Schémas de partage de secret basés sur les codes correcteurs d'erreurs

Jean Gasnier, encadré par Alexis Bonnecaze

02/09/2021

Sommaire

Prérequis

- Notions d'entropie pour la théorie de l'information : définition, entropie conditionnelle.
- Notions de codes correcteurs : notations usuelles, matrices génératrices.
- Notions d'algèbre et d'aléatoire de base : algèbre linéaire, interpolation de Lagrange, variables aléatoires, indépendance.
- Notions de sécurité en cryptographie : modèle adversaire.

Sommaire

Contexte

On se donne :

- un ensemble de n participants $P = [\![1, n]\!]$.
- un tiers de confiance (ou croupier) p_0.
- un entier naturel k inférieur à n.
- un corps fini $\mathbb{F}_q$ où $q \geqslant n + 1$.
- un secret s tiré aléatoirement dans $\mathbb{F}_q$ suivant la loi uniforme.

Le croupier va distribuer des informations aux participants.

On demande comment faire en sorte que, après distribution, tout groupe de k participants puisse retrouver le secret, en garantissant que tout groupe de moins de k participants soit incapable d'obtenir la moindre connaissance sur le secret.

Un schéma de partage de secret (ou SSS) est un protocole qui résout ce problème.

Cas $k = n$: une mauvaise idée

On suppose momentanément que $k = n$ et qu'on peut représenter notre secret par un mot de n bits. Une idée serait de distribuer à chaque participant un bit de la clé.

Cette idée ne fonctionne pas car elle n'est pas sécurisée. Si il manque un seul participant, seul un bit de la clé demeure inconnu, et donc il n'existe que 2 possibilités pour la clé, au lieu de 2^n.

Cas $k = n$: cadenas et clé

On suppose momentanément que $k = n$.

Lemme :

Soit S une variable aléatoire à valeurs dans $\mathbb{F}_q$, et U une variable aléatoire uniforme sur $\mathbb{F}_q$, indépendante de S. Alors $S + U$ suit une loi uniforme sur $\mathbb{F}_q$, indépendante de S.

Le tiers de confiance p_0 tire aléatoirement des éléments $a_1, ..., a_n$ de F_q, appelés fragments. Il divulgue publiquement $s + a_1 + ... + a_n$ et envoie secrètement à chaque participant i le fragment a_i.

Cette idée est généralisable aux cas $k \neq n$, mais demande aux participants de conserver beaucoup d'information.

Le schéma de partage de secret de Shamir

Shamir fait le lien entre le problème et la proposition suivante :

Proposition

Soit $\alpha_1, ..., \alpha_k \in \mathbb{F}_q$ distincts, et $\beta_1, ..., \beta_k \in \mathbb{F}_q$. Il existe un unique polynôme Q de degré inférieur à $k-1$ de $\mathbb{F}_q[X]$ tel que $Q(\alpha_i) = \beta_i$.

Si on connait k évaluations d'un polynôme de degré inférieur à $k-1$ on peut retrouver le polynôme cherché, et son coefficient constant. Si on connait $k-1$ évaluations d'un polynôme (en un élément non nul), pour tout $\alpha \in \mathbb{F}_q$, il existe un unique polynôme candidat de coefficient constant α, donc on ne connait pas son coefficient constant.

Le schéma de partage de secret de Shamir

Le tiers de confiance p_0 choisit publiquement $\alpha_1, ..., \alpha_n \in \mathbb{F}_q^\times$, et choisit aléatoirement le secret s et $c_1, ..., c_{k-1} \in \mathbb{F}_q$ pour construire un polynôme secret :

$$Q = s + \sum_{j=1}^{k-1} c_j X^j$$

Ensuite, p_0 envoie au participant i le fragment $s_i = Q(\alpha_i)$.

Un groupe de k participants au moins peut retrouver le polynôme Q et le secret par l'interpolation de Lagrange.

Sommaire

Structure d'accès

Définition

On appelle **une structure d'accès sur** P une paire (Γ, Δ) où $\Gamma, \Delta \subset 2^P$ sont des ensembles non vides de parties de P disjoints et tels que :

$\forall A \in \Gamma, \forall A' \in 2^P$, si $A \subset A'$ alors $A' \in \Gamma$.

$\forall B \in \Delta, \forall B' \in 2^P$, si $B' \subset B$ alors $B' \in \Delta$.

On appelle les éléments de Γ les groupes **qualifiés** et ceux de Δ les groupes **interdits**.

Structure d'accès

Définition

On dit qu'une structure d'accès est **complète** si $\Gamma = 2^P \setminus \Delta$.

