Zero-Value Point Attacks on Kummer-Based Cryptosystem*

Fangguo Zhang[1], Qiping Lin[1], and Shengli Liu[2]

[1] School of Information Science and Technology
Sun Yat-sen University, Guangzhou 510006, China
[2] Dept. of Computer Science and Engineering,
Shanghai Jiao Tong University, Shanghai 200240, China
isszhfg@mail.sysu.edu.cn

Abstract. The Zero-Value Point (ZVP) attack, one of side channel attacks, is very powerful to recover the secret information of elliptic curve cyrptosystem (ECC) on memory constraint devices by monitoring their power consumptions. In the ZVP attack, the zero-value registers are used in point addition and doubling formula of ECC to resist randomizations. Hence, the countermeasures against the differential power analysis (DPA), like Coron's and Joye-Tymen's randomization, do not work for the ZVP attack. The Kummer surface is a variety associated to the Jacobian of a genus 2 curve with a map. The pseudo-group structure on the Kummer surface defines a scalar multiplication, which is more efficient than that in HECC and comparable to ECC, especially in constraint environments. We inspect the pseudo-addition and doubling formula of the Kummer surface and show how to find zero-value registers. Our analysis shows that the scalar multiplication on the Kummer surface suffers from the ZVP attack, hence all Kummer-based cryptosystems are inevitable to the ZVP attack.

Keywords: Zero-value point attack, Kummer-based cryptosystem, Differential power analysis, Scalar multiplication.

1 Introduction

Elliptic Curve cryptosystem involves only a short key, and is more preferable to other public key variants for cryptographic applications in memory-constraint device. The concept of Hyperelliptic Curve Cryptosystem (HECC) was proposed by Koblitz [18] as a generalization of ECC. In a HECC, the jacobian of a hyperelliptic curve defined over a finite field is used to fulfil the discrete-logarithm-based cryptographic algorithms and protocols. Hyperelliptic curves have richer algebraic structures and are based on a smaller field than elliptic curves to achieve the same level of security. In cryptographic applications, scalar multiplications

* This work is supported by the the National Natural Science Foundation of China (No. 61070168, 61170229 and U1135001) and Scientific innovation projects of Shanghai Education Committee (Grant 12ZZ021).

F. Bao, P. Samarati, and J. Zhou (Eds.): ACNS 2012, LNCS 7341, pp. 293–310, 2012.

are essential and their computations decide the efficiency of the ECC or HECC cryptosystem.

Cantor's pioneering work [4] gave an algorithm to do scalar multiplications for hyperelliptic curves. In the early 1990s, Flynn [11] gave an explicit description of the Jacobian of a genus 2 hyperelliptic curve and suggested a more efficient arithmetic on scalar multiplications.

As for any hyperelliptic curves C of genus 2, there exists a map $J(C) \to K$ sending two opposite points of the Jacobian (except for the 2-torsion points) to a point of the Kummer surface K. The map is not a group-homomorphism, hence the Kummer surface is not structured as a group. However, the map does transform the group structure of the Jocobian to a pseudo-group structure on the Kummer surface. Fast formula for the arithmetic on the Kummer surface was developed with the theory of Theta functions and optimized in [12,14]. Using Montgomery ladder, it is enough for the pseudo-group structure to define scalar multiplications on the Kummer surface. This makes possible the Kummer-based cryptosystems. For example, Smart et al. [28] proposed a Diffie-Hellman protocol implemented on Kummer surface in 1999. It was shown in [12] that the discrete logarithm problem on Kummer sufaces is polynomial time equivalent to the discrete logarithm in the Jocobian of the hyperelliptic curve of genus 2. Fast arithmetic on the Kummer surface was also developed, which is much more efficient than that in ECC or HECC, especially in constraint environment. Therefore, many works have been devoted to fast arithmetic on the Kummer surface [7,8,12,14].

1.1 Side Channel Attacks and Zero-Value Point (ZVP) Attack on Scalar Multiplication

Due to the short key size and fast arithmetics, ECC, HECC and Kummer-Based Cryptosystems are especially adaptable to low-cost and memory-limited cryptographic devices like smartcards. However, cryptographic hardware operations can be an easy target to power analysis by Side Channel Attacks [19,20]. The Side Channel Attacks analyze the instantaneous power consumption of a device to derive the secret information stored in it. Over the years, power analysis evolves from the timing attack, the Simple Power Analysis (SPA), to the Differential Power Analysis (DPA) and Zero-Value Point attack (ZVP), etc.

ECC, HECC and Kummer-Based Cryptosystems generally base their security on the Discrete-Logarithm related assumptions on some additive (pseudo) group, and scalar multiplications are the main computation involved.

In [5], Coron showed how SPA and DPA work on scalar multiplications in ECC. Let d be the secret, and P be a point on ECC, the scalar multiplication dP needs to compute the addition of two different points and the doubling of a point. In the "double and addition" algorithm for dP, each bit of d determines whether both of doubling and addition or only doubling involved, and this causes different power consumption. Simple Power Analysis (SPA) just uses this difference to determine every bit of d.

There are many countermeasures to avoid SPA, like Coron's "double-and-add-always" method [5] and "Montgomery" method [24], "Hesse" type [27,17] or "Jacobi" type [21] of computing doubling and addition in a unified formula. But all the anti-SPA methods do not prevent the Differential Power Analysis (DPA), a much more powerful analysis.

To avoid the DPA, the proposals are to use randomized projective homogeneous coordinates [5] or Jacobian coordinates [21], to work in a random isomorphism of the elliptic curve, or to work in random field isomorphism [16].

In 2003, Goubin observed that randomization does not work very well for some special points[13]. Goubin [13] analyzed two kinds of special points, namely $(x, 0)$ and $(0, y)$, on elliptic curves. Points $(x, 0)$ and $(0, y)$ are expressed as $(X : 0 : Z)$ and $(0 : Y : Z)$ in Jacobian coordinates. Randomization of the Jocobian coordinates results in points $(r^2X : 0 : rZ)$ and $(0 : r^3Y : rZ)$ for some random integer $r \neq 0$. One of the coordinate remains to be zero after the randomization. Power analysis then takes advantage of those special points to derive the secret scalar d. However, Smart showed that Goubin's power-analysis attack for elliptic curves can be easily avoided [26].

Akishita et al. [3] extended Goubin's attack with the so-called "Zero-Value Point" (ZVP) attacks. The ZVP attack is not limited to zero-coordinate points like $(x, 0)$ or $(0, y)$. It collects those points Q such that the computation of the scalar multiplication dQ leads to 0 in the intermediate computation of the doubling or addition formulas. Lots of elliptic curves, including the SECG random curves over prime fields, suffer from the ZVP attack. It seems that the ZVP attack is one of the most powerful attack up to now. In [3], Akishita et al. showed the conditions that the zero-value points exist in elliptic curve, and the ZVP attack suggests a new security criteria for secure implementation of ECC. [10] gave a survey on known side-channel attacks and countermeasures for ECC.

