CORR 2002-19

Message Authentication Codes with Error Correcting Capabilities

Charles C.Y. Lam, Guang Gong*, & Scott Vanstone

Abstract In this paper, we propose classes of Message Authentication Codes (MAC) based on error correcting-codes. We introduce a new notion of error tolerant forgery of has messages. The classes of the keyed hash functions are highly secure, and proved the capabilities of correcting errors on transmission, including burst-errors, which is a typical phenomenon in wireless communications. These classes of hash functions are easily implementable in hardware by means of simple linear feedback shift register structures.