Computational aspects of retrieving a representation of an algebraic geometry code

Irene Márquez-Corbella [a] Edgar Martínez-Moro [b] Ruud Pellikaan [c] Diego Ruano [d]

[a] *GRACE Project, INRIA Sanclay-Île-de-France, Laboratoire d'Informatique (LIX) UMR 7161 X-CNRS, 1 rue Honoré d'Estienne d'Orves, Campus de l'École Polytechnique, 91120 Palaiseau, France.*

[b] *Institute of Mathematics, University of Valladolid, Castilla, Spain and Department of Mathematics and Statistics, Eastern Kentucky University, USA*

[c] *Department of Mathematics and Computing Science, Eindhoven University of Technology, P.O. Box 513, 5600 MB Eindhoven, The Netherlands*

[d] *Department of Mathematical Sciences, Aalborg University, 9220 Aalborg Øst, Denmark*

Abstract

Corrected version, 11 May 2014
Appeared in Journal of Symbolic Computation vol. 64, pp. 67–87, 2014.

Code-based cryptography is an interesting alternative to classic number-theoretic public key cryptosystem since it is conjectured to be secure against quantum computer attacks. Many families of codes have been proposed for these cryptosystems such as algebraic geometry codes. In (Márquez-Corbella et al., 2012) — for so called very strong algebraic geometry codes $C = C_L(\mathcal{X}, \mathcal{P}, E)$, where $\mathcal{X}$ is an algebraic curve over $\mathbb{F}_q$, $\mathcal{P}$ is an n-tuple of mutually distinct $\mathbb{F}_q$-rational points of $\mathcal{X}$ and E is a divisor of $\mathcal{X}$ with disjoint support from $\mathcal{P}$ — it was shown that an equivalent representation $C = C_L(\mathcal{Y}, Q, F)$ can be found. The n-tuple of points is obtained directly from a generator matrix of C, where the columns are viewed as homogeneous coordinates of these points. The curve $\mathcal{Y}$ is given by $I_2(\mathcal{Y})$, the homogeneous elements of degree 2 of the vanishing ideal $I(\mathcal{Y})$. Furthermore, it was shown that $I_2(\mathcal{Y})$ can be computed efficiently as the kernel of certain linear map. What was not shown was how to get the divisor F and how to obtain efficiently an adequate decoding algorithm for the new representation. The main result of this paper is an efficient computational approach to the first problem, that is getting F. The security status of the McEliece public key cryptosystem using algebraic geometry codes is still not completely settled and is left as an open problem.

Key words: Public key cryptosystem, Code-based cryptography, Algebraic Geometry codes, Gröbner basis.

Email addresses: irene.marquez-corbella@inria.fr (Irene Márquez-Corbella), edgar@maf.uva.es (Edgar Martínez-Moro), g.r.pellikaan@tue.nl (Ruud Pellikaan), diego@math.aau.dk (Diego Ruano).

1. Introduction

(McEliece, 1978) introduced the first public key cryptosystem (PKC) based on error-correcting codes. The security of this scheme is based on the hardness of the decoding of random linear codes, or equivalently the problem of finding a minimum-weight codeword in a large linear code without any visible structure. This property makes the scheme of McEliece an interesting candidate for post-quantum cryptography. Another advantage consists of its fast encryption and decryption procedures. So one might hope that it is suitable for constrained devices like RFID tags or sensor networks, see (Eisenbarth et al., 2009) for further results related to this issue. However, it has one important disadvantage: its low encryption size compared to its large key size. This does not mean that code-based cryptography is inherently inefficient. There have been many attempts on how to reduce the key size while keeping the same level of security, see for example (Baldi et al., 2008; Berger et al., 2009; Biasi et al., 2012; Gaborit, 2005; Misoczki and Barreto, 2009; Misoczki et al., 2012; Monico et al., 2000). There are other public-key primitives based on the theory of error-correcting codes like signature schemes (Courtois et al., 2001), stream ciphers (Gaborit et al., 2007) or hash functions (Augot et al., 2005).

The principle of the McEliece cryptosystem is as follows:

Key generation: Given C an $[n, k, d]$ linear code defined over $\mathbb{F}_q$ with an efficient bounded distance decoding algorithm which corrects up to $t \leq \lfloor \frac{d-1}{2} \rfloor$ errors. Let

(1) G be a generator matrix of C,
(2) S be an arbitrary nonsingular matrix of size $k \times k$,
(3) P be an arbitrary permutation matrix of size $n \times n$.

Let $G' = SGP$. Then the *McEliece public key* and the *McEliece private key* are given respectively by

$$\mathcal{K}_{\text{pub}} = (G', t) \quad \text{and} \quad \mathcal{K}_{\text{secret}} = (G, S, P)\,.$$

Encryption: Suppose we want to send a message $\mathbf{m} \in \mathbb{F}_q^k$ using the public key (G', t). First, we choose a random error vector $\mathbf{e}' \in \mathbb{F}_q^n$ with Hamming weight at most t, and then, we compute the ciphertext $\mathbf{y}' = \mathbf{m}G' + \mathbf{e}'$.

Decryption: Using the private key (G, S, P) the receiver first computes

$$\mathbf{y} := \mathbf{y}'P^{-1} = \mathbf{m}G'P^{-1} + \mathbf{e}'P^{-1} = \mathbf{m}SG + \mathbf{e}.$$

Since SG is also a generator matrix of the code C, he can apply the decoding algorithm for C to find $\mathbf{m}S$ and finally obtain the plaintext $\mathbf{m}$ from $\mathbf{m}SS^{-1}$.

McEliece proposed to use a $[1024, 524, 101]$ binary Goppa code. These parameters, however, do not attain the promised security level. We have mainly two different ways of cryptanalyzing the McEliece cryptosystem. There are also some side-channel attacks (Avanzi et al., 2011; Shoufan et al., 2010; Strenzke et al., 2008) but they are beyond the scope of this article.

(1) **Generic decoding attacks:** The best known technique for addressing the general decoding problem in cryptology is *Information Set Decoding* (ISD). The first approach to this method was introduced in (Prange, 1962). The variants which are used today are derived mainly from the algorithms of (Stern, 1989) and (Lee and Brickell, 1988). See (Canteaut and Chabaud, 1998; Peters, 2011) and the reference therein, for recent improvements which were presented independently. (Bernstein et al., 2008) presents the first successful attack on the original parameters of the McEliece scheme that required just under 8

days. More recent results (Becker et al., 2012; Bernstein et al., 2011; Finiasz and Sendrier, 2009; May et al., 2011) provide asymptotic improvements. Note that ISD, though much more efficient than a brute-force search, still needs exponential time in the code length. Therefore, more efficient generic attacks make the use of larger codes in the McEliece scheme necessary.

Another technique is the *Generalized Birthday Algorithm* (GBA). This method has been proposed in (Wagner, 2002) and was generalized in (Minder and Sinclair, 2012). GBA is sometimes faster than ISD.

(2) **Structural attacks:** These attacks try to retrieve the code structure rather than attempting to use an unspecific decoding algorithm. It addresses also the question of distinguishing a code with the prescribed structure from a random one. Structural attacks were efficiently applied to Reed-Solomon codes (Sidelnikov and Shestakov, 1992), concatenated codes (Sendrier, 1994) and Reed-Muller codes (Minder and Shokrollahi, 2007).

(Sendrier, 2000; Loidreau and Sendrier, 2001) gave an attack using the Support Splitting Algorithm. It recognizes binary Goppa codes with a binary Goppa polynomial and the secret-key is recovered for such codes of length 512 and 1024.

(Faugère et al., 2010; Gauthier-Umaña and Leander, 2009) provided an algebraic attack which recovers the secret-key from certain Goppa codes from the public-key using Gröbner basis computations. This attack is efficient against quasi-dyadic and quasi-cyclic codes but is infeasible for the original McEliece system. Therefore, the McEliece scheme remains unbroken for suitable parameters choices. This has lead to the statement that the generator matrix of a Goppa code does not disclose any visible structure that an attacker could exploit. However, in (Faugère et al., 2013) a polynomial-time algorithm is provided that distinguishes between random codes and Goppa codes whose rate is close to 1. This distinguisher is even more powerful in the case of Reed-Solomon codes (Couvreur et al., 2013; Márquez-Corbella and Pellikaan, 2012).

Many attempts to replace Goppa codes by different families of codes have been proven to be insecure as for example using Generalized Reed-Solomon (GRS) codes in (Niederreiter, 1986) which was broken in (Sidelnikov and Shestakov, 1992). Niederreiter's system differs from McEliece system in the public-key structure and in both encryption and decryption mechanism. It uses a parity check matrix instead of a generator matrix. This is an improvement to reduce the key size. However, this dual version of the McEliece cryptosystem is equivalent in terms of security. See (Li et al., 1994). Note that GRS codes are maximum distance separable codes (MDS), that is, they attain the maximum error detection/correction capability. In the McEliece cryptosystem this is interpreted as shorter keys for the same security level in comparison to the classical binary Goppa codes.

Although the Niederreiter scheme with GRS codes is completely broken, (Berger and Loidreau, 2005) proposed another version which is designed to resist the Sidelnikov-Shestakov attack. The main idea of this variant is to work with subcodes of the original GRS code rather than using the complete GRS code. However (Wieschebrink, 2006a, 2010) presented the first feasible attack to this scheme. Moreover, in (Márquez-Corbella et al., 2013) the authors have characterized those subcodes which are weak keys for the Berger-Loidreau cryptosystem. (Wieschebrink, 2006b) proposed another variant of the Niederreiter scheme where a few random columns are added to a generator matrix of a GRS code. In (Baldi et al., 2011) one more variant is presented. This time the structure is hidden differently than in the McEliece cryptosystem. In (Couvreur et al., 2013) a cryptanalysis of these schemes is provided.

Other classes of codes that have efficient bounded decoding algorithms, are proposed. (Sidelnikov, 1994) used Reed-Muller codes which were cryptanalyzed by (Minder and Shokrollahi, 2007). Also LDPC and MDPC codes (Baldi et al., 2008; Misoczki et al., 2012) were proposed but only MDPC codes remained unbroken. See for instance (Baldi and Chiaraluce, 2007). Another proposal used convolutional codes (Löndahl and Johansson, 2012) and was broken by (Landais and Tillich, 2013).

Algebraic geometry codes (AG codes) were introduced by (Goppa, 1977). The interested reader is referred to (Høholdt et al., 1998; Stichtenoth, 2009; Tsfasman and Vlăduţ, 1991). These codes have efficient decoding algorithms that correct up to half the designed minimum distance (Beelen and Høholdt, 2008; Høholdt et al., 1998; Høholdt and Pellikaan, 1995; Lee et al., 2012) which is one of the main requirements for code-based cryptography. (Janwa and Moreno, 1996) proposed to use the collection of AG codes on curves and their subfield subcodes for the McEliece cryptosystem. Recall that the GRS codes can be seen as the special class of algebraic geometry codes on the projective line, that is, the algebraic curve of genus zero. Therefore, this proposal for curves of genus zero is broken by the attack of Sidelnikov-Shestakov. Moreover, (Faure and Minder, 2008) proved that curves of genus $g \leq 2$ are a bad choice; their algorithm is an adaptation of the previous attack. The security status of this proposal for higher genus was not known.

The aim of this article is twofold. Firstly, to present a survey of the security status of code-based cryptography using AG codes. In (Márquez-Corbella et al., 2012) the authors addressed the question of retrieving a triple $(\mathcal{Y}, Q, E)$ which is isomorphic to the original representation triple of the *very strong algebraic geometry code* (VSAG) $C = C_L(\mathcal{X}, \mathcal{P}, F)$ used in a McEliece cryptosystem. The problem of retrieving such triple was solved from a theoretical point of view without giving the computational details. Therefore, the second goal of this article is to provide an efficient way to compute this triple. Efficient decoding algorithms for AG codes are known, but the efficient construction of a decoding algorithm for a given triple is still lacking.

Outline of the paper: In Section 2, we describe the basic notions of algebraic geometry and give some specific techniques applied to coding theory. It is important to note that we define an AG code $C_L(\mathcal{X}, \mathcal{P}, E)$ even when the n-tuple $\mathcal{P}$ is not disjoint from the divisor E. In Section 3, we collect the information from a generator matrix of a VSAG code C. In particular we give the genus g of the curve $\mathcal{X}$ and the degree m of the divisor E such that $C = C_L(\mathcal{X}, P, E)$.

In Section 4 we present the main contributions of the paper, that is how to compute the triple $(\mathcal{Y}, Q, F)$ efficiently. In Section 4.1 we give a constructive proof of how to compute a set of generators of the ideal $I(\mathcal{Y})$. In Section 4.2 we give some bounds for the complexity of obtaining local parameters at the points Q_j for $j = 1, \ldots, n$. In Section 4.3 we describe a method for determining the divisor F. At last, in Section 4.5 the main result of the paper is given. Section 5 provides some examples to illustrate this procedure.

Finally, in Section 6, we indicate some decoding algorithms for the resulting AG-code that can be used in practice.

2. Generalized constructions of AG codes

Let $\mathbb{F}_q$ be a finite field with q elements and let $\mathbb{F}_q[\mathbf{X}] = \mathbb{F}_q[X_1, \ldots, X_r]$ be the polynomial ring in r variables over $\mathbb{F}_q$. We denote by $\mathbb{A}^n$ the n-dimensional *affine space* and by $\mathbb{P}^n$, the n-dimensional projective space.