As for HECC, the power analysis works in the same principle, and the only difference is that scalar multiplication dP works in divisor class groups of hyperelliptic curves, instead of the additive group of points on ECC. Avanzi [1] generalized Goubin's attacks to divisor class groups of hyperelliptic curves, and provided a generalization of the countermeasures.

As far as we know, there is no research work on power analysis of Kummer-based cryptosystems up to now. We will fulfill the analysis of Kummer-based cryptosystems in this paper. Although the Kummer Surface is constructed from hyperelliptic curves with $g = 2$, the ZVP attack on Kummer-based cryptosystems is much different from the ZVP attack on HECC. As we will show in this paper, there are more special points which can be taken advantage of by ZVP attacks on a Kummer surface, compared to its corresponding hyperelliptic curve, and it is also much more difficult to resist ZVP attacks on a Kummer surface.

1.2 Our Contributions

In this paper, we study how to find special points on a Kummer surface, i.e., those points result in zero-value register during the computation of scalar multiplications. We also provide how to use those zero-value points to implement

ZVP attacks on Kummer-based cryptosystem. Finally we show that there are no efficient ways to avoid the ZVP attacks on Kummer surfaces, and propose countermeasures against the ZVP attacks.

Organization. The rest of this paper is organized as follows. In section 2, we review scalar multiplication on a Kummer surface. In section 3, we focus on analyzing what are special points of a Kummer surface, and estimate the number of special points. In section 4, we describe how to carry out the zero-value point attacks on Kummer surface. In section 5, we give the countermeasures against this attacks. Section 6 concludes the paper.

2 Scalar Multiplication on the Kummer Surface

In this section, we will recall the pseudo-addition and doubling algorithm and the Montgomery scalar multiplication on the Kummer surface. The Kummer surface is defined as follows. Let

$$C : y^2 + h(x)y = f(x) \tag{1}$$

be a curve of genus 2 defined over a field F, where $\deg(f) \leq 6$ and $\deg(h) \leq 3$. Let J be the Jacobian variety of C. Then a hypersurface K in $\mathbb{P}^3$ can be associated to the Jacobian variety J. The associated hypersurface K is called the Kummer surface. If the characteristic of F is not 2, i.e., $\mathrm{char}(F) \neq 2$, the curve C of genus 2 has a reduced form

$$C : y^2 = f(x). \tag{2}$$

Cassels and Flynn [6] constructed the Kummer surface associated to the Jacobian variety J of curve $C : y^2 = f(x)$. If $\mathrm{char}(F) = 2$, the general form Eq.(1) can be reduced to the case $\deg(h) = 2$. Duquesne [9] considered how to construct the Kummer surface for this case. Gaudry [12] and Lubicz [14] proposed formulas for the arithmetic of Kummer surfaces based on the theory of algebraic theta functions. Müller [25] developed the general expressions of the Kummer surface for the more general form Eq.(1), which applies to any $\mathrm{char}(F)$.

Given a genus 2 curve C, the Kummer surface is obtained by a map $J(C) \to K$, which maps two opposite points of the Jacobian of a genus 2 curve into one point in K. The quotient of J by the negation map results in the variety K, i.e., the Kummer surface. However, the map is not a group homomorphism, and the Kummer surface does not have a group structure. But the map endows a pseudo-group structure on the Kummer surface, over which a scalar multiplication can be defined with the help of a so-called Montgomery ladder. The scalar multiplication on the Kummer surface associated to a genus 2 curve can be used to design genus 2 cryptosystems. Due to the map $J(C) \to K$, the discrete logarithm problem on the Kummer surfaces can be proved to be polynomial time equivalent to the discrete logarithm problem in the corresponding Jacobian [28].

If $\mathrm{char}(F) \neq 2$, there exists a fast formulae for the scalar multiplication on the Kummer surface associated to a genus 2 curve C using a Montgomery ladder. This make Kummer-based cryptosystems more efficient than hyperelliptic curve

cryptosystems, especially in some hardware configurations, like smart cards. Let a genus 2 curve C be given by

$$C : y^2 = x^5 + f_4x^4 + f_3x^3 + f_2x^2 + f_1x + f_0.$$

Suppose $P_1 = (x, y)$ and $P_2 = (u, v)$ are affine points on curve C. According to [6], a projective embedding of the Kummer surface is given by

$$k_1 = 1, k_2 = x + u, k_3 = xu, k_4 = \frac{F_0(x, u) - 2yv}{(x - u)^2},$$

where

$$F_0(x, u) = (x + u)xu + 2f_4(xu)^2 + f_3(x + u)xu + 2f_2(xu) + f_1(x + u) + 2f_0.$$

The functions k_1, k_2, k_3, k_4 satisfy the quartic equation

$$K(k_1, k_2, k_3, k_4) = K_2(k_1, k_2, k_3)k_4^2 + K_1(k_1, k_2, k_3)k_4 + K_0(k_1, k_2, k_3) = 0,$$

where

$$\begin{aligned}
K_2(k_1, k_2, k_3) &= k_2^2 - 4k_1k_3,\\
K_1(k_1, k_2, k_3) &= -2k_2k_3^2 - 4k_1k_3^2f_4 - 2k_1k_2k_3f_3 - 4k_1^2k_3f_2 - 2k_1^2k_2f_1 - 4k_1^3f_0,\\
K_0(k_1, k_2, k_3) &= k_3^4 - 2k_1k_3^3f_3 - 4k_1k_2k_3^2f_2 - 4k_1k_2^2k_3f_1 - 4k_1k_2^3f_0\\
&\quad + k_1^2k_3^2f_3^2 - 4k_1^2k_3^2f_2f_4 + 2k_1^2k_3^2f_1 - 4k_1^2k_2k_3f_1f_4 + 4k_1^2k_2k_3f_0\\
&\quad - 4k_1^2k_2^2f_0f_4 - 2k_1^3k_3f_1f_3 - 4k_1^3k_2f_0f_3 + k_1^4f_1^2 - 4k_1^4f_0f_2.
\end{aligned}$$

The points of the Kummer surface are of form $(k_1 : k_2 : k_3 : k_4)$. Given two points A and B on the Kummer surface, we can compute $A + B$ if and only if we know $A - B$ firstly. Smart et al. [28] was the first one who proposed to compute scalar multiplication using Montgomery ladder on the Kummer surface. Montgomery ladder can be used to compute the scalar multiplication, because $A-B$ is unchanged at every step of the Montgomery ladder. Duquesne proposed the pseudo-addition and doubling algorithms for $\mathrm{char}(F) \neq 2$ on the Kummer surface in [7] and [2, chapter 14]. Recently, Lin et al. [22] pointed out some minor errors in the algorithms and revised them. Below we recall the revised algorithms in [22].

