Modern Industry Single Key Key Size or Symmetric Key Sizes

In modern industry, symmetric encryption’s key have 3 specific key sizes which are 128 bits, 192 bits and 256 bits.

128 bits refer to there are 128 reserve spaces that can store either all 1 or all 0 or a combination of 0 and 1. The same goes for 192 bits and 256 bits.

In symmetric encryption, they accept any key values with different range as shown below.

128 bits accept value starting from “0” to “340282366920938463463374607431768211455” (2^128 – 1 or 2 to the power of 128 -1) Considering that your key was chosen at random which has the value of “170141183460469231732840225220490952705”. Any attacker has to start from 0 then increment it by 1 until it reaches the value that you use for encryption and decryption. In average an attacker has to go through “340282366920938463463374607431768211456” (2^128 or 2 to the power of 128) different combinations or possible values which is not doable and even if it’s doable, the time needed for them to do so will be consider as life time of a universe. If the attacker was lucky (99% out of 100%) perhaps they only need to go through “170141183460469231731687303715884105728” (2^127 or 2 to the power of 127) different combinations or possible values. If the attacker was extremely lucky (1% out of 100%), the attacker only need to go through “18446744073709551616” (2^64 or 2 to the power of 64) different combinations or possible values.

192 bits and 256 bits act in a similar way like 128 bits.

When big alien quantum computer comes, 256 bits of symmetric encryption key size is enough to withstand the quantum computer. The average combinations or possible values that an attacker or hacker have to go through was reduced by 50%.