A New Algebraic Approach to the Regular Syndrome Decoding Problem and Implications for PCG Constructions

Pierre Briaud, Morten Øygarden

▶ **To cite this version:**

Pierre Briaud, Morten Øygarden. A New Algebraic Approach to the Regular Syndrome Decoding Problem and Implications for PCG Constructions. Eurocrypt 2023 - 42nd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Apr 2023, Lyon, France. pp.391–422, 10.1007/978-3-031-30589-4_14 . hal-03984470

HAL Id: hal-03984470
https://hal.science/hal-03984470

Submitted on 12 Feb 2023

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Distributed under a Creative Commons Attribution 4.0 International License

A New Algebraic Approach to the Regular Syndrome Decoding Problem and Implications for PCG Constructions

Pierre Briaud[1,2] and Morten Øygarden[3]

[1] Sorbonne Universités, UPMC Univ Paris 06
[2] Inria, Team COSMIQ, Paris, France
pierre.briaud@inria.fr
[3] Simula UiB, Norway
morten.oygarden@simula.no

Abstract. The Regular Syndrome Decoding (RSD) problem, a variant of the Syndrome Decoding problem with a particular error distribution, was introduced almost 20 years ago by Augot *et al.*. In this problem, the error vector is divided into equally sized blocks, each containing a single noisy coordinate. More recently, the last five years have seen increased interest in this assumption due to its use in MPC and ZK applications. Generally referred to as "LPN with regular noise" in this context, the assumption allows to achieve better efficiency when compared to plain LPN. In all previous works of cryptanalysis, it has not been shown how to exploit the special feature of this problem in an attack.
We present the first algebraic attack on RSD. Based on a careful theoretical analysis of the underlying polynomial system, we propose concrete attacks that are able to take advantage of the regular noise distribution. In particular, we can identify several examples of concrete parameters where our techniques outperform other algorithms.

1 Introduction

The Regular Syndrome Decoding (RSD) problem is a variant of the well-known Syndrome Decoding (SD) problem, which is the standard assumption in code-based cryptography.

Definition 1 (Computational Syndrome Decoding (SD)). *Let $(n, k, h) \in \mathbb{N}^3$ with $k \leq n$ and $h \leq n$. Sample $\boldsymbol{H} \leftarrow \mathbb{F}^{(n-k)\times n}$ a full-rank matrix over a finite field $\mathbb{F}$ and $\boldsymbol{e} \leftarrow \mathbb{F}^n$ such that $\boldsymbol{e}$ is of Hamming weight $|\boldsymbol{e}| = h$. Given $(\boldsymbol{H}, \boldsymbol{s}^\mathsf{T} := \boldsymbol{H}\boldsymbol{e}^\mathsf{T})$, the goal is to recover the error vector $\boldsymbol{e}$.*

In the following, we will denote by $R := k/n$ (resp. $\rho := h/n$) the rate of the associated linear code (resp. error rate). RSD was introduced by Augot, Finiasz and Sendrier [6] as the underlying assumption for the Fast Syndrome-Based hash function. The only difference with SD lies in the choice of a particular error distribution:

Definition 2 (Computational Regular Syndrome Decoding (RSD)). *Let* $(h, k, \beta) \in \mathbb{N}^3$ *and* $n = h\beta$. *Sample* $\boldsymbol{H} \leftarrow \mathbb{F}^{(n-k)\times n}$ *a full-rank matrix over a finite field* $\mathbb{F}$ *and* $\boldsymbol{e} := (\boldsymbol{e}_1||\ldots||\boldsymbol{e}_h) \leftarrow \mathbb{F}^n$ *such that* $\boldsymbol{e}_i \in \mathbb{F}^\beta$ *is of Hamming weight* $|\boldsymbol{e}_i| = 1$ *for* $1 \leq i \leq h$. *Given* $(\boldsymbol{H}, \boldsymbol{s}^\mathsf{T} := \boldsymbol{H}\boldsymbol{e}^\mathsf{T})$, *recover the error* $\boldsymbol{e}$.

