Topics for Home Assignment

Virendra Sule

September 21, 2021

Topics for Home Assignment to be submitted I

- Weighted 20 marks.
- A single PDF file must be submitted.
- Deadline: Last day before start date of End Sem exam. The deadline will be updated in the assignment post of the EE720 team.
- Choose one of the following topics
  1. Trivium stream cipher.
  2. Grain stream cipher.
  3. Any other published stream cipher of your choice.
- Study the cipher you have chosen from sources on internet or the e-Stream cipher book. Write a brief description of the algorithm and its mathematical model in the form

$$\begin{array}{lccc} \text{State update map} & x(k+1) & = & F(x(k)) \\ \text{Output map} & w(k) & = & f(x(k)) \end{array}$$

Topics for Home Assignment to be submitted II

- Construct a reduced size analog of the cipher by choosing the feedback and output functions in reduced variables and write the mathematical model of the reduced cipher. Reduced analog of the cipher is constructed by reducing the register lengths and choosing the bits in the register for feedback or output connections. Similarly by writing analogous output function of reduced number of variables and degree. The key length and number of bits in IV will also gets reduced accordingly.
- The reduced model should not have less than 32 bits of states.
- Develop a Sagemath code for generating the output stream of the reduced model of the cipher.

Topics for Home Assignment to be submitted III

- For these 100 randomly different IVs and same key compute the linear complexity profiles of each of the output streams upto length 1024, assuming the streams to be periodic after 1024 bits.

Note: Reduced cipher models have enormous variations hence it is not expected that two assignments will have identical reduced models. You are urged not to copy eachother's models. Even if you discuss your reductions make your own variation and develop a distinct model.