# SUMMARY (LIZARD):

After going through the first round of reading:

(1). LIZARD is a modified version of Grain.

(2). While already used stream cipher has n/2 security level, LIZARD operates at 2/3n level of security.

(3). As most of the cipher depends on continuous evaluation of the key while LIZARD taps at selected interval.

(4). LIZARD uses different sets of NFSR as opposite to the GRAIN cipher using a bit value of 31 and the other uses 80 bit key stream.

(5). LIZARD offers better hardware efficiency and operates at low power level.

(6). LIZARD operates at the FP-(1) mode and guarantees a hardware security of (2^31) -1.

(7). While most cipher use only one key to encrypt, LIZARD uses two key additions.

(8). State initialisation of LIZARD takes place in the following steps:

* **Key and IV loading**- 120 bit key and 64 bit public key.
* **Mixin**g- Uses grain like mixing.
* **Second Key addition.**
* **Final Diffusion.**

(9). The next part involves generation of a key stream using non-linear XOR operation of the NFSR1 and the NFSR2 values.