1 Κατανέμοντας την Εμπιστοσύνη

1.1 Διαμοιρασμός Μυστικού

Σε ενα ***σχήμα διαμοιρασμού μυστικού (secret sharing scheme)***, ένα σύνολο παικτών κατέχει κομμάτια πληροφορίες που συνδυασμένα μεταξύ τους μας δίνουν ένα κοινό "μυστικό". Αν ο αριθμός των παικτών που συμμετέχει στον υπολογισμό δεν ξεπερνά το καώφλι, τότε δεν μπορεί να πάρει καμία πληροοφορία για το μυστικό.

Θεωρούμε ένα από παράδειγμα όπου ο dealer D θέλει να κατανήμει ένα μυστικό $S \in \mathbb{Z}_q$ σε ένα σύνολο παικτων P_i για $i = 1, \ldots, n$. Ο dealer διελέγει τυχαία $n-1$ αριθμούς $s_1, \ldots, s_{n-1} \xleftarrow{r} \mathbb{Z}_q$ και θέτει τον n-οστό από αυτούς ως $s_n = S - s_1 - \ldots - s_{n-1} \bmod q$. Ο D κατανέμει το s_i στο P_i το οποίο θα αποτελεί το κομμάτι του.

Στην ειδική περίπτωση των $n = 2$ παικτών, έχουμε πως $s_1 + s_2 = S$, όπου $s_1 \xleftarrow{r} \mathbb{Z}_q$ και $s_2 = S - s_1 \bmod q$. Οι πιθανοτικές κατανομές των s_1, s_2 είναι ίδιες: τα s_1 και s_2 διελέγονται τυχαία από το $\mathbb{Z}_q$ έτσι ώστε ούτε ο P_1 ούτε ο P_2 να μπορεί να ανακτήσει S χωρίς την βοήθεια του άλλου παίκτη. Με παρόμοιο τρόπο μπορούμε να δείξουμε πως κάθε σύνολο $n-1$ παικτών δεν μπορούν να ανακτήσουν ένα μυστικό που μοιράζονται n παίκτες.

1.2 Σχήμα Διαμοιρασμού Μυστικού Shamir

Ορίζουμε τα $p(X) = a_0 + a_1 X + \cdots + a_{t-1} X^{t-1}$ για κάθε $a_i \in \mathbb{Z}_q$. Αν γνωρίζουμε t σημεία $(z_0, y_0), (z_1, y_1), \ldots, (z_{t-1}, y_{t-1})$, με $y_i = p(z_i)$, τότε κατασκευάζουμε το σύστημα

$$\begin{bmatrix} 1 & z_0 & \cdots & z_0^{t-1} \\ 1 & z_1 & \cdots & z_1^{t-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & z_{t-1} & \cdots & z_{t-1}^{t-1} \end{bmatrix} \begin{bmatrix} a_0 \\ a_1 \\ \vdots \\ a_{t-1} \end{bmatrix} \equiv \begin{bmatrix} y_0 \\ y_1 \\ \vdots \\ y_{t-1} \end{bmatrix} \bmod q. \tag{1}$$

Συμβολίζετουμε την (1) με $ZA \equiv Y \bmod q$. Αν η ορίζουσα του Z είναι μη μηδενική, μπορούμε να λύσουμε το $A = Z^{-1}Y$ και να βρούμε τους συντελεστές του $p(X)$ χρησιμοποιώντας την παρεμβολή του Lagrange. Αυτή η μέθοδος είναι η βάση του ***σχήματος διαμοιρασμού μυστικού Shamir (Shamir's secret sharing scheme)***:

Υποθέτουμε πως έχουμε n παίκτες και ένα κατώφλι μυστικού t, δηλαδή λιγότεροι από t παίκτες δεν μπορούν να μάθουν κάτι για το μυστικό. Ο dealer D ορίζετι ένα $p(X)$ τέτοιο ώστε ο σταθερός όρος $a_0 = p(0)$ να είναι το μυστικό και όλοι οι άλλοι συντελεστές να έχουν διαλεχτεί τυχαία: $a_1, \ldots a_{t-1} \xleftarrow{r} \mathbb{Z}_q$. Ο D κατανέμει τα $s_i = p(i)$ σε κάθε παίκτη P_i για $i = 1, \ldots, n$.

