Error-correcting pairs and arrays from algebraic geometry codes

Citation for published version (APA):

Document status and date:
Published: 01/01/2013

Document Version:
Publisher’s PDF, also known as Version of Record (includes final page, issue and volume numbers)

Please check the document version of this publication:
• A submitted manuscript is the version of the article upon submission and before peer-review. There can be important differences between the submitted version and the official published version of record. People interested in the research are advised to contact the author for the final version of the publication, or visit the DOI to the publisher's website.
• The final author version and the galley proof are versions of the publication after peer review.
• The final published version features the final layout of the paper including the volume, issue and page numbers.

Link to publication

General rights
Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

• Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
• You may not further distribute the material or use it for any profit-making activity or commercial gain
• You may freely distribute the URL identifying the publication in the public portal.

If the publication is distributed under the terms of Article 25fa of the Dutch Copyright Act, indicated by the “Taverne” license above, please follow below link for the End User Agreement:
www.tue.nl/taverne

Take down policy
If you believe that this document breaches copyright please contact us at:
openaccess@tue.nl
providing details and we will investigate your claim.
Abstract

The security of the most popular number-theory public key crypto (PKC) systems will be devastatingly affected by the success of a large quantum computer. Code-based cryptography is one of the promising alternatives that are believed to resist classical and quantum computer attacks. Many families of codes have been proposed for these cryptosystems, one of the main requirements is having an efficient $t$-bounded decoding algorithm.

In [16, 17] it was shown that for the so called very strong algebraic geometry codes $C$ which is a collection of codes $C = C_L(X, P, E)$, where $X$ is an algebraic curve over $\mathbb{F}_q$, $P$ is an $n$-tuple of mutually distinct $\mathbb{F}_q$-rational points of $X$ and $E$ is a divisor of $X$ with disjoint support from $P$, an equivalent representation can be found. Moreover in [19] an efficient computational approach is given to retrieve a triple that is isomorphic with the original representation, and, from this representation, an efficient decoding algorithm is obtained.

In this talk, we will show how an efficient decoding algorithm can be retrieved from an algebraic geometry code $C$ by means of error-correcting pairs [20] and arrays directly, that is without the detour via the representation $(X, P, E)$ of the code $C = C_L(X, P, E)$.

As a consequence we will have that algebraic geometry codes with certain parameters are not secure for the code-based McEliece public key cryptosystem.

1 Introduction

The security of code-based cryptosystems is founded on the (supposedly) hardness of decoding up to half the minimum distance. The minimum distance decoding problem was shown by Berlekamp-McEliece-Van Tilborg [1, 3] to be NP-hard. McEliece [21] proposed a PKC system using binary Goppa codes.

All known minimum distance decoding algorithms for general codes have exponential complexity in the length of the code. The complexity exponent of decoding general binary codes up to half the minimum distance has been lowered in a series of papers from above $1/3$ for brute force decoding to below $1/20$ by [2]. However there are several classes of codes such as the generalized Reed-Solomon (GRS), BCH, Goppa or algebraic geometry codes which have polynomial decoding algorithms that correct up to a certain bound which is at most half the minimum distance.

In 1986 [23] Niederreiter presented a dual version of McEliece cryptosystem which is equivalent in terms of security. This system differs from McEliece’s system since it uses a parity check matrix instead of a generator matrix of the code. Several classes of codes are proposed for code-base PKC systems such as subcodes of GRS codes, alternant codes which contains the Goppa codes as subclass, and algebraic geometry codes [12].

It was shown in [6, 14, 24, 26, 28] that the known efficient bounded distance decoding algorithms of the before mentioned codes can be described by a basic algorithm using an error-correcting pair. That means that the proposed McEliece cryptosystem that use these classes of codes can be viewed as using the error-correcting pair as a secret key. Hence the security of these PKC systems is not only based on the inherent intractability of bounded distance decoding but also on the assumption that it is difficult to retrieve an error-correcting pair.
2 Error-correcting pairs and arrays

From now on the dimension of a linear code $C$ will be denoted by $k(C)$ and its minimum distance by $d(C)$. Given two elements $a$ and $b$ in $\mathbb{F}_q^n$, the star multiplication is defined by coordinatewise multiplication, that is $a * b = (a_1 b_1, \ldots, a_n b_n)$ while the standard inner multiplication is defined by $a \cdot b = \sum_{i=1}^n a_i b_i$. In general, for two subsets $A$ and $B$ of $\mathbb{F}_q^n$ the set $A * B$ is given by \{a * b \mid a \in A \text{ and } b \in B\}. Furthermore $A \perp B$ if and only if $a \cdot b = 0$ for all $a \in A$ and $b \in B$.

