

See discussions, stats, and author profiles for this publication at: <https://www.researchgate.net/publication/224871823>

A Distinguisher-Based Attack on a Variant of McEliece's Cryptosystem Based on Reed-Solomon Codes

Article · April 2012

Source: arXiv

CITATIONS

17

READS

86

3 authors, including:



[Ayoub Otmani](#)

Université de Rouen

49 PUBLICATIONS 1,228 CITATIONS

SEE PROFILE

Some of the authors of this publication are also working on these related projects:



Security proofs and code-based cryptography [View project](#)

A Distinguisher-Based Attack on a Variant of McEliece's Cryptosystem Based on Reed-Solomon Codes

Valérie Gauthier¹, Ayoub Otmani¹ and Jean-Pierre Tillich²

¹ GREYC - Université de Caen - Ensicaen

Boulevard Maréchal Juin, 14050 Caen Cedex, France.

valerie.gauthier01@unicaen.fr, ayoub.otmani@unicaen.fr,

² SECRET Project - INRIA Rocquencourt

Domaine de Voluceau, B.P. 105 78153 Le Chesnay Cedex - France

jean-pierre.tillich@inria.fr

Abstract. Baldi et *al.* proposed a variant of McEliece's cryptosystem. The main idea is to replace its permutation matrix by adding to it a rank 1 matrix. The motivation for this change is twofold: it would allow the use of codes that were shown to be insecure in the original McEliece's cryptosystem, and it would reduce the key size while keeping the same security against generic decoding attacks. The authors suggest to use generalized Reed-Solomon codes instead of Goppa codes. The public code built with this method is not anymore a generalized Reed-Solomon code. On the other hand, it contains a very large secret generalized Reed-Solomon code. In this paper we present an attack that is built upon a distinguisher which is able to identify elements of this secret code. The distinguisher is constructed by considering the code generated by component-wise products of codewords of the public code (the so-called "square code"). By using square-code dimension considerations, the initial generalized Reed-Solomon code can be recovered which permits to decode any ciphertext. A similar technique has already been successful for mounting an attack [GOT12] against a homomorphic encryption scheme suggested by [BL11]. This work can be viewed as another illustration of how a distinguisher of Reed-Solomon codes can be used to devise an attack on cryptosystems based on them.

Keywords. Code-based cryptography, McEliece, distinguisher.

1 Introduction

Reed-Solomon codes have been suggested for the first time in a public-key cryptosystem in [Nie86] but it was shown to be insecure in [SS92]. The attack recovers the underlying Reed-Solomon allowing the decoding of any encrypted data obtained from a McEliece-type cryptosystem based on them. The McEliece cryptosystem [McE78] on the other hand uses Goppa codes. Since its apparition, it has withstood many attacks and after more than thirty years now, it still belongs to the very few unbroken public key cryptosystems. This situation substantiates the claim that inverting the encryption function, and in particular recovering the private key from public data, is intractable.

No significant breakthrough has been observed with respect to the problem of recovering the private key [Gib91,LS01]. This has led to claim that the generator matrix of a binary Goppa code does not disclose any visible structure that an attacker could exploit. This is strengthened by the fact that Goppa codes share many characteristics with random codes: for instance they asymptotically meet the Gilbert-Varshamov bound, they typically have a trivial permutation group, *etc.* This is the driving motivation for conjecturing the hardness of the Goppa code distinguishing problem, which asks whether a Goppa code can be distinguished from a random code. This has become a classical belief in code-based cryptography, and semantic security in the random oracle model [NIK08], CCA2 security in the standard model [DMQN09] and security in the random oracle

model against existential forgery [Dal07] of the signature scheme [CFS01] are now proved by using this assumption.

In [FGO⁺11], an algorithm that manages to distinguish between a random code and a Goppa code has been introduced. This work without undermining the security of [McE78] prompts to wonder whether it would be possible to devise an attack based on such a distinguisher. It was found out in [MCP12] that our distinguisher [FGO⁺11] has an equivalent but simpler description in terms of the component-wise product of codes. This notion was first put forward in coding theory to unify many different algebraic decoding algorithms [Pel92,Köt92]. Recently, it was used in [MCMMP11a] to study the security of cryptosystems based on Algebraic-Geometric codes. Powers of codes are also studied in the context of secure multi-party computation (see for example [CCCX09,CCX11]). This distinguisher is even more powerful in the case of Reed-Solomon codes than for Goppa codes because, whereas for Goppa codes it is only successful for rates close to 1, it can distinguish Reed-Solomon codes of any rate from random codes.

In this paper we propose a cryptanalysis against a variant of McEliece’s cryptosystem [McE78] proposed in [BBC⁺11] which is based on the aforementioned version of our distinguisher presented in [MCP12]. The main idea of this proposal is to replace the permutation matrix used to hide the secret generator matrix by another matrix of the form $\mathbf{I} + \mathbf{R}$ where \mathbf{I} is a permutation matrix and \mathbf{R} is a rank 1 matrix. The motivation for this change is twofold: it would allow the use of codes that were shown to be insecure in the original McEliece’s cryptosystem. It also allows to reduce the size of the keys which is a major drawback in code-based cryptography. In this new setting it was suggested to use generalized Reed-Solomon codes. The public code obtained with this method is not anymore a generalized Reed-Solomon code. On the other hand, it contains a very large secret generalized Reed-Solomon code. Our attack consists in identifying this secret Reed-Solomon code by picking at random a very small number of elements of the public code and computing the dimension of the vector space generated by component-wise products of these elements with the public code. This technique is precisely what enables to distinguish a Reed-Solomon code from a random code. In the case at hand, the dimension of the vector space is much smaller when all elements belong to the secret Reed-Solomon code than in the generic case. This is precisely what allows to recover the secret Reed-Solomon code. Once this secret code is obtained, it is then possible to completely recover the initial generalized Reed-Solomon code by using the square-code construction as in [Wie10]. We are then able to decode any ciphertext.

It should also be pointed out that the properties of Reed-Solomon codes with respect to the component-wise product of codes have already been used to cryptanalyze a McEliece-like scheme [BL05] based on subcodes of Reed-Solomon codes [Wie10]. The use of this product is nevertheless different in [Wie10] from the way we use it here. Note also that our attack is not an adaptation of the Sidelnikov and Shestakov approach [SS92]. Our approach is completely new: it illustrates how a distinguisher that detects an abnormal behavior can be used to recover the private key. It should also be added that a very similar technique has been successful to attack [GOT12] a homomorphic encryption scheme based on Reed-Solomon codes [BL11].

Organisation of the paper. In Section 2 we recall important notions from coding theory. In Section 3 we describe the cryptosystem proposed in [BBC⁺11] and in Section 4 we explain an attack of this system.

2 Reed-Solomon Codes and the Square Code

We recall in this section a few relevant results and definitions from coding theory and bring in the fundamental notion which is used in the attack, namely the square code. A linear *code* \mathcal{C} of length n and *dimension* k over a finite field $GF(q)$ of q elements is a subspace of dimension k of the full space $GF(q)^n$. It is generally specified by a full-rank matrix called a generator matrix which is a $k \times n$ matrix \mathbf{G} (with $k \leq n$) over $GF(q)$ whose rows span the code:

$$\mathcal{C} = \{ \mathbf{u}\mathbf{G} \mid \mathbf{u} \in GF(q)^k \}.$$

It can also be specified by a *parity-check* matrix \mathbf{H} , which is a matrix whose right kernel is equal to the code, that is

$$\mathcal{C} = \{ \mathbf{x} \in GF(q)^n \mid \mathbf{H}\mathbf{x}^T = 0 \},$$

where \mathbf{x}^T stands for the column vector which is the transpose of the row vector \mathbf{x} . The *rate* of the code is given by the ratio $\frac{k}{n}$. Code-based public-key cryptography focuses on linear codes that have a polynomial time decoding algorithm. The role of decoding algorithms is to correct errors of prescribed weight. We say that a decoding algorithm corrects t errors if it recovers \mathbf{u} from the knowledge of $\mathbf{u}\mathbf{G} + \mathbf{e}$ for all possible $\mathbf{e} \in \mathbb{F}_q^n$ of weight at most t .

Reed-Solomon codes form a special case of codes with a very powerful low complexity decoding algorithm. It will be convenient to use the definition of Reed-Solomon codes and generalized Reed-Solomon codes as *evaluation codes*

Definition 1 (Reed-Solomon code and generalized Reed-Solomon code). *Let k and n be integers such that $1 \leq k < n \leq q$ where q is a power of a prime number. Let $\mathbf{x} = (x_1, \dots, x_n)$ be an n -tuple of distinct elements of $GF(q)$. The Reed-Solomon code $\mathbf{RS}_k(\mathbf{x})$ of dimension k is the set of $(p(x_1), \dots, p(x_n))$ when p ranges over all polynomials of degree $\leq k-1$ with coefficients in $GF(q)$. The generalized Reed-Solomon code $\mathbf{GRS}_k(\mathbf{x}, \mathbf{y})$ of dimension k is associated to a couple $(\mathbf{x}, \mathbf{y}) \in GF(q)^n \times GF(q)^n$ where \mathbf{x} is chosen as above and the entries y_i are arbitrary non zero elements in $GF(q)$. It is defined as the set of $(y_1 p(x_1), \dots, y_n p(x_n))$ where p ranges over all polynomials of degree $\leq k-1$ with coefficients in $GF(q)$.*

Generalized Reed-Solomon codes are quite important in coding theory due to the conjunction of several factors such as:

1. Their minimum distance d is maximal among all codes of the same dimension k and length n because d is equal to $n - k + 1$.
2. They can be efficiently decoded in polynomial time when the number of errors is less than or equal to $\left\lfloor \frac{d-1}{2} \right\rfloor = \left\lfloor \frac{n-k}{2} \right\rfloor$.

