Analyse de complexité et de performance

Par Dina Benkirane et Zheng Long Yang

29 Avril 2019

1 Analyse Theorique

1.1

S'il $\exists$ une fonction de hachage H, alors soit H $\circ$ H et soit une x et y deux valeurs qui sont différentes. Il y a alors 2 possibilités:

1. H(x) = H(y), alors dans ce cas la nous avons une collision peu importe.
2. H(H(x)) = H(H(y)), $H(x) \neq H(y)$ nous avons une collision dans le deuxieme hachage.

Dans le cas (1) la collision n'est pas possible puisque on utilise une fonction qui est résistant aux collision.

Dans le cas (2) la collision n'est pas possible aussi, car elle se ramene au cas 1 puisque s'il n'y avait eu une collision dans le cas (1) , le deuxieme hachage revient a dire que x= H(x) et y = H(y) qui sont distinct. ce qui nous ramene au cas (1).

1.2

On a que la probabilité d'observer une collision $\lambda = \mathrm{P}(h(x_1) = h(x_2))$ tel que $x_1 \neq x_2$ avec T le nombre de message claire et $|H|$ la taille des message claires, on a la formule suivante qui permet de trouver la la probabilité de colision:

$$T = 2^{(|H|+1)/2}\sqrt{ln\left(\frac{1}{1-\lambda}\right)} \tag{1}$$

$$\frac{T}{2^{(|H|+1)/2}} = \sqrt{ln\left(\frac{1}{1-\lambda}\right)} \tag{2}$$

$$\left(\frac{T}{2^{(|H|+1)/2}}\right)^2 = ln\left(\frac{1}{1-\lambda}\right) \tag{3}$$

$$\exp\left(\frac{T}{2^{(|H|+1)/2}}\right)^2 = \left(\frac{1}{1-\lambda}\right) \tag{4}$$

$$1-\lambda = \frac{1}{\exp\left(\frac{T}{2^{(|H|+1)/2}}\right)^2} \tag{5}$$

$$\lambda = 1 - \frac{1}{\exp\left(\frac{T}{2^{(|H|+1)/2}}\right)^2} \tag{6}$$

On a alors, que pour T= 2^{510} and $|H| = 1024$,

$$\lambda = 1 - \frac{1}{\exp\left(\frac{2^{510}}{2^{(1024+1)/2}}\right)^2} \tag{7}$$

1.3

Pour choisir les parametre du crible algébrique il faut que

1. d soit de degré impair
2. $m \approx n^{1/d}$

n: un nombre premier (celui a factoriser)
m: un nombre premier
d: degré choisi du polynome

1.3.1 Example 1

Par exemple: Soit n = 45 113, alors on choisi un d arbirtraire et impair tel que

$$\text{d} = 3 \text{ et } m \approx 45113^{1/3} \approx 35,59$$

On peut alors choisir m comme étant m = 31 un nombre premier qui est proche du resultat.

$$45113 = 31^3 + 15 * 31^2 + 29 * 31^1 + 8$$

ce qui résulte avec un polynome:

$$f(x) = x^3 + 15x^2 + 29x + 8$$

1.3.2 Exemple 2

Par exemple: Soit n = 17 , alors on choisi un d arbitraire et impaire tel que:

$$\text{d} = 3 \text{ et } m \approx 17^{1/3} \approx 2.57$$

On peut alors choisir m comme étant m = 2 un nombre premier qui est proche du resultat.

$$17 = 2^3 + 2^2 + 2 * 2^1 + 1$$

ce qui résulte avec un polynome:

$$f(x) = x^3 + x^2 + 2x + 1$$

1.3.3 Exemple 3

Par exemple: Soit n = 71 , alors on choisi un d arbitraire et impaire tel que:

$$\text{d} = 5 \text{ et } m \approx 71^{1/5} \approx 2.34$$

On peut alors choisir m comme étant m = 2 un nombre premier qui est proche du resultat.

$$31 = 2^5 + 2^4 + 2 * 2^3 + 2^2 + 2^1 + 3$$

ce qui résulte avec un polynome:

$$f(x) = x^5 + x^4 + 2x^3 + x^2 + x + 3$$

1.4

Dans la génération de RSA, il faut que p et q soit premier entre eux. Ainsi pour un nombre de taille n = pq tel que n est la taille du nombre.
Il existe alors, une fonction pour compter le nombre de nombre premier approximatif pour des valeurs très grande tel que

$$\pi(x) \sim \frac{x}{ln(x)} \tag{8}$$

pour tous les nombres inférieur ou égal a x. en dérivant cette equation on se retrouve avec :

$$\pi'(x) \sim \frac{1}{ln(x)} \tag{9}$$

on cherche alors a générer 2 nombres aléatoire premier ainsi on peux multiplier par 2.

en réarangeant les équations on a que :

$$\pi'(x) \sim \frac{1}{ln(x)} \tag{10}$$

Puisque la formule d'esperance est donné par :

$$E(X) = n \times p = 2 \implies \frac{p}{2} = n \tag{11}$$

1.4.1 Cas 1

Dans le cas où n = 1024, alors on aurait que

$$n = \frac{ln(2^{1024})}{2} \approx 355\ nb\ premiers \tag{12}$$

1.4.2 Cas 2

Dans le cas où n = 2048

$$n = \frac{ln(2^{2048})}{2} \approx 710\ nb\ premiers \tag{13}$$

1.4.3 Cas 3

Dans le cas où n = 3072

$$n = \frac{ln(2^{3072})}{2} \approx 1065\ nb\ premiers \tag{14}$$

1.4.4 Cas 4

Dans le cas où n = 4092

$$n = \frac{ln(2^{4092})}{2} \approx 1418\ nb\ premiers \tag{15}$$