ELSEVIER

Available online at www.sciencedirect.com

SCIENCE DIRECT®

Theoretical Computer Science 321 (2004) 59–72

Theoretical Computer Science

www.elsevier.com/locate/tcs

# The generalized Weil pairing and the discrete logarithm problem on elliptic curves

Theodoulos Garefalakis

*Department of Mathematics, University of Toronto, Ont., Canada M5S 3G3*

Received 5 August 2002; received in revised form 2 May 2003; accepted 1 June 2003

**Abstract**

We review the construction of a generalization of the Weil pairing, which is non-degenerate and bilinear, and use it to construct a reduction from the discrete logarithm problem on elliptic curves to the discrete logarithm problem in finite fields. We show that the new pairing can be computed efficiently for curves with trace of Frobenius congruent to 2 modulo the order of the base point. This leads to an efficient reduction for this class of curves. The reduction is as simple to construct as that of Menezes et al. (IEEE Trans. Inform. Theory, 39, 1993), and is provably equivalent to that of Frey and Rück (Math. Comput. 62 (206) (1994) 865).


*Keywords:* Elliptic curves; Cryptography; Discrete Logarithm Problem

## 1. Introduction

Since the seminal paper of Diffie and Hellman [11], the discrete logarithm problem (DLP) has become a central problem in algorithmic number theory, with direct implications in cryptography. For arbitrary finite groups the problem is defined as follows: Given a finite group $G$, a base point $g \in G$ and a point $y \in \langle g \rangle$ find the smallest non-negative integer $\ell$ such that $y = g^{\ell}$.

In their paper, Diffie and Hellman proposed a method for key agreement, whose security required that DLP be hard for the group $(\mathbb{Z}/p)^*$ of integers modulo a prime $p$. This is the multiplicative group of the finite field $\mathbb{F}_p$. Considering an arbitrary finite field $\mathbb{F}_q$ instead, the method can almost trivially be extended to work in the multiplicative group of $\mathbb{F}_q$, where $q$ is a prime power. The security of the protocol now requires DLP to be hard in this group.

*E-mail address:* theo@comm.utoronto.ca (T. Garefalakis).

0304-3975/$ - see front matter 
doi:10.1016/j.tcs.2003.06.002

The result of the efforts of a number of researchers was the development of the index calculus method [1,3,7,15,19,22] and later the number field sieve and the function field sieve [2,4,10,16]. The methods are designed to compute discrete logarithms in any finite field, and are particularly efficient for finite fields of the form $\mathbb{F}_q$ with $q = p$ a prime, or $q = p^n$ with $p$ a small prime and $n$ large. In both these cases, the above methods run in subexponential time: the index calculus method in time $\exp((c_1 + o(1))(\log q)^{1/2}(\log\log q)^{1/2})$, and the number field and function field sieves in time $\exp((c_2 + o(1))(\log q)^{1/3}(\log\log q)^{2/3})$, where $c_1$ and $c_2$ are small constants.

The above developments, led Miller [21] and Koblitz [18] to consider alternative groups, where the group operation can be efficiently computed, but the DLP is hard. Their proposal was the group of points of an elliptic curve $E$ over a finite field $\mathbb{F}_q$, denoted $E(\mathbb{F}_q)$. Traditionally, the group operation here is denoted additively. Thus the elliptic curve discrete logarithm problem (ECDLP) is defined as follows: Given an elliptic curve $E/\mathbb{F}_q$, a base point $P \in E(\mathbb{F}_q)$ and a point $Q \in \langle P\rangle$ find the smallest non-negative integer $\ell$ such that $Q = \ell \cdot P$.

ECDLP in general remains of exponential time complexity to this day. However, it was the work of Menezes et al. [20] that showed that not all elliptic curves offer the same level of security. The authors used the well-known Weil pairing, $e_m$, to translate the ECDLP from $E(\mathbb{F}_q)$ to the DLP in an extension field $\mathbb{F}^*_{q^k}$, which can subsequently be solved using one of the subexponential methods discussed earlier (MOV reduction). A necessary condition for it to be efficient is the existence a small integer $k$ such that

(1) $E[m] \subseteq E(\mathbb{F}_{q^k})$, where $m = \#\langle P\rangle$,
(2) $m \mid q^k - 1$.

The authors were able to prove that for *supersingular* curves both conditions hold for $k \leqslant 6$. Subsequently, Frey and Rück [13] proposed another reduction, based on the Tate pairing $\phi_m$. The advantage of this method is that $\phi_m(P,S)$ is an $m$th root of unity for an easily computable point $S$ (in most interesting cases $S = P$). Then the only requirement for the reduction to go through is that $m \mid q^k - 1$ for a small $k$. Clearly, this is a less restrictive condition. In fact, one cannot avoid this condition, as *any* isomorphism from $\langle P\rangle$ to a subgroup of $\mathbb{F}_{q^k}$ implies that $\#\langle P\rangle = m \mid q^k - 1$.

Later, Harasawa et al. [17] attempted to generalize the method of Menezes, Okamoto, and Vanstone to apply to a larger class of elliptic curves. Their generalization appeared to be very limited. The main reason is that no efficient method is known to find a point $S \in E[m]$ such that $e_m(P,S)$ is a primitive $m$th root of unity, if $E$ is non-supersingular.

