Hashing to Elliptic Curves of $j = 0$ and Mordell–Weil Groups*

D. Koshelev\textsuperscript{1,2,3**}

\textsuperscript{1}Versailles Saint-Quentin-en-Yvelines University, Versailles, 78035 France
\textsuperscript{2}Infortecs, Moscow, 127287 Russia
\textsuperscript{3}Institute for Information Transmission Problems, Moscow, 127994 Russia

Received June 12, 2020; in final form, June 12, 2020; accepted June 15, 2020

DOI: 10.1134/S0001434620110140

Keywords: pairing-based cryptography, elliptic curves and surfaces of $j$-invariant 0, singular $K3$ surfaces, Mordell–Weil groups.

1. INTRODUCTION

Many protocols of pairing-based cryptography [1] use a certain (not necessarily injective or surjective) map $h: \mathbb{F}_q \to E_b(\mathbb{F}_q)$, often called hashing, from a finite field $\mathbb{F}_q$ (of characteristic $p > 3$) to the ordinary elliptic curve $E_b$: $y^2 = x^3 - b$, whose $j$-invariant is 0. A review of this topic is represented, for example, in [1, Chap. 8]. At the moment, most actually used curves $E_b$ (so-called pairing-friendly curves [1, Sec. 4]) have the restriction $\sqrt{b} \notin \mathbb{F}_q$, that is, $2 \nmid |E_b(\mathbb{F}_q)|$.

In order to construct the hashing $h$, one can try to use the simplified SWU (Shallue–van de Woestijne–Ulas) method, which we explained in the introduction of [2]. This method leads to the very interesting algebraic geometry task (cf. [2, Problem 1]) of finding a rational (possibly singular) $\mathbb{F}_q$-curve (and its proper $\mathbb{F}_q$-parametrization) on the Kummer surface $K_2$ (see, e.g., [2, Sec. 2]) of the direct product $E_b \times E_b'$, where $E_b'$ is the quadratic $\mathbb{F}_q$-twist of $E_b$ (see, e.g., [1, Sec. 2.3.6]). Unfortunately, the severe requirement $\sqrt{b} \notin \mathbb{F}_q$ makes the task very difficult.

Since $E_b$ is assumed to be ordinary, we have $q \equiv 1 \pmod{3}$, that is, $\omega := (1 + \sqrt{-3})/2$ (in other words, $\omega^3 = 1$, $\omega \neq 1$) lies in $\mathbb{F}_q$. Further, let us take any element $c \in (\mathbb{F}_q^*)^3$ such that $c \notin (\mathbb{F}_q^*)^2$. By the second assumption on $c$, we obtain the equations

$$E_b': cy_1^2 = x_1^3 - b, \quad K_2: (x_1^3 - b)t^2 = c(x_0^3 - b) \subset K_3(x_0,x_1,t),$$

where $t := y_0/y_1$.

On $K_2$, there is a natural elliptic fibration $(x_0, x_1, t) \mapsto t$ (so-called Inose fibration [3]); however, we do not know any of its $\mathbb{F}_q$-sections. Instead, we apply the base change $t \mapsto t^3$ and obtain the elliptic surface

$$K_6: (x_1^3 - b)t^6 = c(x_0^3 - b) \subset K_3(x_0,x_1,t),$$

with the section $O := (t^2 : \sqrt{c} : 0) \in \mathbb{P}^2(\mathbb{X}_0:1:1:1)$. The surface $K_6$ is sometimes called the Kuwata surface [4] (also see [5], [6], [7], [8]). It is worth noting that $K_2$, $K_6$ are $K3$ surfaces (see, e.g., [9, Sec. 12]). Moreover, in accordance with [8, Theorem 8.1], they are singular [3], [9, Sec. 12], [10], that is, their Picard $\mathbb{F}_q$-numbers are equal to 20 (the highest possible one for ordinary $K3$ surfaces). By the way, the Picard $\mathbb{F}_q$-number of $K_2$ equals 8 (see, e.g., [2, Sec. 2]), which is the smallest possible one for Kummer surfaces of the direct product of any two elliptic $\mathbb{F}_q$-curves.

*The article was submitted by the author for the English version of the journal.
**E-mail: dishport@yandex.ru
Because of Lüroth’s theorem, any rational $\mathbb{F}_q$-curve on $\mathcal{K}_6$ gives (by means of $t \mapsto t^3$) a rational one on $\mathcal{K}_2$. In this regard, it is natural to study the Mordell–Weil group $\text{MW}(\mathcal{K}_6)$ (see [9, Sec. 6]) and explicitly derive one of its nonzero elements (whose canonical height [9, Sec. 11.6] is as low as possible). This approach is carried out in [11, Sec. 1], [12, Sec. 1], where any elliptic curve of $j \neq 0, 1728$ is taken instead of $E_6$.