Let F_q be a field of characteristic $p \neq 2, 3$ and let C/F_q be a curve of genus 2. Let K_C denote the Kummer surface of C. Assume that the difference $A - B$ is known and the third coordinate of $A-B$ on the Kummer surface is 1 (remember we are in $\mathbb{P}^3(F_q)$) where $A = (k_1 : k_2 : k_3 : k_4)$ and $B = (l_1 : l_2 : l_3 : l_4)$ are two points on the Kummer surface K_C. Then the Kummer surface coordinates for $A + B$ are as follows:

$$\begin{aligned}
k_1(A + B) &= \varphi_{11}(A, B),\\
k_2(A + B) &= 2(\varphi_{12}(A, B) - k_1(A + B)k_2(A - B)),\\
k_3(A + B) &= k_1(A - B)\varphi_{33}(A, B),\\
k_4(A + B) &= 2(\varphi_{14}(A, B) - k_1(A + B)k_4(A - B)),
\end{aligned}$$

where

$$\varphi_{11}(A,B) = ((k_4l_1 - k_1l_4) + (k_2l_3 - k_3l_2))^2;$$

$$\begin{aligned}\varphi_{12}(A,B) = &((k_2l_3 - k_3l_2) + (k_1l_4 - k_4l_1))(f_3(k_1l_3 - k_3l_1) + (k_2l_4 - k_4l_2))\\ &+2(k_1l_3 - k_3l_1)(f_2(k_1l_3 - k_3l_1) + (k_1l_2 - k_2l_1) - (k_3l_4 - k_4l_3))\\ &+2f_4(k_1l_4 - k_4l_1)(k_2l_3 - k_3l_2),\end{aligned}$$

$$\varphi_{33}(A,B) = ((k_3l_4 - k_4l_3) + (k_1l_2 - k_2l_1))^2,$$

$$\begin{aligned}\varphi_{14}(A,B) = &((k_1 + k_3)(l_1 - l_3) + k_1l_3 - k_3l_1)(f_3((k_1l_4 + k_4l_1) - (k_2l_3 + k_3l_2))\\ &+2((k_1l_2 + k_2l_1) - (k_3l_4 + k_4l_3)) + 2f_4(k_1l_1 - k_3l_3))\\ &+2f_2(k_1l_4 - k_2l_3)(k_4l_1 - k_3l_2)\\ &+((k_2 + k_4)(l_2 - l_4) + k_2l_4 - k_4l_2)((k_2l_3 + k_3l_2) - (k_1l_4 + k_4l_1)).\end{aligned}$$

Let $A = (k_1 : k_2 : k_3 : k_4)$, then the Kummer coordinates for $2A = (\delta_1 : \delta_2 : \delta_3 : \delta_4)$ are given by

$$\delta_1 = 2\varphi_{14}(A,A), \delta_2 = 2\varphi_{24}(A,A), \delta_3 = 2\varphi_{34}(A,A), \delta_4 = \varphi_{44}(A,A),$$

where

$$\begin{aligned}\varphi_{14}(A,A) = &2(k_1^2 - k_3^2)(f_3(k_1k_4 - k_2k_3) + 2(k_1k_2 - k_3k_4)\\ &+f_4(k_1^2 - k_3^2)) + 2(k_1k_4 - k_2k_3)(k_4^2 - k_2^2 + f_2(k_1k_4 - k_2k_3)),\end{aligned}$$

$$\begin{aligned}\varphi_{24}(A,A) = &(k_1^2 + k_3^2)(8k_1k_3 - f_3(k_1^2 + k_3^2)) + 2(k_2^2 + k_4^2)(k_3^2 + k_1^2 + k_2k_4 + f_3k_1k_3)\\ &+k_1k_3((f_3^3 - 8f_3 + 8f_2^2 + 8f_4^2 - 4f_2f_3f_4)k_1k_3\\ &+(7 - f_3^2 + 8f_2f_4)k_2k_4 + 8f_2(k_3k_4 + k_1k_2) + 8f_4(k_2k_3 + k_1k_4))\\ &+k_2k_4(4f_2(k_1k_4 + k_2k_3) + 4f_4(k_1k_2 + k_3k_4) + f_3(k_2k_4 + 4(k_1^2 + k_3^2))),\end{aligned}$$

$$\begin{aligned}\varphi_{34}(A,A) = &2(k_1^2 - k_3^2)(f_3(k_1k_2 - k_3k_4) + f_2(k_1^2 - k_3^2) + 2(k_1k_4 - k_2k_3))\\ &+2(k_1k_2 - k_3k_4)(k_2^2 - k_4^2 + f_4(k_1k_2 - k_3k_4)) + k_1k_2(k_1^2 - k_2^2),\end{aligned}$$

$$\begin{aligned}\varphi_{44}(A,A) = &(k_1^2 + k_3^2)((f_3^2 - 4f_2f_4 - 2)(k_1^2 + k_3^2) - 8f_2(k_3k_4 + k_1k_2)\\ &-8f_4(k_1k_4 + k_2k_3) - 4f_3k_1k_3 - 12k_2k_4 + (k_2^2 + k_4^2)(k_2^2 + k_4^2 - 2f_3(k_1^2 + k_3^2))\\ &+k_1k_3(8f_2(k_2k_3 + k_1k_4) + 8f_4(k_1k_2 + k_3k_4) + (16 + 8f_2f_4 - 2f_3^2)k_1k_3)\\ &+2K_2k_4(2f_3k_1k_3 - k_2k_4).\end{aligned}$$

In Algorithm 1, we show how to use Montgomery ladder to compute scalar multiplication on the Kummer surface. At each step, the algorithm performs one addition and one doubling, which makes this method resistant to Simple Power Attacks.

Algorithm 1. Montgomery scalar multiplication algorithm for Kummer surface

Input: A point D on the Kummer surface and $d = (d_{n-1}, \cdots, d_1, d_0)_2$.
Output: dD.

1. $(A, B) \leftarrow ((0, 0, 0, 1), D)$;
2. for $i = n - 1$ down to 0 do
3. If $d_i = 0$, $(A, B) \leftarrow (2A, A + B)$;
4. If $d_i = 1$, $(A, B) \leftarrow (A + B, 2B)$;
5. end for
6. return A.

3 Special Points on Kummer Surface

In this section, we will find some special points of Kummer surface with respect to different pseudo-addition and doubling algorithms. We will also estimate the number of those special points. Special points will serve the zero-value attack in the next section.

In [3], the proposed ZVP attack utilizes the auxiliary register to take zero-values and reduces the computation overhead in ECC. Those points, which results in zeros in the auxiliary registers, are called Zero-Value points of ECC. Similarly, we can also define those special points on Kummer surface, which results in a reduction of computation overhead, as zero-value points.

