A group law with PKC applications

R. DURÁN DÍAZ¹, V. GAYOSO MARTÍNEZ²
L. HERNÁNDEZ ENCINAS², and J. MUÑOZ MASQUE²

¹ Departamento de Automática, Universidad de Alcalá,
E-28871 Alcalá de Henares, Spain
E-mail: raul.duran@uah.es
² Instituto de Tecnologías Físicas y de la Información (ITEFI)
Consejo Superior de Investigaciones Científicas (CSIC),
E-28006 Madrid, Spain
E-mails: {victor.gayoso, luis, jaime}@iec.csic.es

Abstract
Let F be a field, let V = F³, and let A: V → V be a linear map. For every x = (x₁, x₂, x₃) ∈ V, the polynomial P(x) = det(x₁I + x₂A + x₃A²) does not depend on A, but only on its characteristic polynomial χ(X). A law of composition ⊕: V × V → V is defined and it induces an Abelian group law on F² \ P⁻¹(0). The cubic P⁻¹(0) is irreducible if and only if χ is irreducible in F[X], and in this case the group law ⊕ is cyclic. As an application example, a Diffie-Hellman-like key agreement protocol based on the proposed group law is provided.

Keywords: Abelian group law, DLP, norm of an extension, projective cubic curve
Mathematics Subject Classification 2010: Primary 94A60 Secondary 14H52, 14H50, 14L15

1 Introduction

Let F be a field and let us consider a linear endomorphism A: V → V of the vector space V = F³. We define the polynomial P(x) = det(x₁I + x₂A + x₃A²), where x = (x₁, x₂, x₃) ∈ V. The polynomial P is homogeneous of degree 3, and does not depend on A, but only on the characteristic polynomial χ(X) of A.

A new group law is proposed ⊕: V × V → V, which induces an Abelian group law on F² \ P⁻¹(0). The computation of the group law is carried out by means of a single set of formulas, involving coefficients from the base field, which are applicable to any element of the group, with no exception whatsoever.

If the characteristic polynomial χ(X) is irreducible in F[X], then P⁻¹(0) = ∅. In this case, the group law extends to the whole set F²; moreover, if the base field is a finite field Fq, with characteristic different from 2 or 3, then the group G = (F𝑞P², ⊕) is proved to be cyclic.

The latter property permits us to apply the notion of discrete logarithm to the group G. If we fix a generator g ∈ FqP², then any element h of the
group is the addition of $g$ with itself a finite number of times, say $n$, so that $h = g \oplus g \oplus \cdots \oplus g = [n]g$. The number $n$ is the logarithm of $h$ to the base $g$.

Given any element $h \in \mathbb{G}$, and a generator $g$ of the group, the discrete logarithm problem, or DLP, consists in finding the smallest integer $n$, such that $h = [n]g$. In this work, we prove that the DLP over $\mathbb{G}$ with a proper choice of the generator is equivalent to the DLP over the multiplicative group $(\mathbb{F}_q)^\times$.

Popular current cryptosystems are based on the discrete logarithm problem over different groups, such as the group of invertible elements in a finite field, or the group of points of an elliptic curve with the addition of points as group operation. Our proposal could fit perfectly well in the same niche.

As is the case for analogous public key protocols, the users of the presented proposal agree to a single base field $\mathbb{F}_q$ but each one of them is allowed to select at will any (irreducible) polynomial

$$\chi(X) = X^3 - c_1X^2 - c_2X - c_3, \quad c_1, c_2, c_3 \in \mathbb{F}_q.$$  

The public system parameters consist of the base field $\mathbb{F}_q$, the coefficients $c_1, c_2, c_3 \in \mathbb{F}_q$, and the generator $g$.

## 2 The group law defined

**Lemma 2.1.** Let $\mathbb{F}$ be a field and let $V$ be the vector space $\mathbb{F}^3$. If $A : V \to V$ is a linear map such that the endomorphisms $I, A, A^2$ are linearly independent, then the homogeneous cubic polynomial $P(x) = \det(x_1 I + x_2 A + x_3 A^2)$ does not depend on the matrix $A$ but only on the coefficients $c_1, c_2, c_3$ of its characteristic polynomial $\chi(X) = X^3 - c_1X^2 - c_2X - c_3$.

