Construction d'un générateur de nombres aléatoires

Les nombres aléatoires sont très importants dans le monde moderne. En informatique, on les retrouve à de nombreux niveaux, en particulier en cryptographie où ils sont par exemple utilisés pour sécuriser les mots de passe ou les communications.

Il n'est pas possible pour de telles applications d'utiliser les générateurs de nombres pseudo-aléatoires, fournis par exemple avec la bibliothèque standard du langage C, compte tenu de la nature prédictive des valeurs. En effet, à partir d'une graine initiale u_0 que l'on peut modifier (avec la fonction `srand()`), la suite u_n des valeurs fournies par la fonction `rand()` est définie par $u_{n+1} = (a \times u_n + b) \bmod 2^k$ où les valeurs de a et b ont été judicieusement choisies pour que la suite apparaisse la plus aléatoire possible et qu'une même valeur ne revienne au mieux que tous les 2^k tirages, k étant la taille (en bits) d'un entier sur la machine. Connaissant une valeur, une connait facilement les suivantes.

L'objectif de ce projet est de construire un générateur de nombres vraiment aléatoires avec de bonnes propriétés. Des solutions existent déjà, comme par exemple récupérer la température du CPU d'un ordinateur ou encore l'utilisation de lampes à lave comme sur la figure ci-dessous. Malheureusement, ces solutions n'ont pas de bonnes propriétés. Pour les exemples donnés, la température d'un CPU ne varie pas forcément beaucoup au cours du temps et l'intervale des valeurs possibles est relativement faible ; l'utilisation des lampes à lave consomme beaucoup d'énergie et n'est donc pas vraiment *green*.

Dans le cadre de ce projet, le générateur aléatoire pourra basé sur un arbre à vent, devra fournir des nombres aléatoires à intervalles réguliers et potentiellement très rapprochés, et avoir un impact écologique faible (basse consommation d'énergie, matériaux renouvelables, etc.). Les nombres aléatoires ainsi produits devront être accessibles en ligne *via* une API simple.

En fin de projet, le générateur de nombres aléatoires devra être opérationnel, c'est-à-dire physiquement contruit, et un mini site web (écrit avec HTML et PHP) devra être réalisé pour accéder aux nombres générés.

Contact : Éric Renault
Email : `eric.renault@esiee.fr`