As pointed earlier, scalar multiplications on Kummer surface involve the Montgomery adder, and different implementations of pseudo-addition and doubling cooperating with the Montgomery adder result in different Montgomery scalar multiplication algorithms. We will first analyze Duquesne's pseudo-addition and doubling formula [7,22] for the characteristic $p > 3$, and show how to find special points and evaluate the number of special points. Then we will apply our analysis on Gaudry's algorithm of pseudo-addition and doubling formula [12] which use Theta function, and other algorithms of pseudo-addition and doubling formula [8,14] for Characteristic 2.

3.1 The Possible Special Points for Duquesne's Pseudo-addition and Doubling Formula

The special points can occur on the computation of the pseudo-addition or the doubling. Now we analyze Duquesne's pseudo-addition and doubling formula [7,22] for the characteristic $p > 3$ as follows.

Theorem 1. *Let F_q be a field of characteristic $p \neq 2, 3$ and let C/F_q be a curve of genus 2. Let K be a Kummer surface of C and $(k_1 : k_2 : k_3 : k_4)$ a point on K. The point $(k_1 : k_2 : k_3 : k_4)$ is a special point for Montgomery scalar multiplication algorithm, which is instantiated with Duquesne's pseudo-addition and doubling formula [7,22], on the Kummer surface, if either of the following conditions are satisfied ($ord(K)$ denotes the order of K)*

1. $k_i = 0, i \in \{1, 2, 3, 4\}$;
2. $k_1 = \pm k_3 \mod ord(K)$.

Proof.
Kummer-based cryptosystems make use of Montgomery ladder (see algorithm 1), so both of pseudo-addition and doubling are needed per bit of the exponentiation. The cost of scalar multiplication algorithm is $59M + 12S$ according to [22], where M denotes field multiplication and S squaring. Here we assume $M = S$, then the total cost is $71M$ (We assume that $f_2^2, f_3^2, f_4^2, f_2f_4, f_2f_3f_4$ were precomputed. We also assume that before computing pseudo-addition and double, we first precompute $\{k_il_j\}_{i,j=1,\ldots,4}$ and $\{k_ik_j\}_{i,j=1,\ldots,4}$). We examine the conditions listed in the theorem.

Case $k_1 = 0$. The intermediate values related to k_1 in the doubling formulas are as follows:

$$k_1^2, k_1k_2, k_1k_3, k_1k_4, f_3k_1k_3,\ k_1k_2(k_1^2 - k_2^2),$$
$$k_1k_3((f_3^2 - 8f_3 + 8f_2^2 + 8f_4^2 - 4f_2f_3f_4)k_1k_3 + (7 - f_3^2 + 8f_2f_4)k_2k_4$$
$$+8f_2(k_3k_4 + k_1k_2) + 8f_4(k_2k_3 + k_1k_4)),$$
$$k_1k_3(8f_2(k_2k_3 + k_1k_4) + 8f_4(k_1k_2 + k_3k_4) + (16 + 8f_2f_4 - 2f_3^2)k_1k_3).$$

The intermediate values related to k_1 in the pseudo-addition formulas are $k_1l_1, k_1l_2, k_1l_3, k_1l_4$.
When $k_1 = 0$, the cost of doubling formulas can save $9M + 1S$, whereas the cost of addition formulas save $4M$. Therefore, the total cost reduces to $57M$ (let $M = S$) per bit of the Montgomery ladder.

Case $k_3 = 0$. It is the same as $k_1 = 0$, for k_1 and k_3 are symmetric in the Montgomery ladder.

Case $k_2 = 0$. The intermediate values related to k_2 in the doubling formulas are:

$$k_2^2, k_1k_2, k_2k_3, k_2k_4, (7 - f_3^2 + 8f_2f_4)k_2k_4,$$
$$k_2k_4(4f_2(k_1k_4 + k_2k_3) + 4f_4(k_1k_2 + k_3k_4) + f_3(k_2k_4 + 4(k_1^2 + k_3^2))),$$
$$k_1k_2(k_1^2 - k_2^2),\ 2k_2k_4(2f_3k_1k_3 - k_2k_4).$$

The intermediate values related to k_2 in the pseudo-addition formulas are k_2l_1, k_2l_3, k_2l_4.
It saves $7M + 1S$ in the doubling formulas in case of $k_2 = 0$, whereas it saves $3M$ in the addition formulas.

Case $k_4 = 0$. It is the same as $k_2 = 0$, for k_2 and k_4 are also symmetric in the formulas.

Case $k_1 = \pm k_3 \mod ord(K)$**.** In this case, $k_1^2 - k_3^2 = 0$. The intermediate values relating to $k_1^2 - k_3^2$ are as following.

$$2(k_1^2 - k_3^2)(f_3(k_1k_4 - k_2k_3) + 2(k_1k_2 - k_3k_4) + f_4(k_1^2 - k_3^2)),$$
$$2(k_1^2 - k_3^2)(f_3(k_1k_2 - k_3k_4) + f_2(k_1^2 - k_3^2) + 2(k_1k_4 - k_2k_3)).$$

Therefore, it saves $4M$ in the doubling formulas while it remains the same in the addition formulas.

We summarize the results in the following table.

Table 1. The cost of pseudo-addition and doubling in 4 cases

	standard	$k_1 = 0$ or $k_3 = 0$	$k_2 = 0$ or $k_4 = 0$	$k_1 = \pm k_3$
pseudo-addition	$31M$	$27M$	$28M$	$31M$
doubling	$40M$	$30M$	$32M$	$36M$
total	$71M$	$57M$	$60M$	$67M$

3.2 The Number of Special Points for Duquesne's Formula

Now we classify zero-value points on Kummer surface into two types, and estimate the number of points of each type.

type 1 special points: those points satisfying $k_i = 0, i \in \{1, 2, 3, 4\}$;
type 2 special points: those points satisfying $k_1 = \pm k_3 \mod ord(K)$.

Theorem 2. *Let $C : y^2 = f(x)$ be a genus 2 curve over a finite field F_q and κ be the map from the Jacobian of C into Kummer surface K. Then the number of **type 1** special points on this Kummer surface is about $4q$.*

Proof. We only consider the imaginary hyperelliptic curves of form

$$f(x) = x^5 + f_4x^4 + f_3x^3 + f_2x^2 + f_1x + f_0.$$

Then the points $(k_1 : k_2 : k_3 : k_4)$ on the Kummer surface satisfy the following function

$$K(k_1, k_2, k_3, k_4) = K_2(k_1, k_2, k_3)k_4^2 + K_1(k_1, k_2, k_3)k_4 + K_0(k_1, k_2, k_3) = 0.$$

Now we estimate the number of special points. In the case of $k_1 = 0$, the number of special points are equal to the number of solutions of equation $K(0, k_2, k_3, k_4) = 0$ in affine case, where

$$K_2(0, k_2, k_3) = k_2^2,\ K_1(0, k_2, k_3) = -2k_2k_3^2,\ K_0(0, k_2, k_3) = k_3^4.$$

That is

$$k_3^4 - 2k_2k_4k_3^2 + k_2^2k_4^2 = 0,\ \Rightarrow k_3^2 = k_2k_4.$$

Because $k_2, k_3, k_4 \in F_q$, it is easy to see the number of solutions to the equation $k_3^2 = k_2 k_4$ is about q^2. Therefore, there are about q special points for the case of $k_1 = 0$ (Note that the points of Kummer surface are in the projective space $\mathbb{P}^3(F_q)$).

