Hashing into Hessian Curves

Reza Rezaeian Farashahi
Department of Computing
Macquarie University
Sydney, NSW 2109, Australia

Abstract

We describe a hashing function from the elements of the finite field $\mathbb{F}_q$ into points on a Hessian curve. Our function features the uniform and smaller size for the cardinalities of almost all fibers compared with the other known hashing functions for elliptic curves. Moreover, a point on the image set of the function is uniquely given by its abscissa. For ordinary Hessian curves, the cardinality of the image set of the function is exactly given by $(q+i)/2$ for some $i = 1, 2, 3$.

Keywords: Elliptic curve cryptography, Hessian curve, hashing

2000 Mathematics Subject Classification: 11G05, 11T06, 14H52

1 Introduction

It is well-known that many cryptographic schemes based on elliptic curves require efficient hashing of finite field elements into points on a given elliptic curve. Examples are the Boneh- Franklin identity based encryption scheme [1], the SPEKE (Simple Password Exponential Key Ex- change) [10] and the PAK (Password Authenticated Key exchange) [3].

We note that designing an efficient hash function from field elements to points on an elliptic curve has been an open problem for quite a long time. Recently, two constructions have appeared, that of Shallue and van de Woestjine [16] and also of Icart [9]. Furthermore, Farashahi, Shparlinski and Voloch have studied the properties of the

Icart's function and also slightly adjust and prove the asymptotic formula for its image size conjectured in [9]. Also, analogous arguments for both hash functions have recently been presented by Fouque and Tibouchi [6].

Moreover, designing an injective efficient function from fields element into the points of a given elliptic curve is a challenging problem. Such functions will have several applications in many cryptographic schemes based on elliptic curves and in designing cryptographically secure pseudorandom generators with elliptic curves. Alternatively, one may consider functions with the small size of preimages, for instance a function that is $2:1$ for all points.

In this paper, we describe a function from fields element to the points on an elliptic Hessian curves. The use of Hessian curves in cryptography has been studied in [4, 11, 17, 7, 8]. Moreover, recently very efficient and fast unified addition formulas for Hessian curves have provided, see [13, 2]. Our technique to obtain a hash function for Hessian curves is similar to that of Icart's technique [9] which is based on computing the cubic root of a field element. Moreover, our function, is a $2:1$ map at almost all points, which gives the uniform and small size 2 for the cardinalities of the fibers.

Throughout the paper, for a field $\mathbb{F}$, we denote its algebraic closure by $\overline{\mathbb{F}}$ and its multiplicative subgroup by $\mathbb{F}^*$. The letter p always denotes a prime number and the letter q always denotes a prime power. As usual, $\mathbb{F}_q$ is a finite field of size q. The cardinality of a finite set $\mathcal{S}$ is denoted by $\#\mathcal{S}$.

For $p > 2$, let χ be the quadratic character in $\mathbb{F}_q$. So, for $x \in \mathbb{F}_q$, we have $\chi(x) = 0, 1$ or -1, if $x = 0$, $x = w^2$ for some $w \neq 0$ or $x \neq w^2$ for all $w \in \mathbb{F}_q$, respectively. Moreover, for $p = 2$ and $x \in \mathbb{F}_q$, let $\chi(x) = 0$.

2 Backgrounds on Hessian Curves

A Hessian curve H_d over a finite field $\mathbb{F}_q$ is given by the equation

$$\mathrm{H}_d \;:\; x^3 + y^3 + 1 = 3dxy, \tag{1}$$

where $d \in \mathbb{F}_q$ with $d^3 \neq 1$, see [12].

We recall that the set of $\mathbb{F}_q$-rational points of H_d denoted by $\mathrm{H}_d(\mathbb{F}_q)$ forms an Abelian group. For $q \equiv 2 \pmod 3$, the Hessian curve H_d has one $\mathbb{F}_q$-rational point at infinity $\mathcal{O}$ that is the neutral element of the group. For the affine point P of H_d, the x-coordinate of P is denoted by $x(P)$.

Let π_d be the projection map $\pi_d : \mathrm{H}_d(\mathbb{F}_q) \longrightarrow \mathbb{F}_q \bigcup \{\infty\}$ defined by $\pi_d(P) = x(P)$ if $P \neq \mathcal{O}$ and $\pi_d(P) = \infty$ if $P = \mathcal{O}$.

