Title: Generalizations And Algebraic Structures of The Grøstl-based Primitives

Abstract: With the large scale proliferation of networked devices ranging from medical implants like pacemakers and insulin pumps, to corporate information assets, secure authentication, data integrity and confidentiality have become some of the central goals for cybersecurity. Cryptographic hash functions have many applications in information security and are commonly used to verify data authenticity. Our research focuses on the study of the properties that dictate the security of a cryptographic hash functions that use Even-Mansour type of ciphers in their underlying structure. In particular, we investigate the algebraic design requirements of the Grøstl hash function and its generalizations. Grøstl is an iterated hash function with a compression function built from two distinct permutations, crucial for preserving its security. Grøstl is one of the five finalists in the recent NIST SHA-3 competition and is the hash function that probably received the most intense cryptanalysis during the competition. Its elegant design and simplicity inspires continued high interest in the security features of this hash function.