

Equidistribution Among Cosets of Elliptic Curve Points in Intervals

Taechan Kim and Mehdi Tibouchi

Communicated by ???

Abstract. In a recent paper devoted to fault analysis of elliptic curve-based signature schemes, Takahashi et al. (TCHES 2018) described several attacks, one of which assumed an equidistribution property that can be informally stated as follows: given an elliptic curve E over \mathbb{F}_q in Weierstrass form and a large subgroup $H \subset E(\mathbb{F}_q)$ generated by $G(x_G, y_G)$, the points in $E(\mathbb{F}_q)$ whose x -coordinate is obtained from x_G by randomly flipping a fixed, sufficiently long substring of bits (and rejecting cases when the resulting value does not correspond to a point on $E(\mathbb{F}_q)$) are close to uniformly distributed among the cosets modulo H . The goal of this note is to formally state, prove and quantify (a variant of) that property, and in particular establish sufficient bounds on the size of the subgroup and on the length of the substring of bits for it to hold. The proof relies on bounds for character sums on elliptic curves established by Kohel and Shparlinski (ANTS–IV).

Keywords. Character Sums, Statistical Distance, Elliptic Curve Cryptography, Fault Analysis.

2010 Mathematics Subject Classification. 11L40, 14H52, 14G50.

1 Introduction

In their seminal paper on group generators for elliptic curves over finite fields [1], Kohel and Shparlinski used character sum estimates to show that, for an elliptic curve over \mathbb{F}_q in Weierstrass form and any interval I in \mathbb{F}_q of length¹ $\gg q^{1/2+\epsilon}$, the set of points on $E(\mathbb{F}_q)$ whose x -coordinate lies in I generates the group $E(\mathbb{F}_q)$.

This note uses similar techniques to establish a slight variant of that result: namely, we show that for any subgroup $H \subset E(\mathbb{F}_q)$, and any interval $I \subset \mathbb{F}_q$ of length $\gg [E(\mathbb{F}_q) : H]^{1/2} \cdot q^{1/2+\epsilon}$, the points in $E(\mathbb{F}_q)$ whose x -coordinate lies in I are close to uniformly distributed among the cosets modulo H .

This allows us to formalize, prove and quantify an equidistribution assumption

¹ Throughout this paper and as is common in analytic number theory, we use the notation $f \ll g$, or equivalently $g \gg f$, to mean that $f = O(g)$. Usually, both f and g are functions of a size parameter q , and the asymptotic relation holds for $q \rightarrow +\infty$.

made by Takahashi et al. in a recent paper on fault attacks against certain signature schemes constructed over elliptic curves with non-prime order [2].

2 Preliminaries

The following notations frequently appear throughout this paper:

- \mathbb{F}_q : a finite field of characteristic p ;
- E : an elliptic curve defined over \mathbb{F}_q ;
- H : a subgroup of $E(\mathbb{F}_q)$;
- Ω : the group of characters of $E(\mathbb{F}_q)$, i.e. $\Omega = \text{Hom}(E(\mathbb{F}_q), \mathbb{C}^*)$;
- Ω_H : the subgroup of Ω consisting of characters ω that vanish on H ;
- Ψ : the group of additive characters on \mathbb{F}_q , i.e. $\Psi = \text{Hom}(\mathbb{F}_q^+, \mathbb{C}^*)$;
- $|X|$: for any set X , this denotes the cardinality of X ;

2.1 Character Sums

We recall the following standard lemma on character sums of abelian groups.

Lemma 2.1. *Let G be a finite abelian group and let $\widehat{G} = \text{Hom}(G, \mathbb{C}^*)$ be its character group. For any $\omega \in \widehat{G}$, we have*

$$\frac{1}{|G|} \sum_{g \in G} \omega(g) = \begin{cases} 1 & \text{if } \omega = \omega_0 \\ 0 & \text{otherwise,} \end{cases}$$

where ω_0 denotes the trivial character in \widehat{G} . Symmetrically, for any $g \in G$, we have

$$\frac{1}{|\widehat{G}|} \sum_{\omega \in \widehat{G}} \omega(g) = \begin{cases} 1 & \text{if } g = e \\ 0 & \text{otherwise,} \end{cases}$$

where e denotes the identity in G .

