Assumptions

C code:

- The rand() function is commented out and replaced by a counter 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.

VHDL code:

- For simplicity, Random Number generator is replaced by a counter.
- Concatenation of shares is assigned to the input as an STD_LOGIC_VECTOR (e.g. for 4 shares: X= x[4] & x[3] & x[2] & x[0] where & stands for concatenation).