We can estimate the number of special points when $k_i = 0, i \in \{2, 3, 4\}$ in the same way. Therefore, the total number of special points on Kummer surface is about $4q$. □

Theorem 3. *Let $C : y^2 = f(x)$ be a genus 2 curve over a finite field F_q and κ be the map from the Jacobian of C into Kummer surface K. Then the number of **type 2** special points on this Kummer surface is about $2q$.*

Proof. Let $(k_1 : k_2 : k_3 : k_4)$ be a point on the Kummer surface. Now we consider the **type 2 special point** , i.e., $k_1 = \pm k_3$. Since we consider the point in $\mathbb{P}^3(F_q)$, we assume $k_1 = 1$, then $k_3 = 1$ or $k_3 = -1$ as well.

The point $(1, k_2, 1, k_4)$ satisfy the quartic equation

$$K(1, k_2, 1, k_4) = K_2(1, k_2, 1)k_4^2 + K_1(1, k_2, 1)k_4 + K_0(1, k_2, 1) = 0,$$

where

$$\begin{aligned}
K_2(1, k_2, 1) &= k_2^2 - 4, \\
K_1(1, k_2, 1) &= -2k_2(1 + f_1 + f_3) - 4(f_0 + f_2 + f_4), \\
K_0(1, k_2, 1) &= (1 - 2f_3 + f_3^2 + 2f_1 + f_1^2 - 4f_2f_4 - 2f_1f_3 - 4f_0f_2) \\
&\quad + k_2(-4f_2 - 4f_1f_4 + 4f_0 - 4f_0f_3) - 4k_2^2(f_0f_4 + f_1) - 4k_2^3 f_0.
\end{aligned}$$

Let $A_1 = 1 + f_1 + f_3$, $A_2 = f_0 + f_2 + f_4$, $A_3 = 1 - 2f_3 + f_3^2 + 2f_1 + f_1^2 - 4f_2f_4 - 2f_1f_3 - 4f_0f_2$, $A_4 = -4f_2 - 4f_1f_4 + 4f_0 - 4f_0f_3$, $A_5 = f_0f_4 + f_1$, $A_6 = f_0$, then k_2 and k_4 satisfy the following equation

$$(k_2^2 - 4)k_4^2 - (2A_1k_2 + 4A_2)k_4 - 4A_6k_2^3 - 4A_5k_2^2 + A_4k_2 + A_3 = 0.$$

The number of solutions to the above equation is about q. In this proof, we have assumed $k_1 = 1$ which is the first coordinate of the point. So the point denotes its equivalence class. The case of $k_3 = -1$ can be estimated in the same way. Therefore, there are about $2q$ special points for **type 2**. □

In total, there are about $6q$ special points for ZVP, whereas the number of points on a Kummer surface are about q^2 in a finite field F_q. Thus the special points account for $6/q$ of the total points.

In the following, we will give a simple example to show that there are about $6q$ points that have zero values during the computation of scalar multiplication on the Kummer surface. The data in Table 2 was computed via the Magma computer algebra system [23].

Example 1. Consider a hyperelliptic curve $y^2 = x^5 + x^3 + x + 4$ over F_{11}. The order of the Jacobian is 107. The corresponding Kummer surface is:

$$\begin{aligned}
&x_1^4 + 6x_1^3x_2 + 9x_1^3x_3 + 6x_1^3x_4 + 5x_1^2x_2x_3 + 9x_1^2x_2x_4 + 3x_1^2x_3^2 + 6x_1x_2^3 \\
&+7x_1x_2^2x_3 + 9x_1x_2x_3x_4 + 9x_1x_3^3 + 7x_1x_3x_4^2 + x_2^2x_4^2 + 9x_2x_3^2x_4 + x_3^4.
\end{aligned}$$

Choose a random point $P = (1 : 1 : 8 : 7)$ on Kummer surface with order 107. The result of the scalar multiplication iP are listed in Table 2.

Table 2. iP, $i = 1, \cdots, 107$

2P, 105P	(1 : 1 : 2 : 9)	28P, 79P	(0 : 1 : 7 : 5)
3P, 104P	(1 : 2 : 9 : 6)	29P, 78P	(1 : 7 : 8 : 3)
4P, 103P	(1 : 8 : 8 : 7)	30P, 77P	(1 : 7 : 0 : 6)
5P, 102P	(1 : 0 : 8 : 1)	31P, 76P	(0 : 1 : 6 : 3)
6P, 101P	(1 : 4 : 7 : 2)	32P, 75P	(1 : 5 : 0 : 0)
7P, 100P	(1 : 9 : 10 : 4)	33P, 74P	(1 : 8 : 10 : 3)
8P, 99P	(1 : 3 : 6 : 2)	34P, 73P	(1 : 1 : 1 : 10)
9P, 98P	(1 : 0 : 0 : 9)	35P, 72P	(1 : 0 : 3 : 9)
10P, 97P	(1 : 3 : 10 : 4)	36P, 71P	(1 : 6 : 3 : 8)
11P, 96P	(0 : 1 : 10 : 1)	37P, 70P	(1 : 4 : 6 : 9)
12P, 95P	(1 : 5 : 7 : 7)	38P, 69P	(1 : 10 : 0 : 3)
13P, 94P	(1 : 3 : 3 : 6)	39P, 68P	(1 : 6 : 4 : 0)
14P, 93P	(1 : 4 : 8 : 8)	40P, 67P	(1 : 3 : 9 : 9)
15P, 92P	(1 : 4 : 6 : 1)	41P, 66P	(1 : 6 : 1 : 2)
16P, 91P	(1 : 4 : 9 : 2)	42P, 65P	(1 : 5 : 5 : 10)
17P, 90P	(1 : 6 : 4 : 9)	43P, 64P	(1 : 1 : 6 : 8)
18P, 89P	(1 : 6 : 0 : 10)	44P, 63P	(1 : 5 : 1 : 5)
19P, 88P	(1 : 9 : 2 : 9)	45P, 62P	(1 : 1 : 3 : 1)
20P, 87P	(1 : 5 : 5 : 9)	46P, 61P	(1 : 10 : 4 : 1)
21P, 86P	(1 : 7 : 0 : 0)	47P, 60P	(1 : 10 : 0 : 0)
22P, 85P	(1 : 9 : 1 : 9)	48P, 59P	(1 : 2 : 9 : 0)
23P, 84P	(1 : 5 : 0 : 5)	49P, 58P	(0 : 1 : 0 : 0)
24P, 83P	(1 : 10 : 1 : 1)	50P, 57P	(1 : 0 : 8 : 4)
25P, 82P	(1 : 6 : 7 : 10)	51P, 56P	(1 : 3 : 5 : 8)
26P, 81P	(0 : 1 : 5 : 3)	52P, 55P	(1 : 10 : 3 : 10)
27P, 80P	(1 : 6 : 0 : 3)	53P, 54P	(1 : 1 : 2 : 4)
P, 106P	(1 : 1 : 8 : 7)	107P	(0 : 0 : 0 : 1)

We can see there are 27 special points except $(0 : 0 : 0 : 1)$ in Table 2, which constitute for 51% of the total (107-1)/2=53 Kummer points.