Let $\mathcal{X}$ be an absolutely irreducible nonsingular projective curve in $\mathbb{P}^r$ and defined over $\mathbb{F}_q$. The set of $\mathbb{F}_q$-rational points of $\mathcal{X}$ is denoted by $\mathcal{X}(\mathbb{F}_q)$. Let $I(\mathcal{X})$ be the homogeneous vanishing ideal of $\mathcal{X}$ in the polynomial ring $\mathbb{F}_q[\mathbf{X}]$. The ring

$$R = \mathbb{F}_q[X_0, \ldots, X_r]/I(\mathcal{X})$$

is an integral domain, since $\mathcal{X}$ is absolutely irreducible and $I(\mathcal{X})$ is a prime ideal. Hence we can form $\mathbb{Q}(R)$, the field of fractions of R. The *function field* of $\mathcal{X}$, denoted by $\mathbb{F}_q(\mathcal{X})$ is the subfield of $\mathbb{Q}(R)$ defined by

$$\mathbb{F}_q(\mathcal{X}) = \left\{ \frac{F}{G} \mid F, G \in R \text{ both nonzero and of the same degree} \right\} \cup \{0\}.$$

The elements of $\mathbb{F}_q(\mathcal{X})$ are called *rational functions*. Thus, every rational function of $\mathbb{F}_q(\mathcal{X})$ could be written as a fraction of two homogeneous polynomials F and G in $\mathbb{F}_q[\mathbf{X}]$ of the same degree such that $G(P) \notin I(\mathcal{X})$. Note that the fractions $\frac{F}{G}$ and $\frac{\hat{F}}{\hat{G}}$ define the same rational function if $\hat{F}G - F\hat{G} \in I(\mathcal{X})$.

Let P be a point on $\mathcal{X}$. A rational function $f \in \mathbb{F}_q(\mathcal{X})$ is called *regular* at the point P if one can find homogeneous polynomials F and G of the same degree, such that $G(P) \neq 0$ and f is in the coset of $\frac{F}{G}$. Note that, if $\mathcal{X}$ is affine, then the coordinate ring of $\mathcal{X}$ coincides with the ring of regular functions on $\mathcal{X}$; but if $\mathcal{X}$ is projective, then there are no regular functions on $\mathcal{X}$, except constant functions.

Definition 1. Let P be a $\mathbb{F}_q$-rational point of $\mathcal{X}$. The set of rational functions that are regular at P is the *local ring* $\mathcal{O}_P(\mathcal{X})$ of the point P, which is indeed a local ring in the algebraic sense. That is, it has a unique maximal ideal $\mathcal{M}_P$ which consists of the set of functions in $\mathcal{O}_P(\mathcal{X})$ that are zero in P. The factor ring $\mathbb{F}_P = \mathcal{O}_P(\mathcal{X})/\mathcal{M}_P$ is a field called the *residue class field* of P which can be identified with the field of constants $\mathbb{F}_q$. Note that, if $f \in \mathcal{O}_P(\mathcal{X})$, then its coset modulo $\mathcal{M}_P$ is in $\mathbb{F}_q$ and it is called the *value* or *evaluation* of f at P, denoted by $f(P)$.

Moreover, the maximal ideal $\mathcal{M}_P$ is a principal ideal domain. That is to say, $\mathcal{M}_P$ has one generator. See (Høholdt et al., 1998) for more details. Let p be a generator of $\mathcal{M}_P$, called *local parameter* or *prime element* in P. Then, we can write every nonzero rational function $f \in \mathbb{F}_q(\mathcal{X})$ in a unique way as $f = up^m$ where u is a unit of $\mathcal{O}_P(\mathcal{X})$ and $m \in \mathbb{Z}_{\geq 0}$. The integer m does not depend on the chosen local parameter but only on the rational function f and the point P; and it is called the *valuation* of f at P, denoted by $\mathrm{v}_P(f)$. If $\mathrm{v}_P(f) = m > 0$, then P is a *zero* of f of multiplicity (or order) m and if $\mathrm{v}_P(f) = m < 0$, then P is a *pole* of f of order $-m$. We use the convention $\mathrm{v}_P(0) = \infty$. It is easily checked that the map $\mathrm{v}_P : \mathbb{F}_q(\mathcal{X}) \longrightarrow \mathbb{Z}$ satisfies the following properties:

(1) $\mathrm{v}_P(fg) = \mathrm{v}_P(f) + \mathrm{v}_P(g)$.
(2) $\mathrm{v}_P(f + g) \geq \min\{\mathrm{v}_P(f), \mathrm{v}_P(g)\}$.
(3) $\mathrm{v}_P(\lambda f) = \mathrm{v}_P(f)$ for all nonzero $\lambda \in \mathbb{F}_q$.
(4) $\mathrm{v}_P(f) = \infty$ if and only if $f = 0$.

An $\mathbb{F}_q$-rational point corresponds to a place of degree one. More generally, if P is a *place*, then the residue class field of P, denoted by $\mathbb{F}_P$, is a finite extension of the field of constants $\mathbb{F}_q$. The degree of this extension is called the *degree of the place*. If f is regular at P, then $f(P)$, the value f at P, is in $\mathbb{F}_P$, see (Stichtenoth, 2009).

Remark 2. . Let $\mathcal{X}$ be a nonsingular projective curve in $\mathbb{P}^r$ and defined over $\mathbb{F}_q$. Let P be a $\mathbb{F}_q$-rational point of $\mathcal{X}$. Let $\mathcal{L}$ be the tangent line of $\mathcal{X}$ at P. Let h be a homogeneous linear function such that $h = 0$ defines the hyperplane $\mathcal{H}$. Note that the intersection multiplicity of $\mathcal{H}$ with $\mathcal{X}$ at P is at least one if and only if P lies in $\mathcal{H}$, and is at least two if and only if $\mathcal{L}$ lies in $\mathcal{H}$. Therefore, in order to get a local parameter at P one proceeds as follows. Let h_1 and h_2 be two homogeneous linear functions that define the hyperplanes $\mathcal{H}_1$ and $\mathcal{H}_2$, respectively. Suppose that P is in $\mathcal{H}_1$ but $\mathcal{H}_1$ does not contain $\mathcal{L}$, and P is not in $\mathcal{H}_2$. Then $p = \frac{h_1}{h_2}$ is a local parameter of $\mathcal{X}$ at P.

Definition 3. A *divisor* D on $\mathcal{X}$ is a formal finite sum $D = \sum_{P\in\mathcal{X}} n_P P$ with $n_P \in \mathbb{Z}$. If all coefficients n_P are nonnegative, D is called an *effective* divisor, denoted by $D \geq 0$. The *support* $\mathrm{supp}(D)$ of a divisor D is the set $\{P \mid n_P \neq 0\}$. The *degree* $\deg(D)$ of a divisor D is the integer $\sum_{P\in\mathcal{X}} n_P$.

Let $f \in \mathbb{F}_q(\mathcal{X})$ be an arbitrary nonzero rational function. Define the divisor of f, denoted by (f), by

$$(f) = \sum_{P\in\mathcal{X}} v_P(f)P = (f)_0 + (f)_\infty$$

where

$$(f)_0 = \textstyle\sum_{P \text{ zero of } f} \mathrm{v}_P(f)P \quad \text{and} \quad (f)_\infty = \sum_{P \text{ pole of } f} \mathrm{v}_P(f)P\,.$$

Therefore, (f) should be thought of as "the zeros of f minus the poles of f". The divisor of a rational function is called a *principal divisor*. Note that the degree of a principal divisor is zero, since it is the difference of two intersection divisors of the same degree.

Two divisors D and E on a curve are called *rational equivalent* if there exists a rational function f on $\mathcal{X}$ such that $E = D + (f)$, this is denoted by $D \equiv E$. Moreover, the divisors D and E on a curve with disjoint support with $\mathcal{P} = (P_1, \ldots, P_n)$ are called *rational equivalent with respect to* $\mathcal{P}$, and denoted by $D \equiv_{\mathcal{P}} E$, if there exists a rational function f such that f has no poles at the points of $\mathcal{P}$, $E = D + (f)$ and $f(P_j) = 1$ for $j = 1, \ldots, n$.

We define the space of rational functions associated to the divisor D by

$$\mathcal{L}(D) = \left\{ f \in \mathbb{F}_q(\mathcal{X}) \mid f = 0 \text{ or } (f) + D \geq 0 \right\}.$$

Let $\mathcal{P} = (P_1, \ldots, P_n)$ be an n-tuple of mutually distinct $\mathbb{F}_q$-rational points of $\mathcal{X}$ and let $P = P_1 + \cdots + P_n$ be the divisor whose support is the complete set of points of $\mathcal{P}$. Let E be a divisor of $\mathcal{X}$ with disjoint support from P, then the following evaluation map

$$\mathrm{ev}_{\mathcal{P}} : \mathcal{L}(E) \longrightarrow \mathbb{F}_q^n$$

is well defined by $\mathrm{ev}_{\mathcal{P}}(f) = (f(P_1), \ldots, f(P_n))$. Indeed, let f be a nonzero element of $\mathcal{L}(E)$, that is, $(f) \geq -E$, if P_j is not in the support of E, then $\mathrm{v}_{P_j}(f) \geq 0$ and f is regular at P_j, so $f(P_j)$, the value of f at P_j, is well defined.

Definition 4. Let $\mathcal{X}$ be an absolutely irreducible nonsingular projective curve over $\mathbb{F}_q$ of genus g. Let $\mathcal{P} = (P_1, \ldots, P_n)$ be an n-tuple of mutually distinct $\mathbb{F}_q$-rational points of $\mathcal{X}$ and let E be a divisor of $\mathcal{X}$ of degree m with disjoint support from $P = P_1 + \cdots + P_n$. Then, the *algebraic geometry* (AG) code $C_L(\mathcal{X}, \mathcal{P}, E)$ of length n over $\mathbb{F}_q$ is the image of $\mathcal{L}(E)$ under the evaluation map $\mathrm{ev}_{\mathcal{P}}$.

Note that, if $\{f_1, \ldots, f_k\}$ is a basis for $\mathcal{L}(E)$, then the $k \times n$ matrix G with entries $f_i(P_j)$ for $i = 1, \ldots, k$, $j = 1, \ldots, n$ is a generator matrix of the code $C_L(\mathcal{X}, \mathcal{P}, E)$.

The parameters of this code satisfy the following bounds:

Theorem 5. *If $2g-2 < m < n$, then $C_L(\mathcal{X},\mathcal{P},E)$ has dimension $m+1-g$ and minimum distance at least $n-m$.*

Proof. This is a classical result. See (Goppa, 1977; Høholdt et al., 1998; Tsfasman and Vlăduţ, 1991) and in particular (Stichtenoth, 2009, Theorem 2.2.2). □

Remark 6. Recall that the codes C and D are called *generalized equivalent if there exist a permutation matrix P and a diagonal matrix M with nonzero entries on the diagonal such that $PM(C) = D$. The* codes C and D are called *scalar equivalent* (Márquez-Corbella et al., 2012, Definition 2) if there exists a diagonal matrix M with nonzero entries on the diagonal such that $M(C) = D$. There is an easy and efficient way to find such a diagonal matrix if the generators matrices of two scalar equivalent codes are given. Furthermore, if the codes C and D are scalar equivalent, and C has an efficient decoding algorithm, then this algorithm is easily and efficiently transformed in an efficient decoding algorithm for D.

Definition 7. Two representations $(\mathcal{X},\mathcal{P},E)$ and $(\mathcal{Y},\mathcal{Q},F)$ are called *equivalent* or *isomorphic* if there is an isomorphism of curves $\varphi : \mathcal{X} \longrightarrow \mathcal{Y}$ such that $\varphi(\mathcal{P}) = \mathcal{Q}$ and $\varphi(E) \equiv F$. This isomorphism φ is called *strict* if $\varphi(E) \equiv_{\mathcal{Q}} F$.

Proposition 8. *Let $(\mathcal{X},\mathcal{P},E)$ and $(\mathcal{Y},\mathcal{Q},F)$ be two representation triples of the algebraic-geometric codes $\mathcal{C}$ and $\mathcal{D}$, respectively. Then:*
(1) If $(\mathcal{X},\mathcal{P},E)$ and $(\mathcal{Y},\mathcal{Q},F)$ are equivalent, then $\mathcal{C}$ and $\mathcal{D}$ are scalar equivalent.
(2) If $(\mathcal{X},\mathcal{P},E)$ and $(\mathcal{Y},\mathcal{Q},F)$ are strict equivalent, then $\mathcal{C} = \mathcal{D}$.

Proof. See (Márquez-Corbella et al., 2012, Proposition 4). □

Definition 9. A code C over $\mathbb{F}_q$ is called *very strong algebraic-geometric* (VSAG) if C is an AG code represented by a triple $(\mathcal{X},\mathcal{P},E)$ where the curve $\mathcal{X}$ over $\mathbb{F}_q$ has genus g, $\mathcal{P}$ consists of n points and E has degree m such that

$$2g+2 \le m < \tfrac{1}{2}n \quad \text{or} \quad \tfrac{1}{2}n + 2g - 2 < m \le n-4.$$

Remark 10. The dimension of such a code is $k = m+1-g$, thus the dimension satisfies the following bounds

$$g+3 \le k < \tfrac{1}{2}n - g + 1 \quad \text{or} \quad \tfrac{1}{2}n + g - 1 < k \le n-g-3.$$

Note that if a code has a VSAG representation then its dual is also VSAG. Therefore by duality we may just assume that $2g+2 \le m < \frac{1}{2}n$.

