Niveau : 3 **Vert**

La securite parfaite de Claude Shannon

1 Introduction, notations

Claude Channon dans un article de 1949 (« Communication theory of secrecy systems », *Bell System Technical Journal*, vol 328,n. 4,p. 656-715, 1949) introduit la notion de sécurité parfaite ou encore de systèmes cryptographiquement sûrs. Les conditions requises pour avoir un système cryptographiquement sûrs au sens de Shannon sont trop fortes pour s'appliquer en général dans des applications concrètes à usage commercial.

Le lecteur peut se référer au livre : « Cryptographie, principes et mises en œuvre », de P. Bathélemy, R. Rolland et P. Véron aux éditions Hermes-Lavoisier pour des précisions sur la sécurité au sens de Shannon et son évolution vers des modèles plus réalistes pour les applications.

2 Sécurité au sens de Shannon

Nous supposerons que nous étudions un système cryptographique constitué de :
– un ensemble fini $\mathcal{M}$ de textes clairs,
– un ensemble fini $\mathcal{C}$ de textes chiffrés,
– un ensemble fini $\mathcal{K}$ de clés,
– pour chaque clé $k \in \mathcal{K}$ une fonction injective de chiffrement e_k de $\mathcal{M}$ dans $\mathcal{C}$ et une fonction injective de déchiffrement d_k de $e_k(\mathcal{M})$ dans $\mathcal{M}$ de telle sorte que $d_k \circ e_k = Id_{\mathcal{M}}$.

Nous supposerons que ce système est utilisé de la manière suivante : chaque nouveau chiffrement d'un texte clair utilise une nouvelle clé choisie aléatoirement dans l'ensemble des clés conformément à sa loi de probabilité.

L'ensemble des textes clairs $\mathcal{M}$ est muni d'une probabilité $P_{\mathcal{M}}$ et l'ensemble des clés $\mathcal{K}$ est aussi muni d'une probabilité $P_{\mathcal{K}}$. Nous noterons P la probabilité produit sur $\mathcal{M} \times \mathcal{K}$. C'est cette probabilité que nous utiliserons, ce qui signifie en particulier que les clés sont choisies indépendamment des textes clairs, et que chaque chiffrement demande le tirage au sort d'une clé et la donnée d'un texte clair qu'on peut estimer aléatoire dans l'espace $\mathcal{M}$ muni de sa probabilité.
Pour simplifier les notations, par abus de langage :
– si $x \in \mathcal{M}$, nous noterons encore x l'événement $\{x\} \times \mathcal{K}$ et parlerons de ce fait de $P(x)$ cette dernière probabilité valant d'ailleurs $P_{\mathcal{M}}(\{x\})$,
– de la même manière, si $k \in \mathcal{K}$, nous noterons encore k l'événement $\mathcal{M} \times \{k\}$ la probabilité $P(k)$ valant cette fois $P_{\mathcal{K}}(\{k\})$,
– enfin si $y \in \mathcal{C}$, nous noterons encore y l'événement $\{(x,k) \mid e_k(x) = y\}$.

Ainsi, x est l'événement « le texte clair est x », k est l'événement « la clé est k »et y l'événement « le texte chiffré est y ». Remarquons que :

$$\{(x,k) \mid e_k(x) = y\} = \bigcup_{\substack{k \in \mathcal{K} \\ y \in e_k(\mathcal{M})}} \{(d_k(y), k)\},$$

et qu'en conséquence, la probabilité de y est donnée par :

$$P(y) = \sum_{\substack{k \in \mathcal{K} \\ y \in e_k(\mathcal{M})}} P(k)P(d_k(y)).$$

Nous noterons aussi $P(x|y)$ la probabilité conditionnelle de l'événement x sachant y (« le texte clair est x sachant que le texte chiffré est y »).
Remarque: C'est dans le calcul de $P(y)$ qu'intervient le fait qu'une nouvelle clé k est prise aléatoirement pour chaque nouveau message x.

2.1 Systèmes cryptographiquement sûrs

Définition 2.1 *Un système cryptographique, du type décrit précédemment (en particulier pour lequel on choisit une nouvelle clé pour chaque nouveau message), est parfaitement sûr si :*

$$\forall x \in \mathcal{M},\ \forall y \in \mathcal{C},\ \ P(x|y) = P(x).$$

Autrement dit, la probabilité d'un texte clair x sachant que le texte chiffré est y est la même que la probabilité de x. Le texte chiffré dans ce cas n'apporte aucune information sur le texte clair.