Let $\mathcal{X}_d$ be the subset of $\mathbb{F}_q$ given by

$$\mathcal{X}_d = \left\{x \in \mathbb{F}_q : 1 \leq \#\pi_d^{-1}(x) \leq 2\right\}. \tag{2}$$

In other words, $\mathcal{X}_d$ is the the set of elements $x \in \mathbb{F}_q$ so that there exist only one or two affine points P in $\mathrm{H}_d(\mathbb{F}_q)$ with $x(P) = x$.

Proposition 1. *Let $q \equiv 2 \pmod 3$ and let H_d be a Hessian curve over $\mathbb{F}_q$ defined by the equation (1) with $d \neq 1$. For the cardinality of the set $\mathcal{X}_d$, given by equation (2), we have*

$$\#\mathcal{X}_d = \begin{cases} q, & \text{if } d = 0, \\ \left(q + \chi(d^4 - d)\right)/2, & \text{if } d \neq 0. \end{cases}$$

Proof. We note that, the map $\kappa : \mathbb{F}_q \to \mathbb{F}_q$ by $\kappa(x) = x^3$ is a bijection, since $q \equiv 2 \pmod 3$. For an element $x \in \mathbb{F}_q$, we have $\#\pi_d^{-1}(x) = 1$ if and only if the polynomial $g_x = Y^3 - 3dxY + x^3 + 1$ has at most two distinct irreducible factors in $\mathbb{F}_q[Y]$. We distinguish the following possibilities for d and p.

- If $d = 0$, for all $x \in \mathbb{F}_q$ the polynomial g_x has only one root in $\mathbb{F}_q$, since κ is a bijection over $\mathbb{F}_q$. So, $\#\mathcal{X}_d = q$.
- We assume that $d \neq 0$ and $p \neq 2$. For $x \in \mathbb{F}_q$, let Δ_x be the discriminant of g_x, that is

  $$\Delta_x = -27(x^6 + 2(1 - 2d^3)x^3 + 1).$$

  If $\Delta_x \neq 0$, then the number of irreducible factors of g_x over $\mathbb{F}_q$ equals 2 if and only if Δ_x is a quadratic non-residue element of $\mathbb{F}_q$ (see [14, 5] or [15, Corollary 1]). Therefore, we have

  $$\#\mathcal{X}_d = \sum_{x \in \mathbb{F}_q, \chi(\Delta_x) \neq 1} 1.$$

  We recall that the map κ is a bijection over $\mathbb{F}_q$. For $x \in \mathbb{F}_q$, let

  $$\mathcal{D}_x = x^2 + 2(1 - 2d^3)x + 1.$$

For $q \equiv 2 \pmod 3$, we have $\chi(-3) = -1$. Therefore, we obtain

$$\#\mathcal{X}_d = \textstyle\sum_{x \in \mathbb{F}_q, \chi(\mathcal{D}_x) \neq -1} 1 = \sum_{x \in \mathbb{F}_q} \frac{1+\chi(\mathcal{D}_x)}{2} + \sum_{x \in \mathbb{F}_q, \mathcal{D}_x = 0} \frac{1}{2}.$$

We note that $\sum_{x \in \mathbb{F}_q} \chi(\mathcal{D}_x) = -1$ if $d^4 - d \neq 0$. Moreover, there are two distinct values of $x \in \mathbb{F}_q$ with $\mathcal{D}_x = 0$ if and only if $\chi(d^4 - d) = 1$. So, for $d \neq 0$, we have

$$\#\mathcal{X}_d = \tfrac{q-1}{2} + \tfrac{1+\chi(d^4-d)}{2} = \tfrac{q+\chi(d^4-d)}{2}.$$

