Error-correcting pairs: a new approach to code-based cryptography

Irene Márquez-Corbella
INRIA, SACLAY & LIX LIX, CNRS UMR 7161
École Polytechnique 91120 Palaiseau Cedex

Ruud Pellikaan
Department of Mathematics and Computing Science,
Eindhoven University of Technology, P.O. Box 513, 5600 MB Eindhoven

irene.marquez-corbella@inria.fr

Abstract

McEliece proposed the first public-key cryptosystem based on linear error-correcting codes. A code with an efficient bounded distance decoding algorithm is chosen as secret key. It is assumed that the chosen code looks like a random code. The known efficient bounded distance decoding algorithms of the families of codes proposed for code-based cryptography, like Reed-Solomon codes, Goppa codes, alternant codes or algebraic geometry codes, can be described in terms of error-correcting pairs (ECP). That means that, the McEliece cryptosystem is not only based on the intractability of bounded distance decoding but also on the problem of retrieving an error-correcting pair from the public code. In this article we propose the class of codes with a t-ECP whose error-correcting pair that is not easily reconstructed from of a given generator matrix.

Keywords
Code-based cryptography, error-correcting pairs, McEliece cryptosystem

1 Introduction

The notion of Public Key Cryptography was first introduced in 1976 by Diffie and Helman. The problem of building Public Key Cryptosystems (PKC) is tied to the problem of making trapdoor primitives. Roughly, a *trapdoor function* is easy to compute but hard to invert except if you possess some "trapdoor" information. It is stated that

"At the heart of any public-key cryptosystem is a one-way function - a function $y = f(x)$ that is easy to evaluate but for which is computationally infeasible (one hopes) to find the inverse $x = f^{-1}(y)$".

The most famous trapdoor one-way functions are:

- **Integer factorization** where $x = (p, q)$ is a pair of prime numbers and $y = pq$ is its product. The best-known example of PKC is the Rivest-Shamir-Adleman (RSA) cryptosystem whose security is based on the hardness of factoring prime numbers from composite number, i.e. the intractability of inverting this one-way function.
- **Discrete logarithm** for which a group G (written multiplicatively) and an element $a \in G$ are required, then x is an integer and $y = a^x$. The security of the ElGamal cryptosystem or the Diffie-Hellman key exchange depends on the difficulty of finding discrete logarithms modulo a large prime.
- **Elliptic curve discrete logarithm** which it is actually a particular case of the previous function when G (written additively) is taken as an elliptic curve group. Then $x = P$ is a

point on the curve and $y = kP$ is another point on the curve obtained by the multiplication of P with a scalar k. Elliptic Curve Cryptography (ECC) proposed independently by Koblitz and Miller in 1985 is based on the difficulty of this function in the group of points on an elliptic curve over a finite field.

Only two years after the introduction of PKC, McEliece proposed the first PKC based on the theory of Error-correcting codes. Compared to RSA and discrete logarithm based schemes, McEliece has the advantage to resist quantum attacks so far, this property makes this scheme an interesting candidate for post-quantum cryptography. The security of this scheme relies on the difficulty of decoding a random code. Another advantage consists of its fast encryption and decryption schemes. However, its major drawback is the large size of the keys required to have a good security level.

McEliece encryption scheme: Let $\mathcal{F}$ be any family of linear codes with an efficient decoding algorithm. Every element of this family is represented by the triple $(\mathcal{C}, \mathcal{A}_{\mathcal{C}}, t)$ where $\mathcal{A}_{\mathcal{C}}$ denotes an efficient decoding algorithm for $\mathcal{C} \in \mathcal{F}$ correcting all patterns of t errors. The McEliece scheme can be summarized as follows:

Key generation: Consider any element $(\mathcal{C}, \mathcal{A}_{\mathcal{C}}, t) \in \mathcal{F}$. Let G be a generator matrix of $\mathcal{C}$. Then the *public key* and the *private key* are given respectively by

$$\mathcal{K}_{pub} = (G, t) \quad \text{and} \quad \mathcal{K}_{secret} = \mathcal{A}_{\mathcal{C}}.$$

Encryption: $\mathbf{y} = \mathbf{m}G + \mathbf{e}$ where $\mathbf{m}$ is the message and $\mathbf{e}$ is a random error vector of weight at most t.

Decryption: Using $\mathcal{K}_{secret}$, the receiver obtains $\mathbf{m}$.