It has been suggested to use them in a public-key cryptosystem for the first time in [Nie86] but it was discovered that this scheme is insecure in [SS92]. Sidelnikov and Shestakov namely showed that it is possible to recover in polynomial time for any generalized Reed-Solomon code a possible couple (\mathbf{x}, \mathbf{y}) which defines it. This is all what is needed to decode efficiently such codes and is therefore enough to break the Niederreiter cryptosystem suggested in [Nie86] or a McEliece type cryptosystem [McE78] when Reed-Solomon are used instead of Goppa codes.

We could not find a way to adapt the Sidelnikov and Shestakov approach for recovering the secret Generalized Reed-Solomon code from the public generating matrix \mathbf{G}_{pub} in the Baldi et al. scheme. However a Reed-Solomon displays a quite peculiar property with respect to the component-wise product which is denoted by $\mathbf{a} \star \mathbf{b}$ for two vectors $\mathbf{a} = (a_1, \dots, a_n)$ and $\mathbf{b} = (b_1, \dots, b_n)$ and which is defined by $\mathbf{a} \star \mathbf{b} \stackrel{\text{def}}{=} (a_1 b_1, \dots, a_n b_n)$. This can be seen by bringing in the following definition

Definition 2 (Star product of codes – Square code). Let \mathcal{A} and \mathcal{B} be two codes of length n . The star product code denoted by $\langle \mathcal{A} \star \mathcal{B} \rangle$ of \mathcal{A} and \mathcal{B} is the vector space spanned by all products $\mathbf{a} \star \mathbf{b}$ where \mathbf{a} and \mathbf{b} range over \mathcal{A} and \mathcal{B} respectively. When $\mathcal{B} = \mathcal{A}$, $\langle \mathcal{A} \star \mathcal{A} \rangle$ is called the square code of \mathcal{A} and is denoted by $\langle \mathcal{A}^2 \rangle$.

It is clear that $\langle \mathcal{A} \star \mathcal{B} \rangle$ is also generated by the $\mathbf{a}_i \star \mathbf{b}_j$'s where the \mathbf{a}_i 's and the \mathbf{b}_j 's form a basis of \mathcal{A} and \mathcal{B} respectively. Therefore

Proposition 1.

$$\dim(\langle \mathcal{A} \star \mathcal{B} \rangle) \leq \dim(\mathcal{A}) \dim(\mathcal{B}).$$

We expect that the square code when applied to a random linear code should be a code of dimension of order $\min \left\{ \binom{k+1}{2}, n \right\}$. Actually it can be shown by the proof technique of [FGO⁺11] that with probability going to 1 as k tends to infinity, the square code is of dimension $\min \left\{ \binom{k+1}{2}(1 + o(1)), n \right\}$ when k is of the form $k = o(n^{1/2})$, see also [MCP12]. On the other hand generalized Reed Solomon codes behave in a completely different way

Proposition 2. $\langle \mathbf{GRS}_k(\mathbf{x}, \mathbf{y})^2 \rangle = \mathbf{GRS}_{2k-1}(\mathbf{x}, \mathbf{y} \star \mathbf{y})$.

This follows immediately from the definition of a generalized Reed Solomon code as an evaluation code since the star product of two elements $\mathbf{c} = (y_1 p(x_1), \dots, y_n p(x_n))$ and $\mathbf{c}' = (y_1 q(x_1), \dots, y_n q(x_n))$ of $\mathbf{GRS}_k(\mathbf{x}, \mathbf{y})$ where p and q are two polynomials of degree at most $k-1$ is of the form

$$\mathbf{c} \star \mathbf{c}' = (y_1^2 p(x_1) q(x_1), \dots, y_n^2 p(x_n) q(x_n)) = (y_1^2 r(x_1), \dots, y_n^2 r(x_n))$$

where r is a polynomial of degree $\leq 2k-2$. Conversely, any element of the form $(y_1^2 r(x_1), \dots, y_n^2 r(x_n))$ where r is a polynomial of degree less than or equal to $2k-1$ is a linear combination of star products of two elements of $\mathbf{GRS}_k(\mathbf{x}, \mathbf{y})$.

This proposition shows that the square code is only of dimension $2k-1$ when $2k-1 \leq n$, which is quite unusual. This property can also be used in the case $2k-1 > n$. To see this, consider the dual of the Reed-Solomon code. The dual \mathcal{C}^\perp of a code \mathcal{C} of length n over $GF(q)$ is defined by

$$\mathcal{C}^\perp = \{ \mathbf{x} \in GF(q)^n \mid \mathbf{x} \cdot \mathbf{y} = 0, \forall \mathbf{y} \in \mathcal{C} \},$$

where $\mathbf{x} \cdot \mathbf{y} = \sum x_i y_i$ stands for the standard inner product between elements of $GF(q)^n$. The dual of a generalized Reed-Solomon code is itself a generalized Reed-Solomon code, see [MS86, Theorem 4, p.304]

Proposition 3.

$$\mathbf{GRS}_k(\mathbf{x}, \mathbf{y})^\perp = \mathbf{GRS}_{n-k}(\mathbf{x}, \mathbf{y}')$$

where the length of $\mathbf{GRS}_k(\mathbf{x}, \mathbf{y})$ is n and \mathbf{y}' is a certain element of $GF(q)^n$ depending on \mathbf{x} and \mathbf{y} .

Therefore when $2k-1 > n$ a Reed-Solomon code $\mathbf{GRS}_k(\mathbf{x}, \mathbf{y})$ can also be distinguished from a random linear code of the same dimension by computing the dimension of $\langle (\mathbf{GRS}_k(\mathbf{x}, \mathbf{y})^\perp)^2 \rangle$. We have in this case

$$\langle (\mathbf{GRS}_k(\mathbf{x}, \mathbf{y})^\perp)^2 \rangle = \langle \mathbf{GRS}_{n-k}(\mathbf{x}, \mathbf{y}')^2 \rangle = \langle \mathbf{GRS}_{2n-2k-1}(\mathbf{x}, \mathbf{y}' \star \mathbf{y}') \rangle$$

and we obtain a code of dimension $2n - 2k - 1$.

The star product of two codes is the fundamental notion used in the decoding algorithm based on an error correcting pair [Pel92,Köt92] which unifies common ideas to many algebraic decoding algorithms. It has been used for the first time to cryptanalyze a McEliece-like scheme [BL05] based on subcodes of Reed-Solomon codes [Wie10]. The use of the star product is nevertheless different in [Wie10] from the way we use it here. In this paper, the star product is used to identify for a certain subcode \mathcal{C} of a generalized Reed-Solomon code $\mathbf{GRS}_k(\mathbf{x}, \mathbf{y})$ a possible pair (\mathbf{x}, \mathbf{y}) . This is achieved by computing $\langle \mathcal{C}^2 \rangle$ which in the case which is considered turns out to be equal to $\langle \mathbf{GRS}_k(\mathbf{x}, \mathbf{y})^2 \rangle$ which is equal to $\mathbf{GRS}_{2k-1}(\mathbf{x}, \mathbf{y} \star \mathbf{y})$. The Sidelnikov and Shestakov algorithm is then used on $\langle \mathcal{C}^2 \rangle$ to recover a possible $(\mathbf{x}, \mathbf{y} \star \mathbf{y})$ pair to describe $\langle \mathcal{C}^2 \rangle$ as a generalized Reed-Solomon code. From this, a possible (\mathbf{x}, \mathbf{y}) pair for which $\mathcal{C} \subset \mathbf{GRS}_k(\mathbf{x}, \mathbf{y})$ is deduced.

3 Baldi et al. Variant of McEliece's Cryptosystem

The cryptosystem proposed by Baldi et al. in [BBC⁺11] is a variant of McEliece's cryptosystem [McE78]. The main idea is to replace the permutation matrix used to hide the secret generator matrix by one of the form $\mathbf{II} + \mathbf{R}$ where \mathbf{II} is a permutation matrix and \mathbf{R} is a rank-one matrix. From the authors' point of view, this new kind of transformations would allow to use families of codes that were shown insecure in the original McEliece's cryptosystem. In particular, it would become possible to use generalized Reed-Solomon codes in this new framework. The scheme can be summarized as follows.

Secret key.

- \mathbf{G}_{sec} is a generator matrix of a generalized Reed-Solomon code of length n and dimension k over $GF(q)$,
- $\mathbf{Q} \stackrel{\text{def}}{=} \mathbf{II} + \mathbf{R}$ where \mathbf{II} is an $n \times n$ permutation matrix,
- \mathbf{R} is a rank-one matrix over $GF(q)$ such that \mathbf{Q} is invertible,
- \mathbf{S} is a $k \times k$ random invertible matrix over $GF(q)$.

