Side Channel Attacks and Countermeasures on Pairing Based Cryptosystems over Binary Fields

Tae Hyun Kim[1], Tsuyoshi Takagi[2],
Dong-Guk Han[3], Ho Won Kim[3], and Jongin Lim[1]

[1] Center for Information and Security Technologies(CIST),
Korea University, Seoul, Korea
{thkim, jilim}@cist.korea.ac.kr
[2] FUTURE UNIVERSITY-HAKODATE, Japan
takagi@fun.ac.jp
[3] Electronics and Telecommunications Research Institute(ETRI), Korea
{christa, khw}@etri.re.kr

Abstract. Pairings on elliptic curves have been used as cryptographic primitives for the development of new applications such as identity based schemes. For the practical applications, it is crucial to provide efficient and secure implementations of the pairings. There have been several works on efficient implementations of the pairings. However, the research for secure implementations of the pairings has not been thoroughly investigated. In this paper, we investigate vulnerability of the pairing used in some pairing based protocols against side channel attacks. We propose an efficient algorithm secure against such side channel attacks of the eta pairing using randomized projective coordinate systems for the pairing computation.

Keywords: Pairing based cryptosystems, Side channel attacks, Differential Power Analysis, Randomized projective coordinate systems, Eta pairing.

1 Introduction

Since pairings have new and useful cryptographic properties such as bilinearity and non-degeneracy the interest and active research of them in cryptography is growing. Recently many cryptographic schemes based on the Tate pairing and the Weil pairing have been proposed. For example, identity based encryption schemes [6,28], identity based signature schemes [17,8,26], short signature [7], and identity based authenticated key agreement [31].

To accelerate practical applications of pairing based schemes a lot of work has focused on the development of efficient and easy computations of pairings on elliptic curves. Barreto et al. [2] and Galbraith et al. [13] provided the fast computation of the Tate pairing on supersingular elliptic curves over finite fields of characteristic two and three. Duursma and Lee [11] gave a closed formula in the case of characteristic three, and Kwon [21] extended it to supersingular curves over characteristic two. Barreto et al. [1] proposed a general technique

D. Pointcheval, Y. Mu, and K. Chen (Eds.): CANS 2006, LNCS 4301, pp. 168–181, 2006.

for the efficient computation of pairings on supersingular abelian varieties called *the eta pairing*.

Recently such methods of pairings have been implemented in software and hardware to accelerate constrained devices such as smartcards [5,14,30,4,27]. In the implementation of cryptosystems or protocols on such devices, we should consider not only efficiency but also security. If we don't carefully implement cryptosystems on constrained devices then they can be insecure against side channel attacks (SCAs). Thus it is important to consider the secure implementation of pairing based cryptosystems secure against SCAs. We can divide pairing based schemes into two types by whether or not an input of pairing is secret [10]. For example, identity based signature schemes such as short signature scheme by Boneh et al. require the secret information as an input (i.e., the secret scalar) of the elliptic curve scalar multiplication. Side channel attacks and countermeasures on scalar multiplications have well been studied. However, identity based encryption schemes such as Boneh-Franklin encryption scheme [6] use the secret information as an input of the pairing. In this case, there are only few works of SCAs on the pairings [24,29,33]. In [24], Page and Vercauteren showed side channel attacks against the Duursma-Lee algorithm. In [29], Scott suggested countermeasures to provide resistance to more sophisticated simple power analysis (SPA) and differential power analysis (DPA) attacks. Very recently, Whelan and Scott investigated practical pairing algorithms using correlation power analysis (CPA) [33]. However the form of some multiplication used in the eta pairing on the supersingular curves in characteristic two is different to the case of characteristic three. In this paper, we concretely examine the security of the eta pairing on the supersingular curve over $\mathbb{F}_{2^m}$ against timing attack (TA) or SPA attack and DPA attack.

In general, to speed up elliptic curve point addition and doubling, the projective coordinate systems are used instead of the affine coordinate system because the affine coordinate system requires a modular inversion operation, computationally expensive. In [19], Izu and Takagi showed that the Tate pairing on general elliptic curves over prime fields $\mathbb{F}_{p^m}$ is efficiently computed using the projective coordinate systems. Hess et al. [18] extended the eta pairing over supersingular curves to general curves over prime fields $\mathbb{F}_{p^m}$, and then examined efficiency in the projective coordinate systems. However, for providing protection of SCAs, Coron [9] used the randomized projective coordinate. In this paper, to resist SCAs, we propose an explicit algorithm using randomness of the projective coordinate systems of the eta pairing for a curve over characteristic two.

This paper is organized as follows: In the next section we review several methods for the efficient computation of the Tate pairing. Section 3 describes side channel attacks on the eta pairing over supersingular curves in characteristic two. Section 4 presents a countermeasure to prevent the attack described in Section 3. Section 5 compares the proposed countermeasure with the previous methods. Finally we conclude in Section 6.