**Proof.** Let $\overline{\mathbb{F}}$ be the algebraic closure of $\mathbb{F}$. As the endomorphisms $I, A, A^2$ are linearly independent, the annihilator polynomial of $A$ coincides with $\chi(X)$ by virtue of the Cayley-Hamilton theorem. Hence there exists a basis of $\mathbb{F}^3$ such that the matrix of $A$ in this basis equals one of the following three matrices:

\[
M_1 = \begin{pmatrix} 
\alpha_1 & 0 & 0 \\
0 & \alpha_2 & 0 \\
0 & 0 & \alpha_3 
\end{pmatrix},
\]

\[
M_2 = \begin{pmatrix} 
\alpha_1 & 0 & 0 \\
0 & \alpha_2 & 0 \\
0 & 1 & \alpha_2 
\end{pmatrix},
\]

\[
M_3 = \begin{pmatrix} 
\alpha_1 & 0 & 0 \\
1 & \alpha_1 & 0 \\
0 & 1 & \alpha_1 
\end{pmatrix},
\]

and from a simple calculation we obtain

\[
P(x) = \det(x_1 I + x_2 M_i + x_3 (M_i)^2)
= -c_2 x_1 (x_2)^2 + [(c_2)^2 - 2(c_1 c_3)] x_1 x_3 x_2 + c_1 x_1 x_2 x_3
+ [(c_1)^2 + 2c_2] (x_1)^2 x_3 - (c_2 c_3)(x_2)^2 x_3 + (c_1 c_3)(x_2)^2 x_3
- (c_1 c_3 + 3c_3) x_1 x_2 x_3 + (x_1)^3 + c_3 (x_2)^3 + (c_3)^2 (x_3)^3,
\]

for every $i = 1, 2, 3$. \qed
Theorem 2.2. Every linear map \( A : V \rightarrow V \) such that the endomorphisms \( I, A, A^2 \) are linearly independent, induces a law of composition

\[
\oplus : V \times V \rightarrow V,
\]

\[
(x, y) \mapsto z = x \oplus y,
\]

by the following formula:

\[
(3) \quad z_1 + z_2 A + z_3 A^2 = \left( x_1 I + x_2 A + x_3 A^2 \right) \left( y_1 I + y_2 A + y_3 A^2 \right),
\]

where \( x = (x_1, x_2, x_3), \ y = (y_1, y_2, y_3), \ z = (z_1, z_2, z_3). \)

Moreover, the set of elements \( x \in V \) such that \( x \oplus y = (0, 0, 0) \) for some element \( y \in V \setminus \{(0, 0, 0)\} \) coincides with the set \( P^{-1}(0) \), and \( \oplus \) induces a group law

\[
\oplus : (\mathbb{P}^3 \setminus P^{-1}(0)) \times (\mathbb{P}^3 \setminus P^{-1}(0)) \rightarrow (\mathbb{P}^3 \setminus P^{-1}(0)).
\]

If \( C \) denotes the projective cubic curve defined by \( P(x) = 0 \), then the group law \( \oplus \) also induces a group law

\[
\oplus : (\mathbb{P}P^2 \setminus C) \times (\mathbb{P}P^2 \setminus C) \rightarrow \mathbb{P}P^2 \setminus C.
\]

Proof. As \( A^3 = c_1 A^2 + c_2 A + c_3 I, \) and

\[
A^2 \cdot A^3 = A \cdot A^3 = (c_1 c_3) I + (c_1 c_2 + c_3) A + \left( (c_1)^2 + c_2 \right) A^2,
\]

from the formula in \( (3) \) it follows:

\[
(4) \quad z_1 = x_1 y_1 + c_3 (x_2 y_3 + x_3 y_2) + (c_1 c_3) x_3 y_3,
\]

\[
z_2 = x_1 y_2 + x_2 y_1 + c_2 (x_2 y_3 + x_3 y_2) + (c_1 c_2 + c_3) x_3 y_3,
\]

\[
z_3 = x_2 y_2 + x_1 y_3 + x_3 y_1 + c_1 (x_2 y_3 + x_3 y_2) + \left( (c_1)^2 + c_2 \right) x_3 y_3.
\]

In matrix notation, these formulas can equivalently be written as

\[
\begin{pmatrix}
    z_1 \\
    z_2 \\
    z_3
\end{pmatrix} = \begin{pmatrix}
    x_1 & c_3 x_3 & c_1 c_3 x_3 + c_3 x_2 \\
    x_2 & x_1 + c_2 x_3 & c_2 x_2 + c_3 x_3 + c_1 c_2 x_3 \\
    x_3 & x_2 + c_1 x_3 & x_1 + (c_1)^2 x_3 + c_1 x_2 + c_2 x_3
\end{pmatrix} \begin{pmatrix}
    y_1 \\
    y_2 \\
    y_3
\end{pmatrix},
\]

and as a simple computation shows, the determinant of the linear system above is equal to \( P(x) \), where \( P \) is defined by the formula \( (2) \). Hence \( x \oplus y = (0, 0, 0) \), for some \( y \in V \setminus \{(0, 0, 0)\} \), if and only if \( P(x) = 0 \).

