Application des codes correcteurs au partage du secret

Secret sharing algorithms

Sami HARARI

Université de Toulon et du Var, Groupe d'Étude du Codage de Toulon, avenue de l'Université, 83130 LA GARDE.

RÉSUMÉ

Ce qui caractérise une quantité secrète c'est précisemment l'absence d'information sur ses caractéristiques, et notamment sur sa structure. Si une quantité secrète est destinée à être partagé entre plusieurs dépositaires ne devant en connaître qu'une partie, sa structure doit être connue à des fins de reconstitution et de contrôle. En l'absence de tout codage adéquat, cette information sur la structure peut être suffisante pour permettre à des dépositaires une reconstitution illégitime de la quantité secrète à partir de la partie qu'ils détiennent.

Dans ce travail le problème du codage de l'information permettant une révélation de la structure de la quantité secrète et ne permettant pas une reconstitution de la quantité secrète, est repris d'après [1] et [2] et approfondi.

Un autre aspect du partage du secret est le problème dit « des otages ». Un algorithme de partage du secret est sans otage si aucun des dépositaires ne peut reconstituer la quantité secrète à lui tout seul, ni ne peut empêcher sa reconstitution par une réunion d'un nombre suffisant d'autres dépositaires.

Dans ce travail une formalisation du problème est faite. Deux algorithmes de partage de secret sans otage sont proposés.

1. Introduction

La solidité des algorithmes récents à caractère cryptographique est telle que la connaissance d'un cryptogramme (et d'éventuellement d'un clair correspondant) ne fournit aucune information sur la cryptanalyse d'un autre cryptogramme. La sécurité de ces systèmes repose uniquement sur l'effort fourni dans la protection du secret des clés utilisées pour le chiffrement et le déchiffrement.

Ce travail introduit la notion de sécurité des clés d'un système à l'aide de la notion d'entropie.

Suivant [1] la notion de partage de secret sans otage est définie et étudiée.

Deux algorithmes de partage de secret utilisant les codes correcteurs sont proposés, avec des exemples numériques.

2. Sécurité des clés dans un système cryptographique

Si les clés d'un système cryptographique sont tirées de manière équiprobables dans un ensemble de cardinalite M, l'entropie de l'espace des clés (ou bien l'entropie de la clé) est $\log_2 M$.

La notion d'entropie de sécurité d'un système de clés est liée à l'utilisation de l'outil auquel elle est destinée, et de la durée de validité de ces clés, ainsi qu'à l'entropie de l'espace des clés.

Soit N le nombre d'essais de clés possibles pendant la validité d'une clé donnée.

Définissons l'entropie de sécurité d'un système de clés par

$$h_0 = \log_2 N.$$

Une clé secrète C sera dite sûre si son entropie h (C) vérifie

$$h(C) > > h_0.$$

Pour un système cryptographique dont le délai de réponse est de 1 heure, et dont la validité de la clé est de 1 journée, une clé secrète est sûre si son entropie vaut 10 bits.

Pour un système dont le délai de réponse est de 1 ms, et la validité de la clé de 1 an, une clé secrète est sûre si son entropie vaut 60 bits.

3. Le partage du secret

Soit K un espace de clés. Un système de partage de secret entre α dépositaires est la donnée de α espaces de clés $K_1, \ldots, K_\alpha$ et d'une application $\sigma = (\sigma_1, \ldots, \sigma_\alpha)$.

$$\sigma : \quad K \to \Pi_i K_i$$

telle que pour toute quantité secrète sûre S les $\sigma_i(S)$, $i = 1, \ldots, \alpha$ soient des quantités secrètes sûres vérifiant :

(1) La connaissance d'une partie des $\sigma_i(S)$ ne permet pas de reconstituer $\sigma(S)$.

(2) La connaissance de $\sigma(S)$ permet de reconstituer S.

Un tel système est otage de chacun des dépositaires, puisque l'absence de un ou plusieurs dépositaires interdit la reconstitution de S.

