# ICR – Practical Work #3

Fault Attacks against RSA-CRT

Gugger Joël [1]

May 26, 2016

[1] joel.gugger@master.hes-so.ch

## Abstract

A way to accelerate the RSA signature procedure consists in exploiting the fact that one knows the two primes p and q, as it is a private-key operation, and to use the Chinese Remainder Theorem (CRT).

The goal of this practical work consists in implementing a fast RSA signature procedure that exploits the CRT and to study the security of such an implementation at the light of fault attacks. This practical work can be implemented either in C, C++, Java or Python, with the big-numbers arithmetic library of your choice.

# Contents

# Chapter 1

# RSA-CRT

## 1.1 Questions

### 1.1.1 How have you tested that your routines are properly working?

### 1.1.2 What is the gain in terms of speed that you obtain when using RSA-CRT with respect to a standard RSA signature generation procedure?

### 1.1.3 What are the values that one could pre-compute and store besides n and d, in order to speed up as much as possible the signature generation procedure?

## 1.2 Implementation

### 1.2.1 RSA key generation routine

### 1.2.2 Standard RSA signature and verification routines

### 1.2.3 Fast RSA signature procedure

## Abstract

The sources of the project are available on GitHub at the following address:
https://github.com/GuggerJoel/Crypto-ICR-lab003