The commutativity of \( \oplus \) is a direct consequence of the invariance of the formula \( (1) \) under the substitutions \( x_i \mapsto y_i, \ y_i \mapsto x_i, \ 1 \leq i \leq 3. \)

Moreover, the formula \( (3) \) can also be written as follows:

\[
(x \oplus y_1) I + (x \oplus y_2) A + (x \oplus y_3) A^2 = (x_1 I + x_2 A + x_3 A^2) \left( y_1 I + y_2 A + y_3 A^2 \right).
\]

From the associativity of the composition law of endomorphisms we deduce

\[
(x \oplus (y \oplus z)) I + (x \oplus (y \oplus z)) A + (x \oplus (y \oplus z)) A^2 = (x_1 I + x_2 A + x_3 A^2) \cdot \left( (y_1 I + y_2 A + y_3 A^2) \cdot (z_1 I + z_2 A + z_3 A^2) \right)
\]

\[
= ((x_1 I + x_2 A + x_3 A^2) \cdot (y_1 I + y_2 A + y_3 A^2)) \cdot (z_1 I + z_2 A + z_3 A^2)
\]

\[
= ((x \oplus y) \oplus z) I + ((x \oplus y) \oplus z) A + ((x \oplus y) \oplus z) A^2.
\]
Hence \( x \oplus (y \oplus z) = (x \oplus y) \oplus z, \forall x, y, z \in V. \)

From \([4]\) it follows that the unit element is the point \((1,0,0),\) which does not belong to \(P^{-1}(0)\) since \(P(1,0,0) = 1.\)

By taking determinants in the equation \([3]\) we obtain
\[
P(x \oplus y) = P(x)P(y), \quad \forall x, y \in V.
\]

Therefore the opposite element \(y\) of \(x\) exists and it is given by the following formulas:
\[
\begin{align*}
y_1 &= \frac{c_1x_1x_2 + [(c_1)^2 + 2c_2]x_1x_3 - (c_1 + c_2)x_2x_3 + (x_1)^2 - c_2(x_2)^2 + 3(c_2)^2 - c_1c_3]{P(x)}, \\
y_2 &= \frac{-x_1x_2 + (c_1)^2x_2x_3 + (c_1x_2)^2 - (c_1 + c_2)(x_3)^2}{P(x)}, \\
y_3 &= \frac{-x_1x_2 + (c_1x_2)^2 + (x_2)^2 - c_2(x_3)^2}{P(x)}.
\end{align*}
\]

Finally, if \(x, y\) are replaced by \(\lambda x, \mu y,\) respectively, with \(\lambda, \mu \in \mathbb{F}^*;\) then \(z\) transforms into \(\lambda \mu z,\) thus proving that the group law projects onto \(\mathbb{F}P^2 \setminus C.\) \(\square\)

Remark 2.3. Note that the equations in \([4]\), allowing one to compute the \(\oplus\) group operation in terms of the coefficients in the ground field, are applicable to any element of the group, with no exception at all.

Remark 2.4. If \(v_1 = (1,0,0), v_2 = (0,1,0), v_3 = (0,0,1),\) then from \([2]\) we obtain \(P(v_1) = c_3, P(v_2) = (c_3)^2.\) Hence \(v_2\) and \(v_3\) belong to \(\mathbb{F}^3 \setminus P^{-1}(0)\) if and only if \(c_3 \neq 0,\) i.e., when \(A\) is invertible.

3. The basic cubic

Proposition 3.1. Let \(\chi(X) = X^3 - c_1X^2 - c_2X - c_3 \in \mathbb{F}[X]\) be the polynomial introduced in Lemma \([2.1]\) and let \(\alpha = X \mod \chi.\) If \(N: \mathbb{F}[\alpha] \to \mathbb{F}\) is the norm of the extension \(\mathbb{F} \hookrightarrow \mathbb{F}[\alpha],\) then a point \(\beta = \beta_0 + \beta_1\alpha + \beta_2\alpha^2\) belongs to the cubic curve \(C\) defined in Theorem \([2.2]\) if and only if \(N(\beta) = 0.\) In particular, if \(\chi\) is irreducible in \(\mathbb{F}[X],\) then \(C\) has no point in \(\mathbb{F}P^2.\)

Moreover, the polynomial \(\chi\) is irreducible in \(\mathbb{F}[X]\) if and only if the cubic \(C\) is irreducible.

Proof. Every \(\beta \in \mathbb{F}[\alpha]\) induces a \(\mathbb{F}\)-linear endomorphism \(E_{\beta}: \mathbb{F}[\alpha] \to \mathbb{F}[\alpha]\) given by \(E_{\beta}(\xi) = \beta : \xi, \forall \xi \in \mathbb{F}[\alpha],\) and from the very definition of the norm we have \(N(\beta) = \det E_{\beta}.\) As a computation shows, we obtain \(N(\beta) = P(\beta_0, \beta_1, \beta_2),\) thus proving the first part of the statement. Moreover, \(\chi\) is irreducible if and only if \(\mathbb{F}[\alpha]\) is a field and then the norm is injective, thus proving the second part of the statement.

