Evaluation of public-key cryptosystems based on algebraic geometry codes *

Irene Márquez-Corbella[1], Edgar Martínez-Moro[2], and Ruud Pellikaan[3]

imarquez@agt.uva.es, edgar@maf.uva.es, g.r.pellikaan@tue.nl

[1] Department of Algebra, Geometry and Topology, University of Valladolid, Prado de la Magdalena s/n, 47005 Valladolid, Spain.

[2] Department of Applied Mathematics, University of Valladolid, Campus Duques de Soria, E-42004 Soria, Spain.

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

Abstract. In 3rd International Castle Meeting on Coding Theory and Applications
J. Borges and M. Villanueva (eds.)
This paper addresses the question of retrieving the triple $(\mathcal{X}, \mathcal{P}, E)$ from the algebraic geometry code $C_L(\mathcal{X}, \mathcal{P}, E)$, where $\mathcal{X}$ is an algebraic curve over the finite field $\mathbb{F}$, $\mathcal{P}$ is an n-tuple of $\mathbb{F}$-rational points on $\mathcal{X}$ and E is a divisor on $\mathcal{X}$. If $\deg(E) > 2g$ where g is the genus of $\mathcal{X}$, then there is an embedding $\mathcal{Y}$ of $\mathcal{X}$ in the projective space of the linear series of the divisor E. Moreover, if $\deg(E) > 2g + 2$, then $I(\mathcal{Y})$, the vanishing ideal of $\mathcal{Y}$, is generated by $I_2(\mathcal{Y})$, the homogeneous elements of degree two in $I(\mathcal{Y})$. If $n > 2\deg(E)$, then $I_2(\mathcal{Y}) = I_2(\mathcal{Q})$, where $\mathcal{Q}$ is the image of $\mathcal{P}$ under the map from $\mathcal{X}$ to $\mathcal{Y}$. These two results imply that certain algebraic geometry codes are not secure if used in the McEliece public-key cryptosystem.

Keywords: Algebraic geometry codes, public-key cryptosystems

1 Introduction

Algebraic geometry codes (AG codes) also known as Goppa codes were introduced in 1977 by V.D. Goppa. The interested reader is referred to [6, 19, 21]. Let $\mathcal{X}$ be an algebraic curve defined over the finite field $\mathbb{F}$. In this paper a curve is absolutely irreducible and projective and it is assumed to be nonsingular if it is not stated explicitly otherwise. Let $\mathcal{P}$ be an n-tuple of $\mathbb{F}$-rational points on $\mathcal{X}$ and let E be a divisor of $\mathcal{X}$ with disjoint support from $\mathcal{P}$ of degree m.

$\mathbb{F}(\mathcal{X})$ denotes the *function field* of the curve $\mathcal{X}$ with field of constants $\mathbb{F}$, (f) denotes the *principal divisor* of zeros and poles of any nonzero rational function

* The first two authors are partially supported by Spanish MCINN under project MTM2007-64704. First author research is also supported by a FPU grant AP2008-01598 by Spanish MEC. Second author is also supported by Spanish MCINN under project MTM2010-21580-C02-02.

f on the curve $\mathcal{X}$ over $\mathbb{F}$ and recall that two divisors D and E on a curve $\mathcal{X}$ 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 $\mathcal{X}$ with disjoint support with $\mathcal{P}$ are called *rational equivalent with respect to* $\mathcal{P}$ and denoted by $D \equiv_{\mathcal{P}} E$ if there exists a rational function f on $\mathcal{X}$ such that it has no poles at the points of $\mathcal{P}$, $E = D + (f)$ and $f(P_j) = 1$ for all $j = 1, \ldots, n$.

Consider the vector space $L(E) = \{f \in \mathbb{F}(\mathcal{X}) \mid f = 0 \text{ or } (f) \geq -E\}$, and the linear series of E defined by $|E| = \{\ F \mid F \equiv E, F \geq 0\ \}$.

The dimension of the space $L(E)$ is denoted by $l(E)$, thus the projective dimension of the linear series $|E|$ is equal to $l(E) - 1$. The index of speciality of E is defined by $i(E) = l(K - E)$, where K is a canonical divisor.