3.3 Special Points due to other Pseudo-addition and Doubling Formula

The special points vary with different implementations of pseudo-addition and doubling. Other variant algorithms for pseudo-addition and doubling on Kummer surface are Gaudry's algorithm [12] using Theta function, Duquesne's algorithm [8] and GL's algorithm [14] which works for characteristic 2. Similarly, we can exploit special points for these algorithms. We summarize the results in the following theorems, and we omit the proofs since they are similar to that of Theorem 1.

Possible special points with Gaudry's algorithm [12]

Theorem 4. *Let K be a Kummer surface and $(k_1 : k_2 : k_3 : k_4)$ be a point over K. The point $(k_1 : k_2 : k_3 : k_4)$ is a special point for Montgomery scalar multiplication algorithm, which is instantiated with Gaudry's pseudo-addition and doubling formula [12], on the Kummer surface, if either of the following conditions is satisfied*

1. $k_1 = k_2$ *and* $k_3 = k_4$;
2. $k_1 = k_3$ *and* $k_2 = k_4$;
3. $k_2 = k_3 = k_4$.

Possible special points with Duquesne's Algorithm [8]

Theorem 5. *Let F_q be a field of characteristic $p = 2$ and let C/F_q be a curve of genus 2. Let K be a Kummer surface of C and $(k_1 : k_2 : k_3 : k_4)$ be a point over K. The point $(k_1 : k_2 : k_3 : k_4)$ is a special point for Montgomery scalar multiplication algorithm, which is instantiated with Duquesne's pseudo-addition and doubling formula [8] for characteristic $p = 2$, if there exists an $i \in \{1, 2, 3, 4\}$ such that $k_i = 0$.*

Possible special points with GL's Algorithm [14]

Theorem 6. *Let F_q be a field of characteristic $p = 2$ and K be a Kummer surface. Let $(k_1 : k_2 : k_3 : k_4)$ be a point over K. The point $(k_1 : k_2 : k_3 : k_4)$ is a special point for Montgomery scalar multiplication algorithm, which is instantiated with GL's pseudo-addition and doubling formula [14] for characteristic $p = 2$, if either one of the following conditions is satisfied*

1. $k_i = 0$, $i \in \{1, 2, 3, 4\}$;
2. $k_1 = k_2$ *and* $k_3 = k_4$;
3. $k_1 = k_4$ *and* $k_2 = k_3$;
4. $k_1 = k_3$ *and* $k_2 = k_4$.

4 Zero-Value Point Attacks on Kummer Surface

According to Table 1, the special points of type I and II lead to some loss of computational overhead, compared with common points on the Kummer surface. How to make use of this property to exploit the secret scalar is just a kind of Zero-Value-Point (ZVP) attack. The special points on the Kummer space may not all have zeros in some coordinates, but the special points play the same role as the zero-value points in the ZVP attack in [3]. Hence those special points can be regarded as the generalized zero-value points. Here we show some general idea how the ZVP attack exploits the computational difference of the special points to reveal the secret scalar d..

Let $d = (d_{n-1}, d_{n-2}, \ldots, d_0)_2$ be the secret scalar. Suppose that it is free to compute dQ for any point Q on the Kummer surface. The ZVP attack will reveal the secret scalar bit by bit by adaptively choosing the base point Q. Suppose

that the $n-j-1$ most significant bits $(d_{n-1}, d_{n-2}, \cdots, d_{j+1})_2$ are known, the ZVP attack will guess the $n-j$-th bit d_j due to the fact that the zero-value point will result in different computational overhead of pseudo-addition and doubling depending on $d_j = 0$ or $d_j = 1$.

The previous zero-value point attacks(e.g., [2, Chapter 29].) applied to Montgomery ladder scalar multiplication over ECC or HECC. However, things are different on the Kummer surface. As will show in the next subsection, when a special point happens (**type 1** or **type 2**), the doubling formulas will results in a heavier computational loss than the pseudo-addition formulas.

4.1 General Zero-Value Point Attacks on Kummer Surface

In the Montgomery scalar multiplication algorithm of computing dP in section 3, both a pseudo-addition and a doubling are involved in each loop. If the current bit $d_i = 0$, (A, B) is updated by $(2A, A+B)$; if $d_i = 1$, (A, B) is updated by $(A+B, 2B)$. Note that $B = A + P$ always holds in each loop.

If both A and B are common (not special) points then the computation in each loop will be $7\mathbf{1}M$. However, things are different when A or B is a special point, as shown in Table 3 and 4.

Table 3. Computational loss when $A = (k_1 : k_2 : k_3 : k_4)$ is a special point and $B = (l_1 : l_2 : l_3 : l_4)$ is a normal point

	when $k_1 = 0$ or $k_3 = 0$	when $k_2 = 0$ or $k_4 = 0$	when $k_1 = \pm k_3$
$d_i = 0$ Computational loss of $(2A, A+B)$	$14M$	$10M$	$4M$
Ratio of loss	$14/71 = 19.7\%$	$10/71 = 14.1\%$	$4/71 = 5.6\%$
$d_i = 1$ Computational loss of $(A+B, 2B)$	$4M$	$3M$	0
Ratio of loss	$4/71 = 5.6\%$	$3/71 = 4.2\%$	0%

When A is a special point, it may lead to a significant loss of computational overhead for $d_i = 0$, but slight loss for $d_i = 1$. On the other hand, when B is a special point, it may lead to a significant loss of computational overhead for $d_i = 1$, but slight loss for $d_i = 0$. This phenomenon helps us to design a ZVP attack to guess the value of bit d_i.