We will denote for clarity by $\text{MW}(\overline{\mathcal{K}}_6)$ the Mordell–Weil group of all sections of $\mathcal{K}_6$ (not necessarily defined over $\mathbb{F}_q$). According to [7, Sec. 1], [8, Lemma 6.2], we have $\text{MW}(\overline{\mathcal{K}}_6) \cong \mathbb{Z}^6 \oplus \mathbb{Z}/3$. In particular, the torsion subgroup is generated by any one of the two sections $(t^2 : \omega^j \sqrt[3]{c} : 0)$, where $j \in \{1, 2\}$. By contrast, we prove that $\text{MW}(\mathcal{K}_6) \cong \mathbb{Z}/3$, that is, the Mordell–Weil $\mathbb{F}_q$-rank of $\mathcal{K}_6$ is equal to 0. Unfortunately, since the torsion sections lie at infinity (i.e., on the line $X_2 = 0$), we cannot use them to construct the hashing $h$ by the simplified SWU method.

2. MAIN RESULT

The theory of elliptic surfaces over $\mathbb{P}^1$ (i.e., elliptic curves over the function field in one variable $t$) is well represented, for example, in [9] (and in [13] for the case of a finite field $\mathbb{F}_q$). By abuse of notation, we will denote an elliptic $\mathbb{F}_q$-surface $S$ and its generic $\mathbb{F}_q(t)$-fiber by the same letter. Besides, let us identify $S$ with its (unique) Kodaira–Néron model.

**Theorem 1.** The Mordell–Weil group $\text{MW}(\mathcal{K}_6)$ is isomorphic to $\mathbb{Z}/3$.

**Proof.** First of all, we transform $\mathcal{K}_6$ (with $\mathcal{O}$ as the zero section) to its globally minimal [9, Sec. 8.2] Weierstrass form

$$
\mathcal{E}: y^2 = x^3 + \left(\frac{t^6 - c}{2b^2}\right)^2,
$$

by means of the $\mathbb{F}_q(t)$-isomorphism

$$
\varphi: \mathcal{K}_6 \cong \mathcal{E},
\varphi^{-1}: \mathcal{E} \cong \mathcal{K}_6,
$$

$$
\varphi = \begin{cases} 
  x := \frac{t^6 - c}{b(x_0 \sqrt[3]{c} - t^2x_1)}, \\
  y := \frac{-\sqrt[3]{3}(x_0 \sqrt[3]{c} + t^2x_1)}{-2b} \cdot x,
\end{cases}
\varphi^{-1} = \begin{cases} 
  x_0 := \frac{2b^2y - \sqrt{-3}(t^6 - c)}{-2\sqrt{-3} \cdot b \sqrt[3]{c} \cdot x}, \\
  x_1 := \frac{2b^2y + \sqrt{-3}(t^6 - c)}{-2\sqrt{-3} \cdot b t^2 \cdot x}.
\end{cases}
$$

These formulas are verified in [14].

Also, for $j \in \mathbb{Z}/6$, we consider the elliptic surfaces given by globally minimal Weierstrass forms

$$
\mathcal{E}_j: y^2 = x^3 + t^j \left(\frac{t^6 - c}{2b^2}\right)^2.
$$

Note that $\mathcal{E}_j$ is a Weierstrass form for $\mathcal{E}_{4-j}$ minimal at $t = \infty$. By [9, Sec. 4.10] the surfaces $\mathcal{E}_0, \mathcal{E}_1, \mathcal{E}_2$ are geometrically rational, but $\mathcal{E}_5$ is, in turn, a $K3$ surface. Besides, according to [15, Lemma 2.1] we have the following identities between Mordell–Weil ranks:

$$
\text{rk}(\mathcal{E}) = \sum_{j=0}^{5} \text{rk}(\mathcal{E}_j), \quad \text{rk}(\overline{\mathcal{E}}) = \sum_{j=0}^{5} \text{rk}(\overline{\mathcal{E}}_j).
$$