Finally, if \(\chi\) factors in \(\mathbb{F}[X],\) say \(X^3 - c_1X^2 - c_2X - c_3 = (X-h)(X^2+kX+l),\) with \(h, k, l \in \mathbb{F},\) then we have
\[
P(x) = [(x_1)^2 + (k^2 - 2l)x_1x_3 + l(x_2)^2 - klx_2x_3 + l^2(x_3)^2 - kx_1x_2][x_1 + hx_2 + h^2x_3].
\]

Conversely, if \(\chi\) is irreducible in \(\mathbb{F}[X],\) then according to Proposition \([3.1]\) the only solution to the cubic equation \(P(x) = 0\) is \(x = 0.\) Hence \(P\) must be irreducible, as a reducible cubic admits non-trivial solutions in the ground field. \(\square\)
Corollary 3.2. If the characteristic polynomial $\chi$ of $A$ is irreducible in $\mathbb{F}[X]$, then there is no linear transformation $(\lambda_j)_{j=1}^3 \in GL(\mathbb{F}, 3)$ reducing the polynomial $P$ defined in (2) to Weierstrass form.

Proof. Replacing $x_j$ by $x_j = \sum_{i=1}^3 \lambda_i x_i$, $1 \leq j \leq 3$, in (2) we obtain a cubic $\tilde{P}$, which is in Weierstrass form (see [13, §2.1]) if and only if the coefficients $a$, $b$, and $c$ of the terms $(x_3)^3$, $(x_1)^2 x_2$, and $x_1(x_2)^2$, respectively, vanish. As a computation shows, we have $a = \tilde{P}(\lambda_3, \lambda_2, \lambda_1)$, and we can conclude by applying Proposition 3.1.

4 Cyclicity

Theorem 4.1. If $\mathbb{F}_q$ is a finite field of characteristic different from 2 or 3 and the polynomial $\chi(X) = X^3 - c_1 X^2 - c_2 X - c_3$ introduced in Lemma 2.1 is irreducible in $\mathbb{F}_q[X]$, then the group $G = (\mathbb{F}_q P^2, \oplus)$ is cyclic.

Proof. Since char $\mathbb{F}_q \neq 2, 3$, the polynomial $\chi$ is separable and in its splitting field $\mathbb{F}_q'$ we have $\chi(X) = (X - \alpha_1)(X - \alpha_2)(X - \alpha_3)$, the roots $\alpha_1, \alpha_2, \alpha_3$ being pairwise distinct, and in a certain basis of $\mathbb{F}_q' \otimes_{\mathbb{F}_q} V$ the matrix of $A$ is given by the formula (1). As the Galois group $G(\mathbb{F}_q'/\mathbb{F}_q)$ acts transitively on the roots of $\chi$, there exist two automorphisms such that $\sigma_2(\alpha_1) = \alpha_2$ and $\sigma_3(\alpha_1) = \alpha_3$. If $\beta = \beta_1 + \beta_2 \alpha_1 + \beta_3 (\alpha_1)^2$, $\beta_i \in \mathbb{F}_q$, $1 \leq i \leq 3$, is an element in $\mathbb{F}_q[\alpha_1] \cong \mathbb{F}_q^3$, then for every positive integer $n$ we have

$$\left(\beta_1 I + \beta_2 A + \beta_3 A^2\right)^n = \begin{pmatrix} \beta^n & 0 & 0 \\ 0 & \sigma_2(\beta^n) & 0 \\ 0 & 0 & \sigma_3(\beta^n) \end{pmatrix}.$$ 

Consequently, if $\beta$ is a generator of the multiplicative group $(\mathbb{F}_q^3)^*$, then the vector $(\beta_1, \beta_2, \beta_3)$ generates the group $((\mathbb{F}_q^3 \setminus \{(0,0,0)\}, \oplus)$ and its corresponding projective point $[\beta_1, \beta_2, \beta_3]$ is $[\beta, \beta_2, \beta_3]$ mod $\mathbb{F}_q^*$ generates the group $G$, with $\mathbb{F}_q P^2 = ((\mathbb{F}_q^3 \setminus \{(0,0,0)\})/\mathbb{F}_q^*.$

Remark 4.2. It is important to keep in mind that the implication in Theorem 4.1 works only in the way in which it is worded. If one selects a generator of the group $G$, it will in general be a generator of only a subgroup of the whole $(\mathbb{F}_q^3)^*$ group. Consequently, when choosing a generator for $G$, it is convenient to pick it from the set of generators in $(\mathbb{F}_q^3)^*$ and, after that, project it onto $\mathbb{F}_q P^2$.

Remark 4.3. As the order of the group $G = (\mathbb{F}_q P^2, \ominus)$ is $q^2 + q + 1$, the statement of Theorem 4.1 means that there exists an element $\beta \in G$ of order $q^2 + q + 1$. According to the proof of Theorem 4.1 this is equivalent to saying that the matrix $A$ in (1) is of order $q^2 + q + 1$ in the linear group $GL(\mathbb{F}_q, 3)$. A classical result (see [13, Theorem, p. 379]) states that such a collineation always exists, but we need a direct proof of this fact to be able to apply it below in section 5; also see [6, Proposition 2.1].