Assume that the $n-j-1$ most significant bits $(d_{n-1}, d_{n-2}, \cdots, d_{j+1})_2$ of scalar d are known. Now we want to determine the value of the j-th bit $d_j \in \{0, 1\}$. If we have a correct guess of d_j, then $A = \left(\sum_{i=j}^{n-1} d_i 2^{i-j}\right) P$ and $B = \left(\sum_{i=j}^{n-1} d_i 2^{i-j} + 1\right) P$ after $n-j$ loops in the Montgomery scalar multiplication algorithm. If we choose the base point P such that $A = \left(\sum_{i=j}^{n-1} d_i 2^{i-j}\right) P$ or $B =$

Table 4. Computational loss when $A = (k_1 : k_2 : k_3 : k_4)$ is a normal point and $B = (l_1 : l_2 : l_3 : l_4)$ is a special point

	when $l_1 = 0$ or $l_3 = 0$	when $l_2 = 0$ or $l_4 = 0$	when $l_1 = \pm l_3$
$d_i = 0$ Computational loss of $(2A, A + B)$	$4M$	$3M$	0
Ratio of loss	$4/71 = 5.6\%$	$3/71 = 4.2\%$	0%
$d_i = 1$ Computational loss of $(A + B, 2B)$	$14M$	$10M$	$4M$
Ratio of loss	$14/71 = 19.7\%$	$10/71 = 14.1\%$	$4/71 = 5.6\%$

$\left(\sum_{i=j}^{n-1} d_i 2^{i-j} + 1\right) P$ is a special value, the power consumption will be different from the normal consumption during the $n - j + 1$-*th* loop.

On the other hand, if the guess of d_j is not correct, then the power consumption will be as normal as usual during the $n - j + 1$-*th* loop.

Let H be a set of elements including the **type 1** and **type 2** special points. The next algorithm shows how to implement the attack in detail.

Algorithm 2. Zero-value point attack on Kummer surface

Input: H, $(d_{n-1}, d_{n-2}, \cdots, d_{j+1})_2$;
Output: d_j;

0) Guess $d_j = 0$;
1) for $l = 1$ to m
2) Choose an element $P_l \in H$. Compute $k = \sum_{i=j}^{n-1} d_i 2^{i-j}$ and compute point $P'_l = k^{-1} P_l$. Check that

$$(k - d_j + \overline{d}_j) P'_l \text{ not in } H,$$

where $\overline{d}_j = (d_j + 1) \mod 2$, otherwise choose another value for $P_l \in H$.
3) Compute $C_l = dP'_l$ and record the power consumption of C_l as T_l;
4) end for;
5) Compute the average power consumption $T = \frac{1}{m} \sum_{l=1}^{m} T_l$;
1′) for $l = 1$ to m
2′) Choose an element $Q_l \in H$. Compute $k = \sum_{i=j}^{n-1} d_i 2^{i-j} + 1$ and compute point $Q'_l = k^{-1} Q_l$. Check that

$$(k - d_j + \overline{d}_j) Q'_l \text{ not in } H,$$

where $\overline{d}_j = (d_j + 1) \mod 2$, otherwise choose another value for $Q_l \in H$.
3′) Compute $C'_l = dQ'_l$ and record the power consumption of C'_l as T'_l;

4′) end for;

5′) Compute the average power consumption $T' = \frac{1}{m}\sum_{l=1}^{m} T'_l$;

6) If either T or T' is smaller than the normal average power consumption, output $d_j = 0$; otherwise output $d_j = 1$.

Note: When the guess of d_j is correct, Algorithm 2 also suggests a guess of d_{j-1} according to Table 3 and 4. If the power consumption of T is much less than that of T', then $d_{j-1} = 0$; if the power consumption of T' is much less than that of T, then $d_{j-1} = 1$.

4.2 A Variant of Zero-Value Point Attack on Kummer Surface

We observed that there is a big different power consumption between the pseudo-addition and doubling formulas when a special point happens. We can exploit this difference to get a simplified attack.

Given the $n-j-1$ most significant bits $(d_{n-1}, d_{n-2}, \cdots, d_{j+1})_2$ of scalar d, we have $A = \left(\sum_{i=j+1}^{n-1} d_i 2^{i-j-1}\right) P$ and $B = \left(\sum_{i=j+1}^{n-1} d_i 2^{i-j-1} + 1\right) P$ after $n-j-1$ loops in the Montgomery scalar multiplication algorithm. If we choose the base point P such that $A = \left(\sum_{i=j}^{n-1} d_i 2^{i-j}\right) P$, the power consumption of $d_j = 0$ will be much less than that of $d_j = 1$ in the $(n-j)$-th loop.

Let H be a set of elements including the **type 1** and **type 2** special points and $d = (d_{n-1}, \cdots, d_1, d_0)$. Suppose that the most significant bits $d_{n-1}, d_{n-2}, \cdots, d_{j+1}$ of the secret scalar d are known and now we want to discover the next bit d_j.

Algorithm 3. New ZVP attack on Kummer surface

Input: H, $(d_{n-1}, d_{n-2}, \cdots, d_{j+1})_2$;
Output: d_j;

1) for $l = 1$ to m

2) Choose an element $P_l \in H$ and compute $k = \sum_{i=j+1}^{n-1} d_i 2^{i-j-1}$ and $P'_l = k^{-1} P_l$. Check that
$$(k+1)P'_l \text{ not in } H,$$

3) Compute $C_l = dP'_l$ and record the power analysis of C_l as T_l;

4) end for;

5) Compute the average power analysis $T = \frac{1}{m}\sum_{l=1}^{m} T_l$;

6) If T is much less than normal, then output $d_j = 0$, otherwise output $d_j = 1$.

5 Countermeasures Against Zero-Value Point Attacks

Smart showed the method to avoid the ZVP attack on ECC in [26]. In 2004, Avanzi [1] generalized the ZVP attack to HECC and also provided the countermeasures, consisting of scalar randomization and message blinding. Below we will show the principles of those countermeasures and why scalar randomization does not work for the ZVP attack on Kummer-based cryptosystems.

Denote D as a point on a Kummer surface and d a secret scalar. In the following, the order of the Kummer surface is assumed to be known.

Message Blinding Method: To compute dD, we compute an additional scalar multiplication $S = dB$ first, where B is a random point of large order. Then, the scalar multiplication dD is computed as

$$dD = d(D + B) - S.$$

The above blinding process works well for ECC and HECC, it doesn't work on the Kummer surface. The reason is that the computation of $d(D+B)$ needs the information of $D - B$ and the computation of $d(D + B) - S$ needs the value of $d(D + B) + S$ beforehand. Generally it is impossible to get the value of $D - B$ or $d(D + B) + S$. Therefore, the message blinding method won't work on the Kummer surface.

Scalar Blinding Method: The idea of scalar blinding method is to change the representation of the scalar. Given the order of the Kummer surface K, denoted by $ord(K)$, it is easy to see that $dD = (d + i * ord(K))D$ holds for any integer i. Set $d' = d + r \cdot ord(K)$ with r a random integer, then $dD = d'D$.

