

Scholarly Paper on
Cache Attacks and Countermeasures

By Swathy Mudhagouni

Advisor: Dr Kris Gaj
Attending Faculty: Dr Jens-Peter Kaps

December 4th, 2009 11:00 a.m.
Engineering Building – Conference Room 3202

Abstract

The rapid growth in computer architecture and technology is aimed towards better performance, higher throughput, lower power consumption, faster processing, etc. but not towards security. One can say, this left open one of the newly observed side channel attacks, Microarchitectural attacks.

This paper discusses the Microarchitectural components which have been leakage points or targets to security attacks. Cache being one of them, this paper will discuss Cache types, Cache Attacks on secret key cryptosystems and countermeasures.