

Efficient Encryption from Random Quasi-Cyclic Codes

Carlos Aguilar*, Olivier Blazy[†], Jean-Christophe Deneuville[†],
Philippe Gaborit[†] and Gilles Zémor[‡]

*ENSEEIH, Université de Toulouse, France,
carlos.aguilar@enseeiht.fr

[†]XLIM, Université de Limoges, France,
{philippe.gaborit,olivier.blazy,jean-christophe.deneuville}@xlim.fr

[‡]IMB, Université Bordeaux, France,
gilles.zemor@math.u-bordeaux.fr

Abstract

We propose a framework for constructing efficient code-based encryption schemes from codes that do not hide any structure in their public matrix. The framework is in the spirit of the schemes first proposed by Alekhnovich in 2003 and based on the difficulty of decoding random linear codes from random errors of low weight. We depart somewhat from Alekhnovich’s approach and propose an encryption scheme based on the difficulty of decoding random quasi-cyclic codes. We propose two new cryptosystems instantiated within our framework: the Hamming Quasi-Cyclic cryptosystem (HQC), based on the Hamming metric, and the Rank Quasi-Cyclic cryptosystem (RQC), based on the rank metric. We give a security proof, which reduces the IND-CPA security of our systems to a decisional version of the well known problem of decoding random families of quasi-cyclic codes for the Hamming and rank metrics (the respective QCSD and RQCSD problems). We also provide an analysis of the decryption failure probability of our scheme in the Hamming metric case: for the rank metric there is no decryption failure. Our schemes benefit from a very fast decryption algorithm together with small key sizes of only a few thousand bits. The cryptosystems are very efficient for low encryption rates and are very well suited to key exchange and authentication. Asymptotically, for λ the security parameter, the public key sizes are respectively in $\mathcal{O}(\lambda^2)$ for HQC and in $\mathcal{O}(\lambda^{\frac{4}{3}})$ for RQC. Practical parameter compares well to systems based on ring-LPN or the recent MDPC system.

Index Terms

Code-based Cryptography, Public-Key Encryption, Post-Quantum Cryptography, Provable Security

I. INTRODUCTION

A. Background and Motivation

The first code-based cryptosystem was proposed by McEliece in 1978. This system, which can be seen as a general encryption setting for coding theory, is based on a hidden trapdoor associated to a decodable family of codes, hence a strongly structured family of codes. The inherent construction of the system makes it difficult to formally reduce security to the generic difficulty of decoding random codes. Even if the original McEliece cryptosystem, based on the family of Goppa codes, is still considered secure today, many variants based on alternative families of codes (Reed-Solomon codes, Reed-Muller codes or some alternant codes [MB09, BCGO09]) were broken by recovering in polynomial time the hidden structure [FOPT10]. The fact that the hidden code structure may be uncovered (even possibly for Goppa codes) lies like a sword of Damocles over the system, and finding a practical alternative cryptosystem based on the difficulty of decoding unstructured or random codes has always been a major issue in code-based cryptography. The recently proposed MDPC cryptosystem [MTSB13] (somewhat in the spirit of the NTRU cryptosystem [HPS98]) addresses the problem by using a hidden code structure which is significantly weaker than that of previously used algebraic codes like Goppa codes. The cryptosystem [GMRZ13] followed this trend with a similar approach. Beside this weak hidden structure, the MDPC system has very nice features and in particular relatively small key sizes, because of the cyclic structure of the public matrix. However, even if this system is a strong step forward for code-based cryptography, the hidden structure issue has not altogether disappeared.

In 2003, Alekhnovich proposed an innovative approach based on the difficulty of decoding purely random codes [Ale03]. In this system the trapdoor (or secret key) is a random error vector that has been added to a random codeword of a random code. Recovering the secret key is therefore equivalent to solving the problem of decoding a random code – with no hidden structure. Alekhnovich also proved that breaking the system in any way, not necessarily by recovering the secret key, involves decoding a random linear code.

Even if the system was not totally practical, the approach in itself was a breakthrough for code-based cryptography. Its inspiration was provided in part by the Ajtai-Dwork cryptosystem [AD97] which is based on solving hard lattice problems. The Ajtai-Dwork cryptosystem also inspired the Learning With Errors (LWE) lattice-based cryptosystem by Regev [Reg03] which generated a huge amount of work in lattice-based cryptography. Attempts to emulate this approach in code-based cryptography were also made and systems based on the Learning Parity with Noise (LPN) have been proposed by exploiting the analogy with LWE [DV13, KMP14]: the LPN problem is essentially the problem of decoding random

linear codes of fixed dimension and unspecified length over a binary symmetric channel. The first version of the LWE cryptosystem was not very efficient, but introducing more structure in the public key (as for NTRU) lead to the very efficient Ring-LWE cryptosystem [LPR10]. One strong feature of this last paper is that it gives a reduction from the decisional version of the ring-LWE problem to a search version of the problem. Such a reduction is not known for the case of the ring-LPN problem. A ring version (ring-LPN) was nevertheless introduced in [HKL⁺12] for authentication and for encryption in [DP12].

In this paper, we propose an efficient cryptosystem based on the difficulty of decoding random quasi-cyclic codes. It is inspired by Ring-LWE encryption but is significantly adapted to the coding theory setting. Our construction benefits from some nice features: a reduction to a decisional version of the general problem of decoding random quasi-cyclic codes, hence with no hidden structure, and also quite good parameters and efficiency. Since our approach is relatively general, it can also be used with other metrics such as the rank metric. Finally, another strong feature of our approach is that inherently it leads to a precise analysis of the decryption failure probability, which is also a hard point for the MDPC cryptosystem and is not done in detail for other approaches based on the LPN problem. A relative weakness of our system is its relatively low encryption rate, but this is not a major issue for classical applications of public-key encryption schemes such as authentication or key exchange.

B. Our Contributions

We propose the first efficient code-based cryptosystem whose security relies on decoding small weight vectors of random quasi-cyclic codes. We provide a reduction of our cryptosystem to this problem together with a detailed analysis of the decryption failure probability. Our analysis allows us to give small parameters for code-based encryption in Hamming and Rank metrics. When compared to the MDPC [MTSB13] or LRPC [GMRZ13] cryptosystems, our proposal offers higher security (in terms of security bits) and better decryption guarantees for similar parameters (i.e. key and communication size), but with a lower encryption rate. Overall we propose concrete parameters for different levels of security, in both the classical and quantum settings. These parameters show the great potential of rank metric for cryptography especially for higher security settings. When compared to the ring-LPN based cryptosystem [DP12] our system has better parameters with factors 10 and 100 respectively for the size of the ciphertext and the size of the public key. We also give a general table comparing the different asymptotic sizes for different code-based cryptosystems.

C. Overview of Our Techniques

Our cryptosystem is based on two codes. A first code $\mathcal{C}[n, k]$, for which an efficient decoding algorithm $\mathcal{C}.\text{Decode}(\cdot)$ is known. The code \mathcal{C} together with its generator matrix \mathbf{G} are publicly known. The second code is a $[2n, n]$ random double-circulant code in systematic form, with generator matrix $\mathbf{Q} = (\mathbf{I}_n \mid \mathbf{rot}(\mathbf{q}_r))$ (see Eq. (2) for the definition of $\mathbf{rot}(\cdot)$). The general idea of the system is that the double-circulant code is used to generate some noise, which can be handled and decoded by the code \mathcal{C} . The system can be seen as a noisy adaptation of the ElGamal cryptosystem.

The secret key for our cryptosystem is a *short* vector $\mathbf{sk} = (\mathbf{x}, \mathbf{y})$ (for some metric), whose syndrome $\mathbf{s}^\top = \mathbf{Q}(\mathbf{x}, \mathbf{y})^\top$ is appended to the public key $\mathbf{pk} = (\mathbf{G}, \mathbf{Q}, \mathbf{s}^\top)$. To encrypt a message μ belonging to some plaintext space, it is first encoded through the generator matrix \mathbf{G} , then hidden using the syndrome \mathbf{s} and an additional short vector ϵ to prevent information leakage. In other words, encrypting a message simply consists in providing a noisy encoding of it with a particular shape. Formally, the ciphertext is $(\mathbf{v} = \mathbf{r}\mathbf{Q}^\top, \rho)$, for a short random vector $\mathbf{r} = (\mathbf{r}_1, \mathbf{r}_2)$ and $\rho = \mu\mathbf{G} + \mathbf{s} \cdot \mathbf{r}_2 + \epsilon$ for some natural operator \cdot defined in Sec. II. The legitimate recipient can obtain a noisy version of the plaintext $\rho - \mathbf{v} \cdot \mathbf{y}$ using his secret key $\mathbf{sk} = (\mathbf{x}, \mathbf{y})$ and then recover the (noiseless) plaintext using the efficient decoding algorithm $\mathcal{C}.\text{Decode}$.

For correctness, all previous constructions based on a McEliece approach rely on the fact that the error term added to the encoding of the message is less than or equal to the decoding capability of the code being used. In our construction, this assumption is no longer required and the correctness of our cryptosystem is guaranteed assuming the legitimate recipient can remove sufficiently many errors from the noisy encoding ρ of the message using \mathbf{sk} .

The above discussion leads to the study of the probability that a decoding error occurs, which would yield a decryption failure. We study the typical weight of the error vector \mathbf{e} that one needs to decode in order to decrypt (see Sec. V for details). With the reasonable assumption, backed up by simulations, that the weight of \mathbf{e} behaves in a way that is close to a binomial distribution, we manage a precise estimation of a decoding failure and hence calibrate coding parameters accordingly.

Comparison with the McEliece framework. In the McEliece encryption framework, a hidden code is considered. This leads to two important consequences: first, the security depends on hiding the structure of the code, and second, the decryption algorithm consists of decoding the hidden code which cannot be changed. This yields different instantiations depending on the choice of the hidden code, many of which succumb to attacks and few of which resist.

In our framework there is not one unique hidden code, but two independent codes: the random double-

circulant structure guarantees the security of the scheme, and the public code \mathcal{C} guarantees correct decryption. It makes it possible to consider public families of codes which are difficult to hide but very efficient for decoding: also it requires finding a tradeoff for the code \mathcal{C} , between decoding efficiency and practical decoding complexity. But unlike the McEliece scheme, where the decryption code is fixed, it can be changed depending on the application.

The global decryption failure for our scheme depends on the articulation between the error-vector distribution induced by the double-circulant code and the decoding algorithm $\mathcal{C}.\text{Decode}(\cdot)$. After having studied the error-vector distribution for the Hamming metric we associate it with a particular code adapted to low rates and bit error probability of order $1/3$. Notice that the system could possibly be used for greater encryption rate at the cost of higher parameters. This led us to choose tensor product codes, the composition of two linear codes. Tensor product codes are defined (Def. 14) in Sec. VI, and a detailed analysis of the decryption failure probability for such codes is provided there. For the rank metric case, we consider Gabidulin codes and the case when the error-vector is always decodable, with zero decryption failure probability.