Remark 4.4. When the polynomial $\chi$ is reducible, experimental tests carried out in the prime field $\mathbb{F}_p$ show that the projective cubic curve $C$ defined as $P(x) = 0$ has a number of points from the set $\{p^2 + 2p + 1, 3p, p + 1\}$ only. Since the projective space $\mathbb{F}_p P^2$ has a total of $p^2 + p + 1$ points, we have that the group $(\mathbb{F}_p P^2 \setminus C, \oplus)$ is left, respectively, with $\{p^2 - 1, p^2 - p, (p - 1)^2, p^2\}$ points.
If the number of points of $C$ is either $p + 2$ or $2p + 1$, then the group $(\mathbb{F}_pP^2 \setminus C, \oplus)$ is still cyclic, and has the expected number of generators, namely, either $\varphi(p^2 - 1)$ or $\varphi(p^2 - p)$, respectively, where $\varphi$ is Euler’s totient function.

However none of the other two possibilities give rise to a cyclic group. Rather, for the case where $C$ has $3p$ points, there appears a number of cyclic groups, whose cardinalities are the divisors of $p - 1$; it is important to remark that the total number of points left for the group is precisely $(p - 1)^2$. Thus, the group $(\mathbb{F}_pP^2 \setminus C, \oplus)$ can be decomposed as a direct sum of a number of cyclic groups such that the product of their cardinalities is $(p - 1)^2$.

As for the case when $C$ has $p + 1$ points, the group $(\mathbb{F}_pP^2 \setminus C, \oplus)$ is not cyclic either and can be decomposed as a direct sum of 2 cyclic groups with $p$ points each. Remark that now the total number of points left for the group is $p^2$, so again the numbers of points of the cyclic groups of this case match the divisors of $p$.

5 Equivalence of DLP in $\mathbb{G}$ and $\mathbb{(F}_q^3)^\ast$

Proposition 5.1. Let $\mathbb{F}_q$ be a finite field of characteristic $\neq 2$ or 3. Assume the polynomial $\chi(X) = X^3 - c_1X^2 - c_2X - c_3$ in Lemma 2.1 is irreducible in $\mathbb{F}_q[X]$, and let $\alpha \in \mathbb{F}_q^\ast$ be a root of $\chi$.

If $(\gamma_1, \gamma_2, \gamma_3)$ is a generator of the group $((\mathbb{F}_q)^3 \setminus \{(0, 0, 0)\}, \oplus)$ and $(\beta_1, \beta_2, \beta_3)$ belongs to this group, then $n \in \mathbb{N}$ is a solution to the equation

$$(\beta_1, \beta_2, \beta_3) = (\gamma_1, \gamma_2, \gamma_3) \oplus (n \cdot (\gamma_1, \gamma_2, \gamma_3)),$$

if and only if $n$ is a solution to the equation $\beta = \gamma^n$ in the multiplicative group $((\mathbb{F}_q)^\ast, \cdot)$, where $\beta = \beta_1 + \beta_2 \alpha + \beta_3 \alpha^2$, and $\gamma = \gamma_1 + \gamma_2 \alpha + \gamma_3 \alpha^2$.

Therefore, the DLP in the group $((\mathbb{F}_q)^3 \setminus \{(0, 0, 0)\}, \oplus)$ is equivalent to the DLP in $((\mathbb{F}_q)^\ast)$.

Proof. Letting $\alpha = \alpha_1$, the statement follows from the matrix formula in the proof of Theorem 4.1 taking the very definition of the group law $\oplus$ by the formula (3) into account.

In the context of computational complexity, there exists the concept of “problem reduction” (see, for example, [16] Ch. 8], [13] p. 5] whence the next paragraph is quoted):

The idea of a reduction argument is that you can show that hardness of one problem $\mathcal{P}_1$ implies hardness of another problem $\mathcal{P}_2$—or, equivalently, that “easiness” of $\mathcal{P}_2$ would imply easiness of $\mathcal{P}_1$—by showing that anyone who had an algorithm to solve $\mathcal{P}_2$ could use it to solve $\mathcal{P}_1$ with relatively little additional effort; in that case one says that $\mathcal{P}_1$ reduces to $\mathcal{P}_2$.

In the present case, Proposition 5.1 states the “equivalence” because the reduction works both ways, namely, DLP in the group $((\mathbb{F}_q)^3 \setminus \{(0, 0, 0)\}, \oplus)$ reduces to the DLP in $((\mathbb{F}_q)^\ast)$ and the other way around. Hence, Proposition 5.1 proves that the use of the group $\mathbb{G} = (\mathbb{F}_qP^2, \oplus)$ is safe for standard implementations in PKC (e.g., see [14] §1.6]), since the security it provides is equivalent.
to that of DLP in $(\mathbb{F}_q^*)^*$, as long as the caveat stated in Remark 4.2 is taken into account.