The purpose of this paper is to bridge the gap between the MOV reduction and the Frey–Rück reduction. We start from a well-known generalization of the Weil pairing, $e_\psi$ (see [6, p. 45, 23, p. 107]). The construction of the pairing is as simple as that of the Weil pairing, but has the nice property of the (more involved) Tate pairing, namely $e_\psi(P,P)$ is a suitable primitive root of unity. We show how to construct a group isomorphism between $\langle P\rangle$ and $\mu_r$, where $r = \#\langle P\rangle$ is a prime, and $\mu_r$ is the group of $r$th roots of unity. Our construction applies to elliptic curves $E/\mathbb{F}_q$ such that $r \mid q-1$, i.e., $a_q \equiv 2 \pmod r$. For the cases of interest in cryptography, the order $r$ of $P$ is

very close to the order of $E(\mathbb{F}_q)$ (and certainly greater than $2\sqrt{q}$). Then, the condition $r|q-1$ is equivalent to $a_q = 2$. We note that our construction can be generalized to work for $r|q^k - 1$ for any $k \geqslant 1$. If the degree of the extension $k$ is reasonably small, the resulting reduction is efficient. We want to stress that the reduction presented in this work is not a new attack to elliptic curve cryptosystems. It is an alternative, elementary construction of the reduction of Frey and Rück.

The paper is structured as follows. In Section 2, we review the construction of the generalized Weil pairing $e_\psi$ parameterized by an isogeny $\psi$, and state the properties that will be used later. In Section 3, we specialize the isogeny $\psi$ to $1-\phi$, where $\phi$ is the Frobenius endomorphism. In Section 4, we consider curves with trace of Frobenius $a_q = 2$, and show how to find a point $P'$, such that $e_\psi(P,P')$ is a primitive $r$th root of unity. In Section 5, we give an algorithm to compute the pairing in the case of interest. It turns out that for $Q \in \langle P \rangle$, the value $e_\psi(Q,P)$ is the multiplicative inverse of the value $\phi_r(Q,P)$ of the Tate pairing used by Frey and Rück. Finally, in Section 6 we show how to obtain a reduction in the more general case $a_q \equiv 2 \pmod r$.

## 2. The pairing

In this section, we review a generalization of the Weil pairing. As for the rest of the paper, $p$ is prime, and $q = p^k$.

Let $E$ be an elliptic curve over $\mathbb{F}_q$. Also let $\psi : E \to E$ be a non-zero endomorphism of $E$, and denote its dual by $\hat{\psi}$. Let $T \in \ker(\hat{\psi})$—such a point exists, since $\hat{\psi}$ is onto. We denote by $m$ the degree of $\psi$. Then, the divisor $D = m(T) - m(O)$ is principal. Let $f_T \in \bar{\mathbb{F}}_q(E)$ be a function such that

$$\operatorname{div}(f_T) = m(T) - m(O).$$

We consider now the divisor of $f_T \circ \psi$.

$$\begin{aligned}\operatorname{div}(f_T \circ \psi) &= \operatorname{div}(\psi^* f_T) = \psi^* \operatorname{div}(f_T) \\ &= m(\psi^*(T) - \psi^*(O)),\end{aligned}$$

the last equality being true by the definition of $\psi^*$ ($\mathbb{Z}$-linearity). We note that

$$\begin{aligned}\psi^*(T) - \psi^*(O) &= \sum_{\psi P = T} e_\psi(P)(P) - \sum_{\psi R = O} e_\psi(R)(R) \\ &= \deg_i \psi \left( \sum_{\psi R = O} (T' + R) - (R) \right),\end{aligned}$$

where $\psi T' = T$. Here we used the fact that $\psi$ is an isogeny, and therefore $e_\psi(P)$ does not depend on $P$, and equals to $\deg_i(\psi)$. The last line of the derivation shows that the divisor is principal, since it has degree zero, and it sums to

$$[\deg_i \psi] \sum_{\psi R = O} T' = [\deg \psi] T' = \hat{\psi} \circ \psi(T') = \hat{\psi} T = O.$$

So it must be the divisor of some function $g_T \in \bar{\mathbb{F}}_q(E)$. Thus,

$$(f_T \circ \psi) = m \operatorname{div}(g_T) = \operatorname{div}(g_T^m),$$

which implies that

$$g_T^m = f_T \circ \psi \tag{1}$$

$g_T$ is defined up to a multiplicative constant of course. Let now $S \in \ker(\psi)$, and $X$ any point of $E(\bar{\mathbb{F}}_q)$.

$$g_T(X+S)^m = f_T(\psi X + \psi S) = f_T(\psi X) = f_T \circ \psi X = g_T(X)^m.$$

We define the pairing

$$e_\psi : \ker(\psi) \times \ker(\hat{\psi}) \to \mu_m$$

as

$$e_\psi(S,T) = \frac{g_T(X+S)}{g_T(X)}. \tag{2}$$

The above definition does not depend on the choice of $X$. Indeed, if $\tau_S$ denotes the translation by $S$ map

$$\begin{aligned} \tau_S : E &\to E \\ X &\mapsto X + S \end{aligned}$$

then we can write $e_\psi(S,T)$ as

$$e_\psi(S,T) = \frac{g_T \circ \tau_S}{g_T}(X),$$

and the function $g_T \circ \tau_S / g_T$ is constant. To see that, we need to note that $\psi = \psi \circ \tau_S$ because $S \in \ker(\psi)$. Then,

$$\begin{aligned} \operatorname{div}(g_T \circ \tau_S) &= \tau_S^* \operatorname{div}(g_T) \\ &= \tau_S^* \circ \psi^*((T) - (O)) \\ &= (\psi \circ \tau_S)^*((T) - (O)) \\ &= \psi^*((T) - (O)) \\ &= \operatorname{div}(g_T). \end{aligned}$$

Therefore $e_\psi$ is well-defined. Furthermore, it is an easy exercise to show that the generalized Weil pairing is bilinear and non-degenerate. The proofs are essentially the same as in the case of the Weil pairing.

