Cryptographie avancée – Arithmétique flottante

Précision machine :

Arrondi de représentation :

Tailles des nombres format IEEE 754 :

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Nom | Format | Taille |  |  |  |  |
| Binary32 | Simple | 32 | 8 | 24 | -126 | +127 |
| Binary64 | Double | 64 | 11 | 53 | -1022 | +1023 |
| Binary80 | Extended | 80 | 15 | 64 | -16382 | +16383 |
| Binary128 | Quad | 128 | 15 | 113 | -16382 | +16383 |

Valeur d’un nombre flottant :

Où la mantisse vaut :

Lorsque l’on fait un arrondi, on doit rester en dessous de ulp avec :

Valeurs particulières :

* +0, -0 : ou
* +, -: ,
* Not a Number: lève une exception:
  + Les Nan ne sont pas signées : ,
  + sNan: ,
  + qNan: ,
* Dénormalisés: ,

L’ordre des opérations en flottants a une importance.