In particular, we will frequently use that lemma for the pairs $\{\mathbb{F}_q, \Psi\}$ and $\{E(\mathbb{F}_q), \Omega\}$. Additionally, for any subgroup H of $E(\mathbb{F}_q)$, the subgroup Ω_H of Ω consisting of characters that vanish on H is canonically isomorphic to the character group of the quotient $E(\mathbb{F}_q)/H$. Applying the lemma above to that setting, it follows that:

$$\frac{1}{|\Omega_H|} \sum_{\omega \in \Omega_H} \omega(P) = \begin{cases} 1 & \text{if } P \in H \\ 0 & \text{otherwise.} \end{cases}$$

Note also that, since for any finite abelian group, the pairing $G \times \widehat{G} \rightarrow \mathbb{C}^*$ given by $(g, \omega) \mapsto \omega(g)$ is perfect, we have $|G| = |\widehat{G}|$. In particular:

$$|\Omega_H| = |E(\mathbb{F}_q)/H| = [E(\mathbb{F}_q) : H]$$

(the index of H in $E(\mathbb{F}_q)$).

Let f be a non-constant rational function on E defined over \mathbb{F}_q . For characters $\omega \in \Omega$ and $\psi \in \Psi$, we consider the character sum defined by

$$S(\omega, \psi, f) := \sum_{\substack{P \in E(\mathbb{F}_q) \\ f(P) \neq \infty}} \omega(P) \psi(f(P)).$$

The following estimate was established by Kohel and Shparlinski.

Lemma 2.2 ([1, Theorem 1]). *Let ω and ψ be characters on $E(\mathbb{F}_q)$ and \mathbb{F}_q respectively. Let f be a rational function on E . If at least one of ω or ψ is non-trivial, we have:*

$$|S(\omega, \psi, f)| \leq 2 \deg(f) q^{1/2}.$$

We will also rely on a bound on exponential sums on intervals of finite fields. Recall first the definition of an interval in \mathbb{F}_q , for not necessarily prime q (see [1, §4]).

Definition 2.3 (Interval in a finite field). An *interval* in \mathbb{F}_q is a subset $I \subset \mathbb{F}_q$ of the form $B + \{s\beta, (s+1)\beta, \dots, (s+t)\beta\}$, where B is an additive subgroup of \mathbb{F}_q , β is any element of \mathbb{F}_q , and s, t are non-negative integers.

The result we need is then the following.

Lemma 2.4 ([1, Lemma 3]). *For any interval $I \subset \mathbb{F}_q$, we have:*

$$\sum_{\psi \in \Psi} \left| \sum_{\beta \in I} \psi(\beta) \right| \leq q(1 + \log p),$$

where p is the characteristic of \mathbb{F}_q .

3 Main Theorem

In this section, we fix an elliptic curve E over \mathbb{F}_q , a subgroup $H \subset E(\mathbb{F}_q)$ and a non-constant rational function f on E defined over \mathbb{F}_q . Given an interval I of \mathbb{F}_q , our goal is to study how the points $P \in E(\mathbb{F}_q)$ such that $f(P) \in I$ are distributed

among cosets of H . More precisely, we want to prove that for large enough I , that distribution is close to uniform.

To begin with, for an interval $I \subset \mathbb{F}_q$, we let $N(I)$ be the number of points $P \in E(\mathbb{F}_q)$ such that $f(P) \in I$ (and in particular, $f(P) \neq \infty$):

$$N_f(I) := |\{P \in E(\mathbb{F}_q) : f(P) \in I\}|.$$

From now on, we omit the subscript f and simply write $N(I)$ when it is clear from the context. We have the following estimate of $N(I)$.

Lemma 3.1. *For any interval $I \subset \mathbb{F}_q$, we have:*

$$N(I) = |I| \cdot (1 + O(q^{-1/2} + \deg(f)q^{-1})) + O(\deg(f)q^{1/2} \log p),$$

where the constants in the big- O terms are absolute. In particular, if $|I| \gg q^{1/2+\epsilon}$ for some $\epsilon > 0$ and $\deg f = O(1)$, we have $N(I) = |I| \cdot (1 + o(1))$.

