Veridise

Soundness Proof for an Interactive Protocol for the Discrete Logarithm Relation

Alp Bassa
Veridise

1 Introduction

In this note we provide a soundness proof for the interactive proof of knowledge of discrete logarithm introduced in [8, 9], based on Eagen's proof for EC inner products [5]. We show that the discrete logarithm proof gadget as described in [8, Section 4.2.2] and [9] provides an accurate realization of the protocol.

For details about elliptic curves and algebraic function fields we refer to [12] and [13]. For definitions and results on special-soundness see [1, 2].

1.1 Notation

We let $\mathbb{F}_q$ be a finite field of cardinality q, we denote by $\mathbb{P}^1$ the projective line and let E be an elliptic curve in short Weierstrass form over the finite field $\mathbb{F}_q$ given by the equation

$$y^2 = x^3 + a \cdot x + b,\ a, b \in \mathbb{F}_q.$$

Denote by $\mathcal{O}$ the point at infinity. By abuse of notation, we will also use E to denote the $\mathbb{F}_q$-rational points $E(\mathbb{F}_q)$ of E. We will denote its function field by $\mathbb{F}_q(E)$ and the ring of regular functions on the affine part of E (i.e. the ring of functions having pole only at $\mathcal{O}$) by $\mathbb{F}_q[E]$. This ring consists of functions of the form $a(x) - y \cdot b(x)$, for polynomials a and b. For a nonzero function $f \in \mathbb{F}_q(E)$ we denote the associated divisor of E by (f) or $\mathrm{div}(f)$, and its zero divisor by $(f)_0$. We denote scalar multiplication of the point $P \in E$ by the scalar n by $[n] \cdot P$. To distinguish group operations on the elliptic curves from divisors we will use $[n] \cdot P + [m] \cdot Q$ for the former and $n \cdot (P) + m \cdot (Q)$ for the latter. We denote the divisor class group of E (resp. $\mathbb{P}^1$) by $\mathrm{Div}(E)$ (resp. $\mathrm{Div}(\mathbb{P}^1)$).

2 Discrete Logarithm Relation

2.1 Configuration

The configuration $\mathcal{C}_{DL}$ consists of the following information and is agreed upon by the prover and the verifier before the protocol: A finite field $\mathbb{F}_q$ of characteristic p and an elliptic curve E over $\mathbb{F}_q$ given by the equation $y^2 = x^3 + ax + b$. We will denote the group of rational points by E, assume it is cyclic and we fix a generator G and points $B_i = [2^i] \cdot G$, for $i = 0, \ldots k$, where $\sum_{i=0}^{k} 2^i$ is greater or equal to the order of the cyclic group E.

$$\mathcal{C}_{DL} = (\mathbb{F}_q, E, G, (B_0, \ldots, B_k)).$$

2.2 Public Input

The public input consists of a point $P \in E$, for which the prover claims to know the discrete logarithm to base G. The point P is known to both prover and verifier.

2.3 Witness

The witness is the discrete logarithm of P, i.e., an element $a \in \mathbb{Z}$ with $[a] \cdot G = P$. The witness is only known to the verifier. The exponent will be expressed using a base 2 representation as

$$a = \sum_{i=0}^{k} s_i \cdot 2^i,$$

with $s_i \in \mathbb{Z}$. We will assume that $0 \leq s_i < p$, the characteristic of the finite field (in general $\mathbb{F}_q$ will be a prime field and we will have $p = q$). This is necessary as equations involving s_i are checked within $\mathbb{F}_q$ where s_i are reduced modulo p and also agrees with the reasoning in [4, Section 6]. So we have

$$P = [a] \cdot G = \left[\sum_{i=0}^{k} s_i \cdot 2^i\right] \cdot G = \sum_{i=0}^{k} [s_i] \cdot ([2^i] \cdot G) = \sum_{i=0}^{k} [s_i] \cdot B_i.$$

So we can think of the witness as given by the vector $\mathbf{s} = (s_0, \ldots, s_k) \in \mathbb{Z}^{k+1}$.