Public key. $\mathbf{G}_{pub} \stackrel{\text{def}}{=} \mathbf{S}^{-1} \mathbf{G}_{sec} \mathbf{Q}^{-1}$.

Encryption. The ciphertext $\mathbf{c} \in GF(q)^n$ of a plaintext $\mathbf{m} \in GF(q)^k$ is obtained by drawing at random $\mathbf{e} \in GF(q)^n$ of weight less than or equal to $\frac{n-k}{2}$ and computing $\mathbf{c} \stackrel{\text{def}}{=} \mathbf{m} \mathbf{G}_{pub} + \mathbf{e}$.

Decryption. It consists in performing the three following steps:

1. Guessing the value of \mathbf{eR} ;
2. Calculating $\mathbf{c}' \stackrel{\text{def}}{=} \mathbf{cQ} - \mathbf{eR} = \mathbf{mS}^{-1} \mathbf{G}_{sec} + \mathbf{eQ} - \mathbf{eR} = \mathbf{mS}^{-1} \mathbf{G}_{sec} + \mathbf{eII}$ and using the decoding algorithm of the generalized Reed-Solomon code to recover \mathbf{mS}^{-1} from the knowledge of \mathbf{c}' ;
3. Multiplying the result of the decoding by \mathbf{S} to recover \mathbf{m} .

The first step of the decryption, that is guessing the value \mathbf{eR} , boils down to trying q elements (in the worst case) since \mathbf{R} is of rank 1. Indeed, there exist $\boldsymbol{\alpha} \stackrel{\text{def}}{=} (\alpha_1, \dots, \alpha_n)$ and $\boldsymbol{\beta} \stackrel{\text{def}}{=} (\beta_1, \dots, \beta_n)$ in $GF(q)^n$ such that $\mathbf{R} \stackrel{\text{def}}{=} \boldsymbol{\alpha}^T \boldsymbol{\beta}$. Therefore $\mathbf{eR} = \mathbf{e} \boldsymbol{\alpha}^T \boldsymbol{\beta} = \gamma \boldsymbol{\beta}$ where γ is an element of $GF(q)$. The second step of the decryption can also be performed efficiently because \mathbf{eII} is of weight less than or equal to $\frac{n-k}{2}$, and $\frac{n-k}{2}$ errors can be corrected in polynomial time in a generalized Reed-Solomon code of length n and dimension k by well-known standard decoding algorithms.

4 Attack on the Baldi et al. Cryptosystem Using GRS Codes

4.1 Case where $2k + 2 < n$

We define \mathcal{C}_{sec} and \mathcal{C}_{pub} to be the codes generated by the matrices \mathbf{G}_{sec} and \mathbf{G}_{pub} respectively. We denote by n the length of these codes and by k their dimension. We assume in this subsection that

$$2k + 2 < n \quad (1)$$

As explained in Section 3, \mathcal{C}_{sec} is a GRS code. It is also assumed in [BBC⁺11] that the matrix $\mathbf{Q} = \mathbf{\Pi} + \mathbf{R}$ is invertible. It will be convenient to bring in the code $\mathcal{C} \stackrel{\text{def}}{=} \mathcal{C}_{sec} \mathbf{\Pi}^{-1}$. The matrix \mathbf{R} is assumed to be of rank one. From Lemma 3 in Appendix A, the matrix $\mathbf{R} \mathbf{\Pi}^{-1}$ is also of rank one. Hence there exist \mathbf{a} and \mathbf{b} in $GF(q)^n$ such that:

$$\mathbf{R} \mathbf{\Pi}^{-1} = \mathbf{b}^T \mathbf{a}. \quad (2)$$

This code \mathcal{C} , being a permutation of a generalized Reed-Solomon code, is itself a generalized Reed-Solomon code. So there are elements \mathbf{x} and \mathbf{y} in $GF(q)^n$ such that $\mathcal{C} = \mathbf{GRS}_k(\mathbf{x}, \mathbf{y})$. There is a simple relation between \mathcal{C}_{pub} and \mathcal{C} as explained by the following lemma.

Lemma 1. *Let $\boldsymbol{\lambda} \stackrel{\text{def}}{=} -\frac{1}{1+\mathbf{a} \cdot \mathbf{b}} \mathbf{b}$. For any \mathbf{c} in \mathcal{C}_{pub} there exists \mathbf{p} in \mathcal{C} such that:*

$$\mathbf{c} = \mathbf{p} + (\mathbf{p} \cdot \boldsymbol{\lambda}) \mathbf{a}. \quad (3)$$

The proof of this lemma is given in Appendix A. From now on we make the assumption that

$$\boldsymbol{\lambda} \notin \mathcal{C}^\perp. \quad (4)$$

If this is not the case then $\mathcal{C}_{pub} = \mathcal{C} = \mathbf{GRS}_k(\mathbf{x}, \mathbf{y})$ and there is straightforward attack by applying the Sidelnikov and Shestakov algorithm [SS92]. It finds $(\mathbf{x}', \mathbf{y}')$ that expresses \mathcal{C}_{pub} as $\mathbf{GRS}_k(\mathbf{x}', \mathbf{y}')$. This allows to easily decode \mathcal{C}_{pub} .

Our attack relies on identifying a code of dimension $k - 1$ that is both a subcode of \mathcal{C}_{pub} and the Generalized Reed-Solomon code \mathcal{C} . It consists more precisely of codewords $\mathbf{p} + (\mathbf{p} \cdot \boldsymbol{\lambda}) \mathbf{a}$ with \mathbf{p} in \mathcal{C} such that $\mathbf{p} \cdot \boldsymbol{\lambda} = 0$. This particular code which is denoted by $\mathcal{C}_{\boldsymbol{\lambda}^\perp}$ is hence:

$$\mathcal{C}_{\boldsymbol{\lambda}^\perp} \stackrel{\text{def}}{=} \mathcal{C} \cap \langle \boldsymbol{\lambda} \rangle^\perp$$

where $\langle \boldsymbol{\lambda} \rangle$ denotes the vector space spanned by $\boldsymbol{\lambda}$. It is a subspace of \mathcal{C}_{pub} of codimension 1 if $\boldsymbol{\lambda} \notin \mathcal{C}^\perp$. This strongly suggests that $\langle \mathcal{C}_{pub}^2 \rangle$ should have an unusual low dimension since $\langle \mathcal{C}^2 \rangle$ has dimension $2k - 1$ by Proposition 2. More exactly we have here:

Proposition 4.

1. $\langle \mathcal{C}_{pub}^2 \rangle \subset \langle \mathcal{C}^2 \rangle + \mathcal{C} \star \mathbf{a} + \langle \mathbf{a} \star \mathbf{a} \rangle$
2. $\dim(\langle \mathcal{C}_{pub}^2 \rangle) \leq 3k - 1$

The first fact follows immediately from Lemma 1 and the proof of this proposition is given in Appendix A. Experimentally it has been observed that the upper-bound is quite sharp. Indeed, the

dimension of $\langle \mathcal{C}_{\text{pub}}^2 \rangle$ has always been found³ to be equal to $3k - 1$ in all our experiments when choosing randomly the codes and \mathbf{Q} .

The second observation is that when a basis $\mathbf{g}_1, \dots, \mathbf{g}_k$ of \mathcal{C}_{pub} is chosen and l other random elements $\mathbf{z}_1, \dots, \mathbf{z}_l$, then we may expect that the dimension of the vector space generated by all products $\mathbf{z}_i \star \mathbf{g}_j$ with i in $\{1, \dots, l\}$ and j in $\{1, \dots, k\}$ is the dimension of the full space $\langle \mathcal{C}_{\text{pub}}^2 \rangle$ when $l \geq 3$. This is indeed the case when $l \geq 4$ but it is not true for $l = 3$ since we have the following result.

Proposition 5. *Let \mathcal{B} be the linear code spanned by $\{\mathbf{z}_i \star \mathbf{g}_j \mid 1 \leq i \leq 3 \text{ and } 1 \leq j \leq k\}$. It holds that $\dim(\mathcal{B}) \leq 3k - 3$.*

An explanation of this phenomenon is given in Appendix A. Experimentally, it turns out that almost always this upper-bound is quite tight and the dimension is generally $3k - 3$. But if we assume now that $\mathbf{z}_1, \mathbf{z}_2, \mathbf{z}_3$ all belong to $\mathcal{C}_{\lambda^\perp}$, which happens with probability $\frac{1}{q^3}$ since $\mathcal{C}_{\lambda^\perp}$ is a subspace of \mathcal{C}_{pub} of codimension 1 (at least when $\lambda \notin \mathcal{C}^\perp$), then the vectors $\mathbf{z}_i \star \mathbf{g}_j$ generate a subspace with a much smaller dimension.