Let $\mathcal{K}$ be the collection of all generator matrices of a chosen class of codes that have an efficient decoding algorithm that corrects all patterns of t errors. The security of McEliece cryptosystem is based on two assumptions:

A.1 In the average it is difficult to decode t errors for all codes that have the same parameters as the codes used as key.

A.2 It is difficult to distinguish arbitrary codes from those coming from $\mathcal{K}$.

Concerning the first assumption it might be that the class of codes is too small or too rigid. Recent progress is made with respect to the second assumption by [5, 2] where it is shown that one can distinguish between high rate Goppa, alternant and random codes.

In its original algorithm McEliece proposed the use of binary Goppa codes. Many attempts to replace Goppa codes by different families of codes have been proven to be insecure such as Generalized Reed-Solomon codes proposed in [15], subcodes of them in [1], Binary Reed–Muller codes in [18] or Algebraic Geometry codes in [7]; all of these schemes are subject to polynomial or sub-exponential time attacks [18, 14, 20, 4].

It was shown in [16] that the known efficient bounded distance decoding algorithms of Reed-Solomon, BCH, Goppa and algebraic geometry codes can be described by a basic algorithm using an *error correcting pair*. That means that for such classes of codes the security of the McEliece cryptosystem is not only based on the inherent intractability of bounded distance decoding but also on the one-way function

$$x = (A, B) \mapsto y = A * B,$$

where (A, B) is a t-error-correcting pair.

The aim of this paper is to study the subclass of linear codes formed by those linear codes $\mathcal{C}$ whose error correcting pair is not easily reconstructed from $\mathcal{C}$. In [3, 4] an attack is presented against algebraic geometry codes and subcodes of them, this attack consists of the computation of an ECP in order to decode the public code. Take notice that this attack is neither a generic decoding attack like *Information Set Decoding*, nor a structural attack as the structure of the code is not retrieved. It corresponds, rather, to a cryptanalysis of the new trapdoor function of code-based cryptography as presented above.

2 Error-correcting pairs

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 $\mathbf{a}$ and $\mathbf{b}$ in $\mathbb{F}_q^n$, the *Schur product* is defined by coordinatewise multiplication, that is $\mathbf{a} * \mathbf{b} = (a_1 b_1, \ldots, a_n b_n)$. While the *standard inner product* is defined by $\mathbf{a} \cdot \mathbf{b} = \sum_{i=1}^{n} a_i b_i$. In general, for two subsets A and B of $\mathbb{F}_q^n$ the set $A * B$ is given by

$$A * B := \langle \mathbf{a} * \mathbf{b} \mid \mathbf{a} \in A \text{ and } \mathbf{b} \in B \rangle$$

For $B = A$, then $A * A$ is denoted as $A^{(2)}$. A new, we define $A^{(t)}$ by induction: $A^{(1)} = A$ and $A^{(t+1)} = A * A^{(t)}$ for any positive integer t. Furthermore, we denote by $A \perp B$ if $\mathbf{a} \cdot \mathbf{b} = 0$ for all $\mathbf{a} \in A$ and $\mathbf{b} \in B$.

Definition 1. *Let $\mathcal{C}$ be a linear code in $\mathbb{F}_q^n$. A pair (A, B) of $\mathbb{F}_{q^m}$-linear codes of length n is called a* t-error correcting pair *(ECP) for $\mathcal{C}$ if the following conditions hold:*

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

The notion of an error-correcting pair for a linear code was introduced by Pellikaan [16] and independently by Kötter [8]. 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 $\mathcal{O}\left((mn)^3\right)$.

2.1 Examples of existence of ECP for many known codes

Example 1 (Generalized Reed-Solomon codes)**.** *Let $\mathbf{a}$ be an n-tuple of mutually distinct elements of $\mathbb{F}_q$ and $\mathbf{b}$ be an n-tuple of nonzero elements of $\mathbb{F}_q$. Then the* generalized Reed-Solomon *code* $\mathrm{GRS}_k(\mathbf{a}, \mathbf{b})$ *is defined by*

$$\mathrm{GRS}_k(\mathbf{a}, \mathbf{b}) = \{(f(a_1)b_1, \ldots, f(a_n)b_n) \mid f(X) \in \mathbb{F}_q[X] \text{ and } \deg(f(X)) < k\}.$$

