mathematics

MDPI

Article

A Group Law on the Projective Plane with Applications in Public Key Cryptography †

Raúl Durán Díaz [1,*], Luis Hernández Encinas [2,*] and Jaime Muñoz Masqué [2]

[1] Departamento de Automática, Universidad de Alcalá, E-28871 Alcalá de Henares, Spain
[2] Instituto de Tecnologías Físicas y de la Información (ITEFI) Consejo Superior de Investigaciones Científicas (CSIC), E-28006 Madrid, Spain; jaime@iec.csic.es
* Correspondence: raul.duran@uah.es (R.D.D.); luis@iec.csic.es (L.H.E.)
† A preliminary version of this manuscript can be found at arXiv.org under the URL: https://arxiv.org/abs/1802.00246.

Received: 25 March 2020; Accepted: 2 May 2020; Published: 7 May 2020

Abstract: In the context of new threats to Public Key Cryptography arising from a growing computational power both in classic and in quantum worlds, we present a new group law defined on a subset of the projective plane $\mathbb{F}P^2$ over an arbitrary field $\mathbb{F}$, which lends itself to applications in Public Key Cryptography and turns out to be more efficient in terms of computational resources. In particular, we give explicitly the number of base field operations needed to perform the mentioned group law. Based on it, we present a Diffie-Hellman-like key agreement protocol. We analyze the computational difficulty of solving the mathematical problem underlying the proposed Abelian group law and we prove that the security of our proposal is equivalent to the discrete logarithm problem in the multiplicative group of the cubic extension of the finite field considered. We present an experimental setup in order to show real computation times along a comparison with the group operation in the group of points of an elliptic curve. Based on current state-of-the-art algorithms, we provide parameter ranges suitable for real world applications. Finally, we present a promising variant of the proposed group law, by moving from the base field $\mathbb{F}$ to the ring $\mathbb{Z}/pq\mathbb{Z}$, and we explain how the security becomes enhanced, though at the cost of a longer key length.

Keywords: abelian group law; discrete logarithm problem; norm of an extension; projective cubic curve

MSC: Primary 20K01; Secondary 12F05; 14H50; 15A04; 68Q25; 94A60

1. Introduction and Related Work

Neal Koblitz [1] and Victor Miller [2] presented independently but simultaneously proposals that made use of the multiplicative group of a finite field in order to implement certain asymmetric cryptosystems. Koblitz presented an implementation of Diffie-Hellman key-agreement protocol [3] based on the use of elliptic curves. On his part, Miller offered a proposal more on the theoretical side, avoiding comparisons with existing implementations. In all those cases, the security is based on the infeasibility of the discrete logarithm problem over elliptic curves (ECDLP), which is to this day considered as difficult as the integer factorization problem (IFP), upon which RSA [4] cryptosystem is based, or the discrete logarithm problem (DLP) employed in ElGamal cryptosystem [5].

Diffie-Hellman key-agreement protocol for elliptic curves (ECDH) consists essentially in mapping the operations customarily carried out in the multiplicative group $\mathbb{Z}_p^*$ to the set of points of an elliptic curve, endowed with an additive group operation. However, this protocol painfully succumbs in the face of a plain man-in-the-middle attack and, for this reason, Menezes, Qu, and Vanstone

proposed [6] an authenticated variant, known as Elliptic Curve Menezes-Qu-Vanstone key agreement protocol (ECMQV). In general, the outcome of these key-agreement protocols is that the users eventually share a value—the key or a seed to derive the key—which was initially unknown for any of them, and cannot be inferred (more precisely: It is computationally infeasible to infer it) from the information exchanged between the parties.

Along with these key-agreement protocols, several elliptic-curve-based asymmetric cryptosystems have seen the light in these last years. The first proposals of the so-called elliptic-curve cryptosystems (ECC) were revisions adapted from existing systems, such as ElGamal's [5], or Massey-Omura's [7]. They were publicized by Koblitz in [1].

The problem with the elliptic-curve version of ElGamal's and Massey-Omura's cryptosystems is that the user needs to map each possible message to a point of the curve. This fact is an important drawback since, on the one hand, the cardinal of the curve points is finite, so the user is limited to a finite number of possible messages; and, on the other hand, the user needs some kind of "equivalence table" between messages and points in order to cipher and decipher. Therefore, these cryptosystems are limited in practice to those settings in which the set of possible messages is fixed in advance.

In order to overcome these limitations, Menezes and Vanstone proposed in [8] the Elliptic Curve Menezes-Vanstone cryptosystem (ECMV) for elliptic curves over finite fields $\mathbb{F}_q$. In ECMV, each message is represented by elements of the Cartesian product $\mathbb{F}_q^* \times \mathbb{F}_q^*$, not necessarily points of the elliptic curve. The protocol includes a systematic procedure to divide any message into blocks and to codify each block as an element of the Cartesian product. The downside is that ciphertext length depends entirely on plaintext length.

In spite of the efforts, ECC has abandoned the battlefield of cryptosystems in favor of key-agreement protocols as a building block for hybrid cryptosystems. In the latter, ECC permits the users to share a session (ephemeral) key, whence a symmetric key is derived to be used together with a symmetric cryptosystem, such as AES.

In this setting, Mihir Bellare and Philip Rogaway [9] published in 1997 the Discrete Logarithm Augmented Encryption Scheme (DLAES). Along with Michel Abdalla, the system was improved in 1998 by the same authors, and renamed as DHAES (Diffie-Hellman Augmented Encryption Scheme) [10]. Eventually renamed to DHIES (Diffie-Hellman Integrated Encryption Scheme) [11,12], it is an improved extension of ElGamal's cryptosystem [5]. DHIES is really a complex protocol, much more involved than ElGamal or Koblitz's proposal in [1], which includes public key operations, symmetric ciphering, authentication and hash function computation. While ElGamal and Koblitz directly ciphered a message, without any further use of other necessary elements for a proper integrated scheme, DHIES provides security against chosen ciphertext attacks at no extra cost in terms of number of operations or key lengths [11]. Together with other proposals, DHIES was employed in the preparation of standards [13,14].

Finally, it is worth mentioning the so-called ECIES (Elliptic Curve Integrated Encryption Scheme), which embraces several integrated ciphering schemes using DHIES-based elliptic curves and it is described in the relevant security standards, such as [13–15] (a comparison among different ECIES implementations may be found in [16]). Remark that, whenever ECIES is recommended (even with minor differences regarding implementations), it is to be used in a hybrid setting, where a (DH-type) session key agreement protocol is a must.

Setting aside the already mentioned cryptosystems and key-agreement protocols, it is probably in digital signature schemes that elliptic curve cryptography is mostly demanded. The ElGamal-based Elliptic Curve Digital Signature Algorithm (ECDSA) is analogous to the Digital Signature Algorithm (DSA) [17], using additive rather than multiplicative notation. ECDSA has consolidated into an internationally accepted standard [13,18].

When dealing with ECC, one of the most important aspects to keep in mind is the processes of curve generation and selection. Several standards tackle such methods and show examples of curve selection as part of the public-key generation process. Among them, it is worth mentioning X9.63 [13],

IEEE 1363 [19], and FIPS 186-4 [20], issued by the National Institute of Standards and Technology (NIST) of the USA. However, in practice, such standards lack precision and clarity when it comes to selecting seeds for random generation, or prime numbers, thus limiting the ability of serving really practical purposes.

For these reasons, several initiatives have ripened, such as Brainpool [21], considered to be the first international proposal to provide clear and transparent procedures in order to generate the parameters of elliptic curves for cryptographic purposes. Under the Brainpool initiative, several elliptic curves, presented in reduced Weierstrass format, have been considered safe beyond any doubt by many experts.

Later on, researchers Daniel Bernstein and Tania Lange [22] reviewed the elliptic curve generation procedures, including those in Brainpool. In particular, they scrutinized 20 curves from several sources under a number of security requirements that they considered a must. The result was that just only Edwards and Montgomery curves [23] satisfied those requirements. In view of this outcome, the experts decided to propose a new set of curves, known as *SafeCurves* that really met the set of safety requirements [22]. Moreover, Baignères [24] proposed a new Edwards elliptic curve (the so-called *million dollar curve*) by means of a new technique that insists in the randomness of the input parameters to the generation process.

In spite of those efforts, the currently most deployed elliptic curves, both in hardware and software implementations, are those presented in the reduced Weierstrass format, whereas Edwards or Montgomery curves are seldom used, maybe because the additional security provided by them is not worth their lower computation efficiency (multiplications with scalars). A performance comparison among the three types of curves cited above can be found in [25]. In the latter, the authors resorted to the examples provided by the initiative *SafeCurves*, together with a Java implementation developed by them.

Koyama et al. proposed in [26] the use of elliptic curves over the ring $\mathbb{Z}_n$, where n is an odd composite square-free integer. In particular, n is the product of two large primes, as in the RSA cryptosystem. The security of the cryptosystem of Koyama et al.'s is based upon IFP, though the authors did not prove whether solving the IFP was equivalent to breaking their cryptosystem. Later on, Meyer and Müller proved in [27] that breaking a modified version of Koyama's cryptosystem was indeed equivalent to factorizing n. In addition, they proposed a digital signature scheme based on elliptic curves defined over $\mathbb{Z}_n$.