- Now, we assume that $p = 2$ and $d \neq 0$. For $x = 1$, the polynomial g_x has the roots $y = 0, \sqrt{d}$ in $\mathbb{F}_q$. Also, for $x \in \mathbb{F}_q$ with $x \neq 1$, the number of irreducible factors of g_x over $\mathbb{F}_q$ equals 2 if and only if the polynomial $T^2 + T + (-3dx)^3/(x^3+1)^2$ factors over $\mathbb{F}_q$ (see [18, Lemma 4.2]). The latter is equivalent to $\mathrm{Tr}(\Delta_x) = 0$, where
$$\Delta_x = d^3x^3/(x^3+1)^2.$$
Therefore, we have
$$\#\mathcal{X}_d = 1 + \sum_{x \in \mathbb{F}_q, x \neq 1, \mathrm{Tr}(\Delta_x) = 0} 1.$$
For $q \equiv 2$ (mod 3), the map κ is a bijection. Hence,
$$\begin{aligned}\#\mathcal{X}_d &= 1 + \sum_{x \in \mathbb{F}_q,\, x \neq 1,\, \mathrm{Tr}\left(\frac{d^3x}{(x+1)^2}\right) = 0} 1 \\ &= 1 + \sum_{x \in \mathbb{F}_q^*,\, \mathrm{Tr}\left(d^3(\frac{1}{x} + \frac{1}{x^2})\right) = 0} 1 \\ &= \sum_{x \in \mathbb{F}_q,\, \mathrm{Tr}(d^3(x^2+x)) = 0} 1.\end{aligned}$$
Then, one can see that $\#\mathcal{X}_d = q/2$ if $d^3 \neq 0, 1$.

So, the proof of Proposition 1 is complete. □

3 Our Results

Let $\mathbb{F}_q$ be the finite field with $q \equiv 2 \pmod 3$ and let H_d be the Hessian curve over $\mathbb{F}_q$ defined by the equation (1), where $d^3 \neq 1$. In this section, we define an encoding map from the elements of $\mathbb{F}_q$ to the $\mathbb{F}_q$-rational points of H_d. We also describe the bijection between the set of affine points of the image set of this map and the set $\mathcal{X}_d$, give by equation (2). Then, we obtain the cardinality of the image set of the map.

3.1 The encoding map from $\mathbb{F}_q$ to $\mathrm{H}_d(\mathbb{F}_q)$

Let α be a function $\alpha : \mathbb{F}_q \longrightarrow \mathbb{F}_q$. If the function α is not defined at some element of $\mathbb{F}_q$, we adjoin ∞ to $\mathbb{F}_q$ as a possible value of the function α at this element.

For $q \equiv 2 \pmod 3$, we consider the map

$$h_{\alpha;d} : \mathbb{F}_q \longrightarrow \mathrm{H}_d(\mathbb{F}_q) \tag{3}$$

defined by $h_{\alpha;d}(u) = (x, y)$ if $\alpha(u) \neq -1, \infty$, where

$$x = -\alpha(u)\left(\frac{d^3\alpha^3(u)+1}{\alpha^3(u)+1}\right)^{1/3}, \ y = -\left(\frac{d^3\alpha^3(u)+1}{\alpha^3(u)+1}\right)^{1/3} + d\alpha(u) \tag{4}$$

and $h_{\alpha;d}(u) = \mathcal{O}$ if $\alpha(u) = -1, \infty$.

We note that the map $h_{\alpha;d}$ is well defined. We let

$$\mathcal{H}_{\alpha;d} = h_{\alpha;d}(\mathbb{F}_q),$$

that is the image set of the map $h_{\alpha;d}$. We also note that, for a point $P = (x, y) \in \mathrm{H}_d(\mathbb{F}_q)$, we have $P \in \mathcal{H}_{\alpha;d}$ if and only if there exists an element $u \in \mathbb{F}_q$ satisfying

$$d\alpha^2(u) - \alpha(u)y + x = 0. \tag{5}$$

Notice that if $d = 0$, then the Hessian curve H_d is supersingular with $\#\mathrm{H}_d(\mathbb{F}_q) = q + 1$. In this case, the map $h_{\alpha;d}$ is injective if α is injective. In other words, for all points $P \in \mathcal{H}_{\alpha;d}$ we have $\#h^{-1}_{\alpha;d}(P) = 1$, if $\alpha(\mathbb{F}_q) = \mathbb{F}_q$. So, for $d = 0$, we have $\#\mathcal{H}_{\alpha;d} = q$, if α is a bijection over $\mathbb{F}_q$.

3.2 Size of the image set $\mathcal{H}_{\alpha;d}$

From now on, we assume that $d \neq 0$. The following theorem gives the explicit formulas for the cardinality of the image set $\mathcal{H}_{\alpha;d} = h_{\alpha;d}(\mathbb{F}_q)$, where α is a bijection over $\mathbb{F}_q$.

