On Hashing into Elliptic Curves

REZA REZAEIAN FARASHAHI
Department of Computing, Macquarie University
Sydney, NSW 2109, Australia
reza@ics.mq.edu.au

IGOR E. SHPARLINSKI
Department of Computing, Macquarie University
Sydney, NSW 2109, Australia
igor@ics.mq.edu.au

JOSÉ FELIPE VOLOCH
Department of Mathematics, University of Texas
Austin TX 78712 USA
voloch@math.utexas.edu

Abstract

We study the hash function from a finite field $\mathbb{F}_q$ into an elliptic curve over $\mathbb{F}_q$ which has recently been introduced by T. Icart. In particular we slightly adjust and prove the conjectured T. Icart asymptotic formula for the image size of this function.

Keywords: Elliptic curve cryptography, hashing, Chebotarev density theorem

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, see [3] for a short survey of such applications.

Icart [3] has proposed and studied such a hash function, which is more efficient than several previous constructions. Here we further study the properties of this function and also slightly adjust and prove the conjectured in [3] asymptotic formula for its image size.

More precisely, let $\mathbf{E}_{a,b}$ be an elliptic curve over the finite field $\mathbb{F}_q$ of characteristic $p \geq 5$ given by the Weierstraß equation

$$Y^2 = X^3 + aX + b, \tag{1}$$

where $a, b \in \mathbb{F}_q$. As usual, we denote by $\mathbf{E}_{a,b}(\mathbb{F}_q)$ the set of $\mathbb{F}_q$-rational points on $\mathbf{E}_{a,b}$ including the point at infinity $\mathcal{O}$.

For $q \equiv 2 \pmod 3$, Icart [3] has proposed the map

$$f_{a,b} : \mathbb{F}_q \longrightarrow \mathbf{E}_{a,b}(\mathbb{F}_q)$$

defined by $f_{a,b}(u) = (x, y)$ if $u \neq 0$, where

$$x = \left(v^2 - b - \frac{u^2}{27}\right)^{1/3} + \frac{u^2}{3} \qquad \text{and} \qquad y = ux + v,$$

with

$$v = \frac{3a - u^4}{6u},$$

and $f_{a,b}(u) = \mathcal{O}$ if $u = 0$. We note that, the map $f_{a,b}$ is not surjective. It has been conjectured in [3, Conjecture 1], that the expected value of the cardinality of the image set $\mathcal{F}_{a,b} = f_{a,b}(\mathbb{F}_q)$ is about

$$\#\mathcal{F}_{a,b} \sim \frac{5}{8}\#\mathbf{E}_{a,b}(\mathbb{F}_q).$$

Here we confirm this conjecture in a more precise form, for any $a \neq 0$ and also show that $5/8$ has to be replaced with $2/3$ if $a = 0$. More precisely:

Here, we give some estimates for the cardinality of the set $\mathcal{F}_{a,b}$, for $a, b \in \mathbb{F}_q$, defined by the equation (3).

Theorem 1. *Let $\mathbf{E}_{a,b}$ be an elliptic curve over $\mathbb{F}_q$ defined by the equation* (1). *Let $\mathcal{F}_{a,b}$ be the set given by the equation* (3). *For $a \neq 0$, we have*

$$\left|\#\mathcal{F}_{a,b} - \frac{5}{8}\#\mathbf{E}_{a,b}(\mathbb{F}_q)\right| \leq \frac{21}{4}\sqrt{q}\ + 31$$

and for $a = 0$ we have,

$$\left|\#\mathcal{F}_{a,b} - \frac{2}{3}\#\mathbf{E}_{a,b}(\mathbb{F}_q)\right| \leq \frac{8}{3}\sqrt{q} + 12.$$

2 Chebotarev Density Theorem

Our principal too is the Chebotarev density theorem which gives a connection between theory of finite fields and the arithmetic of number and function fields, see [4]. Here, we recall the particular case of the Chebotarev density theorem for extensions of algebraic function fields of elliptic curves, see [5].