From now on, let $\mathcal{X}$ be an irreducible nonsingular projective curve in $\mathbb{P}^r$ and defined over $\mathbb{F}_q$ of degree l. Recall that the degree of a projective curve is the maximal number of points in the intersection with a hyperplane not containing the curve. Let R_d be the subspace of $R = \mathbb{F}_q[\mathbf{X}]/I(\mathcal{X})$ given by cosets modulo $I(\mathcal{X})$ of homogeneous polynomials of degree d. Then, R is a graded $\mathbb{F}_q$-algebra with R_d as its graded part of degree d. Let f and g be homogeneous polynomials of degree d that are not in $I(\mathcal{X})$. Therefore, its cosets are in R_d and $f = 0$ and $g = 0$ define hypersurfaces $\mathcal{Y}$ and $\mathcal{Z}$, respectively of degree d in $\mathbb{P}^r$ such that $\mathcal{X}$ is not contained neither

in $\mathcal{Y}$ nor in $\mathcal{Z}$. By Bézout Theorem, the intersections $\mathcal{X} \cdot \mathcal{Y}$ and $\mathcal{X} \cdot \mathcal{Z}$, where multiplicities are counted, are divisors on $\mathcal{X}$ of degree ld and f/g is a rational function on $\mathcal{X}$ with principal divisor

$$\left(\tfrac{f}{g}\right) = \mathcal{X} \cdot \mathcal{Y} - \mathcal{X} \cdot \mathcal{Z}.$$

In particular, if h is a homogeneous linear polynomial, then $h = 0$ defines a hyperplane $\mathcal{H}$. After a change of coordinates we may assume that $h = X_0$. Then, the complement of this hyperplane is the affine space $\mathbb{A}^r$ and the points in this complement have coordinates $(1 : x_1 : \cdots : x_r)$. Let $x_i = X_i/X_0$. Then the coordinate ring of $\mathbb{A}^r$ is $\mathbb{F}_q[x_1, \ldots, x_r]$. Furthermore $\mathcal{X}_0 = \mathcal{X} \setminus \mathcal{H}$ is an affine curve in $\mathbb{A}^r$ and its vanishing ideal is given by

$$I(\mathcal{X}_0) = \{f(1, x_1, \ldots, x_r) \mid f(X_0 : X_1 : \ldots : X_r) \in I(\mathcal{X})\}.$$

This vanishing ideal is a prime ideal and its factor ring $\mathbb{F}_q[x_1, \ldots, x_r]/I(\mathcal{X}_0)$, is an integral domain and it is called the *coordinate ring* of $\mathcal{X}_0$ and is denoted by $\mathbb{F}_q[\mathcal{X}_0]$. Its field of fractions is isomorphic to the field of rational functions of $\mathcal{X}$:

$$\mathbb{F}_q(\mathcal{X}) \simeq \mathbb{Q}(\mathbb{F}_q[\mathcal{X}_0]).$$

2.1. How to proceed when the n-tuple $\mathcal{P}$ does not meet all the "normal" conditions?

Remark 11. Let $\mathcal{P}$ be an n-tuple of mutually distinct $\mathbb{F}_q$-rational points of $\mathcal{X}$. It is convenient and usually assumed in the definition of the AG code $C_L(\mathcal{X}, \mathcal{P}, E)$ that the affine description of $\mathcal{X}_0 = \mathcal{X} \setminus \mathcal{H}$ of the projective curve $\mathcal{X}$ is given and that the n-tuple $\mathcal{P}$ is disjoint from the hyperplane $\mathcal{H}$, so that it lies in the affine curve $\mathcal{X}_0$.

However, it might be difficult to find a hyperplane that is disjoint from $\mathcal{P}$, or even that all hyperplanes that are defined over $\mathbb{F}_q$ have a nonempty intersection with $\mathcal{P}$. One can remedy this by taking an extension of $\mathbb{F}_q$, as we will see in Example 22. But then, the code is defined over this extension and no longer over $\mathbb{F}_q$ itself. Alternatively, for every point P_j of $\mathcal{P}$ there exists a hyperplane $\mathcal{H}_j$ over $\mathbb{F}_q$ that is disjoint from P_j, and one considers P_j in the affine curve $\mathcal{X} \setminus \mathcal{H}_j$ for every j separately.

Remark 12. Furthermore, it is usually assumed that $\mathcal{P} = (P_1, \ldots, P_n)$ is disjoint from the support of the divisor E. This assumption is convenient but not really necessary as we will see in the following lines. See (Tsfasman and Vlăduţ, 1991, Chap. 3.1, p. 271) for further details.

Suppose the divisor E is given by the formal sum $E = \sum m_Q Q$, and let f be a nonzero element of $\mathcal{L}(E)$, then $(f) \geq -E$, that is, $\mathrm{v}_Q(f) \geq -m_Q$ for all places Q. If $P = P_1 + \ldots + P_n$ is not disjoint from E, then $P_j = Q$ for some place with $m_Q \neq 0$. Let p_j be a local parameter at P_j. Then,

$$\mathrm{v}_{P_j}\left(p_j^{m_q} f\right) = m_q + \mathrm{v}_{P_j}(f) \geq 0,$$

that is, $p_j^{m_Q} f$ is regular at P_j. The value of f at P_j is now defined by the value of $p_j^{m_Q} f$.

Note that this definition depends not only on the P_j's but also on the divisor E and the choice of the local parameter p_j at P_j. Let $\hat{p}_j$ be another local parameter at P_j, then the evaluation f at P_j with respect to $\hat{p}_j$ is the nonzero scalar $(\hat{p}_j/p_j)^{m_Q}$ times the evaluation f at P_j with respect to p_j. Let $\mathbf{p} = (p_1, \ldots, p_n)$ be an n-tuple, where p_j is a local parameter at P_j. In this way the evaluation map

$$\mathrm{ev}_{\mathbf{p},E} : \mathcal{L}(E) \longrightarrow \mathbb{F}_q^n$$

is generalized to an arbitrary divisor E, that is without assuming that the support of E is disjoint from $\mathcal{P}$. The algebraic geometry code $C_L(\mathcal{X}, \mathbf{p}, E)$ constructed using the triple $(\mathcal{X}, \mathbf{p}, E)$ is the image of $\mathcal{L}(E)$ under the evaluation map $\mathrm{ev}_{\mathbf{p},E}$.

Remark 13. From Remarks 6 and 12 we conclude that if $\mathbf{p}$ and $\hat{\mathbf{p}}$ are two n-tuples such that p_j and $\hat{p}_j$ are local parameters of P_j for all j, then $C_L(\mathcal{X}, \hat{\mathbf{p}}, E)$ is scalar equivalent with $C_L(\mathcal{X}, \mathbf{p}, E)$. Hence we have shown that the code $C_L(\mathcal{X}, \mathcal{P}, E)$ is well defined up to scalar equivalence, even if $\mathcal{P}$ is not disjoint from the support of E.

The second way to deal with this problem is to take a rational function f such that the support of $E + (f)$ is disjoint from $\mathcal{P}$. See (Pellikaan et al., 1991, Remark 20). The existence of such a function is assured by the Approximation Theorem (Stichtenoth, 2009, I.6.4). Then the code $C_L(\mathcal{X}, \mathcal{P}, E + (f))$ is well defined. If we take another rational function f' such that the support of $E + (f')$ is disjoint from $\mathcal{P}$, then f'/f is regular at P_j and $\lambda_j = (f'/f)(P_j) \neq 0$ for all j. Therefore the codes $C_L(\mathcal{X}, \mathcal{P}, E + (f))$ and $C_L(\mathcal{X}, \mathcal{P}, E + (f'))$ are both well defined and scalar equivalent with diagonal matrix whose diagonal entries are $(\lambda_1, \ldots, \lambda_n)$.

The connection between the two approaches is as follows. Let p_j be a local parameter at P_j and $E = \sum m_Q Q$. Let

$$f = \prod_{P_j = Q} p_j^{m_Q}.$$

If p_i is regular at P_j and not zero for all $i \neq j$, then the support of $E + (f)$ is disjoint from $\mathcal{P}$ and

$$C_L(\mathcal{X}, \mathcal{P}, E + (f)) = C_L(\mathcal{X}, \mathbf{p}, E).$$

Example 14. This is treated in (Pellikaan et al., 1991, Remark 26). Consider the projective plane curve $\mathcal{X}$ over $\mathbb{F}_2$ of genus 3 given by the nonsingular equation:

$$X_1X_2(X_1 + X_2)(X_1 + X_0) + X_1X_0^2(X_1 + X_0) + X_2^2X_0(X_2 + X_0) = 0.$$

Then this curve has the 7 points of the Fano plane $\mathbb{P}^2(\mathbb{F}_2)$ as its $\mathbb{F}_2$-rational points. Let $\mathcal{P}$ be the 7-tuple of these rational points. The 7 points and the 7 lines of the Fano plane and the intersection divisors of these lines with the curve are given in Table 1.

i	P_i	$\mathcal{L}_i$	$\mathcal{L}_i \cdot \mathcal{X}$
1	(1:0:0)	$X_1 = 0$	$2P_1 + P_2 + P_3$
2	(0:0:1)	$X_0 = 0$	$2P_2 + P_4 + P_6$
3	(1:0:1)	$X_0 + X_2 = 0$	$2P_3 + P_4 + P_7$
4	(0:1:0)	$X_2 = 0$	$P_1 + 2P_4 + P_5$
5	(1:1:0)	$X_0 + X_1 = 0$	$P_2 + 2P_5 + P_7$
6	(0:1:1)	$X_0 + X_1 + X_2 = 0$	$P_3 + P_5 + 2P_6$
7	(1:1:1)	$X_1 + X_2 = 0$	$P_1 + P_6 + 2P_7$

Table 1. The 7 points and the 7 lines of the Fano plane with the intersection divisors of Example 14.

All these 7 lines intersect $\mathcal{X}$ in 3 points. So there is no line defined over $\mathbb{F}_2$ that is disjoint from $\mathcal{X}$. The affine equation of the curve that is in the complement of the line $\mathcal{L}_2$ with equation $X_0 = 0$ is given by

$$x_1x_2(x_1 + x_2)(x_1 + 1) + x_1(x_1 + 1) + x_2^2(x_2 + 1) = 0,$$

with affine coordinates $x_1 = X_1/X_0$ and $x_2 = X_2/X_0$. Then, the points P_2, P_4 and P_6 lie on the line $\mathcal{L}_2$ at "infinity". The points P_1, P_3, P_5 and P_7 lie in the affine part of the curve and have affine

coordinates $(0,0)$, $(0,1)$, $(1,0)$ and $(1,1)$, respectively. Define

$$E = \mathcal{L}_2 \cdot \mathcal{X} = 2P_2 + P_4 + P_6.$$

Then E is a canonical divisor and the divisors of X_1/X_0 and X_2/X_0 are given by

$$\left(\tfrac{X_1}{X_0}\right) = \mathcal{L}_1 \cdot \mathcal{X} - \mathcal{L}_2 \cdot \mathcal{X} = 2P_1 + P_3 - P_2 - P_4 - P_6$$

and

$$\left(\tfrac{X_2}{X_0}\right) = \mathcal{L}_4 \cdot \mathcal{X} - \mathcal{L}_2 \cdot \mathcal{X} = P_1 + P_4 + P_5 - 2P_2 - P_6.$$

So the functions $f_0 = 1$, $f_1 = X_1/X_0$ and $f_2 = X_2/X_0$ are elements of $\mathcal{L}(E)$ and $l(E) = g = 3$. Hence, f_0, f_1 and f_2 form a basis of $\mathcal{L}(E)$. These functions are easily evaluated at the points P_1, P_3, P_5 and P_7 (see Table 2), since they have affine coordinates $(x_1, x_2) = (0,0)$, $(0,1)$, $(1,0)$ and $(1,1)$, respectively.

$\mathrm{ev}_{\mathbf{p},E}$	P_1	P_3	P_5	P_7
$f_0 = 1$	1	1	1	1
$f_1 = x_1$	0	0	1	1
$f_2 = x_2$	0	1	0	1

Table 2. Evaluation of f_0, f_1 and f_2 at the points P_1, P_3, P_5 and P_7.

We need to find local parameters at P_2, P_4 and P_6 to evaluate those functions at these three points. By Remark 11, the points P_4 and P_6 lie on the affine chart $\mathcal{U}_1$, where $\mathcal{U}_1$ is complement of the hyperplane $\mathcal{H}_1$ with equation $\mathcal{X}_1 = 0$. Then, the affine curve $\mathcal{X}_1 = \mathcal{X} \setminus \mathcal{H}_1 = \mathcal{X} \cap \mathcal{U}_1$ has affine equation

$$x_2(1 + x_2)(1 + x_0) + x_0^2(1 + x_0) + x_2^2 x_0(x_2 + x_0) = 0,$$

with affine coordinates $x_0 = X_0/X_1$ and $x_2 = X_2/X_1$. The basis of $\mathcal{L}(E)$ has in these coordinates the form $f_0 = 1$, $f_1 = X_1/X_0 = 1/x_0$ and $f_2 = X_2/X_0 = x_2/x_0$. Using Remark 2, we see that $p_1 = X_0/X_1$ is a local parameter at P_4 and P_6. See Table 3.