Comparison with Ring-LWE. Our scheme may be considered as in the spirit of the Ring-LWE Encryption scheme but with proofs that work in the coding theory context (for both the Hamming and Rank metrics). It may be considered as a special instance. of the general LWE/LPN methodology, as described, for example, in the recent paper [BS⁺16]. As is mentioned there, even though full LWE-based schemes may, given current knowledge, be asymptotically more efficient than their LPN counterparts, there is still significant appeal in providing a workable variation over the more simple binary field (as it was done with Ring-LWE for the LWE setting). This was previously attempted in [DP12] by relying on the Ring-LPN problem. One of the drawbacks of this last work is to be limited to rings of the form $\mathbb{F}_2[X]/(P(X))$ that are extension fields of \mathbb{F}_2 . In contrast, we suggest using $\mathbb{F}_q[X]/(X^n - 1)$, which reduces security to a decoding problem for quasi-cyclic codes and draws upon Coding Theory’s experience of using this family of codes. Quasi-cyclic codes have indeed been studied for a long time by coding-theorists, and many of the records for minimum distance are held by quasi-cyclic codes. However, no efficient generic decoding algorithm for quasi-cyclic codes has been found, lending faith to the assumption that decoding random quasi-cyclic codes is a hard algorithmic problem. Also, this particular setting also allows us to obtain very good parameters compared to the approach of [DP12] with at least a factor 10 for the size of the keys and messages Departing from the strict LWE/LPN paradigm also enabled us to derive a security reduction to decoding quasi-cyclic codes and arguably gives us more flexibility for the error model. Notably the rank-metric variation that we introduce has not been investigated before in the

LWE/LPN setting, and looks very promising. As mentioned before, one of its features is that it enables a zero error probability of incorrect decryption.

D. Road Map

The rest of the paper is organized as follows: Sec. II gives necessary background on coding theory for Hamming and Rank metrics. Sec. III describes the cryptosystem we propose and its security is discussed in Sec. IV. Sec. V and VI study the decryption failure probability and the family of tensor product codes we consider to perform the decoding for small rate codes. Finally, Sec. VII give parameters.

II. PRELIMINARIES

A. General Definitions

Notation. Throughout this paper, \mathbb{Z} denotes the ring of integers, \mathbb{F} denotes a finite (hence commutative) field, typically \mathbb{F}_q for a prime $q \in \mathbb{Z}$ for Hamming codes or \mathbb{F}_{q^m} for Rank Metric codes. \mathcal{V} is a vector space of dimension n over \mathbb{F} for some positive $n \in \mathbb{Z}$. Elements of \mathcal{V} will be represented by lower-case bold letters, and interchangeably considered as row vectors or polynomials in $\mathcal{R} = \mathbb{F}[X]/(X^n - 1)$. By extension \mathcal{R}_q and \mathcal{R}_{q^m} will denote the latter ring when the base field is \mathbb{F}_q or \mathbb{F}_{q^m} instead of \mathbb{F} , respectively. Matrices will be represented by upper-case bold letters.

For any two elements $\mathbf{x}, \mathbf{y} \in \mathcal{V}$, we define their product similarly as in \mathcal{R} , i.e. $\mathbf{x} \cdot \mathbf{y} = \mathbf{c} \in \mathcal{V}$ with

$$c_k = \sum_{i+j \equiv k \pmod n} x_i y_j, \text{ for } k \in \{0, 1, \dots, n-1\}. \quad (1)$$

Notice that as the product of two elements over the *commutative* ring \mathcal{R} , we have $\mathbf{x} \cdot \mathbf{y} = \mathbf{y} \cdot \mathbf{x}$.

For any finite set \mathcal{S} , $x \stackrel{\$}{\leftarrow} \mathcal{S}$ denotes a uniformly random element sampled from \mathcal{S} . For any $x \in \mathbb{R}$, let $\lfloor x \rfloor$ denotes the biggest integer smaller than (or equal to) x . Finally, all logarithms $\log(\cdot)$ will be base-2 unless explicitly mentioned. For a probability distribution \mathcal{D} , we denote by $X \sim \mathcal{D}$ the fact that X is a random variable following \mathcal{D} .

Definition 1 (Circulant Matrix). Let $\mathbf{x} = (x_1, \dots, x_n) \in \mathbb{F}^n$. The circulant matrix induced by \mathbf{x} is defined and denoted as follows:

$$\mathbf{rot}(\mathbf{x}) = \begin{pmatrix} x_1 & x_n & \dots & x_2 \\ x_2 & x_1 & \dots & x_3 \\ \vdots & \vdots & \ddots & \vdots \\ x_n & x_{n-1} & \dots & x_1 \end{pmatrix} \in \mathbb{F}^{n \times n} \quad (2)$$

As a consequence, it is easy to see that the product of any two elements $\mathbf{x}, \mathbf{y} \in \mathcal{V}$ can be expressed as a usual vector-matrix (or matrix-vector) product using the $\mathbf{rot}(\cdot)$ operator as

$$\mathbf{x} \cdot \mathbf{y} = \mathbf{x} \cdot \mathbf{rot}(\mathbf{y})^\top = \left(\mathbf{rot}(\mathbf{x}) \mathbf{y}^\top \right)^\top = \mathbf{y} \cdot \mathbf{rot}(\mathbf{x})^\top = \mathbf{y} \cdot \mathbf{x}. \quad (3)$$

Coding Theory. We now turn to recall some basic definitions and properties relating to coding theory that will be useful to our construction. We mainly focus on generic definitions, and refer the reader to Sec. II-B for instantiations with a specific metric, and also, to [Ove07] for a complete survey on Code-based Cryptography due to space restrictions.

Definition 2 (Linear Code). A Linear Code \mathcal{C} of length n and dimension k (denoted $[n, k]$) is a subspace of \mathcal{V} of dimension k . Elements of \mathcal{C} are referred to as codewords.

Definition 3 (Generator Matrix). We say that $\mathbf{G} \in \mathbb{F}^{k \times n}$ is a Generator Matrix for the $[n, k]$ code \mathcal{C} if

$$\mathcal{C} = \left\{ \boldsymbol{\mu} \mathbf{G}, \text{ for } \boldsymbol{\mu} \in \mathbb{F}^k \right\}. \quad (4)$$

Definition 4 (Parity-Check Matrix). Given an $[n, k]$ code \mathcal{C} , we say that $\mathbf{H} \in \mathbb{F}^{(n-k) \times n}$ is a Parity-Check Matrix for \mathcal{C} if \mathbf{H} is a generator matrix of the dual code \mathcal{C}^\perp , or more formally, if

$$\mathcal{C}^\perp = \{ \mathbf{x} \in \mathbb{F}^n \text{ such that } \sigma(\mathbf{x}) = \mathbf{0} \}. \quad (5)$$

where

$$\sigma(\mathbf{x}) = \mathbf{H} \mathbf{x}^\top$$

denotes the syndrome of \mathbf{x} .

Definition 5 (Minimum Distance). Let \mathcal{C} be an $[n, k]$ linear code over \mathcal{V} and let ω be a norm on \mathcal{V} . The Minimal Distance of \mathcal{C} is

$$d = \min_{\mathbf{x}, \mathbf{y} \in \mathcal{C}, \mathbf{x} \neq \mathbf{y}} \omega(\mathbf{x} - \mathbf{y}). \quad (6)$$

A code with minimum distance d is capable of decoding arbitrary patterns of up to $\delta = \lfloor \frac{d-1}{2} \rfloor$ errors. Code parameters are written denoted $[n, k, d]$.

Code-based cryptography usually suffers from huge keys. In order to keep our cryptosystem efficient, we will use the strategy of Gaborit [Gab05] for shortening keys. This results in Quasi-Cyclic Codes, as defined below.

Definition 6 (Quasi-Cyclic Codes [MTSB13]). View a vector $\mathbf{x} = (\mathbf{x}_1, \dots, \mathbf{x}_s)$ of \mathbb{F}_2^{sn} as s successive blocks (n -tuples). An $[sn, k, d]$ linear code \mathcal{C} is Quasi-Cyclic (QC) of order s if, for any $\mathbf{c} = (\mathbf{c}_1, \dots, \mathbf{c}_s) \in$

\mathcal{C} , the vector obtained after applying a simultaneous circular shift to every block $\mathbf{c}_1, \dots, \mathbf{c}_s$ is also a codeword.

More formally, by considering each block \mathbf{c}_i as a polynomial in $\mathcal{R} = \mathbb{F}[X]/(X^n - 1)$, the code \mathcal{C} is QC of order s if for any $\mathbf{c} = (\mathbf{c}_1, \dots, \mathbf{c}_s) \in \mathcal{C}$ it holds that $(X \cdot \mathbf{c}_1, \dots, X \cdot \mathbf{c}_s) \in \mathcal{C}$.

Definition 7 (Systematic Quasi-Cyclic Codes). A systematic Quasi-Cyclic $[sn, (s - \ell)n]$ code of order s is a quasi-cyclic code with a parity-check matrix of the form:

$$\mathbf{H} = \begin{bmatrix} \mathbf{I}_n & 0 & \cdots & 0 & \mathbf{A}_1 \\ 0 & \mathbf{I}_n & & & \mathbf{A}_2 \\ & & \ddots & & \vdots \\ 0 & & \cdots & \mathbf{I}_n & \mathbf{A}_\ell \end{bmatrix} \quad (7)$$

where $\mathbf{A}_1, \dots, \mathbf{A}_\ell$ are circulant $n \times n$ matrices.

B. Different Types of Metric

The previous definitions are generic and can be adapted to any type of metric.

Besides the well known Hamming metric, we also consider, in this paper, the rank metric which has interesting properties for cryptography.

We recall some definitions and properties of Rank Metric Codes, and refer the reader to [Loi06] for more details. Consider the case where \mathbb{F} is an extension of a finite field, *i.e.* $\mathbb{F} = \mathbb{F}_{q^m}$, and let $\mathbf{x} = (x_1, \dots, x_n) \in \mathbb{F}_{q^m}^n$ be an element of some vector space \mathcal{V} of dimension n over \mathbb{F}_{q^m} . A basic property of field extensions is that they can be seen as vector spaces over the base field they extend. Hence, by considering \mathbb{F}_{q^m} as a vector space of dimension m over \mathbb{F}_q , and given a basis $(\mathbf{e}_1, \dots, \mathbf{e}_m) \in \mathbb{F}_q^m$, one can express each x_i as

$$x_i = \sum_{j=1}^m x_{j,i} \mathbf{e}_j \text{ (or equivalently } x_i = (x_{1,i}, \dots, x_{m,i}) \text{)}. \quad (8)$$

Using such an expression, we can expand $\mathbf{x} \in \mathbb{F}_{q^m}^n$ to a matrix $\mathbf{E}(\mathbf{x})$ such that:

$$\mathbf{x} = \begin{pmatrix} x_1 & x_2 & \cdots & x_n \end{pmatrix} \in \mathbb{F}_{q^m}^n \quad (9)$$

$$\mathbf{E}(\mathbf{x}) = \begin{pmatrix} x_{1,1} & x_{1,2} & \cdots & x_{1,n} \\ x_{2,1} & x_{2,2} & \cdots & x_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ x_{m,1} & x_{m,2} & \cdots & x_{m,n} \end{pmatrix} \in \mathbb{F}_q^{m \times n}. \quad (10)$$

The definitions usually associated to Hamming metric codes such as norm (Hamming weight), support (non-zero coordinates), and isometries ($n \times n$ permutation matrices) can be adapted to the Rank metric setting based on the representation of elements as matrices in $F_q^{m \times n}$.