In terms of cryptanalysis, in principle the logarithm in $\mathbb{G}$ can be computed using “generic” algorithms, i.e., those that assume no particular structure in (or extra knowledge of) the group. The most popular ones are Pohlig-Hellman, Shank’s Baby Step/Giant Step, and Pollard’s Rho algorithm. The first one is really a reduction of the computation in the whole group to the computation of the logarithm in all subgroups of prime order of $\mathbb{G}$.

Our proposal is to use a group $\mathbb{G}$ of prime order $n = p^2 + p + 1$, over a ground prime field $\mathbb{F}_p$. Hence, we are left essentially with Shank’s and Pollard’s algorithms, which need $\tilde{O}(\sqrt{n})$ and $O(\sqrt{n})$ group operations respectively to compute a logarithm. In view of these facts, we conjecture that the expected security level of the DLP in $\mathbb{G}$ is $\log_2 p$. Observe that to offer the same security level, the elliptic curve logarithm needs to operate over a ground field such that $p$ has twice as many bits.

In any case, when the group law introduced above is implemented, it seems sensible to avoid using small characteristics in view of recent cryptanalysis to DLP in $\mathbb{F}_q$ (cf. [1], [3], [7], [11]), and also extensions $\mathbb{F}_{p^n}$ of moderate characteristic included in the range of the following cryptanalysis: [2] (specially), [8], [9], [10], [12], [15], [17], which might prove also applicable to our proposal.

6 Example of application: a key agreement protocol

The group $\mathbb{G} = (\mathbb{F}_qP^2, \oplus)$ lends readily itself as a building block for standard cryptographic applications to be constructed upon it. One of such applications is a Diffie-Hellman-like key agreement protocol, which will be described in the following sections.

6.1 System set-up and system parameters

In the following, we provide the necessary steps to set up the system. Moreover, the users also need to fix some system parameters.

System set-up

To set up the system, the following steps are in order:

1. Choose a ground field $\mathbb{F}_q$ with characteristic different from 2 or 3.

2. Select elements $c_1, c_2, c_3 \in \mathbb{F}_q$ such that the polynomial

\[ \chi(X) = X^3 - c_1X^2 - c_2X - c_3 \]

is irreducible in $\mathbb{F}_q[X]$.

3. Consider $\mathbb{F}_{q^3} \simeq \mathbb{F}_q[X]/(\chi(X))$. Select $\alpha \in (\mathbb{F}_{q^3})^*$ such that it is a generator of $(\mathbb{F}_{q^3})^*$.

4. Compute the coordinates of $\alpha$ seen as a vector over $\mathbb{F}_q$, which will be denoted as $(\alpha_1, \alpha_2, \alpha_3) \in (\mathbb{F}_q)^3 \setminus \{0, 0, 0\}$.
5. Under the canonical projection \( \pi: (F_q)^3 \setminus \{0,0,0\} \to F_qP^2 \), compute \([\beta_1, \beta_2, \beta_3] = \pi(\alpha_1, \alpha_2, \alpha_3)\).

**System parameters**

Following the previous notation, the system parameters are defined by the set \( S = \{F_q, [\beta_1, \beta_2, \beta_3], c_1, c_2, c_3\} \).

**6.2 Key agreement protocol**

The key agreement follows the well-known Diffie-Hellman paradigm. Any two users \( A, B \), willing to agree on a common value, which remains secret, set up a system and agree on its parameters, as stated previously.

The protocol runs as follows:

1. User \( A \) selects \( n_A \in \mathbb{Z}_\ell \), with \( \ell = q^2 + q + 1 \), computes
   \[ [\gamma_1^A, \gamma_2^A, \gamma_3^A] = \oplus^{n_A}[\beta_1, \beta_2, \beta_3] \in F_qP^2 \]
   and sends it to user \( B \).

2. User \( B \) selects \( n_B \in \mathbb{Z}_\ell \), computes
   \[ [\gamma_1^B, \gamma_2^B, \gamma_3^B] = \oplus^{n_B}[\beta_1, \beta_2, \beta_3] \in F_qP^2 \]
   and sends it to user \( A \).

3. User \( A \) computes \( k_A = \oplus^{n_A}[\gamma_1^B, \gamma_2^B, \gamma_3^B] \).

4. User \( B \) computes \( k_B = \oplus^{n_B}[\gamma_1^A, \gamma_2^A, \gamma_3^A] \).

According to the definitions, the following equalities clearly hold:

\[
k_A = \oplus^{n_A}[\gamma_1^B, \gamma_2^B, \gamma_3^B] = \oplus^{n_A} (\oplus^{n_B}[\beta_1, \beta_2, \beta_3]) = \oplus^{n_B} (\oplus^{n_A}[\beta_1, \beta_2, \beta_3]) = \oplus^{n_B}[\gamma_1^A, \gamma_2^A, \gamma_3^A] = k_B.
\]

Hence, the properties of the operation \( \oplus \) in \( G \) ensure that actually \( k_A = k_B \), which is the common value expected as the output of the protocol.