Proof. By definition, we have:

$$N(I) = \sum_{\substack{P \in E(\mathbb{F}_q) \\ f(P) \neq \infty}} [f(P) \in I] = \sum_{\beta \in I} \sum_{\substack{P \in E(\mathbb{F}_q) \\ f(P) \neq \infty}} [\beta - f(P) = 0],$$

where the terms in brackets follow the Iverson notation (e.g., $[f(P) \in I] = 1$ if $f(P) \in I$ and 0 otherwise). Now according to Lemma 2.1, we have:

$$[f(P) - \beta = 0] = \frac{1}{q} \sum_{\psi \in \Psi} \psi(\beta - f(P)).$$

Therefore:

$$N(I) = \frac{1}{q} \sum_{\psi \in \Psi} \sum_{\substack{P \in E(\mathbb{F}_q) \\ f(P) \neq \infty}} \overline{\psi(f(P))} \sum_{\beta \in I} \psi(\beta) = \frac{1}{q} \sum_{\psi \in \Psi} \overline{S(\omega_0, \psi, f)} \sum_{\beta \in I} \psi(\beta). \quad (3.1)$$

The contribution of the trivial character ψ_0 is simply:

$$\frac{1}{q} \sum_{\substack{P \in E(\mathbb{F}_q) \\ f(P) \neq \infty}} |I| = \frac{|E(\mathbb{F}_q)| - |f^{-1}(\infty)|}{q} \cdot |I| = \frac{q + O(q^{1/2} + \deg f)}{q} \cdot |I|,$$

by the Hasse bound. As for the sum over non-trivial characters, it is bounded as:

$$\begin{aligned} \frac{1}{q} \sum_{\substack{\psi \in \Psi \\ \psi \neq \psi_0}} |S(\omega_0, \psi, f)| \cdot \left| \sum_{\beta \in I} \psi(\beta) \right| &\leq 2 \deg(f) q^{-1/2} \sum_{\psi \in \Psi} \left| \sum_{\beta \in I} \psi(\beta) \right| \\ &\leq 2 \deg(f) q^{-1/2} \cdot q(1 + \log p), \end{aligned}$$

where the first inequality follows from Lemma 2.4 and the second inequality from Lemma 2.2. This concludes the proof.

Note that the implied constant in the first big- O term can be taken as $2 + 1$ according to the Hasse bound, and the constant in the second big- O term can be taken as $2 \cdot (1 + 1/\log 2)$. Therefore, those constants are independent of any of the parameters of the problem, and hence absolute. \square

In order to analyze the distribution of points $P \in E(\mathbb{F}_q)$ such that $f(P) \in I$ among cosets modulo H , we also introduce a notation for the number of points in each coset. For a fixed $P_0 \in E(\mathbb{F}_q)$, we denote by $N(P_0; I)$ the number such points P in the coset $P_0 + H$, i.e.:

$$N(P_0; I) := |\{P \in P_0 + H : f(P) \in I\}|.$$

Our goal is to prove that the distribution among cosets is close to uniform, i.e., to bound the *statistical distance* between the uniform distribution on $E(\mathbb{F}_q)/H$ and the distribution modulo H of the points $P \in E(\mathbb{F}_q)$ such that $f(P) \in I$. That statistical distance is the following quantity:

$$\Delta_1 = \frac{1}{2} \sum_{P_0 \in E(\mathbb{F}_q)/H} \left| \frac{N(P_0; I)}{N(I)} - \frac{1}{|\Omega_H|} \right|,$$

where the sum is taken over an arbitrary set of representatives of the cosets modulo H . In order to bound Δ_1 , we first obtain a bound on the following related quantity.

