Introduction

A finite state machine, is a mathematical model of computation used to design both computer programs and sequential logic circuits [1]. Sequential logic is used to construct linear-feedback shift registers. They are divided into one-to-many and many-to-one types [2]. Our linear-feedback shift register has many-to-many configuration. It generates the Galois field different from finite field formed Galois linear-feedback shift register. The paper is structured as follow: section 2 gives a brief introduce to the principles of a linear-feedback shift register; section 3 describes our principle of a many-to-many configuration and discusses some issues related with its implementation on a finite state machine; finally, section 4 briefly shows inference for appropriate primitive polynomial.