Un système de partage de secret de type (α, β) où $\beta < \alpha$ est un système de partage de secret où la condition (1) est remplacée par

(1) La connaissance de moins de β quantités $\sigma_i(S)$ ne permet pas de reconstituer $\sigma(S)$, la connaissance d'au moins β des quantités $\sigma_i(S)$ permet de reconstituer $\sigma(S)$.

Un système de type (α, β) est dit sans otage.

Le codage consistant en un simple partage des données constituant S entre les dépositaires est un système de type (α, α) (à condition que chacune des parties soit une quantité secrète sûre).

3.1. Codage et décodage

Le partage du secret comporte deux parties. Un algorithme de codage σ qui calcule les données devant être détenues par chacun des dépositaires, à partir de la quantité secrète initiale S. Un algorithme de décodage qui permet de reconstituer S à partir des données $\sigma_i(S)$, en nombre suffisant qui sont fournies au décodeur.

Une source fournit une quantité numérique S gardée secrète. L'application de codage σ calcule $\sigma(S)$ en $c_1 = \sigma_1(S), \ldots, c_\alpha = \sigma_\alpha(S)$ qui doit être précisé.

Il est suivi d'une distribution des c_i. Chaque dépositaire ne connaît que la quantité qui lui est destinée.

Pour reconstituer S, β dépositaires fournissent l'information en leur possession. Le décodeur reconstruit $\sigma(S)$ et en déduit S.

3.2. Considérations sur l'entropie

Soit h_0 l'entropie de sécurité de l'application considérée. Afin de déjouer des attaques par essai systématique, certaines quantités doivent avoir une entropie de sécurité :

3.2.1. La quantité secrète S doit avoir une entropie $\geqslant h_0$ en particulier si les dépositaires ont accès à l'application cryptographique dont S est la clé.

3.2.1. Tout dépositaire est en possession d'une quantité secrète sûre d'où :

$$H(c_i) \geqslant h_0 \qquad i = 1, \ldots, \alpha.$$

D'autre part les quantités détenues par chacun des dépositaires sont mutuellement indépendantes, l'entropie de l'image de S est donc minorée :

3.2.2. $H(\sigma(S)) \geqslant \alpha . h_0$.

4. Codes correcteurs et partage de secret

La description d'un algorithme de partage de secret comporte deux parties appelées codage et partage et le rassemblement et décodage. On supposera que la quantité S sera transcodée pour être de forme admissible par le codeur.

On associe à S de manière injective et secrète un mot d'un code (n, k, d).

Étant donné λ dépositaires on considère un vecteur « bruit » $f(\lambda, c)$ de poids $w(f(\lambda, c))$ de longueur n.

On suppose connue la somme

$$D = C + f(\lambda, c)$$

On sait par la théorie du codage que si $w(f(\lambda, c)) < d'$ on peut retrouver C.

$d' = d$ en cas d'effacements.

$d' = [d/2]$ en cas d'erreurs additives aléatoires.

Le choix de $f(\lambda, c)$ doit être tel que

$$\forall \lambda \geqslant \beta, \quad w(f(\lambda, c)) < d'$$
$$\forall \lambda < \beta, \quad w(f(\lambda, c)) > d'$$

4.1. Les codes correcteurs utilisés en correction d'effacement

Soit C le mot de code associé à S.

On écrit C sous la forme

$$C = C_1 + C_2 + \ldots + C_\alpha$$

où C_i est égal au vecteur alloué au dépositaire i.

On suppose que les positions des composantes non nulles de C_i sont connues.

λ dépositaires étant présents on calcule

$$D = C_{i_1} + \ldots + C_{i_\lambda}.$$

On a donc

$$D = f(\lambda, C) + C.$$

où

$$f(\lambda, C) = -(C_{j_1} + \ldots + C_{j_\lambda}).$$

λ' étant le nombre de dépositaires absents.

Soit **C** un code de Reed. Solomon de longueur n sur $\mathbf{F}_q$, de distance minimale d. Pour construire un codage de partage de secret de type (α, β) à partir de **C** on opère comme suit.

(1) L'application σ consiste à associer à S un mot C du code **C**, de manière injective.