**Theorem 2.1.** *Let $p$ be a prime, and $q = p^k$. Let $E/\mathbb{F}_q$ be an elliptic curve, $\psi : E \to E$ be an endomorphism of $E$ of degree $m$ prime to $p$, and $\hat{\psi}$ its dual. Then there exist a pairing*

$$e_\psi : \ker(\psi) \times \ker(\hat{\psi}) \to \mu_m$$

*with the following properties*:

(1) *Bilinear*:

$$e_\psi(S_1 + S_2, T) = e_\psi(S_1, T)e_\psi(S_2, T),$$

$$e_\psi(S, T_1 + T_2) = e_\psi(S, T_1)e_\psi(S, T_2).$$

(2) *Non-degenerate*:

$$If\ e_\psi(S, T) = 1 \quad for\ all \quad T \in \ker(\psi), \quad then\ T = O.$$

**Remark.** The pairing in Theorem 2.1 is defined for any endomorphism $\psi$ with the property $p \nmid \deg(\psi)$. If we specialize $\psi$ to be the multiplication by $n$ map, and $p \nmid n$, then we recover the Weil paring. This justifies the name "generalized Weil pairing".

## 3. A special pairing

In this section, we use the generalized Weil pairing to construct an isomorphism between a subgroup of $E(\mathbb{F}_q)$ and a suitable group of roots of unity in $\bar{\mathbb{F}}_q$. Our goal is to reduce the DLP on certain elliptic curves to the DLP in the multiplicative group of finite fields. The notation throughout the paper is as follows: A point $P \in E(\mathbb{F}_q)$ is given, of prime order $r$. We wish to solve the DLP in $\langle P \rangle$ by constructing an efficiently computable isomorphism $\langle P \rangle \to \mu_r$.

Most of the ingredients for the proposed isomorphism are present. In particular, $e_\psi$ maps pairs of points to roots of unity, which form a group. We need to specialize the isogeny $\psi$, so that $\ker(\psi)$ is related to the group $E(\mathbb{F}_q)$. Let $\psi = 1 - \phi$, where $\phi$ is the $q$th power Frobenius automorphism. Then we have $\ker(\psi) = E(\mathbb{F}_q)$, and $\hat{\psi} = 1 - \hat{\phi}$. Also

$$\#\ker(\hat{\psi}) \,|\, \deg(\hat{\psi}) = \deg(\psi) = \#E(\mathbb{F}_q) = N,$$

where the divisibility comes from the fact that

$$\ker(\hat{\psi}) = \deg_s(\hat{\psi}) \quad \text{and} \quad \deg(\hat{\psi}) = \deg_s(\hat{\psi})\deg_i(\hat{\psi}).$$

Assuming that $p$ does not divide $N$, we have a bilinear, non-degenerate pairing

$$e_\psi : E(\mathbb{F}_q) \times \ker(\hat{\psi}) \to \mu_N.$$

We stress that this pairing exists and is bilinear and non-degenerate for *any* elliptic curve $E$ and *any* finite field $\mathbb{F}_q$.

The group of $r$th roots of unity, $\mu_r$, is contained in the smallest extension of $\mathbb{F}_q$, say in $\mathbb{F}_q k$ such that $r | q^k - 1$. We will mainly be concerned with the case $r | q - 1$, i.e., when all the $r$th roots of unity are contained in $\mathbb{F}_q$. Then, the condition reads $r | q - 1$, or equivalently

$$a_q \equiv 2 \,(\mathrm{mod}\, r). \tag{3}$$

In cryptography, the point $P$ is chosen to have very large order $r$, close to the order of the whole group $E(\mathbb{F}_q)$. Thus $r$ is of order $q$, which implies that Eq. (3) is equivalent (for such a choice of $P$) to $a_q = 2$. This will be the main case in our investigation.

## 4. Curves with trace equal to 2

In this section, we consider elliptic curves with trace of Frobenius $a_q = 2$. Let $\phi$ be the $q$th power Frobenius map. Let $Q \in \#E(\mathbb{F}_q)$. We wish to find the point $\hat{\phi}(Q)$. For that we consider the following:

$$(1-\phi)\circ(1-\hat{\phi}) = 1-\phi-\hat{\phi}+[q].$$

From the above observation, we have that

$$(1-\phi)\circ(1-\hat{\phi})Q = O.$$

Therefore,

$$Q-\phi(Q)-\hat{\phi}(Q)+[q]Q = O,$$

which implies $\hat{\phi}(Q) = [q]Q$. We know that $q+1-a_q = \#E(\mathbb{F}_q)$, therefore $[q]Q = [a_q-1]Q$. Thus, $\hat{\phi}(Q) = [a_q-1]Q$.