**6.3 Cost of the \( \oplus \) operation in \( G \)**

Let \( s \) and \( p \) be the number of field operations in order to perform an addition and a multiplication respectively in \( F_q \). From the formulas (4) it follows that the total number of operations for computing \( x \oplus y \) is equal to \( 10s + 15p \), once the \( 2s + 3p \) precomputations of \( c_1c_3 \), \( c_1c_2 + c_3 \), and \((c_1)^2 + c_2 \) are assumed.

Additionally, two multiplications and one inversion are needed to eventually project the resulting point back to \( F_qP^2 \). However, in a typical setting their cost can be neglected when compared with the relatively much larger number of sums that are to be carried out.
6.4 A toy example

If we take the prime field $\mathbb{F}_p$, with $p = 131$, it is case that $p^2 + p + 1 = 17293$ is also prime. Accordingly, the group $\mathbb{G}$ is cyclic. We set the parameters $c_1 = 13$, $c_2 = 18$, $c_3 = 73$, since the polynomial $\chi(X) = X^3 - 13X^2 - 18X - 73$ is irreducible in $\mathbb{F}_{131}$.

Let us take the projective point $X = [126, 16, 1]$ as a generator of $\mathbb{G}$. If we select now another projective point $Y = [86, 120, 1]$, we find by exhaustive search the integer $n$ such that $Y = \oplus^n X$:

\[
[126, 16, 1] \rightarrow [117, 130, 1] \rightarrow [11, 15, 1] \rightarrow [71, 56, 1] \rightarrow [16, 98, 1] \\
\rightarrow [72, 62, 1] \rightarrow [111, 125, 1] \rightarrow [110, 130, 1] \rightarrow [130, 114, 1] \rightarrow [86, 120, 1].
\]

Since the operation has been iterated ten times, we conclude $Y = \oplus^{10} X$ for this particular pair, so that $\log_X Y = 10$.

6.5 Experimental results

We have conducted several experiments in order to assess the computation time of the $\oplus$ operation in $\mathbb{G}$. The basic setup consists in selecting prime fields, $\mathbb{F}_p$, such that $p$ has increasing bit lengths. For each particular bit length, we repeat the operation a number of times and take the mean computation time value.

In order to compare computation times, we repeated the same experiment for the point addition in elliptic curves over $\mathbb{F}_p$, using the same range of bit lengths. Choosing the point addition operation in elliptic curves as the term of comparison with the $\oplus$ operation seems sensible since both operations share a relatively large number of basic operations (namely, additions, multiplications and inversions) in the ground field. In particular, we used projective coordinates according to the formulas given in [4, §13.2.1.b].

We implemented the experiments using Java SE Runtime Environment version 1.8.0_171-b11 and the execution was carried out on an Intel Core i7-4790 platform running at 3.60 GHz. We performed the experiment in the range 32–512 bits in steps of 32 bits. The experiments yielded the results shown in Table 1, where for each bit length we give the average computation time of one operation measured in microseconds.

A graph of the combined results for both the $\oplus$ operation in $\mathbb{G}$ and for point addition in elliptic curves over $\mathbb{F}_p$ is shown in Figure 1. The $x$-axis represents each bit-length step and the $y$-axis show the mean computation time for one operation, both taken from Table 1.

Since elliptic curve logarithm needs twice as many bits as the logarithm in $\mathbb{G}$ to provide an equivalent security level, we present in Figure 2 the comparison between computation times for equivalent bit lengths.

The following is remarkable:

- The computation times shown in Figure 1 for both settings show a essentially linear growth.
- Though the point addition is slightly slower than the $\oplus$ operation in $\mathbb{G}$, they keep a rather constant ratio between them, which is roughly equal to 0.7.
Observing Figure 2, it is apparent that the $\oplus$ operation is much faster than its counterpart in elliptic curves of an equivalent security level. For example, when using 256 bits in $\mathbb{G}$, equivalent to 512 bit in elliptic curves, the $\oplus$ operation is roughly 2.9 times as fast as the sum of points in the equivalent elliptic curve (see Table 1).

Acknowledgments: This research has been partially supported by Ministerio de Economía, Industria y Competitividad (MINECO), Agencia Estatal de Investigación (AEI), and Fondo Europeo de Desarrollo Regional (FEDER, UE) under project COPCIS, reference TIN2017-84844-C2-1-R, and by Comunidad de Madrid (Spain) under project reference S2013/ICE-3095-CIBERDINE-CM, also co-funded by European Union FEDER funds.

References

[1] G. Adj, A. Menezes, T. Oliveira, F. Rodríguez-Henríquez. Computing discrete logarithms using Joux’s algorithm. ACM Comm. Computer Algebra 49 (2): 60 (2015).