Lemma 2. *Let $\mathbf{E}$ be an elliptic curve over $\mathbb{F}_q$ and let $\mathbb{K} = \mathbb{F}_q(X, Y)/\mathbf{E}$ be the function field of $\mathbf{E}$. Let $f(X, Y, U) \in \mathbb{K}[U]$ be an irreducible separable polynomial considered as a univariate polynomial over K with the discriminant $\Delta_f(X, Y) \in \mathbb{K}$. Let $\mathbb{L}$ be the splitting field of f over $\mathbb{K}$ with Galois group $G = \mathrm{Gal}(\mathbb{L}/\mathbb{K})$. For a conjugacy class C in G, let N_C be the number of affine points $(x, y) \in \mathbf{E}(\mathbb{F}_q)$ with $\Delta_f(x, y) \neq 0$ and $f(x, y, U)$ having the same factorization type as the cycle type of C. If $\mathbb{F}_q$ is algebraically closed in $\mathbb{L}$, then*

$$\left| N_C - \frac{\#C}{\#G}\#\mathbf{E}(\mathbb{F}_q) \right| \leq 2g_{\mathbb{L}}\frac{\#C}{\#G}\sqrt{q} + (1 + \frac{\#C}{\#G})D + 1,$$

where $g_{\mathbb{L}}$ is the genus of the function field $\mathbb{L}$ and D is the number of affine points $(x, y) \in \mathbf{E}(\mathbb{F}_q)$ with $\Delta_f(x, y) = 0$.

3 Irreducibility and Galois Groups of Some Auxiliary Polynomials

We consider the elliptic curve $\mathbf{E}_{a,b}$ over $\mathbb{F}_q$ of characteristic $p \neq 2, 3$ given by the equation (1). Let $\mathcal{C}_{a,b}$ be the affine curve over $\mathbb{F}_q$ defined by the following equations.

$$\left(X - \frac{U^2}{3}\right)^3 = V^2 - b - \frac{U^2}{27}, \quad V = \frac{3a - U^4}{6U}, \quad Y = UX + V. \tag{2}$$

Moreover, for $a, b \in \mathbb{F}_q$, let

$$\mathcal{F}_{a,b} = \{(x, y) \ : \ (x, y, u, v) \in \mathcal{C}_{a,b}(\mathbb{F}_q)\} \cup \{\mathcal{O}\}, \tag{3}$$

where $\mathcal{O}$ is the point at infinity. Our goal is to estimate the cardinality of $\mathcal{F}_{a,b}$, for $a, b \in \mathbb{F}_q$.

We recall that by [3, Lemma 3] the system of equations (2) is equivalent to the following system:

$$Y^2 = X^3 + aX + b \qquad \text{and} \qquad \frac{H_{a,b}(X,Y,U)}{U} = 0,$$

where

$$H_{a,b}(X,Y,U) = \begin{cases} U^4 - 6XU^2 + 6YU - 3a, & \text{if } a \neq 0, \\ U^3 - 6XU + 6Y, & \text{if } a = 0. \end{cases} \tag{4}$$

In other words, for all points $P = (x,y) \in \mathbb{A}^2(\mathbb{F}_q)$, we have $P \in \mathcal{F}_{a,b}$ if and only if $P \in \mathbf{E}_{a,b}(\mathbb{F}_q)$ and the polynomial $H_{a,b}(x,y,U)$ has a non-zero root in $\mathbb{F}_q$. So,

$$\mathcal{F}_{a,b} = \left\{(x,y) \in \mathbf{E}_{a,b}(\mathbb{F}_q) \ : \ H_{a,b}(x,y,u) = 0 \text{ for some } u \in \mathbb{F}_q^*\right\} \cup \{\mathcal{O}\}\,. \tag{5}$$