2.4 Relation

Fixing the configuration $\mathcal{C}_{DL}$ and hence the finite field $\mathbb{F}_q$, the elliptic curve E, the generator G, and its multiples $B_i = [2^i] \cdot G$, for $i = 0, \ldots k$, the protocol will provide a proof for the relation

$$\mathcal{R}_{DL} = \{(a \in \mathbb{Z}; P \in E) | P = [a] \cdot G\}.$$

More precisely, we consider the relation

$$\mathcal{R}_{DL} = \{(\mathbf{s} = (s_0, \ldots, s_k) \in \mathbb{Z}^{k+1}, 0 \leq s_i < p; P \in E) | P = \sum_{i=0}^{k} [s_i] \cdot B_i\}.$$

3 Protocol for relation $\mathcal{R}_{DL}$

Figure 1 provides a protocol for the relation $\mathcal{R}_{DL}$. Note that the protocol is not complete, but the completeness error is small (see below for details). We give a proof of special soundness of the protocol. As classically known, this implies knowledge soundness of the protocol. It is a 3 move public coin protocol, with one challenge from the verifier drawn randomly from a set of size $(\#E)^2$. The checks performed by the verifier have degree at most 2.

3.1 Soundness

In this section we provide a soundness proof for the protocol Π. The witness $\mathbf{s}$ has length $k+1$. The proof reduces to convincing the verifier, that a divisor α with $\leq k+2$ different points in its support obtained from $\mathbf{s}$ is the divisor of zeros of a function $D(x, y) = a(x) - y \cdot b(y)$. As the divisor of zeros of $D(x, y)$ is only defined for $D(x, y) \neq 0$, we will assume this. See Section 3.2 for

Configuration
$\mathcal{C}_{DL} = (\mathbb{F}_q, E, G, (B_0, \ldots, B_k))$

Prover $\mathrm{P}(\mathcal{C}_{DL}, \mathbf{s}, P)$ | **Verifier** $\mathrm{V}(\mathcal{C}_{DL}, P)$

Compute:
Let $P' = -P$.
$D(x, y) = a(x) - b(x)y$ s.t.
$(D(x, y))_0 = (P') + \sum s_i \cdot (B_i)$

$\xrightarrow{\mathbf{s}, a(x), b(x)}$

$A_0, A_1 \leftarrow_{\$} E$

$\xleftarrow{A_0, A_1}$

Compute:
$A_2 = -(A_0 + A_1)$,
line $L(x, y) = 0$ through A_0, A_1, A_2,

Abort if:
- A_0, A_1, A_2 are not distinct,
- $A_i = \mathcal{O},\ i = 0, 1, 2$
- $D(A_i) = 0,\ i = 0, 1, 2$
- $L(B_i) = 0,\ i = 0, \ldots, k$
- $L(P') = 0$

Compute:
$h_i = D'(A_i)/D(A_i),\ i = 0, 1, 2,$
$g_{P'} = -1/L(P')$

$\xrightarrow{h_0, h_1, h_2, g_{P'}}$

Compute:
$P' = -P$, $A_2 = -(A_0 + A_1)$ and
line $L(x, y) = 0$ through A_0, A_1, A_2.

Check:
$\sum h_i \frac{dx(A_i)}{dz} = g_{P'} + \sum_{i=0}^{k} \frac{-1}{L(B_i)} \cdot s_i,$
$h_i \cdot D(A_i) = D'(A_i)\ i = 0, 1, 2,$
$g_{P'} \cdot L(P') = -1,$

Figure 1: Protocol Π for the relation $\mathcal{R}_{DL}$ for configuration $\mathcal{C}_{DL} = (\mathbb{F}_q, E, G, (B_0, \ldots, B_k))$

details on how this is ensured. Moreover, as $D(x, y)$ vanishes at at most $k + 2$ points (counting multiplicities), we require

$$\max\{2 \deg a(x), 2 \deg b(x) + 3\} \leq k + 2. \tag{1}$$

We will use the notion of special-soundness. For details see [1, 2]. We will show that Π is a $13kq$-out-of-$(\#E(\mathbb{F}_q))^2$-special-sound protocol. The challenge set has size $(\#E(\mathbb{F}_q))^2$ and a witness can be extracted from $13kq$ accepting transcripts with common first message.

Assume $k, q > 18$ (this is not necessary, but used to simplify the expression in the statement below). Note that by the Hasse bound the number n of rational points of the elliptic curve E over $\mathbb{F}_q$ satisfies $|n - (q + 1)| \leq 2q\sqrt{q}$. In particular $n = \mathcal{O}(q)$.