(2) Le partage de $\sigma(S)$ consiste en le groupement des symboles du mot de code C en α groupes de symboles consécutifs, distribués aux dépositaires, dans un ordre connu de tous.

Le décodeur de reconstitution de secret consiste en un décodeur de correction d'effacement du Reed. Solomon. En effet si β dépositaires fournissent au décodeur les symboles en leur possession, il faut retrouver les symboles manquants par un algorithme de correction d'effacement afin de reconstituer $\sigma(S)$, et ensuite S.

Soient (N, K, D) les paramètres du code de Reed. Solomon considéré sur $\mathbf{F}_q$. Posons $m = \log_2 q$.

Les conditions de sécurité sur les entropies entraînent des contraintes sur les paramètres du code.

Les conditions 3.2.2 et 3.2.1 se traduisent par les conditions suivantes sur les longueurs dans le cas d'une répartition uniforme des symboles entre les dépositaires.

$$(q-1).m \geqslant \alpha.h_1.$$

Soit n le nombre de symboles détenus par chaque dépositaire. On doit avoir

$$\pi.m \geqslant h_1 \text{ ce qui entraîne que } \mathrm{N}.m \geqslant \alpha.h_0.$$

Afin que S ait une entropie de sécurité il faut aussi que

$$\mathrm{K} \geqslant h_0.$$

De même pour que la reconstitution puisse avoir lieu uniquement en la présence d'au moins β dépositaires il faut que δ vérifie

$$\mathrm{D} \geqslant \beta.$$

4.1.1. *Exemple numérique de réalisation*

Un système de partage de secret de type (3,2) reposant sur le principe de correction d'effacement peut être réalisé à partir du code de Reed. Solomon sur $\mathbf{F}_{64}$ de dimension 34 et de distance 30.

L'image du secret S est un mot du code. On distribue à chaque dépositaire 19 symboles de $\mathbf{F}_{64}$, composantes du mot de code dans un ordre connu de tous les dépositaires. Un exemple de telle répartition est que le premier dépositaire soit en position des 19 premières composantes, le second des 19 suivantes, les derniers des 19 suivantes. Les 6 dernières composantes sont connues de tous les dépositaires.

Pour la reconstitution chaque dépositaire restitue les composantes en sa possession. En l'absence d'un dépositaire le décodeur pourra reconstituer les symboles manquants par un algorithme de correction d'effacement, ceci est rendu possible par le fait que le code est de distance minimale 29.

On vérifie aisément que les conditions sur les entropies sont satisfaites.

En effet chaque symbole est d'entropie 6.

La quantité détenue par chaque dépositaire est d'entropie $6.19 = 154$.

L'entropie du code est $6.34 = 204$.

4.2. Les codes correcteurs utilisés en correction d'erreurs

Dans ce cas on alloue à chaque dépositaire un vecteur

$$\mathrm{A}_i \qquad (i = 1 \ldots \alpha).$$

On pose

$$\mathrm{A} = \mathrm{A}_1 + \ldots + \mathrm{A}_\alpha.$$

On suppose connu de tous le vecteur $\mathrm{D}' = \mathrm{C} + \mathrm{A}$.

λ dépositaires étant présents, on calcule

$$\mathrm{A}' = \mathrm{A}_{i^1} + \ldots + \mathrm{A}_{i_\lambda}.$$

et le vecteur

$$\mathrm{D} = \mathrm{D}' + \mathrm{A}'.$$

On a donc

$$\mathrm{D} = \mathrm{C} + f(\lambda, \mathrm{C})$$

où

$$f(\lambda, \mathrm{C}) = \mathrm{A} + \mathrm{A}_{i_1} + \ldots + \mathrm{A}_{i_\lambda}.$$

Soit **C** un code linéaire de type (n, k, d) sur F_q satisfaisant aux mêmes contraintes sur les entropies de sécurité. Pour construire un code de partage de secret de type (α, β), à partir de **C**, opérer comme suit.

(1) choisir C un mot de code **C**, et choisir un vecteur aléatoire A de longueur n, à coefficients dans F_q, de poids $\geqslant \alpha.d$.