Définition

On appelle **structure d'accès à k-seuil** si
$\Gamma = \{A \in 2^P | \text{card}(A) \geqslant k\}$ et $\Delta = \{B \in 2^P | \text{card}(B) \leqslant k-1\}$.
C'est une structure complète.

La structure d'accès de l'exemple introductif est une structure à seuil.

Modèle de sécurité

- On suppose qu'il existe un canal sécurisé entre le croupier et chaque participant, et entre tous les participants. On suppose que les participants et le croupier disposent d'un générateur aléatoire sécurisé. (modèle *secure channel*)
- On suppose que les participants suivent le protocole (ne sont pas **corrompus**) et que l'ensemble des participants adversaires (dits **curieux**) est toujours un élément de Δ. (modèle *mixt adversary*)

SSS

Définition

Un **schéma de partage de secrets (SSS)** Σ sur $Q = P \cup \{p_0\}$ est une collection $(S_i)_{i \in Q}$ de variables aléatoires discrètes telle que S_{p_0} est non constante.

Pour $A \subset Q$, on note S_A le vecteur aléatoire $(S_i)_{i \in A}$.

Définition

On définit la structure d'accès d'un SSS Σ comme (Γ, Δ) où :

$$\Gamma = \{A \subset P | H(S_{p_0}|S_A) = 0\}.$$
$$\Delta = \{B \subset P | H(S_{p_0}|S_B) = H(S_{p_0})\}.$$

où $H(.|.)$ désigne l'entropie conditionnelle.

Définition équivalente

Définition

On définit la structure d'accès d'un SSS Σ comme (Γ, Δ) où :

$\Gamma = \{A \subset P | \text{il existe une fonction } f \text{ telle que } S_{p_0} = f(S_A)\}$.

$\Delta = \{B \subset P | S_{p_0} \text{ est indépendante de } S_B\}$.

Sommaire

Point de vue linéaire

On peut voir la création de fragments dans le SSS de Shamir de la manière suivante :

$$\begin{pmatrix} s & c_1 & \dots & c_{k-1} \end{pmatrix} G = \begin{pmatrix} s_1 & s_2 & \dots & s_n \end{pmatrix}$$

où $G = \begin{pmatrix} 1 & 1 & \dots & 1 \\ \alpha_1 & \alpha_2 & \dots & \alpha_n \\ \vdots & \vdots & \dots & \vdots \\ \alpha_1^{k-1} & \alpha_2^{k-1} & \dots & \alpha_n^{k-1} \end{pmatrix}$.

On peut voir G comme la matrice génératrice d'un code correcteur d'erreurs linéaire de Reed-Solomon.

SSS linéaire : construction de Shamir

Définition

Soit C un code linéaire de dimension k de $\mathbb{F}_q^n$ et de distance minimale d (on note $[n, k, d]_q$) de matrice génératrice G où $2 \leqslant k \leqslant n$. On définit le SSS basé sur la construction de Shamir généré par G pour l'ensemble de participants $P = [\![1, n]\!]$ comme :

- S_{p_0} est une variable aléatoire uniforme sur $\mathbb{F}_q$, et est le secret du tiers de confiance.
- $C_1, ..., C_{k-1}$ sont des variables aléatoires indépendantes mutuellement et avec S_{p_0}.
- $\begin{pmatrix} S_1 & ... & S_n \end{pmatrix} = \begin{pmatrix} S_{p_0} & C_1 & ... & C_{k-1} \end{pmatrix} G$ définit les fragments.

On note $g_1, ..., g_n$ les colonnes de G.

Retrouver le secret

Théorème : Structure d'accès pour la construction de Shamir

La structure d'accès du SSS basé sur la construction de Shamir généré par G est complète et l'ensemble des groupes qualifiés est :

$$\Gamma = \{A \subset P | \exists (x_1, ..., x_n) \in \mathbb{F}_q^n, \varepsilon := \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} = \sum_{i=1}^{n} x_i g_i$$

$$\text{et } \mathrm{Supp}((x_1, ..., x_n)) \subset A\}.$$

Autrement dit, ce sont les sous-ensembles A de $[\![1, n]\!]$ tels qu'il existe une relation de dépendance linéaire entre ε et les $(g_i)_{i \in A}$.