For an element \mathbf{x} of $\mathbb{F}_{q^m}^n$ we define its rank norm $\omega(\mathbf{x})$ as the rank of the matrix $\mathbf{E}(\mathbf{x})$. A rank metric code \mathcal{C} of length n and dimension k over the field \mathbb{F}_{q^m} is a subspace of dimension k of $\mathbb{F}_{q^m}^n$ embedded with the rank norm. In the following, \mathcal{C} is a rank metric code of length n and dimension k over \mathbb{F}_{q^m} , where $q = p^\eta$ for some prime p and positive $\eta \geq 1$. The matrix \mathbf{G} denotes a $k \times n$ generator matrix of \mathcal{C} and \mathbf{H} is one of its parity check matrices. The minimum rank distance of the code \mathcal{C} is the minimum rank of non-zero vectors of the code. We also consider the usual inner product which allows to define the notion of dual code.

Let $\mathbf{x} = (x_1, x_2, \dots, x_n) \in \mathbb{F}_{q^m}^n$ be a vector of rank r . We denote by $E = \langle x_1, \dots, x_n \rangle$ the \mathbb{F}_q -subspace of \mathbb{F}_{q^m} generated by the coordinates of \mathbf{x} i.e. $E = \text{Vect}(x_1, \dots, x_n)$. The vector space E is called the *support* of \mathbf{x} and denoted $\text{Supp}(\mathbf{x})$. Finally, the notion of *isometry* which in Hamming metric corresponds to the action of the code on $n \times n$ permutation matrices, is replaced for the Rank metric by the action of $n \times n$ invertible matrices over the base field \mathbb{F}_q .

Bounds for Rank Metric Codes. The classical bounds for Hamming metric have straightforward rank metric analogues.

Singleton Bound. The classical Singleton bound for linear $[n, k]$ codes of minimum rank r over \mathbb{F}_{q^m} applies naturally in the Rank metric setting. It works in the same way as for linear codes (by finding an information set) and reads $r \leq 1 + n - k$. When $n > m$ this bound can be rewritten [Loi06] as

$$r \leq 1 + \left\lfloor \frac{(n - k)m}{n} \right\rfloor. \quad (11)$$

Codes achieving this bound are called Maximum Rank Distance codes (MRD).

Deterministic Decoding. Unlike the situation for the Hamming metric, there do not exist many families of codes for the rank metric which are able to decode rank errors efficiently up to a given norm. When we are dealing with deterministic decoding, there is essentially only one known family of rank codes which can decode efficiently: the family of Gabidulin codes [Gab85]. These codes are an analogue of Reed-Solomon codes [RS60] where polynomials are replaced by q -polynomials. These codes are defined over \mathbb{F}_{q^m} and for $k \leq n \leq m$, Gabidulin codes of length n and dimension k are optimal and satisfy the Singleton bound for $m = n$ with minimum distance $d = n - k + 1$. They can decode up to $\lfloor \frac{n-k}{2} \rfloor$ rank errors in a deterministic way.

Probabilistic Decoding. There also exists a simple family of codes which has been described for the subspace metric in [SKK10] and can be straightforwardly adapted to rank metric. These codes reach

asymptotically the equivalent of the Gilbert-Varshamov bound for the rank metric, however their non-zero probability of decoding failure makes them less interesting for the cases we consider in this paper.

C. Difficult Problems for Cryptography

In this section we describe difficult problems which can be used for cryptography. We give generic definitions for these problems which are usually instantiated with the Hamming metric but can also be instantiated with the rank metric. After defining the problems we discuss their complexity.

All problems are variants of the *decoding problem*, which consists of looking for the closest codeword to a given vector: when dealing with linear codes, it is readily seen that the decoding problem stays the same when one is given the *syndrome* of the received vector rather than the received vector. We therefore speak of *Syndrome Decoding* (SD).

Definition 8 (SD Distribution). *For positive integers, n , k , and w , the $\text{SD}(n, k, w)$ Distribution chooses $\mathbf{H} \stackrel{\$}{\leftarrow} \mathbb{F}^{(n-k) \times n}$ and $\mathbf{x} \stackrel{\$}{\leftarrow} \mathbb{F}^n$ such that $\omega(\mathbf{x}) = w$, and outputs $(\mathbf{H}, \sigma(\mathbf{x}) = \mathbf{H}\mathbf{x}^\top)$.*

Definition 9 (Search SD Problem). *Let ω be a norm over \mathcal{V} . On input $(\mathbf{H}, \mathbf{y}^\top) \in \mathbb{F}^{(n-k) \times n} \times \mathbb{F}^{(n-k)}$ from the SD distribution, the Syndrome Decoding Problem $\text{SD}(n, k, w)$ asks to find $\mathbf{x} \in \mathbb{F}^n$ such that $\mathbf{H}\mathbf{x}^\top = \mathbf{y}^\top$ and $\omega(\mathbf{x}) = w$.*

Depending on the metric the above problem is instantiated with, we denote it either by SD for the Hamming metric or by Rank-SD (RSD) for the Rank metric.

For the Hamming distance the SD problem has been proven to be NP-complete in [BMvT78]. This problem can also be seen as the Learning Parity with Noise (LPN) problem with a fixed number of samples [AIK07]. The RSD problem has recently been proven difficult with a probabilistic reduction to the Hamming setting in [GZ16]. For cryptography we also need a Decisional version of the problem, which is given in the following Definition:

Definition 10 (Decisional SD Problem). *On input $(\mathbf{H}, \mathbf{y}^\top) \stackrel{\$}{\leftarrow} \mathbb{F}^{(n-k) \times n} \times \mathbb{F}^{(n-k)}$, the Decisional SD Problem $\text{DSD}(n, k, w)$ asks to decide with non-negligible advantage whether $(\mathbf{H}, \mathbf{y}^\top)$ came from the $\text{SD}(n, k, w)$ distribution or the uniform distribution over $\mathbb{F}^{(n-k) \times n} \times \mathbb{F}^{(n-k)}$.*

As mentioned above, this problem is the problem of decoding random linear codes from random errors. The random errors are often taken as independent Bernoulli variables acting independently on vector coordinates, rather than uniformly chosen from the set of errors of a given weight, but this hardly makes any difference and one model rather than the other is a question of convenience. The DSD problem

has been shown to be polynomially equivalent to its search version in [AIK07]. The rank metric version of the problem is denoted by DRSD, by applying the transformation described in [GZ16] it can be shown that the problem can be reduced to a search problem for the Hamming metric. Hence even if the reduction is not optimal, it nevertheless shows the hardness of the problem.

Finally, as for both metrics our cryptosystem will use QC-codes, we explicitly define the problem on which our cryptosystem will rely. The following Definitions describe the DSD problem in the QC configuration, and are just a combination of Def. 6 and 10. Quasi-Cyclic codes are very useful in cryptography since their compact description allows to decrease considerably the size of the keys. In particular the case $s = 2$ corresponds to double circulant codes with generator matrices of the form $(\mathbf{I}_n \mid \mathbf{A})$ for \mathbf{A} a circulant matrix. Such double circulant codes have been used for almost 10 years in cryptography (cf [GG07]) and more recently in [MTSB13]. Quasi-cyclic codes of order 3 are also considered in [MTSB13].

Definition 11 (*s*-QCSD Distribution). *For positive integers n, k, w and s , the s -QCSD(n, k, w, s) Distribution chooses uniformly at random a parity matrix $\mathbf{H} \xleftarrow{\$} \mathbb{F}^{(sn-k) \times sn}$ of a systematic QC code \mathcal{C} of order s (see Definition 7) together with a vector $\mathbf{x} = (\mathbf{x}_1, \dots, \mathbf{x}_s) \xleftarrow{\$} \mathbb{F}^{sn}$ such that $\omega(\mathbf{x}_i) = w, i = 1..s$, and outputs $(\mathbf{H}, \mathbf{H}\mathbf{x}^\top)$.*

Definition 12 ((Search) *s*-QCSD Problem). *For positive integers n, k, w, s , a random parity check matrix \mathbf{H} of a systematic QC code \mathcal{C} and $\mathbf{y} \xleftarrow{\$} \mathbb{F}^{sn-k}$, the Search *s*-Quasi-Cyclic SD Problem s -QCSD(n, k, w) asks to find $\mathbf{x} = (\mathbf{x}_1, \dots, \mathbf{x}_s) \in \mathbb{F}^{sn}$ such that $\omega(\mathbf{x}_i) = w, i = 1..s$, and $\mathbf{y} = \mathbf{x}\mathbf{H}^\top$.*

It would be somewhat more natural to choose the parity-check matrix \mathbf{H} to be made up of independent uniformly random circulant submatrices, rather than with the special form required by (7). We choose this distribution so as to make the security reduction to follow less technical. It is readily seen that, for fixed s , when choosing quasi-cyclic codes with this more general distribution, one obtains with non-negligible probability, a quasi-cyclic code that admits a parity-check matrix of the form (7). Therefore requiring quasi-cyclic codes to be systematic does not hurt the generality of the decoding problem for quasi-cyclic codes. A similar remark holds for the slightly special form of weight distribution of the vector \mathbf{x} .

Assumption 1. *Although there is no general complexity result for quasi-cyclic codes, decoding these codes is considered hard by the community. There exist general attacks which uses the cyclic structure of the code [Sen11, HT15] but these attacks have only a very limited impact on the practical complexity of the problem. The conclusion is that in practice, the best attacks are the same as those for non-circulant codes up to a small factor.*

The problem has a decisional form:

Definition 13 (Decisional s -QCSD Problem). For positive integers n, k, w, s , a random parity check matrix \mathbf{H} of a systematic QC code \mathcal{C} and $\mathbf{y} \xleftarrow{\$} \mathbb{F}^{sn}$, the Decisional s -Quasi-Cyclic SD Problem s -DQCSD(n, k, w) asks to decide with non-negligible advantage whether $(\mathbf{H}, \mathbf{y}^\top)$ came from the s -QCSD(n, k, w) distribution or the uniform distribution over $\mathbb{F}^{(sn-k) \times sn} \times \mathbb{F}^{sn-k}$.

As for the ring-LPN problem, there is no known reduction from the search version of s -QCSD problem to its decisional version. The proof of [AIK07] cannot be directly adapted in the quasi-cyclic case, however the best known attacks on the decisional version of the problem s -QCSD remain the direct attacks on the search version of the problem s -QCSD.

The situation is similar for the rank versions of these problems which are respectively denoted by s -RQCSD and s -DRQCSD, and for which the best attacks over the decisional problem consist in attacking the search version of the problem.

D. Practical Attacks

The practical complexity of the SD problem for the Hamming metric has been widely studied for more than 50 years. For small weights the best known attacks are exponential in the weight of the researched codeword. The best attacks can be found in [BJMM12].

The RSD problem is less known in cryptography but has also been studied for a long time, ever since a rank metric version of the McEliece cryptosystem was introduced in 1991 [GPT91]. We recall the main types of attack on the RSD problem below.