Proposition 6. *If \mathbf{z}_i is in $\mathcal{C}_{\lambda^\perp}$ for i in $\{1, 2, 3\}$ then for all j in $\{1, \dots, k\}$:*

$$\mathbf{z}_i \star \mathbf{g}_j \subset \langle \mathcal{C}^2 \rangle + \langle \mathbf{z}_1 \star \mathbf{a} \rangle + \langle \mathbf{z}_2 \star \mathbf{a} \rangle + \langle \mathbf{z}_3 \star \mathbf{a} \rangle \quad (5)$$

and if \mathcal{B} is the linear code spanned by $\{\mathbf{z}_i \star \mathbf{g}_j \mid 1 \leq i \leq 3 \text{ and } 1 \leq j \leq k\}$ then

$$\dim(\mathcal{B}) \leq 2k + 2. \quad (6)$$

The proof of this proposition is straightforward and is given in Appendix A. The upper-bound given in (6) on the dimension follows immediately from (5). This leads to Algorithm 1 which computes a basis of $\mathcal{C}_{\lambda^\perp}$. It is essential that the condition in (1) holds in order to distinguish the case when the dimension is less than or equal to $2k + 2$ from higher dimensions.

The first phase of the attack, namely finding a suitable triple $\mathbf{z}_1, \mathbf{z}_2, \mathbf{z}_3$ runs in expected time of the form $O(k^3 q^3)$ because each test in the **repeat** loop 1 has a chance of $\frac{1}{q^3}$ to succeed. Indeed, $\mathcal{C}_{\lambda^\perp}$ is of codimension 1 in \mathcal{C}_{pub} and therefore a fraction $\frac{1}{q}$ of elements of \mathcal{C}_{pub} belongs to $\mathcal{C}_{\lambda^\perp}$. The whole algorithm runs in expected time of the form $O(k^3 q^3) + O(k^4 q) = O(k^3 q^3)$ since $k = O(q)$ and the first phase of the attack is dominant in the complexity. Once $\mathcal{C}_{\lambda^\perp}$ is recovered, it still remains to recover the secret code and \mathbf{a} . The problem at hand can be formulated like this: we know a very large subcode, namely $\mathcal{C}_{\lambda^\perp}$, of a GRS code that we want to recover. This is exactly the problem which was solved in [Wie10]. Applying the approach of this paper to our problem amounts to compute $\langle \mathcal{C}_{\lambda^\perp}^2 \rangle$ which turns out to be equal to $\mathbf{GRS}_{2k-1}(\mathbf{x}, \mathbf{y} \star \mathbf{y})$ (see [MCMMP11b] for more details). It suffices to use the Sidelnikov and Shestakov algorithm [SS92] to compute a pair $(\mathbf{x}, \mathbf{y} \star \mathbf{y})$ describing $\langle \mathcal{C}_{\lambda^\perp}^2 \rangle$ as a GRS code. From this, we deduce a pair (\mathbf{x}, \mathbf{y}) defining the secret code \mathcal{C} as a GRS code. The final phase, that is, recovering a possible (λ, \mathbf{a}) pair and using it to decode the public code \mathcal{C}_{pub} , is detailed in Appendix B.

³ There are however cases where the dimension might be even smaller. Let us take for instance $\mathbf{a} \in \mathbf{GRS}_l(\mathbf{x}, \mathbf{y})$ for some integer $l \geq 1$ where $\mathbf{GRS}_k(\mathbf{x}, \mathbf{y}) = \mathcal{C}$. From Proposition 2 we know that $\langle \mathcal{C}^2 \rangle = \mathbf{GRS}_{2k-1}(\mathbf{x}, \mathbf{y} \star \mathbf{y})$ and it can be checked similarly that $\mathcal{C} \star \mathbf{a} \subset \mathbf{GRS}_{k+l-1}(\mathbf{x}, \mathbf{y} \star \mathbf{y})$. It follows immediately from the first statement of Proposition 4 that the dimension of $\langle \mathcal{C}_{\text{pub}}^2 \rangle$ is upperbounded by $\max\{2k - 1, k + l - 1\} + 1$ which can be obviously smaller than $3k - 1$.

Algorithm 1 Recovering $\mathcal{C}_{\lambda^\perp}$.**Input:** A basis $\{g_1, \dots, g_k\}$ of \mathcal{C}_{pub} .**Output :** A basis \mathcal{L} of $\mathcal{C}_{\lambda^\perp}$.

```

1: repeat
2:   for  $1 \leq i \leq 3$  do
3:     Randomly choose  $z_i$  in  $\mathcal{C}_{\text{pub}}$ 
4:   end for
5:    $\mathcal{B} \leftarrow \langle \{z_i \star g_j \mid 1 \leq i \leq 3 \text{ and } 1 \leq j \leq k\} \rangle$ 
6: until  $\dim(\mathcal{B}) \leq 2k + 2$  and  $\dim(\langle z_1, z_2, z_3 \rangle) = 3$ 
7:  $\mathcal{L} \leftarrow \{z_1, z_2, z_3\}$ 
8:  $s \leftarrow 4$ 
9: while  $s \leq k - 1$  do
10:  repeat
11:    Randomly choose  $z_s$  in  $\mathcal{C}_{\text{pub}}$ 
12:     $\mathcal{T} \leftarrow \langle \{z_i \star g_j \mid i \in \{1, 2, s\} \text{ and } 1 \leq j \leq k\} \rangle$ 
13:  until  $\dim(\mathcal{T}) \leq 2k + 2$  and  $\dim(\langle \mathcal{L} \cup \{z_s\} \rangle) = s$ 
14:   $\mathcal{L} \leftarrow \mathcal{L} \cup \{z_s\}$ 
15:   $s \leftarrow s + 1$ 
16: end while
17: return  $\mathcal{L}$ ;

```

4.2 Using duality when the rate is larger than $\frac{1}{2}$

The codes suggested in [BBC⁺11, §5.1.1, §5.1.2] are all of rate significantly larger than $\frac{1}{2}$, for instance Example 1 p.15 suggests a GRS code of length 255, dimension 195 over $GF(256)$, whereas Example 2. p.15 suggests a GRS code of length 511, dimension 395 over $GF(512)$. The attack suggested in the previous subsection only applies to rates smaller than $\frac{1}{2}$. There is a simple way to adapt the previous attack for this case by considering the dual $\mathcal{C}_{\text{pub}}^\perp$ of the public code. Note that by Proposition 3, there exists \mathbf{y}' in $GF(q)^n$ for which we have $\mathcal{C}^\perp = \mathbf{GRS}_{n-k}(\mathbf{x}, \mathbf{y}')$. Moreover, $\mathcal{C}_{\text{pub}}^\perp$ displays a similar structure as \mathcal{C}_{pub} .

Lemma 2. *For any \mathbf{c} from $\mathcal{C}_{\text{pub}}^\perp$ there exists an element \mathbf{p} in \mathcal{C}^\perp such that:*

$$\mathbf{c} = \mathbf{p} + (\mathbf{p} \cdot \mathbf{a})\mathbf{b}. \quad (7)$$

The proof of this lemma is given in Appendix A. It implies that the whole approach of the previous subsection can be carried out over $\mathcal{C}_{\text{pub}}^\perp$. It allows to recover the secret code \mathcal{C}^\perp and therefore also \mathcal{C} . This attack needs that $2(n - k) + 2 < n$, that is $2k > n + 2$. In summary, there is an attack as soon as k is outside a narrow interval around $n/2$ which is $[\frac{n-2}{2}, \frac{n+2}{2}]$. We have implemented this attack on magma for the aforementioned set of parameters suggested in [BBC⁺11], namely $n = 255$, $q = 2^8$, $k = 195$ and the average running time over 25 attacks was about 2 weeks.