Define by induction $\mathbf{a}^1 = \mathbf{a}$ and $\mathbf{a}^{i+1} = \mathbf{a} * \mathbf{a}^i$. Then $\mathrm{GRS}_k(\mathbf{a}, \mathbf{b})$ is generated by the elements $\mathbf{b} * \mathbf{a}^i$ with $i = 0, \ldots, k-1$. If $k \leq n \leq q$, then $\mathrm{GRS}_k(\mathbf{a}, \mathbf{b})$ is an $[n, k, n-k+1]$ code. Furthermore the dual of a GRS code is again a GRS code, in particular $\mathrm{GRS}_k(\mathbf{a}, \mathbf{b})^{\perp} = \mathrm{GRS}_{n-k}(\mathbf{a}, \mathbf{c})$ for some $\mathbf{c}$ that is explicitly known.

GRS codes are the prime examples of codes that have a t-ECP. Indeed, let

$$A = \mathrm{GRS}_{t+1}(\mathbf{a}, \mathbf{b}), \quad B = \mathrm{GRS}_t(\mathbf{a}, \mathbf{c}) \quad \text{and} \quad C = \mathrm{GRS}_{2t}(\mathbf{a}, \mathbf{b} * \mathbf{c})^{\perp}.$$

Then (A, B) is a t-ECP for C. Conversely let $C = \mathrm{GRS}_k(\mathbf{a}, \mathbf{b})$, then $A = \mathrm{GRS}_{t+1}(\mathbf{a}, \mathbf{c})$ and $B = \mathrm{GRS}_t(\mathbf{a}, \mathbf{1})$ is a t-ECP for C where $t = \left\lfloor \frac{n-k}{2} \right\rfloor$ and $\mathbf{c} \in \mathbb{F}_q^n$ is a nonzero vector such that $\mathrm{GRS}_k(\mathbf{a}, \mathbf{b})^{\perp} = \mathrm{GRS}_{n-k}(\mathbf{a}, \mathbf{c})$.

Moreover if C is an $[n, n-2t, 2t+1]$ code which has a t-error-correcting pair, then C is a GRS code. This is trivial if $t = 1$, proved for $t = 2$ in [17, Theorem 6.5] and for arbitrary t in [12].

The family of GRS codes was mentioned by Niederreiter [15] for the McEliece cryptosystem as an attempt to shorten the key size (since GRS are MDS codes) while keeping the same security level in comparison to the classical binary Goppa codes. However GRS codes have been proven to be insecure by Sidelnikov-Shestakov [18].

Example 2 (Algebraic geometry codes)**.** *Let $\mathcal{X}$ be a smooth projective geometrically connected curve over a finite field $\mathbb{F}_q$ of genus g, $\mathcal{P} = (P_1, \ldots, P_n)$ be an n-tuple of mutually distinct $\mathbb{F}_q$-rational points of $\mathcal{X}$ and E be a divisor of $\mathcal{X}$ of degree m with disjoint support from $\mathcal{P}$.*

The algebraic geometry (AG) code $\mathcal{C}_L(\mathcal{X}, P, E)$ of length n over $\mathbb{F}_q$ 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 $\mathrm{ev}_P : \ L(E) \longrightarrow \mathbb{F}_q^n$ defined by $\mathrm{ev}_P(f) = (f(P_1), \ldots, f(P_n))$.

If $A = \mathcal{C}_L(\mathcal{X}, P, E)$ and $B = \mathcal{C}_L(\mathcal{X}, P, F)$, then $A * B \subseteq \mathcal{C}_L(\mathcal{X}, P, E + F)$, so there are abundant ways of constructing error-correcting pairs of an AG code. Indeed, the codes (A, B) defined by $A = \mathcal{C}_L(\mathcal{X}, P, F)$ and $B = \mathcal{C}_L(\mathcal{X}, P, E - F)$ with $\deg(E) > \deg(F) \geq t + g$ is a t-ECP for $\mathcal{C}_L(\mathcal{X}, P, E)^{\perp}$, where g is the genus of the curve $\mathcal{X}$, see [16, Theorem 3.3]. Such a pair (A, B) for $\mathcal{C}_L(\mathcal{X}, P, E)^{\perp}$ always exists whenever $\deg(E) > 2g - 2$. Moreover, if e is sufficiently large, then there exists a t-ECP over $\mathbb{F}_{q^e}$ with $t = \lfloor (d^* - 1)/2 \rfloor$ by [17, Proposition 4.2].