Theorem 1. *The protocol Π for the relation $\mathcal{R}_{DL}$ is $13kq$-out-of-$(\#E(\mathbb{F}_q))^2$-special-sound.*

Proof. Consider the extractor returning $\mathbf{s} = (\mathbf{s_0}, \ldots, \mathbf{s_k})$. We have to prove that

$$P = \sum_{i=0}^{k} [s_i] \cdot B_i.$$

Let $P' = -P$. We have to show that $P' + \sum_{i=0}^{k} [s_i] \cdot B_i = \mathcal{O}$. We have the following Lemma:

Lemma 2. *Let $A = \sum_{P \in E} a_i \cdot (P)$ be an effective divisor of degree d. Then we have*

$$\sum_{P \in E} [a_i] \cdot P = \mathcal{O}$$

if and only if there exists a function $D(x, y) \in \mathbb{F}_q[E] \backslash \{0\}$ with

$$\big(D(x, y)\big)_0 = A.$$

Proof. Clearly $\sum_{P \in E} [a_i] \cdot P = \mathcal{O}$ if and only if $\sum_{P \in E} [a_i] \cdot P - [d] \cdot \mathcal{O} = \mathcal{O}$. As $\sum_{P \in E} a_i \cdot (P) - d \cdot (\mathcal{O})$ is a divisor of degree zero, by [12, Corollary 3.5], this is equivalent to

$$\sum_{P \in E} a_i \cdot (P) - d \cdot (\mathcal{O}) = \big(D(x, y)\big)$$

for some $D(x, y) \in \mathbb{F}_q[E] \backslash \{0\}$, i.e. if $A = \sum_{P \in E} a_i \cdot (P) = \big(D(x, y)\big)_0$. □

Hence we have to show that there exists a function $D(x, y) \in \mathbb{F}_q[E] \backslash \{0\}$, with

$$(P') + \sum_{i=0}^{k} s_i \cdot (B_i) = (D(x, y))_0. \tag{2}$$

We will show that sufficiently many accepting transcripts with common first message $(\mathbf{s}, D(x, y))$ and distinct challenges (A_0^j, A_1^j) imply (2).

Let $\alpha = (P') + \sum_{i=0}^{k} s_i \cdot (B_i)$, and $\beta = (D(x, y))_0$. Denote the degree of α by M. We will show that each accepting transcripts with common first message $(\mathbf{s}, D(x, y))$ will imply a particular relation between α and β. More precisely, if $\alpha = \sum \alpha_i \cdot (P_i)$ and $\beta = \sum \beta_i \cdot (Q_i)$ then each transcript will yield a linear function $L = y - (\lambda x + \mu)$, such that

$$-\sum_{P_i} \frac{\alpha_i}{L(P_i)} = -\sum_{Q_i} \frac{\beta_i}{L(Q_i)}.$$

We will show that $\Big((2M-1)\cdot q+2\Big)$ many distinct such relations imply $\alpha=\beta$ and that these relations are implied by $6\cdot\Big((2M-1)\cdot q+2\Big)$ distinct accepting transcripts.

Given a challenge $(A_0,A_1)\in E\times E$, we let $A_2=-(A_0+A_1)$ and $L(x,y)=0$ be the line through A_0,A_1 and A_2. By assumption, the points A_0,A_1 and A_2 are distinct and $\neq\mathcal{O}$, hence the line through them is not vertical and not tangent to the elliptic curve. Not all distinct challenges yield distinct lines. Two out of the three points determine the line and given 3 points on the line, there are 6 different ways of choosing A_0 and A_1 defining the line. Hence having $6\cdot\Big((2M-1)\cdot q+2\Big)$ accepting transcripts (i.e. this many distinct challenges), will define at least $(2M-1)\cdot q+2$ distinct lines $L^{(j)}(x,y)=0, j=0,\dots(2M-1)\cdot q+1$. Let the corresponding challenge points be $(A_0^{(j)},A_1^{(j)})$, and let $A_2^{(j)}=-(A_0^{(j)}+A_1^{(j)})$ be the third point on the line.

