Cryptology ePrint Archive: Report 2011/705

Differential Attacks on Generalized Feistel Schemes

Valerie Nachef and Emmanuel Volte and Jacques Patarin

Abstract: While generic attacks on classical Feistel schemes and unbalanced Feistel schemes have been studied a lot, generic attacks on severa generalized Feistel schemes like type-1, type-2 and type-3 and Alternating Feistel schemes, as defined in~\cite{HR}, have not been systematica investigated. This is the aim of this paper. We give our best Known Plaintext Attacks and non-adaptive Chosen Plaintext Attacks on these sche and we determine the maximum number of rounds that we can attack. It is interesting to have generic attacks since there are well known block c networks that use generalized Feistel schemes: CAST-256 (type-1), RC-6 (type-2), MARS (type-3) and BEAR/LION (alternating). Also, Typ and Type-2 Feistel schemes are respectively used in the construction of the hash functions $Lesamnta$ and $SHAvite-3_{512}$.

Category / Keywords: secret-key cryptography / generalized Feistel schemes, generic attacks on encryption schemes, block ciphers

Date: received 26 Dec 2011, last revised 27 Dec 2011

Contact author: valerie nachef at u-cergy fr