L'aléatoire en informatique

Tom Lecoq

2024-02-14

1 Introuction

J'ai toujours aimé les jeux de hasard, que ce soit le poker, le blackJack ou encore la roulette. Mais lorsque je vais au casino je prefère toujours jouer sur table avec un croupier car je n'ai aucune confiance en la génération aléatoire des machines. C'est pour cela que je souhaite réaliser ce rapport sur les moyens de générer aléatoirement des nombres en informatique. Bien que le concept d'aléatoire parle à n'importe quel humain, il est bien plus difficile de l'apréhender pour un ordinateur par définition déterministe (Chantrel 2021). Cela signifie qu'il répondra toujours de la même manière à un problème qu'on lui pose. Par conséquent l'aléatoire n'a pas sa place dans un algorithme.Il existe cependant des moyens de générer des valeurs plus ou moins aléatoires informatiquement et c'est ce que nous verrons au sein de ce rapport.

2 Application de l'aléatoire en informatique

A l'air du digitale au tout est informatisé, il est parfois nécessaire de générer des valeurs aléatoires. C'est le cas par exemple lorsque l'on veut simuler un jeu de hasard, tirage de dés, poker électronique, roulettes etc. La garantie du phénomène aléatoire devient encore plus importante lorsque l'on parle de jeux d'argent. Certains jeux vidéos font également intervenir des situations aléatoires. Dans le secteur de la sécurité informatique cette question est également cruciale car tout l'intéret de chiffrer des données est d'empêcher un potentiels attaquant de prévoir les valeurs prisent par l'algorithme afin de protéger les clés secrètes de code d'authentification par exemple. En cryptographie on parle de nonces qui sont des valeurs aléatoires à usages uniques.

3 Le pseudo-aléatoire

3.1 Définition

C'est le plus courament employé, l'ordinateur utilise ses paramètres internes comme par exemple l'horloge qu'il transforme grâce à des fonctions mathématiques en valeurs pseudo-aléatoires. Parmi les fonctions de GNPA (génération de nombres pseudo aléatoires) on retrouve notament BCryptGenRandom sur Windows, Get-Random() sur Linux ou encore Math.random() en javascript. Ces fonctions sont qualifiées de non cryptographiquement sécurisées, ce qui signifie qu'elles peuvent être utilisées pour un usage non critique mais en aucun cas à des fins de sécurité. Dans le cas de l'utilisation de l'horloge, elle génère une entropie externe casi nulle. En informatique, l'entropie, c'est la mesure de la quantité de hasard d'une séquence de bits ("Générez Des Nombres Aléatoires" n.d.). Plus l'entropie est élevée, plus il est difficil de prévoir la valeur de cette séquence de bits. On peut également définir une graine qui sera ensuite traitée par une fonction GNPA pour générer une nouvelle valeur plus ou moins aléatoire selon la méthode utilisée.

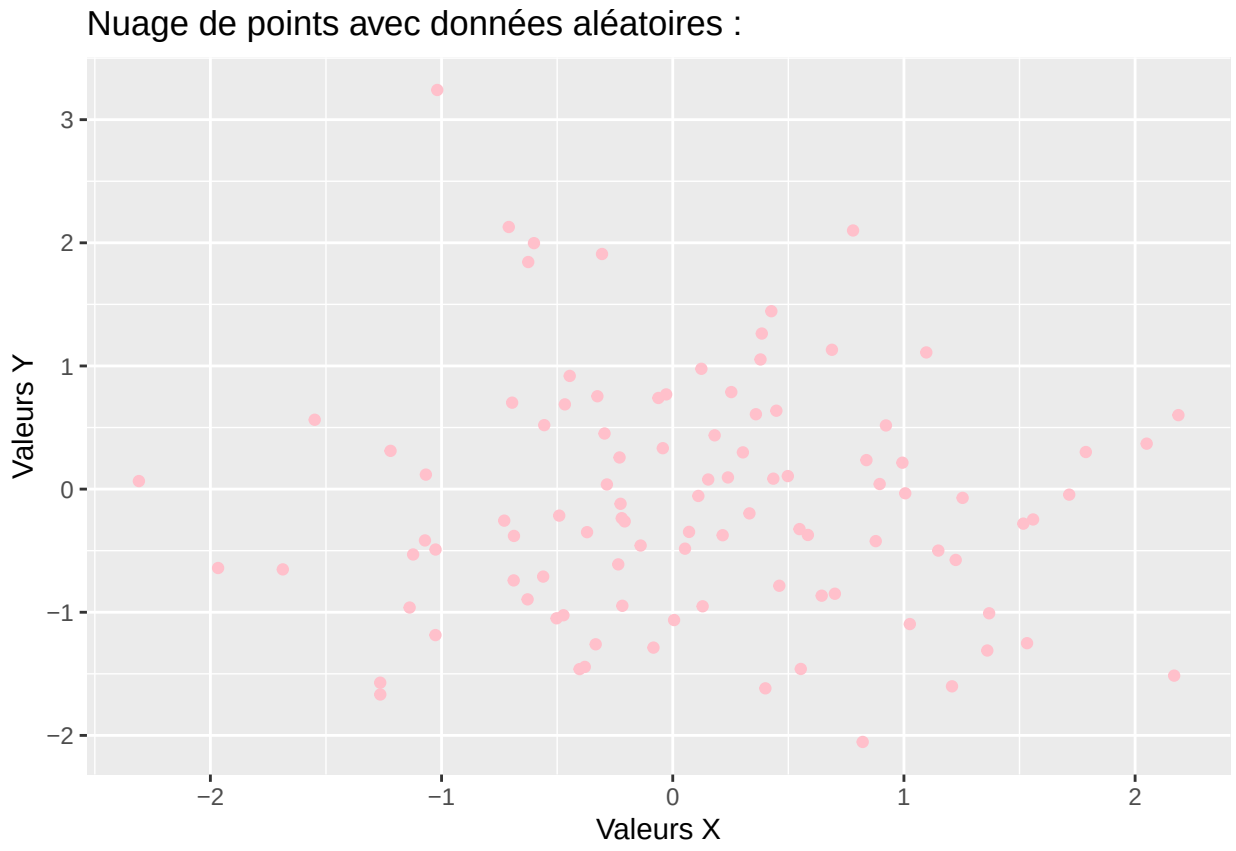
3.2 Graphique

```r
# Charger la library ggplot2
library(ggplot2)

# Définir la graine aléatoire pour la reproductibilité
set.seed(123)

# Générer des données aléatoires
data <- data.frame(x = rnorm(100), y = rnorm(100))

# Créer un graphique
ggplot(data, aes(x = x, y = y)) +
  geom_point(color = "pink") +
  ggtitle("Nuage de points avec données aléatoires :") +
  xlab("Valeurs X") +
  ylab("Valeurs Y")
```