$\mathrm{ev}_{\mathbf{p},E}$	P_4	P_6
$p_1 f_0 = x_0$	0	0
$p_1 f_1 = 1$	1	1
$p_1 f_2 = x_2$	0	1

Table 3. Evaluation of f_0, f_1 and f_2 at the points P_4 and P_6.

Now $p_2 = X_1/X_2$ is a local parameter at P_2, but the multiplicity of E at P_2 is 2. So we have to evaluate $p_2^2 f_0 = X_1^2/X_2^2$, $p_2^2 f_1 = X_1^3/X_0X_2^2$ and $p_2^2 f_2 = X_1^2/X_0X_2$ at P_2. The divisors of these functions are given by

$$\begin{aligned}
\left(\tfrac{X_1^2}{X_2^2}\right) &= 2P_1 + 2P_2 + 2P_3 - 4P_4 - 2P_5, \\
\left(\tfrac{X_1^3}{X_0X_2^2}\right) &= 4P_1 + P_2 + 2P_3 - 5P_4 - P_5 - P_6, \\
\left(\tfrac{X_1^2}{X_0X_2}\right) &= 3P_1 + P_3 - 3P_4 - P_6.
\end{aligned}$$

Thus, $p_2^2 f_0$, $p_2^2 f_1$ and $p_2^2 f_2$ are regular at P_2 and

$$p_2^2 f_0(P_2) = 0,\ p_2^2 f_1(P_2) = 0 \ \text{ and } \ p_2^2 f_2(P_2) \neq 0\,.$$

The only option for $p_2^2 f_2(P_2)$ is 1, since the value is binary and not zero. See Table 4.

$\mathrm{ev}_{\mathbf{p},E}$	P_2
$p_2^2 f_0 = x_1^2$	0
$p_2^2 f_1 = x_1^3/x_0$	0
$p_2^2 f_2 = x_1^2/x_0$	1

Table 4. Evaluation of f_0, f_1 and f_2 at the point P_2.

Therefore the code $C_L(\mathcal{X}, \mathbf{p}, E)$ has generator matrix

$$G = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \end{pmatrix} \in \mathbb{F}_2^{3\times 7}.$$

Remark 15. We mention the following papers that are devoted to the construction of the Riemann-Roch space $\mathcal{L}(E)$ using the theory of Brill-Noether and Coates and the construction of AG codes by (Gorenstein, 1952), (Le Brigand, 1986b,a; Le Brigand and Risler, 1988), (Duval, 1987, 1989), (Huang and Ierardi, 1994), (Hoeij, 1994, 1997), (Laursen, 1997a,b), (Matsumoto and Miura, 2000) and (Hess, 1999, 2002). Computer algebra packages are developed for Axiom by (Haché, 1995; Haché and Le Brigand, 1995; Haché, 1996, 1998), for Magma by (Pecquet and Wocjan, 2000; Pecquet, 2001; Wocjan, 1999) and for Singular by (Campillo and Farrán, 2002, 2004).

3. Retrieving the genus and the degree of the divisor

Let $\mathcal{X}$ be a curve over the perfect field $\mathbb{F}$ of genus g. Let E be a divisor on $\mathcal{X}$. Let $\mathcal{L}(E)^{(d)}$ be the vector space generated by d-fold products of elements in $\mathcal{L}(E)$, that is generated by $f_1 \cdots f_d$, with $f_1, \ldots, f_d \in \mathcal{L}(E)$. Let C be a linear code in $\mathbb{F}_q^n$. Then $C^{(d)}$ is the subcode of $\mathbb{F}_q^n$ that is generated by $\mathbf{c}_1 * \cdots * \mathbf{c}_d$, with $\mathbf{c}_1, \ldots, \mathbf{c}_d \in C$, where $*$ is the component-wise or Schur product of $\mathbb{F}_q^n$. See (Cascudo et al., 2009, §4 Definition 6) and (Wieschebrink, 2010; Márquez-Corbella et al., 2012).

We consider $C^{(2)}$, for retrieving the genus and the degree m of the divisor. We shall use the following results.

Proposition 16. *Let $\mathcal{X}$ be a curve over the perfect field $\mathbb{F}$ of genus g. Let E be a divisor on $\mathcal{X}$ of degree m. If $m \geq 2g+1$ and $d \geq 1$, then*

$$\mathcal{L}(E)^{(d)} = \mathcal{L}(dE).$$

Proof. See (Mumford, 1970; Saint-Donat, 1972). In case E is a canonical divisor on a non-hyperelliptic curve this is called the Theorem of Max Noether-Enriques-Petri. See (Noether, 1880; Saint-Donat, 1973), (Griffiths and Harris, 1978, Chap. 2 §3) and (Schreyer, 1991, Theorem 1.2). □

Corollary 17. *Let $\mathcal{X}$ be a curve over $\mathbb{F}_q$ of genus g. Let E be a divisor on $\mathcal{X}$ of degree m. Let $C = C_L(\mathcal{X}, \mathcal{P}, E)$. If $m \geq 2g + 1$ and $d \geq 1$, then*

$$C^{(d)} = C_L(\mathcal{X}, \mathcal{P}, dE).$$

Proof. Notice that $C_L(\mathcal{X}, \mathcal{P}, E)^{(d)} = \mathrm{ev}_{\mathcal{P}}(\mathcal{L}(E)^{(d)})$, since $\mathrm{ev}_{\mathcal{P}}(fg) = \mathrm{ev}_{\mathcal{P}}(f) * \mathrm{ev}_{\mathcal{P}}(g)$ for all f, g in $\mathcal{L}(E)$. Now this corollary is a direct consequence of Proposition 16. □

Proposition 18. *Let C be an AG code represented by the triple $(\mathcal{X}, \mathcal{P}, E)$. Let g denote the genus of the algebraic curve $\mathcal{X}$ and let m be the degree of the divisor E. Let k_1 and k_2 be the dimension of C and $C^{(2)}$, respectively. If $2g + 1 \leq m < \frac{1}{2}n$, then*

$$m = k_2 - k_1 \ \text{ and } \ g = k_2 - 2k_1 + 1.$$

Proof. Let $(\mathcal{X}, \mathcal{P}, E)$ be a representation of C. Assume that $2g + 2 \leq m < \frac{1}{2}n$. Then $C^{(d)} = C_L(\mathcal{X}, \mathcal{P}, dE)$ for all d by Corollary 17. So $k_1 = m - g + 1$ and $k_2 = 2m - g + 1$, since $\deg(dE) < n$ for $d = 1$ and $d = 2$. Hence $k_2 - k_1 = m$ and $k_2 - 2k_1 + 1 = g$. □

Therefore any attacker, knowing a generator matrix $G \in \mathbb{F}_q^{k_1 \times n}$ of a VSAG code C, will be able to obtain the values of m and g, since by duality we may assume that $2g + 2 \leq m < \frac{1}{2}n$.

4. Computing the triple $(\mathcal{Y}, \mathbf{q}, F)$

Suppose that we are using algebraic geometry codes in the McEleice public key cryptosystem. In the following we make a distinction in notation between the *secret key* $(\mathcal{X}, \mathbf{p}, E)$ and the triple $(\mathcal{Y}, \mathbf{q}, F)$ that will be obtained from the *public key*, that is a generator matrix G of the code $C_L(\mathcal{X}, \mathbf{p}, E)$. Now $\mathcal{X}$ is a projective curve of genus g in $\mathbb{P}^r$ and defined over $\mathbb{F}_q$, $\mathcal{P}$ is an n-tuple of mutually distinct $\mathbb{F}_q$-rational points of $\mathcal{X}$ and E is a divisor of $\mathcal{X}$ of degree m. Let $I(\mathcal{X})$ be the homogeneous vanishing ideal of $\mathcal{X}$ in the polynomial ring $\mathbb{F}_q[X_0, X_1, \ldots, X_r]$ with factor ring $R = \mathbb{F}_q[X_0, X_1, \ldots, X_r]/I(\mathcal{X})$.

In (Márquez-Corbella et al., 2012) the authors address the question of retrieving a triple $(\mathcal{Y}, \mathcal{Q}, F)$ that is isomorphic to the triple $(\mathcal{X}, \mathcal{P}, E)$ from a given $k \times n$ generator matrix G of a very strong algebraic geometry (VSAG) code $C_L(\mathcal{X}, \mathcal{P}, E)$, see definition 9. Then, the dimension k of this code is $m+1-g$. By duality we may, from now on, assume that $2g+2 \leq m < \frac{1}{2}n$. Let $s = k - 1$, take the columns of G as homogeneous coordinates of points in $\mathbb{P}^s(\mathbb{F}_q)$, this gives the associated projective system $\mathcal{Q} = (Q_1, \ldots, Q_n)$. By (Márquez-Corbella et al., 2012, Proposition 7) there exists an embedding of the curve $\mathcal{X}$ in $\mathbb{P}^s$ of degree m

$$\begin{aligned} \varphi_E : \mathcal{X} &\longrightarrow \mathbb{P}^s \\ P &\longmapsto \varphi_E(P) = (f_0(P), \ldots, f_s(P)) \end{aligned}$$

where $\{f_0, \ldots, f_s\}$ is a basis of $\mathcal{L}(E)$ such that $\mathcal{X}$ is isomorphic to the curve $\mathcal{Y} = \varphi_E(\mathcal{X})$ in $\mathbb{P}^s$ of degree m that is defined over $\mathbb{F}_q$. Now $\mathcal{Q} = \varphi_E(\mathcal{P})$ is an n-tuple of mutually distinct $\mathbb{F}_q$-rational points of $\mathcal{Y}$. And $\varphi_E(E) \equiv \mathcal{Y} \cdot \mathcal{H}$ for all hyperplanes $\mathcal{H}$ of $\mathbb{P}^s$, see (Hirschfeld et al., 2008, Theorems 7.33 and 7.40). Moreover, if E is effective, then $\varphi_E(E) = \mathcal{Y} \cdot \mathcal{H}$ for some hyperplane $\mathcal{H}$ and if $F = \varphi_E(E)$, then $(\mathcal{Y}, \mathcal{Q}, F)$ is also a representation of the code C which is strict isomorphic to the original triple $(\mathcal{X}, \mathcal{P}, E)$.

In fact any hyperplane $\mathcal{H}$ outside the points of Q will do. But sometimes there is no such hyperplane. In order to meet with this problem, the construction of the AG code, $C_L(\mathcal{X}, \mathcal{P}, E)$, is generalized to the code $C_L(\mathcal{X}, \mathbf{p}, E)$ in Section 2, where $\mathbf{p}$ is an n-tuple of local parameters at the points of $\mathcal{P}$. Now it is allowed that the hyperplane $\mathcal{H}$ and the divisor F have a nonempty intersection with Q. The triple $(\mathcal{Y}, \mathbf{q}, F)$ is called *isomorphic* with $(\mathcal{X}, \mathbf{p}, E)$ if φ_E gives an isomorphism of curves from $\mathcal{X}$ to $\mathcal{Y}$, $\varphi_E(E) \equiv F$ and p_j and $\varphi^*(q_j)$ are local parameters at the same point for all j. If $(\mathcal{Y}, \mathbf{q}, F)$ is isomorphic to $(\mathcal{X}, \mathbf{p}, E)$, then $C_L(\mathcal{Y}, \mathbf{q}, F)$ is scalar equivalent with $C_L(\mathcal{X}, \mathbf{p}, E)$.

Let $I(\mathcal{Y})$ be the homogeneous vanishing ideal of $\mathcal{Y}$ in the polynomial ring $\mathbb{F}_q[Y_0, Y_1, \ldots, Y_s]$ with factor ring $S = \mathbb{F}_q[Y_0, Y_1, \ldots, Y_s]/I(\mathcal{Y})$.

Remark 19. What is meant by: "to compute efficiently the triple $(\mathcal{Y}, \mathbf{q}, F)$"?
Suppose we have as input the generator matrix G of the VSAG code $C = C_L(\mathcal{X}, \mathbf{p}, E)$.
Then as output we ask for:

(1) An l-tuple $\mathcal{G} = (g_1, \ldots, g_l)$ of polynomials in $\mathbb{F}_q[Y_0, Y_1, \ldots, Y_s]$ that generates $I(\mathcal{Y})$.
(2) An n-tuple $\mathbf{q}$ where q_j is a local parameter of Q_j for all $j = 1, \ldots, n$.
(3) The triple $(\mathcal{X}, \mathbf{p}, E)$ is isomorphic to $(\mathcal{Y}, \mathbf{q}, F)$, where $\mathcal{H}$ is a hyperplane of $\mathbb{P}^s(\mathbb{F}_q)$,
(4) A Gröbner basis $\mathcal{F}$ of the vanishing ideal of $F = \mathcal{Y} \cdot \mathcal{H}$,
(5) A basis $\mathcal{B}$ of the vector space $\mathcal{L}(F)$,
(6) The complexity of obtaining the quadruple $(\mathcal{G}, \mathbf{q}, \mathcal{F}, \mathcal{B})$ is polynomial in n.

A stronger version of (1) is given by:

(1') A Gröbner basis $\mathcal{G}$ of $I(\mathcal{Y})$,

but we were not able to get a result for this stronger version.