The complexity of practical attacks grows very quickly with the size of parameters: there is a structural reason to this. For the Hamming distance, attacks typically rely on enumerating the number of words of length n and support size (weight) t , which amounts to the Newton binomial coefficient $\binom{n}{t}$, whose value is bounded from above by 2^n . In the rank metric case, counting the number of possible supports of size r for a rank code of length n over \mathbb{F}_{q^m} corresponds to counting the number of subspaces of dimension r in \mathbb{F}_{q^m} : this involves the *Gaussian binomial coefficient* of size roughly $q^{(m-r)m}$, whose value is also exponential in the blocklength but with a quadratic term in the exponent.

There exist two types of generic attacks on the problem:

- **Combinatorial attacks:** these attacks are usually the best ones for small values of q (typically $q = 2$) and when n and k are not too small: when q increases, the combinatorial aspect makes them less efficient. The best combinatorial attack has recently been updated to $(n - k)^3 m^3 q^{(r-1) \lfloor \frac{(k+1)m}{n} \rfloor}$ to take into account the value of n [GRS16].

- **Algebraic attacks:** the particular nature of the rank metric makes it a natural field for algebraic attacks using Gröbner bases, since these attacks are largely independent of the value of q and in some cases may also be largely independent of m . These attacks are usually the most efficient when q increases. For the cases considered in this paper where q is taken to be small, the complexity is greater than the cost of combinatorial attacks (see [LdVP06, FdVP08, GRS16]).

Note that the recent improvements on decoding random codes for the Hamming distance correspond to birthday paradox attacks. An open question is whether these improvements apply to rank metric codes. Given that the support of the error on codewords in rank metric is not related to the error coordinates, the birthday paradox strategy has failed for the rank metric, which for the moment seems to keep these codes protected from the aforementioned advances.

III. A NEW ENCRYPTION SCHEME

A. Encryption and Security

Encryption Scheme. An encryption scheme is a tuple of four polynomial time algorithms (Setup, KeyGen, Encrypt, Decrypt):

- Setup(1^λ), where λ is the security parameter, generates the global parameters **param** of the scheme;
- KeyGen(**param**) outputs a pair of keys, a (public) encryption key **pk** and a (private) decryption key **sk**;
- Encrypt(**pk**, μ , θ) outputs a ciphertext **c**, on the message μ , under the encryption key **pk**, with the randomness θ ;
- Decrypt(**sk**, **c**) outputs the plaintext μ , encrypted in the ciphertext **c** or \perp .

Such an encryption scheme has to satisfy both *Correctness* and *Indistinguishability under Chosen Plaintext Attack* (IND-CPA) security properties.

Correctness: For every λ , every **param** \leftarrow Setup(1^λ), every pair of keys (**pk**, **sk**) generated by KeyGen, every message μ , we should have $P[\text{Decrypt}(\text{sk}, \text{Encrypt}(\text{pk}, \mu, \theta)) = \mu] = 1 - \epsilon(\lambda)$ for ϵ a negligible function, where the probability is taken over varying randomness θ .

IND-CPA [GM84]: This notion formalized by the adjacent game, states that an adversary shouldn't be able to efficiently guess which plaintext has been encrypted even if he knows it is one among two plaintexts of his choice.

The global advantage for polynomial time adversaries (running in time less than t) is:

$$\mathbf{Adv}_{\mathcal{E}}^{\text{ind}}(\lambda, t) = \max_{\mathcal{A} \leq t} \mathbf{Adv}_{\mathcal{E}, \mathcal{A}}^{\text{ind}}(\lambda), \quad (12)$$

where $\text{Adv}_{\mathcal{E},\mathcal{A}}^{\text{ind}}(\lambda)$ is the advantage the adversary \mathcal{A} has in winning game $\text{Exp}_{\mathcal{E},\mathcal{A}}^{\text{ind}-b}(\lambda)$:

$\text{Exp}_{\mathcal{E},\mathcal{A}}^{\text{ind}-b}(\lambda)$

1. $\text{param} \leftarrow \text{Setup}(1^\lambda)$
2. $(\text{pk}, \text{sk}) \leftarrow \text{KeyGen}(\text{param})$
3. $(\mu_0, \mu_1) \leftarrow \mathcal{A}(\text{FIND} : \text{pk})$
4. $\mathbf{c}^* \leftarrow \text{Encrypt}(\text{pk}, \mu_b, \theta)$
5. $b' \leftarrow \mathcal{A}(\text{GUESS} : \mathbf{c}^*)$
6. RETURN b'

$$\text{Adv}_{\mathcal{E},\mathcal{A}}^{\text{ind}}(\lambda) = \left| \Pr[\text{Exp}_{\mathcal{E},\mathcal{A}}^{\text{ind}-1}(\lambda) = 1] - \Pr[\text{Exp}_{\mathcal{E},\mathcal{A}}^{\text{ind}-0}(\lambda) = 1] \right|. \quad (13)$$

B. Presentation of the Scheme

We begin this Section by describing a generic version of the proposed encryption scheme. This description does not depend on the particular metric used. The particular case of the Hamming metric is denoted by HQC (for Hamming Quasi-Cyclic) and RQC (for Rank Quasi-Cyclic) in the case of the rank metric. Parameter sets for binary Hamming Codes and Rank Metric Codes can be respectively found in Sec. VII-A and VII-B.

Presentation of the scheme. Recall from the introduction that the scheme uses two types of codes, a decodable $[n, k]$ code which can correct δ errors and a random double-circulant $[2n, n]$ code. In the following, we assume \mathcal{V} is a vector space on some field \mathbb{F} , ω is a norm on \mathcal{V} and for any \mathbf{x} and $\mathbf{y} \in \mathcal{V}$, their distance is defined as $\omega(\mathbf{x} - \mathbf{y}) \in \mathbb{R}^+$. Now consider a linear code \mathcal{C} over \mathbb{F} of dimension k and length n (generated by $\mathbf{G} \in \mathbb{F}^{k \times n}$), that can correct up to δ errors via an efficient algorithm $\mathcal{C}.\text{Decode}(\cdot)$. The scheme consists of the following four polynomial-time algorithms:

- **Setup**(1^λ): generates the global parameters $n = n(1^\lambda)$, $k = k(1^\lambda)$, $\delta = \delta(1^\lambda)$, and $w = w(1^\lambda)$. The plaintext space is \mathbb{F}^k . Outputs $\text{param} = (n, k, \delta, w)$.
- **KeyGen**(param): generates $\mathbf{q}_r \xleftarrow{\$} \mathcal{V}$, matrix $\mathbf{Q} = (\mathbf{I}_n \mid \text{rot}(\mathbf{q}_r))$, the generator matrix $\mathbf{G} \in \mathbb{F}^{k \times n}$ of \mathcal{C} , $\text{sk} = (\mathbf{x}, \mathbf{y}) \xleftarrow{\$} \mathcal{V}^2$ such that $\omega(\mathbf{x}) = \omega(\mathbf{y}) = w$, sets $\text{pk} = (\mathbf{G}, \mathbf{Q}, \mathbf{s} = \text{sk} \cdot \mathbf{Q}^\top)$, and returns (pk, sk) .
- **Encrypt**($\text{pk} = (\mathbf{G}, \mathbf{Q}, \mathbf{s}), \mu, \theta$): uses randomness θ to generate $\epsilon \xleftarrow{\$} \mathcal{V}$, $\mathbf{r} = (\mathbf{r}_1, \mathbf{r}_2) \xleftarrow{\$} \mathcal{V}^2$ such that $\omega(\epsilon), \omega(\mathbf{r}_1), \omega(\mathbf{r}_2) \leq w$, sets $\mathbf{v}^\top = \mathbf{Q}\mathbf{r}^\top$ and $\boldsymbol{\rho} = \mu\mathbf{G} + \mathbf{s} \cdot \mathbf{r}_2 + \epsilon$. It finally returns $\mathbf{c} = (\mathbf{v}, \boldsymbol{\rho})$, an encryption of μ under pk .

- $\text{Decrypt}(\text{sk} = (\mathbf{x}, \mathbf{y}), \mathbf{c} = (\mathbf{v}, \boldsymbol{\rho}))$: returns $\mathcal{C}.\text{Decode}(\boldsymbol{\rho} - \mathbf{v} \cdot \mathbf{y})$.

Notice that the generator matrix \mathbf{G} of the code \mathcal{C} is publicly known, so the security of the scheme and the ability to decrypt do not rely on the knowledge of the error correcting code \mathcal{C} being used.

Correctness. The correctness of our new encryption scheme clearly relies on the decoding capability of the code \mathcal{C} . Specifically, assuming $\mathcal{C}.\text{Decode}$ correctly decodes $\boldsymbol{\rho} - \mathbf{v} \cdot \mathbf{y}$, we have:

$$\text{Decrypt}(\text{sk}, \text{Encrypt}(\text{pk}, \boldsymbol{\mu}, \theta)) = \boldsymbol{\mu}. \quad (14)$$

And $\mathcal{C}.\text{Decode}$ correctly decodes $\boldsymbol{\rho} - \mathbf{x} \cdot \mathbf{y}$ whenever

$$\omega(\mathbf{s} \cdot \mathbf{r}_2 - \mathbf{v} \cdot \mathbf{y} + \boldsymbol{\epsilon}) \leq \delta \quad (15)$$

$$\omega((\mathbf{x} + \mathbf{q}_r \cdot \mathbf{y}) \cdot \mathbf{r}_2 - (\mathbf{r}_1 + \mathbf{q}_r \cdot \mathbf{r}_2) \cdot \mathbf{y} + \boldsymbol{\epsilon}) \leq \delta \quad (16)$$

$$\omega(\mathbf{x} \cdot \mathbf{r}_2 - \mathbf{r}_1 \cdot \mathbf{y} + \boldsymbol{\epsilon}) \leq \delta \quad (17)$$

In order to provide an upper bound on the decryption failure probability, an analysis of the distribution of the error vector $\mathbf{x} \cdot \mathbf{r}_2 - \mathbf{r}_1 \cdot \mathbf{y} + \boldsymbol{\epsilon}$ is provided in Sec. V.

IV. SECURITY OF THE SCHEME

In this section we prove the security of our scheme, the proof is generic for any metric, and the security is reduced to the respective quasi-cyclic problems defined for Hamming and rank metric in Section 2.

Theorem 1. *The scheme presented above is IND-CPA under the 2-DQCSD and 3-DQCSD assumptions.*

Proof. To prove the security of the scheme, we are going to build a sequence of games transitioning from an adversary receiving an encryption of message $\boldsymbol{\mu}_0$ to an adversary receiving an encryption of a message $\boldsymbol{\mu}_1$ and show that if the adversary manages to distinguish one from the other, then we can build a simulator breaking the DQCSD assumption, for QC codes of order 2 or 3 (codes with parameters $[2n, n]$ or $[3n, 2n]$), and running in approximately the same time.

Game \mathcal{G}_0 : This is the real game, we run an honest KeyGen algorithm, and after receiving $(\boldsymbol{\mu}_0, \boldsymbol{\mu}_1)$ from the adversary we produce an encryption of $\boldsymbol{\mu}_0$.

Game \mathcal{G}_1 : In this game we start by forgetting the decryption key sk , and taking \mathbf{s} at random, and then proceed honestly.

