E.1.4 Potential Bias Due to Modular Arithmetic for Curves Over F_p

Given an integer x in the range 0 to 2^N-1, the r^{th} bit of x depends solely upon whether $\left\lfloor \frac{x}{2^r} \right\rfloor$ is odd or even. If all of the values in this range are sampled uniformly, the r^{th} bit will be 0 exactly ½ of the time. But if x is restricted to F_P, i.e., to the range 0 to p-1, this statement is no longer true.

By excluding the $k = 2^N - p$ values p, p+1, ..., 2^N –1 from the set of all integers in Z_N, the ratio of ones and zeroes in the r^{th} bit is altered from $2^{N-1} / 2^{N-1}$ to a value that can be no smaller than $(2^{N-1} - k)/ 2^{N-1}$. For all the primes p used in this Recommendationt, $k/2^{N-1}$ is smaller than 2^{-31}. Thus, the ratio of ones and zeroes in any bit is within at least 2^{-31} of 1.0.

To detect this small difference from random, a sample of 2^{64} outputs is required before the observed distribution of 1's and 0's is more than one standard deviation away from flat random. This effect is dominated by the bias addressed below in section E.2.