We use the Chebotarev density theorem to estimate the cardinality of $\mathcal{F}_{a,b}$, for $a, b \in \mathbb{F}_q$. Let

$$\mathbb{K}_{a,b} = \mathbb{F}_q(X,Y)/\mathbf{E}_{a,b}$$

be the function field of the elliptic curve $\mathbf{E}_{a,b}$. We consider the polynomial $H_{a,b}$, given by (4), as a univariate polynomial in $\mathbb{K}_{a,b}[U]$. We show that $H_{a,b}$ is a separable irreducible polynomial in $\mathbb{K}_{a,b}[U]$. Next, we consider the splitting field of $H_{a,b}$ over $\mathbb{K}_{a,b}$ and compute its Galois group over $\mathbb{K}_{a,b}$. Finally, we use Lemma 2 to estimate the number of points (x,y) of $\mathbf{E}_{a,b}(\mathbb{F}_q)$ where $H_{a,b}(x,y,U)$ has a non-zero root in $\mathbb{F}_q$.

Lemma 3. *Let $H_{a,b}$ be the polynomial given by* (4) *over $\mathbb{K}_{a,b}$. Then, $H_{a,b}$ is a separable irreducible polynomial in $\overline{\mathbb{F}}_q(X,Y)[U]$.*

Proof. We recall that $\mathbb{F}_q$ has characteristic $p \neq 2, 3$. We also note that, the ring $\overline{\mathbb{F}}_q[X,Y]$ is integrally closed since the curve $\mathbf{E}_{a,b}$ is smooth by hypothesis. Assume that $H_{a,b}$ is not irreducible. We have two following cases:

- Suppose $a \neq 0$. If $H_{a,b}$ has a root α in $\overline{\mathbb{F}}_q[X,Y]$, then α is integral over $\overline{\mathbb{F}}_q[X,Y]$ and hence α is in $\overline{\mathbb{F}}_q[X,Y]$. Since the constant coefficient of $H_{a,b}$, that is, $-3a$, is a non zero constant, we see that α is a unit in $\overline{\mathbb{F}}_q[X,Y]$ and hence is constant. Moreover, it is clear that $H_{a,b}$ has no constant root.

If $H_{a,b}$ factors as $(U^2+\alpha_1 U+\beta_1)(U^2+\alpha_2 U+\beta_2)$ over $\overline{\mathbb{F}}_q[X,Y]$, then again, for $i=1,2$, we have $\alpha_i,\beta_i\in\overline{\mathbb{F}}_q[X,Y]$ and we similarly conclude that β_1,β_2 are non-zero constants. We also get

$$\alpha_2=-\alpha_1,\ (\beta_2-\beta_1)\alpha_1=6Y \qquad \text{and} \qquad \alpha_1^2=6X+\beta_1+\beta_2.$$

It follows that α_1 is a constant multiple of Y and the equation $\alpha_1^2=6X+\beta_1+\beta_2$ leads to a contradiction. So $H_{a,b}$ is irreducible.

- Suppose $a=0$. If $H_{a,b}$ has a root α in $\overline{\mathbb{F}}_q[X,Y]$, then α is in $\overline{\mathbb{F}}_q[X,Y]$. Moreover, this root is a divisor of the constant coefficient of $H_{a,b}$, that is, $6Y$. Since $6Y$ is an irreducible element of $\overline{\mathbb{F}}_q[X,Y]$, we have $\alpha=cY$, where c is anon-zero constant. Furthermore, $H_{a,b}(X,Y,cY)\neq 0$ and we have a contradiction. So, $H_{a,b}$ has no root in $\overline{\mathbb{F}}_q[X,Y]$. Hence, $H_{a,b}$ is irreducible.

Moreover, the irreducible polynomial $H_{a,b}$ is separable, since its derivative is nonzero. □

Now, let $\mathbb{L}_{a,b}$ be the splitting field of the polynomial $H_{a,b}$ over $\mathbb{K}_{a,b}$. Then, $\mathbb{L}_{a,b}$ is a Galois extension of $\mathbb{K}_{a,b}$ and let $G_{a,b}=\mathrm{Gal}(\mathbb{L}_{a,b}/\mathbb{K}_{a,b})$ be the Galois group of $\mathbb{L}_{a,b}$ over $\mathbb{K}_{a,b}$. It is known that $G_{a,b}$ is isomorphic to a subgroup of the symmetric group S_d where $d=\deg H_{a,b}$. In the following, we show that $G_{a,b}$ is isomorphic to S_d.