Game \mathcal{G}_2 : Now that we no longer know the decryption key, we can start generating random ciphertexts. So instead of picking correctly weighted $\mathbf{r}_1, \mathbf{r}_2, \boldsymbol{\epsilon}$, the simulator now picks random vectors in the full space.

Game G_3 : We now encrypt the other plaintext. We chose $\mathbf{r}'_1, \mathbf{r}'_2, \epsilon'$ uniformly and set $\mathbf{v}^\top = \mathbf{Q}\mathbf{r}'^\top$ and $\rho = \mu_1\mathbf{G} + \mathbf{s} \cdot \mathbf{r}'_2 + \epsilon'$.

Game G_4 : In this game, we now pick $\mathbf{r}'_1, \mathbf{r}'_2, \epsilon'$ with the correct weight.

Game G_5 : We now conclude by switching the public key to an honestly generated one.

The only difference between Game G_0 and Game G_1 is the s in the public key sent to the attacker at the beginning of the IND-CPA game. If the attacker has an algorithm \mathcal{A} able to distinguish these two games he can build a distinguisher for the DQCSD problem. Indeed for a DQCSD challenge (Q, s) he can: adjoin G to build a public key; run the IND-CPA game with this key and algorithm \mathcal{A} ; decide on which Game he is. He then replies to the DQCSD challenge saying that (Q, s) is uniform if he is on Game G_1 or follows the QCSD distribution if he is in Game G_0 .

In both Game G_1 and Game G_2 the plaintext encrypted is known to be μ_0 the attacker can compute:

$$\begin{pmatrix} \mathbf{v} \\ \rho - \mu_0\mathbf{G} \end{pmatrix} = \begin{pmatrix} \mathbf{I}_n & \mathbf{0} & \mathbf{rot}(\mathbf{q}_r) \\ \mathbf{0} & \mathbf{I}_n & \mathbf{rot}(\mathbf{s}) \end{pmatrix} \cdot (\mathbf{r}_1, \epsilon, \mathbf{r}_2)^\top$$

The difference between Game G_1 and Game G_2 is that in the former $(\mathbf{v}, \rho - \mu_0\mathbf{G})$ follows the QCSD distribution (for a $2n \times 3n$ QC matrix of order 3), and in the latter it follows a uniform distribution (as \mathbf{r}_1 and ϵ are uniformly distributed and independently chosen One-Time Pads). If the attacker is able to distinguish Game G_1 and Game G_2 he can therefore break the 3 – DQCSD assumption.

The outputs from Game G_2 and Game G_3 follow the exact same distribution, and therefore the two games are indistinguishable from an information-theoretic point of view. Indeed, for each tuple (\mathbf{r}, ϵ) of Game G_2 , resulting in a given (\mathbf{v}, ρ) , there is a one to one mapping to a couple (\mathbf{r}', ϵ') resulting in Game G_3 in the *same* (\mathbf{v}, ρ) , namely $\mathbf{r}' = \mathbf{r}$ and $\epsilon' = \mu_0\mathbf{G} + \mu_1\mathbf{G}$. This implies that choosing uniformly (\mathbf{r}, ϵ) in Game G_2 and choosing uniformly (\mathbf{r}', ϵ') in Game G_3 leads to the same output distribution for (\mathbf{v}, ρ) .

Game G_3 and Game G_4 are the equivalents of Game G_2 and Game G_1 except μ_1 is used instead of μ_0 . A distinguisher between these two games breaks therefore the 3 – DQCSD assumption too. Similarly Game G_3 and Game G_5 are the equivalents of Game G_1 and Game G_0 and a distinguisher between these two games breaks the DQCSD assumption.

We managed to build a sequence of games allowing a simulator to transform a ciphertext of a message μ_0 to a ciphertext of a message μ_1 . Hence the advantage of an adversary against the IND-CPA experiment is bounded:

$$\mathbf{Adv}_{\mathcal{E}, \mathcal{A}}^{\text{ind}}(\lambda) \leq 2 \cdot \left(\mathbf{Adv}^{2\text{-DQCSD}}(\lambda) + \mathbf{Adv}^{3\text{-DQCSD}}(\lambda) \right). \quad (18)$$

□

V. ANALYSIS OF THE DISTRIBUTION OF THE ERROR VECTOR OF THE SCHEME FOR HAMMING DISTANCE

The aim of this Section is to determine the probability that the condition in Eq. (17) holds. In order to do so, we study the error distribution of the error vector $\mathbf{e} = \mathbf{x} \cdot \mathbf{r}_2 - \mathbf{r}_1 \cdot \mathbf{y} + \boldsymbol{\epsilon}$.

The vectors $\mathbf{x}, \mathbf{y}, \mathbf{r}_1, \mathbf{r}_2, \boldsymbol{\epsilon}$ have been taken to be uniformly and independently chosen among vectors of weight w . A very close probabilistic model is when all these independent vectors are chosen to follow the distribution of random vectors whose coordinates are independent Bernoulli variables of parameter $p = w/n$. To simplify analysis we shall assume this model rather than the constant weight uniform model. Both models are very close, and our cryptographic protocols work just as well in both settings.

We first evaluate the distributions of the products $\mathbf{x} \cdot \mathbf{r}_2$ and $\mathbf{r}_1 \cdot \mathbf{y}$.

Proposition 2. *Let $\mathbf{x} = (X_1, \dots, X_n)$ be a random vector where the X_i are independent Bernoulli variables of parameter p , $P(X_i = 1) = p$. Let $\mathbf{y} = (Y_1, \dots, Y_n)$ be a vector following the same distribution and independent of \mathbf{x} . Let $\mathbf{z} = \mathbf{x} \cdot \mathbf{y} = (Z_1, \dots, Z_n)$ as defined in Eq. (1). Then*

$$\begin{cases} \Pr[Z_k = 1] = \sum_{\substack{0 \leq i \leq n, \\ i \text{ odd}}} \binom{n}{i} p^{2i} (1-p^2)^{n-i}, \\ \Pr[Z_k = 0] = \sum_{\substack{0 \leq i \leq n, \\ i \text{ even}}} \binom{n}{i} p^{2i} (1-p^2)^{n-i}. \end{cases} \quad (19)$$

Proof. We have

$$Z_k = \sum_{i+j=k \bmod n} X_i Y_j \pmod{2}. \quad (20)$$

Every term $X_i Y_j$ is the product of two independent Bernoulli variables of parameter p , and is therefore a Bernoulli variable of parameter p^2 . The variable Z_k is the sum of n such products, which are all independent since every variable X_i is involved exactly once in (20), for $0 \leq i \leq n-1$, and similarly every variable Y_j is involved once in (20). Therefore Z_k is the sum modulo 2 of n independent Bernoulli variables of parameter p^2 . □

Let us denote by $\tilde{p} = \tilde{p}(n, w) = \Pr[z_k = 1]$ from Eq. (19). We will be working in the regime where $w = \omega\sqrt{n}$, meaning $p^2 = (\frac{w}{n})^2 = \omega^2/n$. When n goes to infinity we have that the binomial distribution of the weight of the binary n -tuple

$$(X_i X_j)_{i+j=k \bmod n}$$

converges to the Poisson distribution of parameter ω^2 so that, for fixed $\omega = w/\sqrt{n}$,

$$\tilde{p}(n, w) = \Pr[z_k = 1] \xrightarrow{n \rightarrow \infty} e^{-\omega^2} \sum_{\ell \text{ odd}} \frac{\omega^{2\ell}}{\ell!} = e^{-\omega^2} \sinh \omega^2. \quad (21)$$

Let $\mathbf{x}, \mathbf{y}, \mathbf{r}_1, \mathbf{r}_2$ be independent random vectors whose coordinates are independently Bernoulli distributed with parameter p . Then the k -th coordinates of $\mathbf{x} \cdot \mathbf{r}_2$ and of $\mathbf{r}_1 \cdot \mathbf{y}$ are independent and Bernoulli distributed with parameter \tilde{p} . Therefore their modulo 2 sum $\mathbf{t} = \mathbf{x} \cdot \mathbf{r}_2 - \mathbf{r}_1 \cdot \mathbf{y}$ is Bernoulli distributed with

$$\begin{cases} \Pr[t_k = 1] = 2\tilde{p}(1 - \tilde{p}), \\ \Pr[t_k = 0] = (1 - \tilde{p})^2 + \tilde{p}^2. \end{cases} \quad (22)$$

Finally, by adding the final term ϵ to \mathbf{t} , we obtain the distribution of the coordinates of the error vector $\mathbf{e} = \mathbf{x} \cdot \mathbf{r}_2 - \mathbf{r}_1 \cdot \mathbf{y} + \epsilon$. Since the coordinates of ϵ are Bernoulli of parameter p and those of \mathbf{t} are Bernoulli distributed as (22) and independent from ϵ , we obtain :

Theorem 3. *Let $\mathbf{x}, \mathbf{y}, \mathbf{r}_1, \mathbf{r}_2 \sim \mathcal{B}(n, \frac{w}{n})$, $\epsilon \sim \mathcal{B}(n, \epsilon)$, and let $\mathbf{e} = \mathbf{x} \cdot \mathbf{r}_2 - \mathbf{r}_1 \cdot \mathbf{y} + \epsilon$. Then*

$$\begin{cases} \Pr[e_k = 1] = 2\tilde{p}(1 - \tilde{p})(1 - \frac{\epsilon}{n}) + ((1 - \tilde{p})^2 + \tilde{p}^2) \frac{\epsilon}{n}, \\ \Pr[e_k = 0] = ((1 - \tilde{p})^2 + \tilde{p}^2) (1 - \frac{\epsilon}{n}) + 2\tilde{p}(1 - \tilde{p}) \frac{\epsilon}{n}. \end{cases} \quad (23)$$

Theorem 3 gives us the probability that a coordinate of the error vector \mathbf{e} is 1. In our simulations to follow, which occur in the regime $p = \omega\sqrt{n}$ with constant ω , we make the simplifying assumption that the coordinates of \mathbf{e} are independent, meaning that the weight of \mathbf{e} follows a binomial distribution of parameter p^* , where p^* is defined as in Eq. (23): $p^* = p^*(n, w) = 2\tilde{p}(1 - \tilde{p})(1 - \frac{\epsilon}{n}) + ((1 - \tilde{p})^2 + \tilde{p}^2) \frac{\epsilon}{n}$. This approximation will give us, for $0 \leq d \leq \min(2w^2 + \epsilon, n)$,

$$\Pr[\omega(\mathbf{e}) = d] = \binom{n}{d} (p^*)^d (1 - p^*)^{(n-d)}. \quad (24)$$

In practice, the results obtained by simulation on the decryption failure are very coherent with this assumption.

VI. DECODING CODES WITH LOW RATES AND GOOD DECODING PROPERTIES

The previous Section allowed us to determine the distribution of the error vector \mathbf{e} in the configuration where a simple linear code is used. Now the decryption part corresponds to decoding the error described in the previous section. Any decodable code can be used at this point, depending on the considered application: clearly small dimension codes will allow better decoding, but at the cost of a lower encryption rate. The particular case that we consider corresponds typically to the case of key exchange or authentication, where only a small amount of data needs to be encrypted (typically 80, 128 or 256 bits,

a symmetric secret key size). We therefore need codes with low rates which are able to correct many errors. Again, a tradeoff is necessary between efficiently decodable codes but with a high decoding cost and less efficiently decodable codes but with a smaller decoding cost.