Suppose now that the curve has $a_q = 2$. Then, for every point $Q \in E(\mathbb{F}_q)$ we have $(1-\hat{\phi})Q = O$, i.e., $E(\mathbb{F}_q) \subseteq \ker(1-\hat{\phi})$.

Furthermore,

$$\#\ker(1-\hat{\phi}) = \deg_s(1-\hat{\phi}) \leqslant \deg(1-\hat{\phi}) = \deg(1-\phi) = \#E(\mathbb{F}_q).$$

This implies that

$$\ker(1-\hat{\phi}) = E(\mathbb{F}_q).$$

To summarize, for a curve $E$ with trace of Frobenius $a_q = 2$, we have a pairing

$$e_\psi : E(\mathbb{F}_q) \times E(\mathbb{F}_q) \to \mu_N,$$

where $N = \#E(\mathbb{F}_q)$. Note that $N = q-1$, and $p$ (the characteristic) does not divide $N$. Therefore from Theorem 2.1 it must be bilinear and non-degenerate.

### 4.1. A structure theorem

We need to introduce some more notation for this section. The group $E(\mathbb{F}_q)$ is isomorphic to $\mathbb{Z}/n_1\mathbb{Z} \oplus \mathbb{Z}/n_2\mathbb{Z}$, with $n_2 | n_1$, and $n_2 | q-1$. This means that $\#E(\mathbb{F}_q) = N = n_1 n_2$. We denote by $(T_1, T_2)$ a pair of generators of $E(\mathbb{F}_q)$. We recall that $P$ is a point in $E(\mathbb{F}_q)$ of prime order $r$. For the remainder of this paper, we assume that $n_1 = lr^k$, $r \nmid l$ and that $n_2 | l$, i.e., $r$ does not divide $n_2$. This is usually the case in cryptography, as the point $P$ is chosen to have very large order. Then $\langle P \rangle$ is contained in $\langle T_1 \rangle$. Our goal is to show that $e_\psi(P,P)$ is a primitive $r$th root of unity.

**Lemma 4.1.** *There exist points $T,S\in E(\mathbb{F}_q)$ such that $e_\psi(T,S)$ is a primitive $n_1$st root of unity.*

**Proof.** The image of $e_\psi(T,S)$ as $T$ and $S$ range over $E(\mathbb{F}_q)$ is a subgroup of $\mu_N$, say equal to $\mu_d$. Then it follows that for all $(T,S)\in E(\mathbb{F}_q)\times E(\mathbb{F}_q)$.

$$1 = e_\psi(T,S)^d = e_\psi([d]T,S).$$

The non-degeneracy of the $e_\psi$ pairing implies that $[d]T=O$ for all $T\in E(\mathbb{F}_q)$. In particular, if $T=T_1$ then it must be $d=n_1$. □

**Lemma 4.2.** *The order of $e_\psi(T_1,T_1)$ is divisible by $r^k$.*

**Proof.** Let $T=[x_1]T_1+[x_2]T_2$ and $S=[y_1]T_1+[y_2]T_2$ be one pair of points such that $e_\psi(T,S)$ is a primitive $n_1$st root of unity, which exists by Lemma 4.1. Suppose now to the contrary, that $r^k$ does not divide $e_\psi(T_1,T_1)$. Then

$$e_\psi(T,S) = e_\psi(T_1,T_1)^{x_1y_1}e_\psi(T_1,T_2)^{x_1y_2}e_\psi(T_2,T_1)^{x_2y_1}e_\psi(T_2,T_2)^{x_2y_2}.$$

Note now that the order of $e_\psi(T_1,T_1)$ divides $n_1=lr^k$, but by assumption $r^k$ does not divide it. Therefore, the order of $e_\psi(T_1,T_1)$ divides $lr^{k-1}$. Obviously, the orders of $e_\psi(T_1,T_2)$, $e_\psi(T_2,T_1)$, and $e_\psi(T_2,T_2)$ divide $l$. Thus we have,

$$e_\psi(T_1,T_1)^{lr^{k-1}} = e_\psi(T_1,T_2)^{lr^{k-1}} = e_\psi(T_2,T_1)^{lr^{k-1}} = e_\psi(T_2,T_2)^{lr^{k-1}} = 1.$$

Therefore,

$$e_\psi(T,S)^{lr^{k-1}} = 1,$$

which is a contradiction, since $lr^{k-1}<n_1$. □

**Theorem 4.3.** *Let $P'\in E(\mathbb{F}_q)$, be a point of order $r^d$. Then, $e_\psi(P,P')$ is a primitive $r$th root of unity if and only if $k<d+1$.*

**Proof.** It is clear that $e_\psi(P,P')$ is either a primitive $r$th root of unity or 1. This is because

$$e_\psi(P,P')^r = e_\psi([r]P,P') = e_\psi(O,P') = 1.$$

We recall that $\langle P\rangle$, and $\langle P'\rangle$ are subgroups of $\langle T_1\rangle$. It follows that $P=[lr^{k-1}]T_1$ and $P'=[lr^{k-d}]T_1$. *Then we have*

$$\begin{aligned} e_\psi(P,P') &= e_\psi([lr^{k-1}]T_1,[lr^{k-d}]T_1) \\ &= e_\psi(T_1,T_1)^{l^2r^{2k-d-1}}. \end{aligned}$$

Then Lemma 4.2 implies,

$$e_\psi(P,P')=1 \quad\Leftrightarrow\quad 2k-d-1\geqslant k \quad\Leftrightarrow\quad k\geqslant d+1. \qquad \square$$

We note, that if $r^d$ is the exact power of $r$ dividing $N$, then the point $P'$ of the previous theorem can be computed efficiently using the probabilistic method described by Frey et al. [12]. More importantly, in cryptography the point $P$ is chosen to have very large order $r$ (practically on the same order as $q$). For that reason, we state the following corollary.