Another interesting question is the ever growing necessity of implementing elliptic curve cryptography on ubiquitous portable devices (smartphones, smart cards, pen-drives, and the like), which gives rise to new challenges. Actually, these devices normally present severe limitations regarding storage capacity or processing power, as compared with ordinary desktop computers. Elliptic curve cryptography is amenable to these devices since key sizes are much smaller than in other cryptosystems (for example, RSA) for similar security levels.

It is very common nowadays to find elliptic curve cryptography on such devices, and hence implementations of multiplication operations. These operations, in turn, are threatened by the ever more powerful side channel and fault injection attacks. For example, Reference [28] documents recent developments on those side channel attacks to ECC implementations. It is completely necessary to implement the multiplication algorithms in such a way that they do not leak any information to possible attackers. Reference [29] describes some options to avoid such attacks when implementing scalar multiplications for elliptic curves.

It is also very well known that the advent of a universal quantum computer with sufficient computation power could break the most commonly used asymmetric cryptosystems. In fact, Shor's algorithm [30], proposed in 1997, is known to solve IFP and DLP (or ECDLP) in polynomial time if such quantum computer does exist; however, there is no agreement as to how many qubits would be required to execute Shor's or other quantum algorithms, but some estimations point to a number of qubits several orders of magnitude larger than the number of qubits available in currently existing

quantum computers [31]. Should such number of qubits be available, IFP or DLP could be solved in a bunch of hours. For example, a personal computer needs, roughly speaking, $\mathcal{O}\left(2^{\sqrt[3]{\log n}}\right)$ bit operations to factor a number n, whereas a quantum computer executing Shor's algorithm could perform such factorization with only $\mathcal{O}\left(\log^3 n\right)$ bit operations and using $\mathcal{O}(\log n)$ bit storage.

Though it seems that a quantum computer with the required computation power will not be available any time soon, the new source of attacks coming from quantum world and the need to ensure that the information protected by current asymmetric systems continues to be accessible forced the NIST to launch an international call [32] for new cryptographic algorithms resilient to the power leveraged by quantum computation: the so-called quantum-resistant algorithms. These are expected to cover at least proposals for new asymmetric encryption schemes, digital signature schemes, and key encapsulation mechanisms (KEM). The main quantum-resistant proposals include difficult problems stemming from coding theory, lattices, hash functions, and isogenies over elliptic curves, to mention just a few. In January 2019, the NIST published the list of submitted algorithms that have passed on to the second round of the call [33]. Among them, there stands the proposal SIKE as a key encapsulation mechanism that is based on isogenies over elliptic curves.

The previous paragraphs summarize the current state of affairs regarding classic and quantum cryptography and make it clear that there is much to be done in both classic and quantum worlds. Taking that current context into account, this work presents a new group law defined on a subset of the projective plane $\mathbb{F}P^2$ over an arbitrary field $\mathbb{F}$, which lends itself to applications in public key cryptography. Apart from the mathematical novelty implied, this new group law presents several features worth public key cryptosystems, such as:

- a Diffie-Hellman-like key agreement, since such protocol remains a basic piece for any hybrid cryptosystem, as commented above.
- an extension to the ring $\mathbb{Z}_{pq}$ providing enhanced security, following the same vein as the one followed by [26,27].
- no side channel attacks known to date, given the recentness of this proposal and due to the particular group law defined.
- gives rise to new research lines, such as defining isogenies over the group structure, thus opening the path to a possibly new quantum-resistant problem.

In a nutshell, the main contribution of this paper is to propose a new group law, defined on the complement of a projective cubic plane curve, prove its properties, and consider the possibility of using it as a building block for cryptographic applications in the field of Public Key Cryptography (PKC).

The paper is organized as follows: Section 2 presents the group law and its main characteristics and properties. In particular, we define the mathematical problem associated with the considered group law, and we give the explicit formulas to compute the group operation of any two elements of the group. These formulas, which involve coefficients from the base field, are applicable to any pair of elements of the group with no exception whatsoever, which is advantageous in view of possible cryptographic applications, since this feature helps, for example, to withstand side channel attacks.

As an application of the defined group law to PKC, a cryptographic protocol, in particular, a Diffie-Hellman-like key agreement protocol, is defined in Section 3. We also analyze the computational difficulty of solving the mathematical problem underlying the defined group law, and we prove that the hardness of our problem is equivalent to that of the discrete logarithm problem on the multiplicative group of the cubic extension of the finite field considered.

In Section 4, we consider an entirely analogous system, but shifting the general base field to the ring $\mathbb{Z}/pq\mathbb{Z}$. We make it clear that this last proposal enhances the security of the system, since it now depends not only on DLP but also on the factorization problem, though at the price of doubling the key length.

The last section is devoted to the conclusions.

2. The Group Law Defined

Our purpose in this section is to search for a particular (finite) group endowed with an internal operation that makes it cyclic provided that certain conditions hold. In the latter case, we define yet another (discrete) logarithm operation, which, if found to be difficult to carry out, may give rise to cryptographic applications.

We will work with three-dimensional vector spaces and their associated two-dimensional projective spaces, defined over finite fields. We will consider certain cubic curve defined over this ambient projective space, so that the set over which we will define our new group operation is precisely the set of points of the projective space that do not belong to that cubic curve.

We will show the conditions under which the cubic curve has no points in the projective space, which means that the group embraces the the full projective space. We will provide the explicit formulas to compute the group law in the base field and the good piece of news is that these formulas are the same for any of the elements in the group, a feature much cherished in cryptographic settings.

Let $\mathbb{F}$ be a field and let us consider a linear endomorphism $A\colon V \to V$ of the vector space $V = \mathbb{F}^3$. We define the polynomial $Q(\mathbf{x}) = \det(x_1 I + x_2 A + x_3 A^2)$, where $\mathbf{x} = (x_1, x_2, x_3) \in V$. The polynomial Q is homogeneous of degree 3, and does not depend on A, but only on the characteristic polynomial $\chi(X)$ of A.

A new group law is proposed $\oplus\colon V \times V \to V$. Let the multiplicative group $\mathbb{F}^*$ act on V by the diagonal action, i.e., $\lambda \cdot (x_1, x_2, x_3) = (\lambda x_1, \lambda x_2, \lambda x_3)$, and let $\mathbb{F}P^2$ denote the projective plane, namely $\mathbb{F}P^2 = (V \setminus \{(0,0,0)\})/\mathbb{F}^*$. Then, the proposed group law induces an Abelian group law on $\mathbb{F}P^2 \setminus Q^{-1}(0)$.

If the characteristic polynomial $\chi(X)$ is irreducible in $\mathbb{F}[X]$, then $Q^{-1}(0) = \{(0,0,0)\}$, and therefore the group law extends to the whole projective plane $\mathbb{F}P^2$; moreover, if the base field is a finite field $\mathbb{F}_q$, with characteristic different from 2 or 3, then the group $\mathbb{G} = (\mathbb{F}_q P^2, \oplus)$ is proved to be cyclic.

The latter property permits us to apply the notion of discrete logarithm to the group $\mathbb{G}$. If we fix a generator $g \in \mathbb{F}_q P^2$, then any element h of the group is the addition of g with itself a finite number of times, say n, so that $h = g \oplus g \oplus \overset{(n)}{\cdots} \oplus g = [n]g$. 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 (DLP) consists of 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 $(\mathbb{F}_{q^3})^*$.

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 present proposal agree to a single base field $\mathbb{F}_q$ and an (irreducible) polynomial:

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

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

Next, we prove that the polynomial Q does not depend on A, but only on the characteristic polynomial $\chi(X)$ of A.

Lemma 1. *Let $\mathbb{F}$ be a field and let V be the vector space $\mathbb{F}^3$. If $A\colon V \to V$ is a linear map such that the endomorphisms I, A, A^2 are linearly independent, then the homogeneous cubic polynomial $Q(\mathbf{x}) = \det(x_1 I + x_2 A + x_3 A^2)$ does not depend on the matrix A but only on the coefficients c_1, c_2, c_3 of its characteristic polynomial $\chi(X) = X^3 - c_1 X^2 - c_2 X - c_3$.*

Proof. Let $\bar{\mathbb{F}}$ 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 $\bar{\mathbb{F}}^3$ such that the matrix of A in this basis equals one of the following three matrices:

$$M_1 = \begin{pmatrix} \alpha_1 & 0 & 0 \\ 0 & \alpha_2 & 0 \\ 0 & 0 & \alpha_3 \end{pmatrix}, M_2 = \begin{pmatrix} \alpha_1 & 0 & 0 \\ 0 & \alpha_2 & 0 \\ 0 & 1 & \alpha_2 \end{pmatrix}, M_3 = \begin{pmatrix} \alpha_1 & 0 & 0 \\ 1 & \alpha_1 & 0 \\ 0 & 1 & \alpha_1 \end{pmatrix}, \tag{1}$$

and, from a simple calculation, we obtain

$$\begin{array}{rcl} Q(\mathbf{x}) & = & \det(x_1 I + x_2 M_i + x_3 (M_i)^2) \\ & = & -c_2 x_1 (x_2)^2 + \left[(c_2)^2 - 2(c_1 c_3)\right] x_1 (x_3)^2 + c_1 (x_1)^2 x_2 \\ & & + \left[(c_1)^2 + 2c_2\right] (x_1)^2 x_3 - (c_2 c_3) x_2 (x_3)^2 + (c_1 c_3)(x_2)^2 x_3 \\ & & - (c_1 c_2 + 3c_3)\, x_1 x_2 x_3 + (x_1)^3 + c_3 (x_2)^3 + (c_3)^2 (x_3)^3, \end{array} \tag{2}$$

for every $i = 1, 2, 3$. □

Theorem 1. *Every linear map $A\colon V \to V$ such that the endomorphisms I, A, A^2 are linearly independent, induces a law of composition*

$$\begin{array}{c} \oplus\colon V \times V \to V, \\ (\mathbf{x}, \mathbf{y}) \mapsto \mathbf{z} = \mathbf{x} \oplus \mathbf{y}, \end{array}$$

by the following formula:

$$z_1 I + z_2 A + z_3 A^2 = \left(x_1 I + x_2 A + x_3 A^2\right)\left(y_1 I + y_2 A + y_3 A^2\right), \tag{3}$$

