Politecnico di Milano
Scuola di Ingegneria Industriale e dell'informazione
Corso di Laurea Magistrale in Ingegneria Informatica

The title

Advisor (Politecnico di Milano): Vittorio Zaccaria

Co-Advisor (ACME Inc.): ABC
(ACME Inc.): XYZ

Tesi di Laurea Magistrale di:
This guy
matricola XYZ

Academic Year 2010-2011

This thesis has been developed
at *put here where you did your thesis.*

Dedicato a tutti coloro che mi hanno voluto bene
e che mi hanno sostenuto in questi anni.
Grazie.

Sommario

Abstract tradotto in italiano

Abstract

One page in english describing the summary of your work

Contents

1 Introduction **1**

Bibliography **3**

List of Figures

Listings

List of Abbreviations

AES Advanced Encryption Standard

ASIC Application-Specific Integrated Circuit

AST Abstract Syntax Tree

CAD Computer-Aided Design

CASCA Countermeasure Against Side-Channel Attack

CMOS Complementary Metal-Oxide Semiconductor

CPA Correlation Power Analysis

DAG Directed Acyclic Graph

DES Data Encryption Standard

DEMUX Demultiplexer

DPA Differential Power Analysis

DSL Domain-Specific Language

DSEL Domain-Specific Embedded Language

FHDL Functional Hardware Description Language

FF Flip-flop

FPGA Field Programmable Gate Array

FSM Finite-State Machine

GADT Generalized Algebraic Data Type

GF Galois Field

GE Gate Equivalent

HD Hamming Distance

HDL Hardware Description Language

HOF Higher-Order Function

HW Hamming Weight

IC Integrated Circuit

IP Intellectual Property

LHS Left Hand Side

LSB Least Significant Bit

LUT Look-up Table

MSB Most Significant Bit

MPC Multi-Party Computation

MUX Multiplexer

REPL Read–Eval–Print Loop

RHS Right Hand Side

RTL Register-Transfer Level

SAT Boolean Satisfiability Problem

SCA Side-Channel Attack

SMT Satisfiability Modulo Theories

SNR Signal-to-Noise Ratio

SPA Simple Power Analysis

Chapter 1

Introduction

Example of citation [1]

Bibliography

[1] N.I.S.T. Announcing the Advanced Encryption Standard (AES), November, 26 2001. Federal Information Processing Standards Publication, n. 197.