References

- BBC⁺11. M. Baldi, M. Bianchi, F. Chiaraluce, J. Rosenthal, and D. Schipani. Enhanced public key security for the McEliece cryptosystem. submitted, 2011. arxiv:1108.2462v2[cs.IT].
- BL05. T. P. Berger and P. Loidreau. How to mask the structure of codes for a cryptographic use. *Designs Codes and Cryptography*, 35(1):63–79, 2005.
- BL11. A. Bogdanov and C.H. Lee. Homomorphic encryption from codes. Accepted at STOC 2012, <http://arxiv.org/abs/1111.4301>, 2011.
- CCCX09. I. Cascudo, H. Chen, R. Cramer, and C. Xing. Asymptotically Good Ideal Linear Secret Sharing with Strong Multiplication over Any Fixed Finite Field. In S. Halevi, editor, *Advances in Cryptology - CRYPTO 2009*, volume 5677 of *Lecture Notes in Computer Science*, pages 466–486. Springer Berlin / Heidelberg, 2009.
- CCX11. I. Cascudo, R. Cramer, and C. Xing. The Torsion-Limit for Algebraic Function Fields and Its Application to Arithmetic Secret Sharing. In P. Rogaway, editor, *Advances in Cryptology CRYPTO 2011*, volume 6841 of *Lecture Notes in Computer Science*, pages 685–705. Springer Berlin / Heidelberg, 2011.
- CFS01. N. T. Courtois, M. Finiasz, and N. Sendrier. How to achieve a McEliece-based digital signature scheme. *Lecture Notes in Computer Science*, 2248:157–174, 2001.
- Dal07. L. Dallot. Towards a concrete security proof of Courtois, Finiasz and Sendrier signature scheme. In *WEWoRC*, pages 65–77, 2007.
- DMQN09. R. Dowsley, J. Müller-Quade, and A. C. A. Nascimento. A CCA2 secure public key encryption scheme based on the McEliece assumptions in the standard model. In *CT-RSA*, pages 240–251, 2009.
- FGO⁺11. J.-C. Faugère, V. Gauthier, A. Otmani, L. Perret, and J.-P. Tillich. A distinguisher for high rate McEliece cryptosystems. In *Proceedings of the Information Theory Workshop 2011, ITW 2011*, pages 282–286, Paraty, Brasil, 2011.
- Gib91. J. Gibson. Equivalent goppa codes and trapdoors to McEliece's public key cryptosystem. In Donald Davies, editor, *Advances in Cryptology - EUROCRYPT 91*, volume 547 of *Lecture Notes in Computer Science*, pages 517–521. Springer Berlin / Heidelberg, 1991.
- GOT12. Valérie Gauthier, Ayoub Otmani, and Jean-Pierre Tillich. A distinguisher-based attack of a homomorphic encryption scheme relying on reed-solomon codes. Cryptology ePrint Archive, Report 2012/168, 2012. <http://eprint.iacr.org/>.
- Köt92. R. Kötter. A unified description of an error locating procedure for linear codes. In *Proc. Algebraic and Combinatorial Coding Theory*, pages 113–117, Voneshta Voda, 1992.
- LS01. P. Loidreau and N. Sendrier. Weak keys in the McEliece public-key cryptosystem. *IEEE Transactions on Information Theory*, 47(3):1207–1211, 2001.
- McE78. R. J. McEliece. *A Public-Key System Based on Algebraic Coding Theory*, pages 114–116. Jet Propulsion Lab, 1978. DSN Progress Report 44.
- MCMMP11a. I. Márquez-Corbella, E. Martínez-Moro, and R. Pellikaan. Evaluation of public-key cryptosystems based on algebraic geometry codes. In J. Borges and M. Villanueva, editors, *Proceedings of the Third International Castle Meeting on Coding Theory and Applications*, pages 199–204, Barcelona, Spain, September 11-15 2011.
- MCMMP11b. I. Márquez-Corbella, E. Martínez-Moro, and R. Pellikaan. The non-gap sequence of a subcode of a generalized Reed-Solomon code. In M. Finiasz N. Sendrier, P. Charpin and A. Otmani, editors, *Proceedings of the 7-th International Workshop on Coding and Cryptography WCC 2011*, pages 183–193, April 2011.
- MCP12. I. Márquez-Corbella and R. Pellikaan. Error-correcting pairs for a public-key cryptosystem. preprint, 2012. preprint.
- MS86. F. J. MacWilliams and N. J. A. Sloane. *The Theory of Error-Correcting Codes*. North-Holland, Amsterdam, fifth edition, 1986.
- Nie86. H. Niederreiter. Knapsack-type cryptosystems and algebraic coding theory. *Problems Control Inform. Theory*, 15(2):159–166, 1986.
- NIKM08. R. Nojima, H. Imai, K. Kobara, and K. Morozov. Semantic security for the McEliece cryptosystem without random oracles. *Des. Codes Cryptography*, 49(1-3):289–305, 2008.
- Pel92. R. Pellikaan. On decoding by error location and dependent sets of error positions. *Discrete Mathematics*, 106-107:368–381, 1992.
- SS92. V.M. Sidelnikov and S.O. Shestakov. On the insecurity of cryptosystems based on generalized Reed-Solomon codes. *Discrete Mathematics and Applications*, 1(4):439–444, 1992.
- Wie10. C. Wieschebrink. Cryptanalysis of the Niederreiter Public Key Scheme Based on GRS Subcodes. In N. Sendrier, editor, *Post-Quantum Cryptography, Third International Workshop, PQCrypto 2010*, volume 6061 of *Lecture Notes in Computer Science*, pages 61–72, Darmstadt, Germany, May 2010. Springer.

A Proofs of Section 4

The first result that will be used throughout this section is a lemma expressing $\mathbf{R}\mathbf{\Pi}^{-1}$ in terms of two vectors in $GF(q)^n$:

Lemma 3. *Assume that \mathbf{R} is of rank 1, then $\mathbf{R}\mathbf{\Pi}^{-1}$ is of rank 1 and there exist \mathbf{a} and \mathbf{b} in $GF(q)^n$ such that*

$$\mathbf{R}\mathbf{\Pi}^{-1} = \mathbf{b}^T \mathbf{a}.$$

Proof. The dimension of the column space of \mathbf{R} is the same as the dimension of the column space of $\mathbf{R}\mathbf{\Pi}^{-1}$. Since \mathbf{R} is of rank 1, this column space has dimension 1 which implies that $\mathbf{R}\mathbf{\Pi}^{-1}$ is also of rank 1. From the fact that the column space of $\mathbf{R}\mathbf{\Pi}$ is of dimension 1, this implies that we can find b_1, \dots, b_n and a_1, \dots, a_n in $GF(q)$ such that

$$\mathbf{R}\mathbf{\Pi}^{-1} = (b_i a_j)_{\substack{1 \leq i \leq n \\ 1 \leq j \leq n}}.$$

We let $\mathbf{a} \stackrel{\text{def}}{=} (a_j)_{1 \leq j \leq n}$ and $\mathbf{b} \stackrel{\text{def}}{=} (b_i)_{1 \leq i \leq n}$. □

From now on we define

$$\mathbf{P} \stackrel{\text{def}}{=} \mathbf{I} + \mathbf{R}\mathbf{\Pi}^{-1} = \mathbf{I} + \mathbf{b}^T \mathbf{a}.$$

We will also need the following lemma

Lemma 4. *If \mathbf{Q} is invertible, then so is \mathbf{P} and*

$$\mathbf{P}^{-1} = \mathbf{I} - \frac{1}{1 + \mathbf{a} \cdot \mathbf{b}} \mathbf{b}^T \mathbf{a}.$$

Proof. We first observe that $\mathbf{Q} = \mathbf{\Pi} + \mathbf{R} = (\mathbf{I} + \mathbf{R}\mathbf{\Pi}^{-1})\mathbf{\Pi} = \mathbf{P}\mathbf{\Pi}$. Therefore \mathbf{P} is invertible if and only if \mathbf{Q} is invertible. Moreover

$$\begin{aligned} \mathbf{P} \left(\mathbf{I} - \frac{1}{1 + \mathbf{a} \cdot \mathbf{b}} \mathbf{b}^T \mathbf{a} \right) &= (\mathbf{I} + \mathbf{b}^T \mathbf{a}) \left(\mathbf{I} - \frac{1}{1 + \mathbf{a} \cdot \mathbf{b}} \mathbf{b}^T \mathbf{a} \right) \\ &= \mathbf{I} + \left(1 - \frac{1}{1 + \mathbf{a} \cdot \mathbf{b}} \right) \mathbf{b}^T \mathbf{a} - \frac{1}{1 + \mathbf{a} \cdot \mathbf{b}} \mathbf{b}^T \mathbf{a} \mathbf{b}^T \mathbf{a} \\ &= \mathbf{I} + \frac{\mathbf{a} \cdot \mathbf{b}}{1 + \mathbf{a} \cdot \mathbf{b}} \mathbf{b}^T \mathbf{a} - \frac{\mathbf{a} \cdot \mathbf{b}}{1 + \mathbf{a} \cdot \mathbf{b}} \mathbf{b}^T \mathbf{a} \\ &= \mathbf{I}. \end{aligned}$$

□

A.1 Proof of Lemma 1

Let

$$\begin{aligned} \boldsymbol{\lambda} &\stackrel{\text{def}}{=} -\mathbf{P}^{-1} \mathbf{b}^T = - \left(\mathbf{I} - \frac{1}{1 + \mathbf{a} \cdot \mathbf{b}} \mathbf{b}^T \mathbf{a} \right) \mathbf{b}^T \\ &= -\mathbf{b}^T + \frac{\mathbf{a} \cdot \mathbf{b}}{1 + \mathbf{a} \cdot \mathbf{b}} \mathbf{b}^T \\ &= -\frac{1}{1 + \mathbf{a} \cdot \mathbf{b}} \mathbf{b}^T. \end{aligned} \tag{8}$$

Let \mathbf{c} be an element of \mathcal{C}_{pub} . Since $\mathcal{C}_{\text{sec}} = \mathcal{C}_{\text{pub}}\mathbf{Q} = \mathcal{C}_{\text{pub}}(\mathbf{\Pi} + \mathbf{R}) = \mathcal{C}_{\text{pub}}(\mathbf{I} + \mathbf{R}\mathbf{\Pi}^{-1})\mathbf{\Pi} = \mathcal{C}_{\text{pub}}\mathbf{P}\mathbf{\Pi}$ we obtain $\mathcal{C}_{\text{sec}}\mathbf{\Pi}^{-1} = \mathcal{C}_{\text{pub}}\mathbf{P}$ and therefore

$$\mathcal{C}_{\text{pub}} = (\mathcal{C}_{\text{sec}}\mathbf{\Pi}^{-1})\mathbf{P}^{-1} = \mathcal{C}\mathbf{P}^{-1}.$$

