ABSTRACT

Stream ciphers play an important role in cryptographic applications where the resources are at a premium. eSTREAM project was a multi-year effort to identify new stream ciphers for wide adoption. Trivium, one of the finalists of eSTREAM project, is shown to be vulnerable against fault attacks. Differential fault analysis and a number of its variants pose a major threat against Trivium which exploits the weakness in nonlinearity and reversibility of the cipher. This thesis analyses the fault attacks on Trivium and show how Cellular Automata (CA) based stream ciphers can effectively be deployed to prevent these attacks. In general, CA based stream ciphers use three-neighbourhood CA which are widely studied and accepted as suitable cryptographic primitive. A 3-neighbourhood nonlinear CA with rule 30 was proposed as an ideal candidate for cryptographic primitive but was later shown to be vulnerable. The cryptographic properties like diffusion and randomness increase with increase in neighbourhood radius and thus open the possibility of exploring the cryptographic properties of 4-neighbourhood CA. We explore whether 4-neighbourhood CA can be a better cryptographic primitive. We construct a class of cryptographically suitable 4-neighbourhood nonlinear CA rules that resembles rule 30 and study its cryptographic properties. Four-neighbourhood nonlinear CA are shown to be resistant against Meier-Staffelbach attack on rule 30, justifying the applicability of 4-neighbourhood CA as better cryptographic primitives. We use 4-neighbourhood CA to design a fault-resistant CA based cipher which is also shown to be secure against other major attacks.

Keywords: *Cellular Automata, Stream Cipher, Fault Attack, 4-neighbourhood CA, nonlinear CA rules, cryptographic properties of CA, CA rule 30*