An example of such a family of codes with good decoding properties, meaning a simple decoding algorithm which can be analyzed, is given by Tensor Product Codes, which are used for biometry [BCC⁺07], where the same type of issue appears. More specifically, we will consider a special simple case of Tensor Product Codes (BCH codes and repetition codes), for which a precise analysis of the decryption failure can be obtained in the Hamming distance case.

A. Tensor Product Codes

Definition 14 (Tensor Product Code). *Let \mathcal{C}_1 (resp. \mathcal{C}_2) be a $[n_1, k_1, d_1]$ (resp. $[n_2, k_2, d_2]$) linear code over \mathbb{F} . The Tensor Product Code of \mathcal{C}_1 and \mathcal{C}_2 denoted $\mathcal{C}_1 \otimes \mathcal{C}_2$ is defined as the set of all $n_2 \times n_1$ matrices whose rows are codewords of \mathcal{C}_1 and whose columns are codewords of \mathcal{C}_2 .*

More formally, if \mathcal{C}_1 (resp. \mathcal{C}_2) is generated by \mathbf{G}_1 (resp. \mathbf{G}_2), then

$$\mathcal{C}_1 \otimes \mathcal{C}_2 = \left\{ \mathbf{G}_2^\top \mathbf{X} \mathbf{G}_1 \text{ for } \mathbf{X} \in \mathbb{F}^{k_2 \times k_1} \right\} \quad (25)$$

Remark 4. *Using the notation of the above Definition, the tensor product of two linear codes is a $[n_1 n_2, k_1 k_2, d_1 d_2]$ linear code.*

B. Specifying the Tensor Product Code

Even if tensor product codes seem well-suited for our purpose, an analysis similar to the one in Sec. V becomes much more complicated. Therefore, in order to provide strong guarantees on the decryption failure probability for our cryptosystem, we chose to restrict ourselves to a tensor product code $\mathcal{C} = \mathcal{C}_1 \otimes \mathcal{C}_2$, where \mathcal{C}_1 is a BCH(n_1, k, δ_1) code of length n_1 , dimension k , and correcting capability δ_1 (i.e. it can correct up to δ_1 errors), and \mathcal{C}_2 is the repetition code of length n_2 and dimension 1, denoted $\mathbb{1}_{n_2}$. (Notice that $\mathbb{1}_{n_2}$ can decode up to $\delta_2 = \lfloor \frac{n_2-1}{2} \rfloor$.) Subsequently, the analysis becomes possible and remains accurate but the negative counterpart is that there probably are some other tensor product codes achieving better efficiency (or smaller key sizes).

In the Hamming metric version of the cryptosystem we propose, a message $\boldsymbol{\mu} \in \mathbb{F}^k$ is first encoded into $\boldsymbol{\mu}_1 \in \mathbb{F}^{n_1}$ with a BCH($n_1, k_1 = k, \delta_1$) code, then each coordinate $\mu_{1,i}$ of $\boldsymbol{\mu}_1$ is re-encoded into $\tilde{\mu}_{1,i} \in \mathbb{F}^{n_2}$ with a repetition code $\mathbb{1}_{n_2}$. We denote $n = n_1 n_2$ the length of the tensor product code (its dimension is $k = k_1 \times 1$), and by $\tilde{\boldsymbol{\mu}}$ the resulting encoded vector, i.e. $\tilde{\boldsymbol{\mu}} = (\tilde{\mu}_{1,1}, \dots, \tilde{\mu}_{1,n_1}) \in \mathbb{F}^{n_1 n_2}$.

The efficient algorithm used for the repetition code is the majority decoding, *i.e.* more formally:

$$\mathbb{1}_{n_2}.\text{Decode}(\tilde{\boldsymbol{\mu}}_{1,j}) = \begin{cases} 1 & \text{if } \sum_{i=0}^{n_2-1} \tilde{\mu}_{1,j,i} \geq \lceil \frac{n_2+1}{2} \rceil, \\ 0 & \text{otherwise.} \end{cases} \quad (26)$$

Decryption Failure Probability. With a tensor product code $\mathcal{C} = \text{BCH}(n_1, k, \delta) \otimes \mathbb{1}_{n_2}$ as defined above, a decryption failure occurs whenever the decoding algorithm of the BCH code does not succeed in correcting errors that would have arisen after wrong decodings by the repetition code. Therefore, the analysis of the decryption failure probability is again split into three steps: evaluating the probability that the repetition code does not decode correctly, the conditional probability of a wrong decoding for the BCH code given an error weight and finally, the decryption failure probability using the law of total probability.

Step 1. We now focus on the probability that an error occurs while decoding the repetition code. As shown in Sec. V, the probability for a coordinate of $\mathbf{e} = \mathbf{x} \cdot \mathbf{r}_2 - \mathbf{r}_1 \cdot \mathbf{y} + \boldsymbol{\epsilon}$ to be 1 is $p^* = p^*(n_1 n_2, w, \epsilon)$ (see Eq. (23)). As mentioned above, $\mathbb{1}_{n_2}$ can decode up to $\delta_2 = \lfloor \frac{n_2-1}{2} \rfloor$ errors. Therefore, assuming that the error vector \mathbf{e} has weight γ (which occurs with the probability given in Eq. (24)), the probability of getting a decoding error on a single block of the repetition code $\mathbb{1}_{n_2}$ is hence given by:

$$\bar{p}_\gamma = \bar{p}_\gamma(n_1, n_2) = \sum_{i=\lfloor \frac{n_2-1}{2} \rfloor + 1}^{n_2} \binom{n_2}{i} \left(\frac{\gamma}{n_1 n_2} \right)^i \left(1 - \frac{\gamma}{n_1 n_2} \right)^{n_2-i}. \quad (27)$$

Step 2. We now focus on the $\text{BCH}(n_1, k, \delta_1)$ code, and recall that it can correct up to δ_1 errors. Now the probability \mathcal{P} that the $\text{BCH}(n_1, k, \delta_1)$ code fails to decode correctly the encoded message $\boldsymbol{\mu}_1$ back to $\boldsymbol{\mu}$ is given by the probability that an error occurred on at least $\delta_1 + 1$ blocks of the repetition code. Therefore, we have

$$\mathcal{P} = \mathcal{P}(\delta_1, n_1, n_2, \gamma) = \sum_{i=\delta_1+1}^{n_1} \binom{n_1}{i} (\bar{p}_\gamma)^i (1 - \bar{p}_\gamma)^{n_1-i}. \quad (28)$$

Step 3. Finally, using the law of total probability, we have that the decryption failure probability is given by the sum, over all the possible weights, of the probability that the error has this specific weight times the probability of a decoding error for this weight. This is captured in the following theorem, whose proof is a straightforward consequence of the formulae of Sec. V and VI-A.

Theorem 5. Let $\mathcal{C} = \text{BCH}(n_1, k, \delta) \otimes \mathbb{1}_{n_2}$, $(pk, sk) \leftarrow \text{KeyGen}$, $\boldsymbol{\mu} \stackrel{\$}{\leftarrow} \mathbb{F}_2^k$, and some randomness $\theta \in \{0, 1\}^*$, then with the notations above, the decryption failure probability is

$$p_{\text{fail}} = \Pr[\text{Decrypt}(\text{sk}, \text{Encrypt}(\text{pk}, \boldsymbol{\mu}, \theta)) \neq \boldsymbol{\mu}.] \quad (29)$$

$$= \sum_{\gamma=0}^{\min(2w^2+\epsilon, n_1 n_2)} \Pr[\omega(\mathbf{e}) = \gamma] \cdot \mathcal{P}(\delta_1, n_1, n_2, \gamma) \quad (30)$$

VII. PARAMETERS

A. HQC Instantiation for Hamming Metric

In this Section, we describe our new cryptosystem in the Hamming metric setting. As mentioned in the previous Section, we use a tensor product code (Def. 14) $\mathcal{C} = \text{BCH}(n_1, k, \delta) \otimes \mathbb{1}_{n_2}$. A message $\boldsymbol{\mu} \in \mathbb{F}^k$ is encoded into $\boldsymbol{\mu}_1 \in \mathbb{F}^{n_1}$ with the BCH code, then each coordinate $\mu_{1,i}$ of $\boldsymbol{\mu}_1$ is encoded into $\tilde{\mu}_{1,i} \in \mathbb{F}^{n_2}$ with $\mathbb{1}_{n_2}$. To match the description of our cryptosystem in Sec. III-B, we have $\boldsymbol{\mu}\mathbf{G} = \tilde{\boldsymbol{\mu}} = (\tilde{\mu}_{1,1}, \dots, \tilde{\mu}_{1,n_1}) \in \mathbb{F}^{n_1 n_2}$. To obtain the ciphertext, $\mathbf{r} = (\mathbf{r}_1, \mathbf{r}_2) \stackrel{\$}{\leftarrow} \mathcal{V}^2$ and $\boldsymbol{\epsilon} \stackrel{\$}{\leftarrow} \mathcal{V}$ are generated and the encryption of $\boldsymbol{\mu}$ is $\mathbf{c} = (\mathbf{r}\mathbf{Q}^\top, \boldsymbol{\rho} = \boldsymbol{\mu}\mathbf{G} + \mathbf{s} \cdot \mathbf{r}_2 + \boldsymbol{\epsilon})$.

Parameters for Our Scheme. We provide two sets of parameters: the first one in Tab. I targets different pre-quantum security levels while the second one in Tab. II is quantum-safe. For each parameter set, the parameters are chosen so that the minimal workfactor of the best known attack exceeds the security parameter. For classical attacks, best known attacks include the works from [CC98, BLP08, FS09, BJMM12] and for quantum attacks, the work of [Ber10]. We consider $w = \mathcal{O}(\sqrt{n})$ and follow the complexity described in [CS16].

Note that our cryptosystem is quite efficient since the decryption simply involves a decoding of a repetition code and a small length BCH code.