4.1. Generators of the ideal $I(\mathcal{Y})$

Note that (Márquez-Corbella et al., 2012, Corollary 1) states that the construction of $I(\mathcal{Y})$ is reduced to the computation of a set of generators of $I_2(Q)$ which can be performed in $O\left(n^2\binom{s}{2}\right)$ elementary operations. Recall that $I_2(Q)$ is the ideal generated by the homogeneous elements of degree 2 in the vanishing ideal of Q. In the following lines we present a constructive proof of how to compute the set of generators of the ideal $I_2(Q)$.

Lemma 20. *Let Q be an n-tuple of points in $\mathbb{P}^s(\mathbb{F}_q)$ not in a hyperplane. An upper bound on the complexity of the computation of $I_2(Q)$ is given by $O(n^4)$.*

Proof. Let $k = s + 1$ and G_Q be the $k \times n$ matrix associated to Q and C be the subspace of $\mathbb{F}_q^n$ generated by the rows of G_Q. We enumerate the rows of G_Q by $\{\mathbf{g}_1, \ldots, \mathbf{g}_k\}$. Let $\mathcal{S}^2(C)$ be the second symmetric power of C, i.e. the symmetric tensor product of C by itself. If $x_i = \mathbf{g}_i$, then $\mathcal{S}^2(C)$ has basis $\{x_i x_j \mid 1 \leq i \leq j \leq n\}$ and dimension $\binom{k+1}{2}$. Now we consider the linear map $\sigma : \mathcal{S}^2(C) \longrightarrow C^{(2)}$ where $x_i x_j$ is mapped to $\mathbf{g}_i * \mathbf{g}_j$. We denote the kernel of this map by $K^2(C)$. By (Márquez-Corbella et al., 2012, Proposition 15), a basis of $K^2(C)$ gives directly a generating set of $I_2(Q)$. Recall that $C^{(2)}$ is generated by the elements $\left\{\mathbf{g}_i * \mathbf{g}_j \mid 1 \leq i \leq j \leq k\right\}$, which form a matrix M of size $m \times n$, where $m = \binom{k+1}{2}$. The vector space $K^2(C)$ is equal to the right kernel of M^T.

Performing Gaussian elimination by rows on M^T gives a matrix N in row reduced row echelon form. If the pivots of N are all at the left hand side, then N is of the form $(I_l|B)$ after deleting the zero rows. Then the right kernel of M^T is equal to the right kernel of $(I_l|B)$ and is generated by the rows of $(-B^T|I_{m-l})$. A similar result holds if the pivots are not all at the start.

An upper bound on the complexity of bringing M^T in reduced row echelon form is given by $O(mn \min\{m,n\})$ which is at most $O(n^3)$ if $m \leq n$ and $O(n^4)$ if $m \geq n$, since $m = O(n^2)$. □

4.2. The n-tuples $\mathcal{Q}$ and $\mathbf{q}$

Obtaining the n-tuple $\mathcal{Q}$ is trivial, since $\mathcal{Q} = (Q_1, \ldots, Q_n)$ is the projective system associated to G. So Q_j is the point in $\mathbb{P}^s(\mathbb{F}_q)$ which has as homogeneous coordinates the j-th column of G.

In order to construct a representation of the code $C = C_L(\mathcal{Y}, \mathcal{Q}, F)$ in $\mathbb{P}^s$, we need to find a local parameter q_j at Q_j for all j. Let Q be an $\mathbb{F}_q$-rational point. Let $\mathcal{L}$ be the tangent line of $\mathcal{Y}$ at Q. Let h_1 and h_2 be homogeneous linear polynomials that define the hyperplanes $\mathcal{H}_1$ and $\mathcal{H}_2$ such that Q is in $\mathcal{H}_1$, but $\mathcal{H}_1$ does not contain $\mathcal{L}$ and Q is not in $\mathcal{H}_2$. Then h_1/h_2 is a local parameter of $\mathcal{Y}$ at Q as it is explained in Remark 2.

Let the vanishing ideal $I(\mathcal{Y})$ in $\mathbb{F}_q[Y_0, Y_1, \ldots, Y_s]$ be generated by $f_1, \ldots, f_l$. Then the tangent line $\mathcal{L}$ of $\mathcal{Y}$ at $Q = (Q_0 : Q_1 : \cdots : Q_s)$ is defined by the intersection of the hyperplanes with equations

$$\sum_{i=0}^{s} \frac{\partial f_j}{\partial Y_i}(Q)(Y_i - Q_i) = 0 \text{ for } j = 1, \ldots, l.$$

After a coordinate change we may assume that $Q = (1 : 0 : \cdots : 0)$ and that the tangent line $\mathcal{L}$ is given by the equations $Y_2 = 0, \ldots, Y_s = 0$. Therefore we can take $h_1 = Y_1$ and $h_2 = Y_0$.

Let d be the maximal degree of the polynomials f_j. Then the complexity of the computation of the value of the partial derivatives $\frac{\partial f_j}{\partial Y_i}(Q)$ is upper bounded by $O(ls\binom{s+d+1}{d})$. The complexity defining the tangent line in normal form is given by $O(ls \min\{l, s\})$, since it is obtained by Gaussian elimination of a linear system of l equations in $s+1$ variables.

In the particular situation of Section 4.1 we have a $k \times n$ matrix as input. So $s = k - 1$ and $I(\mathcal{Y})$ is generated by $l = \binom{k+1}{2}$ polynomials of degree $d = 2$. Therefore $O(nk^5)$ and $O(n^6)$ are bounds for the complexity of obtaining the local parameters of all the Q_j for $j = 1, \ldots, n$, since it is dominated by the complexity of the computation of the partial derivatives.

4.3. Gröbner basis for $I(\mathcal{Y} \cdot \mathcal{H})$

Let $\mathcal{H}$ be the hyperplane given by the linear equation $g(Y) = 0$. We claim that the vanishing ideal $\mathcal{Y} \cap H$ is the sum ideal $\langle I_2(\mathcal{Y})\rangle + \langle g\rangle$. Indeed, the vanishing ideal $I(\mathcal{Y})$ is generated by polynomials of degree 2 and the result holds by (Márquez-Corbella et al., 2012, Corollary 1).

Note that the ideal $I = \langle I_2(\mathcal{Y})\rangle + \langle g\rangle$ is of projective dimension zero, that is $\mathbb{F}_q[Y_0, Y_1, ..., Y_s]/I$ is graded of Krull dimension one and thus the variety $V(I)$ consists of a finite number of projective points. (Lundqvist, 2012) has recently devised a procedure to compute the (projective) points of such type of variety. He associates an affine ring of dimension zero whose multiplication matrices coincide with the projective multiplication matrices of the projective ring.

The following is adapted from (Lundqvist, 2012, Algorithm 5.6) to our special case:

(1) First, compute the Gröbner basis elements of degree 1 and 2 of the ideal

$$I = \langle I_2(\mathcal{Y})\rangle + \langle g(X)\rangle \subseteq \mathbb{K}[Y_1, \ldots, Y_s].$$

Note that the maximal degree of the elements of the Gröbner basis of I is bounded by m that denotes the degree of the divisor F which we know in advance (see Proposition 18), since the degree of a function determines the maximum number of solutions that a function can have and $F = \mathcal{Y} \cdot \mathcal{H}$. This bound is sharp and is attained for one-point divisors using the lexicographic ordering (see for instance Example 23).

(2) If $q < m$, where m is again the degree of the divisor F, then we must enlarge our field $\mathbb{F}_q$ by a field extension $\mathbb{F}_{q^e}$ such that this extension contains at least m elements. The complexity of finding an extension $\mathbb{F}_{q^e}$ such that $q^e \geq n \geq m$, is polynomial in n. See (Shparlinski, 1993, 1999).

(3) Choose a random change of coordinates

$$\begin{cases} \hat{Y}_0 := Y_0 + a_1 Y_1 + \cdots + a_s Y_s, \\ \hat{Y}_i := Y_i \ \text{ for all } \ i = 1, \ldots, s. \end{cases}$$

such that $\hat{Y}_0$ is non zero at all points in the variety $V(I)$ over the extension field $\mathbb{F}_{q^e}$, in other words $\hat{Y}_0$ is a non-zero divisor of $F_q[Y_0, \ldots, Y_s]/I$.

Note that equivalently to stage **K3** of (Lundqvist, 2012, Algorithm 5.6) if we could not find such a change of coordinates then we go back to **Step 1** and we compute Gröbner basis elements of degree d with $d = 3, \ldots, m$ following a sequential order until we get such a non-zero divisor. Note that for the right d, for almost all changes of coordinates $\hat{Y}_0$ is a non-zero divisor. Moreover, (Lundqvist, 2012, Proposition 3.2) gives a constructive proof which directly provides an algorithm for computing a nonzero divisor.

(4) Apply the FGLM algorithm (Faugère et al., 1993) to find the rational points of the affine variety with coordinates $\hat{Y}_i/\hat{Y}_0$ for $i = 1, \ldots, s$. We suggest to use the FGLM algorithm but any other method for finding roots of an affine variety is also suitable here.

Recall that there is a one-to-one correspondence between the rational points on affine varieties defined by a zero-dimensional ideal and common eigenvectors of the so-called multiplication matrices. This step provides multiplication matrices for the affine ring. If we add to this set the identity matrix then it coincides with the projective multiplication matrices for the projective ring. This step is equivalent to the stages **K4-K6** of (Lundqvist, 2012, Algorithm 5.6).

(5) Finally, for each projective point obtained (which is defined over the extension field $\mathbb{F}_{q^e}$) apply the inverse coordinate transformation given on **Step 3** and check whether it belongs to the original defining field $\mathbb{F}_q$. This step is equivalent to the stage **K7** of (Lundqvist, 2012, Algorithm 5.6).

The overall complexity of the procedure is dominated by steps (3) and (4). Thus, the main time of the algorithm is devoted to compute Gröbner basis element of I. However, we will not suffer from explosive exponent growth since the maximal degree of elements in our Gröbner basis is bound by the degree of the divisor F.

(Lundqvist, 2012) shows that the behavior of the proposed method is asymptotically better than the classical Buchberger-Möller algorithm, see (Marinari et al., 1993). The complexity of the proposed method is at most $O\left(\min(m, s)m^3\right)$, where m is the degree of the divisor F, or equivalently the degree of the curve $\mathcal{Y}$, which is defined in the projective space $\mathbb{P}^s$, see (Lundqvist, 2012) for a detailed complexity analysis.

4.4. A basis of the vector space $\mathcal{L}(F)$

Let $g(Y)$ be the linear polynomial that defines the chosen hyperplane $\mathcal{H}$. Then the quotients $Y_i/g(Y)$ of the cosets of Y_i and $g(Y)$ in $\mathbb{F}_q[Y_0, Y_1, ..., Y_s]/I$ form a basis of $\mathcal{L}(F)$. This step is immediate and does not contribute to the complexity of obtaining the quadruple $(\mathcal{G}, \mathbf{q}, \mathcal{F}, \mathcal{B})$.

4.5. Overall complexity

Compiling the above results we can conclude the following theorem which determines the complexity of obtaining a representing triple of a VSAG code from its generator matrix.

Theorem 21. *Let G be a $k \times n$ generator matrix of a VSAG code C defined over $\mathbb{F}_q$ and Q_j be the point in $\mathbb{P}^{k-1}$ which has as homogeneous coordinates the j-th column of G for $j = 1, \ldots, n$. Then, a representing triple $(\mathcal{Y}, \mathbf{q}, F)$ of the code C or its dual, $C^\perp$, can be retrieved efficiently with complexity $O\left(n^6\right)$.*

The triple $(\mathcal{Y}, \mathbf{q}, F)$ is defined by $\mathcal{Y}$ which is a projective curve in $\mathbb{P}^{k-1}$ defined over $\mathbb{F}_q$, by the n-tuple $\mathbf{q} = (q_1, \ldots, q_n)$ such that q_j is a local parameter of Q_j for all j, and by the divisor F of the curve $\mathcal{Y}$ of degree m.

Proof. Let $s = k - 1$. Note that the construction of an l-tuple $\mathcal{G} = (g_1, \ldots, g_l)$ of polynomials in $\mathbb{F}_q[Y_0, \ldots, Y_s]$ that generates $I(\mathcal{Y})$ can be performed in $O\left(n^4\right)$ elementary operations by Lemma 20. Moreover, Section 4.2 states that the complexity of obtaining the n-tuple $\mathbf{q} = (q_1, \ldots, q_n)$ where q_j is a local parameter of Q_j for all $j = 1, \ldots, n$ is at most $O\left(n^6\right)$. Finally, a Gröbner basis of the vanishing ideal of the divisor F is at most $O\left(\min(m, s) \cdot m^3\right)$ by (Lundqvist, 2012, Algorithm 5.6). However, since C is a VSAG code then $m < \frac{1}{2}n$. Thus, $O\left(\min(m, s) \cdot m^3\right)$ is bounded by $O\left(n\left(\frac{n}{2}\right)^3\right) \sim O\left(n^4\right)$.

Therefore, in the worst case the complexity of our method is polynomial on the length of the code since it is upper bounded by $O\left(n^6\right)$. □

As a final remark, note that we have assumed by duality that $2g + 2 \leq m < \frac{1}{2}n$. Therefore, we are able to retrieve a representation for C or its dual.