Lemma 3.2. *With the notations above, we have:*

$$\sum_{P_0 \in E(\mathbb{F}_q)/H} \left| N(P_0; I) - \frac{N(I)}{|\Omega_H|} \right|^2 \leq 4 \deg(f)^2 q(1 + \log p)^2.$$

Proof. We first observe that, like $N(I)$, the number $N(P; I)$ admits an expression as a character sum. Indeed, using the Iverson notation again, we have:

$$N(P_0; I) = \sum_{\substack{P \in E(\mathbb{F}_q) \\ f(P) \neq \infty}} [P_0 - P \in H] \cdot \sum_{\beta \in I} [\beta - f(P) = 0],$$

and both Iverson brackets are expressed are character sums:

$$N(P_0; I) = \sum_{\substack{P \in E(\mathbb{F}_q) \\ f(P) \neq \infty}} \frac{1}{|\Omega_H|} \sum_{\omega \in \Omega_H} \omega(P_0 - P) \sum_{\beta \in I} \frac{1}{q} \sum_{\psi \in \Psi} \psi(\beta - f(P)).$$

Reordering terms, this yields:

$$N(P_0; I) = \frac{1}{|\Omega_H|} \sum_{\omega \in \Omega_H} \omega(P_0) \sum_{\psi \in \Psi} \overline{S(\omega, \psi, f)} \cdot \frac{1}{q} \sum_{\beta \in I} \psi(\beta).$$

In that sum, the contribution of the trivial character ω_0 is given by:

$$\frac{1}{|\Omega_H|} \sum_{\psi \in \Psi} \overline{S(\omega_0, \psi, f)} \cdot \frac{1}{q} \sum_{\beta \in I} \psi(\beta) = \frac{N(I)}{|\Omega_H|}$$

in view of Equation (3.1). As a result, for all P_0 , we have:

$$N(P_0; I) - \frac{N(I)}{|\Omega_H|} = \frac{1}{|\Omega_H|} \sum_{\substack{\omega \in \Omega_H \\ \omega \neq \omega_0}} \omega(P_0) \sum_{\psi \in \Psi} \overline{S(\omega, \psi, f)} \cdot \frac{1}{q} \sum_{\beta \in I} \psi(\beta).$$

For simplicity, we will call that difference δ_{P_0} , and also write $\alpha(\psi) = \frac{1}{q} \sum_{\beta \in I} \psi(\beta)$.

We are trying to obtain a bound on the sum $\sum_{P_0 \in E(\mathbb{F}_q)/H} |\delta_{P_0}|^2$. Now we have:

$$\begin{aligned} \sum_{P_0 \in E(\mathbb{F}_q)/H} |\delta_{P_0}|^2 &= \sum_{P_0 \in E(\mathbb{F}_q)/H} \frac{1}{|\Omega_H|^2} \sum_{\substack{\omega, \omega' \in \Omega_H \\ \omega, \omega' \neq \omega_0}} \omega(P_0) \overline{\omega'(P_0)} \\ &\quad \sum_{\psi, \psi' \in \Psi} \overline{S(\omega, \psi, f)} \alpha(\psi) \cdot S(\omega', \psi', f) \overline{\alpha(\psi')} \\ &= \frac{1}{|\Omega_H|^2} \sum_{\substack{\omega, \omega' \in \Omega_H \\ \omega, \omega' \neq \omega_0}} \sum_{P_0 \in E(\mathbb{F}_q)/H} (\omega/\omega')(P_0) \\ &\quad \sum_{\psi, \psi' \in \Psi} \overline{S(\omega, \psi, f)} \alpha(\psi) \cdot S(\omega', \psi', f) \overline{\alpha(\psi')}. \end{aligned}$$

Now, by Lemma 2.1 the sum $\sum_{P_0 \in E(\mathbb{F}_q)/H} (\omega/\omega')(P_0)$ vanishes for $\omega \neq \omega'$, and

is equal to $|E(\mathbb{F}_q)/H| = |\Omega_H|$ otherwise. Hence:

$$\begin{aligned}
\sum_{P_0 \in E(\mathbb{F}_q)/H} |\delta_{P_0}|^2 &= \frac{1}{|\Omega_H|} \sum_{\substack{\omega \in \Omega_H \\ \omega \neq \omega_0}} \sum_{\psi, \psi' \in \Psi} \overline{S(\omega, \psi, f)\alpha(\psi)} \cdot S(\omega, \psi', f)\alpha(\psi') \\
&= \frac{1}{|\Omega_H|} \sum_{\substack{\omega \in \Omega_H \\ \omega \neq \omega_0}} \left| \sum_{\psi \in \Psi} \overline{S(\omega, \psi, f)\alpha(\psi)} \right|^2 \\
&\leq \frac{1}{|\Omega_H|} \sum_{\substack{\omega \in \Omega_H \\ \omega \neq \omega_0}} \left(\sum_{\psi \in \Psi} 2 \deg(f)q^{1/2} \cdot |\alpha(\psi)| \right)^2 \\
&\leq (2 \deg(f)q^{1/2} \cdot (1 + \log p))^2 = 4 \deg(f)^2 q (1 + \log p)^2,
\end{aligned}$$

which concludes the proof. \square

We can then use the previous lemma to obtain the desired bound on the statistical distance, which is our main result.

Theorem 3.3. *For any interval $I \subset \mathbb{F}_q$, the statistical distance Δ_1 between the uniform distribution on the set of points $P \in E(\mathbb{F}_q)/H$ such that $f(P) \in I$ and the uniform distribution on $E(\mathbb{F}_q)/H$ is bounded as:*

$$\Delta_1 \leq \frac{1}{N(I)} \cdot |\Omega_H|^{1/2} \cdot 2 \deg(f)q^{1/2}(1 + \log p).$$

In particular, if $|I| \gg q^{1/2+\epsilon}$ for some $\epsilon > 0$ and $\deg f = O(1)$, we have:

$$\Delta_1 = O\left(\frac{|\Omega_H|^{1/2}q^{1/2}\log p}{|I|}\right).$$

Proof. Indeed, we have:

$$\Delta_1 = \frac{1}{N(I)} \sum_{P_0 \in E(\mathbb{F}_q)/H} |\delta_{P_0}|$$

and hence, by the Cauchy–Schwarz inequality, it follows that:

$$\Delta_1 \leq \frac{1}{N(I)} \sqrt{|\Omega_H|} \cdot \sqrt{\sum_{P_0 \in E(\mathbb{F}_q)/H} |\delta_{P_0}|^2},$$

which yields the first estimate. The second estimate follows directly from the first combined with Lemma 3.1. \square

In cryptographic parlance, this result says in particular that if $\deg(f)$ is constant and $|I| \gg \sqrt{|\Omega_H|} \cdot q^{1/2+\epsilon}$, the statistical distance is *negligible*, and hence the distribution among cosets is indistinguishable from uniform.

Note that this result is non-trivial even for subgroups H of order as small as q^δ , $\delta > 0$ (or even $\log^{1+\delta} p$), whereas a more direct applications of the techniques of [1] would presumably only provide a non-trivial result for subgroups of order at least $q^{1/2}$.

4 Application to Fault Attacks

4.1 Fault Attacks against qDSA Signatures

In this section, we discuss cryptographic application of our result in the case when the corresponding rational function is simply $f = x$, the x -coordinate in general Weierstrass form (which is a non-constant rational function of degree $\deg(f) = 2$).

Recently, Takahashi, Tibouchi and Abe presented fault attacks against the qDSA signature instantiated over the Curve25519 Montgomery curve [2].

Description of fault attack with uniform faulty point in \mathbb{F}_p Let $E_{A,B} : y^2 = x(x^2 + Ax + B)$ the Montgomery curve over \mathbb{F}_p under our consideration. Then, $E_{A,B} \cong \mathbb{Z}_8 \times \mathbb{Z}_n$ for a prime n . Their idea is to inject faults on the base point P of prime order n yielding a faulty point \tilde{P} still in the same curve, but with a different order. During the signature generation with the faulty point, one can deduce information on the least significant bits on the nonce k . This bias can be used to apply Bleichenbacher's attacks and reveals the secret information.