[2] R. Barbulescu, P. Gaudry, A. Guillevic, F. Morain. New record in $\mathbb{F}_{p^n}$, Cattel Workshop, École Polytechnique, October 2015, URL: https://webusers.imj-prg.fr/~razvan.barbuau/p3dd52.pdf

[3] R. Barbulescu, P. Gaudry, A. Joux, E. Thomé. A heuristic quasi-polynomial algorithm for discrete logarithm in finite fields of small characteristic. Advances in Cryptology-EUROCRYPT 2014, Lecture Notes in Comput. Sci., 8441, 1–16 (2014).

[4] H. Cohen, G. Frey, R. Avanzi, C. Doche, T. Lange, K. Nguyen, F. Vercauteren. Handbook of Elliptic and Hyperelliptic Curve Cryptography. Chapman and Hall/CRC, Taylor & Francis Group, New York, USA, 2005.

[5] A. Cossidente, M.J. de Resmini. Remarks on Singer cyclic groups and their normalizers. Des. Codes Cryptogr. 32: 97–112 (2004).

[6] S. R. Ghorpade, S. U. Hasan, M. Kumari. Primitive polynomials, Singer cycles and word-oriented linear feedback shift registers. Des. Codes Cryptogr. 58: 123–134 (2011).

[7] R. Granger, T. Kleinjung, J. Zumbrägel. Indiscreet logarithms in finite fields of small characteristic. arXiv:1604.03837v1 [math.NT].

[8] R. Granger, T. Kleinjung, J. Zumbrägel. On the discrete logarithm problem in finite fields of fixed characteristic. arXiv:1507.01495v2 [math.NT].

[9] K. Hayasaka, K.Aoki, T. Kobayashi, T. Takagi. A construction of 3-dimensional lattice sieve for number field sieve over $GF(p^n)$. Cryptology ePrint Archive, 2015/1179 (2015).

[10] A. Joux, A. Odlyzko, C. Pierrot. The past, evolving present, and future of the discrete logarithm. Open problems in mathematics and computational science, 5–36 (2014).
[11] A. Joux, C. Pierrot. Technical history of discrete logarithms in small characteristic finite fields: The road from subexponential to quasi-polynomial complexity. Des. Codes Cryptogr. 78 (1): 73–85 (2016).

[12] T. Kleinjung, C. Diem, A. K. Lenstra, C. Priplata, C. Stahlke. Computation of a 768-Bit Prime Field Discrete Logarithm, Advances in Cryptology-EUROCRYPT 2017, Lecture Notes in Comput. Sci., 10210, 185–201 (2017).

[13] N. Koblitz, A. J. Menezes. Another look at “Provable Security”. J. Cryptology 20: 3–37 (2007).

[14] A. J. Menezes. Elliptic Curve Public Key Cryptosystems. The Kluwer International Series in Engineering and Computer Science, 234. Communications and Information Theory. Kluwer Academic Publishers, Boston, MA, 1993.

[15] A. M. Odlyzko. Discrete logarithms in finite fields and their cryptographic significance. Advances in Cryptology-EUROCRYPT 1984, Lecture Notes in Comput. Sci., 209, 224–314 (1985).

[16] C. H. Papadimitriou. Computational complexity. Addison-Wesley Publishing Company, Reading, MA, 1994.

[17] O. Schirokauer. The impact of the number field sieve on the discrete logarithm problem in finite fields. Algorithmic Number Theory 44: 397–420 (2008).

[18] J. Singer. A theorem in finite projective geometry and some applications to number theory. Trans. Amer. Math. Soc. 43 (3): 377–385 (1938).

| Bit length | Operation $\oplus$ in $G$ (µs) | Point addition in elliptic curves (µs) |
|------------|---------------------------------|-------------------------------------|
| 32         | 1.10396044                      | 1.07039673                          |
| 64         | 1.68166612                      | 1.97707724                          |
| 96         | 1.97807208                      | 2.55200463                          |
| 128        | 2.19050201                      | 2.86859637                          |
| 160        | 2.52811554                      | 3.35108746                          |
| 192        | 2.77264771                      | 3.72361810                          |
| 224        | 3.15689638                      | 4.29066712                          |
| 256        | 3.36514379                      | 4.65996446                          |
| 288        | 3.77635547                      | 5.34568703                          |
| 320        | 4.11391404                      | 5.84153419                          |
| 352        | 4.60391914                      | 6.33152050                          |
| 384        | 4.86727126                      | 6.97227992                          |
| 416        | 5.41088866                      | 7.75588654                          |
| 448        | 5.77817335                      | 8.32544612                          |
| 480        | 6.31956718                      | 9.02521134                          |
| 512        | 6.70272949                      | 9.61432718                          |

Table 1: Computation time for one single operation in each setting
Figure 1: Comparison of average computation times for both settings

Figure 2: Comparison of computation times for equivalent security level