Όταν t παίκτες συναντιώνται, μπορούν να λύσουν ένα σύστημα παρόμοιο με το (1). Θα συμβολίζουμε αυτό το σύνολο παικτών ως $\{P'_j\}$ για $j = 1, \ldots, t$, όπου κάθε ένας από τους t συμμετέχοντες παίκτες έχει το αντίστοιχο κομμάτι s'_j. Χρησιμοποιώντας την παρεμβολή του Lagrange μπορούν να πάρουν το $a_0 = \lambda_1 s'_1 + \ldots + \lambda_t s'_t$, όπου κάθε λ_j είναι ένα δημόσια κατασκευάσιμος συντελεστής Lagrange. Σημειώνουμε πως με αυτή τη μέθοδο, $t-1$ παίκτες δεν μπορούν να υπολογίσουν καμία πληροφορία για το a_0, ενώ t παίκτες μπορούν να ανακτήσουν το πλήρες μυστικό.

1.3 Κατανέμοντας Ικανότητες Αποκρυπτογράφησης

Επιστρέφουμε τώρα στο σχήμα κρυπτογράφησης ElGamal με δημόσιο κλειδί $pk = \langle \langle p, m, g \rangle, h \rangle$ και μυστικό κλειδί $sk = x$ τέτοιο ώστε $h = g^x$. Χρησιμοποιώντας το σχήμα διαμοιρασμού κλειδιού, μπορούμε να διαμοιράσουμε το μυστικό κλειδί σε n παίκτες έτσι ώστε t (ή περισσότεροι) από αυτούς να μπορούν μαζί να πάρουν το x και να αποκρυπτογραφήσουν το ElGamal κρυπτογράφημα. Το μυστικό x όμως, μπορεί να χρησιμοποιηθεί όμως μια φορά: μετά την ανασκευή του είναι διαθέσιμο σε ολους τους παίκτες. Τώρα εισάγουμε την ***κρυπτογράφηση κατωφλίου***, που επιτρέπει στο x να ξαναχρησιμοποιηθεί.

¨Εστω $\langle G, H\rangle = \langle g^r, h^r M\rangle$ να είναι ένα κρυπτογράφημα ElGamal με $h = g^x$ και $x = p(0)$, όπου το $p(X)$ ορίζεται όπως στην Ενότητα 1.2. Κατανέμουμε το $s_i = p(i)$ στον i-οστό παίκτη P_i με $i = 1, \ldots, n$.

Όταν ένα σύνολο t παικτών P'_j, $j = 1, \ldots, t$, αποφασίζει να αποκρυπτογραφήσει το $\langle G, H\rangle$, τότε κάθε P'_j δημοσιεύει $G_j = G^{s'_j}$.

P'_1	P'_2	$\cdots$	P'_t
s'_1	s'_2	$\cdots$	s'_t
G_1	G_2	$\cdots$	G_t

Χρησμοποιώντας τους συντελεστές Lagrange, οι t παίκτες υπολογίζουν

$$\begin{aligned} G_1^{\lambda_1} G_2^{\lambda_2} \cdots G_t^{\lambda_t} &= G^{\lambda_1 s'_1} \cdots G^{\lambda_t s'_t} \\ &= G^{p(0)} \\ &= G^x \\ &= g^{rx} \\ &= h^r \end{aligned}$$

Συνεπάγεται πως το απλό μήνυμα M μπορεί να ανακτηθεί ως

$$M = H / G_1^{\lambda_1} G_2^{\lambda_2} \cdots G_t^{\lambda_t}.$$

Εφαρμογές στο E-Voting

Definition 1.3.1. Δεδομένων δύο ομάδων $(X, +)$ και $(Y, \cdot)$[1], ενας ***ομομορφισμός ομάδας (group homomorphism)*** είναι μια συνάρτηση $\varphi\colon X \longrightarrow Y$ τέτοια ώστε για κάθε $\alpha, \beta \in X$, ισχύει πως

$$\varphi(\alpha + \beta) = \varphi(\alpha) \cdot \varphi(\beta).$$

Αυτό συνεπάγεται πως ο φ πρέπει να διατηρεί τα μοναδιαία στοιχεία και τους αντίστροφους.

