SPA and DPA attack on the A5/1 Stream Cipher

Martin Jurecek, Jiri Bucek, Robert Lorencz
Czech Technical University in Prague

Abstract

In our contribution we describe cryptanalysis of the A5/1 stream cipher based on power analysis where we utilize the fact that the power consumption while clocking 3 LFSRs is different than when clocking 2 LFSRs. Main part of our contribution is the presentation of a key recovery algorithm that uses information gathered by a simple power analysis (SPA) attack. We also discuss possible use of an existing differential power analysis (DPA) attack for providing input to the key recovery. The SPA attack was demonstrated on a simple prototype implementation of A5/1 on an 8-bit microcontroller. The attack does not require (nor use) any knowledge of the keystream. For key recovery, we assume the SPA provides correct sequence of how many registers were shifted in each clock of the initialization phase (100 empty clocks). DPA also provides information which registers were shifted. The key recovery attack has a 100% success rate and requires minimal storage. An average time complexity of our attack based on SPA is $2^{(33.27)}$ where the computation unit is a resolution of system of linear equations over the Z_2. Recovering the secret key using information from DPA has a constant complexity.