Lemma 4. *Let $\Delta_{a,b}$ be the discriminant of $H_{a,b}$, given by (4), as a univariate polynomial in $\mathbb{K}_{a,b}[U]$. Then $\Delta_{a,b}$ is not square in $\mathbb{K}_{a,b}$.*

Proof. First, we let $a\neq 0$. Then

$$\Delta_{a,b}=-2^4 3^3(9X^6+18aX^4+90bX^3-39a^2X^2-54abX+16a^3+81b^2).$$

If $\Delta_{a,b}$ is a square in $\mathbb{K}_{a,b}$ then it is either a square in $\mathbb{F}_q(X)$ or X^3+aX+b times a square in $\mathbb{F}_q(X)$. Since

$$\Delta_{a,b}=-2^4 3^5(X^3+aX+b)(X^3+aX+9b)+2^8 3^3 a(3aX^2+9bX-a^2),$$

we see that X^3+aX+b does not divide $\Delta_{a,b}$ as $6a\neq 0$. Moreover, we have

$$\Delta_{a,b}=-2^4 3^5(X^3+ax+5b)^2+2^8 3^3(3a^2X^2+9abX-a^3+9b^2).$$

So, if $\Delta_{a,b}$ is a square in $\mathbb{F}_q(X)$ then it must be $-2^4 3^5 (X^2 + ax + 5b)^2$ which again is impossible when $6a \neq 0$, which is equivalent to $a \neq 0$. as $p \geq 5$.

Now, we assume that $a = 0$. We have $\Delta_{a,b} = -2^2 3^3 (X^3 + 9b)$. Similarly, we see that $\Delta_{a,b}$ is not a square when $6b \neq 0$. We note that $b \neq 0$, since the curve $\mathbf{E}_{a,b}$ is smooth. Since $p \geq 5$, this concludes the proof. $\square$

Lemma 5. *For $a \neq 0$, let $R_{a,b}(X, Y, U)$ be the cubic resolvent of the quartic polynomial $H_{a,b}$, given by* (4) *over $\mathbb{K}_{a,b}$. Then, $R_{a,b}$ is irreducible over $\mathbb{K}_{a,b}$.*

Proof. The cubic resolvent of $H_{a,b}$ is

$$R_{a,b}(X, Y, U) = U^3 + 12XU^2 + (36X^2 + 12a)U + 36(X^3 + aX + b).$$

Suppose $R_{a,b}$ is reducible over $\mathbb{K}_{a,b}$. Then, it has a root α which is integral over $\mathbb{F}_q[X, Y]$. Since this ring is integrally closed, we have $\alpha \in \mathbb{F}_q[X, Y]$. Moreover, α divides $X^3 + aX + b$, so it has zeros at points of order two of $\mathbf{E}_{a,b}$ of multiplicity at most two and a pole only at infinity of multiplicity at most 6. It follows that α is in $\mathbb{F}_q[X]$ and divides $X^3 + aX + b$ or $\alpha = cY$, where c is a constant. Now, we consider these cases.

- If $\alpha = cY$, we have

  $$\begin{aligned} R_{a,b}(X, Y, \alpha) &= 12(X^3 + aX + b)(c^2 X + 3) \\ &\quad + c(c^2(X^3 + aX + b) + 36X^2 + 12a)Y. \end{aligned}$$

  Then, $R_{a,b}(X, Y, \alpha) = 0$ implies $c = 0$ which is impossible.

