# Описание лавинного эффекта.

Батарин Егор

По определению, хэш-функция обладает свойсвом лавинного эффекта, если при изменении одного бита входной последовательности меняется в среднем половина битов выходной последовательности. Цель проекта - проверить, выполняется ли данный критерий для алгоритма Keccak.

Для этого в проекте генерируются пары строк, отличающихся на один бит - входные последовательности. Далее сравнимаются выходные последовательности и считается количество измененных бит. По полученным данным строятся графики, на оси абсцисс которых отображен процент измененных бит, а ось ординат выражает меру количества таких строк. Стоит ожидать, что максимум графика будет достигаться при 50%.

Ниже приведена таблица, которая в зависимости от размера хэша и количества проведенных раундов показывает среднее значение модифицированных бит в процентах.

| Размер хэша | Число раундов | | | | | | |
|---|---|---|---|---|---|---|---|
| | 1 | 2 | 3 | 4 | 8 | 12 | 24 |
| 224 | 37.995 | 48.504 | 50.041 | 50.151 | 50.196 | 49.882 | 49.882 |
| 256 | 36.716 | 48.32 | 49.991 | 49.875 | 50.067 | 50.102 | 50.045 |
| 384 | 37.689 | 48.609 | 50.03 | 49.949 | 50.092 | 49.997 | 50.003 |
| 512 | 40.136 | 49.256 | 50.072 | 49.996 | 49.979 | 49.999 | 49.981 |

Как видим, уже начиная с числа раундов, равным 3, лавинный эффект проявляется в полной мере.

По графикам также можно сделать два качественных заключения по распределению доли модифицированных бит. Во-первых, начиная с третьего раунда, распределение очень хорошо аппроксимируется нормальным, как видно из картинки ниже.

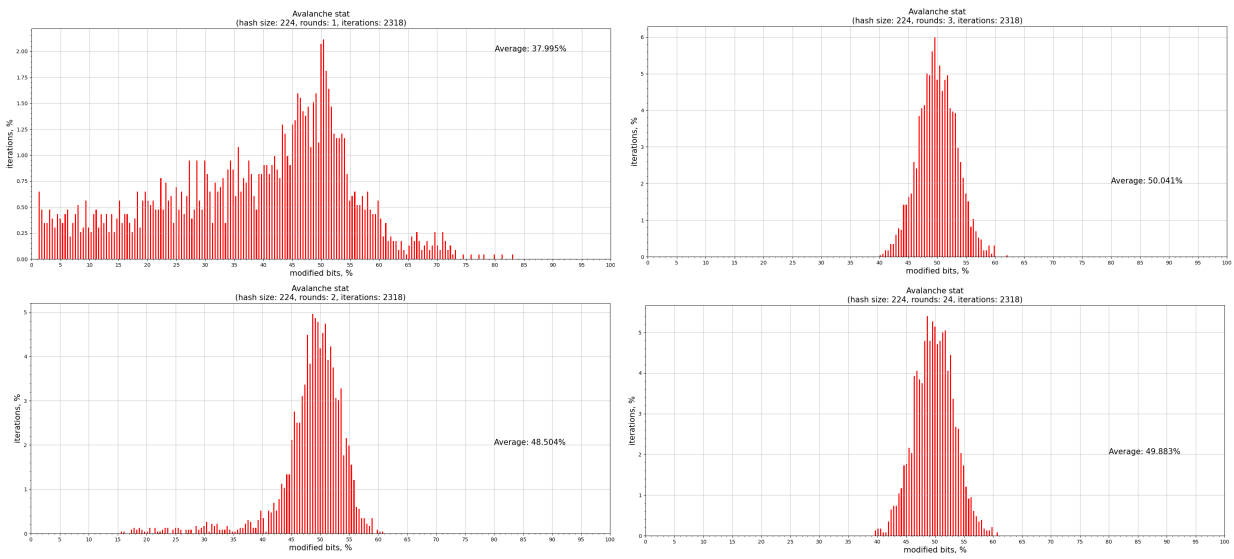


Рис. 1: Хэш 224 бита с числом раундов 1, 2, 3 и 24

Во-вторых, чем выше размер хэша, чем меньше дисперсия нормального распределенения. Ниже сравнение хэшей 224 и 512 бит с числом раундов, равным 24.