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

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

$$\oplus\colon (\mathbb{F}^3 \setminus Q^{-1}(0)) \times (\mathbb{F}^3 \setminus Q^{-1}(0)) \to (\mathbb{F}^3 \setminus Q^{-1}(0)).$$

If C denotes the projective cubic curve defined by $Q(\mathbf{x}) = 0$, then the group law $\oplus$ also induces a group law

$$\oplus\colon (\mathbb{F}P^2 \setminus C) \times (\mathbb{F}P^2 \setminus C) \to \mathbb{F}P^2 \setminus C.$$

Proof. As $A^3 = c_1 A^2 + c_2 A + c_3 I$, and

$$\begin{array}{rcl} A^2 \cdot A^2 & = & A \cdot A^3 \\ & & = (c_1 c_3)\, I + (c_1 c_2 + c_3)\, A + \left[(c_1)^2 + c_2\right] A^2, \end{array}$$

from the formula in (3), it follows:

$$\begin{array}{rcl} z_1 = & x_1 y_1 + c_3 (x_2 y_3 + x_3 y_2) + (c_1 c_3)\, x_3 y_3, \\ z_2 = & x_1 y_2 + x_2 y_1 + c_2 (x_2 y_3 + x_3 y_2) + (c_1 c_2 + c_3)\, x_3 y_3, \\ z_3 = & x_2 y_2 + x_1 y_3 + x_3 y_1 + c_1 (x_2 y_3 + x_3 y_2) + \left((c_1)^2 + c_2\right) x_3 y_3. \end{array} \tag{4}$$

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 $Q(\mathbf{x})$, where Q is defined by the formula (2). Hence, $\mathbf{x} \oplus \mathbf{y} = (0,0,0)$, for some $\mathbf{y}$ in $V \setminus \{(0,0,0)\}$, if and only if $Q(\mathbf{x}) = 0$.

The commutativity of $\oplus$ is a direct consequence of the invariance of the formula (4) under the substitutions $x_i \mapsto y_i$, $y_i \mapsto x_i$, $1 \leq i \leq 3$.

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

$$(\mathbf{x} \oplus \mathbf{y})_1 I + (\mathbf{x} \oplus \mathbf{y})_2 A + (\mathbf{x} \oplus \mathbf{y})_3 A^2 = \left(x_1 I + x_2 A + x_3 A^2\right)\left(y_1 I + y_2 A + y_3 A^2\right).$$

From the associativity of the composition law of endomorphisms, we deduce

$$\begin{aligned}
&(\mathbf{x} \oplus (\mathbf{y} \oplus \mathbf{z}))_1 I + (\mathbf{x} \oplus (\mathbf{y} \oplus \mathbf{z}))_2 A + (\mathbf{x} \oplus (\mathbf{y} \oplus \mathbf{z}))_3 A^2 \\
&= \left(x_1 I + x_2 A + x_3 A^2\right) \cdot \left(\left(y_1 I + y_2 A + y_3 A^2\right) \cdot \left(z_1 I + z_2 A + z_3 A^2\right)\right) \\
&= \left(\left(x_1 I + x_2 A + x_3 A^2\right) \cdot \left(y_1 I + y_2 A + y_3 A^2\right)\right) \cdot \left(z_1 I + z_2 A + z_3 A^2\right) \\
&= ((\mathbf{x} \oplus \mathbf{y}) \oplus \mathbf{z})_1 I + ((\mathbf{x} \oplus \mathbf{y}) \oplus \mathbf{z})_2 A + ((\mathbf{x} \oplus \mathbf{y}) \oplus \mathbf{z})_3 A^2.
\end{aligned}$$

Hence, $\mathbf{x} \oplus (\mathbf{y} \oplus \mathbf{z}) = (\mathbf{x} \oplus \mathbf{y}) \oplus \mathbf{z}$, $\forall \mathbf{x}, \mathbf{y}, \mathbf{z} \in V$.

From Equation (4), it follows that the unit element is the point $(1,0,0)$, which does not belong to $Q^{-1}(0)$ since $Q(1,0,0) = 1$.

By taking determinants in Equation (3), we obtain

$$Q(\mathbf{x} \oplus \mathbf{y}) = \quad Q(\mathbf{x})Q(\mathbf{y}), \quad \forall \mathbf{x}, \mathbf{y} \in V.$$

Therefore, the opposite element $\mathbf{y}$ of $\mathbf{x}$ exists and it is given by the following formulas:

$$\begin{aligned}
y_1 &= \tfrac{1}{Q(\mathbf{x})}\left(c_1 x_1 x_2 + \left[(c_1)^2 + 2c_2\right] x_1 x_3 - (c_3 + c_1 c_2)\, x_2 x_3 + (x_1)^2 - c_2 (x_2)^2 + \left[(c_2)^2 - c_1 c_3\right] (x_3)^2\right), \\
y_2 &= \tfrac{-1}{Q(\mathbf{x})}\left(x_1 x_2 + (c_1)^2 x_2 x_3 + c_1 (x_2)^2 - (c_1 c_2 + c_3)\, (x_3)^2\right), \\
y_3 &= \tfrac{1}{Q(\mathbf{x})}\left(-x_1 x_3 + c_1 x_2 x_3 + (x_2)^2 - c_2 (x_3)^2\right).
\end{aligned}$$

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

Remark 1. *Note that the Equations* (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. *If* $\mathbf{v}_1 = (1,0,0)$, $\mathbf{v}_2 = (0,1,0)$, $\mathbf{v}_3 = (0,0,1)$*, then, from Equation* (2)*, we obtain* $Q(\mathbf{v}_2) = c_3$, $Q(\mathbf{v}_3) = (c_3)^2$*. Hence,* $\mathbf{v}_2$ *and* $\mathbf{v}_3$ *belong to* $\mathbb{F}^3 \setminus Q^{-1}(0)$ *if and only if* $c_3 \neq 0$*, i.e., when* A *is invertible.*

2.1. The Basic Cubic

Proposition 1. *Let* $\chi(X) = X^3 - c_1 X^2 - c_2 X - c_3 \in \mathbb{F}[X]$ *be the polynomial introduced in* Lemma 1 *and let* $\alpha = X \bmod \chi$*. If* $N\colon \mathbb{F}[\alpha] \to \mathbb{F}$ *is the norm of the extension* $\mathbb{F}[\alpha]$ *of* $\mathbb{F}$*, then a point* $\beta = \beta_0 + \beta_1\alpha + \beta_2\alpha^2$ *belongs to the cubic curve* C *defined in* Theorem 1 *if and only if* $N(\beta) = 0$*. In particular, if* χ *is irreducible in* $\mathbb{F}[X]$*, then* C *has no point in* $\mathbb{F}P^2$*.*

Proof. Every $\beta \in \mathbb{F}[\alpha]$ induces an $\mathbb{F}$-linear endomorphism $E_\beta\colon \mathbb{F}[\alpha] \to \mathbb{F}[\alpha]$ given by $E_\beta(\xi) = \beta \cdot \xi$, $\forall \xi \in \mathbb{F}[\alpha]$, and, from the very definition of the norm, we have $N(\beta) = \det E_\beta$. As a computation shows, we obtain $N(\beta) = Q(\beta_0, \beta_1, \beta_2)$, thus proving the first part of the statement.

Moreover, χ is irreducible if and only if $\mathbb{F}[\alpha]$ is a field, and then the only element with norm 0 is in fact $\mathbf{0} \in \mathbb{F}[\alpha]$. To see this, assume on the contrary that $N(\mathbf{x}) = 0$, with $\mathbf{x} \neq \mathbf{0}$ and $\mathbf{x} \in \mathbb{F}[\alpha]$. Since the norm is a group homomorphism, we can write

$$1 = N(\mathbf{1}) = N(\mathbf{x} \cdot \mathbf{x}^{-1}) = N(\mathbf{x}) \cdot N(\mathbf{x}^{-1}) = 0 \cdot N(\mathbf{x}^{-1}) = 0,$$

which is a contradiction. Consequently, the curve C has no point in $\mathbb{F}P^2$. □

Corollary 1. *The polynomial χ is irreducible in $\mathbb{F}[X]$ if and only if the cubic C is irreducible.*

Proof. Actually, if χ 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

$$Q(\mathbf{x}) = [(x_1)^2 + (k^2 - 2l)x_1x_3 + l(x_2)^2 - klx_2x_3 + l^2(x_3)^2 - kx_1x_2][x_1 + hx_2 + h^2x_3].$$

Conversely, if χ is irreducible in $\mathbb{F}[X]$, then, according to the second part of Proposition 1, the only solution to the cubic equation $Q(\mathbf{x}) = 0$ is $\mathbf{x} = \mathbf{0}$. Hence, Q must be irreducible, as a reducible cubic admits non-trivial solutions in the ground field. □