Lemma 3. *Let $\mathcal{P}=\{P_i\}$ and $\mathcal{Q}=\{Q_i\}$ be multisets of points in $\mathbb{A}^2$ (both $\mathcal{P}$ and $\mathcal{Q}$ can contain multiple instances of a point) each having at most M distinct points. Assume $\mathcal{P}$ and $\mathcal{Q}$ are invariant under the action of the Galois group $\mathrm{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)$, i.e. Galois conjugate points appear with the same multiplicity in the multiset. If for ar least one point the multiplicity in $\mathcal{P}$ and $\mathcal{Q}$ do not agree modulo p (the characteristic), then there are at most $(2M-1)\cdot q+1$ non-vertical lines $L(x,y)=0$ over $\mathbb{F}_q$ with $L(P_i),L(Q_i)\neq 0$, such that*

$$\sum_{P_i\in\mathcal{P}}\frac{1}{L(P_i)}=\sum_{Q_i\in\mathcal{Q}}\frac{1}{L(Q_i)}. \tag{3}$$

Proof. Given a non-vertical line $y=\lambda x+\mu$ with $L(P_i),L(Q_i)\neq 0$, Equation (3) can be written as

$$\sum_{P_i\in\mathcal{P}}\frac{1}{y(P_i)-\lambda x(P_i)-\mu}-\sum_{Q_i\in\mathcal{Q}}\frac{1}{y(Q_i)-\lambda x(Q_i)-\mu}=0. \tag{4}$$

As $\mathcal{P}$ and $\mathcal{Q}$ are Galois invariant, both terms will be defined over $\mathbb{F}_q$. Clearing denominators we obtain

$$\frac{f(\lambda,\mu)}{\prod_{P_i\in\mathcal{P}}L(P_i)\prod_{Q_i\in\mathcal{Q}}L(Q_i)}=0.$$

As $\mathcal{P}$ and $\mathcal{Q}$ together contain at most $2M$ distinct points, the numerator is a polynomial expression $f(\lambda,\mu)$ in λ and μ of degree $\leq 2M-1$. Assume that the multiplicity of the point R in $\mathcal{P}$ and $\mathcal{Q}$ do not agree modulo p. Evaluating the numerator at a point (λ_0,μ_0), possibly from an extension field, where only the linear factor $L(R)$ vanishes, but none of the other $L(P_i)$ or $L(Q_i)$, we get a nonzero result (the difference of the multiplicity of R in $\mathcal{P}$ and $\mathcal{Q}$ multiplied by the values of the $L(P_i)$ and $L(Q_i)$ at (λ_0,μ_0)). Hence the numerator is nonzero. The rational points $(\lambda,\mu)\in\mathbb{F}_q^2$ on the hypersurface (curve) defined by $f(\lambda,\mu)=0$ will correspond to lines $y=\lambda\cdot x+\mu$ satisfying Equation (3). Hence by the Serre bound (see [10, 11]), their number of will be at most $(2M-1)\cdot q+1$. □

Note that if all points in a multiset $\mathcal{P}$ are rational (have coordinates in $\mathbb{F}_q$) then $\mathcal{P}$ will be trivially Galois invariant.

Lemma 4. *Let $\alpha=\sum\alpha_i\cdot(P_i)$ and $\beta=\sum\beta_i\cdot(Q_i)$ be effective divisors of $E/\mathbb{F}_q$ such that $0\leq\alpha_i,\beta_i<p$ and each of α and β have at most M distinct points in their support. Assume there are $(2M-1)\cdot q+2$ distinct linear function $L^{(j)}=y-\lambda^{(j)}x+\mu^{(j)}$, such that*

$$-\sum_{P_i}\frac{\alpha_i}{L(P_i)}=-\sum_{Q_i}\frac{\beta_i}{L(Q_i)},\ \textit{for } j=0,\dots,(2M-1)\cdot q+1. \tag{5}$$

Then $\alpha=\beta$.

Proof. Let $\mathcal{P}$ respectively $\mathcal{Q}$ be the multiset having each point in the support of α respectively β appear with multiplicity corresponding to the coefficient in the divisor (this is possible as both divisors are effective). As the divisors are defined over $\mathbb{F}_q$, the multisets will be Galois invariant. If $\alpha \neq \beta$, then there would be at most $(2M-1)\cdot q+1$ lines satisfying $L^{(j)}(\alpha) = L^{(j)}(\beta)$. Hence by Lemma 3 the multiplicity of each point in α and β agree modulo p. As $0 \leq \alpha_i, \beta_i < p$, we have $\alpha = \beta$. □

Next we will show how for $\beta = (D(x,y))_0$ the right hand side of Equation (5) can be computed directly on the elliptic curve from the function $D(x,y)$ and points A_0, A_1, A_2 determining L. The following claim from [5] was proven in [4, Section 4]:

Lemma 5. *Let $D(x,y) = a(x) - y\cdot b(x)$ be a rational function on E having only poles at $\mathcal{O}$, let $L = y - \lambda\cdot x - \mu$ and consider the subfield $\mathbb{F}_q(L)$ of the function field of $\mathbb{F}_q(E)$ of E. Denote by N the field norm from $\mathbb{F}_q(E)$ to $\mathbb{F}_q(L)$. Let $\mathcal{L}$ denote the logarithmic derivative in $\mathbb{F}_q(L)$ with respect to L, i.e.*

$$\mathcal{L} : \mathbb{F}_q(L)^\times \to \mathbb{F}_q(L)$$

is given by

$$f \mapsto \frac{\delta(f)}{f},$$

where δ denotes the derivation with respect to L. Let $(L=0)$ be the zero of L in $\mathbb{F}_q(L)$. Then

$$\mathcal{L}\Big(N\big(D\big)\Big)\big((L=0)\big) = \sum_{i=0}^{2} \frac{\big(a'(x(A_i)) - \frac{3x(A_i)^2+A}{2y(A_i)} b(x(A_i)) - y(A_i)b'(x(A_i))\big)}{D(x(A_i), y(A_i))} \cdot \frac{2y(A_i)}{3x(A_i)^2 + A - \lambda\cdot 2y(A_i)}.$$

Corresponding to the extension $\mathbb{F}_q(E)/\mathbb{F}_q(L)$ we have a covering of curves $\phi : E \to \mathbb{P}^1$. In the notation of [12] we have the inclusion $\phi^* : \mathbb{F}_q(L) \to \mathbb{F}_q(E)$ and the norm map $\phi_* = N : \mathbb{F}_q(E)^\times \to \mathbb{F}_q(L)^\times$ as defined above. We have corresponding maps on the group of divisors of E and $\mathbb{P}^1$:

$$\phi^* : \mathrm{Div}(\mathbb{P}^1) \to \mathrm{Div}(E) \quad \text{and} \quad \phi_* : \mathrm{Div}(E) \to \mathrm{Div}(\mathbb{P}^1)$$

which are defined on points by

$$\phi^*(Q) = \sum_{P \in \phi^{-1}(Q)} e_\phi(P)\cdot(P) \quad \text{and} \quad \phi_*(P) = \phi(P),$$

and extended to divisors linearly. Here $e_\phi(P)$ denotes the ramification index of P in the covering given by ϕ. For basic properties of ϕ^* and ϕ_* see [12, Section II.3]. For a nonzero rational function f and a divisor $\sum n_P\cdot(P)$ (with f having neither pole nor zero on points in the support of the divisor) we define

$$f\big(\sum n_P\cdot(P)\big) = \prod_P f(P)^{n_P}.$$

By [6, Theorem 8.3.8.], we have $\mathrm{div}(N(D)) = \phi_*\mathrm{div}(D)$ for the rational function D on E. As $\mathrm{div}(D) = \sum_{Q_i} \beta_i\cdot(Q_i) - (\deg\beta)\cdot(\mathcal{O})$, we have

$$\mathrm{div}(N(D)) = \sum_{Q_i} \beta_i\cdot(\phi(Q_i)) - (\deg\beta)\cdot(\phi(\mathcal{O})),$$

and hence

$$N(D) = k \cdot \prod_{Q_i} \big(L - L(Q_i)\big)^{\beta_i}$$

for some constant $k \in \mathbb{F}_q^\times$.

Taking logarithmic derivatives and evaluating at $(L = 0)$, we obtain

$$\mathcal{L}\Big(N\big(D\big)\Big)\big((L = 0)\big) = -\sum_{Q_i} \frac{\beta_i}{L(Q_i)}. \tag{6}$$

By Lemma 5, we can evaluate the left hand side of Equation (6) on the curve E, using the points A_0, A_1, A_2. Combining Equation (6) and Lemma 5 we obtain the following result:

