 = \frac{1}{2}P[\mathcal{A}_2(C_{01}) = 1] + \frac{1}{2}P[\mathcal{A}_2(C_{00}) = 0] - \frac{1}{2} \quad (10)$$

Αντίστοιχα με παραπάνω, έχουμε ότι ϵ_2 αμελητέο.

Τέλος Από τον ορισμό των ϵ_1, ϵ_2 , έχουμε ότι $|P_0 - P_2| \leq \epsilon_1 + \epsilon_2$.

Επιπλέον, παρατηρούμε ότι στο P_2 , η είσοδος του \mathcal{A} είναι ανεξάρτητη του b , άρα $P_2 = \frac{1}{2}$.

Οπότε, έχουμε $|P_0 - 1/2| \leq \epsilon_1 + \epsilon_2$. Ισοδύναμα, και αντικαθιστώντας το $\epsilon_1 + \epsilon_2 = \epsilon$ προκύπτει ότι $P_0 \leq 1/2 + \epsilon$

Που είναι και το ζητούμενο.