Retrouver le secret

Si il existe $x_{i_1}, ..., x_{i_l} \in \mathbb{F}_q$ tels que $\sum_{j=1}^{l} x_{i_j} g_{i_j} = \varepsilon$, on peut retrouver le secret en remarquant que

$$S_{p_0} = \begin{pmatrix} S_{p_0} & C_1 & \dots & C_{k-1} \end{pmatrix} \cdot \varepsilon = \begin{pmatrix} S_{p_0} & C_1 & \dots & C_{k-1} \end{pmatrix} \left(\sum_{j=1}^{l} x_{i_j} g_{i_j}\right)$$

$$= \sum_{i=1}^{l} x_{i_j} \begin{pmatrix} S_{p_0} & C_1 & \dots & C_{k-1} \end{pmatrix} \cdot g_{i_j} = \sum_{j=1}^{l} x_{i_j} S_{i_j}.$$

SSS linéaire : construction de Massey

Définition

Soit C un code $[n+1, k, d]_q$ de matrice génératrice $G = \begin{pmatrix} g_0 & g_1 & \dots & g_n \end{pmatrix}$. Soit $U = \begin{pmatrix} U_1 & \dots & U_k \end{pmatrix}$ une variable aléatoire de loi uniforme sur $\mathbb{F}_q^k$, alors

$$\begin{pmatrix} S_{p_0} & S_1 & \dots & S_n \end{pmatrix} = U \cdot G.$$

On dit que $(S_i)_{i \in Q}$ est le SSS basé sur la construction de Massey généré par G.

Retrouver le secret

Théorème : Structure d'accès pour la construction de Massey

Soit $(S_i)_{i \in Q}$ un SSS basé sur la construction de Massey généré par une matrice G génératrice d'un code C. Sa structure d'accès est complète, et l'ensemble des groupes qualifiés est

$$\Gamma = \{A \subset P | \exists (1, x_1, ..., x_n) \in C^{\perp}, \text{Supp}((x_1, ..., x_n)) \subset A\}.$$

Autrement dit, un groupe A est qualifié si et seulement si il existe une relation de dépendance linéaire entre g_0 et les colonnes $(g_i)_{i \in A}$.

Sommaire

Polymatroïdes

Définition

On appelle **polymatroïde** une paire (Q, f) où Q est un ensemble fini, appelé **fondation** de la polymatroïde, et $f : 2^Q \longrightarrow \mathbb{R}$, appelée **fonction de rang**, telle que :

- $f(\emptyset) = 0$.
- f est croissante : si $A \subset B \subset Q$, alors $f(A) \leqslant f(B)$.
- f est sous-modulaire : $f(A \cup B) + f(A \cap B) \leqslant f(A) + f(B)$.

Polymatroïdes entropiques

Définition

On appelle **entropie de** X le réel

$$H(X) = \sum_{x \in \mathcal{X}} p_X(x) \log(\frac{1}{p_X(x)})$$

où est log désigne le logarithme en base 2.

Définition

Soit (Q, h) une polymatroïde, on dit qu'elle est **entropique** s'il existe $(S_i)_{i \in Q}$ une famille de variables aléatoires discrètes telles que

$$h(\emptyset) = 0 \text{ et } \forall \emptyset \neq A \subset Q, h(A) = H(S_A).$$

Un SSS induit une polymatroïde entropique.

Polymatroïdes linéaire

Définition

Soit (Q, f) une polymatroïde. On dit qu'elle est $\mathbb{K}$-**linéaire** si il existe $(V_i)_{i \in Q}$ une famille d'espaces vectoriels telle que

$$\forall A \subset Q, f(A) = \dim \sum_{i \in A} V_i.$$

Théorème :

Toute polymatroïde linéaire (Q, f) pour un corps fini est multiple d'une polymatroïde entropique (Q, h) i.e. il existe une constante $c \in \mathbb{R}_+^*$ telle que $f = ch$.

Structure d'accès de polymatroïdes

Définition

Soit (Q, f) une polymatroïde, soit $X, Y \subset Q$, on définit

$$f(X|Y) = f(X \cup Y) - f(Y).$$

Définition

Soit $\mathcal{S} = (Q, f)$ une polymatroïde, et $P_0 \subset Q$ tel que $f(P_0) > 0$. On pose $P = Q \setminus P_0$. On définit la structure d'accès de $\mathcal{S}$ comme la paire (Γ, Δ) où :

$$\Gamma = \{A \subset P | f(P_0|A) = 0\}.$$

$$\Delta = \{B \subset P | f(P_0|B) = f(P_0)\}.$$

Schéma de preuve

- La structure d'accès d'un SSS est la même que celle de la polymatroïde entropique qu'il induit.
- La structure d'accès est invariante parmi les multiples d'une même polymatroïde.
- La structure d'accès d'une polymatroïde linéaire est définie par des contraintes linéaires en les V_i.
- La polymatroïde entropique induite par un SSS linéaire est multiple d'une polymatroïde linéaire où les V_i sont les $\mathrm{Vect}(g_i)$.

Sommaire

Calcul multiparti sécurisé

Le but du calcul multiparti sécurisé est de permettre à un groupe de participants de réaliser un calcul ensemble sans que de l'information non nécessaire ne fuite dans le processus.