Theorem 2. *Let $q \equiv 2 \pmod 3$ and let H_d be a Hessian curve over $\mathbb{F}_q$ defined by the equation (1) with $d \neq 0, 1$. Let $h_{\alpha;d}$ be the map defined by the equation (3). If $\alpha : \mathbb{F}_q \longrightarrow \mathbb{F}_q$ is a bijective function, for the cardinality of the image set $\mathcal{H}_{\alpha;d} = h_{\alpha;d}(\mathbb{F}_q)$, we have*

$$\#\mathcal{H}_{\alpha;d} = \left(q + \chi(d^4 - d) + 2\right)/2.$$

Proof. We note that

$$\#\mathcal{H}_{\alpha;d} = \sum_{P \in \mathcal{H}_{\alpha;d}} \frac{1}{\#h^{-1}_{\alpha;d}(P)}.$$

Let

$$N_k = \#\left\{P : P \in \mathcal{H}_{\alpha;d},\ \#h^{-1}_{\alpha;d}(P) = k\right\}, \qquad k = 1, 2, \dots.$$

From the definition of the map $h_{\alpha;d}$, we have $\#h^{-1}_{\alpha;d}(P) = 1$ if $P = \mathcal{O}$. Moreover, from the equation (5), for a point $P = (x, y) \in \mathrm{H}_d(\mathbb{F}_q)$, we have $P \in \mathcal{H}_{\alpha;d}$ if and only if the equation

$$d\alpha^2(U) - \alpha(U)y + x = 0 \tag{6}$$

has a solution $u \in \mathbb{F}_q$. Furthermore, the number of distinct roots of the equation (6) equals $\#h^{-1}_{\alpha;d}(P)$. Since α is a bijective function, we see that $1 \leq \#h^{-1}_{\alpha;d}(P) \leq 2$. Therefore, $N_k = 0$ for $k > 2$. Moreover, $N_1 + N_2 = q$. Then,

$$\#\mathcal{H}_{\alpha;d} = \sum_{k=1}^{2} \frac{N_k}{k} = \frac{q + N_1}{2}. \tag{7}$$

As we noticed before, the value $N_1 - 1$ is equal to the number of points $P = (x, y) \in \mathrm{H}_d(\mathbb{F}_q)$ where the equation (6) has exactly one root in $\mathbb{F}_q$. To compute the value of N_1, we distinguish the following possibilities for p the characteristic of the finite field $\mathbb{F}_q$.

- If $p \neq 2$, for a point $(x, y) \in \mathrm{H}_d(\mathbb{F}_q)$, the equation (6) has only one root in $\mathbb{F}_q$ if and only if $y^2 - 4dx = 0$. This implies that $z^2 + 16d^3z + 64d^3 = 0$ with $z = y^3$. The discriminant of above quadratic equation is $4^4d^3(d^3 - 1)$. Since $q \equiv 2 \pmod 3$, then $N_1 = 1$ if $\chi(d^4 - d) = -1$ and $N_1 = 3$ if $\chi(d^4 - d) = 1$.
- If $p = 2$, for a point $(x, y) \in \mathrm{H}_d(\mathbb{F}_q)$, the equation (6) has only one root in $\mathbb{F}_q$ if and only if $x = 1$, $y = 0$ with $\alpha^2(u) = 1/d$. Hence, $N_1 = 2$.

So, we have $N_1 = 2 + \chi(d^4 - d)$, where $d \neq 0$. Then, using (7), we obtain the explicit formulas for the cardinality of $\mathcal{H}_{\alpha;d}$. □

3.3 Correspondence between the sets $\mathcal{X}_d$ and $\mathcal{H}_{\alpha;d}$

We recall the set $\mathcal{X}_d$, given by (2), that is the set of elements $x \in \mathbb{F}_q$ such that the number of affine points in $\mathrm{H}_d(\mathbb{F}_q)$ with x-coordinate equal to x is one or two.

We consider the restriction of the projection mao π_d to the set $\mathcal{H}_{\alpha;d}$. So, let $\pi_{\alpha;d}$ be the map

$$\pi_{\alpha;d} : \mathcal{H}_{\alpha;d} \longrightarrow \mathcal{X}_d \bigcup \{\infty\} \tag{8}$$

defined by $\pi_{\alpha;d}(P) = x(P)$ if $P \neq \mathcal{O}$ and $\pi_{\alpha;d}(P) = \infty$ if $P = \mathcal{O}$.

The following lemma shows that the map $\pi_{\alpha;d}$ is injective.

