## failure probability of ciphertexts