**Corollary 4.4.** *Let $P \in E(\mathbb{F}_q)$ be a point of order $r$, such that $r^2$ does not divide $\#E(\mathbb{F}_q)$. Then $e_\psi(P,P)$ is a primitive $r$th root of unity.*

We want to emphasize that Corollary 4.4 is in sharp contrast with the properties of the Weil pairing. For the Weil pairing, $e_r(P,P)$ for every $P \in E[N]$. In our case, when $k=1$ the value $e_\psi(P,P)$ is not trivial, and in fact is a primitive $r$th root of unity. This eliminates a major obstacle of the Weil pairing approach: The point that makes $e_\psi(P,\cdot)$ a primitive $r$th root of unity is defined over $\mathbb{F}_q$ (in the case of the Weil pairing it exists in a *very* large extension, unless the curve is supersingular). Furthermore, it is known in advance. We have the following theorem.

**Theorem 4.5.** *Let $P$ be a point in $E(\mathbb{F}_q)$ of prime order $r$, such that $r^d$ does not divide $N$. Then there is an efficiently computable point $P'$ such that the map*

$$V : \langle P \rangle \to \mu_r, \quad Q \mapsto e_\psi(Q,P')$$

*is a group isomorphism. In particular, if $d=2$, then $P'=P$.*

## 5. Computing the pairing

We turn now to the computation of the generalized Weil pairing. A computation using the definition directly would result in an exponential time algorithm. Thus, we need some other formula suitable for the computation. Such a formula can be found using Galois cohomology. This formula, not surprisingly, also provides the connection between our construction and the Frey–Rück construction that uses the Tate pairing. Although part of the material of this section is well known, we choose to include it, in order to keep the paper as self-contained as possible.

Let $E/\mathbb{F}_q$ be an elliptic curve, and let $\psi : E \to E$ be an isogeny. We start from the following exact sequence:

$$0 \to \ker(\psi) \to E(\bar{\mathbb{F}}_q) \xrightarrow{\psi} E(\bar{\mathbb{F}}_q) \to 0. \tag{4}$$

Taking $\mathrm{Gal}(\bar{\mathbb{F}}_q/\bar{\mathbb{F}}_q)$ cohomology, we obtain the following long sequence:

$$\begin{aligned} &0 \to E(\mathbb{F}_q) \cap \ker(\psi) \to E(\mathbb{F}_q) \xrightarrow{\psi} E(\mathbb{F}_q) \\ &\xrightarrow{\delta} H^1(G, \ker(\psi)) \to H^1(G, E(\bar{\mathbb{F}}_q)) \xrightarrow{\psi} H^1(G, E(\bar{\mathbb{F}}_q)), \end{aligned}$$

where $G = \mathrm{Gal}(\bar{\mathbb{F}}_q/\mathbb{F}_q)$. We can extract now the short exact sequence, sometimes called the *Kummer sequence* for $E/\mathbb{F}_q$,

$$0 \to \frac{E(\mathbb{F}_q)}{\psi E(\mathbb{F}_q)} \xrightarrow{\delta} H^1(G, \ker(\psi)) \to H^1(G, E(\bar{\mathbb{F}}_q))[\psi] \to 0, \tag{5}$$

where $H^1(G, E(\bar{\mathbb{F}}_q))[\psi]$ denotes the subgroup of $H^1(G, E(\bar{\mathbb{F}}_q))$ that is sent to the zero cocycle class by $\psi$. The connecting homomorphism $\delta$ is defined as follows. Let $P \in E(\mathbb{F}_q)$, and let $Q \in E(\bar{\mathbb{F}}_q)$ such that $\psi(Q) = P$. Then a 1-cocycle representing $\delta(P)$ is given by

$$G \to \ker(\psi),$$
$$\sigma \mapsto Q^\sigma - Q,$$

that is

$$\delta(P)(\sigma) = Q^\sigma - Q.$$

From this point on, we specialize $\psi = 1 - \phi$, the case of interest here. Then we know that $\ker(\psi) = E(\mathbb{F}_q)$, so the action of $G$ on $\ker(\psi)$ becomes trivial, and therefore

$$H^1(G, \ker(\psi)) = Hom(G, \ker(\psi)).$$

Furthermore, Hilbert's Theorem 90 provides the isomorphism

$$\frac{\mathbb{F}_q^*}{(\mathbb{F}_q^*)^r} \cong H^1(G, \mu_r).$$

Assume further, that $a_q \equiv 2 \pmod r$, for a prime $r$. Then we know that $q - 1 \equiv 0 \pmod r$, and therefore, $\mathbb{F}_q$ contains all the $r$th roots of unity. Denote by $\mu_r$ the group of $r$th roots of unity in $\mathbb{F}_q$. Then $G$ acts trivially on $\mu_r$, so