Given $D(x, y) \in \mathbb{F}_q[E]$, with $(D(x, y))_0 = \beta = \sum_{Q_i} \beta_i \cdot (Q_i)$ (i.e., $(D(x, y)) = \beta - (\deg \beta) \cdot \mathcal{O}$), a non-vertical line L through the distinct points A_0, A_1, A_2 on E, and a divisor $\alpha = \sum \alpha_i \cdot (P_i)$ if

$$\sum_{i=0}^{2} \frac{\big(a'(x(A_i)) - \frac{3x(A_i)^2+A}{2y(A_i)} b(x(A_i)) - y(A_i)b'(x(A_i))\big)}{D(x(A_i), y(A_i))} \cdot \frac{2y(A_i)}{3x(A_i)^2 + A - \lambda \cdot 2y(A_i)} = -\sum_{P_i} \frac{\alpha_i}{L(P_i)}$$

then

$$-\sum_{P_i} \frac{\alpha_i}{L(P_i)} = -\sum_{Q_i} \frac{\beta_i}{L(Q_i)}.$$

As $\mathbf{s}$ has length $k+1$, the divisor α has at most $k+2$ distinct points in its support. The degree of $D(x, y)$ is also fixed accordingly in (1). So $M \leq k+2$. Hence $6 \cdot \Big((2M-1) \cdot q+2\Big) \leq (12k+18)q+12$ distinct accepting transcripts will give $\Big((2M - 1) \cdot q + 2\Big)$ distinct lines, which will imply $\alpha = \beta$ by Lemma 4. So Π is $(12k + 18)q + 12$-special sound. To simplify the expression, note that if $k, q > 18$, we have $13kq > (12k + 18)q + 12$. □

Using [1] we obtain

Corollary 6. *The protocol* Π *has witness extended emulation and is knowledge sound with knowledge error*

$$\kappa \leq \frac{13kq - 1}{(\#E(\mathbb{F}_q))^2} \sim 13k/q.$$

3.2 Ensuring nonzero $D(x, y)$

The soundness proof in Section 3.1 depends on $D(x, y) \neq 0$, as a divisor can only be associated to nonzero functions. There are several ways of ensuring this:

- Eagen [5] requires the lowest order coefficient to be nonzero and normalizes it to be 1, i.e., $a(0) = 1$.
- The discrete logarithm gadget introduced in [8, 9] requires the coefficient of x in $D(x, y)$ to be nonzero and normalizes it to be 1.

Both solutions make representing certain divisors impossible and hence affect the completeness of the protocol. As the size q of the finite field is large, the proportion of not representable divisors will be negligible.

3.3 Completeness

There are several reasons for the protocol to be not complete:

(i) The two random challenge points sampled by the verifier are assumed to be distinct. Moreover we require that the third point on the line defined by the two challenge points $A_2 = -(A_0 + A_1)$ is not equal to A_0 or A_1. These conditions imply that A_0, A_1, A_2 will be distinct points on E and that the line they define is not tangent to the elliptic curve at the given point.

(ii) The two random challenge points sampled by the verifier are assumed to be not the inverse of each other. Hence the line they define is not vertical and of the form $y = \lambda x + \mu$.

(iii) The line defined by the two random challenge points should not pass through any of the points B_i or P'. This would make the expression $g_{B_i} = s_i/L(B_i)$ or $g_{P'} = 1/L(P')$ undefined, as the denominator will be zero.

(iv) None of the functions $D, y, 3x^2 + A - \lambda \cdot 2y$ should vanish at any of the points A_0, A_1, A_2, as this would make the expression in Lemma 5 undefined.

(v) To ensure that the function $D(x, y)$ is nonzero, one of its coefficients will be set as 1, resulting in non-represenatability of divisors having the relevant coefficient 0.

Let $n = \#E(\mathbb{F}_q)$ denote the number of rational points on the curve E. By the Hasse bound we have $n < q + 1 + 2\sqrt{q}$, so in particular $n < 2q$.

(i) Non-distinct points A_0, A_1, A_2 will correspond lines L tangent to the elliptic curve. As there are at most n points of tangency, we have to exclude at most n lines to avoid this.

(ii) There are at most q different vertical lines intersecting the elliptic curve at two finite rational points (in fact only x values such that $x^3 + ax + b$ is a square, so around $q/2$ many).

(iii) To ensure that the line L does not pass through P' or any of the $k + 1$ points $B_0, \ldots, B_k$, we have to exclude at most $(k + 2) \cdot q$ non-vertical lines through these points (potentially less, as we need the line to pass through 2 other rational points on the curve).

(iv) The divisor D will have at most $k+2$ distinct zeros on E. The functions y and $3x^2+A-\lambda\cdot 2y$ will vanish in at most 3 rational points on E each. Excluding all $(k + 8) \cdot q$ non-vertical lines through these points will ensure that D does not vanish at A_0, A_1, A_2.

