IFT 3275 - Sécurité Informatique

Arnaud L'Heureux

2 février 2021

Cryptanalyse Différentielle

Voici comment générer la table démontrant les fréquences des différences de sortie Δ_y (colonnes) pour chaque différence d'entrée Δ_x (lignes) :

Pour chaque différence d'entrée possible Δ_x :

- Pour chaque entrée x' possible :
  - Calculer x'' t.q. $x' \oplus x'' = \Delta_x$. Il suffit de faire ce calcul :

    $$x' \oplus \Delta_x = x''$$

    Preuve :
    $$x' \oplus \Delta_x = x' \oplus x' \oplus x'' = 0 \oplus x'' = x''$$
  - Calculer la sortie de la boîte à substitution y' correspondant à l'entrée x'. Nous devons tout simplement regarder la valeur dans la table de correspondances que nous notons :

    $$y' = S(x')$$
  - Calculer la sortie de la boîte à substitution y'' correspondant à l'entrée x''. Similairement au point précédent, nous avons :

    $$y'' = S(x'') = S(x' \oplus \Delta_x)$$
  - Calculer la différence de sortie $\Delta_y = y' \oplus y''$
- Compter combien de fois nous obtenons chaque Δ_y au point précédent. Nous inscrivons ces comptes dans les colonnes des Δ_y à la ligne Δ_x.