$$H^1(G, \mu_r) = Hom(G, \mu_r),$$

and we have the isomorphism

$$\delta_K \colon \mathbb{F}_q^*/(\mathbb{F}_q^*)^r \to Hom(G, \mu_r)$$
$$b \cdot (\mathbb{F}_q^*)^r \mapsto (\sigma \mapsto \beta^\sigma/\beta),$$

where $b \in \mathbb{F}_q^*$, $\beta \in \bar{\mathbb{F}}_q^*$, and $\beta^r = b$. In other words, for some $b \in \mathbb{F}_q^*$, $\delta_K(b)$ is a homomorphism from $G$ to $\mu_r$, and

$$\delta_K(b)(\sigma) = \frac{\beta^\sigma}{\beta}. \tag{6}$$

Then it can be shown (see [23, Section X.1] or [6, Section V.2]), that there exists a pairing

$$B \colon \frac{E(\mathbb{F}_q)}{\psi E(\mathbb{F}_q)} \times \ker(\psi) \to \frac{\mathbb{F}_q^*}{(\mathbb{F}_q^*)^r},$$

such that

$$e_\psi(\delta(S), T) = \delta_K(B(S, T)).$$

We note that $\delta(S)$ is not a point in $\ker(\psi)$, and $\delta_K(B(S,T))$ is not an $r$th root of unity. The above relation is to be interpreted as follows.

$$\text{For any} \quad \sigma \in G, \quad e_\psi(\delta(S)(\sigma), T) = \delta_K(B(S, T))(\sigma). \tag{7}$$

The crucial thing is that the bilinear pairing $B$ can be computed efficiently, at least in the case of interest. In fact, if $T \in \ker(\psi)$ is a point of order $r$, and $S \neq T$, then

$$B(S, T) \equiv f_T(S) \,(\mathrm{mod}\, (\mathbb{F}_q^*)^r),$$

where $f_T$ is a function with divisor

$$\mathrm{div}(f_T) = r(T) - r(O).$$

If $T = S$, then we can use bilinearity to obtain

$$B(T, T) = f_T(-T)^{-1}.$$

More generally, for any point $X \neq T$ we have

$$\begin{aligned} B(S, T) &= B(S + X - X, T) = B(S + X, T)\, B(-X, T) \\ &= B(S + X, T) B(X, T)^{-1} = \frac{f_T(S + X)}{f_T(X)}. \end{aligned}$$

We recall that now that our problem is the following: Given points $P, Q \in E(\mathbb{F}_q)$, with $\#\langle P\rangle = r$, we want to compute $e_\psi(Q, P)$. We deal with elliptic curves with $a_q \equiv 2 \,(\mathrm{mod}\, r)$. From Eq. (7) we have

$$e_\psi(\delta(S)(\sigma), P) = \delta_K(B(S, P))(\sigma), \tag{8}$$

where $\delta(S)(\sigma) = R^\sigma - R$ for some point $R$ such that $\psi(R) = S$.

If we choose $\sigma$ to be the $q$-power Frobenius automorphism in $G = \mathrm{Gal}(\bar{\mathbb{F}}_q/\mathbb{F}_q)$, and $S = -Q$, then we have

$$\phi(R) = R^\sigma \quad \text{for any } R \in E. \tag{9}$$

Also,

$$\begin{aligned} &\psi(R) = S \quad \Rightarrow \\ &R - \phi(R) = S \quad \Rightarrow \\ &\phi(R) - R = -S \quad \Rightarrow \\ &R^\sigma - R = -S \quad \Rightarrow \\ &\delta(S)(\sigma) = Q. \end{aligned}$$

Thus, Eq. (8) has become

$$e_\psi(Q,P) = \delta_K(B(-Q,P))(\sigma), \tag{10}$$

where $\sigma$ is now fixed (and equal to the Frobenius automorphism).

It remains to compute $\delta_K(B(-Q,P))(\sigma)$. We recall from Eq. (6) that

$$\delta_K(B(-Q,P))(\sigma) = \frac{\beta^\sigma}{\beta},$$

where

$$\beta^r = B(-Q,P) = B(Q,P)^{-1} \equiv f_P(Q)^{-1} \,(\mathrm{mod}\,(\mathbb{F}_q^*)^r).$$

We have,

$$\frac{\beta^\sigma}{\beta} = \frac{\beta^q}{\beta} = \beta^{q-1}.$$

Therefore, $\delta_K(B(-Q,P))(\sigma)$ can be computed as

$$\delta_K(B(-Q,P))(\sigma) = \left(\frac{f_P(X)}{f_P(X+Q)}\right)^{(q-1)/r}$$

for any point $X \in E(\bar{\mathbb{F}}_q)$, $X \neq P$. Putting everything together, we have

$$e_\psi(Q,P) = \left(\frac{f_P(X)}{f_P(X+Q)}\right)^{(q-1)/r}. \tag{11}$$

Eq. (11) can now be used to compute the value $e_\psi(Q,P)$. One first computes $f_P(X+Q)$ and $f_P(X)$ using repeated doubling. The point $X$ has to be chosen suitably, so that the points $X$ and $X+Q$ do not appear in the support of the divisors of the functions that appear in the computation. Those functions have divisors with support contained in $\langle P\rangle$, so one wants to avoid $X \in \langle P\rangle$. Thus one may choose $X \in E(\mathbb{F}_q)$, which in the case $q-1 > r$ yields a useful point with probability at least $\frac{1}{2}$, or one may even choose $X \in E(\mathbb{F}_{q^2})$, which yields a useful point with probability at least $1-1/q$. The algorithm for computing the classical Weil pairing was first given by Miller. An elegant presentation of the same algorithm is contained in [12]. The value $(f_P(X)/f_P(X+Q))^{(q-1)/r}$ is computed using repeated squaring in $\mathbb{F}_q$.

