CORR 2001-11

Efficient Implementation of "Large" Stream Cipher Systems

Palash Sarkar and Subhamoy Maitra*

Abstract A standard model of stream cipher combines the outputs of several independent Linear Feedback Shift Register (LFSR) sequences using a nonlinear Boolean function to produce the keystream. Here we present a low cost hardware architecture for such secret-key cryptosystems using a relatively large number of LFSRs. We propose implementation of the LFSRs using Cellular Automata in VLSI. This provides a regular and uniform two dimensional array of flip flops with only local interconnections. The main bottleneck in the implementation of stream ciphers using a relatively large number of LFSRs is the implementation of the combining Boolean function. We show that this bottleneck can be removed and it is feasible to implement "large" cryptographically secure Boolean functions using a reconfigurable pipelined architecture.

Keywords Stream Ciphers, Boolean functions, Linear Feedback Shift Registers, Cellular Automata, Reconfigurable Hardware, Pipelined Architecture.