1- The old issue has been addressed. It does not generate [1,1] in factorization. The problem was that each bin was not padded properly.

2- It does not uses any Paillier instances to generate a random value.

3- For the set element size s (e.g. 32) we only need extra 8 bits, so we can safely pick 2d+1 random x\_i values from that range, where d is a bin’s capacity. For instance, when d=100, then we need 201 x\_i values and 2^8 provides all those values.