Cryptology ePrint Archive: Report 2011/496

On the Public Indifferentiability and Correlation Intractability of the 6-Round Feistel Construction

Avradip Mandal and Jacques Patarin and Yannick Seurin

Abstract: We show that the Feistel construction with six rounds and random round functions is publicly indifferentiable from a random invertible permutation (a result that is not known to hold for full indifferentiability). Public indifferentiability (pub-indifferentiability for short) is a variant of indifferentiability introduced by Yoneyama et al. \cite{YoneyamaMO09} and Dodis et al. \cite{DodisRS09} where the simulator knows all queries made by the distinguisher to the primitive it tries to simulate, and is useful to argue the security of cryptosystems where all the queries to the ideal primitive are public (as e.g. in many digital signature schemes). To prove the result, we introduce a new and simpler variant of indifferentiability, that we call sequential indifferentiability (seq-indifferentiability for short) and show that this notion is in fact equivalent to pub-indifferentiability for stateless ideal primitives. We then prove that the 6-round Feistel construction is seq-indifferentiable from a random invertible permutation. We also observe that sequential indifferentiability implies correlation intractability, so that the Feistel construction with six rounds and random round functions yields a correlation intractable invertible permutation, a notion we define analogously to correlation intractable functions introduced by Canetti et al. \cite{CanettiGH98}.

Category / Keywords: foundations / indifferentiability, correlation intractability, Feistel construction

Date: received 12 Sep 2011

Contact author: yannick seurin at m4x org