From this obtain that there exists \mathbf{p} in \mathcal{C} such that

$$\begin{aligned} \mathbf{c} &= \mathbf{p}\mathbf{P}^{-1} \\ &= \mathbf{p} \left(\mathbf{I} - \frac{1}{1 + \mathbf{a} \cdot \mathbf{b}} \mathbf{b}^T \mathbf{a} \right) \\ &= \mathbf{p} - \frac{\mathbf{b} \cdot \mathbf{p}}{1 + \mathbf{a} \cdot \mathbf{b}} \mathbf{a} \\ &= \mathbf{p} + (\boldsymbol{\lambda} \cdot \mathbf{p}) \mathbf{a}. \end{aligned}$$

A.2 Proof of Proposition 4

Let \mathbf{c} and \mathbf{c}' be two elements in \mathcal{C}_{pub} . By applying Lemma 1 to them we know that there exist two elements \mathbf{p} and \mathbf{p}' in \mathcal{C} such that

$$\begin{aligned} \mathbf{c} &= \mathbf{p} + (\boldsymbol{\lambda} \cdot \mathbf{p}) \mathbf{a} \\ \mathbf{c}' &= \mathbf{p}' + (\boldsymbol{\lambda} \cdot \mathbf{p}') \mathbf{a}. \end{aligned}$$

This implies that

$$\begin{aligned} \mathbf{c} \star \mathbf{c}' &= (\mathbf{p} + (\boldsymbol{\lambda} \cdot \mathbf{p}) \mathbf{a}) \star (\mathbf{p}' + (\boldsymbol{\lambda} \cdot \mathbf{p}') \mathbf{a}) \\ &= \mathbf{p} \star \mathbf{p}' + ((\boldsymbol{\lambda} \cdot \mathbf{p}) \mathbf{p}' + (\boldsymbol{\lambda} \cdot \mathbf{p}') \mathbf{p}) \star \mathbf{a} + (\boldsymbol{\lambda} \cdot \mathbf{p})(\boldsymbol{\lambda} \cdot \mathbf{p}') \mathbf{a} \star \mathbf{a} \end{aligned} \tag{9}$$

It will be convenient to bring the notation

$$\mathbf{x}^i = \underbrace{\mathbf{x} \star \mathbf{x} \star \dots \star \mathbf{x}}_{i \text{ times}}.$$

In other words with this notation, $\mathcal{C} = \mathbf{GRS}_k(\mathbf{x}, \mathbf{y})$ is generated by the $\mathbf{y} \star \mathbf{x}^i$'s for i in $\{0, 1, \dots, k-1\}$. Since $\boldsymbol{\lambda} \notin \mathcal{C}^\perp$, there exists $i_0 \in \{0, \dots, k-1\}$ such that $\boldsymbol{\lambda} \cdot (\mathbf{y} \star \mathbf{x}^{i_0}) \neq 0$. For i in $\{0, 1, \dots, k-1\}$, let

$$\begin{aligned} \mathbf{u}_i &\stackrel{\text{def}}{=} \boldsymbol{\lambda} \cdot (\mathbf{y} \star \mathbf{x}^{i_0}) \mathbf{y} \star \mathbf{x}^i + \boldsymbol{\lambda} \cdot (\mathbf{y} \star \mathbf{x}^i) \mathbf{y} \star \mathbf{x}^{i_0} + \boldsymbol{\lambda} \cdot (\mathbf{y} \star \mathbf{x}^{i_0}) \boldsymbol{\lambda} \cdot (\mathbf{y} \star \mathbf{x}^i) \mathbf{a} \\ \mathbf{v}_{ij} &\stackrel{\text{def}}{=} \boldsymbol{\lambda} \cdot (\mathbf{y} \star \mathbf{x}^j) \mathbf{y} \star \mathbf{x}^i + \boldsymbol{\lambda} \cdot (\mathbf{y} \star \mathbf{x}^i) \mathbf{y} \star \mathbf{x}^j + \boldsymbol{\lambda} \cdot (\mathbf{y} \star \mathbf{x}^i) \boldsymbol{\lambda} \cdot (\mathbf{y} \star \mathbf{x}^j) \mathbf{a} \end{aligned}$$

We claim that

Lemma 5. *Let V be the vector space generated by the \mathbf{v}_{ij} 's for i, j in $\{0, 1, \dots, k-1\}$. The dimension of V is less than or equal to k .*

Proof. We prove that V is generated by the u_i 's for i in $\{0, 1, \dots, k-1\}$. This can be proved by noticing that

$$\begin{aligned}
& \frac{\lambda \cdot y \star x^j}{\lambda \cdot y \star x^{i_0}} u_i + \frac{\lambda \cdot y \star x^i}{\lambda \cdot y \star x^{i_0}} u_j - \frac{(\lambda \cdot y \star x^i)(\lambda \cdot y \star x^j)}{(\lambda \cdot y \star x^{i_0})(\lambda \cdot y \star x^{i_0})} u_{i_0} \\
&= (\lambda \cdot y \star x^j) y \star x^i + \frac{(\lambda \cdot y \star x^i)(\lambda \cdot y \star x^j)}{\lambda \cdot y \star x^{i_0}} y \star x^{i_0} + (\lambda \cdot y \star x^i)(\lambda \cdot y \star x^j) a \\
&\quad + \\
&\quad (\lambda \cdot y \star x^i) y \star x^j + \frac{(\lambda \cdot y \star x^i)(\lambda \cdot y \star x^j)}{\lambda \cdot y \star x^{i_0}} y \star x^{i_0} + (\lambda \cdot y \star x^i)(\lambda \cdot y \star x^j) a \\
&\quad - \\
&\quad \left(2 \frac{(\lambda \cdot y \star x^i)(\lambda \cdot y \star x^j)}{\lambda \cdot y \star x^{i_0}} y \star x^{i_0} + (\lambda \cdot y \star x^i)(\lambda \cdot y \star x^j) a \right) \\
&= (\lambda \cdot y \star x^j) y \star x^i + (\lambda \cdot y \star x^i) y \star x^j + (\lambda \cdot y \star x^i)(\lambda \cdot y \star x^j) a \\
&= v_{ij}
\end{aligned}$$

□

To simplify notation we assume here that \star takes precedence over the dot product, that is $\lambda \cdot y \star x^j = \lambda \cdot (y \star x^j)$. Observe now that Equation (9) implies that $c \star c'$ belongs to $\langle \mathcal{C}^2 \rangle + V \star a$. The space generated by the $c \star c'$'s has therefore a dimension which is upper-bounded by $2k-1+k=3k-1$.

A.3 Proof of Proposition 5

This follows immediately from the fact that we can express z_i in terms of the g_j 's, say

$$z_i = \sum_{1 \leq j \leq k} a_{ij} g_j.$$

We observe now that we have the following three relations between the $z_i \star g_j$'s:

$$\sum_{1 \leq j \leq n} a_{2j} z_1 \star g_j - \sum_{1 \leq j \leq n} a_{1j} z_2 \star g_j = 0 \quad (10)$$

$$\sum_{1 \leq j \leq n} a_{3j} z_1 \star g_j - \sum_{1 \leq j \leq n} a_{1j} z_3 \star g_j = 0 \quad (11)$$

$$\sum_{1 \leq j \leq n} a_{2j} z_3 \star g_j - \sum_{1 \leq j \leq n} a_{3j} z_2 \star g_j = 0 \quad (12)$$

(10) can be verified as follows

$$\sum_{1 \leq j \leq n} a_{2j} z_1 \star g_j - \sum_{1 \leq j \leq n} a_{1j} z_2 \star g_j = z_1 \star z_2 - z_1 \star z_2 = 0.$$

The two remaining identities can be proved in a similar fashion.

A.4 Proof of Proposition 6

Assume that the z_i 's all belong to $\mathcal{C}_{\lambda^\perp}$. For every g_j there exists p_j in \mathcal{C} such that $g_j = p_j + \lambda \cdot p_j a$. We obtain now

$$\begin{aligned}
z_i \star g_j &= z_i \star (p_j + (\lambda \cdot p_j) a) \\
&= z_i \star p_j + (\lambda \cdot p_j) z_i \star a \\
&\in \langle \mathcal{C}^2 \rangle + \langle z_1 \star a \rangle + \langle z_2 \star a \rangle + \langle z_3 \star a \rangle
\end{aligned} \quad (13)$$

This proves the first part of the proposition, the second part follows immediately from the first part since it implies that the dimension of the vector space generated by the $\mathbf{z}_i \star \mathbf{g}_j$'s is upperbounded by the sum of the dimension of $\langle \mathcal{C}^2 \rangle$ (that is $2k - 1$) and the dimension of the vector space spanned by the $\mathbf{z}_i \star \mathbf{a}$'s (which is at most 3).

