NSU-2023-T06L2e01

32-битный генератор псевдослучайных чисел Блюм-Блюма-Шуба

Алгоритм Блюм-Блюма-Шуба (BBS), названный по фамилиям изобретателей – интересная техника, практически применяемая в области защиты данных. Для криптографических задач полезно генерировать серии чисел, выглядящие и ведущие себя, как если бы они были оцифрованным случайным шумом. В Википедии и других публикациях можно найти дополнительную информацию. Однако, это упражнение не зависит от вашего понимания тонкостей теории чисел, на которых основан алгоритм. Вот что вам требуется сделать

Последовательность BBS начинается с произвольного числа, называемого ключом (в английском языке это число обычно называют seed), которое мы будем обозначать a_0. Генератор имеет тактовую частоту, и он производит 32-битное выходное значение a_k на каждом цикле с номером k по следующей формуле:

$$a_k = a_{k-1}^2 \bmod M$$

Здесь, $p \bmod q$ – это остаток от деления p на q, например $10 \bmod 3 = 1$, $8 \bmod 4 = 0$, и т.д.

Выбор значения M очень важен для безопасности и других свойств генератора. Однако, мы заинтересованы только в проектировании устройства, поэтому мы выберем достаточно хорошее число $52999 \times 56299 = 2983790701$ (причины, по которым это число можно считать хорошим, требуют знания теории чисел). Это число представляется при помощи 32 бит и обеспечивает длинную труднопредсказуемую (особенно если противник не знает, что M – произведение именно этих чисел) последовательность.

Подробности дизайна

Используйте один 32-битный регистр для текущего значения a. Включите в ваш дизайн умножитель и делитель из библиотеки *Arithmetics*.

Заметьте, что умножитель может перемножать два 32-битных числа и выдает 64-битный результат двумя порциями. Аналогично, делитель делит 64-битное делимое на 32-битный делитель, порождая 32-битное частное и 32-битный остаток.

Ваше устройство должно ввести ключ на цикле 0 и произвести 15 результатов на последующих тактах, поднимая сигнал `stop` в конце 15-го такта.

Как отправлять вашу работу на проверку

Не перемещайте входные и выходные контакты, потому что Logisim присоединяет к ним тестовую схему, основываясь на их положении, а не по имени (это неудобно, но мы ничего не можем с этим сделать). Если вы хотите, вы можете присоединить туннели к контактам и разместить другие концы туннелей в удобные для вас места на макетной плате. Таким образом, вы можете размещать вашу схему удобным для вас образом и, в то же время, быть уверенными, что тестирующий робот будет правильно подсоединен к схеме.

Проверьте устройство, нажимая входные контакты при помощи ручных контролов и записывая ваши наблюдения. Ответьте на это сообщение, присоединив файл схемы с вашим решением.