Ορίζουμε ως $(X, +)$ την ομάδα απλών μυνημάτων και ως $(Y, \cdot)$ την ομάδα των κρυπτογραφημάτων όπου $\cdot$ κάποια πράξη ομάδας πάνω σε κρυπτογραφήματα. Δεδομένων $C_1, C_2 \in Y$ τέτοιων ώστε $C_1 = \mathcal{E}(pk, M_1)$ and $C_2 = \mathcal{E}(pk, M_2)$ for $M_1, M_2 \in X$, θα ονομάζουμε ως $\mathcal{E}$ a ***ομομορφική συνάρτηση κρυπτογράφησης (homomorphic encryption function)*** μια συνάρτηση ποθ ικανοποιεί

$$\mathcal{E}(pk, M_1 + M_2) \approx C_1 \cdot C_2{}^2.$$

Σαν παράδειγμα, θεωρούμε την κρυπτογράφηση ElGamal. Έστω $\mathbb{Z}_m$ να είναι μια ομάδα απλών μηνυμάτων (κάτω από πρόσθεση υπόλοιπο m) και έστω $\langle \mathbb{Z}_p^*, \mathbb{Z}_p^*\rangle$ να είναι μια ομάδα κρυπτογραφημάτων για κάποιο πρώτο p. Δεδομένου οποιουδήποτε κρυπτογραφήματος έχουμε $\langle G, H\rangle = \langle g^r, h^{r+M}\rangle$ με $M \in \mathbb{Z}_m$. Για να αποκρυπτογραφήσουμε το $\langle G, H\rangle$, υπολογίζουμε το $H/G^x = h^M$ και ψάχνουμε όλες τις δυνατές επιλογές για το $\{h^{M_1}, h^{M_2}, \ldots, h^{M_m}\}$. Αυτή η συνάρτηση κρυπτογράφησης ικανοποιεί τις επιθυμητές ιδιότητες ομομορφισμού, αλλά είναι αποτελεσματική μόνο για μικρά m.

Χρησιμοποιώντας της ιδιότητες ομομορφισμού του ElGama μπορούμε να δημιουργήσουμε ένα κρυπτογραφικό σύστημα κατωφλίου για ένα σύστημα ηλεκτρονικής ψηφοφόρησης με n ψηφοφόρους. Υποθέτουμε πως ο i-οστός ψηφοφόρος μας πιστοποεί την ταυτότητά του και καταθέτει $\langle G(i), H(i)\rangle = \langle g^{r_i}, h^{r_i + M_i}\rangle$, όπου $M_i \in \{0, 1\}$ (`No`=0, `Yes`=1). Έστω $A = \sum r_i$ and $B = \sum M_i$ for $i = 1, \ldots, n$. Παρατειρούμε πως το

$$\left\langle \prod_{i=1}^{n} G(i), \prod_{i=1}^{n} H(i) \right\rangle = \langle g^A, h^A h^B\rangle$$

[1]Προς διασαφηνιση, γράφουμε το X χρημσιοποιώντας προσθετικό συμβολισμό και το Y χρησιμοποιώντας πολλαπλασιαστικό συμβολισμό, παρότι και οι δύο πράξεις στα X και Y μπορεί να διαφέρουν αρκετά από τις συνήθεις αντίστοιχες πράξεις.

[2]Το σύμβολο $\approx$ αναπαριστά την ταυτοτική κατανομή

είναι ένα κρυπτογράφημα που κρυπτογραφεί τον αριθμό των ψηφοφόρων που απάντησαν `N` : $B = \sum_{i=1}^{n} M_i$.

Η ερώτηση είναι αν το $\langle G(i), H(i)\rangle$ είναι ένα έγκυρο κρυπτογράφημα για το $M_i \in \{0, 1\}$. Σημειώνουμε πως αν το $M_i = 0$, τότε $\log_g h = \log_{G(j)} H(j)$ και αν $M_i = 1$, τότε $\log_g h = \log_{G(j)} H(j)/h$. Αφού τα $g, h, G(i), H(i)$ είναι δημόσια πληροφορία, ο V_i μπορεί να αποδειξει πως γνωρίζει έναν από τους δύο διακριτούς λογαρίθμους χρησιμοποιώντας την διάζευξη των αποδείξεων μηδενικής γνώσης.

Γυρνάμε την προσοχη μας στον (δημόσια) επαληθεύσιμο διαμοιρασμό μυστικού και διαμοιρασμό μυστικού χωρίς τον Dealer, στα οποία εφαρμόζονται ειδικές μορφές του διαμοιρασμού μυστικού.

