Master Thesis Proposal

Dual rail logic in software as LLVM-IR transformation

Alexander Schlögl

January 13, 2019

1 Introduction

Embedded devices very rarely utilize instruction level parallelism. Thus, as the power consumption is directly related to the bits in intermediate results that are set to 1, their power consumption directly reflects their computation results without much noise. If the device is running a cryptographic operation, this can result in a leakage of keys. This is known as a power analysis side channel attack. [1]

While there exist many different defenses against this, both in software and in hardware, the most versatile of them is Dual-Rail-Logic. [2] Unlike most other defense mechanisms, Dual-Rail-Logic can be applied to any program. Unfortunately, using Dual-Rail-Logic requires alterations to the hardware, and almost doubles the required circuitry size, making it unsuitable for small embedded applications like e.g. SmartCards. In order to create a way of hardening *any* application against side channel attacks, even when there are tight constraints on space, I would like to implement Dual-Rail-Logic in software.

2 Background

aoeu

3 Related Work

aoeu

4 Intended Methodology

aoeu

References

[1] Paul Kocher, Joshua Jaffe, and Benjamin Jun. Differential power analysis. In *Annual International Cryptology Conference*, pages 388–397. Springer, 1999.

[2] Danil Sokolov, Julian Murphy, Alexander Bystrov, and Alexandre Yakovlev. Design and analysis of dual-rail circuits for security applications. *IEEE Transactions on Computers*, 54(4):449–460, 2005.