A.5 Proof of Lemma 2

The key to Lemma 2 is the fact that the dual of \mathcal{C}_{pub} is equal to $\mathcal{C}^\perp \mathbf{P}^T$. Indeed $\mathcal{C}_{\text{pub}} = \mathcal{C} \mathbf{P}^{-1}$ and therefore for any element \mathbf{c} of \mathcal{C}_{pub} there exists an element \mathbf{p} of \mathcal{C} such that $\mathbf{c} = \mathbf{p} \mathbf{P}^{-1}$. Observe now that every element \mathbf{c}^\perp in $\mathcal{C}_{\text{pub}}^\perp$ satisfies $\mathbf{c} \cdot \mathbf{c}^\perp = 0$ and that

$$0 = \mathbf{c} \cdot \mathbf{c}^\perp = \mathbf{p} \mathbf{P}^{-1} \cdot \mathbf{c}^\perp = \mathbf{p} \cdot \mathbf{c}^\perp (\mathbf{P}^{-1})^T.$$

Therefore $\mathcal{C}_{\text{pub}}^\perp = \mathcal{C}^\perp \mathbf{P}^T$. This discussion implies that there exists an element \mathbf{p}^\perp in \mathcal{C}^\perp such that

$$\begin{aligned} \mathbf{c}^\perp &= \mathbf{p}^\perp \mathbf{P}^T \\ &= \mathbf{p}^\perp (\mathbf{I} + \mathbf{b}^T \mathbf{a})^T \\ &= \mathbf{p}^\perp + \mathbf{p}^\perp \mathbf{a}^T \mathbf{b} \\ &= \mathbf{p}^\perp + (\mathbf{p}^\perp \cdot \mathbf{a}) \mathbf{b}. \end{aligned}$$

B Recovering \mathbf{a} and $\boldsymbol{\lambda}$ from \mathcal{C} and $\mathcal{C}_{\boldsymbol{\lambda}^\perp}$

B.1 The structure of $\mathcal{C}_{\text{pub}} \cap \mathcal{C}$ and $\mathcal{C}_{\text{pub}}^\perp \cap \mathcal{C}^\perp$

The attack which was given in Section 4 enables to find \mathcal{C} and $\mathcal{C}_{\boldsymbol{\lambda}^\perp}$ which is equal to the intersection $\mathcal{C}_{\text{pub}} \cap \mathcal{C}$. From this we deduce \mathcal{C}^\perp and $\mathcal{C}^\perp \cap \mathcal{C}_{\text{pub}}^\perp$. These intersections are related to $\boldsymbol{\lambda}$ and \mathbf{a} by

Lemma 6.

$$\mathcal{C}_{\text{pub}} \cap \mathcal{C} = \{\mathbf{p} \in \mathcal{C} \mid \mathbf{p} \cdot \boldsymbol{\lambda} = 0\} \quad (14)$$

$$\mathcal{C}_{\text{pub}}^\perp \cap \mathcal{C}^\perp = \{\mathbf{p} \in \mathcal{C}^\perp \mid \mathbf{p} \cdot \mathbf{a} = 0\} \quad (15)$$

Proof. Since it is assumed that $\boldsymbol{\lambda} \notin \mathcal{C}^\perp$, we deduce that $\mathcal{C}_1 \stackrel{\text{def}}{=} \{\mathbf{p} \in \mathcal{C} \mid \mathbf{p} \cdot \boldsymbol{\lambda} = 0\}$ is a subcode of \mathcal{C} of dimension $k - 1$. Let \mathbf{p} be an element of \mathcal{C}_1 . Notice now that $\mathbf{c} \stackrel{\text{def}}{=} \mathbf{p} + (\boldsymbol{\lambda} \cdot \mathbf{p})\mathbf{a}$ belongs to \mathcal{C}_{pub} from Lemma 1 and that $\mathbf{c} = \mathbf{p}$ since $\boldsymbol{\lambda} \cdot \mathbf{p} = 0$ by definition of \mathcal{C}_1 . Therefore $\mathcal{C}_1 \subset \mathcal{C}_{\text{pub}} \cap \mathcal{C}$. Since $\mathcal{C}_{\text{pub}} \neq \mathcal{C}$ by assumption, we obtain that $\dim(\mathcal{C}_{\text{pub}} \cap \mathcal{C}) < k$. This implies that $\mathcal{C}_1 = \mathcal{C}_{\text{pub}} \cap \mathcal{C}$ because the dimension of \mathcal{C}_1 is $k - 1$ as explained above. This proves Equation (14).

To prove Equation (15), let us first compute the dimension of $\mathcal{C}_{\text{pub}}^\perp \cap \mathcal{C}^\perp$:

$$\dim(\mathcal{C}_{\text{pub}}^\perp \cap \mathcal{C}^\perp) = \dim(\mathcal{C}_{\text{pub}}^\perp) + \dim(\mathcal{C}^\perp) - \dim(\mathcal{C}_{\text{pub}}^\perp + \mathcal{C}^\perp) \quad (16)$$

$$= (n - k) + (n - k) - \dim((\mathcal{C}_{\text{pub}} \cap \mathcal{C})^\perp) \quad (17)$$

$$= (n - k) + (n - k) - (n - (k - 1)) \quad (18)$$

$$= n - k - 1. \quad (19)$$

Let $\mathcal{C}_2 \stackrel{\text{def}}{=} \{\mathbf{p} \in \mathcal{C}^\perp \mid \mathbf{p} \cdot \mathbf{a} = 0\}$. We first claim that $\dim \mathcal{C}_2 = n - k - 1$.

If this were not the case we would have $\dim \mathcal{C}_2 = n - k$ which would imply that $\mathcal{C}_2 = \mathcal{C}^\perp$ and $\mathbf{a} \in \mathcal{C}$. Consider now an element \mathbf{c} of $\mathcal{C}_{\text{pub}}^\perp$. By Lemma 2 we know that there exists \mathbf{p} in \mathcal{C}^\perp such that $\mathbf{c} = \mathbf{p} + (\mathbf{a} \cdot \mathbf{p})\mathbf{b}$. Since $(\mathbf{a}, \mathbf{p}) = 0$, this would imply that $\mathbf{c} = \mathbf{p}$ and that \mathbf{c} would also be in \mathcal{C}^\perp . This would prove that $\mathcal{C}^\perp = \mathcal{C}_{\text{pub}}^\perp$ which would itself imply that $\mathcal{C} = \mathcal{C}_{\text{pub}}$. This is a contradiction.

We finish the proof similarly to the previous case by invoking Lemma 2 for an element \mathbf{p} in \mathcal{C}_2 and arguing that:

(i) $\mathbf{c} = \mathbf{p} + (\mathbf{a} \cdot \mathbf{p})\mathbf{b}$ is in $\mathcal{C}_{\text{pub}}^\perp$ by Lemma 2,

(ii) $\mathbf{c} = \mathbf{p}$ because $\mathbf{a} \cdot \mathbf{p} = 0$ and therefore $\mathcal{C}_2 \subset \mathcal{C}_{\text{pub}}^\perp \cap \mathcal{C}^\perp$. The equality of both subspaces is proved by a dimension argument (both have dimension $n - k - 1$). \square

B.2 Recovering a valid $(\mathbf{a}, \boldsymbol{\lambda})$ pair

Choose now an arbitrary element \mathbf{r}_1 in $\mathcal{C}_{\text{pub}}^\perp \setminus \mathcal{C}^\perp$ and choose any element \mathbf{b}_0 in $(\mathcal{C}_{\text{pub}} \cap \mathcal{C})^\perp \setminus \mathcal{C}^\perp$ and any element \mathbf{a}_0 in $(\mathcal{C}_{\text{pub}}^\perp \cap \mathcal{C}^\perp)^\perp \setminus \mathcal{C}$ such that

$$\mathbf{a}_0 \cdot \mathbf{r}_1 \neq 0 \quad (20)$$

$$\mathbf{a}_0 \cdot \mathbf{b}_0 = 0 \quad (21)$$

This is obviously possible by arguing on the dimensions of $(\mathcal{C}_{\text{pub}} \cap \mathcal{C})^\perp$ and $(\mathcal{C}_{\text{pub}}^\perp \cap \mathcal{C}^\perp)^\perp$. We are going to show that up to a multiplicative constant these two elements can be chosen as a valid $(\mathbf{a}, \boldsymbol{\lambda})$ pair, where we use the following definition

Definition 3 (valid $(\mathbf{a}, \boldsymbol{\lambda})$ pair for $(\mathcal{C}_{\text{pub}}, \mathcal{C})$). We say that a couple $(\mathbf{a}_0, \boldsymbol{\lambda}_0)$ of elements of $GF(q)^n \times GF(q)^n$ forms a valid $(\mathbf{a}, \boldsymbol{\lambda})$ pair for $(\mathcal{C}_{\text{pub}}, \mathcal{C})$ if and only if

(i) $\mathbf{a}_0 \cdot \boldsymbol{\lambda}_0 \neq -1$,

(ii) for any element \mathbf{c} in \mathcal{C}_{pub} there exists an element \mathbf{p} in \mathcal{C} such that $\mathbf{c} = \mathbf{p} + (\boldsymbol{\lambda}_0 \cdot \mathbf{p})\mathbf{a}_0$.

We will see in Subsection B.3 that we can easily decode the public code \mathcal{C}_{pub} with the help of such a valid $(\mathbf{a}, \boldsymbol{\lambda})$ pair.