Lemma 3. *Let $q \equiv 2 \pmod 3$ and let H_d be a Hessian curve over $\mathbb{F}_q$ defined by the equation* (1) *with $d \neq 0, 1$. Let $\pi_{\alpha;d}$ be the map defined by* (8)*. Then, $\pi_{\alpha;d}$ is an injective function.*

Proof. First, we show that the map $\pi_{\alpha;d}$ is well defined. We note only the point $\mathcal{O}$ is mapped to ∞. Then, let P be an affine point of $\mathcal{H}_{\alpha;d}$. We have

$$x(P) = -\alpha(u) \left(\tfrac{d^3\alpha^3(u)+1}{\alpha^3(u)+1}\right)^{1/3}$$

for some $u \in \mathbb{F}_q$. We distinguish the following cases for the characteristic p of $\mathbb{F}_q$.

- For $p \neq 2$, from the proof of Proposition 1, we have $x(P) \in \mathcal{X}_d$ if and only if $\chi(\Delta_{x(P)}) \neq 1$, where $\Delta_x = -27(x^6 + 2(1-2d^3)x^3 + 1)$ for $x \in \mathbb{F}_q$. Next,

  $$\Delta_{x(P)} = -27 \left(\tfrac{d^3\alpha^6(u)+2d^3\alpha^3(u)+1}{\alpha^3(u)+1}\right)^2.$$

  So, $\chi(\Delta_{x(P)}) \neq 1$, since $\chi(-3) \neq 1$. Hence, $x(P) \in \mathcal{X}_d$.

- For $p = 2$, form the proof of Proposition 1, we have $x(P) \in \mathcal{X}_d$ if and only if $x(P) = 1$ or $\mathrm{Tr}(\Delta_{x(P)}) = 0$, where $\Delta_x = d^3x^3/(x^3+1)^2$ for $x \in \mathbb{F}_q, x \neq 1$. Then,

  $$\Delta_{x(P)} = z^2 + z,\ z = \tfrac{d^3\alpha^3(u)+1}{d^3\alpha^6(u)+1}.$$

  So, $\mathrm{Tr}(\Delta_{x(P)}) = 0$ if $x(P) \neq 1$. Hence, $x(P) \in \mathcal{X}_d$.

Next, we shall prove that the map $\pi_{\alpha;d}$ is injective, i.e., for all elements x in $\mathcal{X}_d$, we have $\#\pi_{\alpha;d}^{-1}(x) \leq 1$. Again, we consider the following cases for p.

- We assume that $p \neq 2$. By the definition of the set $\mathcal{X}_d$ and the proof of Proposition 1, for $x \in \mathcal{X}_d$ there is only one point on $\mathrm{H}_d(\mathbb{F}_q)$ with $x(P) = x$ if $\Delta_x \neq 0$, where

  $$\Delta_x = -27(x^6 + 2(1-2d^3)x^3 + 1).$$

  So, for $x \in \mathcal{X}_d$ with $\Delta_x \neq 0$, we have $\#\pi_{\alpha;d}^{-1}(x) \leq 1$.

  Next, suppose $x \in \mathbb{F}_q$ with $\Delta_x = 0$. Then, $x^3 = 2d^3 - 1 + 2ds$, where s is a square root of $d^4 - d$ in $\mathbb{F}_q$. Next, the points (x, y_1), (x, y_2) with $y_1 = (d^2 - s)x^2$, $y_2 = 2(s - d^2)x^2$ are the only points of $\mathrm{H}_d(\mathbb{F}_q)$ with the x-coordinate equal to x. Moreover, from the equation (5), for a point $P = (x, y) \in \mathrm{H}_d(\mathbb{F}_q)$, we have $P \in \mathcal{H}_{\alpha;d}$ if and only if $\chi(y^2 - 4dx) \neq -1$. Furthermore, we have

  $$y_1^2 - 4dx = -3dx = -3y_1^2.$$

  Since $\chi(-3) = -1$ and $d \neq 0$, we see that $(x, y_1) \notin \mathcal{H}_{\alpha;d}$. Also, we have $y_2^2 - 4dx = 0$. So, (x, y_2) is a point of $\mathcal{H}_{\alpha;d}$ and $\#\pi_{\alpha;d}^{-1}(x) = 1$.

