PRNG mul xor PRNG