The following example illustrates our method for retrieving a representation of a VSAG code C with the only knowledge of a generator matrix of C.

Example 22. Consider the curve $\mathcal{X}$ of Example 14. The line $\mathcal{L}$ with equation $X_0 = 0$ intersects the curve $\mathcal{X}$ in three points P_2, P_4 and P_6. Let us compute this set of projective points using the previous algorithm.

First note that the number of $\mathbb{F}_2$-rational points of our curve is 7 which is greater than the cardinality of the defining field. Therefore we need to enlarge the field to $\mathbb{F}_8 = \mathbb{F}_2[\alpha]$, where α is a root of $X^3 + X + 1$. Actually we only need to enlarge the field to $\mathbb{F}_4$ but let us assume that we do not know in advance the number of intersections points. Recall that, in the situation of the curve $\mathcal{Y}$ that comes from a VSAG codes, if we know a generator matrix of the code, then we know its degree by Proposition 18.

Note that the change of coordinates T defined by

$$\begin{cases} \hat{X}_0 := X_0 + \alpha X_1 + \alpha^2 X_2, \\ \hat{X}_i := X_i \text{ for } i = 1, 2. \end{cases} \tag{1}$$

verifies that $T(\hat{X}_0)(P_j) \neq 0$ for all points P_j of $\mathcal{X}$. Now the set of points of $\mathcal{X}$ becomes

$$\begin{aligned} \hat{P}_1 &= (1:0:0) & \hat{P}_5 &= (1+\alpha:1:0) \\ \hat{P}_2 &= (\alpha^2:0:1) & \hat{P}_6 &= (\alpha+\alpha^2:1:1) \\ \hat{P}_3 &= (1+\alpha^2:0:1) & \hat{P}_7 &= (1+\alpha+\alpha^2:1:1) \\ \hat{P}_4 &= (\alpha:1:0) \end{aligned}$$

Now we can take the affine equation of the curve $\mathcal{X}$ and the line $\mathcal{L}$ with affine coordinates $x_1 = \hat{X}_1/\hat{X}_0$ and $x_2 = \hat{X}_2/\hat{X}_0$:

$$\mathcal{X} : x_1x_2(x_1+x_2)(x_1+1) + x_1(x_1+1) + x_2^2(x_2+1) = 0$$
$$\text{and} \quad \mathcal{L} : 1 + \alpha x_1 + \alpha^2 x_2 = 0.$$

If we compute a Gröbner basis of the affine zero-dimensional ideal generated by the above polynomials, which could be solved by FGLM techniques we obtain

$$x_1^2(x_1+\alpha^2+1)(x_1+\alpha+1) \quad \text{and} \quad x_2 + (\alpha^2+1)x_1 + (\alpha^2+\alpha+1)$$

This gives the intersection affine points and their multiplicities: $2\hat{P}_2 + \hat{P}_4 + \hat{P}_6$, where

$$\hat{P}_2 = (0, \alpha^2+\alpha+1), \ \hat{P}_4 = (\alpha^2+1, 0) \quad \text{and} \quad \hat{P}_6 = (\alpha+1, \alpha+1).$$

Once we unmake the change of coordinates described in Equation (1) we rise to three projective points in $\mathbb{P}^3(\mathbb{F}_2)$ which correspond to the original intersection points P_2, P_4 and P_6.

5. Examples

We consider in this section several examples. These are low-dimensional examples to illustrate the complete process of recovering the triple $(\mathcal{Y}, \mathcal{Q}, F)$ from a generator matrix of a VSAG code.

Example 23. Consider the Hermitian curve $\mathcal{X}$ over $\mathbb{F}_{16}$ with homogeneous equation

$$X_1^5 - X_0X_2^4 - X_0^4X_2 = 0.$$

The affine equation of $\mathcal{X}$ is $x_1^5 - x_2^4 - x_2 = 0$ with $x_1 = X_1/X_0$ and $x_2 = X_2/X_0$. This curve has genus $g = 6$. Moreover, $\mathcal{X}$ has $Q = (0:0:1)$ as the only point at infinity and other 64 distinct $\mathbb{F}_{16}$-rational points. Let $P_1, \ldots, P_{64}$ be an enumeration of all the $\mathbb{F}_{16}$-rational points of $\mathcal{X}$ except the point at infinity Q .

If we consider a divisor of the form $E = mQ$, then the algebraic code C defined by the triple $(\mathcal{X}, \mathcal{P}, E)$ where $\mathcal{P} = \{P_1, \ldots, P_{64}\}$, has length $n = 64$ and dimension $k = m-g+1$. Let $f_{i,j} = x_1^i x_2^j$. Then a basis for the Riemann-Roch space $\mathcal{L}(E)$ is

$$\left\{ x_1^i x_2^j \mid 0 \leq i \leq 4 \text{ and } 4i + 5j \leq m \right\}.$$

Table 5 gives the basis of functions and their corresponding pole orders also called weights: For $m = 14 = 2g + 2$ we have $k = l(E) = 9$. A basis for $\mathcal{L}(E)$ is

$$\mathcal{B} = \left\{ \begin{array}{c} f_0 = 1, \ \ f_1 = x_1, \ \ f_2 = x_2, \ \ f_3 = x_1^2, \ \ f_4 = x_1x_2, \\ f_5 = x_2^2, \ \ f_6 = x_1^3, \ \ f_7 = x_1^2x_2, \ \ f_8 = x_1x_2^2 \end{array} \right\}$$

x_2^5				
x_2^4	$x_1x_2^4$			
x_2^3	$x_1x_2^3$	$x_1^2x_2^3$		
x_2^2	$x_1x_2^2$	$x_1^2x_2^2$	$x_1^3x_2^2$	$x_1^4x_2^2$
x_2	x_1x_2	$x_1^2x_2$	$x_1^3x_2$	$x_1^4x_2$
1	x_1	x_1^2	x_1^3	x_1^4

25				
20	24			
15	19	23		
10	14	18	22	26
5	9	13	17	21
0	4	8	12	16

Table 5. Basis of functions of $\mathcal{L}(E)$ and their corresponding weights.

A generator matrix G of C is by definition the matrix obtained by evaluating the functions $f_i \in \mathcal{B}$ for $i = 1, \ldots, 9$ at $\mathcal{P} = \{P_1, \ldots, P_{64}\}$, that is a generator matrix for C is given by

$$G = \begin{pmatrix} f_0(P_1) & \ldots & f_0(P_{64}) \\ \vdots & \ddots & \vdots \\ f_8(P_1) & \ldots & f_8(P_{64}) \end{pmatrix} \in \mathbb{F}_{16}^{9\times 64}.$$

The only information available to the attacker is the matrix G. Then:

- Take the columns of G as homogeneous coordinates of projective points in $\mathbb{P}^8(\mathbb{F}_{16})$. We obtain the projective system $\mathcal{Q} = (Q_1, \ldots, Q_{64})$ where Q_j is given by $\big(f_0(P_j) : \ldots : f_8(P_j)\big)$.
- Define the curve $\mathcal{Y}$ as the set of solutions of the vanishing ideal generated by the elements of $K_2(C)$. Since $\frac{1}{2}n \geq m \geq 2g + 2$ (Márquez-Corbella et al., 2012, Proposition 15) states that a generator set of $I(\mathcal{Y})$ is generated by the following set of quadrics in $\mathbb{F}_{16}[Y_0, Y_1, \ldots, Y_8]$:

1. $Y_0Y_2 + Y_6Y_3 + Y_5^2$	2. $Y_0Y_3 + Y_1^2$	3. $Y_8Y_5 + Y_0Y_4 + Y_6^2$
4. $Y_0Y_5 + Y_2^2$	5. $Y_0Y_6 + Y_3Y_1$	6. $Y_0Y_7 + Y_3Y_2$
7. $Y_8Y_0 + Y_4Y_2$	8. $Y_8Y_5 + Y_6^2 + Y_2Y_1$	9. $Y_4Y_1 + Y_3Y_2$
10. $Y_5Y_1 + Y_4Y_2$	11. $Y_6Y_1 + Y_3^2$	12. $Y_7Y_1 + Y_4Y_3$
13. $Y_8Y_1 + Y_4^2$	14. $Y_6Y_2 + Y_4Y_3$	15. $Y_7Y_2 + Y_4^2$
16. $Y_8Y_2 + Y_5Y_4$	17. $Y_5Y_3 + Y_4^2$	18. $Y_7Y_3 + Y_6Y_4$
19. $Y_8Y_3 + Y_6Y_5$	20. $Y_7Y_4 + Y_6Y_5$	21. $Y_8Y_4 + Y_7Y_5$
22. $Y_8Y_6 + Y_7^2$		

- Since the first row of G is the all-ones vector, the hyperplane at infinity $Y_0 = 0$ is a hyperplane of $\mathbb{P}^8(\mathbb{F}_{16})$ that is disjoint from the set $\mathcal{Q}$. A Gröbner basis of the ideal $I = \langle I_2(\mathcal{Y})\rangle + \langle Y_0\rangle$ gives us the points and their multiplicities that constitute the divisor F. For this purpose, we will use the adaptation of Lundqvist's Algorithm presented in Section 4.3.

(1) We make the following change of variables:

$$\hat{Y}_8 = Y_8 + Y_4 + Y_0 \quad \text{and} \quad \hat{Y}_i = Y_i \text{ for } i = 0, \ldots, 7,$$

such that $T(Y_i)(P) \neq 0$ for all points $P \in V(I)$.

(2) We compute a Gröbner basis $\mathcal{G}$ of the affine zero-dimensional ideal generated by the affine equations of $I_2(\mathcal{Y})$ with affine coordinates $y_i = \frac{\hat{Y}_i}{\hat{Y}_8}$ for $i = 1, \ldots, 7$ and the hyperplane $Y_0 = 0$

with respect to the lexicographical order induced by the following ordering on the variables $y_0 > y_1 > y_2 > y_3 > y_4 > y_5 > y_6 > y_7$ is

$$\left\{ \begin{array}{c} y_0,\ y_1 + y_7^{10},\ y_2 + y_7^{9},\ y_3 + y_7^{11} + y_7^{6}, \\ y_4 + y_7^{5},\ y_5 + y_7^{9} + y_7^{4},\ y_6 + y_7^{12} + y_7^{7} + y_7^{2}, y_7^{14} \end{array} \right\}$$

Therefore the affine solution is $(0,0,0,0,0,0,0,0)$ with multiplicity 14, whether the corresponding projective point is $P = (0:0:0:0:0:0:0:0:1)$.

Thus the search divisor is $F = 14P \in \mathbb{P}^8(\mathbb{F}_{16})$.

By (Márquez-Corbella et al., 2012, Proposition 7), $(\mathcal{Y}, Q, F)$ is a representation of C that is strict isomorphic to $(\mathcal{X}, \mathcal{P}, E)$.

Example 24. Consider again the Hermitian curve of Example 23 but now we take a multipoint divisor $E = mP_\infty - aP_{00}$, where $P_\infty = (0:0:1)$ is the point at infinity and $P_{00} = (1:0:0)$.

By (Duursma and Kirov, 2011, Lemma 6.2) we obtain a basis for $\mathcal{L}(E)$ by excluding the monomials that have zeros at P_{00} of multiplicity less than a. In other words, a basis for the space $\mathcal{L}(D)$ where $D = d(4+1)P_\infty - aP_\infty - bP_{00}$ for $d \in \mathbb{Z}$, $0 \leq a$ and $b \leq 4$, is given by the monomials:

$$x_1^i x_2^j \text{ such that } \begin{cases} 0 \leq i \leq 4, \ \ 0 \leq j \text{ and } i + j \leq d \\ a \leq i \text{ for } i + j = d \\ b \leq i \text{ for } j = 0 \end{cases}$$

In particular, for $E = 15P_\infty - P_{00}$ we have the following basis for its Riemann-Roch space:

$$\mathcal{B} = \left\{ \begin{array}{c} f_0 = x_1,\ \ f_1 = x_1^2,\ \ f_2 = x_1^3,\ \ f_3 = x_2,\ \ f_4 = x_1x_2, \\ f_5 = x_1^2x_2,\ \ f_6 = x_2^2,\ \ f_7 = x_1x_2^2,\ f_8 = x_2^3 \end{array} \right\}$$

We consider the algebraic code C defined by the triple $(\mathcal{X}, \mathcal{P}, E)$ where $\mathcal{P}$ is the set of 63 rational points of $\mathcal{X}$ that do not belong to the support of E. This code has length $n = 63$ and dimension $k = 9$.

Let $P_1, \ldots, P_{63}$ be an enumeration of all the set of points of $\mathcal{P}$. A generator matrix G of C is the matrix given by

$$G = \begin{pmatrix} f_0(P_1) & \ldots & f_0(P_{63}) \\ \vdots & \ddots & \vdots \\ f_8(P_1) & \ldots & f_8(P_{63}) \end{pmatrix} \in \mathbb{F}_{16}^{9\times 63}.$$

Observe that all the coordinates of the fourth row of G are nonzero. Therefore we replace the matrix G by the matrix $\hat{G} = \lambda * G$ where $\lambda = (1/g_{21}, \ldots, 1/g_{2n})$ and g_{ij} denotes the entry of G in the i-th row and the j-th column. Thus the second row of the new matrix consists of ones.

