Power Analysis by Exploiting Chosen Message and Internal Collisions – Vulnerability of Checking Mechanism for RSA-Decryption*

Sung-Ming Yen[1], Wei-Chih Lien[1], SangJae Moon[2], and JaeCheol Ha[3]

[1] Laboratory of Cryptography and Information Security (LCIS),
Dept of Computer Science and Information Engineering,
National Central University, Chung-Li, Taiwan 320, R.O.C.
{yensm, cs222058}@csie.ncu.edu.tw
http://www.csie.ncu.edu.tw/~yensm/
[2] School of Electronic and Electrical Engineering,
Kyungpook National University,
Taegu, Korea 702-701
sjmoon@ee.knu.ac.kr
[3] Dept of Computer and Information,
Korea Nazarene University, Choong Nam, Korea 330-718
jcha@kornu.ac.kr

Abstract. In this paper, we will point out a new side-channel vulnerability of cryptosystems implementation based on BRIP or square-multiply-always algorithm by exploiting specially chosen input message of order two. A recently published countermeasure, BRIP, against conventional simple power analysis (SPA) and differential power analysis (DPA) will be shown to be vulnerable to the proposed SPA in this paper. Another well known SPA countermeasure, the square-multiply-always algorithm, will also be shown to be vulnerable to this new attack. Further extension of the proposed attack is possible to develop more powerful attacks.

Keywords: Chosen-message attack, Cryptography, Side-channel attack, Simple power analysis (SPA), Smart card.

1 Introduction

During the past few years many research results have been published on considering smart card side-channel attacks because of the popular usage of smart cards on implementing cryptosystems. This new branch of cryptanalysis is usually called the *side-channel attack* (SCA).

The power analysis attack is an important category of SCA originally published by Kocher [1] in which both simple power analysis (SPA) and differential power analysis (DPA) were considered. SPA tries to extract the private key by

* This work was supported by University IT Research Center Project.

E. Dawson and S. Vaudenay (Eds.): Mycrypt 2005, LNCS 3715, pp. 183–195, 2005.

observing on a single or a very few number of power consumption traces collected from the smart card. DPA consists in performing a statistical analysis of many power consumption traces (say a few thousands or more) of the same algorithm with different inputs.

Exponentiation and its analogy, point scalar multiplication on elliptic curve, are of central importance in modern cryptosystems implementation as they are of the basic operation of almost all modern public-key cryptosystems, e.g., the RSA system [2] and the elliptic curve cryptography [3,4]. Therefore, many side-channel attacks and also the related countermeasures on implementing exponentiation and point scalar multiplication have been reported in the literature.

Some recent works of power analysis attack, e.g., refined power analysis (RPA) [5], zero-value point attack (ZPA) [6], and doubling attack [7], threaten most existing countermeasures for implementing exponentiation and point scalar multiplication, e.g., some countermeasures in [8]. Recently, Mamiya *et al* proposed an enhanced countermeasure which was claimed to resist against RPA, ZPA, classical DPA and SPA, and also doubling attack by introducing a new random blinding technique and also exploiting a well known regular program execution trick (say the square-multiply-always like approach) for each loop iteration.

The main contribution of this paper is that a new SPA by exploiting specific chosen message is proposed in which collecting a single power trace is sufficient to mount a successful attack. An important result obtained is that both the well known SPA resistant countermeasure by using the square-multiply-always algorithm [8] and also the recent and enhanced BRIP algorithm [9] are shown to be vulnerable to this new attack. Further extension on the attack is also pointed out by selecting more general and random input messages which makes the detection of a specific message employed in the basic attack be infeasible and this leads to a more powerful extended attack. Furthermore, the proposed attack is also applicable to implementation of RSA with CRT speedup. Another important observation is that cryptographic padding (e.g., RSA-OAEP [10,11]) is not always useful against simple power attack.

2 Preliminary and Related Works

In this paper, we consider the problem of computing modular exponentiation. In the context of RSA private computation (for example, generating a digital signature or ciphertext decryption), we consider the computation of $S = M^d \bmod n$ where M, d, and n are the input message, the private key, and the modulus integer, respectively.

2.1 Exponentiation Algorithm

Let $\sum_{i=0}^{m-1} d_i 2^i$ be the binary expansion of exponent d. The computation $S = M^d \bmod n$ needs efficient exponentiation algorithms to speedup its implementation.