Abstract

Hassan Shokry El-Dib

Synthesis of Masking Countermeasures against Side Channel Attacks

We propose a new synthesis method for generating countermeasures for cryptographic software code to mitigate power analysis based side channel attacks. Side channel attacks may arise when computers and microchips leak sensitive information about the software code and data that they process, e.g., through power dissipation electromagnetic radiation. Such information leaks have been exploited in commercial systems in the embedded space. Our new method takes an unprotected C program as input and returns a functionally equivalent but side channel leak free new program as output. The new program is guaranteed to be perfectly masked in that all intermediate computation results are made statistically independent from the secret data. We have implemented our new method in a tool based on the LLVM compiler and the Yices SMT solver. Our experiments on a set of cryptographic software benchmarks show that the new method is both effective and scalable for applications of realistic size.