Master 1 Master de Mathématiques et Applications Cours en commun : Université Paris VII et Université VIII
(Parcours ACC et CSSD)
Programmation en cryptographie S. Mesnager

Primitives du chiffrement symétrique : Fonctions Booléennes I - Forme Algébrique Normale, Degré

Une fonction booléenne est toute fonction de $\mathbb{F}_2^n$ dans $\mathbb{F}_2$ (le corps $\mathbb{F}_2$ est par définition le corps à deux éléments $\mathbb{F}_2 = \{0, 1\}$ muni de l'addition et de la multiplication modulo 2).

Les primitives de chiffrement symétrique font largement appel aux fonctions booléennes, et leur sécurité dépend de maniere essentielle des propriétés cryptographiques de ces dernières. La recherche dans ce domaine consiste à la fois à étudier les propriétés cryptographiques de fonctions booléenes impliquées dans des schémas existants et à proposer de nouvelles fonctions booléennes ayant de bonnes propriétés cryptographiques.

Exercice 1.
Toute fonction booléenne f de $\mathbb{F}_2^n$ admet une unique représentation de la forme

$$f(x_1, \ldots, x_n) = \bigoplus_{S \subset [\![1,n]\!]} a_S x_S$$

ou x_S désigne le monôme $\prod_{i \in S} x_i$ et où les coefficients a_S appartiennent à $\mathbb{F}_2$. Cette représentation est appelée la Forme Algébrique Normale (en anglais "ANF").

(1) Ecrire une procédure qui donne la forme algébrique normale d'une fonction booléenne.
(2) Donner l'ANF fonction booléenne f definie sur $\mathbb{F}_2^3$ donnée par sa table de vérité [0,1,1,0,0,1,0,1].

Exercice 2.

(1) Soit x un mot machine. Que donne les lignes de commandes suivantes ?
   (a) `x=(x&0x55555555)+((x>>1)&0x55555555);`
   (b) `x=(x&0x33333333)+((x>>2)&0x33333333);`
   (c) `x=(x&0x0f0f0f0f)+((x>>4)&0x0f0f0f0f);`
   (d) `x=(x&0x00ff00ff)+((x>>8)&0x00ff00ff);`
(2) Ecrire une fonction `int poids(unsigned x)` qui rend le poids binaire d'un mot machine:
   poids(0) —> 0
   poids(1) —> 1
   poids(9) —> 2
(3) En utilisant la fonction " poids", programmer une fonction qui rend le degré d'une fonction booléenne.
(4) Vérifier que la fonction booléenne f definie sur $\mathbb{F}_2^3$ donnée par sa table de vérité [0,1,1,0,0,1,0,1] est de degré 2.

Exercice 3.
Soient $x = (x_i)_{1 \le i \le m}$ et $y = (y_i)_{1 \le i \le m}$ deux mots de $\mathbb{F}_2^m$.
On appelle produit scalaire de deux mots binaires x et y, noté $x \cdot y$, la valeur de $x_1 y_1 \oplus \cdots \oplus x_m y_m$.

(1) On fixe $m = 32$ et on décide de représenter les mots de $\mathbb{F}_2^{32}$ par des tableaux d'entiers à 32 éléments. Écrire une fonction `ProdScal1` qui retourne le produit scalaire $x \cdot y$ de deux mots x et y donnés en argument de la fonction.

(2) Étant donné un mot de $\mathbb{F}_2^m$, on appelle parité de ce mot la parité du nombre de 1 dans ce mot. Par exemple:

`partie`$(0) = 0$ car il y a zéro 1.
`partie`$(7) = 1$ car il y a un nombre impair de 1 dans la représentation binaire de 7 (`7 = 111`).
`partie`$(9) = 0$ car il y a un nombre pair de 1 dans la représentation binaire de 9 (`9 = 1001`).

(a) Quelle est la parité de 11 ? et de 312 ?
(b) Ecrire une fonction `int parite(unsigned x)` qui rend la parité d'un nombre dans un mot x de 32 bits.
(c) Comment calculer $x \cdot y$ à l'aide de la fonction "parité" ?
(d) Vérifier que la fonction booléenne définie sur $\mathbb{F}_2^3 \times \mathbb{F}_2^5$ par: (x,y) –> π(x).y est de degré 4 où π est une fonction vectorielle de $\mathbb{F}_2^3$ dans $\mathbb{F}_2^5$ définie par (en représentation Héxa): $\pi(0)$=0x0b, $\pi(1)$=0x07, $\pi(2)$= 0x1e, $\pi(3)$= 0x1b, $\pi(4)$= 0x1d, $\pi(5)$=0x0f, $\pi(6)$= 0x1f, $\pi(7)$=0x17.