Low-complexity DPA Countermeasure for Resource-Constrained Embedded McEliece Implementation

Martin Petrvalský[1], Tania Richmond[2], Miloš Drutarovský[1], Pierre-Louis Cayrel[3], Viktor Fischer[3]

[1] Dept. of Electronics & Multimedia Communications,
Technical University of Kosice,
Park Komenskeho 13,
041 20 Kosice, Slovakia
{martin.petrvalsky,milos.drutarovsky}@tuke.sk
[2] Institut de Mathématiques
B.P. 20132,
83957, La Garde, France.
tania.richmond@univ-tln.fr
[3] Laboratoire Hubert Curien,
Rue du Prof. Benoît Lauras, 18,
42000, Saint-Étienne, France.
{pierre.louis.cayrel,fischer}@univ-st-etienne.fr

Abstract. In this paper, we present a differential power analysis attack on the McEliece public-key cryptosystem. We demonstrate that a part of a private key - permutation matrix - can be recovered using the power analysis. We attack a software implementation of a 'secure' permutation that was proposed by Strenzke et al at PQCrypto 2008. The cryptosystem is implemented on a 32-bit ARM based microcontroller and power consumption measurements of the device provide us leakage. In addition, we outline a novel countermeasure against the introduced attack. The countermeasure uses properties of linear codes and does not require large amount of random bits which can be profitable for low-cost embedded devices.

Keywords: Differential power analysis, McEliece cryptosystem, side-channel attack, secure implementation.