Finally, it is interesting to note that for elliptic curves with $a_q \equiv 2 \,(\mathrm{mod}\, r)$, and if $P$ is a point of order $r$, then

$$e_\psi(Q,P) = \phi_r(Q,P)^{-1},$$

where $\phi_r$ is the Tate pairing, used by Frey et al. [12].

We note that what is important for the efficient computation of both the Tate pairing and $e_{1-\phi}$ is the fact that we are able to express its values in terms of values of the rational function $f_P$, whose divisor has very few points, all defined over the base field (a small extension would also do). The repeated doubling procedure mentioned above is the simplest way to use formula (11) to compute $e_{1-\phi}$. Indeed, there are

more efficient ways to evaluate the Tate pairing (and thus $e_{1-\phi}$). Such methods are described for instance in [5,14].

## 6. Curves with trace congruent to 2

We can relax the requirement $a_q = 2$ a little, and assume only that $a_q \equiv 2 \pmod r$. This is equivalent to say $r|q-1$. Then, it is not in general the case that $\ker(1-\hat{\phi}) = E(\mathbb{F}_q)$. However, if in the above derivation we take $Q \in \langle P \rangle$. Then we conclude that

$$\hat{\phi}(Q) = [a_q - 1]Q = Q,$$

because $a_q \equiv 2 \pmod n$ and $[r]Q = O$. Thus, we have

$$\langle P \rangle \subseteq \ker(1-\hat{\phi}).$$

For simplicity, we will only consider the case that no higher power of $r$ divides $N = \#E(\mathbb{F}_q)$—which is the only interesting case in cryptography. Then we claim that $e_\psi(P,P)$ is again a primitive $r$th root of unity.

**Lemma 6.1.** *There exist a point $S \in \ker(1-\hat{\phi})$, such that $e_\psi(P,S)$ is a primitive $r$th root of unity.*

**Proof.** It is clear that $e_\psi(P,S)$ is an $r$th root of unity. Furthermore, as the point $S$ ranges over $\ker(1-\hat{\phi})$, the values $e_\psi(P,S)$ are in a subgroup of $\mu_N$, say $\mu_d$. It follows that for all $S \in \ker(1-\hat{\phi})$, we have

$$1 = e_\psi(P,S)^d = e_\psi([d]P,S).$$

The non-degeneracy of $e_\psi$ then implies that $[d]P = O$, i.e., $r$ divides $d$. It follows that the order of $e_\psi(P,S)$ is exactly $r$ for some point $S$. □

As we pointed out in Section 3, we have $\hat{N} = \#\ker(1-\hat{\phi})\,|N$. We also showed that $r|\#\ker(1-\hat{\phi})$. We adopt the following notation: $N = lr$, and $\hat{N} = \hat{l}r$, with $\hat{l}|l$. Also, $\ker(1-\hat{\phi})$ is the product of at most two cyclic groups, one of which contains $\langle P \rangle$. If $(S_1, S_2)$ is a pair of generators for $\ker(1-\hat{\phi})$, it follows that the order of $e_\psi(P,S_1)$ divides $r$. If the order was 1, then it would violate the non-degeneracy of $e_\psi$ (the argument is virtually the same as in Lemma 4.2 followed by Theorem 4.3 for $k=1$). Then, since $P \in \langle S_1 \rangle$, it will be $P = [l']S_1$. Therefore,

$$1 = e_\psi(P,P)^d = e_\psi(P,S_1)^{l'd}$$

which implies that $d$ has to be $r$ (since $r^2 \nmid \hat{N}$). Therefore, we have the theorem.

**Theorem 6.2.** *Let $E/\mathbb{F}_q$ be an elliptic curve, $P \in E(\mathbb{F}_q)$ a point of prime order $r$ such that $r^2 \nmid N$, and assume that $a_q \equiv 2 \pmod r$. Then $e_\psi(P,P)$ is a primitive $r$th root of unity.*

We also note that the proof given in Section 5 goes through in this more general case word by word. Therefore, the algorithm of the previous section works in the case $a_q \equiv 2 \pmod{r}$ as it is.

## 7. Conclusions

We have reviewed the construction of a well-known generalization of the Weil pairing, which associates a bilinear and non-degenerate pairing $e_\psi$ to every endomorphism $\psi$ of the elliptic curve. We focus at the special case $\psi = 1-\phi$, where $\phi$ is the Frobenius endomorphism, and show how $e_{1-\phi}$ can be used to obtain a reduction of the elliptic curve discrete logarithm problem to the discrete logarithm problem in the underlying finite field. The construction is efficient if $a_q \equiv 2 \pmod{r}$, where $a_q$ is the trace of Frobenius, and $r$ is the order of the base point. An important step of the reduction is the efficient computation of the pairing. We prove a formula that can be used directly for the computation of $e_{1-\phi}$. As a side result of this formula we obtain a connection between $e_{1-\phi}$ and the Tate pairing, used by Frey and Rück for the same reduction.