Let $\rho(\mathcal{E}_j)$ be the Picard $\overline{\mathbb{F}_q}$-number of $\mathcal{E}_j$. Using Tate’s algorithm [9, Sec. 4.2] (also see [14]), the main theorem of [16], and the Shioda–Tate formula [13, Sec. 3.5], we immediately obtain all the cells of the Table, except for $\text{MW}(\overline{\mathcal{E}}_5), \rho(\overline{\mathcal{E}}_5)$. Since $\text{rk}(\mathcal{E}) = 6$, we also obtain $\text{rk}(\overline{\mathcal{E}}_5) = 0$ and, as a result, $\mathcal{E}_5$ is a singular $K3$ surface. Moreover, $\mathcal{E}_5$ is the so-called extremal elliptic surface; hence, by row 297 of [17, Table 2], we have $\text{MW}(\overline{\mathcal{E}}_5)_{\text{tor}} = 0$. Thus, that table is completely filled.
It remains to prove that \( \text{rk}(\mathcal{E}_1) = \text{rk}(\mathcal{E}_2) = 0 \). For \( k \in \mathbb{Z}/3 \) consider the sections
\[
P_k := \left( \omega^k(t - c), \frac{\sqrt[n]{n} (t - c)}{b \sqrt[n]{n} b^2} \right), \quad Q_k := \left( \omega^k \frac{\sqrt[n]{n} (t - c)}{b \sqrt[n]{n} b^2}, \frac{t^2 + ct}{2b^2} \right)
\]
of \( \mathcal{E}_1 \) and \( \mathcal{E}_2 \) respectively. Since each triple have the same \( y \)-coordinate, we obviously obtain
\[
P_0 + P_1 + P_2 = \mathcal{O}, \quad Q_0 + Q_1 + Q_2 = \mathcal{O}.
\]
The canonical height matrices
\[
\tilde{h}_{L_1} = \begin{pmatrix} 1/3 & -1/6 \\ -1/6 & 1/3 \end{pmatrix}, \quad \tilde{h}_{L_2} = \begin{pmatrix} 2/3 & -1/3 \\ -1/3 & 2/3 \end{pmatrix}
\]
on the lattices \( L_1 := \langle P_0, P_1 \rangle \) and \( L_2 := \langle Q_0, Q_1 \rangle \) are not hard to derive by looking at [18, Theorem 8.6]. Instead, we use in [14] one of Magma functions in order to reduce the amount of computations. The given matrices are nondegenerate, hence the sections \( P_0, P_1 \) (resp. \( Q_0, Q_1 \)) are linearly independent.

Besides, we have the following possible Frobenius actions \( \text{Fr} \) on \( L_1 \):
\[
\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \quad \begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix}, \quad \begin{pmatrix} 0 & 1 \\ -1 & 1 \end{pmatrix}
\]
if the third-power residue symbol \( (4b/q)_3 = 1, \omega, \omega^2 \), respectively. In turn, the Frobenius \( \text{Fr} \) on \( L_2 \) is given by one of the matrices
\[
\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix}, \quad \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}
\]
if \( (b/q)_3 = 1, \omega, \omega^2 \), respectively. However, the first case is ruled out by our assumption. In all remaining cases,
\[
\text{rk}(\mathcal{E}_1) = \text{rk}(L_1^{\text{Fr}}) = 0, \quad \text{rk}(\mathcal{E}_2) = \text{rk}(L_2^{\text{Fr}}) = 0,
\]
where \( L_1^{\text{Fr}}, L_2^{\text{Fr}} \) are the sublattices of \( \text{Fr} \)-invariants. Thus, the theorem is proved. \( \square \)

**Table.** The surfaces \( \mathcal{E}_j \), where \( \mathcal{E}_0 \simeq_{\mathbb{F}_q(t)} \mathcal{E}_4, \mathcal{E}_1 \simeq_{\mathbb{F}_q(t)} \mathcal{E}_3 \)

| \( \mathcal{E}_j \) | singular fibers | lattice T | \( \text{MW}(\mathcal{E}_j) \) | \( \rho(\mathcal{E}_j) \) |
|-----------------|-----------------|----------|----------------|----------|
| \( \mathcal{E}_0 \) | \( \text{IV}, \text{IV}^* \) | \( \mathbb{A}_2 \oplus \mathbb{E}_6 \) | \( \mathbb{Z}/3 \) | 10 |
| \( \mathcal{E}_1 \) | \( \text{II}, \text{IV}, \text{I}_0^* \) | \( \mathbb{A}_2 \oplus \mathbb{D}_4 \) | \( \mathbb{Z}^2 \) | 20 |
| \( \mathcal{E}_2 \) | \( 3\cdot \text{IV} \) | \( \mathbb{A}_2^{\oplus 3} \) | \( \mathbb{Z}^2 \oplus \mathbb{Z}/3 \) | 0 |
| \( \mathcal{E}_3 \) | \( \text{IV}, 2\cdot \text{IV}^* \) | \( \mathbb{A}_2 \oplus \mathbb{E}_8^{\oplus 2} \) | \( \mathbb{Z}^2 \oplus \mathbb{Z}/3 \) | 0 |

**Remark.** As we see in the proof, if \( (b/q)_3 = 1 \), then \( L_2^{\text{Fr}} = L_2 \). At the same time, since \( \text{rk}(L_1^{\text{Fr}}) = 0 \) as before, we have \( \text{rk}(\mathcal{K}_0) = 2 \) in this case.

Since the base change \( t \mapsto t^3 \) obviously transforms an affine (i.e., \( X_2 \neq 0 \)) \( \mathbb{F}_q \)-section of \( \mathcal{K}_2 \) to that of \( \mathcal{K}_6 \), we have also established the following theorem.