- We assume that α is a divisor of $X^3 + aX + b$ in $\mathbb{F}_q[X]$. If α is a cubic or quadratic polynomial in $\mathbb{F}_q[X]$, then degree considerations lead to a contradiction. So, we assume $\alpha = mX + n$, with $m, n \in \mathbb{F}_q$. We have

  $$\begin{aligned} R_{a,b}(X, Y, \alpha) &= (m^3 + 12m^2 + 36m + 36)X^3 + 3n(m^2 + 8m + 12)X^2 \\ &\quad + 3(mn^2 + 4am + 4n^2 + 12a)X + n^3 + 12an + 36b. \end{aligned}$$

  Then, $R_{a,b}(X, Y, \alpha) = 0$ implies that either $n = 0$ or $m^2 + 8m + 12 = 0$ since $p \neq 3$. If $n = 0$ then $b = 0$ and

  $$m^3 + 12m^2 + 36m + 36 = 4a(m + 3) = 0$$

  which is not possible since $a \neq 0$. If $m^2 + 8m + 12 = 0$ then

  $$m^3 + 12m^2 + 36m + 36 \neq 0$$

  since $p \neq 2, 3$ (which is easy to check via, for example, the resultant computation).

Therefore, the cubic resolvent $R_{a,b}(X, Y, U)$ is irreducible over $\mathbb{K}_{a,b}$. $\square$

Lemma 6. *Let $\mathbb{L}_{a,b}$ be the splitting field of the polynomial $H_{a,b}$, given by* (4)*, over $\mathbb{K}_{a,b}$. Let $d = \deg H_{a,b}$. Let $G_{a,b} = \mathrm{Gal}(\mathbb{L}_{a,b}/\mathbb{K}_{a,b})$ be the Galois group of $\mathbb{L}_{a,b}$ over $\mathbb{K}_{a,b}$. Then, $G_{a,b}$ is isomorphic to S_d.*

Proof. Lemma 3 shows that $H_{a,b}$ is an irreducible separable polynomial over $\mathbb{K}_{a,b}$.

If $a \neq 0$, from Lemma 5, we see that the cubic resolvent of $H_{a,b}$ is irreducible. Furthermore, Lemma 4 shows that the discriminant of $H_{a,b}$ is not a square in $\mathbb{K}_{a,b}$. Therefore, the Galois group of $H_{a,b}$ over $\mathbb{K}_{a,b}$ is the symmetric group S_4, for example, see [2, Section 14.6].

If $a = 0$, from Lemma 4, we see that the discriminant of $H_{a,b}$ is not a square in $\mathbb{K}_{a,b}$. Hence, the Galois group of $H_{a,b}$ over $\mathbb{K}_{a,b}$ is the symmetric group S_3, for example, see [2, Section 14.6]. $\square$

4 Proof of Theorem 1

Our proof is based on Lemma 2. First, we present the necessary requirements.

We consider the polynomial $H_{a,b}$ defined by (4) over the function field $\mathbb{K}_{a,b} = \mathbb{F}_q(X, Y)$ of $\mathbf{E}_{a,b}$. The splitting field $\mathbb{L}_{a,b}$ of the irreducible separable polynomial $H_{a,b}$ is a Galois extension of $\mathbb{K}_{a,b}$ (see Lemma 3). Moreover, Lemma 6, shows that the Galois group $G_{a,b} = \mathrm{Gal}(\mathbb{L}_{a,b}/\mathbb{K}_{a,b})$ is S_d where as before $d = \deg H_{a,b}$.

Since the polynomial $H_{a,b}$ is irreducible in $\overline{\mathbb{F}}_q(X, Y)[U]$, then $\mathbb{F}_q$ is algebraically closed in $\mathbb{L}_{a,b}$ (for example, see [6, Prposition 3.6.6]).

We consider $\Delta_{a,b}$, that is, the discriminant of $H_{a,b}$ (see Lemma 4). Let D be the number of affine points $(x, y) \in E(\mathbb{F}_q)$ with $\Delta_{a,b}(x, y) = 0$. Then, we see $D \leq 12$ if $a \neq 0$ and $D \leq 6$ if $a = 0$.

Let $g_{a,b}$ be the genus of the function field $\mathbb{L}_{a,b}$. From the *Hurwitz* formula, we see that, $g_{a,b} \leq 7$ if $a \neq 0$ and $g_{a,b} \leq 4$ if $a = 0$.

As defined in Lemma 2, for a conjugacy class C in $G_{a,b}$, let N_C be the number of affine points $(x, y) \in E(\mathbb{F}_q)$ with $\Delta_{a,b}(x, y) \neq 0$ and $H_{a,b}(x, y, U)$ having the same factorization type as the cycle type of C.

