CORR 2001-40

Low Cost Hardware Architecture for Secure Stream Cipher Cryptosystems

Palash Sarkar & Subhamoy Maitra*

Abstract We design low cost hardware architecture for secure stream cipher cryptosystems. Our architecture provides the first practical method of implementing state-of-the-art theoretical constructions of secure Boolean functions suitable for stream ciphers. Using a pipelined architecture, we show that it is possible to implement systems which use Boolean functions of a relatively large number (around 24) of variables. Our architecture is reconfigurable and provides a universal circuit for a certain class of secure Boolean functions. We also propose the use of Cellular Automata to replace the Linear Feedback Shift Registers in stream ciphers. This provides certain design advantages without affecting the overall security of the system. We present concrete real-life designs of an 8-variable and a 24-variable stream cipher system.

Index Terms Cryptography, Stream Cipher, Boolean functions, Linear Feedback Shift Register, Cellular Automaton, Reconfigurable Hardware, Pipeline Architecture.