RUHR-UNIVERSITÄT BOCHUM

Side-Channel Attacks On Implementations Of Lattice-Based Cryptosystems

Julian Speith, Felix Haarmann

Seminarausarbeitung
May 21, 2016
Embedded Security Group - Prof. Dr.-Ing. Christof Paar

Abstract

The following text[1] describes what your abstract should be about.

The abstract should convey to the reader concisely and accurately within the space of a few sentences, the claim to knowledge that the authors are making. It should indicate the boundaries of space and time within which the enquiry has occurred. If there is a claim to generality beyond the boundaries of the enquiry the basis of that claim should be given, for example that a random sample is thought to be representative of a larger population. There should also be a hint of the method of enquiry.

The boundaries of an enquiry are important - and are unfortunately too often omitted from abstracts. This is due to the regrettable tendency for researchers to generalise their results from, for example, a few schools to all schools, and to imply that what was true at a particular time, is true for all time. Some reference to the geographical location of the children, or teachers, or schools on whom the claim to knowledge rests should be made. Because of the international nature of the research community it is worth making clear in what country the research took place. Also the period in which the data was collected should be stated.

The abstract should be a condensation of the substance of the paper, not a trailer, nor an introduction. Journals and thesis regulations usually put a limit of around 200 to 300 words to the length of an abstract. Trailer is a term borrowed from the cinema industry to describe a showing of a few highlights in order to win an audience. An Introduction tells that something is coming, but doesnt reveal its substance. These are not what is needed.

Abstracts are recycled in abstract journals and electronic networks and provide the main vehicle for other researchers to become aware of particular studies. Hence the more clearly they convey the claim to knowledge of the original paper the more useful they are in helping the reader to decide whether it is worth taking the trouble to obtain and read the original and possibly cite it in his/her own writing.

Both the abstract and the paper should make sense without the other.

[1] Shamelessly ripped from `http://www.leeds.ac.uk/educol/abstract.htm`

Contents

Acronyms

1. Introduction

Describe the aim of your thesis and motivate this aim. Describe previous work and cite some stuff [BGT83, EG92], . Describe how your thesis is structured...

2. Theoretical Background

2.1. Notation

2.2. Ideal Lattices

2.3. Learning with Errors Problem

2.4. Discrete Gaussian Distributions

2.5. Cryptographic Algorithms

2.5.1. Ring-LWE Encryption Scheme

2.5.2. BLISS Signature Scheme

2.6. Side-Channel Attack Terminology

3. Masking the Ring-LWE Encryption Scheme I

3.1. Implementation

3.2. Evaluation

4. Masking the Ring-LWE Encryption Scheme II

4.1. Implementation

4.2. Evaluation

5. Flush+Reload Cache Attack on Bliss

5.1. Gaussian Sampling

5.1.1. CDT Sampling

5.1.2. Rejection Sampling

5.2. Attacking the Sampling Algorithms

5.3. Evaluation

6. Blinding Countermeasures

6.1. Blinding Polynomial Multiplication

6.2. Blinding Gaussian Sampling

7. Conclusion

Conclude your thesis and discuss your results...

List of Figures

List of Tables

A. Bibliography

[BGT83] A. Bayliss, C. I. Goldstein, and E. Turkel. An iterative method for the Helmholtz equation. *J. Comp. Phys.*, 49:443–457, 1983.

[EG92] O. Ernst and G. Golub. A domain decomposition approach to solving the Helmholtz equation with a radiation boundary condition. Technical Report NA-92-08, August 1992.