Corollary 2. *If the characteristic polynomial χ of A is irreducible in $\mathbb{F}[X]$, then there is no linear transformation $(\lambda_{ij})_{i,j=1}^3 \in GL(\mathbb{F}, 3)$ reducing the polynomial Q defined in (2) to Weierstrass form.*

Proof. Replacing x_j by $X_j = \sum_{i=1}^3 \lambda_{ij}x_i$, $1 \leq j \leq 3$, in (2), we obtain a cubic $\bar{Q}$, which is in Weierstrass form (see [34] [§2.1]) if and only if the coefficients a, b, and c of the terms $(x_3)^3$, $(x_1)^2x_2$, and $x_1(x_2)^2$, respectively, vanish. As a computation shows, we have $a = \bar{Q}(\lambda_{31}, \lambda_{32}, \lambda_{33})$, and we can conclude by applying Proposition 1. □

2.2. Cyclicity

Theorem 2. *If $\mathbb{F}_q$ is a finite field of characteristic different from 2 or 3 and the polynomial $\chi(X) = X^3 - c_1X^2 - c_2X - c_3$ introduced in* Lemma 1 *is irreducible in $\mathbb{F}_q[X]$, then the group $\mathbb{G} = (\mathbb{F}_qP^2, \oplus)$ is cyclic.*

Proof. Since $\operatorname{char} \mathbb{F}_q \neq 2, 3$, the polynomial χ 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 χ, 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 β 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 $[\beta_1, \beta_2, \beta_3] = (\beta_1, \beta_2, \beta_3) \bmod \mathbb{F}_q^*$ generates the group $\mathbb{G}$, with $\mathbb{F}_qP^2 = \left((\mathbb{F}_q)^3 \setminus \{(0,0,0)\}\right)/\mathbb{F}_q^*$. □

Remark 3. *It is important to keep in mind that the implication in Theorem 2 works only in the way in which it is worded. If one selects a generator of the group $\mathbb{G}$, 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 $\mathbb{G}$, it is convenient to pick it from the set of generators in $(\mathbb{F}_{q^3})^*$ and,* after that, *project it onto $\mathbb{F}_qP^2$.*

Remark 4. *As the order of the group* $\mathbb{G} = (\mathbb{F}_q P^2, \oplus)$ *is* $q^2 + q + 1$*, the statement of Theorem 2 means that there exists an element* $\beta \in \mathbb{G}$ *of order* $q^2 + q + 1$*. According to the proof of Theorem 2, 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 [35] [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 3.1; see also [36] [Proposition 2.1].*

Remark 5. *When the polynomial* χ *is reducible, experimental tests carried out in the prime field* $\mathbb{F}_p$ *show that the projective cubic curve C defined as* $Q(\mathbf{x}) = 0$ *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, 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* $(\mathbb{F}_p P^2 \setminus C, \oplus)$ *is still cyclic, and has the expected number of generators, namely, either* $\varphi(p^2 - 1)$ *or* $\varphi(p^2 - p)$*, respectively, where* φ *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* $(\mathbb{F}_p P^2 \setminus C, \oplus)$ *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* $(\mathbb{F}_p P^2 \setminus C, \oplus)$ *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.*

Remark 6. *Hasse's theorem states [37] [Theorem 4.1] that the number of points in an elliptic curve* $E(\mathbb{F}_q)$ *verifies that* $|\#E(\mathbb{F}_q) - (q + 1)| \leq 2\sqrt{q}$*, i.e.,* $\#E(\mathbb{F}_q) = O(q)$*. However, the projective space in our proposal has* $O(q^2)$ *points, thus rendering brute-force and known-message attacks much more difficult.*

3. A Cryptographic Protocol

We have presented the group $\mathbb{G} = (\mathbb{F}_q P^2, \oplus)$ and the conditions under which it is cyclic. In this section, we will show how this group can be profited as a basic building block for cryptographic applications, and we will assess its cryptographic security level.

We resort to current state-of-the-art algorithms deployed to attack the discrete logarithm problem. Among them, index-calculus algorithm stands out since it displays a subexponential expected running time.

Equipped with these tools, we will show how this group permits us to set up a basic, à la Diffie-Hellman, key-exchange protocol, and what cryptographic security is to be expected from it. Actually, we will present the range in which the protocol setup parameters should lie in order to achieve a certain security level.

We also provide an experimental setup that we have carried out in order to obtain computation times for the new group operation on a real setting, along with a comparison with computation times required to sum points on elliptic curves.

First of all, we establish the computational security of the mathematical problem defined over the cyclic group considered. Later on, as an example of cryptographic protocol, we present a Diffie-Hellman-like key agreement protocol.

3.1. Equivalence of DLP in $\mathbb{G}$ *and* $(\mathbb{F}_{q^3})^*$

Proposition 2. *Let* $\mathbb{F}_q$ *be a finite field of characteristic* $\neq 2$ *or* 3*. Assume the polynomial* $\chi(X) = X^3 - c_1 X^2 - c_2 X - c_3$ *in* Lemma 1 *is irreducible in* $\mathbb{F}_q[X]$*, and let* $\alpha \in \mathbb{F}_{q^3}$ *be a root of* χ*.*

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*

$$(\beta_1, \beta_2, \beta_3) = (\gamma_1, \gamma_2, \gamma_3) \oplus \overset{(n)}{\cdots} \oplus (\gamma_1, \gamma_2, \gamma_3),$$

if and only if n is a solution to the equation $\beta = \gamma^n$ *in the multiplicative group* $(\mathbb{F}_{q^3})^*$, *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* $(\mathbb{F}_{q^3})^*$.

Proof. Letting $\alpha = \alpha_1$, the statement follows from the matrix formula in the proof of Theorem 2 taking the very definition of the group law $\oplus$ by formula (3) into account. □

In the present case, Proposition 2 states the "equivalence" because the reduction of problems (see, for example, [38] [p. 5], [39] [Ch. 8]) works both ways, namely, DLP in the group $((\mathbb{F}_q)^3 \setminus \{(0,0,0)\}, \oplus)$ reduces to the DLP in $(\mathbb{F}_{q^3})^*$ and the other way around. Hence, Proposition 2 proves that the use of the group $\mathbb{G} = (\mathbb{F}_q P^2, \oplus)$ is safe for standard implementations in PKC (e.g., see [34] [§1.6]), since the security it provides is equivalent to that of DLP in $(\mathbb{F}_{q^3})^*$, as long as the caveat stated in Remark 3 is taken into account.

In terms of cryptanalysis, logarithms 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 (which reduces the computation in the whole group to the computation of the logarithm in all subgroups of prime order of $\mathbb{G}$), Shank's Baby Step/Giant Step, and Pollard's Rho algorithm. All of them need an exponential computation time.

However, there exists the so-called index-calculus algorithm, which is much faster as it is able to compute discrete logarithms in the multiplicative group of a finite field in subexponential time (see, e.g., [40]). Since the operations in the proposed group $\mathbb{G} = (\mathbb{F}_q P^2, \oplus)$ can be efficiently transferred to those in $(\mathbb{F}_{q^3})^*$, it follows that index-calculus algorithm can be applied to the multiplicative group of the latter. This fact does not render the group operation automatically useless in the face of possible cryptographic applications, as long as proper key lengths are utilized.

For general finite fields, such as the proposed one, with a multiplicative group of size N, current state-of-the-art algorithms (including index-calculus) report computation times of

$$L_N(\alpha, c) = \exp\left((c + o(1))(\log N)^{\alpha}(\log\log N)^{1-\alpha}\right), \tag{5}$$

where α and c are parameters in the ranges $0 < \alpha < 1$ and $c > 0$ (sometimes c is omitted and we default to $L_N(\alpha)$). Actually, α drives the transition from an exponential-time algorithm (when α approaches 1) to a pure polynomial-time algorithm (as α tends to 0).

The first subexponential algorithms had complexity $L_N(1/2)$ and applied only to prime fields. Soon $L_N(1/3)$ was achieved for any finite field, with values for c ranging from $(64/3)^{1/3}$ for fields with high characteristic to $(128/9)^{1/3}$ for medium characteristic. When dealing with small characteristic fields, recent research brought down the complexity to $L_N(1/4)$ [41] and even to quasi-polynomial time [42,43]. If the group size is $N = p^n$, and we write $p = L_{p^n}(l_p)$, then the characteristic is considered "small", "medium-sized" or "large" depending on whether $l_p \leq 1/3$, $1/3 < l_p < 2/3$, or $l_p \geq 2/3$, respectively.

In any case, the previous results have been applied in practice and several cryptanalysis have been successfully carried out (see [44,45]), so it seems sensible to avoid using small characteristics and also extensions of moderate characteristic included in the range threatened by recent cryptanalytic techniques [42,43,46]. However, these algorithms are heuristic and are proved to work only for certain particular cases, not difficult to circumvent: for example, if one has $N = p^n$, it suffices to choose both p and n to be prime in order to thwart both [42,43]. For a detailed account of history and current status, see [47] (in particular §4.2), and [48].

Our proposal is to use a group $\mathbb{G}$ of prime order $n = q^2 + q + 1$, over a ground field $\mathbb{F}_q$. Using formula (5), we can compute how many elements in $\mathbb{G}$ provide a given security level. Since the number of elements is roughly the square of the value of q, it follows that q can be represented with only one half of the bits needed for n. This has a direct impact on the computation time of the $\oplus$ operation in $\mathbb{G}$, since it is performed in $\mathbb{F}_q$ (see Equation (4) and cost analysis in Section 3.4).