AG codes have efficient decoding algorithms that correct up to half the designed minimum distance which makes them particularly appealing for code-based cryptography. Janwa and Moreno [7] proposed to use the collection of AG codes and their subfield subcodes for the McEliece cryptosystem. The proposal of using AG code is broken; firstly by Faure and Minder [6] for codes on curves of genus $g \leq 2$ and recently, for arbitrary genus in [10, 11] and [4] where the authors propose a polynomial time attack on the code length.

Example 3 ((Subfield) subcodes)**.** *Let C be an $\mathbb{F}_q$-linear code that is a (subfield)subcode of an $\mathbb{F}_{q^m}$-linear code D that has (A, B) as t-ECP. Then condition (E.1) holds for (A, B) with respect to D, i.e. $\mathbf{a} * \mathbf{b} \cdot \mathbf{d} = 0$ for all $\mathbf{d}$ in D. Hence $\mathbf{a} * \mathbf{b} \cdot \mathbf{c} = 0$ for all $\mathbf{c}$ in C, since $C \subseteq D$. Moreover, conditions $(E.2)$, $(E.3)$ and $(E.4)$ hold. So (A, B) is also a t-ECP for C.*

Although the PKC with GRS codes is completely broken, subsequent variants [1, 19] were proposed in a bid to hide the strong algebraic structure of these codes but without success. The main idea is to use subcodes of the original GRS codes rather than the GRS code itself. See [20, 9, 2] for several cryptanalysis of these schemes. Recall that GRS codes is the subclass of AG codes on the projective line, that is the algebraic curve of genus zero. For the general case, the proposal of using subcodes of AG codes is also not secure [3].

Example 4 (Alternant codes)**.** *Let C be a subfield subcode of a code D that has (A, B) as a t-ECP, then (A, B) is also a t-ECP for C.*

Let $\mathbf{a}$ be an n-tuple of mutually distinct elements of $\mathbb{F}_{q^m}$ and $\mathbf{b}$ be an n-tuple of nonzero elements of $\mathbb{F}_{q^m}$. The alternant code $\mathrm{Alt}_r(\mathbf{a}, \mathbf{b})$ is the $\mathbb{F}_q$-linear restriction: $\mathrm{Alt}_r(\mathbf{a}, \mathbf{b}) = \mathbb{F}_q^n \cap \mathrm{GRS}_r(\mathbf{a}, \mathbf{b})^\perp$.

Therefore, let us define the codes $A = \mathrm{GRS}_{t+1}(\mathbf{a}, \mathbf{1})$ and $B = \mathrm{GRS}_t(\mathbf{a}, \mathbf{b})$ over $\mathbb{F}_{q^m}$, then (A, B) is a t-ECP over $\mathbb{F}_{q^m}$ for $\mathrm{Alt}_{2t}(\mathbf{a}, \mathbf{b})$.

Example 5 (Goppa codes)**.** *A Goppa code associated to a Goppa polynomial of degree r can be viewed as an alternant code. Therefore this family of codes has an $\lfloor \frac{r}{2} \rfloor$-error correcting pair. In the binary case with an associated square free polynomial the Goppa code has an r-ECP.*

The McEliece cryptosystem with Goppa codes is still unbroken for suitable parameters choices.

3 Distinguishing a code with an ECP

Let $\mathcal{K}$ be a collection of generator matrices of codes that have a t-ECP. In this section we address assumption A.2 whether we can distinguish arbitrary codes from those coming from $\mathcal{K}$.

Theorem 1. *Let C be an $[n, k]$ code with $n > \binom{k+1}{2}$ chosen at random. Then the dimension of the square code $C^{(2)}$ is equal to $\binom{k+1}{2}$ with high probability.*

Proof. See [13, Proposition 2]. □

This theorem could be used for detecting the family of codes that have an ECP since this family have a different behavior from the one that one would expect from a random code.

Remark 1. *Let (A, B) be a pair of codes with parameters $[n, t+1, n-1]$ and $[n, t, n-t+1]$, respectively; and define the code $C = (A * B)^\perp$, then (A, B) is a t-ECP for C by [17, Corollary 3.4].*

If $t(t+1) < n$, then the dimension of $A * B$ is at most $t(t+1)$. Moreover, in [13, Appendix A] we have shown that the dimension of C is equal to $n - t(t+1)$ for random choices of A and B.