- For the case of $p = 2$, from the definition of the set $\mathcal{X}_d$ and the proof of Proposition 1, we have $\#\pi_{\alpha;d}^{-1}(x) \leq 1$, where $x \in \mathcal{X}_d$, $x \neq 1$. Moreover, for $x = 1$, we have $\pi_{\alpha;d}^{-1}(x) = \{(1, 0)\}$.

Therefore for all $x \in \mathcal{X}_d$, we have $\#\pi_{\alpha;d}^{-1}(x) \leq 1$, which completes the proof of this lemma. □

Corollary 4. *Let* $q \equiv 2 \pmod 3$ *and let* H_d *be a Hessian curve over* $\mathbb{F}_q$ *defined by the equation* (1) *with* $d \neq 0, 1$. *Let* $\pi_{\alpha;d}$ *be the map defined by the equation* (8). *If* α *is a bijective function, then the map* $\pi_{\alpha;d}$ *is a bijection.*

Proof. From Lemma 3, $\pi_{\alpha;d}$ is an injective function. We note that the point $\mathcal{O}$ is mapped to ∞. If α is a bijective function, then from Proposition 1 and Theorem 2, we have $\#\mathcal{H}_{\alpha;d} = 1 + \#\mathcal{X}_d$. Hence, the map $\pi_{\alpha;d}$ is a bijection. □

4 Concluding Remarks

In this paper, we gave an efficient hashing of the elements of $\mathbb{F}_q$ into the $\mathbb{F}_q$-rational points of the Hessian curve H_d. The size of the image set of this function is about $q/2$ if $d \neq 0$ and q if $d = 0$. We remark that the case $d = 0$ is corresponded to the supersingular Hessian curve.

For ordinary Hessian curves, if α is an injective function over $\mathbb{F}_q$, then our encoding map $h_{\alpha;d}$, given by equation (3), is a $2:1$ map at all points except at one or three points that is $1:1$ and it depends on the value of $\chi(d^4-4)$, see the proof of Theorem 2. So, in comparison with Icart's map, [9], our map have the uniform size 2 for the cardinalities of almost all fibers. We recall that the size of fibers of Icart's map is varied between 1 and 4.

Moreover, we observed a bijection between the image set $\mathcal{H}_{\alpha;d}$ and the set $\mathcal{X}_d \cup \{\infty\}$, where the function α is a bijection over $\mathbb{F}_q$. This observation, leads us to extract random bits from the points in the image set $\mathcal{H}_{\alpha;d}$ by extracting random bits from the elements of $\mathcal{X}_d$. This extractor can be used for several application in many cryptographic scheme and pseudorandom generators based on elliptic curves.

We note that our map $h_{\alpha;d}$ is not surjective. Moreover, we can extend this map to a surjective map defined from $\mathbb{F}_q \times \mathbb{F}_q$ to $\mathrm{H}_d(\mathbb{F}_q)$, see [9]. Using the map $h_{\alpha;d}$, we consider the map

$$f_{\alpha;d} : \mathbb{F}_q \times \mathbb{F}_q \longrightarrow \mathrm{H}_d(\mathbb{F}_q) \tag{9}$$

defined by $f_{\alpha;d}(u,v) = h_{\alpha;d}(u) + h_{\alpha;d}(v)$, for u, v in $\mathbb{F}_q$. To show that the map $f_{\alpha;d}$ is surjective, one needs to prove that all fibers are non-empty sets. This can be easily checked if the cardinality of $\mathrm{H}_d(\mathbb{F}_q)$ is at most q. Moreover, one can see that generally a fiber of the map $h_{\alpha;d}$ relates to an absolutely irreducible curve defined over $\mathbb{F}_q$. So, from the Hasse-Weil theorem, all fibers are non-empty if q is large enough. For the bijective function α, and for all Hessian curves H_d over $\mathbb{F}_q$ with $q \equiv 2 \pmod 3$ and $q \geq 11$, our experiments show that all fibers are nonempty sets.

In the following theorem, we give estimates for the cardinality of the fibers of the map $h_{\alpha;d}$, where α is a bijection. We leave the proof of the following theorem for the future work.