Le protocole doit faire en sorte que tout ce passe comme si tous les participants envoyaient secrètement un paramètre à un tiers de confiance, qui ferait le calcul et enverrait le résultat nécessaire à chaque participant.

En pratique, on peut demander d'implémenter seulement l'addition et la multiplication car les fonctions arithmétiques peuvent se décomposer en composition de sommes et de produits.

Modèle de sécurité

On suppose que strictement plus de la moitié des participants sont honnêtes et qu'ils suivent tous le protocole. Il a été montré que la première hypothèse est nécessaire pour la réalisation d'un protocole de calcul multiparti sécurisé. L'autre hypothèse est nécessaire car on utilise le SSS de Shamir, qui est vulnérable à des attaques actives.

On note $k = \lceil \frac{n}{2} \rceil - 1$. Un groupe de $k + 1$ participants contient donc au moins un participant honnête.

Envoi des paramètres au tiers de confiance

L'idée de cette étape est que chaque participant doit donner à son paramètre une forme utilisable dans les calculs. Puisqu'on souhaite utiliser le protocole de Shamir, on demande aux participants de générer des polynômes secrets P_i de degrés k dont les coefficients constants sont les paramètres secrets x_i et dont les autres coefficients sont tirés aléatoirement.

Comme pour le protocole de Shamir, on fixe $\alpha_1, ..., \alpha_n \in \mathbb{F}_q^\times$ distincts. Chaque participant i envoie à chaque participant j le fragment $P_i(\alpha_j)$.

Calcul de somme

Chaque participant i dispose de $P_1(\alpha_i)$ et $P_2(\alpha_i)$ où P_1 est un polynôme de degré k et de secret $P_1(0) = s_1$, et P_2 est un polynôme de degré k et de secret $P_2(0) = s_2$. Chaque participant i calcule $Q(\alpha_i) := P_1(\alpha_i) + P_2(\alpha_i)$. Maintenant, si les participants souhaitent retrouver $s_1 + s_2$, ils utilisent les fragments $Q(\alpha_i)$.

Calcul de produit

Chaque participant i dispose de $P_1(\alpha_i)$ et $P_2(\alpha_i)$ où P_1 est un polynôme de degré k et de secret $P_1(0) = s_1$, et P_2 est un polynôme de degré k et de secret $P_2(0) = s_2$. Chaque participant i calcule $Q(\alpha_i) := P_1(\alpha_i)P_2(\alpha_i)$.

Problème : Q est de degré $2k$ dans certains cas.

Réduction de degré

Idée : retrouver le coefficient constant de Q et créer un nouveau polynôme. Pour garantir la sécurité, on ajoute un terme aléatoire et on le retire après.

Chaque participant i tire aléatoirement et indépendamment selon la loi uniforme des coefficients $r_i, u_{i,1}, ..., u_{i,k}, v_{i,1}, ..., v_{i,2k} \in \mathbb{F}_q$ et construisent $R_k^i := r_i + \sum_{j=1}^{k} u_{i,j} X^j$ et $R_{2k}^i := r_i + \sum_{j=1}^{2k} v_{i,j} X^j$. On pose $R_k = \sum_{i=1}^{n} R_k^i$ et $R_{2k} = \sum_{i=1}^{n} R_{2k}^i$, deux polynômes de coefficient constant $r := \sum_{i=1}^{n} r_i$, et dont les autres coefficients sont indépendants. Alors, comme vu précédemment, les participants peuvent calculer les $R_k(\alpha_i), R_{2_k}(\alpha_i)$.

Les participants peuvent alors retrouver $Q - R_{2k}$ sans avoir d'information sur $Q(0)$ (car $2k < n$). On pose $\delta = Q - R_{2k}(0)$.

Réduction de degré

Chaque participant peut donc calculer le fragment $Q'(\alpha_i) = R_k(\alpha_i) + \delta$. Alors le polynôme $Q' := R_k + \delta$ est de degré k et $Q'(0) = Q(0)$.

Résultat

Les participants peuvent retrouver le résultat du calcul en utilisant l'interpolation de Lagrange.

Références

- I. Damgård and J. Nielsen, *Scalable and unconditionally secure multiparty computation*, CRYPTO 2007, Springer, pp. 572–590.
- Y. Lindell, *Secure multiparty computation*, Communnications of the ACM **64** (2021), no. 1, 86–96.
- C. Padró, *Lecture Notes in Secret Sharing*, Éléments du cours Applications of Combinatorics to Information-Theoretic Cryptography, Nanyang Technological University, Singapore, 2013.
- A. Shamir, *How to share a secret*, Communications of the ACM (1979).