Let $D = C^\perp$, then

$$\dim(D^{(2)}) \leq \binom{t+2}{2}\binom{t+1}{2}$$

which is about half the expected $\binom{t(t+1)}{2}$ in case $\binom{t(t+1)}{2} < n$ by Theorem 1.

References

[1] T. Berger and P. Loidreau. How to mask the structure of codes for a cryptographic use. *Des. Codes Cryptogr.*, 35:63–79, 2005.

[2] A. Couvreur, P. Gaborit, V. Gauthier-Umaña, A. Otmani, and J. P. Tillich. Distinguisher-based attacks on public-key cryptosystems using Reed-Solomon codes. *Designs, Codes and Cryptography*, pages 1–26, 2014.

[3] A. Couvreur, I. Márquez-Corbella, and R. Pellikaan. Cryptanalysis of public-key cryptosystems that use subcodes of algebraic geometry codes. Submitted to the conference 4ICMCTA, 2014.

[4] A. Couvreur, I. Márquez-Corbella, and R. Pellikaan. A polynomial time attack against algebraic geometry code based public key cryptosystems. Accepted for the conference ISIT 2014, 2014.

[5] J.-C. Faugere, V. Gauthier-Umana, A. Otmani, L. Perret, and J.-P. Tillich. A distinguisher for high-rate McEliece cryptosystems. *Information Theory, IEEE Transactions on*, 59(10):6830–6844, 2013.

[6] C. Faure and L. Minder. Cryptanalysis of the McEliece cryptosystem over hyperelliptic codes. In *ACCT 2008*, pages 99–107, 2008.

[7] H. Janwa and O. Moreno. McEliece public cryptosystem using algebraic-geometric codes. *Des. Codes Cryptogr.*, 8:293–307, 1996.

[8] R. Kötter. A unified description of an error locating procedure for linear codes. In *Proceedings of Algebraic and Combinatorial Coding Theory*, pages 113–117, Voneshta Voda, 1992.

[9] I. Márquez-Corbella, E. Martínez-Moro, and R. Pellikaan. The non-gap sequence of a subcode of a generalized Reed-Solomon code. *Des. Codes Cryptogr.*, 66(1-3):317–333, 2013.

[10] I. Márquez-Corbella, E. Martínez-Moro, and R. Pellikaan. On the unique representation of very strong algebraic geometry codes. *Designs, Codes and Cryptography*, 70(1-2):215–230, 2014.

[11] I. Márquez-Corbella, E. Martínez-Moro, R. Pellikaan, and D. Ruano. Computational aspects of retrieving a representation of an algebraic geometry code. *Journal of Symbolic Computation*, 64(0):67 – 87, 2014. Mathematical and computer algebra techniques in cryptology.

[12] I. Márquez-Corbella and R. Pellikaan. A characterization of MDS codes that have an error-correcting pair. Preprint.

[13] I. Márquez-Corbella and R. Pellikaan. Error-correcting pairs for a public-key cryptosystem. *arXiv preprint:1205.3647v1*, 2012.

[14] L. Minder and A. Shokrollahi. Cryptanalysis of the Sidelnikov cryptosystem. In *EUROCRYPT 2007*, volume 4515 of *Lecture Notes in Comput. Sci.*, pages 347–360. Springer-Verlag Berlin Heidelberg, 2007.

[15] H. Niederreiter. Knapsack-type cryptosystems and algebraic coding theory. *Problems of Control and Information Theory*, 15(2):159–166, 1986.

[16] R. Pellikaan. On decoding by error location and dependent sets of error positions. *Discrete Math.*, 106–107:369–381, 1992.

[17] R. Pellikaan. On the existence of error-correcting pairs. *Statistical Planning and Inference*, 51:229–242, 1996.

[18] 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.

[19] C. Wieschebrink. Two NP-complete Problems in Coding Theory with an Application in Code Based Cryptography. In *IEEE International Symposium on Information Theory*, pages 1733–1737. 2006.

[20] C. Wieschebrink. Cryptanalysis of the Niederreiter public key scheme based on GRS subcodes. In *Post-Quantum Cryptography*, volume 6061 of *Lecture Notes in Comput. Sci.*, pages 61–72. Springer-Verlag Berlin Heidelberg, 2010.