Research on hash functions based on controlled substitution-permutation networks and their application in authenticated text encryption.

Mithpasa Phoumivong

Abstract: This thesis investigates the construction of hash functions based on controlled substitution-permutation networks (CSPNs) and their application in authenticated encryption for text. While conventional hash functions rely on fixed, static structures, CSPNs introduce dynamic, data-dependent transformations, enhancing cryptographic strength against differential and linear cryptanalysis. The research proposes a novel design methodology where control signals, derived from the input message, dynamically reconfigure the substitution and permutation layers at each round. This approach significantly increases the complexity of collision and preimage attacks. Furthermore, the study develops an authenticated encryption scheme integrating the proposed CSPN-based hash function, ensuring both data confidentiality and integrity. Security analysis demonstrates that the construction achieves strong avalanche effects and resistance to known attacks. Performance evaluations indicate competitive efficiency compared to standard algorithms. The findings contribute a robust, adaptable framework for designing lightweight cryptographic primitives suitable for resource-constrained environments, offering a viable alternative for secure text authentication and encryption.

Keywords: hash functions, substitution-permutation network, controlled operations, authenticated encryption