failure probability of ciphertexts