Soit $\mathrm{D} = \mathrm{C} + \mathrm{A}$ le vecteur somme.

(2) Les composantes de D sont supposées connues de tous.

(3) Écrire A sous le forme

$$\mathrm{A} = \mathrm{A}_1 + \mathrm{A}_2 + \ldots + \mathrm{A}_\alpha$$

où les A_i sont des vecteurs de longueur n à composantes dans F_q avec

$$w(\mathrm{A}) \geqslant d$$

et

$$w(\mathrm{A}_i) \geqslant dd, \qquad i = 1 \ldots \alpha.$$

pour tout λ-uple avec $\lambda \geqslant \beta - 1$ on doit aussi avoir

$$w(\mathrm{A} + \mathrm{A}_{i_1} + \ldots + \mathrm{A}_{i_\lambda}) \geqslant d$$

ainsi que pour tout λ-uple avec $\lambda \geqslant \beta$

$$w(\mathrm{A} + \mathrm{A}_{i_1} + \ldots + \mathrm{A}_{i_\lambda}) < d.$$

Les vecteurs A_i sont distribuées aux dépositaires.

Si ces conditions sont satisfaites, en présence d'au moins β dépositaires la reconstitution partielle du vecteur A fournit un vecteur A′ de poids $< d$. Posons $D' = D + A'$.

En présence d'au moins β dépositaires le vecteur D′ est à une distance $< d$ de C, le décodeur retrouvera de manière unique le vecteur C.

Si moins de β dépositaires sont présents, le vecteur D′ sera à une distance $> d$ de C, et le décodeur ne pourra pas trouver C.

4.2.2. *Exemple numérique de réalisation*

On suppose dans l'ensemble qui suit que l'entropie de sécurité vaut 55.

Un système de partage de secret de type (3,2) peut être réalisé à partir d'un code de Reed et Muller de longueur 1 024 du deuxième ordre. Sa dimension est 55, et sa distance est 256. Il corrige 127 erreurs.

On choisit un vecteur A binaire de longueur 1 024, de poids 381. On partitionne l'ensemble des indices où les coordonnées de A sont nulles en 3 sous ensembles de 127 éléments disjoints 2 à 2, soit E_1, E_2, E_3.

A_i sera un vecteur de poids 127 ayant ses coordonnées non nulles dans $E_i (i = 1, 2, 3)$.

Pour reconstituer le secret les dépositaires fournissent au décodeur leurs coordonnées. Celui-ci les rajoute au vecteur D. En l'absence de l'un des dépositaires le vecteur résultat sera à une distance 127 du mot de code. L'algorithme de décodage permet de corriger les erreurs, donc de déduire $\sigma(S)$.

Conclusion

Les deux méthodes présentées offrent, avec un choix de paramètres adéquats, une même sécurité pour le partage du secret puisqu'elles reposent sur le même principe.

La deuxième présente un avantage supplémentaire. En effet le gestionnaire du système peut changer la quantité secrète S sans avoir à modifier les quantités détenues par les dépositaires.

Ceci entraîne une plus grande sécurité pour l'application dont S est la clé.

L'auteur remercie les experts, pour les suggestions d'amélioration, notamment aux paragraphes 2 et 4.

Manuscrit reçu le 4 *septembre* 1986.

BIBLIOGRAPHIE

[1] M. Hellman, An extension of the Shannon theory approach to cryptography, *IEEE Trans. on Inf. Theory*, IT, 21 sept. 1975.

[2] E. D. Karnin, J. W. Greene et M. E. Hellman, On secret sharing systems, *IEEE trans; on Inf. Theory*, IT19, n° 1, January 1983.

[3] K. Koyama, Cryptographic key sharing methods for multigroups and security analysis, *Trans. of the IECE of Japan*, E66, n° 1, Jan. 1983.

[4] M. Mignotte, « *How to share a secret* ». *Cryptography*, Th. Beth éd., *Lecture Notes on Computer Science*, 149, Springer Verlag, 1983.

[5] H. Yamamoto, On secret sharing communication systems with two or three channels, *IEEE Trans. on Inf. Theory*, IT32, May 1986.