In this case the attacker:

- Take the columns of $\hat{G}$ as the projective system $Q = (Q_1, \ldots, Q_{63})$.
- Define the curve $\mathcal{Y}$ whose vanishing ideal is generated by the following set of quadrics in

$\mathbb{F}_{16}[Y_0, Y_1, \ldots, Y_8]$.

1. $Y_7Y_4 + Y_5^2 + Y_1Y_0$	2. $Y_3Y_0 + Y_2Y_1$	3. $Y_4Y_0 + Y_3Y_1$
4. $Y_5Y_0 + Y_2^2$	5. $Y_6Y_0 + Y_3Y_2$	6. $Y_7Y_0 + Y_3^2$
7. $Y_8Y_0 + Y_4Y_3$	8. $Y_8Y_4 + Y_6Y_5 + Y_1^2$	9. $Y_5Y_1 + Y_3Y_2$
10. $Y_6Y_1 + Y_3^2$	11. $Y_7Y_1 + Y_4Y_3$	12. $Y_8Y_1 + Y_4^2$
13. $Y_4Y_2 + Y_3^2$	14. $Y_6Y_2 + Y_5Y_3$	15. $Y_7Y_2 + Y_5Y_4$
16. $Y_8Y_2 + Y_6Y_4$	17. $Y_6Y_3 + Y_5Y_4$	18. $Y_7Y_3 + Y_6Y_4$
19. $Y_8Y_3 + Y_7Y_4$	20. $Y_7Y_5 + Y_6^2$	21. $Y_8Y_5 + Y_7Y_6$
22. $Y_8Y_6 + Y_7^2$		

This set of quadrics coincides with the right kernel of a generator matrix of the square code $C^{(2)}$.

- A Gröbner basis of the ideal $\langle I_2(\mathcal{Y})\rangle + \langle Y_1\rangle$ gives us the points and their multiplicities that constitute the divisor F. Similar to the previous example, for this purpose:

(1) We make the following change of variables:

$$\hat{Y}_1 = Y_1 + Y_0 + Y_8 \quad \text{and} \quad \hat{Y}_i = Y_i \text{ for } i = 0, 2, \ldots, 8$$

such that $T(\hat{Y}_1)(P) \neq 0$ for all points in the vanishing ideal $I(\mathcal{Y}) + < Y_1 >$.

(2) We compute a Gröbner basis $\mathcal{G}$ of the affine zero-dimensional ideal generated by the affine equations of $I_2(\mathcal{Y})$ with affine coordinates $y_i = \frac{\hat{Y}_i}{\hat{Y}_1}$ and the hyperplane $Y_1 = 0$, relative to the lexicographical ordering induced by the following ordering on the variables: $y_0 > y_8 > y_6 > y_5 > y_4 > y_3 > y_2 > y_7$.

$$\mathcal{G} = \left\{ \begin{array}{c} y_0 + y_8 + 1, y_8^2 + y_8, y_8y_2 + y_7^7, y_8y_7 + y_7, y_6 + y_7^2, \\ y_5 + y_2^2 + y_7^3, y_4 + y_7^5, y_3 + y_7^6, y_2^4, y_2y_7 + y_7^8, y_7^{10} \end{array} \right\}$$

Thus we have two affine solutions which give the two associated projective points: $P_1 = (1 : 0 : 0 : 0 : 0 : 0 : 0 : 0 : 0 : 0)$ with multiplicity 4 and $P_2 = (0 : 0 : 0 : 0 : 0 : 0 : 0 : 0 : 0 : 1)$ with multiplicity 10.

Therefore the search divisor is $F = 4P_1 + 10P_2$.

By (Márquez-Corbella et al., 2012, Proposition 7), $(\mathcal{Y}, \mathcal{Q}, F)$ is a representation of C that is strict isomorphic to $(\mathcal{X}, \mathcal{P}, E)$.

6. Some remarks on decoding

Once we have recovered the triple $(\mathcal{Y}, \mathcal{Q}, F)$, the last computation for recovering the message in a McEliece PKC consists in applying a decoding algorithm for the resulting AG-code. Note that proposing a novel decoding algorithm is not the purpose of this paper but to give the complete description of the code and to indicate some decoding algorithms that can be used in practice, without considering their feasibility, that is we do not claim in this work that an efficient decoding is always possible.

Note that previous steps in this paper can be seen as a pre-computation from the point of view of decoding, and therefore also for the recovering of the message. We remark that one should

consider decoding algorithms for (possible) multipoint evaluation AG-codes defined from a non-plane curve. Taking into account the previous remarks we propose to use (Beelen and Høholdt, 2008; Høholdt and Pellikaan, 1995; Lee et al., 2012).

The algorithm in (Lee et al., 2012) works for general AG codes. In order to apply this algorithm one should first compute the Miura-Pellikaan or standard form of the curve (Geil and Pellikaan, 2002; Miura, 1998). Such a representation of the curve relies on a Gröbner basis computation involving the ideal of the curve and the basis of the Riemann-Roch space by (Tang, 1998, Theorem 4.1). Once we have precomputed such a form, that can become a bottleneck since a Gröbner basis computation is involved, the remaining steps are very fast, the decoding complexity is $O((n + 4g)(n + 2g)g)$.

Another algorithm for decoding general AG codes is given in (Beelen and Høholdt, 2008; Høholdt and Pellikaan, 1995). This algorithm is based on a syndrome formulation of the basic algorithm and an interpolation step followed by a majority voting scheme. The authors of (Beelen and Høholdt, 2008) extend this algorithm for performing list-decoding, this algorithm is equivalent to the well-known Guruswami-Sudan algorithm (Guruswami and Sudan, 1999) but it solves a smaller system of equations and hence it is faster than the original Guruswami-Sudan algorithm. The precise size of the system of equations can be found in (Beelen and Høholdt, 2008, Section 2.7).

Note that both procedures decode up to half of some generalized order bounds. One might defend the message by introducing a number of errors, where this number is between one half these bounds and the error correcting capability of the code. In this case it is clear from the coding theory point of view that a list-decoding algorithm will provide a list with a single element for those type of errors. For instance, one may consider the list-decoding algorithm in (Beelen and Høholdt, 2008).

Acknowledgment

This research was partly supported by the Danish National Research Foundation and the National Science Foundation of China (Grant No. 11061130539) for the Danish-Chinese Center for Applications of Algebraic Geometry in Coding Theory and Cryptography and by Spanish grants MTM2007-64704, MTM2010-21580-C02-02 and MTM2012-36917-C03-03. Part of the research of the second author is also funded by the Vernon Wilson Endowed Chair at Eastern Kentucky University during his sabbatical leave.

We thank Ulrich Tipp for his remarks concerning the typos in Examples 14, 23 and 24.

References

Augot, D., Finiasz, M., Sendrier, N., 2005. A family of fast syndrome based cryptographic hash functions, in: Dawson, E., Vaudenay, S. (Eds.), Mycrypt 2005. Springer-Verlag Berlin Heidelberg. volume 3715 of *Lecture Notes in Computer Science*, pp. 64–83.

Avanzi, R., Hoerder, S., Page, D., Tunstall, M., 2011. Side-channel attacks on the McEliece and Niederreiter public-key cryptosystems. Journal of Cryptographic Engineering 1, 271–281.

Baldi, M., Bianchi, M., Chiaraluce, F., Rosenthal, J., Schipani, D., 2011. Enhanced public key security for the McEliece cryptosystem. arXiv preprint arXiv:1108.2462 .

Baldi, M., Bodrato, M., Chiaraluce, F., 2008. A new analysis of the McEliece cryptosystem based on QC-LDPC codes, in: 6th International Conference, SCN 2008. Springer-Verlag Berlin Heidelberg. volume 5229 of *Lecture Notes in Computer Science*, pp. 246–262.

Baldi, M., Chiaraluce, F., 2007. Cryptanalysis of a new instance of McEliece cryptosystem based on QC-LDPC Codes, in: ISIT 2007. IEEE Information Theory Society, pp. 2591–2595.

Becker, A., Joux, A., May, A., Meurer, A., 2012. Decoding random binary linear codes in $2^{n/20}$: How 1 + 1 = 0 improves information set decoding, in: Pointcheval, D., Johansson, T. (Eds.), EUROCRYPT 2012. Springer-Verlag Berlin Heidelberg. volume 7237 of *Lecture Notes in Computer Science*, pp. 520–536.

Beelen, P., Høholdt, T., 2008. The decoding of algebraic geometry codes, in: Advances in algebraic geometry codes. World Sci. Publ., Hackensack, NJ. volume 5 of *Ser. Coding Theory Cryptol.*, pp. 49–98.

Berger, T., Cayrel, P., Gaborit, P., Otmani, A., 2009. Reducing key length of the McEliece cryptosystem, in: Preneel, B. (Ed.), AFRICACRYPT 2009. Springer-Verlag Berlin Heidelberg. volume 5580 of *Lecture Notes in Computer Science*, pp. 77–97.

Berger, T., Loidreau, P., 2005. How to mask the structure of codes for a cryptographic use. Designs, Codes and Cryptography 35, 63–79.

Bernstein, D.J., Lange, T., Peters, C., 2008. Attacking and Defending the McEliece Cryptosystem, in: Buchmann, J., Ding, J. (Eds.), PQCrypto 2008. Springer-Verlag Berlin Heidelberg. volume 5299 of *Lecture Notes in Computer Science*, pp. 31–46.

Bernstein, D.J., Lange, T., Peters, C., 2011. Smaller Decoding Exponents: Ball-Collision Decoding, in: Advances in cryptology—CRYPTO 2011. Springer-Verlag Berlin Heidelberg. volume 6841 of *Lecture Notes in Computer Science*, pp. 743–760.

Biasi, F., Barreto, P., Misoczki, R., Ruggiero, W., 2012. Scaling efficient code-based cryptosystems for embedded platforms. arXiv preprint arXiv:1212.4317 .

Campillo, A., Farrán, J., 2002. Symbolic Hamburger-Noether expressions of plane curves and applications to AG codes. Math. Comput. 71, 1759–1780.

Campillo, A., Farrán, J., 2004. Adjoints and codes. Rend. Sem. Mat. Univ. Politec. Torino 62, 209–223.

Canteaut, A., Chabaud, F., 1998. A new algorithm for finding minimum-weight words in a linear code: application to McEliece's cryptosystem and to narrow-sense BCH codes of length 511. IEEE Transactions on Information Theory 44, 367–378.

Cascudo, I., Chen, H., Cramer, R., Xing, X., 2009. Asymptotically good ideal linear secret sharing with strong multiplication over any fixed finite field, in: Halevi, S. (Ed.), CRYPTO 2009. Springer-Verlag Berlin Heidelberg. volume 5677 of *Lecture Notes in Computer Science*, pp. 466–486.

Courtois, N., Finiasz, M., Sendrier, N., 2001. How to achieve a McEliece-based digital signature scheme, in: Boyd, C. (Ed.), ASIACRYPT 2001. Springer-Verlag Berlin Heidelberg. volume 2248 of *Lecture Notes in Computer Science*, pp. 157–174.

Couvreur, A., Gaborit, P., Gauthier-Umaña, V., Tillich, J.P., 2013. Distinguisher-Based Attacks on Public-Key Cryptosystems using Reed-Solomon Codes, in: WCC 2013, pp. 180–193.

Duursma, I., Kirov, R., 2011. Improved two-point codes on Hermitian curves. IEEE Trans. Inform. Theory 57, 4469–4476.

Duval, D., 1987. Diverses questions relatives au calcul formel avec des nombres algébriques. Ph.D. thesis. Université Scientifique, Technologique et Médicale de Grenoble.

Duval, D., 1989. Rational puiseux expansions. Compositio Mathematica 70, 119–154.

Eisenbarth, T., Güneysu, T., Stefan, H., Christof, P., 2009. MicroEliece: McEliece for Embedded Devices, in: Clavier, C., Gaj, K. (Eds.), Cryptographic Hardware and Embedded Systems - CHES 2009. Springer-Verlag Berlin Heidelberg. volume 5747 of *Lecture Notes in Computer Science*, pp. 49–64.

Faugère, J.C., Gauthier-Umaña, V., Otmani, A., Perret, L., Tillich, J.P., 2013. A Distinguisher for High-Rate McEliece Cryptosystems. IEEE Transactions on Information Theory 59, 6830–6844.

Faugère, J.C., Gianni, P., Lazard, D., Mora, T., 1993. Efficient computation of zero-dimensional Gröbner bases by change of ordering. J. Symbolic Comput. 16, 329–344.

Faugère, J.C., Otmani, A., Perret, L., Tillich, J.P., 2010. Algebraic Cryptanalysis of McEliece Variants with Compact Keys, in: Gilbert, H. (Ed.), EUROCRYPT 2010. Springer-Verlag Berlin Heidelberg. volume 6110 of *Lecture Notes in Computer Science*, pp. 279–298.

Faure, C., Minder, L., 2008. Cryptanalysis of the McEliece cryptosystem over hyperelliptic codes, in: ACCT 2008, pp. 99–107.

Finiasz, M., Sendrier, N., 2009. Security Bounds for the Design of Code-Based Cryptosystems, in: Matsui, M. (Ed.), ASIACRYPT 2009. Springer-Verlag Berlin Heidelberg. volume 5912 of *Lecture Notes in Computer Science*, pp. 88–105.