The additional computation caused by the scalar blinding depends on the bit length of r. To resist the zero-value point attacks, r should be big enough, yet not too big (for example, $r \approx 2^{20}$).

It seems that the scalar blinding method is the only one to resist the zero-value point attack on the Kummer surface.

6 Conclusion

In this paper, we proposed zero-value point attacks on the Kummer-based cryptosystem. We found some special points on Kummer surface and estimated the number of those special points on Kummer surface. We showed that there are as many as $6q$ special points on a Kummer surface associated with a hyperelliptic curve of genus 2, compared to about q ZVPs on the corresponding hyperelliptic curve over $\mathbb{F}_q$. On the other hand, most of the countermeasures against ZVP attacks on HECC do not work for Kummer surfaces, which makes ZVP attacks a more powerful side-channel attacks for Kummer-based cryptosystems. We pointed out that the only possible countermeasure to avoid ZVP attacks is to blind random scalars to scalar multiplications.

References

1. Avanzi, R.M.: Aspects of Hyperelliptic Curves over Large Prime Fields in Software Implementations. In: Joye, M., Quisquater, J.-J. (eds.) CHES 2004. LNCS, vol. 3156, pp. 148–162. Springer, Heidelberg (2004)
2. Avanzi, R., Cohen, H., Doche, C., Frey, G., Lange, T., Nguyen, K., Vercauteren, F.: Handbook of elliptic and hyperelliptic curve cryptography. CRC Press, Boca Raton (2005)
3. Akishita, T., Takagi, T.: Zero-Value Point Attacks on Elliptic Curve Cryptosystem. In: Boyd, C., Mao, W. (eds.) ISC 2003. LNCS, vol. 2851, pp. 218–233. Springer, Heidelberg (2003)
4. Cantor, D.G.: Computing on the Jacobin of a hyperelliptic curve. Math. Comp. 48, 95–101 (1987)
5. Coron, J.-S.: Resistance against Differential Power Analysis for Elliptic Curve Cryptosystems. In: Koç, Ç.K., Paar, C. (eds.) CHES 1999. LNCS, vol. 1717, pp. 292–302. Springer, Heidelberg (1999)
6. Cassels, J.W.S., Flynn, E.V.: Prolegomena to a middlebrow arithmetic of curves of genus 2. Cambridge University Press, Cambridge (1996)
7. Duquesne, S.: Montgomery Scalar Multiplication for Genus 2 Curves. In: Buell, D.A. (ed.) ANTS 2004. LNCS, vol. 3076, pp. 153–168. Springer, Heidelberg (2004)
8. Duquesne, S.: Montgomery Ladder for All Genus 2 Curves in Characteristic 2. In: von zur Gathen, J., Imaña, J.L., Koç, Ç.K. (eds.) WAIFI 2008. LNCS, vol. 5130, pp. 174–188. Springer, Heidelberg (2008)
9. Duquesne, S.: Traces of the group law on the Kummer surface of a curve of genus 2 in characteristic 2. Math. Comput. Sci. 3, 173–183 (2010)
10. Fan, J., Guo, X., De Mulder, E., Schaumont, P., Preneel, B., Verbauwhede, I.: State-of-the-art of secure ECC implementations: a survey on known side-channel attacks and countermeasures. In: Hardware-Oriented Security and Trust (HOST 2010), pp. 76–87. IEEE (2010)
11. Flynn, E.V.: The group law on the jacobian of a curve of genus 2. J. Reine. Angew. Math. 439, 45–69 (1995)
12. Gaudry, P.: Fast genus 2 arithmetic based on Theta functions. Journal of Mathematical Cryptology 1, 243–265 (2007)
13. Goubin, L.: A Refined Power-Analysis Attack on Elliptic Curve Cryptosystems. In: Desmedt, Y.G. (ed.) PKC 2003. LNCS, vol. 2567, pp. 199–210. Springer, Heidelberg (2002)
14. Gaudry, P., Lubicz, D.: The arithmetic of characteristic 2 Kummer surfaces and of elliptic Kummer lines. Finite Fields and Their Applications 15(2), 246–260 (2009)
15. Harley, R.: Fast arithmetic on genus 2 curves (2000), `http://cristal.inria/fr/~harley/hyper`
16. Joye, M., Tymen, C.: Protections against Differential Analysis for Elliptic Curve Cryptography. In: Koç, Ç.K., Naccache, D., Paar, C. (eds.) CHES 2001. LNCS, vol. 2162, pp. 377–390. Springer, Heidelberg (2001)
17. Joye, M., Quisquater, J.-J.: Hessian Elliptic Curves and Side-Channel Attacks. In: Koç, Ç.K., Naccache, D., Paar, C. (eds.) CHES 2001. LNCS, vol. 2162, pp. 402–410. Springer, Heidelberg (2001)
18. Koblitz, N.: Hyperelliptic cryptosystems. J. Cryptology 1, 139–150 (1989)
19. Kocher, P., Jaffe, J., Jun, B.: Introduction to Differential Power Analysis and Related Attacks. Technical Report, Cryptography Research Inc. (1998), `http://www.cryptography.com/dpa/technical/index.html`

20. Kocher, P.C., Jaffe, J., Jun, B.: Differential Power Analysis. In: Wiener, M. (ed.) CRYPTO 1999. LNCS, vol. 1666, p. 388. Springer, Heidelberg (1999)
21. Liardet, P.-Y., Smart, N.P.: Preventing SPA/DPA in ECC Systems Using the Jacobi Form. In: Koç, Ç.K., Naccache, D., Paar, C. (eds.) CHES 2001. LNCS, vol. 2162, pp. 391–411. Springer, Heidelberg (2001)
22. Lin, Q., Zhang, F.: Scalar Multiplication on Kummer Surface Revisited. IEICE Trans. Fundamentals E95-A(1), 410–413 (2012)
23. MAGMA Computational Algebra System, `http://magma.maths.usyd.edu.au/magma/`
24. Montgomery, P.L.: Speeding up the Pollard and elliptic curve methods of factorization. Mathematics of Computation 48(177), 243–264 (1987)
25. Müller, J.S.: Explicit Kummer surface formulas for arbitrary characteristic. LMS J. Comput. Math. 13, 47–64 (2010)
26. Smart, N.P.: An Analysis of Goubin's Refined Power Analysis Attack. In: Walter, C.D., Koç, Ç.K., Paar, C. (eds.) CHES 2003. LNCS, vol. 2779, pp. 281–290. Springer, Heidelberg (2003)
27. Smart, N.P.: The Hessian Form of an Elliptic Curve. In: Koç, Ç.K., Naccache, D., Paar, C. (eds.) CHES 2001. LNCS, vol. 2162, pp. 118–125. Springer, Heidelberg (2001)
28. Smart, N., Siksek, S.: A fast Diffie-Hellman protocol in genus 2. J. of Cryptology 12, 67–73 (1999)