NEUVIEME COLLOQUE SUR LE TRAITEMENT DU SIGNAL ET SES APPLICATIONS

NICE du 16 au 20 MAI 1983

LE PARTAGE DU SECRET

S. HARARI

U.E.R. de Mathématiques
33 rue Saint-Leu (80039)AMIENS Cedex

CNET - RPE
38, Av du Gal Leclerc (92131)ISSY-LES-MOULINEAUX

RESUME

Dans ce travail nous définissons le problème du partage d'une quantité secrète S entre A dépositaires, soumis aux contraintes suivantes :

1) B dépositaires doivent pouvoir déterminer S. (B<A, est donné d'avance).

2) (B-1) dépositaires ne doivent pas être en mesure de déterminer S.

3) Chaque dépositaire possède une quantité secrète.

Nous donnons des bornes sur les paramètres des codes possibles. Nous établissons une théorie de l'information d'un tel système. Sans hypothèse sur S un codage est nécessaire pour parvenir à satisfaire les conditions 1), 2), 3). Nous montrons que parmi tous les codes susceptibles de résoudre ce problème, les codes correcteurs offrent une solution optimale : B et A étant donnés le codage qui a S associe le mot d'un code correcteur bien choisi est celui qui a le mot de code le plus court.

Nous donnons deux exemples de réalisation avec des codes de Reed Solomon sur un grand corps premier, ainsi que des performances d'un tel système : le temps nécessaire pour effectuer le codage et le décodage.

SUMMARY

In this paper we define the problem of sharing a secret S between A sharers with the following constraints :

1) B sharers mustbe able to find the secret quantity S with their own share (B<A is given beforehand)

2) (B-1) sharers must not be able to determine S

3) Each sharer possesses a secret quantity.

We establish an information theory of such systems. We obtain bounds on the adapted codes ; satisfying 1), 2), 3).

We show that among all codes error correcting codes offer an optimal solution : a code whose codewords are shortest possible.

We give an example of realisation with a Reed Solomon code on a large prime field and the caracteristics of such a system.

G R E T S I 83

I - La sécurité des systèmes de partage de secret

La notion de sécurité d'une clé secrète est liée à l'utilisation de l'outil, auquel elle est destinée, et de la durée de validité de cette clé.

Nous dirons qu'une clé secrète est sûre pour un outil informatique si le temps nécessaire pour déterminer cette clé par essai systématique de toutes ses valeurs possibles est très long par rapport à la durée de validité de la clé.

Exemple 1 : Pour un outil dont le délai de réponse est de une heure, et la validité de la clé de une journée, une clé secrète sera sûre si elle a 2^{10} valeurs possibles.

Exemple 2 : Pour un outil dont le délai de réponse est de une milliseconde, et la validité de la clé de un an une clé secrète sera sûre si elle a 2^{60} valeurs possibles. Cette notion de sécurité de clé secrète est de grande utilité dans le cas des terminaux informatiques financiers, ou pour résoudre le problème des mots de passe. Dans la suite, on dira qu'une clé secrète est sûre si son entropie est supérieure à ho entropie de sécurité. Dans la pratique ho = 60 bits.

II - Introduction

: Soit S une quantité secrète sûre. Nous nous proposons de résoudre le problème suivant : b et a étant deux entiers donnés (b < a) peut-on effectuer un codage de S satisfaisant aux conditions :

(p) Le mot de code c(S) associé à S peut être partagé en a quantités secrètes sûres.

(r) Tout sous ensemble de b dépositaires peuvent déterminer c(S) à l'aide de leurs données propres, de l'algorithme de décodage,
(b-1) ne pouvant pas le faire dans les mêmes conditions.

De plus, peut-on définir une notion d'optimalité pour de tels codes, et existe-t-il une famille de codes optimaux, ou bien asymptotiquement optimaux, quand b et a augmentent indéfiniment.

III - Théorie de l'information du partage du secret :

Le simple partage des symboles composant S entre les a dépositaires satisfait à la condition p) si ce nombre de symboles est suffisamment grand.

Il ne satisfait pas à la condition R).

Un codage est donc nécessaire, qui donne lieu aux diagrammes fonctionnels suivants :

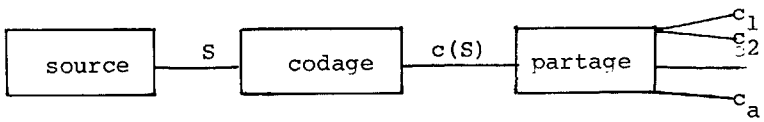

figure 1 : codage et partage du secret

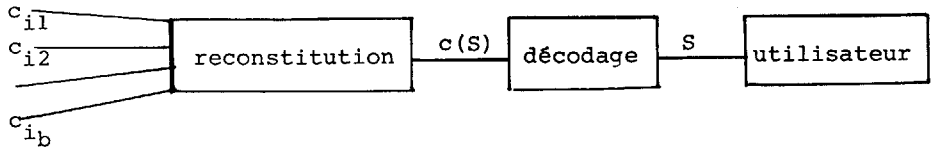

figure 2 : reconstitution et décodage

Une source fournit des données S à coder. Un algorithme de codage associe le mot de code c(S). Les symboles de c(S) sont partagés entre les a dépositaires $(c_1, c_2, \ldots, c_a)$.

Au décodage b dépositaires (au moins) fournissent à l'algorithme de reconstitution leur partie de secret. c(S) est déterminé à partir de ces données. Le décodeur fournit S à l'utilisateur à partir de c(S).