Gaborit, P., 2005. Shorter keys for code based cryptography, in: Ytrehus, O. (Ed.), WCC 2005. Springer-Verlag Berlin Heidelberg. volume 3969 of *Lecture Notes in Computer Science*, pp. 81–90.

Gaborit, P., Laudaroux, C., Sendrier, N., 2007. SYND: a Very Fast Code-Based Stream Cipher with a Security Reduction, in: ISIT 2007, pp. 186–190.

Gauthier-Umaña, V., Leander, G., 2009. Practical key recovery attacks on two McEliece variants. IACR Cryptology ePrint Archive 509.

Geil, O., Pellikaan, R., 2002. On the structure of order domains. Finite Fields Appl. 8, 369–396.

Goppa, V., 1977. Codes associated with divisors. Probl. Inform. Transmission 13, 22–26.

Gorenstein, D., 1952. An arithmetic theory of adjoint plane curves. Trans. Amer. Math. Society 72, 414–436.

Griffiths, P., Harris, J., 1978. Principles of algebraic geometry. Wiley-Interscience Publication, New York.

Guruswami, V., Sudan, M., 1999. Improved decoding of Reed-Solomon and algebraic-geometry codes. IEEE Trans. Inform. Theory 45, 1757–1767.

Haché, G., 1995. Computation in algebraic function fields for effective construction of Algebraic-Geometric Codes, in: Algebraic algorithms and error correcting codes (AAECC). Springer-Verlag Berlin Heidelberg. volume 948 of *Lecture Notes in Computer Science*, pp. 262–278.

Haché, G., 1996. Construction effective des codes géométriques. Ph.D. thesis. Univ. Paris VI, INRIA.

Haché, G., 1998. L'algorithme de Brill-Noether appliqué aux courbes réduites. Rapport de recherche du Laboratoire LACO .

Haché, G., Le Brigand, D., 1995. Effective construction of algebraic geometry codes. IEEE Transactions on Information Theory 41, 1615–1628.

Hess, F., 1999. Zur Divisorenklassengruppenberechnung in globalen Funktionenkörpern. Ph.D. thesis. Technischen Universität Berlin.

Hess, F., 2002. Computing Riemann-Roch spaces in algebraic function fields and related topics. J. Symbolic Comput. 33, 425–445.

Hirschfeld, J.W.P., Kochmáros, G., Torres, F., 2008. Algebraic curves over a finite field. Princeton Univ. Press, Princeton.

Hoeij, M.v., 1994. An Algorithm for Computing an Integral Basis in an Algebraic Function Field. J. Symbolic Comput. 18, 209–227.

Hoeij, M.v., 1997. Rational Parametrizations of Algebraic Curves using a Canonical Divisor. J. Symbolic Comput. 23, 353–363.

Høholdt, T., Lint, J.v., Pellikaan, R., 1998. Algebraic geometry codes, in: Pless, V., Huffman, W. (Eds.), Handbook of coding theory. North-Holland, Amsterdam. volume 1, pp. 871–961.

Høholdt, T., Pellikaan, R., 1995. On decoding algebraic-geometric codes. IEEE Transactions on Information 41, 1589–1614.

Huang, M.D.A., Ierardi, D., 1994. Efficient Algorithms for the Riemann-Roch Problem and for Addition in the Jacobian of a Curve. J. Symbolic Comput. 18, 519–539.

Janwa, H., Moreno, O., 1996. McEliece public key cryptosystems using algebraic-geometric codes. Designs, Codes and Cryptography 8, 293–307.

Landais, G., Tillich, J.P., 2013. An Efficient Attack of a McEliece Cryptosystem Variant Based on Convolutional Codes, in: Gaborit, P. (Ed.), Post-Quantum Cryptography. Springer Berlin Heidelberg. volume 7932 of *Lecture Notes in Computer Science*, pp. 102–117.

Laursen, K., 1997a. The computational complexity of effective construction of geometric Goppa codes, in: ISIT-97. IEEE Information Theory Society, p. 380.

Laursen, K., 1997b. Constructing geometric Goppa codes. Ph.D. thesis. Aalborg University.

Le Brigand, D., 1986a. A [32, 17, 14] - geometric code coming from a singular curve, in: Coding Theory and Applications, pp. 106–115.

Le Brigand, D., 1986b. On computational complexity of some algebraic curves over finite fields, in: Algebraic algorithms and error correcting codes (AAECC). Springer-Verlag Berlin Heidelberg. volume 229 of *Lecture Notes in Computer Science*, pp. 223–227.

Le Brigand, D., Risler, J.J., 1988. Algorithme de Brill-Noether et codes de Goppa. Bull. Soc. Math. France 116, 231–253.

Lee, K., Bras-Amorós, M., O'Sullivan, M., 2012. Unique Decoding of General AG Codes. arXiv preprint arXiv:1210.3101 .

Lee, P.J., Brickell, E.F., 1988. An observation on the security of McEliece's public-key cryptosystem, in: Günther, C.G. (Ed.), EUROCRYPT'88. Springer-Verlag Berlin Heidelberg. volume 330 of *Lecture Notes in Computer Science*, pp. 275–280.

Li, Y., Deng, R., Wang, X., 1994. On the equivalence of McEliece's and Niederreiter's public-key cryptosystems. IEEE Trans. Inform. Theory 40, 271–273.

Loidreau, P., Sendrier, N., 2001. Weak keys in the McEliece public-key cryptosystem. IEEE Trans. Inform. Theory 47, 1207–1211.

Löndahl, C., Johansson, T., 2012. A new version of McEliece PKC based on convolutional codes, in: Chim, T., Yuen, T. (Eds.), Information and Communications Security. Springer Berlin Heidelberg. volume 7618 of *Lecture Notes in Computer Science*, pp. 461–470.

Lundqvist, S., 2012. Multiplication matrices and ideals of projective dimension zero. Math. Comput. Sci. 6, 43–59.

Marinari, M., Möller, H., Mora, T., 1993. Gröbner bases of ideals defined by functionals with an application to ideals of projective points. Applicable Algebra in Engineering, Communication and Computing 4, 103–145.

Márquez-Corbella, I., Martínez-Moro, E., Pellikaan, R., 2012. On the unique representation of very strong algebraic geometry codes. Designs, Codes and Cryptography , 1–16.

Márquez-Corbella, I., Martínez-Moro, E., Pellikaan, R., 2013. The non-gap sequence of a subcode of a generalized Reed-Solomon code. Designs, Codes and Cryptography 66, 317–333.

Márquez-Corbella, I., Pellikaan, R., 2012. Error-correcting pairs for a public-key cryptosystem. arXiv preprint arXiv:1205.3647 .

Matsumoto, R., Miura, S., 2000. Finding a basis of a linear system with pairwise distinct discrete valuations on an algebraic curve. J. Symbolic Comput. 30, 309–324.

May, A., Meurer, A., Thomae, E., 2011. Decoding random linear codes in $O(2^{0.054n})$, in: Lee, D., Wang, X. (Eds.), ASIACRYPT. Springer-Verlag Berlin Heidelberg. volume 7073 of *Lecture Notes in Computer Science*, pp. 107–124.

McEliece, R.J., 1978. A public-key cryptosystem based on algebraic coding theory. DSN Progress Report 42–44, 114–116.

Minder, L., Shokrollahi, A., 2007. Cryptanalysis of the Sidelnikov cryptosystem, in: EUROCRYPT 2007. Springer-Verlag Berlin Heidelberg. volume 4515 of *Lecture Notes in Computer Science*, pp. 347–360.

Minder, L., Sinclair, A., 2012. The extended k-tree algorithm. J. Cryptol. 25, 349–382.

Misoczki, R., Barreto, P.S., 2009. Compact McEliece Keys from Goppa Codes, in: Jacobson, M.J.J.J., Rijmen, V., Safavi-Naini, R. (Eds.), Selected Areas in Cryptography. Springer-Verlag Berlin Heidelberg. volume 5867 of *Lecture Notes in Computer Science*, pp. 376–392.

Misoczki, R., Tillich, J.P., Sendrier, N., Barreto, P.S.L.M., 2012. MDPC-McEliece: New McEliece variants from moderate density parity-check codes. IACR Cryptology ePrint Archive 409.

Miura, S., 1998. Linear codes on affine algebraic curves. Trans. IEICE 81, 1398–1421.

Monico, C., Rosenthal, J., Shokrollahi, A., 2000. Using low density parity check codes in the McEliece cryptosystem, in: IEEE International Symposium on Information Theory, p. 215.

Mumford, D., 1970. Varieties defined by quadratic equations, in: Questions on algebraic varieties, C.I.M.E., III Ciclo, Varenna, 1969. Edizioni Cremonese, Rome, pp. 29–100.

Niederreiter, H., 1986. Knapsack-type crypto systems and algebraic coding theory. Problems of Control and Information Theory 15, 159–166.

Noether, M., 1880. Über die invariante Darstellung algebraischer Funktionen. Math. Ann. 17, 263–284.

Pecquet, L., 2001. List decoding of algebraic geometric codes. Ph.D. thesis. Univ. Paris VI.

Pecquet, L., Wocjan, P., 2000. Building algebraic-geometric codes in Magma. Third European Congress of Mathematics, Barcelona Spain .

Pellikaan, R., Shen, B., van Wee, G., 1991. Which linear codes are algebraic-geometric ? IEEE Trans. Inform. Theory 37, 583–602.

Peters, C., 2011. Curves, Codes and Cryptography. Ph.D. thesis. Technische Universiteit Eindhoven.

Prange, E., 1962. The use of information sets in decoding cyclic codes. IRE Transactions on Information Theory 8, 5–9.

Saint-Donat, B., 1972. Sur les équations définissant une courbe algébrique. C. R. Acad. Sc. Paris 274, 324–327, 487–489.

Saint-Donat, B., 1973. On Petri's analysis of the linear system of quadrics through a canonical curve. Math. Ann. 206, 157–175.

Schreyer, F.O., 1991. A standard basis approach to syzygies of canonical curves. J. Reine Angew. Math. 421, 83–123.

Sendrier, N., 1994. On the structure of a randomly permuted concatenated code, in: Charpin, P. (Ed.), EUROCODE '94. Abbaye de la Bussière sur Ouche, France, pp. 169–173.

Sendrier, N., 2000. Finding the permutation between equivalent linear codes: the support splitting algorithm. IEEE Trans. Inform. Theory 46, 1193–1203.

Shoufan, A., Strenzke, F., Molter, H., Stöttinger, M., 2010. A Timing Attack against Patterson Algorithm in the McEliece PKC, in: Lee, D., Hong, S. (Eds.), Information, Security and Cryptology, ICISC 2009. Springer-Verlag Berlin Heidelberg. volume 5984 of *Lecture Notes in Computer Science*, pp. 161–175.

Shparlinski, I., 1993. Finding irreducible and primitive polynomials. Appl. Alg. Engin. Commun. Comp. 4, 263–268.

Shparlinski, I., 1999. Finite fields: Theory and computation. volume 477 of *Mathematics and its Applications*. Kluwer Acad. Publ.

Sidelnikov, V., 1994. A public-key cryptosystem based on binary Reed-Muller codes 4.

Sidelnikov, V.M., Shestakov, S.O., 1992. On the insecurity of cryptosystems based on generalized Reed-Solomon codes. Discrete Math. Appl. 2, 439–444.

Stern, J., 1989. A method for finding codewords of small weight, in: Cohen, G.D., Wolfmann, J. (Eds.), Coding theory and applications. Springer-Verlag Berlin Heidelberg. volume 388 of *Lecture Notes in Computer Science*, pp. 106–113.

Stichtenoth, H., 2009. Algebraic function fields and codes. volume 254 of *Graduate Texts in Mathematics*. Springer-Verlag, Berlin. second edition.

Strenzke, F., Tews, E., Molter, H., Overbeck, R., Shoufan, A., 2008. Side Channels in the McEliece PKC, in: Buchmann, J., Ding, J. (Eds.), Post-Quantum Cryptography. Springer-Verlag Berlin Heidelberg. volume 5299 of *Lecture Notes in Computer Science*, pp. 216–229.

Tang, L.Z., 1998. A Gröbner basis criterion for birational equivalence of affine varieties. J. Pure Appl. Algebra 123, 275–283.

Tsfasman, M., Vlăduţ, S., 1991. Algebraic-geometric codes. Kluwer Academic Publishers, Dordrecht.

Wagner, D., 2002. A Generalized Birthday Problem, in: Proceedings of the 22nd Annual International Cryptology Conference on Advances in Cryptology. Springer-Verlag Berlin Heidelberg. CRYPTO '02, pp. 288–303.

Wieschebrink, C., 2006a. An attack on the modified Niederreiter encryption scheme, in: PKC. Springer-Verlag Berlin Heidelberg. volume 3958 of *Lecture Notes in Computer Science*, pp. 14–26.

Wieschebrink, C., 2006b. Two NP-complete Problems in Coding Theory with an Application in Code Based Cryptography, in: IEEE International Symposium on Information Theory, pp. 1733–1737.

Wieschebrink, C., 2010. Cryptanalysis of the Niederreiter public key scheme based on GRS subcodes, in: Post-Quantum Cryptography. Springer-Verlag Berlin Heidelberg. volume 6061 of *Lecture Notes in Computer Science*, pp. 61–72.

Wocjan, P., 1999. Brill-Noether Algorithm; Construction of geometric Goppa codes and absolute factorization of polynomials. Master's thesis. Univ. Karlsruhe.