Assumptions

C code:

- The rand() function is commented out and replaced by a constant value to evaluate results with the same behavior.

- All calculations are exploiting uint64_t type which forces the k to be less equal than 64.

- The A2Bq and B2Aq functions are implemented based on 2 shares. Therefore, results for these two operations are reported when n is equal to 2.

- For A2Bq and B2Aq, 2 first shares of x are passed as inputs.

VHDL code:

- All random number are replaced by a constant value.
- Concatenation of shares is assigned to the input as a STD_LOGIC_VECTOR (e.g. for 4 shares: X= x[4] & x[3] & x[2] & x[0] where & stands for concatenation).