Théorème 2.2 *Si on suppose que $\forall y \in \mathcal{C}$ on a $P(y) > 0$ et que le système est parfaitement sûr, alors :*

$$|\mathcal{K}| \geq |\mathcal{C}| \geq |\mathcal{M}|.$$

Preuve.Remarquons que la condition $P(y) > 0$ est naturelle dans la mesure où un texte chiffré qui a une probabilité nulle d'être atteint peut être supprimé de l'ensemble $\mathcal{C}$ (nous sommes dans le cadre d'ensembles finis).
Fixons $x \in \mathcal{M}$ tel que $P(x) > 0$. Pour chaque $y \in \mathcal{C}$ on a :

$$P(x|y) = P(x).$$

D'après le théorème de Bayes :

$$P(y)P(x|y) = P(y|x)P(x),$$

donc :

$$P(y|x) = P(y) > 0.$$

Ceci signifie qu'il existe au moins une clé $k \in \mathcal{K}$ telle que $e_k(x) = y$.
Par suite :

$$|\mathcal{K}| \geq |\mathcal{C}|.$$

Comme e_k est injective on a :

$$|\mathcal{C}| \geq |\mathcal{M}|.$$

□

Théorème 2.3 *Soit un système cryptographique vérifiant :*

$$|\mathcal{K}| = |\mathcal{C}| = |\mathcal{M}|,$$

ainsi que $P(y) > 0$ pour tout $y \in \mathcal{C}$. Il est à sécurité parfaite si et seulement si les deux conditions suivantes sont réalisées :

a) toutes les clés sont équiprobables,

b) pour chaque $x \in \mathcal{M}$ et chaque $y \in \mathcal{C}$ il existe une unique clé k vérifiant $e_k(x) = y$.

Preuve.Si les conditions sont vérifiées, pour tout $y \in \mathcal{C}$ on a successivement :

$$P(y) = \sum_{\substack{k \in \mathcal{K} \\ y \in e_k(\mathcal{M})}} P(k)P(d_k(y)),$$

$$P(y) = \frac{1}{|\mathcal{K}|} \sum_{k \in \mathcal{K}} P(d_k(y)),$$

$$P(y) = \frac{1}{|\mathcal{K}|} \sum_{x \in \mathcal{M}} P(x) = \frac{1}{|\mathcal{K}|}.$$

D'autre part pour $x \in \mathcal{M}$ et $y \in \mathcal{C}$ puisqu'il n'y a qu'une clé k qui vérifie $e_k(x) = y$ on a :

$$P(y|x) = \sum_{k|e_k(x)=y} P(k) = \frac{1}{|\mathcal{K}|}.$$

La formule de Bayes nous donne alors :

$$P(x|y) = \frac{P(x)P(y|x)}{P(y)},$$

$$P(x|y) = \frac{P(x)/|\mathcal{K}|}{1/|\mathcal{K}|} = P(x).$$

La sécurité est donc parfaite.
Réciproquement, supposons la sécurité parfaite. Comme dans le lemme précédent, on montre que pour chaque couple $(x, y) \in \mathcal{M} \times \mathcal{C}$ il existe une clé k telle que $e_k(x) = y$. Pour x fixé on a donc :

$$\{e_k(x) \mid k \in \mathcal{K}\} = \mathcal{C},$$

ce qui montre que pour x fixé l'ensemble des $e_k(x)$ est de cardinal $|\mathcal{C}| = |\mathcal{K}|$. Ces $e_k(x)$ sont donc distincts deux à deux et pour chaque $y \in \mathcal{C}$, la clé k vérifiant $e_k(x) = y$ est unique.
Pour deux clés k_1 et k_2, comparons $P(k_1)$ et $P(k_2)$. Pour cela fixons y et désignons par x_1 et x_2 les uniques éléments de $\mathcal{M}$ vérifiant $e_{k_1}(x_1) = y$ et $e_{k_2}(x_2) = y$ (chaque e_k est injective et donc ici bijective). Grâce au théorème de Bayes et à la sécurité parfaite on obtient :

$$P(y) = P(y|x_1) = \sum_{k|e_k(x_1)=y} P(k) = P(k_1).$$

Le même calcul peut être fait avec k_2. Ce qui prouve que $P(k_1) = P(k_2)$. □

2.2 Un exemple

Le *one-time-pad* vérifie très exactement les conditions du théorème (2.3). C'est un système parfaitement sûr. Rappelons ce qu'est le one-time-pad, ou encore chiffrement de Vernam, ou encore masque jetable.