So in total we will have to remove less than $n + q + 2(k + 8)q$ lines. As $n < 2q$, this will be less than $(2k + 19)q$, and for $k > 18$ less than $3kq$. To completeness error satisfies

$$\delta \leq \frac{3kq}{(\#E(\mathbb{F}_q))^2} \sim 3k/q.$$

4 Discrete Logarithm Gadget as proposed in [8, 9]

The discrete logarithm gadget proposed in [8, 9] is an instantiation of the above protocol for the case $k = 255$. A minor modification is that rather than computing $h_i = D'(A_i)/D(A_i)$ and checking $\sum h_i \frac{dx(A_i)}{dz} = g_{P'} + \sum_{i=0}^{k} g_{B_i}$, the quotient $h_i = D'(A_i)/D(A_i) \cdot \frac{dx(A_i)}{dz}$ is computed and the check is modified accordingly. In this note we have preferred to isolate the part of the

expression involving the function $D(x, y)$. Moreover the function $D(x, y)$ is expressed in terms of coefficients $d_\star$ rather than the polynomials $a(x)$ and $b(x)$. These are just aesthetic differences and do not change the soundness proof.

The function $D(x, y)$ is normalized so that the coefficient of x (which is required to be nonzero) is 1.

In the presentation in [8, 9], there are the following minor typos:

- Definition of *Divisor challenge*:
  - definition of p_{0_d}: d_{xy_i} should be d_{yx_i}
- Definition of *DiscreteLog*:
  - $f = Inverse(\mu - (-y + (\delta \cdot x)))$ should be $f = Inverse(\mu - (-y - (\delta \cdot x)))$
  - $(G_i.y + (\delta \cdot G_i.x))$ (last line) should be $(G_i.y - (\delta \cdot G_i.x))$

References

[1] Attema, Thomas, Cramer, Ronald, Kohl, Lisa, *A compressed Σ-protocol theory for lattices*, CRYPTO 2021, Part II, Ed. by Tal Malkin and Chris Peikert, Vol. 12826 of LNCS, Springer, Heidelberg, pp. 549–579.

[2] Attema, Thomas, Fehr, Serge, Klooß, Michael, *Fiat-Shamir Transformation of Multi-round Interactive Proofs*,TCC 2022, Part I. Ed. by Eike Kiltz and Vinod Vaikuntanathan, Vol. 13747 of LNCS, Springer, Heidelberg, Nov. 2022, pp. 113–142.

[3] Bassa, Alp, *Soundness Proof for Eagen's Proof of Sums of Points*, Veridise Technical Report.

[4] Bassa, Alp, *On the Use of Logarithmic Derivatives in Eagen's Proof of Sums of Points*, Veridise Technical Report.

[5] Eagen, Liam, *Zero Knowledge Proofs of Elliptic Curve Inner Products from Principal Divisors and Weil Reciprocity*, Cryptology ePrint Archive, Paper 2022/596, `https://eprint.iacr.org/2022/596`.

[6] Galbraith, Steven, *Mathematics of Public Key Cryptography*, Cambridge University Press, 2012.

[7] Haböck, Ulrich, *Multivariate lookups based on logarithmic derivatives*, Cryptology ePrint Archive, Paper 2022/1530, `https://eprint.iacr.org/2022/1530`.

[8] Parker, Luke "Kayaba", *FCMP++*, manuscript, May 8, 2024.

[9] Parker, Luke "Kayaba", *A R1CS Gadget for a 2k-bit Scaling of a Fixed Generator in 7 Multiplicative Constraints*, manuscript, May 9, 2024.

[10] Serre, Jean-Pierre, *Lettre à M. Tsfasman*, Journées Arithmétiques, 1989, (Luminy, 1989), Astérisque, vol. 198-200, Société Mathématique de France, Paris, 1991, pp. 351–353.

[11] Sørensen, Anders Bjært, *Projective Reed-Muler codes*, IEEE Trans. Inform. Theory 37 (1991), no. 6, 1567–1576.

[12] Silverman, Joseph H., *The arithmetic of elliptic curves*, 2nd ed., Graduate Texts in Mathematics 106, Springer Verlag, 2009.

[13] Stichtenoth, Henning, *Algebraic function fields and codes*, 2nd ed., Graduate Texts in Mathematics 254, Springer Verlag, 2009.