Specific structural attacks. Quasi-cyclic codes have a special structure which may potentially open the door to specific structural attacks. Such attacks have been studied in [GJL15, LJK+16, Sen11], these attacks are especially efficient in the case when the polynomial $x^n - 1$ has many small factors. These attacks become inefficient as soon as $x^n - 1$ has only two factors of the form $(x - 1)$ and $x^{n-1} + x^{n-2} + \dots + x + 1$, which is the case when n is primitif in \mathbb{F}_q , for $q = 2$ it corresponds to cases when 2 generates $(\mathbb{Z}/n\mathbb{Z})^*$, such numbers are known up to very large values. We consider such n for our parameters. In Tab. I and II, n_1 denotes the length of the BCH code, n_2 the length of the repetition code $\mathbb{1}$ so that the length of the tensor product code \mathcal{C} is $n = n_1 n_2$ (actually the smallest primitive prime greater than $n_1 n_2$). k is the dimension of the BCH code and hence also the dimension of \mathcal{C} . δ is the decoding capability of the BCH code, *i.e.* the maximum number of errors that the BCH can decode. w

Cryptosystem Parameters									
Instance	n_1	n_2	$n_1 n_2 = n$	k	δ	w	$\epsilon = 3w$	security	p_{fail}
Toy	255	25	6,379	63	30	36	108	64	$< 2^{-64}$
Low	255	37	9,437	79	27	45	135	80	$< 2^{-80}$
Medium	255	53	13,523	99	23	56	168	100	$< 2^{-100}$
Strong	511	41	20,959	121	58	72	216	128	$< 2^{-128}$

Table I

PARAMETER SETS FOR OUR CRYPTOSYSTEM IN HAMMING METRIC. THE TENSOR PRODUCT CODE USED IS $\mathcal{C} = \text{BCH}(n_1, k, \delta) \otimes \mathbb{1}_{n_2}$. THE PARAMETERS FOR THE BCH CODES WERE TAKEN FROM [PW72]. SECURITY IN THE FIRST FOUR INSTANCES IS GIVEN IN BITS, IN THE CLASSICAL MODEL OF COMPUTING. IN THE LAST FOUR INSTANCES, THE SECURITY LEVEL IS THE EQUIVALENT OF THE CLASSICAL SECURITY LEVEL BUT IN THE QUANTUM COMPUTING MODEL, FOLLOWING THE WORK OF [BER10]. THE PUBLIC KEY SIZE, CONSISTING OF $(\mathbf{q}_r, \mathbf{x} + \mathbf{q}_r \cdot \mathbf{y})$, HAS SIZE $2n$ (IN BITS) (ALTHOUGH CONSIDERING A SEED FOR \mathbf{q}_r , THE SIZE CAN BE REDUCED TO n PLUS THE SIZE OF THE SEED), AND THE SECRET KEY (CONSISTING OF \mathbf{x} AND \mathbf{y} BOTH OF WEIGHT w) HAS SIZE $2w \lceil \log_2(n) \rceil$ (BITS) - WHICH AGAIN CAN BE REDUCED TO THE SIZE OF A SEED. FINALLY, THE SIZE OF THE ENCRYPTED MESSAGE IS $2n$.

Cryptosystem Parameters									
Instance	n_1	n_2	$n_1 n_2 = n$	k	δ	w	$\epsilon = 3w$	security	p_{fail}
Toy	255	65	16,603	63	87	72	216	64	$< 2^{-64}$
Low	511	47	24,019	76	85	89	267	80	$< 2^{-80}$
Medium	255	141	35,963	99	23	112	336	100	$< 2^{-100}$
Strong	511	109	55,711	121	58	143	429	128	$< 2^{-128}$

Table II

PARAMETERS FOR QUANTUM-SAFE HQC. ALL PARAMETERS ARE SIMILAR TO TAB. I.

is the weight of the n -dimensional vectors \mathbf{x} , \mathbf{y} , \mathbf{r}_1 , and \mathbf{r}_2 and similarly $\epsilon = \omega(\epsilon) = 3 \times w$ for our cryptosystem.

Computational Cost. The most expensive part of the encryption and decryption is the matrix vector product, in practice the complexity is hence $\mathcal{O}(n^{\frac{3}{2}})$ (for $w = \mathcal{O}(\sqrt{n})$). Asymptotically the cost becomes linear in n .

Notice that it would be possible to consider other types of decodable codes in order to increase the encryption rate to 1/4 (say), but at the cost of an increase of the length of the code, for instance using

LDPC (3,6) codes would increase the rate, but multiply the length by a factor of roughly three.

B. RQC Instantiation for Rank Metric

Error distribution and decoding algorithm: no decryption failure. The case of the rank metric is much more simpler than for Hamming metric. Indeed in that case the decryption algorithm of our cryptosystem asks to decode an error $\mathbf{e} = \mathbf{x} \cdot \mathbf{r}_2 - \mathbf{r}_1 \cdot \mathbf{y} + \epsilon$ where the words (\mathbf{x}, \mathbf{y}) and $(\mathbf{r}_1, \mathbf{r}_2)$ have rank weight w . At the difference of Hamming metric the rank weight of the vector $\mathbf{x} \cdot \mathbf{r}_2 - \mathbf{r}_1 \cdot \mathbf{y}$ is almost always w^2 and is in any case bounded above by w^2 . In particular with a strong probability the rank weight of $\mathbf{x} \cdot \mathbf{r}_2 - \mathbf{r}_1 \cdot \mathbf{y}$ is the same than the rank weight of $\mathbf{x} \cdot \mathbf{r}_2$ since \mathbf{x} and \mathbf{y} share the same rank support, so as \mathbf{r}_1 and \mathbf{r}_2 . Hence for decoding, we consider Gabidulin $[n, k]$ codes over \mathbb{F}_{q^n} , which can decode $\frac{n-k}{2}$ rank errors and choose our parameters such that $w^2 + \epsilon \leq \frac{n-k}{2}$, so that, unlike the Hamming metric case, there is no decryption failure.

Parameters for Our Scheme. In Tab. III and IV, n denotes the length of the Rank metric code, k its dimension, q is the number of elements in the base field \mathbb{F}_q , and m is the degree of the extension. Similarly to the Hamming instantiation, w is the rank weight of vectors \mathbf{x} , \mathbf{y} , \mathbf{r}_1 , and \mathbf{r}_2 , and ϵ the rank weight of ϵ .

Specific structural attacks. Specific attacks were described in [HT15, GRSZ14] for LRPC cyclic codes. These attack use the fact that the targeted code has a generator matrix formed from shifted low weight codewords and in the case of [HT15], also uses multi-factor factorization of $x^n - 1$. These attack corresponds to searching for low weight codewords of a given code of rate 1/2. In the present case the attacker has to search for a low weight word associated to a non null syndrome, such that previous attacks imply considering a code with a larger dimension so that in practice these attacks do no improve on direct attacks on the syndrome. Meanwhile in practice by default, we choose n a primitive prime number, such that the polynomial $x^n - 1$ has no factor of degree less than $\frac{n-1}{2}$ except $x - 1$. The best attacks consists in decoding a random double-circulant $[2n, n]$ over \mathbb{F}_{q^m} for rank weight ω .

Examples of parameters are given in Tab. III according to best known attacks (combinatorial attacks in practice) described in Sec. II-D. Quantum-safe parameters for RQC are given in Tab. IV. For the case of rank metric, we always consider $n' = n = m$.

Remark. The system is based on cyclic codes, which means considering polynomials modulo $x^n - 1$, interestingly enough, and only in the case of the rank metric, the construction remains valid when considering not only polynomials modulo $x^n - 1$ but also modulo a polynomial with coefficient in the

Cryptosystem Parameters									
Instance	n	k	m	q	w	ϵ	plaintext	key size	security
RQC-I	53	13	53	2	4	4	689	2,809	95
RQC-II	61	3	61	2	5	4	183	3,721	140
RQC-III	83	3	83	2	6	4	249	6,889	230

Table III

PARAMETER SETS FOR RQC: OUR CRYPTOSYSTEM IN RANK METRIC. THE PLAINTEXTS, KEY SIZES, AND SECURITY ARE EXPRESSED IN BITS.

Cryptosystem Parameters									
Instance	n	k	m	q	w	ϵ	plaintext	key size	security
RQC-I	61	3	61	2	5	4	183	3,721	70
RQC-II	83	3	83	2	6	4	249	6,889	115
RQC-III	61	3	61	4	5	4	366	7,442	132
RQC-IV	89	5	89	3	6	6	705	12,555	192

Table IV

PARAMETER SETS FOR QUANTUM-SAFE RQC, WITH RESPECT TO [GHT16]. PARAMETERS ARE ANALOG TO TAB. III.

base field $GF(q)$. Indeed in that case the modulo does not change the rank weight of a codeword. Such a variation on the scheme may be interesting to avoid potential structural attacks which may use the factorization of the quotient polynomial for the considered polynomial ring.

Computational Cost. The encryption cost corresponds to a matrix-vector product over \mathbb{F}_{q^m} , for a multiplication cost of elements of \mathbb{F}_{q^m} in $m \log(m) \log(\log(m))$, we obtain an encryption complexity in $\mathcal{O}(n^2 m \log(m) \log(\log(m)))$. The decryption cost is also a matrix-vector multiplication plus the decoding cost of the Gabidulin codes, both have the complexities in $\mathcal{O}(n^2 m \log(m) \log(\log(m)))$.

C. Comparison with Other Code-based Cryptosystems

In the following we consider the different types of code-based cryptosystems and express different parameters of the different systems in terms of the security parameters λ , considering best known attacks of complexity $2^{\mathcal{O}(w)}$ for decoding a word of weight w for Hamming distance and complexity in $2^{\mathcal{O}(wn)}$ for decoding a word of rank weight w for a code of double-circulant code of length $2n$ for rank metric.

Cryptosystem		Code Length	Public Key Size	Ciphertext Size	Hidden Structure	Cyclic Structure
Goppa-McEliece	[McE78]	$\mathcal{O}(\lambda \log \lambda)$	$\mathcal{O}(\lambda^2 (\log \lambda)^2)$	$\mathcal{O}(\lambda \log \lambda)$	Strong	No
MDPC	[MTSB13]	$\mathcal{O}(\lambda^2)$	$\mathcal{O}(\lambda^2)$	$\mathcal{O}(\lambda^2)$	Weak	Yes
LRPC	[GMRZ13]	$\mathcal{O}(\lambda^{\frac{2}{3}})$	$\mathcal{O}(\lambda^{\frac{4}{3}})$	$\mathcal{O}(\lambda^{\frac{4}{3}})$	Weak	Yes
HQC	[Sec. VII-A]	$\mathcal{O}(\lambda^2)$	$\mathcal{O}(\lambda^2)$	$\mathcal{O}(\lambda^2)$	No	Yes
RQC	[Sec. VII-B]	$\mathcal{O}(\lambda^{\frac{2}{3}})$	$\mathcal{O}(\lambda^{\frac{4}{3}})$	$\mathcal{O}(\lambda^{\frac{4}{3}})$	No	Yes

Table V

PARAMETERS COMPARISON FOR DIFFERENT CODE-BASED CRYPTOSYSTEMS WITH RESPECT TO THE SECURITY PARAMETER

λ

McEliece-Goppa corresponds to the original scheme proposed by McEliece [McE78] of dimension rate $\frac{1}{2}$.

Tab. V shows that even if the recent cryptosystem MDPC has a smaller public key and a weaker hidden structure than the McEliece cryptosystem, the size of the ciphertext remains non negligible. The HQC benefits from the same type of parameters than the MDPC systems but with no hidden structure at the cost of a smaller encryption rate. Finally, the table shows the very strong potential of rank metric based cryptosystems, whose parameters remain rather low compared to MDPC and HQC cryptosystems.

VIII. CONCLUSION AND FUTURE WORK

We have presented an efficient approach for constructing code-based cryptosystems. This approach originates in Alekhovich's blueprint [Ale03] on random matrices. Our construction is generic enough so that we provide two instantiations of our cryptosystem: one for the Hamming metric (HQC), and one for the Rank metric (RQC). Both constructions are pretty efficient and compare favourably to previous work, especially for the rank metric setting. Additionally, we provide for the Hamming setting an analysis of the error term yielding a concrete, precise and easy-to-verify decryption failure.