4 Le vrai aléatoire

4.1 Définition

Afin de répondre au problème de la possibilité de prévoir les valeurs, l'ordinateur est également capable de générer des valeurs dites réellement aléatoires donc plus sécurisées. Cepandant seul, l'ordinateur reste dans sa logique deterministe, il utilise alors des phénomènes physisques externes comme source d'entropie générant bien plus de hasard qu'un de ses paramètres internes. Le logiciel PGP utilise par exemple la position de la souris ("Générez Des Nombres Aléatoires" n.d.). Dans le cas de serveur, qui ne possèdent donc pas de périphériques externes, ils utilisent des paramètres physique tels que la température d'un composant ou encore le bruit électromagnétique (Guignant 2018). Dans le futur on pourrait immaginer un ordinateur qui tirerait son entropie de lois de la physique quantique, en effet il est impossible de prévoir la vitesse de désintégration d'un atome. Ainsi, grâce à ce modèle probabiliste, l'ordinateur génèrerait des valeurs parfaitement aléatoires ("Pourquoi l'aléatoire n'existe Pas En Informatique ? - Blog" n.d.).

4.2 Les limites

La génération de nombre réellement aléatoire peut parfois prendre très longtemps et consomme une grande quantité de ressources. Ainsi, dans la plupart des cas, on utilise ce type de fonctions afin de générer la graine dont se serviront les fonctions pseudo aléatoires pour créer le reste de la clé de sécurité. Ainsi cette graine apporte l'entropie qu'il manque aux GNPA pour être suffisament sûres.

5 Conclusion

Pour conclure, un ordinateur par nature deterministe, n'est pas capable de générer une valeur aléatoire mais peut générer des valeurs plus ou moins difficiles à prévoir en fonction de la quantité d'entropie extérieure qu'il utilise. Pour la génération de valeurs dites pseudo aléatoires, l'ordinateur utilise des paramètres internes comme l'horloge en guise de source d'entropie. Cependant, si le pseudo aléatoire fonctionne pour une utilisation commune, il reste malgrès tout trop prévisble pour un logiciel malveillant pour une utilisation comme clé de sécurité ou dans le cadre de jeux d'argent. Dans ces cas là, il faut utiliser des fonctions bien plus couteuses en ressources se basant sur des paramètres physiques externes comme source d'entropie afin de générer des valeurs presque totalement aléatoires.

Bibliographie

Chantrel, Bastien. 2021. "Ordinateurs Et Aléatoire : Le Hasard Existe-t-Il ?" *Cortex*. https://www.le-cortex.com/media/articles/ordinateurs-et-aleatoire-le-hasard-existe-t-il.

"Générez Des Nombres Aléatoires." n.d. *OpenClassrooms*. Accessed February 17, 2024. https://openclassrooms.com/fr/courses/1757741-securisez-vos-donnees-avec-la-cryptographie/6031863-generez-des-nombres-aleatoires.

Guignant, Arnaud. 2018. "Comment Un Ordinateur Génère Un Nombre Aléatoire ?" *Arnaud Guignant*. https://gafish.fr/comment-un-ordinateur-genere-un-nombre-aleatoire/.

"Pourquoi l'aléatoire n'existe Pas En Informatique ? - Blog." n.d. *Code-Garage*. Accessed February 17, 2024. https://code-garage.fr/blog/pourquoi-aleatoire-n-existe-pas-en-informatique.