Since the support of E is disjoint from $\mathcal{P} = (P_1, \ldots, P_n)$, the following evaluation map:

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

is well defined by $\mathrm{ev}_{\mathcal{P}}(f) = (f(P_1), \ldots, f(P_n))$. The algebraic geometry code $C_L(\mathcal{X}, \mathcal{P}, E)$ is the image of $L(E)$ under the evaluation map $\mathrm{ev}_{\mathcal{P}}$. The parameters of these codes satisfy the following bounds:

Proposition 1. *If $m < n$ then the dimension of the code $C_L(\mathcal{X}, \mathcal{P}, E)$ is equal to $m + 1 - g + i(E) \geq m + 1 - g$ and its minimum distance is at least $n - m$. Moreover, if $m > 2g - 2$, then $C_L(\mathcal{X}, \mathcal{P}, E)$ has dimension $m + 1 - g$.*

Proof. The statement about the minimum distance is a consequence of the fact that a principal divisor has degree zero. The dimension of the code follows from the Theorem of Riemann-Roch [19, 21]. □

The following proposition is related with the dual code of an AG code.

Proposition 2. *Let ω be a differential form with a simple pole at P_j with residue 1 for all $j = 1, \ldots, n$. Let K be the canonical divisor of ω. Let m be the degree of the divisor E on $\mathcal{X}$ with disjoint support from $\mathcal{P}$. Let $E^{\perp} = \mathcal{P} - E + K$ and $m^{\perp} = \deg(E^{\perp})$. Then $m^{\perp} = 2g - 2 - m + n$ and $C_L(\mathcal{X}, \mathcal{P}, E)^{\perp} = C_L(\mathcal{X}, \mathcal{P}, E^{\perp})$.*

Proof. See [19, Proposition 2.2.10]. □

Definition 3. *A code $\mathcal{C}$ over $\mathbb{F}$ is called weakly algebraic-geometric (WAG) if $\mathcal{C}$ is equal to $C_L(\mathcal{X}, \mathcal{P}, E)$. In this case the triple $(\mathcal{X}, \mathcal{P}, E)$ is called a WAG representation of $\mathcal{C}$.*

Proposition 4. *Every code has a WAG representation.*

Proof. See [16, Theorem 2]. □

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

Proposition 5. *Let $(\mathcal{X}, \mathcal{P}, E)$ and $(\mathcal{Y}, \mathcal{Q}, F)$ be WAG representations of the 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 equivalent.*
(2) *If $(\mathcal{X}, \mathcal{P}, E)$ and $(\mathcal{Y}, \mathcal{Q}, F)$ are strict equivalent, then $\mathcal{C} = \mathcal{D}$.*

Proof. If $\mathcal{X} = \mathcal{Y}$ and $\mathcal{P} = \mathcal{Q}$, then the proof of (1) is given in [19, Prop. 2.2.14 (a)] and it specializes to strict equivalence in case (2) where $E \equiv_{\mathcal{P}} F$. Both cases are generalized in a straight forward matter. □

Let $r = l(E) - 1$ and $\{f_0, \ldots, f_r\}$ be a basis of $L(E)$. Consider the following map:

$$\varphi_E : \mathcal{X} \longrightarrow \mathbb{P}^r$$

defined by $\varphi_E(P) = (f_0(P), \ldots, f_r(P))$.

If $m > 2g$, then $r = m - g$ and φ_E defines an embedding of the curve $\mathcal{X}$, $\mathcal{Y} = \varphi_E(\mathcal{X})$, in $\mathbb{P}^r$ of degree m. Now let $Q_j = \varphi_E(P_j)$ and $\mathcal{Q} = (Q_1, \ldots, Q_n)$ then $\varphi_E(E) = \mathcal{X} \cdot H = F$ for some hyperplane H of $\mathbb{P}^{m-g}$ that is disjoint from $\mathcal{Q}$. See [8, Theorems 7.33 and 7.40]. Furthermore if $\mathcal{C} = C_L(\mathcal{X}, \mathcal{P}, E)$ we have that $(\mathcal{Y}, \mathcal{Q}, F)$ is also a WAG representation of the code $\mathcal{C}$ that is strict isomorphic with $(\mathcal{X}, \mathcal{P}, E)$. Therefore we have shown the following proposition:

Proposition 6. *Let $(\mathcal{X}, \mathcal{P}, E)$ be a WAG representation of the code $\mathcal{C}$ such that $m > 2g$. Let $\mathcal{Y} = \varphi_E(\mathcal{X})$, $\mathcal{Q} = \varphi_E(\mathcal{P})$ and $F = \varphi_E(E)$. Then $(\mathcal{Y}, \mathcal{Q}, F)$ is representation of $\mathcal{C}$ that is strict isomorphic with $(\mathcal{X}, \mathcal{P}, E)$.*

