Fully Parallel Implementation of the MK Transformation Encryption Algorithm on FPGA

By Werner, Gordon

Authenticated encryption (AE) algorithms provide both data security and integrity. While a number of AE algorithms exist, they can prove inefficient and difficult to use. Recent efforts have focused on the development of secure, efficient and easy to use AE algorithms. MK-3 is one such algorithm; developed through a joint effort between Rochester Institute of Technology (RIT) and the Harris Corporation. The algorithm uses the duplex construction, which builds on the sponge primitive popularized by Keccak, the SHA-3 competition winner. MK-3 is intended for hardware implementations; its novelty is the use of 16-bit substitution boxes as opposed to the 8-bit set used by the Advanced Encryption Standard (AES). In this paper we introduce a fully parallel hardware implementation of MK-3 on Field Programmable Gate Arrays (FPGAs) as well as lay the groundwork for future design optimizations.

Biography

Gordon Werner is a second year Ph.D. student in the B. Thomas Golisano College of Computing & Information Sciences. His research focuses on the development and implementation of authenticated encryption algorithms in hardware as well as their applications in secure computing systems.