More precisely, in the qDSA signature, the scalar multiplication by the nonce k is carried out by x -only arithmetic based on Montgomery ladder. As in [2], suppose the fault injection yields a faulty point \tilde{P} whose x -coordinate $\tilde{x} \in \mathbb{F}_p$ is uniformly random in \mathbb{F}_p . With the probability of approximately $1/2$, \tilde{x} is the x -coordinate of a point in $E(\mathbb{F}_p)$. Even though the value of \tilde{x} is unknown, one obtains the x -coordinate x_R of $R = [k]\tilde{P}$ from the signature. From the value of x_R , it is easy to check whether \tilde{P} is of order $8n$ by computing $[4n]R = [4nk]\tilde{P}$. Since the probability of \tilde{P} being on $E(\mathbb{F}_p)$ is $1/2$, one obtain a faulty base point \tilde{P} of order exactly $8n$ with the probability approximately $1/4$. Once such \tilde{P} is obtained, one can deduce 3 least significant bits of k as discussed in [2].

Attack with faulty point uniform in an interval $I \subset \mathbb{F}_p$ The authors of [2] also gave a heuristic argument to justify the applicability of their attack when \tilde{x} is non-uniform. Their observation is that, for the attack to succeed, it suffices that the faulty base point \tilde{P} be of order $8n$ with significant probability.

We provide a more rigorous argument by applying our result in Section 3. In short, our result implies that if \tilde{x} is uniformly random in an interval in \mathbb{F}_p of size $p^{1/2+\epsilon}$, instead of \mathbb{F}_p itself, then \tilde{P} is indistinguishable from a uniformly random element in $E(\mathbb{F}_p)/\langle P \rangle \cong \mathbb{Z}_8$ with negligible deviation. Since \tilde{P} is of order exactly $8n$ if and only if it corresponds to elements in \mathbb{Z}_8^* , we deduce that the probability of a faulty base point yielding an element of order $8n$ is $1/2 \cdot 1/2 = 1/4$ (where the former $1/2$ is from \tilde{P} to be in the original curve and the latter comes from $|\mathbb{Z}_8^*|/|\mathbb{Z}_8| = 1/2$).

Concretely speaking, this means that a fault attack which randomly flips a fixed substring of bits in x of length slightly higher than half of the entire length of x provably satisfies the desired condition. Indeed, the set of resulting x -coordinates is a subset of \mathbb{F}_p of the form $\{x_0, x_0+2^k, x_0+2^k \cdot 2, \dots, x_0+2^k \cdot (2^\ell - 1)\}$ (where k is the position of the least significant bit modified by the fault attack, ℓ is the length of the corresponding bit string, and x_0 is the value obtained from x by zeroing out that substring of bits). This subset I is an interval in the sense of Definition 2.3, with $\beta = 2^k$, $s = (x_0/2^k) \bmod p$ and $t = 2^\ell - 1$, as required. Note that the distribution of points on $E(\mathbb{F}_p)$ obtained by taking a random x in I and choosing a corresponding curve point if it exists (and try again otherwise) is not necessarily *identical* to the uniform distribution of points of $E(\mathbb{F}_p)$ with an x -coordinate in I , because a given x may correspond to either one or two curve points. However, the two distributions are always *statistically close*, because there are at most 3 values of x with only one corresponding curve point (namely, the roots of the Weierstrass polynomial), and they only account for a negligible fractions of I . This is therefore sufficient for the stated purpose.

The fault model described above (a random flip of a substring of bits of x) can typically be realized using optical fault injection techniques (such as laser faults on memory), as discussed in [2].

Bibliography

- [1] David R. Kohel and Igor E. Shparlinski, On Exponential Sums and Group Generators for Elliptic Curves over Finite Fields, in: *Algorithmic Number Theory, 4th International Symposium, ANTS-IV, Leiden, The Netherlands, July 2-7, 2000, Proceedings*, pp. 395–404, 2000.
- [2] Akira Takahashi, Mehdi Tibouchi and Masayuki Abe, New Bleichenbacher Records: Fault Attacks on qDSA Signatures, *IACR Trans. Cryptogr. Hardw. Embed. Syst.* **2018** (2018), 331–371.

Received ???.

Author information

Taechan Kim, 3-9-11, Midori-cho, Musashino-shi, Tokyo-8585, Japan.

E-mail: taechan.kim.ym@hco.ntt.co.jp

Mehdi Tibouchi, 3-9-11, Midori-cho, Musashino-shi, Tokyo 180-8585, Japan.

E-mail: mehdi.tibouchi.br@hco.ntt.co.jp