The main task of this paper is recovering the triple $(\mathcal{X}, \mathcal{P}, E)$ from the code $C_L(\mathcal{X}, \mathcal{P}, E)$ using first the fact that the code $C_L(\mathcal{X}, \mathcal{P}, E)$ gives a projective system $\mathcal{Q}$ of points in the projective space $\mathbb{P}^r$ where $\mathcal{Q} = \varphi_E(\mathcal{P})$. Indeed let G be a generator matrix of a nondegenerate code $\mathcal{C}$ of dimension k over $\mathbb{F}$. Then G has no zero columns. Take the columns of G as homogeneous coordinates of points in $\mathbb{P}^{k-1}(\mathbb{F})$. This gives the projective system $\mathcal{P}_G$ over $\mathbb{F}$ of G.

Furthermore under some assumptions not only the pair $(\mathcal{X}, E)$ gives an embedding $\varphi_E(\mathcal{X})$ of the curve in the projective r-space such that the embedded curve is defined by quadratic equations (see Section 2) but also the quadratic polynomials that vanish on $\mathcal{Q}$ generate the vanishing ideal of the embedded curve (see Section 3).

Finally we provide an understanding of the security of the McEliece PKC system based on algebraic geometry codes.

2 Curves defined by quadratic equations

In the early 90's it was shown by Enriques [4], Babbage [3] and Petri [17] that the canonical model of a non-singular non-hyperelliptic projective curve of genus at least three is the intersection of quadrics and cubics, and of quadrics only except in case of a trigonal curve and a plane quintic. This result for the canonical divisor was generalized for arbitrary divisors E under certain constraints on the

degree. See [2, 11, 13, 14, 18] and [7, p. 528–535] and [1, Chap. III, §2 and §3].

The polynomial ring $R = \mathbb{F}[X_0, X_1, \ldots, X_r]$ is graded by

$$R_d = \{\ f(X) \in R \mid f(X) \text{ is zero or is homogeneous of degree d }\}.$$

So it can be expressed in the form $R = \oplus_{d=0}^{\infty} R_d$. We define $R_{\leq d} = \oplus_{e=0}^{d} R_e$. Let I be an ideal, in a similar way, we define $I_d = I \cap R_d$ and $I_{\leq d} = I \cap R_{\leq d}$.

Proposition 7. *Let $\mathcal{X}$ be an absolutely irreducible and nonsingular curve of genus g over the perfect field $\mathbb{F}$. Let E be a divisor on $\mathcal{X}$ of degree m. If $m \geq 2g+2$ then $\mathcal{Y} = \varphi_E(\mathcal{X})$ is a normal curve in $\mathbb{P}^{m-g}$ which is the intersection of quadrics, in particular $I(\mathcal{Y})$ is generated by $I_2(\mathcal{Y})$.*

Proof. See [18]. □

3 Determination of $I_2(\mathcal{Q})$

Now suppose that an n-tuple $\mathcal{Q}$ of mutually distinct $\mathbb{F}$-rational points of $\mathcal{Y}$ in $\mathbb{P}^r$ is given such that $I(\mathcal{Y})$ is generated by $I_2(\mathcal{Y})$. In this section we will deduce which hypothesis guarantees that $I_2(\mathcal{Q}) = I_2(\mathcal{Y})$. In order to shorten this abstract we will show the following results without proofs.

Proposition 8. *Let m, r and n be integers such that $r \geq 2$ and $n > dm$. Let $\mathcal{Y}$ be an absolutely irreducible curve in $\mathbb{P}^r$ of degree m. If $\mathcal{Q}$ is an n-tuple of points that lies on the curve $\mathcal{Y}$, then $I_{\leq d}(\mathcal{Q}) = I_{\leq d}(\mathcal{Y})$.*