Pairings on elliptic curves have recently found many positive applications in cryptography (see for instance [8,9]). The efficiency and generality of our construction may, thus, be useful in the construction of cryptographic protocols such as the ones mentioned above.

## Acknowledgements

I am grateful to Allan Borodin for encouraging my research, Kumar Murty, Daniel Panario, and Ian Blake for numerous enlightening discussions on the subject, and to Nigel Boston and Igor Shparlinski for reading the manuscript and providing many helpful comments.

## References

[1] L.M. Adleman, A subexponential algorithm for the discrete logarithm problem with applications to cryptography, in: Proc. 20th IEEE Foundation on Computer Science Symp. 1979, pp. 55–60.
[2] L.M. Adleman, The function field sieve, in: 1st Internat. Algorithmic Number Theory Symp.—ANTS I, LNCS-Lecture Notes in Computer Science, Vol. 877, Berlin, Germany, Springer, Berlin, 1994, pp. 108–121.
[3] L.M. Adleman, J. DeMarrais, A subexponential algorithm for discrete logarithms over all finite fields, in: D.R. Stinson (Ed.), Proc. CRYPTO 93, Lecture Notes in Computer Science, Vol. 773, Springer, Berlin, 1994, pp. 147–158.
[4] L.M. Adleman, M.D. Huang, Function field sieve method for discrete logarithms over finite fields, INFCTRL: Inform. Comput. (formerly Information and Control) 151 (1999) 5–16.
[5] P.S.L.M. Barreto, H.Y. Kim, B. Lynn, M. Scott, Efficient algorithms for pairing-based cryptosystems, in: M. Yung (Ed.), Advances in Cryptology—Crypto 2002, Lecture Notes in Computer Science, Vol. 2442, Springer, Berlin, 2002, pp. 354–368.
[6] I. Blake, G. Seroussi, N. Smart, Elliptic curves in Cryptography, London Mathematical Society, Lecture Note Series, Vol. 265, Cambridge University Press, Cambridge, 1999.

[7] I.F. Blake, R. Fuji-Hara, R.C. Mullin, S.A. Vanstone, Computing logarithms in finite fields of characteristic two, SIAM J. Algorithm Disc. Methods 5 (1985) 276–285.
[8] D. Boneh, M. Franklin, Identity-based encryption from the weil pairing, in: Advances in Cryptology—Crypto 2001, Lecture Notes in Computer Science, Vol. 2139, Springer, Berlin, 2001, pp. 213–229.
[9] D. Boneh, B. Lynn, H. Shacham, Short signatures from the Weil pairing, in: Advances in Cryptology—Asiacrypt 2001, Lecture Notes in Computer Science, Vol. 2248, Springer, Berlin, 2001, pp. 514–532.
[10] D. Coppersmith, Fast evaluation of logarithms in fields of characteristic two, IEEE Trans. Inform. Theory IT-30 (1984) 587–594.
[11] W. Diffie, M. Hellman, New directions in cryptography, IEEE Trans. Inform. Theory 22 (1976) 472–492.
[12] G. Frey, M. Müller, H.G. Rück, The Tate pairing and the discrete logarithm applied to elliptic curve cryptosystems, IEEE Trans. Inform. Theory 45 (5) (1999) 1717–1719.
[13] G. Frey, H.G. Rück, A remark concerning $m$-divisibility and the discrete logarithm in the divisor class group of curves, Math. Comput. 62 (206) (1994) 865–874.
[14] S.D. Galbraith, K. Harrison, D. Soldera, Implementing the tate pairing, in: Algorithmic Number Theory Symp.—ANTS-V, Lecture Notes in Computer Science, Vol. 2369, Springer, Berlin, 2002, pp. 324–337.
[15] T. Garefalakis, D. Panario, The index calculus method using non-smooth polynomials, Math. Comput. 70 (235) (2001) 1253–1264.
[16] D.M. Gordon, Discrete logarithms in GF($p$) using the number field sieve, SIAM J. Disc. Math. 6(1) (February 1993) 124–138.
[17] R. Harasawa, J. Shikata, J. Suzuki, H. Imai, Comparing the MOV and FR reductions in elliptic curve cryptography, in: Advances in Cryptology—Eurocrypt '99, Lecture Notes in Computer Science, Vol. 1592, Springer, Berlin, 1999, pp. 190–205.
[18] N. Koblitz, Elliptic curve cryptosystems, Math. Comput. 48 (177) (1987) 203–209.
[19] K.S. McCurley, The discrete logarithm problem, Proc. Symp. Appl. Math. 42 (1990) 49–74.
[20] A. Menezes, E. Okamoto, S. Vanstone, Reducing elliptic curve logarithms to logarithms in a finite field, IEEE Trans. Inform. Theory 39 (1993) 1639–1646.
[21] V.S. Miller, Uses of elliptic curves in cryptography, in: H.C. Williams (Ed.), Advances in Cryptology—Crypto '85, Proc. Lecture Notes in Computer Science, Vol. 218, Springer, Berlin, 1986, pp. 417–426.
[22] C. Pomerance, Fast, rigorous factorization and discrete logarithm algorithms, in: Discrete Algorithms, and Complexity, Proc. Japan–US Joint Seminar, Academic Press, New York, 1986, pp. 119–143.
[23] J.H. Silverman, The Arithmetic of Elliptic Curves, Graduate Texts in Mathematics, Vol. 106, Springer, Berlin, 1986.