Differential Power Analysis under Constrained Budget: Low Cost Education of Hackers

Filip Štěpánek, Jiří Buček, Martin Novotný
Czech Technical University in Prague

Abstract

The differential power analysis is popular technique in exploiting weaknesses of the embedded systems—mostly of the smart cards. This approach is understandable as the DPA does not require expensive equipment or strong theoretical background on the device under attack. Therefore it is ideal for education of beginners or students in the field of computer security.

The aim of our talk is to share our experience regarding expenses for laboratory equipment and the parameters that this equipment must satisfy. We also like to share our experience with teaching the fundamentals of side channel analysis.

Our experience shows that differential power analysis is feasible even with a very limited budget. Total expenses were below $23,000 the whole lab (10 workplaces), i.e. just $2,300 per one measuring set (oscilloscope, programmer, smart cards, card reader, interface HW board, etc.). The key can be found even with the oscilloscope having just 8 bit resolution. On the other hand, communication speed over USB showed to be crucial for breaking the system in reasonable time.