Le cryptosystème de Vernam utilise une clé secrète très longue qui devrait de manière idéale représenter une suite aléatoire de bits où chaque bit est indépendant des autres et a un probabilité $1/2$ d'être 0 et bien entendu une probabilité $1/2$ d'être 1.
Si on a un message m de n bits à chiffrer, on considère les n premiers bits de la clé qui constituent un mot K et on calcule le « ou exclusif bit à bit »entre le message et cette partie de la clé, c'est-à-dire

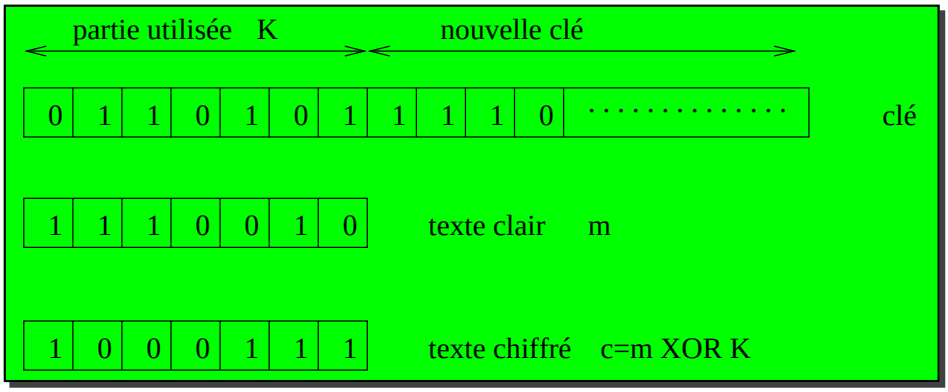

FIG. 1 – Le one-time-pad

que le texte chiffré s'écrit sous la forme $c = m \oplus K$. Ainsi la partie K de la clé sert de masque. Le destinataire qui partage la même clé extrait de la même façon la partie K et récupère alors le texte clair m en calculant $m = c \oplus K$. Les deux interlocuteurs jettent la partie K utilisée et peuvent effectuer une nouvelle transaction en procédant de même avec le reste de la clé.

Ce système réalise évidemment les conditions du théorème de Shannon sur la sécurité parfaite : une nouvelle clé est tirée à chaque chiffrement, la clé est aussi longue que le texte clair, l'ensemble des clés a une probabilité équirépartie.

Construire une clé aussi longue et qui de plus soit une suite aléatoire de bits n'est pas chose facile. Il est possible de réaliser approximativement un tel système à partir d'un générateur pseudo-aléatoire et d'un germe. Bien entendu dans ce cas, le germe est la véritable clé secrète du système, et les conditions de Shannon ne sont plus satisfaites.

2.3 Le paradoxe de la cryptographie à clé publique

Soit X une variable aléatoire discrète définie sur un espace probabilisé Ω. On appelle entropie de X, la quantité :

$$H(X) = -\sum_{\omega \in \Omega} \mathtt{Pr}(X = \omega) \log_2 \mathtt{Pr}(X = \omega).$$

Cette fonction introduite en 1948 par C.E. Shannon dans son célèbre article « A mathematical Theory of Communication »possède plusieurs interprétations équivalentes. Notamment, de façon informelle, $H(X)$ correspond à une mesure moyenne de l'incertitude sur la valeur de X. Si X prend ses valeurs dans un ensemble à n éléments, on peut encoder de façon naïve chaque élément sur $\log_2 n$ bits, $H(X)$ fournit sur une échelle graduée de 0 à $\log_2 n$, une valeur traduisant l'incertitude moyenne sur X. Par exemple, si $H(X) = 10$, ceci signifie qu'il suffit en moyenne de connaître 10 bits pour déterminer entièrement les valeurs prises par X. Ainsi ces valeurs peuvent être codées sur 10 bits au lieu de $\log_2 n$. Cela dépend évidemment de la loi de probabilité de X. On définit de même l'entropie conditionnelle de X sachant Y, et on note $H(X|Y)$, la valeur qui mesure l'incertitude moyenne sur X connaissant Y.
Soient M, C et K les variables aléatoires discrètes associées aux choix d'un message m, d'un cryptogramme c et d'une clé k, on peut alors donner une définition de la confidentialité parfaite en termes d'entropie.

Définition 2.4 *On dit qu'un système de chiffrement à clé secrète est à confidentialité parfaite si* $H(M|C) = H(M)$.

Cette définition est, bien entendu, équivalente à la définition donnée précédemment. En d'autres termes ceci signifie que la connaissance d'un cryptogramme c n'apporte aucune information sur le texte clair m.
En cryptographie à clé publique, l'attaquant dispose du cryptogramme et de la valeur de la clé publique k. On s'intéresse donc à la quantité $H(M|C, K)$. Étant donné qu'un message clair est entièrement déterminé par un cryptogramme c et une clé publique k, un résultat classique sur la fonction d'entropie permet d'affirmer que $H(M|C, K) = 0$. Ce résultat « surprenant », stipule qu'il n'existe pas de système de chiffrement à clé publique à confidentialité parfaite et que de plus il y a suffisamment d'information dans un cryptogramme c et dans la clé publique k pour déterminer le message clair correspondant. Cependant ce résultat ne nous dit pas comment utiliser cette information, ni même si cette dernière peut être exploitée en temps raisonnable. C'est là tout le paradoxe de la cryptographie à clé publique.