This analysis was facilitated by the shape of the tensor product code, and more complex-to-analyze tensor product codes might yield slightly shorter keys and better efficiency.

However, for such a tensor product code the analysis of the decryption failure probability becomes much more tricky, and finding suitable upper bounds for it will involve future work.

REFERENCES

- [AD97] Miklós Ajtai and Cynthia Dwork. A public-key cryptosystem with worst-case/average-case equivalence. In *FOCS* 1997.
- [AIK07] Benny Applebaum, Yuval Ishai, and Eyal Kushilevitz. Cryptography with constant input locality. In Alfred Menezes, editor, *CRYPTO 2007*, volume 4622 of *LNCS*, pages 92–110. Springer, Heidelberg, August 2007.
- [Ale03] Michael Alekhnovich. More on average case vs approximation complexity. In *44th FOCS*, pages 298–307. IEEE Computer Society Press, October 2003.
- [BCC⁺07] Julien Bringer, Hervé Chabanne, Gérard Cohen, Bruno Kindarji, and Gilles Zémor. Optimal iris fuzzy sketches. In *Biometrics: Theory, Applications, and Systems, 2007. BTAS 2007. First IEEE International Conference on*, pages 1–6. IEEE, 2007.
- [BCGO09] Thierry P. Berger, Pierre-Louis Cayrel, Philippe Gaborit, and Ayoub Otmani. Reducing key length of the McEliece cryptosystem. In Bart Preneel, editor, *AFRICACRYPT 09*, volume 5580 of *LNCS*, pages 77–97. Springer, Heidelberg, June 2009.
- [Ber10] Daniel J Bernstein. Grover vs. mceliece. In *Post-Quantum Cryptography*, pages 73–80. Springer, 2010.
- [BJMM12] Anja Becker, Antoine Joux, Alexander May, and Alexander Meurer. Decoding random binary linear codes in $2^{n/20}$: How $1 + 1 = 0$ improves information set decoding. In David Pointcheval and Thomas Johansson, editors, *EUROCRYPT 2012*, volume 7237 of *LNCS*, pages 520–536. Springer, Heidelberg, April 2012.
- [BS⁺16] Eli Ben-Sasson, Iddo Bentov, Ivan Damgård, Yuval Ishai, and Noga Ron-Zewi. On Public Key Encryption from Noisy Codewords. In *Public Key Cryptography* pages 417-446. 2016.
- [BLP08] Daniel J Bernstein, Tanja Lange, and Christiane Peters. Attacking and defending the mceliece cryptosystem. In *Post-Quantum Cryptography*, pages 31–46. Springer, 2008.
- [BMvT78] Elwyn R Berlekamp, Robert J McEliece, and Henk CA van Tilborg. On the inherent intractability of certain coding problems. *IEEE Transactions on Information Theory*, 24(3):384–386, 1978.
- [CC98] Anne Canteaut and Florent Chabaud. A new algorithm for finding minimum weight words in a linear code: application to mceliece cryptosystem and to narrow-sense bch codes of length 511. *IEEE Transactions on Information Theory*, 44(1):367–378, 1998.
- [CS16] Rodolfo Canto Torres and Nicolas Sendrier. Analysis of information set decoding for a sub-linear error weight. In Takagi [Tak16], pages 144–161.
- [DP12] Ivan Damgård and Sunoo Park. Is public-key encryption based on lpn practical? *IACR Cryptology ePrint Archive*, 2012:699, 2012.
- [DV13] Alexandre Duc and Serge Vaudenay. Helen: a public-key cryptosystem based on the lpn and the decisional minimal distance problems. In *International Conference on Cryptology in Africa*, pages 107–126. Springer, 2013.
- [FdVP08] Jean-Charles Faugère, Françoise Levy dit Vehel, and Ludovic Perret. Cryptanalysis of minrank. In David Wagner, editor, *CRYPTO 2008*, volume 5157 of *LNCS*, pages 280–296. Springer, Heidelberg, August 2008.
- [FOPT10] Jean-Charles Faugère, Ayoub Otmani, Ludovic Perret, and Jean-Pierre Tillich. Algebraic cryptanalysis of McEliece variants with compact keys. In Gilbert [Gil10], pages 279–298.
- [FS09] Matthieu Finiasz and Nicolas Sendrier. Security bounds for the design of code-based cryptosystems. In Mitsuru Matsui, editor, *ASIACRYPT 2009*, volume 5912 of *LNCS*, pages 88–105. Springer, Heidelberg, December 2009.
- [Gab85] Ernest Mukhamedovich Gabidulin. Theory of codes with maximum rank distance. *Problemy Peredachi Informatsii*, 21(1):3–16, 1985.

- [Gab05] Philippe Gaborit. Shorter keys for code based cryptography. In *Proceedings of the 2005 International Workshop on Coding and Cryptography (WCC 2005)*, pages 81–91, 2005.
- [GG07] Philippe Gaborit and Marc Girault. Lightweight code-based identification and signature. In *2007 IEEE International Symposium on Information Theory*, pages 191–195. IEEE, 2007.
- [GHT16] Philippe Gaborit, Adrien Hauteville, and Jean-Pierre Tillich. Ranksynd a PRNG based on rank metric. In Takagi [Tak16], pages 18–28.
- [Gil10] Henri Gilbert, editor. *EUROCRYPT 2010*, volume 6110 of *LNCS*. Springer, Heidelberg, May 2010.
- [GM84] Shafi Goldwasser and Silvio Micali. Probabilistic encryption. *Journal of Computer and System Sciences*, 28(2):270–299, 1984.
- [GMRZ13] Philippe Gaborit, Gaétan Murat, Olivier Ruatta, and Gilles Zémor. Low rank parity check codes and their application to cryptography. In *Proceedings of the Workshop on Coding and Cryptography WCC'2013*, Bergen, Norway, 2013. Available on www.selmer.uib.no/WCC2013/pdfs/Gaborit.pdf.
- [GPT91] Ernst M. Gabidulin, A. V. Paramonov, and O. V. Tretjakov. Ideals over a non-commutative ring and thier applications in cryptology. In Donald W. Davies, editor, *EUROCRYPT'91*, volume 547 of *LNCS*, pages 482–489. Springer, Heidelberg, April 1991.
- [GRS16] Philippe Gaborit, Olivier Ruatta, and Julien Schrek. On the complexity of the rank syndrome decoding problem. *IEEE Transactions on Information Theory*, 62(2):1006–1019, 2016.
- [GRSZ14] Philippe Gaborit, Olivier Ruatta, Julien Schrek, and Gilles Zémor. New results for rank-based cryptography. In David Pointcheval and Damien Vergnaud, editors, *AFRICACRYPT 14*, volume 8469 of *LNCS*, pages 1–12. Springer, Heidelberg, May 2014.
- [GZ16] Philippe Gaborit and Gilles Zémor. On the hardness of the decoding and the minimum distance problems for rank codes. *IEEE Trans. Information Theory* 62(12): 7245-7252 (2016).
- [GJL15] Qian Guo and Thomas Johansson and Carl Löndahl, A New Algorithm for Solving Ring-LPN With a Reducible Polynomial, In *IEEE Trans. Information Theory*, vol. 61,(11), pp. 6204–6212, (2015)
- [HKL⁺12] Stefan Heyse, Eike Kiltz, Vadim Lyubashevsky, Christof Paar, and Krzysztof Pietrzak. Lapin: An efficient authentication protocol based on ring-lpn. In *Fast Software Encryption*, pages 346–365. Springer, 2012.
- [HPS98] Jeffrey Hoffstein, Jill Pipher, and Joseph H. Silverman. NTRU: A ring-based public key cryptosystem. In Joe Buhler, editor, *Algorithmic Number Theory, Third International Symposium, ANTS-III, Portland, Oregon, USA, June 21-25, 1998, Proceedings*, volume 1423, pages 267–288. Springer, 1998.
- [HT15] Adrien Hauteville and Jean-Pierre Tillich. New algorithms for decoding in the rank metric and an attack on the lrpc cryptosystem. In *2015 IEEE International Symposium on Information Theory (ISIT)*, pages 2747–2751. IEEE, 2015.
- [LJK+16] Carl Löndahl and Thomas Johansson and Masoumeh Koochak Shooshtari and Mahmoud Ahmadian-Attari and Mohammad Reza Aref, Squaring attacks on McEliece public-key cryptosystems using quasi-cyclic codes of even dimension. In *Des. Codes Cryptography*, Vol. 80, pp. 359–377,2016.
- [KMP14] Eike Kiltz, Daniel Masny, and Krzysztof Pietrzak. Simple chosen-ciphertext security from low-noise LPN. In Hugo Krawczyk, editor, *PKC 2014*, volume 8383 of *LNCS*, pages 1–18. Springer, Heidelberg, March 2014.
- [LdVP06] Françoise Levy-dit Vehel and L Perret. Algebraic decoding of rank metric codes. *Proceedings of YACC*, 2006.
- [Loi06] Pierre Loidreau. Properties of codes in rank metric. *arXiv preprint cs/0610057*, 2006.
- [LPR10] Vadim Lyubashevsky, Chris Peikert, and Oded Regev. On ideal lattices and learning with errors over rings. In Gilbert [Gil10], pages 1–23.

- [MB09] Rafael Misoczki and Paulo S. L. M. Barreto. Compact McEliece keys from goppa codes. In Michael J. Jacobson Jr., Vincent Rijmen, and Reihaneh Safavi-Naini, editors, *SAC 2009*, volume 5867 of *LNCS*, pages 376–392. Springer, Heidelberg, August 2009.
- [McE78] Robert J McEliece. A public-key cryptosystem based on algebraic. *Coding Thv*, 4244:114–116, 1978.
- [MTSB13] Rafael Misoczki, Jean-Pierre Tillich, Nicolas Sendrier, and Paulo SLM Barreto. Mdpc-mceliece: New mceliece variants from moderate density parity-check codes. In *Information Theory Proceedings (ISIT), 2013 IEEE International Symposium on*, pages 2069–2073. IEEE, 2013.
- [Ove07] Raphael Overbeck. *Public key cryptography based on coding theory*. PhD thesis, TU Darmstadt, 2007.
- [PW72] William Wesley Peterson and Edward J Weldon. *Error-correcting codes*. MIT press, 1972.
- [Reg03] Oded Regev. New lattice based cryptographic constructions. In *35th ACM STOC*, pages 407–416. ACM Press, June 2003.
- [RS60] Irving S Reed and Gustave Solomon. Polynomial codes over certain finite fields. *Journal of the society for industrial and applied mathematics*, 8(2):300–304, 1960.
- [Sen11] Nicolas Sendrier. Decoding one out of many. In *International Workshop on Post-Quantum Cryptography*, pages 51–67. Springer, 2011.
- [SKK10] Danilo Silva, Frank R Kschischang, and Ralf Kotter. Communication over finite-field matrix channels. *IEEE Transactions on Information Theory*, 56(3):1296–1305, 2010.
- [Tak16] Tsuyoshi Takagi, editor. *Post-Quantum Cryptography - 7th International Workshop, PQCrypto 2016, Fukuoka, Japan, February 24-26, 2016, Proceedings*, volume 9606 of *Lecture Notes in Computer Science*. Springer, 2016.