3.2. System Setup and System Parameters for a Key Agreement Protocol

The group $\mathbb{G} = (\mathbb{F}_q P^2, \oplus)$ 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.

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

System Setup

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, such that $\ell = q^2 + q + 1$ is prime.
2. Select elements $c_1, c_2, c_3 \in \mathbb{F}_q$ such that the polynomial
$$\chi(X) = X^3 - c_1 X^2 - c_2 X - c_3$$
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 α 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. Consider a projection $\pi\colon (\mathbb{F}_q)^3 \setminus \{(0,0,0)\} \to \mathbb{F}_q P^2$, such that $[\beta_1, \beta_2, \beta_3] = \pi(\alpha_1, \alpha_2, \alpha_3)$, and $Q(\beta_1, \beta_2, \beta_3) = 1$.

   Observe that $N(\alpha) = Q(\alpha_1, \alpha_2, \alpha_3)$ (see proof of Proposition 1). If we compute $a = N(\alpha)^{-e}$, where $e = 3^{-1} \pmod{q-1}$, we have that $N(a\alpha) = 1$. Therefore, the projection π consists simply in computing $\beta_i = a\alpha_i$, for $1 \leq i \leq 3$.

   Defining the projection π in this way is convenient, since it automatically gives rise to a generator in $\mathbb{F}_q P^2$ with a unitary norm, which means that all the elements generated by it will enjoy also a unitary norm.

   Remark en passant that the previous device works only if 3 is invertible in $\mathbb{Z}_{q-1}$. Fortunately, this is always the case since otherwise the following implications hold: $3|(q-1) \Rightarrow q \equiv 1 \pmod 3 \Rightarrow \ell = q^2 + q + 1 \equiv 0 \pmod 3$ and the latter equation would contradict the fact that we chose ℓ as a prime.

Remark 7. *In order to save space, we can always find an irreducible χ such that $c_1 = 0$. Obviously, c_3 cannot be 0, but we may wonder whether we could in addition take $c_2 = 0$. However, this is not possible according to [49] (Lemma 7). The latter reference studies the number of irreducible binomials $X^t - a \in \mathbb{F}_q[X]$, with $a \in \mathbb{F}_q^*$, and concludes that the number of such irreducible binomials $N_t(q)$ is*

$$N_t(q) = \begin{cases} \frac{\varphi(t)}{t}(q-1), & \text{if } \mathrm{rad}_4(t) | (q-1), \\ 0, & \text{otherwise.} \end{cases}$$

The largest square-free number that divides $t \neq 0$ is denoted by $\mathrm{rad}(t)$ and

$$\mathrm{rad}_4(t) = \begin{cases} \mathrm{rad}(t) & \text{if } 4 \nmid t \\ 2\mathrm{rad}(t) & \text{otherwise.} \end{cases}$$

For our case, $t = 3$, hence $\mathrm{rad}_4(t) = 3$. However, then $N_t(q) = 0$, since we chose $\ell = q^2 + q + 1$ to be a prime, thus implying $3 \not| (q-1)$.

Accordingly, we conclude that c_1 and c_2 cannot be simultaneously taken as 0.

System Parameters

The system parameters are defined by the set $\mathcal{S} = \{\mathbb{F}_q, [\beta_1, \beta_2, \beta_3], c_1, c_2, c_3\}$, following the notation and conditions explained above.

3.3. The 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 $n_A \in \mathbb{Z}_\ell$ uniformly at random, with $\ell = q^2 + q + 1$, computes

$$[\gamma_1^A, \gamma_2^A, \gamma_3^A] = \oplus^{n_A}[\beta_1, \beta_2, \beta_3] \in \mathbb{F}_q P^2$$

   and sends it to user B.
2. User B selects $n_B \in \mathbb{Z}_\ell$ uniformly at random, computes

$$[\gamma_1^B, \gamma_2^B, \gamma_3^B] = \oplus^{n_B}[\beta_1, \beta_2, \beta_3] \in \mathbb{F}_q P^2$$

   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:

$$\begin{aligned} k_A = \oplus^{n_A}[\gamma_1^B, \gamma_2^B, \gamma_3^B] &= \oplus^{n_A}\left(\oplus^{n_B}[\beta_1, \beta_2, \beta_3]\right) \\ &= \oplus^{n_B}\left(\oplus^{n_A}[\beta_1, \beta_2, \beta_3]\right) \\ &= \oplus^{n_B}[\gamma_1^A, \gamma_2^A, \gamma_3^A] = k_B. \end{aligned}$$

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

3.4. Cost of the $\oplus$ Operation in $\mathbb{G}$

Let S and P be the number of field operations in order to perform an addition and a multiplication respectively in $\mathbb{F}_q$. From the formula (4), it follows that the total number of operations for computing $\mathbf{x} \oplus \mathbf{y}$ is equal to $10S + 15P$, once the $2S + 3P$ precomputations of $c_1 c_3$, $c_1 c_2 + c_3$, and $(c_1)^2 + c_2$ are assumed.

3.5. A Toy Example

We provide hereafter an example of computing a discrete logarithm by brute-force search. In general, this algorithm is, of course, infeasible, but we choose very small parameters in order to illustrate the operation of the group $\mathbb{G}$.

Let us take the prime field $\mathbb{F}_p$, with $p = 131$, for which $p^2 + p + 1 = 17{,}293$ is also a 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 $\mathbb{F}_{131}$.

We select the element $\mathbf{x} = (126, 16, 1)$ as a generator in $(\mathbb{F}_q^3)^*$. As explained above, it is convenient to project it onto a unitary norm point of $\mathbb{F}_q P^2$. To achieve this goal, we perform the following steps:

$$\begin{aligned} N(\mathbf{x}) &= Q(126, 16, 1) = 90, \\ e &= 3^{-1} \pmod{130} = 87, \\ a &= 1/N(\mathbf{x})^e = 23, \\ X &= \pi(\mathbf{x}) = a \cdot (126, 16, 1) = [16, 106, 23]. \end{aligned}$$

Observe that indeed $Q(16, 106, 23) = 1$. We choose a target point $\mathbf{y} = (86, 120, 1)$ and performing a similar computation we get $Y = [15, 91, 87]$. The problem is to find the discrete logarithm of Y to the base X, i.e., find the integer n such that $Y = \oplus^n X$. Iterating the operation, we carry out an exhaustive search:

$$\begin{aligned} [16, 106, 23] \to [44, 78, 53] \to [65, 41, 125] \to [40, 50, 43] \to \\ [35, 67, 125] \to [115, 59, 58] \to [11, 95, 6] \to [8, 69, 62] \to \\ [122, 109, 9] \to [15, 91, 87]. \end{aligned}$$

Eventually, we come up with the target point. Since the operation has been iterated ten times, we conclude $Y = \oplus^{10} X$ for this particular pair, so that $\log_X Y = 10$. Remark that, to perform each step, it suffices to follow the formula (4).

3.6. 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 of selecting prime fields, $\mathbb{F}_p$, over which the $\oplus$ operation will be tested. Observe that, according to formula (4), performing the operation boils down to a number of additions and multiplications over the base field; hence, the expected computation time will depend on the size of its elements; informally, *size* (also known as bit length) means the number of bits in the binary representation of such elements. The selected prime fields, $\mathbb{F}_p$, will have increasing values for the size of p, i.e., increasing bit lengths in the representation of their elements.

Taking the previous considerations into account the experiment is conducted as follows: we take increasing values of p and, for each value, we perform all the required computations to add two random points in $\mathbb{G}$, following formula (4). We repeat the experiment a large number of times for distinct points and record the mean computation time for each value of p.

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. As before, the idea is selecting random points and adding them using, in particular, projective coordinates according to the formulas given in [50] [§13.2.1.b]. Repeating the computation a large number of times, we record the mean computation time for each value of p. 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.

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 (Santa Clara, CA, USA) 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. In each line, the first column represents the number of bits of the binary representation of the elements in $\mathbb{F}_p$, the ground field. The second and third columns represent the mean computation time needed to perform the addition of two points in the group $\mathbb{G}$ via the operation $\oplus$, and in an elliptic curve over $\mathbb{F}_p$, respectively. All the computation times are measured in microseconds.

Table 1. Computation time for one single operation in each setting.

Bit Length	$\oplus$ Operation in $\mathbb{G}$ (µs)	Point Addition in Elliptic Curves (µs)
32	1.10306044	1.07039673
64	1.68166612	1.97707724
96	1.97807208	2.55200463
128	2.19050201	2.86859037
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	6.43152050
384	4.86727126	6.97227992
416	5.41008866	7.75588654
448	5.77817335	8.32544612
480	6.31956718	9.02521134
512	6.70272949	9.61432718

Having a visual idea of the results reported in Table 1 is best achieved by depicting them in a combined graph. To this end, we show in Figure 1 the graphical representation of the computation times for both operations, as reported in Table 1. Both graphs are conveniently labeled so that one of them depicts the computation time for the $\oplus$ operation in $\mathbb{G}$, and the other one depicts the computation time for the point addition in elliptic curves over $\mathbb{F}_p$. The x-axis represents the bit length of p common for both operations.

