Title: **An efficient and secure two-flow zero-knowledge identification protocol**

Authors: **Stinson D.R. and Wu J.**

Published in: *J. Math. Crypt.* **1** (2007), 201–220

Review by: Mario Forcinito

In addition of the presentation of a new zero-knowledge identification protocol, the paper gives an excellent overview of the paradigms of attack models for identification schemes and identification protocols plus a review of attacks on other identification protocols.

In this work the authors formalize and thoroughly analyze the ideas first suggested by Darmgård into a detailed protocol for which they offer proof of security with respect to a wide range of attacks.

The authors show that the resultant two-flow zero-knowledge scheme is provably secure in a random oracle model under the strongest model of attack if the Knowledge of Exponent and the intractability of the Computational Diffie-Hellman problem assumtions hold, retaining an efficiency reasonably close to that of the Schnorr scheme.