

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 several generalized Feistel schemes like type-1, type-2 and type-3 and Alternating Feistel schemes, as defined in~\cite{HR}, have not been systematically investigated. This is the aim of this paper. We give our best Known Plaintext Attacks and non-adaptive Chosen Plaintext Attacks on these schemes 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 cipher networks that use generalized Feistel schemes: CAST-256 (type-1), RC-6 (type-2), MARS (type-3) and BEAR/LION (alternating). Also, Type-1 and Type-2 Feistel schemes are respectively used in the construction of the hash functions \$Lesamnta\$ and \$SHA\text{vite-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

Available formats: [PDF](#) | [BibTeX Citation](#)

Version: 20111227:181632 ([All versions of this report](#))

Discussion forum: [Show discussion](#) | [Start new discussion](#)

[[Cryptology ePrint archive](#)]