Let $C$ be a linear code in $\mathbb{F}_q^n$. The pair $(A, B)$ of linear codes over $\mathbb{F}_q^n$ of length $n$ is called a \textit{t-error-correcting pair} (ECP) for $C$ if the following properties hold:

E.1 $(A * B) \perp C$,
E.2 $k(A) > t$,
E.3 $d(B^\perp) > t$,
E.4 $d(A) + d(C) > n$.

The notion of an error-correcting pair for a linear code was introduced in 1988 by Pellikaan [24, 26] and independently by Kötter [14, 15] in 1992. It is shown that a linear code in $\mathbb{F}_q^n$ with a $t$-error-correcting pair has a decoding algorithm which corrects up to $t$ errors with complexity $O((en)^3)$.

The existence of ECP’s for GRS and algebraic geometry codes was shown in [24, 26]. For many cyclic codes Duursma and Kötter in [6, 14, 15] have found ECP’s which correct beyond the designed BCH capacity.

An \textit{error-correcting array} is defined in [13, 27] for a sequence of codes. From it follows the \textit{Feng-Rao designed minimum distance} of the codes and the majority voting scheme of Feng-Rao [4, 5, 8] gives a decoding algorithm that decodes these codes up to half the Feng-Rao designed minimum distance with complexity $O(n^3)$. An equivalent formulation is given in terms of (weakly) well-behaving sequences [9, 10, 11].

3 Algebraic geometry codes

Let $\mathcal{X}$ be an algebraic curve defined over $\mathbb{F}_q$ with genus $g$. Let $\mathcal{P}$ be an $n$-tuple of $\mathbb{F}_q$-rational points on $\mathcal{X}$ and let $E$ be a divisor of $\mathcal{X}$ with disjoint support from $\mathcal{P}$ of degree $m$. Then the algebraic geometry code $C_L(\mathcal{X}, \mathcal{P}, E)$ is the image of the Riemann-Roch space $L(E)$ of rational functions with prescribed behavior of zeros and poles at $E$ under the evaluation map $ev_\mathcal{P}$. If $m < n$, then the dimension of the code $C_L(\mathcal{X}, \mathcal{P}, E)$ is at least $m + 1 - g$ and its minimum distance is at least $n - m$. If $m > 2g - 2$, then its dimension is $m + 1 - g$. The dual code $C_L(\mathcal{X}, \mathcal{P}, E)^\perp$ is again AG. If $m > 2g - 2$, then the dimension of the code $C_L(\mathcal{X}, \mathcal{P}, E)^\perp$ is at least $n - m - 1 + g$ and its minimum distance is at least $d^* = m - 2g + 2$, which is called the \textit{designed minimum distance}. If $m < n$, then its dimension is $n - m - 1 + g$.

Algebraic geometry codes were proposed by Niederreiter [23] and Janwa-Moreno [12] for code-based PKC systems. This system was broken for genus zero [29], one and two [7, 22] and for arbitrary genus for so called VSAP codes [16, 17, 18, 19].

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

$$\varphi_E : \mathcal{X} \rightarrow \mathbb{P}^r(\mathbb{F}_q)$$

defined by $\varphi_E(P) = (f_0(P) : \ldots : f_r(P))$. If $m > 2g$, then $r = m - g$. So $\varphi_E$ defines an embedding of the curve $\mathcal{X}$ of degree $m$ in $\mathbb{P}^r$. More precisely, let $\mathcal{Y} = \varphi_E(\mathcal{X})$, $Q_j = \varphi_E(P_j)$ and $Q = (Q_1, \ldots, Q_n)$. Then $\mathcal{Y}$ is a curve in $\mathbb{P}^{m-g}$ of degree $m$ and $\varphi_E$ is an isomorphism from $\mathcal{X}$ to $\mathcal{Y}$. Now $\varphi_E(E) = \mathcal{Y} \cdot H$ for every hyperplane $H$ of $\mathbb{P}^{m-g}(\mathbb{F}_q)$. If moreover $E$ is effective, then $\varphi_E(E) = \mathcal{Y} \cdot H$ for some hyperplane $H$ of $\mathbb{P}^{m-g}(\mathbb{F}_q)$. Let $F = \varphi_E(E)$, then $(\mathcal{Y}, Q, F)$ is a representation of $\mathcal{C}$ that is strict isomorphic with $(\mathcal{X}, \mathcal{P}, E)$.