Theorem 5. *Let $q \equiv 2 \pmod 3$ with $q \geq 11$ and let H_d be a Hessian curve over $\mathbb{F}_q$ defined by the equation (1) with $d \neq 0, 1$. Let $f_{\alpha;d}$ be the map defined by (9). If $\alpha : \mathbb{F}_q \longrightarrow \mathbb{F}_q$ is a bijective function, then for all points $P \in \mathrm{H}_d(\mathbb{F}_q)$ and for the cardinality of the pre-image set $\mathcal{I}(P) = f^{-1}_{\alpha;d}(P)$, we have*

$$|\#\mathcal{I}(P) - q| = \begin{cases} q + O\left(\sqrt{q}\right), & \text{if } x(P) = 0, \\ O\left(\sqrt{q}\right), & \text{if } x(P) \neq 0. \end{cases}$$

References

[1] D. Boneh and M. K. Franklin. Identity-based encryption from the weil pairing. In Joe Kilian, editor, *CRYPTO*, volume 2139 of *LNCS*, pages 213229. Springer, 2001.

[2] D. J. Bernstein and T. Lange. Explicit-formulas database. `http://www.hyperelliptic.org/EFD/`.

[3] V. Boyko, P. D. MacKenzie and S. Patel. Provably secure password-authenticated key exchange using diffie-hellman. In EUROCRYPT, pages 156171, 2000.

[4] D. V. Chudnovsky and G. V. Chudnovsky. Sequences of numbers generated by addition in formal groups and new primality and factorization tests. *Advances in Applied Mathematics*, 7(4):385–434, 1986.

[5] K. Dalen. On a theorem of Stickelberger. *Math. Scand.* **3**, 1955, 124–126.

[6] P.-A. Fouque and M. Tibouchi. Estimating the size of the image of deterministic hash functions to elliptic curves. *Cryptology ePrint Archive*, Report 2010/037, 2010, (available from `http://eprint.iacr.org/2010/037`).

[7] H. Hisil, G. Carter, and E. Dawson. New formulæ for efficient elliptic curve arithmetic. In K. Srinathan, C. P. Rangan, and M. Yung, editors, *INDOCRYPT 2007*, volume 4859 of *LNCS*, pages 138–151. Springer, 2007.

[8] H. Hisil, K. K.-H. Wong, G. Carter, and E. Dawson. Faster group operations on elliptic curves. In L. Brankovic and W. Susilo, editors, *Australasian Information Security Conference (AISC 2009)*, volume 98, pages 7–19. Conferences in Research and Practice in Information Technology (CRPIT), 2009.

[9] T. Icart. How to hash into elliptic curves. *Proc. Crypto'2009*, Lect. Notes in Comp. Sci., vol. 5677 , Springer-Verlag, 2009, 303–316.

[10] D. P. Jablon. Strong password-only authenticated key exchange. SIGCOMM Comput. Commun. Rev., 26(5):5 26, 1996.

[11] M. Joye and J.-J. Quisquater. Hessian elliptic curves and side-channel attacks. In Ç. K. Koç, D. Naccache, and C. Paar, editors, *CHES 2001*, volume 2162 of *LNCS*, pages 402–410. Springer, 2001.

[12] O. Hesse. Über die Elimination der Variabeln aus drei algebraischen Gleichungen vom zweiten Grade mit zwei Variabeln. *Journal für die reine und angewandte Mathematik*, 10:68–96, 1844.

[13] R. R. Farashahi and M. Joye. Efficient Arithmetic on Hessian Curves. In P. Nguyen and D. Pointcheval editors, *Public Key Cryptography*, volume 6056 of *LNCS*, pages 243–260. Springer, 2010.

[14] L. Stickelberger. Über eine neue Eigenschaft der Diskriminanten algebraischer Zahlkörper. *Verh.* **1** *Internat. Math. Kongresses*, Zürich 1897, Leipzig 1898, 182–193.

[15] R. G. Swan. Factorization of Polynomials over Finite Fields. *Pac. J. Math.* **19**, 1962, 1099–1106.

[16] A. Shallue and C. van de Woestjine. Construction of rational points on elliptic curves over finite fields'. *Proc. ANTS-VII*, Lect. Notes in Comp. Sci., vol. 4076, Springer- Verlag, 2006, 510–524.

[17] N. P. Smart. The Hessian form of an elliptic curve. In Ç. K. Koç, D. Naccache, and C. Paar, editors, *CHES 2001*, volume 2162 of *LNCS*, pages 118–125. Springer, 2001.

[18] U. Vishne. Factorization of Trinomials over Galois Fields of Characteristic 2. *Finite Fields and Their Applications* **3**, 1997, 370–377.