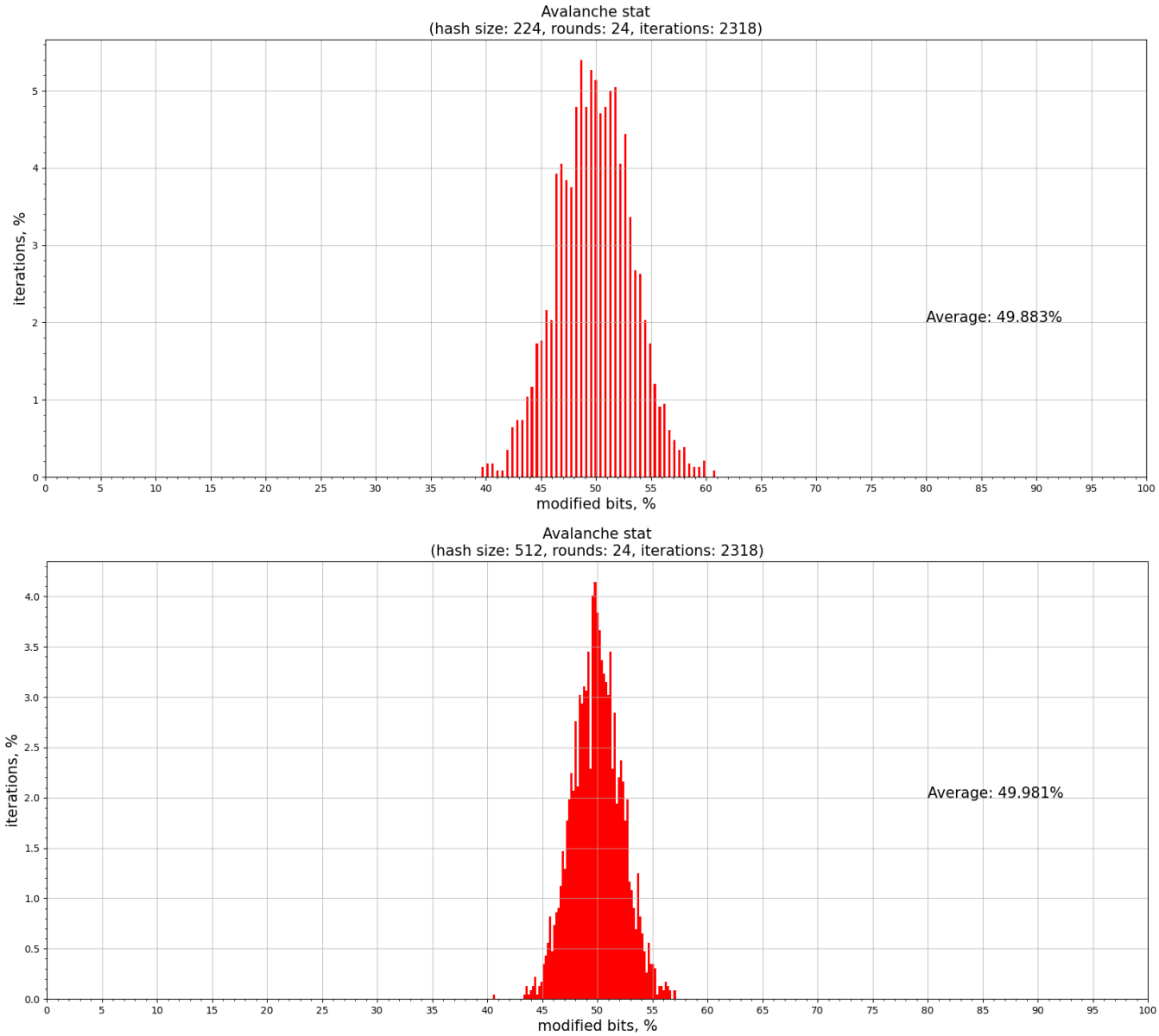


Рис. 2: Хэш 224 бита с числом раундов 1, 2, 3 и 24