If $m \geq 2g + 2$, then $I(\mathcal{Y})$ is generated by $I_2(\mathcal{Y})$. If moreover $n > 2m$, then $I_2(Q) = I_2(\mathcal{Y})$. Now $C_L(\mathcal{X}, \mathcal{P}, E)$ is called a \textit{very strong algebraic geometry (VSAG) code} if

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

It was shown that the representation by the triple $(\mathcal{X}, \mathcal{P}, E)$ of a VSAG code $C_L(\mathcal{X}, \mathcal{P}, E)$ is unique up to isomorphisms [16, 17, 18] and that such a triple can be retrieved efficiently [19].

130
4 Error-correcting pairs and arrays from VSAG codes

Let $C = C_L(X, P, E)^\perp$ be an AG code on a curve of genus $g$ with designed minimum distance $d^\ast$ and $m = \deg(E) > 2g-2$. Let $A = C_L(X, P, E - F)$, $B = C_L(X, P, F)$ and $C = C_L(X, P, E)^\perp$. Then $(A \ast B) \subseteq C^\perp$. If moreover $t = \left\lfloor (d^\ast - 1 - g)/2 \right\rfloor$ and $\deg(F) = m - t - g$, then $(A, B)$ is a $t$-ECP over $\mathbb{F}_q$ by [25, Theorem 1] and [26, Theorem 3.3]. So there are abundant ways to construct error-correcting pairs of an AG code.

This approach needs the efficient computation of the Riemann–Roch spaces $L(F)$ and $L(E-F)$ and such algorithms are available. If $e$ is sufficiently large and $m > 4g - 3$, then there exists a $\left(\lfloor (d^\ast - 1)/2 \rfloor\right)$-ECP over $\mathbb{F}_q^e$ by [28, Proposition 4.2], but no efficient way to obtain the pair is known.

In the following we construct ECP’s directly using subspaces of $\mathbb{F}_q^n$ and circumventing the use of the Riemann–Roch spaces. If we take $F = (m - t - g)P_1$ where $P_1$ is the first rational point of $\mathcal{P}$, then $L(E-F)$ is a subspace of $L(E)$, and $A = C_L(X, P, E - F)$ is a subspace of $C^\perp = C_L(X, P, E)$.

In fact $A$ is the space of those codewords in $C^\perp$ that are zero at the first position of multiplicity $m - t - g$ and this multiplicity can be controlled, since we have computed $I_2(Q)$ efficiently. Define $B_0 = (A \ast C)^\perp$, then $B_1 = (A \ast C) \subseteq B^\perp$. So $d(B_0^\perp) \geq d(B^\perp) > t$. Hence $(A, B_0)$ is a $t$-ECP for $C$.

There is one technical detail, note that $P_1$ is in the support of $E - F$ and $F$, but there is a generalized way to define algebraic geometry codes, using a local parameter as explained in [19], where it is no longer necessary to assume that $\mathcal{P}$ is disjoint from the support of the divisor $E$ in the definition of the code $C_L(X, P, E)$.

Similarly we can decode up to $\left\lfloor (d^\ast - 1)/2 \right\rfloor$ errors using arrays or well-behaving sequences and majority voting [4, 5, 9, 10, 11].

References


algebraic geometry codes.


[16] I. Márquez-Corbella, E. Martínez-Moro, and R. Pellikaan. Cryptanalysis of public-key cryp-
tosystems based on algebraic geometry codes. *Oberwolfach Preprints*, OWP 2012-01:1–17,
2012.

[17] I. Márquez-Corbella, E. Martínez-Moro, and R. Pellikaan. On the unique representation of

[18] I. Márquez-Corbella, E. Martínez-Moro, and R. Pellikaan. Evaluation of public-key cryp-
tosystems based on algebraic geometry codes. In *Proceedings of the Third International Cas-
tle Meeting on Coding Theory and Applications*, pages 199–204, Cardona Castle, Barcelona,
September 11-15, 2011.

of retrieving a representation of an algebraic geometry code. *submitted to Designs, Codes and
Cryptography*, 2013.

[20] I. Márquez-Corbella and R. Pellikaan. A characterization of MDS codes that have an error-
correcting pair. Lyngby, Denmark, 2012.


[23] H. Niederreiter. Knapsack-type crypto systems and algebraic coding theory. *Problems of


[27] R. Pellikaan. On the efficient decoding of algebraic-geometric codes. In *Eurocode ’92 (Udine,


[29] V.M. Sidelnikov and S.O. Shestakov. On the insecurity of cryptosystems based on generalized