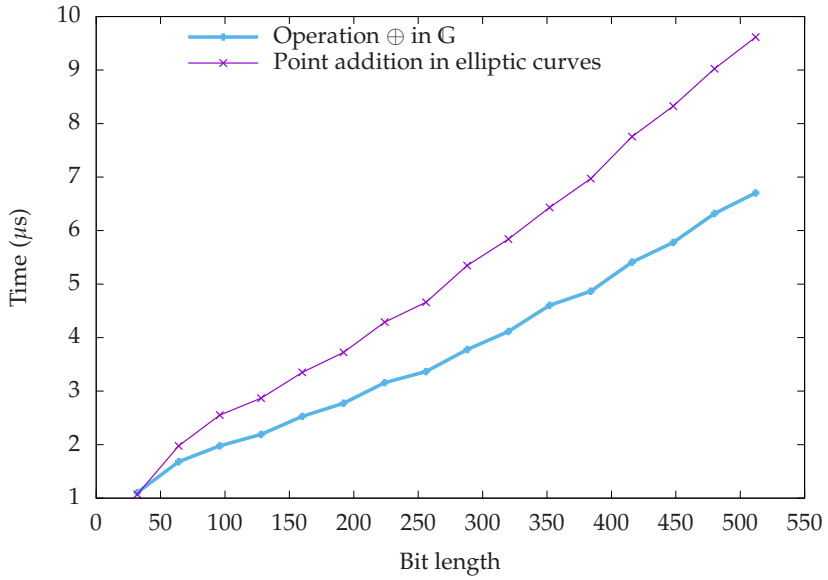

Figure 1. Comparison of average computation times for both settings.

The graph pushes to the foreground some interesting remarks:

- The computation times shown in Figure 1 for both settings show a essentially linear growth, which is convenient in view of practical applications.
- Though the point addition in elliptic curves is slightly slower than the $\oplus$ operation in $\mathbb{G}$ for the same bit length over the ground field, they keep a rather constant ratio between them, which is roughly equal to 0.7.

3.7. Real World Parameters

In order to assess the size for real world parameters, we resort to the recommendations issued by NIST [51]. These recommendations are based on the knowledge of the execution time of the best algorithms solving any particular problem. We will reproduce here an excerpt of Table 2 in that reference, which summarizes the bit sizes for the relevant parameters applicable to our proposal.

Table 2. Comparable cryptographic strengths.

Security Strength	Group Order	Base Field Size
112	2048	1024
128	3072	1536
192	7680	3840
256	15,360	7680

We explain hereafter the meaning of the columns. To begin with, Security strength represents the binary logarithm of the estimated time taken by the best known algorithm for solving the problem (which is proportional to the number of cryptographic operations), thus breaking the cryptosystem. The center column, labeled as Group order, is related to the group where the cryptosystem is defined; in our case, it is the projective space $\mathbb{F}_q P^2$ where $\mathbb{F}_q$ is the base field. In particular, each line in this column represents the binary logarithm of the number of elements in the projective space needed to achieve the security strength indicated in the leftmost column.

Since we propose that the number of points in the projective space is $n = q^2 + q + 1$, the base field size (namely, the binary logarithm of q) is half the size of n, as represented in the rightmost column. Remark that this is a nice feature, since the multiplication cost in the base field is intimately related to the size of the latter.

Finally, the public key consists of one projective point. Since we chose unitary norm for such point, it can be represented with just two elements of the base field. Therefore, public key size is twice as much as the base field size (it needs twice as many bits).

4. A More Robust System

The security of the cryptosystem proposed in the previous sections can be increased by extending the theory developed for a field to the case of a unitary commutative ring R.

Essentially, we will stick to the ring $\mathbb{Z}/m\mathbb{Z}$, where $m = pq$ is an integer, the product of two primes of similar size, p and q. We will strain ourselves in order to apply all the concepts developed in the previous sections to this new setting in an attempt to improve the security and efficiency of the proposed scheme.

We will manage to obtain the definition of a group law acting over the direct product of two projective spaces, $\mathbb{F}_p P^2 \times \mathbb{F}_q P^2$. In this new setting, the security is reinforced since an attacker is forced to sequentially solve an instance of the integer factorization problem and an instance (actually two instances, but they can be parallelized) of the discrete logarithm problem.

In fact, let M be a free R-module of finite rank and let $A\colon M \to M$ be an R-linear map with characteristic polynomial $\chi_A(X) = \det(XI - \Lambda)$, X being an indeterminate, I the identity matrix of order $r = \operatorname{rank} M$, and Λ the matrix of A in an arbitrary basis for M. According to [52] [III, §8, 11.Proposition 20], the Cayley-Hamilton Theorem holds in this setting, namely $\chi_A(A) = 0$.

Hence, if $M = R^3$ and $\chi_A(X) = X^3 - c_1X^2 - c_2X - c_3$, $c_1, c_2, c_3 \in R$, then $A^3 = c_1A^2 + c_2A + c_3I$.

As above, we can define a degree-3 homogeneous polynomial in $R[x_1, x_2, x_3]$ by setting $Q(x_1, x_2, x_3) = \det\left(x_1 I + x_2\Lambda + x_3\Lambda^2\right)$. As a computation shows, we have

$$\begin{aligned} Q(x_1, x_2, x_3) = &-c_2 x_1 (x_2)^2 + \left[(c_2)^2 - 2(c_1 c_3)\right] x_1 (x_3)^2 + c_1 (x_1)^2 x_2 \\ &+ \left[(c_1)^2 + 2c_2\right] (x_1)^2 x_3 - (c_2 c_3) x_2 (x_3)^2 + (c_1 c_3)(x_2)^2 x_3 \\ &- (c_1 c_2 + 3c_3)\, x_1 x_2 x_3 + (x_1)^3 + c_3 (x_2)^3 + (c_3)^2 (x_3)^3, \end{aligned}$$

thus proving that Lemma 1 still holds in this case; i.e., Q depends on χ_A only, but not on the matrix Λ.

The projective plane over R is then defined as follows: $RP^2 = (R^3 \setminus \{\mathbf{0}\})/R^*$, where R^* denotes the multiplicative group of invertible elements in R and R^* acts on $R^3 \setminus \{\mathbf{0}\}$ by

$$\lambda \cdot (x_1, x_2, x_3) = \quad (\lambda x_1, \lambda x_2, \lambda x_3), \quad \forall \lambda \in R^*, \quad \forall (x_1, x_2, x_3) \in R^3 \setminus \{\mathbf{0}\}.$$

Proceeding as in the previous sections, a composition law $\oplus\colon R^3 \times R^3 \to R^3$, $(\mathbf{x}, \mathbf{y}) \mapsto \mathbf{z} = \mathbf{x} \oplus \mathbf{y}$, $\mathbf{x} = (x_1, x_2, x_3)$, $\mathbf{y} = (y_1, y_2, y_3)$, $\mathbf{z} = (z_1, z_2, z_3)$, can be defined by the formula

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

and similarly we deduce

$$\begin{pmatrix} z_1 \\ z_2 \\ z_3 \end{pmatrix} = \begin{pmatrix} x_1 & c_3 x_3 & c_1 c_3 x_3 + c_3 x_2 \\ x_2 & x_1 + c_2 x_3 & c_2 x_2 + c_3 x_3 + c_1 c_2 x_3 \\ x_3 & x_2 + c_1 x_3 & x_1 + (c_1)^2 x_3 + c_1 x_2 + c_2 x_3 \end{pmatrix} \begin{pmatrix} y_1 \\ y_2 \\ y_3 \end{pmatrix}. \tag{6}$$

The determinant of the matrix of (6) is equal to $Q(x_1, x_2, x_3)$. Hence, $\oplus$ induces a composition law $\oplus\colon Q^{-1}(R^*) \times Q^{-1}(R^*) \to Q^{-1}(R^*)$. If C denotes the set of classes modulo R^* of points $\mathbf{x} \in R^3$ such that $Q(\mathbf{x}) \in R \backslash R^*$, then $\oplus$ also induces a composition law $\oplus\colon PQ^{-1}(R^*) \times PQ^{-1}(R^*) \to PQ^{-1}(R^*)$, where $PQ^{-1}(R^*) = RP^2 \setminus C$, as if $Q(\mathbf{x})$ is invertible and $\lambda \in R^*$, then $Q(\lambda\mathbf{x}) = \lambda^3 Q(\mathbf{x})$ is also invertible.

The same proof given in the case of a field shows that the composition law $\oplus$ is associative, commutative, and admits an identity element, which is the vector $(1, 0, 0)$.

If $m = pq$ with $p \neq q$ prime integers, then from Chinese Remainder Theorem there is a ring isomorphism between $\mathbb{Z}/m\mathbb{Z}$ and the product ring $\mathbb{F}_p \times \mathbb{F}_q$. Hence, each vector $\mathbf{x} \in R^3$ can be assigned a pair $(\mathbf{x}', \mathbf{x}'')$ in $(\mathbb{F}_p)^3 \times (\mathbb{F}_q)^3$ and the group $(\mathbb{Z}/m\mathbb{Z})^* = (\mathbb{F}_p)^* \times (\mathbb{F}_q)^*$ acts on R^3 in the same way as $(\mathbb{F}_p)^*$ acts on $(\mathbb{F}_p)^3$ and $(\mathbb{F}_q)^*$ does on $(\mathbb{F}_q)^3$.