Let $\mathcal{C}$ be a k dimensional subspace of $\mathbb{F}^n$ with basis $\{\mathbf{g}_1, \ldots, \mathbf{g}_k\}$. We denote by $S^2(\mathcal{C})$ the second symmetric power of $\mathcal{C}$, or equivalently the symmetrized tensor product of $\mathcal{C}$ with itself. If $x_i = \mathbf{g}_i$, then $S^2(\mathcal{C})$ has basis $\{x_i x_j \mid 1 \leq i \leq j \leq n\}$ and dimension $\binom{k+1}{2}$. Furthermore we denote by $\langle \mathcal{C} * \mathcal{C} \rangle$ or $\mathcal{C}^{(2)}$ the square of $\mathcal{C}$, that is, the linear subspace in $\mathbb{F}^n$ generated by $\{\mathbf{a} * \mathbf{b} | \mathbf{a}, \mathbf{b} \in C\}$, see [10, 22]. Now we can consider the linear map $\sigma : S^2(\mathcal{C}) \longrightarrow \mathcal{C}^{(2)}$, where the element $x_i x_j$ is mapped to $\mathbf{g}_i * \mathbf{g}_j$. The kernel of this map will be denoted by $K^2(\mathcal{C})$.

Proposition 9. *Let $G_{\mathcal{Q}}$ be the $k \times n$ matrix associated to $\mathcal{Q}$ and $\mathcal{C}$ be the subspace of $\mathbb{F}^n$ Let $\mathcal{Q}$ be an n-tuple of points in $\mathbb{P}^r$ over $\mathbb{F}$ not in a hyperplane, $k = r + 1$, $G_{\mathcal{Q}}$ be the $k \times n$ matrix associated to $\mathcal{Q}$ and $\mathcal{C}$ be the subspace of $\mathbb{F}^n$ generated by the rows of $G_{\mathcal{Q}}$. Then*

$$I_2(\mathcal{Q}) = \{\ \textstyle\sum_{1 \leq i \leq j \leq k} a_{ij} X_i X_j \mid \sum_{1 \leq i \leq j \leq k} a_{ij} x_i x_j \in K^2(\mathcal{C})\ \}.$$

Corollary 10. *Let $\mathcal{Q}$ be an n-tuple of points in $\mathbb{P}^r$ over $\mathbb{F}$ not in a hyperplane. Then $\mathcal{O}(n^2\binom{r}{2})$ is an upper bound on the complexity of the computation of $I_2(\mathcal{Q})$.*

In the general case we can define the spaces $S^d(\mathcal{C})$, $\mathcal{C}^{(d)}$ and $K^d(\mathcal{C})$ for any positive integer d, then we have a similar result to that in Proposition 9 relating $I_d(\mathcal{Q})$ and $K^d(\mathcal{C})$. Furthermore we have that $\mathcal{O}(n^2\binom{k+d-1}{d})$ is an upper bound on the complexity of the computation of $I_d(\mathcal{Q})$.

4 Very strong algebraic-geometric codes

Definition 11. *A code $\mathcal{C}$ over $\mathbb{F}$ is called very strong algebraic-geometric (VSAG) if $\mathcal{C}$ is equal to $C_L(\mathcal{X}, \mathcal{P}, E)$ where the curve $\mathcal{X}$ over $\mathbb{F}$ has genus g, $\mathcal{P}$ consists of n points and E has degree m such that*

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

The dimension of a such a code is $k = m + 1 - g$. Thus the dimension satisfies the following bound

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

Note that if a code has a VSAG representation then its dual is also VSAG.

Theorem 12. *Let $\mathcal{C}$ be a VSAG code then a VSAG representation can be obtained from its generator matrix. Moreover all VSAG representations of $\mathcal{C}$ are strict isomorphic.*

5 Cryptanalysis of PKC's using VSAG codes

In 1978, McEliece [12] introduced the first public key cryptosystem (PKC) based on the theory of error-correcting codes in particular he proposed to use a $[1024, 524]$ classical binary Goppa code. The security of this scheme is based on the hardness of the decoding problem for general linear codes and the hardness of distinguishing a code with the prescribed structure from a random one.

Many attempts to replace Goppa codes with different families of codes have been proven to be insecure as for example using GRS codes such as the original Niederreiter system [15] which was broken by Sidelnikov and Shestakov [20] in 1992. Later Janwa and Moreno [9] proposed to use the collection of AG codes on curves for the McEliece cryptosystem. This system was broken for codes on curves of genus $g \leq 2$ by Faure and Minder [5]. The security status of this proposal for higher genus was not known. Theorem 12 implies that one should not use VSAG codes for the McEliece PKC system in the range

$$\gamma \leq R \leq \tfrac{1}{2} - \gamma \quad \text{or} \quad \tfrac{1}{2} + \gamma \leq R \leq 1 - \gamma,$$

where $R = \frac{k}{n}$ is the *information rate* and $\gamma = \frac{g}{n}$ the *relative genus* if $n \to \infty$, since there is an efficient attack by our result. By a puncturing argument also algebraic geometry codes in the half rate region should be excluded.

