Pierre Dusart ⋆ **Etude du générateur aléatoire BBS**

Résumé : Le générateur BBS est un algorithme standard proposé par le NIST. Il est basé sur des calculs de carrés modulaires.

Travail à faire : L'objectif est de comprendre la formalisation des notions statistiques (imprédictibilité, ...) et les outils de performance (période de la suite, rapidité, ...) Une mise en oeuvre avec des exemples est demandée.

Références :

- `https://fr.wikipedia.org/wiki/Blum_Blum_Shub`
- Lenore Blum, Manuel Blum, et Michael Shub. "A Simple Unpredictable Pseudo-Random Number Generator", SIAM Journal on Computing, volume 15, pages 364–383, mai 1986.