**Theorem 2.** The elliptic \( \mathbb{F}_q \)-surface \( \mathcal{K}_2 \) is not Jacobian, that is, it has no \( \mathbb{F}_q \)-section.
3. FURTHER QUESTIONS

Let us shortly discuss what other Jacobian elliptic $\mathbb{F}_q$-fibrations can be potentially used to construct a rational $\mathbb{F}_q$-curve on the Kummer surface $K_2$. First, it is very natural to formulate the following.

Remark 1. Is there a number $n \in \mathbb{N}$ such that the Mordell–Weil group $\text{MW}(K_{6n})$ of the elliptic surface

$$K_{6n} : (x^3 - b) t^{6n} = c(x_0^3 - b) \subset K^3_{(x_0,x_1,t)}$$

(with $t^{2n} : \sqrt{t} : 0$ as the zero section) is of non-zero rank?

The base change $t \mapsto t^{6n}$ allows to transform rational $\mathbb{F}_q$-curves on $K_{6n}$ into rational ones on $K_2$. As well as for $K_6$, we verified in [14] that

$$y^2 = x^3 + \left(\frac{t^{6n} - c}{2b^2}\right)$$

is a globally minimal Weierstrass form for $K_{6n}$. Therefore, the arithmetic genus of its Kodaira–Néron model is equal to $2n$, and hence, for $n > 1$, we deal with a surface of Kodaira dimension one.

We can also consider elliptic fibrations immediately on $K_2$. All of them were classified (without explicit formulas) in [19, Table 1.3] over an algebraically closed field. This leads to the following good question: Which of them are Jacobian $\mathbb{F}_q$-fibrations? Finally, one may wonder about the existence of other dominant rational maps from (elliptic) $K3$ surfaces to $K_2$. This topic is highlighted, for example, in [20, Sec. 3].

ACKNOWLEDGMENTS

The author expresses his deep gratitude to his scientific advisor M. Tsfasman and thanks A. Trepalin for help and useful comments.

FUNDING

This work was supported in part by the Russian Foundation for Basic Research under grant no. 19-31-90029/19.

REFERENCES

1. N. El Mrabet and M. Joye, Guide to Pairing-Based Cryptography, in Cryptography and Network Security Series (Chapman and Hall/CRC, New York, 2016).
2. D. Koshelev, Hashing to Elliptic Curves of j-Invariant 1728, in IACR Cryptology, https://eprint.iacr.org/2019/1294 (2019).
3. H. Inose, in Proceedings of the International Symposium on Algebraic Geometry (Books Kinokuniya, Kyoto, 1977), pp. 495–502.
4. M. Kuwata, Rikkyo Daigaku Sugaku Zasshi 49 (1), 91 (2000).
5. R. Kloosterman, Commentarii Mathematici Universitatis Sancti Pauli 54 (1), 69 (2005).
6. A. Kumar and M. Kuwata, Nagoya Mathematical Journal 228, 124 (2017).
7. T. Shioda, in Proceedings of the Japan Academy, Series A, Mathematical Sciences 76 (5), 68 (2000).
8. T. Shioda, Journal of the Mathematical Society of Japan 60 (4), 1083 (2008).
9. T. Shioda and M. Sch++tt, in Mordell–Weil Lattices, A Series of Modern Surveys in Mathematics (Springer-Verlag, Singapore, 2019), Vol. 70, pp. 79–114.
10. T. Shioda and H. Inose, in Complex Analysis and Algebraic Geometry (Cambridge University Press, Cambridge, 1977), pp. 119–136.
11. M. Kuwata and L. Wang, International Mathematics Research Notices 1993 (4), 113 (1993).
12. J.-F. Mestre, in Comptes Rendus de l’Académie des Sciences, Series I – Mathematics 314 (12), 919 (1992).
13. D. Ulmer, in Arithmetic of L-functions, IAS / Park City Mathematics 18, 211 (2011).
14. D. Koshelev, Magma Code, github: https://github.com/dishport/Hashing-to-elliptic-curves-of-j-0-and-Mordell–Weil-groups (2020).
15. J. Chahal, M. Meijer, and J. Top, Commentarii Mathematici Universitatis Sancti 49 (1), 79 (1999).
16. K. Oguiso and T. Shioda, Rikkyo Daigaku Sugaku Zasshi 40 (1), 83 (1991).
17. I. Shimada and D. Zhang, Nagoya Mathematical Journal 161, 23 (2001).
18. T. Shioda, Rikkyo Daigaku Sugaku Zasshi 39 (2), 211 (1990).
19. K. Nishiya, Japanese Journal of Mathematics 22 (2), 293 (1996).
20. S. Ma, in Proceedings of the American Mathematical Society 141 (1), 131 (2013).