From (5), we see that $\#\mathcal{F}_{a,b} - 1$ equals the cardinality of the set of points $(x, y) \in \mathbf{E}_{a,b}(\mathbb{F}_q)$ where the polynomial $H_{a,b}(x, y, U)$ has a nonzero root in $\mathbb{F}_q$. It is easy to see that, for $(x, y) \in \mathbf{E}_{a,b}(\mathbb{F}_q)$ with $\Delta_{a,b}(x, y) = 0$, the polynomial $H_{a,b}(x, y, U)$ has a root in $\mathbb{F}_q$.

Now, we distinguish the following cases.

- Assume that $a \neq 0$. Then, $G_{a,b}$ is S_4. Let C_1 and C_2 be the conjugacy classes in $G_{a,b}$ of cycle types (12)(34) and (1234), respectively. Moreover, for each point $(x, y) \in \mathbf{E}_{a,b}(\mathbb{F}_q)$, the polynomial $H_{a,b}(x, y, U)$ has no root in $\mathbb{F}_q$ (and in $\mathbb{F}_q^*$ as well, since $a \neq 0$) if and only if the factorization type of $H_{a,b}(x, y, U)$ is the same as the cycle type of either C_1 or C_2. So, we have

$$\#\mathcal{F}_{a,b} = \#\mathbf{E}_{a,b}(\mathbb{F}_q) - N_{C_1} - N_{C_2}.$$

  We note that $\#C_1 = 3$ and $\#C_2 = 6$. From Lemma 2, we obtain

$$\left| N_{C_1} - \frac{1}{8}\#\mathbf{E}_{a,b}(\mathbb{F}_q) \right| \leq \frac{7}{4}\sqrt{q} + \frac{29}{2},$$

$$\left| N_{C_2} - \frac{1}{4}\#\mathbf{E}_{a,b}(\mathbb{F}_q) \right| \leq \frac{7}{2}\sqrt{q} + 16.$$

  So, the proof is complete for $a \neq 0$.

- Assume that $a = 0$. Then, $G_{a,b}$ is S_3. Let C_1 be the conjugacy class in $G_{a,b}$ of cycle types (123). Clearly, $\#C_1 = 2$. ¿From Lemma 2, we have

$$\left| N_{C_1} - \frac{1}{3}\#\mathbf{E}_{a,b}(\mathbb{F}_q) \right| \leq \frac{8}{3}\sqrt{q} + 9.$$

  Furthermore,

$$\#\mathcal{F}_{a,b} = \#\mathbf{E}_{a,b}(\mathbb{F}_q) - N_{C_1} - e,$$

  where e is the number of points $(x, y) \in \mathbf{E}_{a,b}(\mathbb{F}_q)$ with $H_{a,b}(x, y, U)$ has only 0 as a root in $\mathbb{F}_q$. For such a point point (x, y), we have $y = 0$ (see (4)). So, we see $e \leq 3$. Hence, the proof is complete when $a = 0$.

Acknowledgements. This work was supported in part by ARC Grant DP0881473, Australia, (for R.R.F. and I.S.), by NRF Grant CRP2-2007-03, Singapore, (for I.S) and by NSA Grant MDA904-H98230-09-1-0070, USA, (for J.F.V).

References

[1] R. Avanzi, H. Cohen, C. Doche, G. Frey, T. Lange, K. Nguyen and F. Vercauteren, *Handbook of elliptic and hyperelliptic curve cryptography*, CRC Press, 2005.

[2] D. S. Dummit and R. M. Foote, *Abstract algebra*, Wiley, 2004.

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

[4] M. D. Fried and M. Jarden, *Field arithmetic*, Springer-Verlag, 2008.

[5] V. K. Murty and J. Scherk, 'Effective versions of the Chebotarev density theorem for function fields', *Comp. Rend. Acad. Sci. Paris, Série I*, **319** (1994), 523–528.

[6] H. Stichtenoth, *Algebraic function fields and codes*, Springer-Verlag, Berlin, 2009.