Soit S une quantité secrète c(S) le mot de code associé, ho l'entropie de sécurité, c_i (i=1,...,a) les blocs remis à chacun des dépositaires,

Les conditions suivantes doivent alors être vérifiées.

Pour tout l-uple $l \leq b-1$. On doit avoir :

$$H(c(S) \mid c_{i_1}, \ldots, c_{i_l}) \geq h_o$$

Pour tout l-uple avec $b \leq l$ on doit avoir

$$H(c(S) \mid c_{i_1}, \ldots, c_{i_l}) = 0$$

En particulier on en déduit que $H(c_i) \geq ho$ pour i=1,...,a.

Définition : Un code de partage de secret sera de type (a,b) s'il permet de partager le secret entre a dépositaires, permet à b dépositaires parmi les a de le reconstituer.

Ceci nous laisse définir une notion d'optimalité pour les codes de partage de secret.

Soit $(C_i, a_i, b_i)\, i \in I$ une famille de codes de partage de secret ; chaque code C_i étant de type (a_i, b_i). Soit C_i^j $j=1,\ldots,a_i$ le bloc de symboles remis à chaque dépositaire ; pour le code C_i . La famille C_i sera optimale si

$\lim_{i\to\infty} H(C_i^j) = h_o$ pour $j=1,\ldots a_i$.

IV - Bornes sur les paramètres d'un code :

Nous supposerons que les codes de partage de secret ont des mots de longueur constante et sont linéaires. Les symboles sont dans un alphabet F_q , de cardinalité q est de la forme p^s , p premier . Nous supposerons de même que les $\log_2 q \geq h_o$.

Sous ces hypothèses chaque dépositaire sera en possession d'un symbole et le code sera un sous espace vectoriel de dimension 1 .

Nous nous intéressons aux relations entre a,b,n.

Il vient que $a \leq n$; $1 \leq b$.

Nous allons dénombrer les configurations décodables correctement par le système. Nous supposons pour simplifier les calculs sans nuire à la généralité que n=a.

la donnée de b symboles du mot c(S) doit donner lieu à un décodage correct

$\binom{n}{b} q^{n-b}$ configurations sont donc décodables.

la donnée de b+1 symboles de c(S) donnent lieu à un décodage correct

$\binom{n}{b+1} q^{n-b-1}$ configurations sont donc décodables.

.....

la donnée de n symboles donne lieu à un décodage correct

$\binom{n}{n}$ configuration est décodable.

Les configurations non décodables doivent être suffisamment nombreuses pour qu'un tirage au hasard ne donne pas lieu à un décodage correct. Il y a q^n configurations au total. Ces conditions sont assurées si l'inégalité suivante est vérifiée :

$$\log_2 \left[q^n - \binom{n}{b} \cdot q^{n-b} \ldots - \binom{n}{n-1} \cdot q - 1 \right] \geq h_o \cdot$$

V - Exemples de réalisations avec un code de Reed Solomon :

Choisissons q=163.

Le code de Reed Solomon sur F_{163} est de longueur 162.

Chaque symbole est d'entropie 7,34 bits.

Tout dépositaire devra être en possession de 9 symboles. Ce code permet le partage du secret entre 18 dépositaires. La dimensions du code est au moins 9 ; donc sa distance minimale est au plus 155.

En utilisant une stratégie de correction d'erreur on a $b \geq 8$. Ce code est la base d'un système de type (18,8). Pour q=47 le code de Reed Solomon sur F_{47} est de longueur 46.

Chaque symbole est d'entropie 5,5 bits.

Tout dépositaire doit être en possession de 11 symboles. La distance minimale du code est au plus 37.

Ce code permet la mise en oeuvre d'un système (4,1) avec stratégie de correction d'erreur.

Temps de codage :

En longueur 162 il existe une transformée aux nombres entiers rapide. Sur un Microprocesseur de 8 bits de définition à 4MHZ, le temps de codage est de l'ordre de 3 secondes.

Le temps de décodage est de l'ordre de 40 secondes avec un algorithme de décodage par transformée de Fourier discrète.

En longueur 47 dans les mêmes conditions le temps de codage est de 3 secondes. Le temps de décodage est ramené à 10 secondes vu le peu d'erreurs à prendre en compte dans l'algorithme.

VI - Optimalité des codes linéaires :

En vertu du théorème de Shannon, il existe une famille de codes correcteurs, binaires linéaires $(C_i, n_i, k_i, d_i)_{i \in I}$ C_i étant un sous espace de dimension k_i de l'espace n_i , de distance minimale d_i .

C_i permet de définir un code de type (a_i, b_i) de partage de secret. En prenant $b_i = a_i - 1$, et en posant C_i^j comme la part de secret de chaque dépositaire, on voit aisément que $\lim_i H(C_i^j) = ho$.

VII - Conclusion :

Nous avons étudié les systèmes de partage du secret. Les paramètres des codes de partage de secret sont difficiles à obtenir à priori. Les codes correcteurs sont une exception à cette règle. Grâce à leur distance minimale on obtient aisément les paramètres de partage de secret. De plus les familles optimales de codes correcteurs, sont aussi optimales pour le partage du secret. Ce ne sont pas les seules.

Bibliographie : (1) On secret Sharnig systems. Karnin,Greene Hellman (EEE Trans on Inf. Theory. Vol IT29. Jan. 1983

(2) Me Williams Sloane. Error Correcting Codes. North Holland 1977.