Consequently, $\mathbf{x} \neq 0$ if and only if at least one of its two components $\mathbf{x}', \mathbf{x}''$ is distinct from $\mathbf{0}$, so that

$$\begin{aligned} R^3 \setminus \{\mathbf{0}\} = &\left[\{\mathbf{0}\} \times \left((\mathbb{F}_q)^3 \setminus \{\mathbf{0}\}\right)\right] \sqcup \left[\left((\mathbb{F}_p)^3 \setminus \{\mathbf{0}\}\right) \times \{\mathbf{0}\}\right] \sqcup \\ &\left[\left((\mathbb{F}_p)^3 \setminus \{\mathbf{0}\}\right) \times \left((\mathbb{F}_q)^3 \setminus \{\mathbf{0}\}\right)\right]. \end{aligned} \tag{7}$$

Therefore, $(\mathbb{Z}/pq\mathbb{Z})P^2 = \mathbb{F}_p P^2 \sqcup \mathbb{F}_q P^2 \sqcup \left(\mathbb{F}_p P^2 \times \mathbb{F}_q P^2\right)$.

Moreover, letting $\mathbf{z} = (\mathbf{z}', \mathbf{z}'') = \mathbf{x} \oplus \mathbf{y}$, as a computation shows, one obtains $\mathbf{z}' = \mathbf{x}' \oplus \mathbf{y}'$ and $\mathbf{z}'' = \mathbf{x}'' \oplus \mathbf{y}''$, and $Q(\mathbf{x})$ is invertible if and only if $Q(\mathbf{x}) \bmod p$ and $Q(\mathbf{x}) \bmod q$ both are invertible in $\mathbb{Z}/p\mathbb{Z}$ and $\mathbb{Z}/q\mathbb{Z}$, respectively. If $\mathbf{x} \in R^3$ corresponds to $(\mathbf{x}', \mathbf{x}'')$ in $(\mathbb{F}_p)^3 \times (\mathbb{F}_q)^3$, then $Q(\mathbf{x}) = (Q'(\mathbf{x}'), Q''(\mathbf{x}''))$, where $Q'(\mathbf{x}') = \det\left(x_1' I + x_2' \Lambda' + x_3' \Lambda'^2\right)$, $Q''(\mathbf{x}'') = \det\left(x_1'' I + x_2'' \Lambda'' + x_3'' \Lambda''^2\right)$, and $\Lambda' = \Lambda \bmod p$, $\Lambda'' = \Lambda \bmod q$. Hence,

$$Q^{-1}(R^*) = \left\{(\mathbf{x}', \mathbf{x}'') \in (\mathbb{F}_p)^3 \times (\mathbb{F}_q)^3 : Q'(\mathbf{x}') \neq 0, Q''(\mathbf{x}'') \neq 0\right\}. \tag{8}$$

We set

$$\left.\begin{array}{ll}\chi'(X) = X^3 - c_1'X^2 - c_2'X - c_3' \in \mathbb{F}_p[X], & c_i' = c_i \bmod p \\ \chi''(X) = X^3 - c_1''X^2 - c_2''X - c_3'' \in \mathbb{F}_q[X], & c_i'' = c_i \bmod q\end{array}\right\} 1 \leq i \leq 3.$$

If both χ' and χ'' are irreducible polynomials in $\mathbb{F}_p[X]$ and $\mathbb{F}_q[X]$, respectively, then, according to Proposition 1, the points of the associated curves C' and C'' reduce to the origin; i.e., $Q'^{-1}(0) = \{\mathbf{0}_p\}$, $Q''^{-1}(0) = \{\mathbf{0}_q\}$, where $\mathbf{0}_p$ and $\mathbf{0}_q$ denote the origin in $(\mathbb{F}_p)^3$ and $(\mathbb{F}_q)^3$, respectively.

From (7), taking (8) into account, it follows: $PQ^{-1}(R^*) = \mathbb{F}_pP^2 \times \mathbb{F}_qP^2$. Consequently, we conclude that $PQ^{-1}(R^*) \cong S_p \times S_q$, where S_p and S_q are the subgroups given by

$$S_p = (\mathbb{F}_pP^2 \times \{(1,0,0)\}, \oplus), \quad S_q = (\{(1,0,0)\} \times \mathbb{F}_qP^2, \oplus),$$

and, from Theorem 2, we thus obtain

Proposition 3. *If the polynomials χ' and χ'' are irreducible in $\mathbb{F}_p[X]$ and $\mathbb{F}_q[X]$, respectively, then the group $(PQ^{-1}(R^*) = \mathbb{F}_pP^2 \times \mathbb{F}_qP^2, \oplus)$ is isomorphic to the direct product of the cyclic groups S_p and S_q. Hence, $(PQ^{-1}(R^*), \oplus)$ is cyclic if and only if $a = p^2 + p + 1$ and $b = q^2 + q + 1$ are coprimes; i.e., $\gcd(a, b) = 1$.*

Remark 8. *If $d = \gcd(a, b)$, then $a = da'$, $b = db'$, with $\gcd(a', b') = 1$. The cyclic subgroup S in $\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$ spanned by $(1 \bmod a, 1 \bmod b)$ is of order $\frac{ab}{d}$. As $d < pq$ and $a = O(p^2)$, $b = O(q^2)$, it follows: $\frac{ab}{d} > \frac{O(p^2q^2)}{pq} = O(pq)$, which indicates that in general the group S is large enough, even if a and b are not coprimes.*

Remark 9. *It is clear that the group $(PQ^{-1}(R^*), \oplus)$ is also amenable as a building block for a key-agreement protocol by choosing $R = \mathbb{Z}_m$, with m composite. Observe that its security is enhanced with respect to its counterpart $\mathbb{F}_q$, q a prime power, since the algorithms known to be efficient to compute discrete logarithms only work in the multiplicative group of a field. This means that one is forced to factorize m in order to apply such algorithms to the present case, thus increasing the time complexity and the security of the system, though at the price of doubling the key length.*

5. Conclusions

In this work, we have defined a group law, $\oplus$, over the set $\mathbb{F}_qP^2$, and considered the discrete logarithm problem associated with them. We have analyzed their properties and stated the security of the problem considered. Moreover, based on it, we have defined a cryptographic key agreement protocol as one possible application of this problem to public key cryptography. Finally, we shift the system to the group $(PQ^{-1}(R^*), \oplus)$ over the ring $\mathbb{Z}/pq\mathbb{Z}$, which turns out to be completely analogous to the previous one and offers an enhanced security, though at the cost of some extra key length.

As future work, we think that it is possible to extend this discrete logarithm problem in order to define new cryptographic protocols for encryption/decryption and digital signatures, among others, in a similar way as ElGamal or elliptic curve cryptosystems were defined from the Diffie-Hellman key agreement protocol.

Author Contributions: Conceptualization, R.D.D., L.H.E. and J.M.M.; Funding acquisition, L.H.E.; Investigation, R.D.D., L.H.E. and J.M.M.; Methodology, R.D.D., L.H.E. and J.M.M.; Writing—original draft, R.D.D., L.H.E. and J.M.M.; Writing—review & editing, R.D.D., L.H.E. and J.M.M. All authors have read and agreed to the published version of the manuscript.

Funding: This research has been partially supported by Ministerio de Economía, Industria y Competitividad (MINECO), Agencia Estatal de Investigación (AEI), and European Regional Development Fund (ERDF, EU), through project COPCIS, Grant No. TIN2017-84844-C2-1-R, and by Comunidad de Madrid (Spain) through project CYNAMON, Grant No. P2018/TCS-4566-CM, co-funded along with ERDF.

Conflicts of Interest: The authors declare no conflict of interest.

Abbreviations

The following abbreviations are used in this manuscript:

DLP Discrete Logarithm Problem
PKC Public Key Cryptography

References

1. Koblitz, N. Elliptic curve cryptosystems. *Math. Comput.* **1987**, *48*, 203–209. [CrossRef]
2. Miller, V.S. Use of elliptic curves in cryptography. *Lect. Notes Comput. Sci.* **1986**, *218*, 417–426. [CrossRef]
3. Diffie, W.; Hellman, M.E. New directions in cryptography. *IEEE Trans. Inform. Theory* **1976**, *22*, 644–654. [CrossRef]
4. Rivest, R.; Shamir, A.; Adleman, L.M. A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. *Commun. ACM* **1978**, *21*, 120–126. [CrossRef]
5. ElGamal, T. A public key cryptosystem and a signature scheme based on discrete logarithms. *IEEE Trans. Inform. Theory* **1985**, *31*, 469–472. [CrossRef]
6. Menezes, A.J.; Qu, M.; Vanstone, S.A. Some new key agreement protocols providing implicit authentication. In Proceedings of the 2nd Workshop on Selected Areas in Cryptography (SAC '95), Carleton University, Ottawa, ON, Canada, 18–19 May 1995; pp. 22–32.
7. Massey, J.L.; Omura, J.K. Method and Apparatus for Maintaining the Privacy of Digital Messages Conveyed by Public Transmission. 1986. Available online: www.google.com/patents/US4567600 (accessed on 1 March 2020).
8. Menezes, A.; Vanstone, S. Elliptic curve cryptosystems and their implementation. *J. Cryptol.* **1993**, *6*, 209–224. [CrossRef]
9. Bellare, M.; Rogaway, P. Minimizing the use of random oracles in authenticated encryption schemes. *Lect. Notes Comput. Sci.* **1997**, *1334*, 1–16. [CrossRef]
10. Abdalla, M.; Bellare, M.; Rogaway, P. DHAES: An encryption scheme based on the Diffie-Hellman problem; Available online: http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.28.2910 (accessed on 1 March 2020).
11. Abdalla, M.; Bellare, M.; Rogaway, P. DHIES: An Encryption Scheme Based on the Diffie-Hellman Problem. 2001. Available online: http://web.cs.ucdavis.edu/~rogaway/papers/dhies.pdf (accessed on 1 March 2020).
12. Abdalla, M.; Bellare, M.; Rogaway, P. The oracle Diffie-Hellman assumptions and an analysis of DHIES. *Lect. Notes Comput. Sci.* **2001**, *2020*, 143–158. [CrossRef]
13. ANSI. *Public Key Cryptography for the Financial Services Industry: Key Agreement and key Transport Using Elliptic Curve Cryptography*; American National Standards Institute: New York, NY, USA, 2001.
14. IEEE. *Standard Specifications for Public Key Cryptography-Amendment 1: Additional Techniques*; Institute of Electrical and Electronics Engineers: Piscataway, NJ, USA, 2004.
15. ISO/IEC. *Information Technology-Security Techniques-Encryption Algorithms-Part 2: Asymmetric Ciphers*; International Organization for Standardization/International Electrotechnical Commission: Geneva, Switzerland, 2006.
16. Gayoso Martínez, V.; Hernández Álvarez, F.; Hernández Encinas, L.; Sánchez Ávila, C. Analysis of ECIES and other cryptosystems based on elliptic curves. *J. Inf. Assur. Secur.* **2011**, *6*, 285–293.
17. NIST. *Digital Signature Standard (DSS)*; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2000.
18. ANSI. *Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA)*; American National Standards Institute: New York, NY, USA, 2005.
19. IEEE. *Standard Specifications for Public Key Cryptography*; Institute of Electrical and Electronics Engineers: Piscataway, NJ, USA, 2000.
20. National Institute of Standard and Technology. *Digital Signature Standard (DSS)*; NIST FIPS 186-4; National Institute of Standard and Technology: Gaithersburg, MD, USA, 2009.
21. Lochter, M.; Merkle, J. Elliptic Curve Cryptography (ECC) Brainpool Standard Curves and Curve Generation. *Request for comments (RFC 5639), Internet Engineering Task Force*. 2010. Available online: https://datatracker.ietf.org/doc/rfc5639/ (accessed on 1 March 2020).

22. Bernstein, D.J.; Lange, T. SafeCurves, 2014. Available online: http://safecurves.cr.yp.to/ (accessed on 1 March 2020).
23. Edwards, H. A normal form for elliptic curves. *Bull. Am. Math. Soc.* **2007**, *44*, 393–422. [CrossRef]
24. Baignères, T.; Delerablée, C.; Finiasz, M.; Goubin, L.; Lepoint, T.; Rivain, M. Trap Me If You Can. Million Dollar Curve. *Cryptology ePrint Archive: Report 2015/1249* 2016. Available online: https://eprint.iacr.org/2015/1249 (accessed on 1 March 2020).
25. Gayoso Martínez, V.; Hernández Encinas, L.; Martín Muñoz, A.; Durán Díaz, R. Secure elliptic curves and their performance. *Log. J. IGPL* **2019**, *27*, 277–238. [CrossRef]
26. Koyama, K.; Maurer, U.M.; Okamoto, T.; Vanstone, S.A. New Public-Key Schemes Based on Elliptic Curves over the Ring $\mathbb{Z}_n$. *Lect. Notes Comput. Sci.* **1992**, *576*, 252–266. [CrossRef]
27. Meyer, B.; Müller, V. A Public Key Cryptosystem Based on Elliptic Curves over $\mathbb{Z}/n\mathbb{Z}$ Equivalent to Factoring. *Lect. Notes Comput. Sci.* **1996**, *1070*, 49–59. [CrossRef]
28. Papachristodoulou, L.; Batina, L.; Mentens, N. Recent Developments in Side-Channel Analysis on Elliptic Curve Cryptography Implementations. In *Hardware Security and Trust: Design and Deployment of Integrated Circuits in a Threatened Environment*; Sklavos, N., Chaves, R., Di Natale, G., Regazzoni, F., Eds.; Springer International Publishing: Berlin, Germany, 2017; pp. 49–76. [CrossRef]
29. Gayoso Martínez, V.; Hernández Encinas, L.; Martín Muñoz, A. Implementation of Cryptographic Algorithms for Elliptic Curves. In *Geometry, Algebra and Applications: From Mechanics to Cryptography*; Springer: Cham, Switzerland, 2016; Chapter 11, pp. 121–133. [CrossRef]
30. Shor, P. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. *SIAM J. Comput.* **1997**, *26*, 1484–1509. [CrossRef]
31. Gidney, C.; Ekeå, M. How to Factor 2048 bit RSA Integers in 8 Hours Using 20 Million Noisy Qubits. *arXiv* **2009**, arXiv:1905.09749.
32. NIST. Post-Quantum Cryptography. On-Line Publication, 2017. Available online: https://csrc.nist.gov/Projects/Post-Quantum-Cryptography (accessed on 1 March 2020).
33. NIST. Post-Quantum Cryptography, 2nd round. On-line publication: 2019. Available online: https://csrc.nist.gov/projects/post-quantum-cryptography/round-2-submissions (accessed on 1 March 2020).
34. Menezes, A.J. *Elliptic Curve Public Key Cryptosystems*; The Kluwer International Series in Engineering and Computer Science. Communications and Information Theory; Kluwer Academic Publishers: Boston, MA, USA, 1993; Volume 234. [CrossRef]
35. Singer, J. A theorem in finite projective geometry and some applications to number theory. *Trans. Am. Math. Soc.* **1938**, *43*, 377–385. [CrossRef]
36. Ghorpade, S.R.; Hasan, S.U.; Kumari, M. Primitive polynomials, Singer cycles and word-oriented linear feedback shift registers. *Des. Codes Cryptogr.* **2011**, *58*, 123–134. [CrossRef]
37. Silverman, J.H.; Tate, J.T. *Rational Points on Elliptic Curves*; Undergraduate Texts in Mathematics, Springer International Publishing: Cham, Switzerland, 2015. [CrossRef]
38. Koblitz, N.; Menezes, A.J. Another look at "Provable Security". *J. Cryptol.* **2007**, *20*, 3–37. [CrossRef]
39. Papadimitriou, C.H. *Computational Complexity*; Addison-Wesley Publishing Company: Reading, MA, USA, 1994. [CrossRef]
40. Odlyzko, A.M. *Handbook of Finite Fields*; CRC Press: Boca Raton, FL, USA, 2013; pp. 393–401.
41. Joux, A. A New Index Calculus Algorithm with Complexity $L(1/4 + o(1))$ in Small Characteristic. In *International Conference on Selected Areas in Cryptography*; Springer: Berlin/Heidelberg, Germany, 2014; Volume 8282; pp. 355–379. [CrossRef]
42. Barbulescu, R.; Gaudry, P.; Joux, A.; Thomé, E. A heuristic quasi-polynomial algorithm for discrete logarithm in finite fields of small characteristic. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*; Springer: Berlin/Heidelberg, Germany, 2014. [CrossRef]
43. Granger, R.; Kleinjung, T.; Zumbrägel, J. On the discrete logarithm problem in finite fields of fixed characteristic. *Trans. Am. Math. Soc.* **2018**, *370*, 3129–3145. [CrossRef]
44. Adj, G.; Menezes, A.; Oliveira, T.; Rodríguez-Henríquez, F. Computing discrete logarithms using Joux's algorithm. *ACM Comm. Computer Algebra* **2015**, *49*, 60.v [CrossRef]
45. Kleinjung, T.; Diem, C.; Lenstra, A.K.; Priplata, C.; Stahlke, C. Computation of a 768-Bit Prime Field Discrete Logarithm. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*; Springer: Cham, Switzerland, 2017; Volume 10210, pp. 185–201. [CrossRef]

46. Hayasaka, K.; Aoki, K.; Kobayashi, T.; Takagi, T. A construction of three-dimensional lattice sieve for number field sieve over $GF(p^n)$. Cryptology ePrint Archive, 2015/1179, 2015. Available online: https://eprint.iacr.org/2015/1179.pdf (accessed on 1 March 2020).
47. Joux, A.; Odlyzko, A.; Pierrot, C. *Open problems in Mathematics and Computational Science*; Springer International Publishing: Cham, Switzerland, 2014; pp. 5–36. [CrossRef]
48. Granger, R.; Kleinjung, T.; Zumbrägel, J. Indiscreet logarithms in finite fields of small characteristic. *Adv. Math. Commun.* **2018**, *12*, 263–286. [CrossRef]
49. Heyman, R.; Shparlinski, I.E. Counting irreducible binomials over finite fields. *Finite Fields Their Appl.* **2016**, *38*, 1–12. [CrossRef]
50. Cohen, H.; Frey, G.; Avanzi, R.; Doche, C.; Lange, T.; Nguyen, K.; Vercauteren, F. *Handbook of Elliptic and Hyperelliptic Curve Cryptography*; Chapman and Hall/CRC, Taylor & Francis Group: New York, NY, USA, 2005. [CrossRef]
51. Barker, E. *Recommendation for Key Management, Part 1: General*. NIST: Gaithersburg, MD, USA, 2016. Available online: https://csrc.nist.gov/publications/detail/sp/800-57-part-1/rev-4/final (accessed on 1 March 2020).
52. Bourbaki, N. *Éléments de Mathématique. Algèbre. Chapitres 1 à 3*; Herman: Paris, France, 1970. [CrossRef]