Acknowledgments. The research reported in this paper was made possible by means of the "Research in Pairs" program of the MFO, the Mathematical Research Institute at Oberwolfach during the period January 24-February 5, 2011. We like to thank Stanislav Bulygin and Xin-Wen Wu for their valuable discussions on the topics of this paper.

References

1. E. Arbarello, M. Cornalba, P.A. Griffiths and J. Harris, Geometry of algebraic curves, Springer-Verlag, New York (1985).
2. E. Arbarello and E. Sernesi, Petri's approach to the study of the ideal associated to a special divisor, Invent. Math., 49, 99–119 (1978).
3. D.W. Babbage, A note on the quadrics though a canonical curve, Journ. London Math. Soc., 14, 310–315 (1939).
4. F. Enriques, Sulle curve canoniche di genere p dello spazio a $p-1$ dimensioni, Rend. Accad. Sci. Ist. Bologna, 23, 80–82 (1919).
5. C. Faure and L. Minder, Cryptanalysis of the McEliece cryptosystem over hyperelliptic codes, 11'th Int. Workshop Algebraic and Combinatorial Coding Theory, Pamporovo Bulgaria, 99–107 (2008).
6. V.D. Goppa, Codes associated with divisors, Probl. Inform. Transmission, 13, 22–26 (1977).
7. P. Griffiths and J. Harris, Principles of algebraic geometry, Wiley-Interscience Publication, New York (1978).
8. J. W. P. Hirschfeld, G. Kochmáros and F. Torres, F, Algebraic curves over a finite field, Princeton Univ. Press, Princeton (2008).
9. H. Janwa and O. Moreno, McEliece public crypto system using algebraic-geometric codes, Designs, Codes and Cryptography, 8, 293–307 (1996).
10. I. Márquez-Corbella, E. Martínez-Moro, R. Pellikaan, The non-gap sequence of a subcode of a generalized Reed-Solomon code, Proceedings of the Seventh International Workshop on Coding and Cryptography, April 11-15, Paris, France, 183–193 (2011).
11. M. Mancini, Projectively normal curves defined by quadrics, Rend. Sem. Mat. Univ. Politec. Torino, 59, 269–275 (2001).
12. R. J. McEliece, A public-key cryptosystem based on algebraic coding theory, DSN Progress Report, 42–44, 114–116 (1978).
13. D. Mumford, Varieties defined by quadratic equations, Questions on algebraic varieties, C.I.M.E., III Ciclo, Varenna, 1969, 29–100, Edizioni Cremonese, Rome (1970).
14. D. Mumford, Curves and their Jacobians, Univ. Michigan Press, Ann Arbor (1975).
15. H. Niederreiter, Knapsack-type crypto systems and algebraic coding theory, Problems of Control and Information Theory, 15, 159-166 (1986).
16. R. Pellikaan, B. Z. Shen and G. J. M van Wee, Which linear codes are algebraic-geometric?, IEEE Trans. Inform. Theory, 37, 583–602 (1991).
17. K. Petri, Über die invariante Darstellung algebraischer Funktionen einer Veränderlichen, Math. Ann., 88, 242–289 (1923).
18. B. Saint-Donat, Sur les équations définissant une courbe algébrique, C. R. Acad. Sci. Paris Sr. A, 274, 324–327 (1972).
19. H. Stichtenoth, Algebraic function fields and codes, Springer, Berlin (1993).
20. V.M. Sidelnikov and S.O. Shestakov, On the insecurity of cryptosystems based on generalized Reed-Solomon codes, Discrete Math. Appl., 2, 439–444 (1992).
21. M. A. Tsfasman and S. G. Vlădut, Algebraic-geometric codes, Kluwer Academic Publishers, Dordrecht (1991).
22. C. Wieschebrink, Cryptanalysis of the Niederreiter public key scheme based on GRS subcodes, Post-Quantum Cryptography, Lecture Notes in Computer Science, Springer, Berlin, 6061, 61–72 (1993).