I read the article of the probability of an attacker that takes over a shard is (https://github.com/ethereum/wiki/wiki/Sharding-FAQ#how-is-the-randomness-for-random-sampling-generated)

$X =$

where N is the size of a sample and p is the percentage of attackers in the pool. This could work if there is only one shard. However, in the case of M shards in the network, the attack probability of at least one shard

being attacked in the M shards (i.e., 1 - P(all shards are safe)) should be (assuming the random variables of all shards being attacked are i.i.d.)

$Y = 1 - (1 - X)^M$, which is about $X * M$ if X is small.

E.g., if $N = 150$, $p = 0.333333$, and $M = 1024$, then

$X = 1.83e-5$

while

$Y = 0.0185$

Should the security level of random sampling with sharding work like this? I searched for several ETH2.0 documents but cannot find related explanation.