**Thesis Title:**
**Side Channel Attacks on Stream Ciphers and Countermeasures**
**Author: Sandip Karmakar**

## Abstract:

With the advent of electronic commerce and portable devices for communications, cryptography has become an exceedingly important science in the present day. Communications by and large take place through insecure channels. Hence, cryptography becomes a necessity and as well as a challenge in modern day communications. Other than mathematical strength, cryptographic algorithms need to prevent implementation attacks. The implementation attacks are broadly known as the side channel attacks and are the topic of current research. The side channel attacks explored in this research work are, scan based side channel attacks and fault attacks. The countermeasures use the random behaviour of Cellular Automata. Fault attacks are one of the most efficient forms of side channel attack against implementations of cryptographic algorithms. In this attack, faults are injected during cipher operations. The attacker then analyzes the fault free and faulty cipher-texts to deduce partial or full value of the secret key. The literature shows that both the block ciphers and stream ciphers are analyzable using fault attack. However, stream ciphers have not been vastly explored. The current research focuses the vulnerability of stream ciphers against fault attacks. We investigate fault attacks on eStream winners, in particular, the Grain and MICKEY family of ciphers. Scan-chain based attack is another kind of side channel attack, which targets one of the most important features of today's integrated circuit hardware - the test circuitry. Design for Testability (DFT) is a design technique that adds certain testability features to a hardware design. On the other hand, this very feature opens up a side channel for cryptanalysis, rendering crypto-devices vulnerable to scan-based attack. We again explore eStream winners, Trivium, Grain and MICKEY under scan based side channel attacks. The attacks need to be protected. Hence, another area of this research is development of countermeasures for side channel attacks in general and scan attack, fault attack in particular. In this respect, our research proposes a variety of countermeasures against different type of side channel attacks. The proposals are to prevent scan attacks, fault attacks and power attacks using Cellular Automata. The pseudorandom behaviour of Cellular Automata can be employed to generate good masking and scrambling algorithms to thwart side channel attacks on stream ciphers.

**Keywords:** Fault Attack, Scan Attack, eStream ciphers, Grain, MICKEY, Side Channel Attacks, Countermeasures to side channel attacks.