Relative Doubling Attack Against Montgomery Ladder*

Sung-Ming Yen¹, Lee-Chun Ko¹, SangJae Moon², and JaeCheol Ha³

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, cs222085}@csie.ncu.edu.tw
http://www.csie.ncu.edu.tw/~yensm/

² School of Electronic and Electrical Engineering, Kyungpook National University, Taegu 702-701, Korea
sjmoon@ee.knu.ac.kr

³ Dept of Computer and Information, Korea Nazarene University, Choong Nam 330-718, Korea
jcha@kornu.ac.kr

Abstract. Highly regular execution and the cleverly included redundant computation make the square-multiply-always exponentiation algorithm well known as a good countermeasure against the conventional simple power analysis (SPA). However, the doubling attack threatens the square-multiply-always exponentiation by fully exploiting the existence of such redundant computation. The Montgomery ladder is also recognized as a good countermeasure against the conventional SPA due to its highly regular execution. Most importantly, no redundant computation is introduced into the Montgomery ladder. In this paper, immunity of the Montgomery ladder against the doubling attack is investigated. One straightforward result is that the Montgomery ladder can be free from the original doubling attack. However, a non-trivial result obtained in this research is that a relative doubling attack proposed in this paper threatens the Montgomery ladder. The proposed relative doubling attack uses a totally different approach to derive the private key in which the relationship between two adjacent private key bits can be obtained as either \( d_i = d_{i-1} \) or \( d_i \neq d_{i-1} \). Finally, a remark is given to the problem of whether the upward (right-to-left) regular exponentiation algorithm is necessary against the original doubling attack and the proposed relative doubling attack.

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

1 Introduction

Cryptographic hardware devices like smart cards are widely used nowadays. During the past few years many research results have been published on considering

---

* This work was supported by University IT Research Center Project.
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. The power analysis attack is an important category of side-channel attack originally pointed out by Kocher [1] in which both simple power analysis (SPA) and differential power analysis (DPA) were considered.

In a SPA, the attacker observes on one or a few collected power traces of the smart card executing an algorithm and tries to identify the occurrence of an instruction execution or a specific operand/data access which are driven by a part of the private key. Through the above observation, if precise enough, the private key can be derived. In a DPA, the attacker tries to verify his guess on a part of the private key by analyzing on only some specific bits of the result of a specific intermediate step of an algorithm which is a function of the private key. In order to largely enhance the signal to noise ratio to mount a successful DPA, it usually collects much more power traces than in a SPA and partitions the power traces into some groups according to the guessed key bits and a underlying attack design. Difference of the above power traces of different groups is therefore used to verify the guess on key bits. Usually, a DPA is mounted by analyzing on many executions of the same algorithm with different random inputs, and theoretically those inputs will be better if statistically unrelated.

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], the ElGamal system [3], and the elliptic curve cryptography [4, 5]. Therefore, many side-channel attacks and also the related countermeasures on implementing exponentiation and point scalar multiplication have been reported in the literature.

The square-multiply-always exponentiation (or point scalar multiplication) algorithm [6] is a well-known SPA countermeasure which exploits a simple and useful trick to design a regularly executing algorithm by introducing redundant computation into each loop iteration when necessary. Unfortunately, Fouque and Valette proposed the doubling attack [7] to threaten the square-multiply-always algorithm (more precisely, the left-to-right version of the algorithm) by exploiting the existence of redundant computation in a novel approach.

Joye and Yen proposed an enhanced SPA countermeasure based on the Montgomery ladder [8] which was demonstrated to be also regularly executed but based on a totally different idea from the original square-multiply-always exponentiation. The most special thing about the Montgomery ladder is that no redundant computation exists in the algorithm which is also helpful to be immune from some hardware fault attacks [9, 10].

However, no research has been reported on whether the Montgomery ladder can be immune from the doubling attack or any doubling-like attack in the light of the fact of no redundant computation within the algorithm. The main contribution of this paper is that a totally different approach of doubling attack

\[ \text{It usually collects a few thousands or more power traces in order to obtain a meaningful average power trace.} \]