1.4 Δημόσια Επαληθεύσιμος Διαμοιρασμός Μυστικού

Σε ένα σύστημα αποκρυπτογραφησης κατωφλίου, προβλήματα παρουσιάζονται όταν ένας από τους t συνεισφέροντες παίκτες δημοσιεύει εσφαλμένα το κομμάτι του. Οι $t-1$ τίμιοι παικτες μποκάρονται από το μυστικό ενώ ο κακόβουλος παίκτης μπορεί να το ανασκευάσει. Για να το αποφύγουμε αυτο, βάζουμε μια τρίτη μεριά ή ένα δικαστή στον οποίον κάθε παίκτης πρέπει να αποδεικνύει την εγκυρότητα του κομματιού που ανακοινώνει. Πρώτα θα παρουσιάσουμε μια λύση, η οποία όμως εξασθενίζει την ασφάλεια του σχηματος.

Υποθέτουμε πως ο dealer δημοσιεύει τα

$$\langle g^{a_0}, g^{a_1}, \ldots, g^{a_{t-1}}\rangle = \langle V_0, V_1, \ldots, V_{t-1}\rangle.$$

Αν το s_i αντιστοιχίζεται στον i-οστο παίκτη, παρατηρούμε πως

$$\begin{aligned} V_0 V_1^i \cdots V_{t-1}^{i^{t-1}} &= g^{a_0} g^{a_1 i} \cdots g^{a_{t-1} i^{t-1}} \\ &= g^{p(i)} \\ &= g^{s_i}. \end{aligned}$$

Συνεπώς ο i-οστός παίκτης μπορεί να παρουσιάσει μια τιμή που μπορεί να επικυρωθει από έναν δικαστή. Αυτό λύνει το πρόβλημα αλλά όπως είπαμε εξασθενίζει την ασφάλεια αφού ένας αντίπαλος μπορεί παρόμοια να κατασκευάσει μια τιμή και να την παρουσιάσει στον δικαστή.

Μια καλύτερη λύση χρησιμοποιεί αποδείξεις μηδενικής γνώσης. Σημειώνουμε πως τα G, g, g^{s_i} είναι δημόσια και πως ο i-οστός παίκτης ισχυρίζεται ότι $G_i = G^{s_i}$. Αυτό μπορεί κανείς να το επικυρώσει ελέγχοντας ότι $\log_G G_i = \log_g g^{s_i}$. Για να αποδείξει πως είναι τίμιος, ο i-στός παίκτης δίνει μια απόδειξη μηδενικής γνώσης για το διακριτό λογάριθμο όπως συζητήθηκε σε προηγούμενες ενότητες.

1.5 Κατανέμοντας τον Dealer

Στα προηγούμενα σχήματα είχαμε ένα σημαντικό πρόβλημα πως ο Dealer γνωρίζει το μυστικό, επιπρόσθετα με το κομμάτι του κάθε παίκτη, κάτι το οπόιο θα θέλαμε να το . Για να το αποφύγουμε θα πρεπει μοιράσουμε τις υποχρεωσεις του Dealer στους παίκτες.

Έστω πως ο P_i διαλέγει το S_i ως το μυστικό του. Ο P_i χρησιμοποιεί το προσωπικό του πολυώνυμο $p_i(X) = a_{i,0} + a_{i,1}X + \ldots + a_{i,t-1}X^{t-1}$ για να υπολογίσει το $S_{i,j} = p_i(j)$. Δίνει το $S_{i,j}$ στον P_j ως το j-στό κομμάτι του S_i. Ο P_i τότε δημοσιεύει τα $V_{i,0}, V_{i,1}, \ldots, V_{i,t-1}$.

Ο j-στός παίκτης συλλέγει τα $S_{1,j}, S_{2,j}, \ldots, S_{n,j}$ από τους άλλους παίκτες και υπολογιζει το κομμάτι του ως $s_j = \sum_{i=1}^{n} S_{i,j}$. Το διαμοιραζόμενο μυστικό είναι το $\sum_{i=1}^{n} p_i(0)$ και οι τιμές επαλήθευσεις είναι οι $V_k = \prod_{i=1}^{n} V_{i,k}$ for $k = 0, \ldots, t-1$. Σημειώνουμε καμία οντότητα που δεν συνεργάζεται δεν ξέρει το μυστικό και πως μπορεί να ανακτηθεί από κάθε προσπάθεια t χρηστών.

Notes by S. Pehlivanoglu, J. Todd, & H.S. Zhou