We first observe that

Lemma 7. There exist α_0 and β_0 in $GF(q) \setminus \{0\}$, \mathbf{p}_0 in \mathcal{C} , \mathbf{q}_0 in \mathcal{C}^\perp such that

$$\mathbf{a}_0 = \mathbf{p}_0 + \alpha_0 \mathbf{a} \quad (22)$$

$$\mathbf{b}_0 = \mathbf{q}_0 + \beta_0 \mathbf{b}. \quad (23)$$

Proof. $(\mathcal{C}_{\text{pub}} \cap \mathcal{C})^\perp$ is a subspace of dimension $n - k + 1$ which contains \mathcal{C}^\perp and $\boldsymbol{\lambda}$, and therefore also \mathbf{b} . \mathbf{b} does not belong to \mathcal{C}^\perp since $\boldsymbol{\lambda}$ is assumed to be outside \mathcal{C}^\perp . This implies that

$$(\mathcal{C}_{\text{pub}} \cap \mathcal{C})^\perp = \mathcal{C}^\perp + \langle \mathbf{b} \rangle \quad (24)$$

Since \mathbf{b}_0 does not belong to \mathcal{C}^\perp by definition, there necessarily exist β_0 in $GF(q) \setminus \{0\}$ and \mathbf{q}_0 in \mathcal{C}^\perp such that

$$\mathbf{b}_0 = \mathbf{q}_0 + \beta_0 \mathbf{b}.$$

The statement on \mathbf{a}_0 is proved similarly. □

Choose now an arbitrary element \mathbf{p}_1 in $\mathcal{C} \setminus \mathcal{C}_{\text{pub}}$. Let

$$\gamma \stackrel{\text{def}}{=} \frac{-(\mathbf{p}_1 \cdot \mathbf{r}_1)}{(\mathbf{b}_0 \cdot \mathbf{p}_1)(\mathbf{a}_0 \cdot \mathbf{r}_1)} \quad (25)$$

This definition make sense because $\mathbf{a}_0 \cdot \mathbf{r}_1 \neq 0$ by choice of \mathbf{a}_0 and $\mathbf{b}_0 \cdot \mathbf{p}_1 \neq 0$ because $\mathbf{p}_1 \in \mathcal{C} \setminus \mathcal{C}_{\text{pub}}$ and by the characterization of the intersection $\mathcal{C} \cap \mathcal{C}_{\text{pub}}$ of Lemma 6.

Proposition 7. $(\mathbf{a}_0, \gamma \mathbf{b}_0)$ is a valid $(\mathbf{a}, \boldsymbol{\lambda})$ pair for $(\mathcal{C}_{\text{pub}}, \mathcal{C})$.

Proof. The first property of an $(\mathbf{a}, \boldsymbol{\lambda})$ pair is clearly met:

$$\mathbf{a}_0 \cdot \gamma \mathbf{b}_0 = 0 \neq -1$$

by using (21).

Let us now prove that for every \mathbf{p} in \mathcal{C} , we have

$$\mathbf{p} + \gamma \mathbf{b}_0 \cdot \mathbf{p} \mathbf{a}_0 \in \mathcal{C}_{\text{pub}}.$$

First consider a \mathbf{p} which belongs to $\mathcal{C} \cap \mathcal{C}_{\text{pub}}$. We have

$$\begin{aligned} \gamma \mathbf{b}_0 \cdot \mathbf{p} &= \gamma \beta_0 \mathbf{b} \cdot \mathbf{p} + \mathbf{q}_0 \cdot \mathbf{p} \\ &= \gamma (\beta_0 \mathbf{b} \cdot \mathbf{p} + \mathbf{q}_0 \cdot \mathbf{p}) \\ &= 0 \end{aligned}$$

because $\beta_0 \mathbf{b} \cdot \mathbf{p} = 0$ from the characterization of $\mathcal{C} \cap \mathcal{C}_{\text{pub}}$ given in Lemma 6 and $\mathbf{q}_0 \cdot \mathbf{p} = 0$ because \mathbf{q}_0 belongs to \mathcal{C}^\perp and \mathbf{p} belongs to \mathcal{C} . This implies

$$\mathbf{p} + (\gamma \mathbf{b}_0 \cdot \mathbf{p}) \mathbf{a}_0 = \mathbf{p}$$

which belongs to \mathcal{C}_{pub} by definition of \mathbf{p} .

Let us prove now that $\mathbf{c}_1 \stackrel{\text{def}}{=} \mathbf{p}_1 + (\gamma \mathbf{b}_0 \cdot \mathbf{p}_1) \mathbf{a}_0$ also belongs to \mathcal{C}_{pub} . For this purpose we are going to prove that \mathbf{c}_1 is orthogonal to all elements of $\mathcal{C}_{\text{pub}}^\perp$. We achieve this by first proving that \mathbf{c}_1 is orthogonal to any element \mathbf{q}_2 in the intersection $\mathcal{C}_{\text{pub}}^\perp \cap \mathcal{C}^\perp$:

$$\begin{aligned} \mathbf{c}_1 \cdot \mathbf{q}_2 &= (\mathbf{p}_1 + (\gamma \mathbf{b}_0 \cdot \mathbf{p}_1) \mathbf{a}_0) \cdot \mathbf{q}_2 \\ &= \mathbf{p}_1 \cdot \mathbf{q}_2 + \gamma (\mathbf{b}_0 \cdot \mathbf{p}_1) \mathbf{a}_0 \cdot \mathbf{q}_2 \\ &= 0 \end{aligned}$$

because $\mathbf{p}_1 \cdot \mathbf{q}_2 = 0$ from the fact that $\mathbf{p}_1 \in \mathcal{C}$ and $\mathbf{q}_2 \in \mathcal{C}^\perp$ and $\mathbf{a}_0 \cdot \mathbf{q}_2 = 0$ by using the characterization of $\mathcal{C}_{\text{pub}}^\perp \cap \mathcal{C}^\perp$ given in Lemma 6. We finish the proof by proving that \mathbf{c}_1 is also orthogonal to \mathbf{r}_1 :

$$\begin{aligned} \mathbf{c}_1 \cdot \mathbf{r}_1 &= (\mathbf{p}_1 + (\gamma \mathbf{b}_0 \cdot \mathbf{p}_1) \mathbf{a}_0) \cdot \mathbf{r}_1 \\ &= \mathbf{p}_1 \cdot \mathbf{r}_1 + \gamma (\mathbf{b}_0 \cdot \mathbf{p}_1) \mathbf{a}_0 \cdot \mathbf{r}_1 \\ &= \mathbf{p}_1 \cdot \mathbf{r}_1 - \frac{\mathbf{p}_1 \cdot \mathbf{r}_1}{(\mathbf{b}_0 \cdot \mathbf{p}_1)(\mathbf{a}_0 \cdot \mathbf{r}_1)} (\mathbf{b}_0 \cdot \mathbf{p}_1)(\mathbf{a}_0 \cdot \mathbf{r}_1) \\ &= 0. \end{aligned}$$

This implies that \mathbf{c}_1 belongs to \mathcal{C}_{pub} . Notice now that the mapping $\phi : \mathbf{u} \rightarrow \mathbf{u} + (\gamma \mathbf{b}_0 \cdot \mathbf{u}) \mathbf{a}_0$ is a one-to-one linear mapping whose inverse is given by $\mathbf{v} \rightarrow \mathbf{v} + (\boldsymbol{\delta} \cdot \mathbf{v}) \mathbf{a}_0$ where $\boldsymbol{\delta} = -\frac{1}{1+\gamma \mathbf{b}_0 \cdot \mathbf{a}_0} \gamma \mathbf{b}_0 = -\gamma \mathbf{b}_0$ since $\gamma \mathbf{b}_0 \cdot \mathbf{a}_0 = 0$ by using (21). We have therefore proved that a basis of \mathcal{C} is transformed into a basis of \mathcal{C}_{pub} by the mapping ϕ . By linearity of the mapping, we deduce that for any element \mathbf{c} in \mathcal{C}_{pub} there exists an element \mathbf{p} in \mathcal{C} such that $\mathbf{c} = \mathbf{p} + (\gamma \mathbf{b}_0 \cdot \mathbf{p}) \mathbf{a}_0$. \square

B.3 Decoding the public code

Assume that we have a valid $(\mathbf{a}, \boldsymbol{\lambda})$ pair for $(\mathcal{C}_{\text{pub}}, \mathcal{C})$, say it is $(\mathbf{a}_0, \boldsymbol{\lambda}_0)$. We want to decode the vector $\mathbf{z} \stackrel{\text{def}}{=} \mathbf{c} + \mathbf{e}$ where \mathbf{e} is an error of a certain Hamming weight which can be corrected by the decoding algorithm chosen for \mathcal{C} and \mathbf{c} is an element of the public code. We know that there exists \mathbf{p} in \mathcal{C} such that

$$\mathbf{c} = \mathbf{p} + (\boldsymbol{\lambda}_0 \cdot \mathbf{p}) \mathbf{a}_0. \quad (26)$$

We compute $\mathbf{z}(\alpha) \stackrel{\text{def}}{=} \mathbf{z} + \alpha \mathbf{a}_0$ for all elements α in $GF(q)$. One of these elements α is equal to $-\boldsymbol{\lambda}_0 \cdot \mathbf{p}$ and we obtain $\mathbf{z}(\alpha) = \mathbf{p} + \mathbf{e}$ in this case. Decoding $\mathbf{z}(\alpha)$ in \mathcal{C} will reveal \mathbf{p} and this gives \mathbf{c} by using (26).