CORR 2001-54

A Parallel Algorithm for Extending Cryptographic Hash Functions

Palash Sarkar and Paul J. Schellenberg

Abstract We describe a parallel algorithm for extending a small domain hash function to a very large domain has function. Our construction can handle messages of any practical length and preserves the security properties of the basic hash function. The construction can be viewed as a parallel version of the well known Merkle-Damgård construction, which is a sequential construction. Our parallel algorithm provides a significant reduction in the computation time of the message digest, which is a basic operation in digital signatures.

Keywords cryptographic hash function, Merkle-Damgård construction, parallel algorithm, collision resistance.