Approximation de l'addition par le XOR : comment aller (un peu) plus loin que P. Sarkar

Didier Alquié
DGA, CELAR
didier.alquie@laposte.net

2 septembre 2009

Les concepteurs d'algorithmes cryptographiques sont particulièrement intéressés par les fonctions non linéaires faciles à calculer. L'addition arithmétique est un bon candidat pour celles-ci. Par exemple, son degré algébrique augmente rapidement en fonction des bits d'entrées. De célèbres algorithmes, comme SHA-1 ou SHA-2 utilise l'addition arithmétique de plus de deux termes (en fait jusqu'à 7 termes).

L'analyse générale des fonctions de hachage utilise l'approximation de l'addition par le XOR, supposant que la probabilité que les deux résultats soient égaux est égale à $1/2$. Le travail de P. Sarkar, pour lequel nous donnons quelques résultats supplémentaires, dit essentiellement que cette approximation est asymptotiquement la bonne. Plus précisément :

- quand le nombre n de sommandes est fixé, la probabilité que le i-ième bit de le somme et du XOR soient égaux a une limite quand $i \to +\infty$, égale à $1/2$ si n est pair, et à $1/2 + (-1)^{(n-1)/2}\varepsilon_n$ pour n impair ;
- $\varepsilon_n \to 0$ quand $n \to +\infty$.

En d'autres termes, en remplaçant l'addition par le XOR, on fait une bonne approximation à moins qu'il y ait un "petit" nombre impair de sommandes.

Dans ce papier, nous étudions l'approximation de l'addition par le XOR, prenant comme référence et point de départ la publication eprint 2009/047 de P. Sarkar. Dans ce travail, parmi des résultats variés, il est dit que les formules explicites semblent difficiles à trouver lorsque le nombre de sommandes est plus grand que 5. Dans la première partie de notre travail, nous montrons une façon systématique pour trouver des formules explicites : la complexité de leur calcul est $O(n^3)$, ce qui autorise de grandes valeurs de n. Nous présentons quelques calculs numériques et soulignons une observation - conjecturale - sur les coefficients.

Dans la deuxième partie, nous étudions une généralisation du travail de P. Sarkar à l'addition q-aire, au lieu de binaire. Nous montrons que le mécanisme de l'addition est essentiellement le même que celui du cas binaire. En particulier, la suite des retenues se comporte de manière très similaire : c'est une chaîne de Markov dont la matrice de transition peut être calculée. Quelques expériences sur des petites valeurs de n nous emmènent vers une conjecture, dont la première partie est intuitive et la deuxième partie révèle une surprenante coïncidence.