More recently, this problem has gained a renewed interest since its introduction in secure computation. Its first use in this context is due to Hazai, Orsini, Scholl and Soria-Vazques in their *TinyKeys* approach to design MPC-protocols with improved efficiency [31]. Later, Boyle *et al.* suggested to rely on this assumption to build efficient Pseudo Random Correlation Generators (PCGs). These primitives enable the generation of long sources of correlated randomness for more advanced MPC and ZK applications [18]. This latter idea has been further considered in a series of works [19,20,44,42], where RSD is often referred to as "LPN with regular noise".

LPN-based cryptography. In these more recent constructions, the LPN problem is instantiated either with the *primal* or the *dual* formulation. The search version of dual LPN is the computational SD problem stated in Definition 1 while primal LPN is the standard decoding problem for linear codes. Even though these formulations are clearly equivalent in theory, choosing one instead of the other has an impact in terms of efficiency. This can be seen when trying to design a simple PRG relying on LPN. Given a seed $(\boldsymbol{m}, \boldsymbol{e}) \in \mathbb{F}^k \times \mathbb{F}^n$ and a public matrix $\boldsymbol{G} \in \mathbb{F}^{k\times n}$ with $|\boldsymbol{e}| = h$, the output of the naive primal LPN-based PRG is $\boldsymbol{m}\boldsymbol{G} + \boldsymbol{e} \in \mathbb{F}^n$. In particular, it is generally acknowledged by the community that this construction can only achieve quadratic stretch [18, Section 1.2 page 4][11, Section 2.5 page 9]. This is due to the fact that the length n cannot be chosen too large compared to k and h, otherwise there will be k error-free positions with non-negligible probability. On the contrary, the dual construction $\boldsymbol{e} \mapsto \boldsymbol{e}\boldsymbol{H}^\mathsf{T} \in \mathbb{F}^{n-k}$ whose seed is just the low weight vector $\boldsymbol{e}$ does not exhibit the same constraint. By fixing the weight and increasing n, one can indeed get an output size mostly independent of the seed size. Other advantages of the dual formulation is that the product $\boldsymbol{e}\boldsymbol{H}^\mathsf{T}$ is cheap to compute and the matrix $\boldsymbol{H}$ can be seen as a compression mapping $\mathbb{F}^n \to \mathbb{F}^{n-k}$. This may represent a useful property for practical applications.

To improve computational efficiency without affecting security, it was proposed to choose d-local codes in the primal formulation, *i.e.,* matrices $\boldsymbol{G}$ such that the Hamming weight of each column is a small integer d [4]. Such codes are not suitable in the dual construction, see for instance [18,11]. Therefore, other code families such as quasi-cyclic codes [1] or MDPC codes [37] have be chosen in this case. More importantly for us, and for the same purpose of efficiency, various constructions have adopted a regular distribution for $\boldsymbol{e}$ [19,20,44,18,42].

Parameter range. LPN instances used in the context of [19,20,44,18,42] typically have a higher size for the secret k, as well as a lower noise, than parameters encountered in code-based cryptography. Echoing the above remark on primal

and dual LPN, the few proposed parameter sets may be divided into two categories depending on the application:

- instances used in the primal formulation have a rather small code rate R (non-constant) and noise rate ρ slightly larger than $\mathcal{O}(n^{-1/2})$.
- instances used in the dual formulation have constant code rate (often $1/2$ or $3/4$) and a weight h mostly independent from n.

Finally, the standard LPN problem is usually stated over the binary field $\mathbb{F}_2$, but some constructions require an LPN assumption over a larger field $\mathbb{F}$ of size typically $|\mathbb{F}| \geq 256$, for example [19,18,42], or even over more general integer rings [10,11] or polynomial rings [21].

Exploiting the regular distribution. A first security analysis of this type of LPN instances (over $\mathbb{F}_{2^{128}}$) was performed by Boyle et al. in [18, §5.1]. Later constructions also use it as a black box to derive their parameters [44,42]. In this particular regime, the best attacks are the folklore Gaussian attack and the Pooled Gauss variant [27], ISD algorithms [39,28,14,35,12,36] which may all be seen as refinements of the original Prange algorithm [38] and finally Statistical Decoding [32,23]. More recently, [34] studied the assumption for the same parameter range, but in a more general setting (larger fields or integer rings, not only Bernoulli distribution). Notably, they claim that some of the estimates of [18] are too conservative over large fields: ISD algorithms are still the best attack in this case, but the advantage of advanced ISD variants compared to Pooled Gauss (*e.g.*, Prange) quickly deteriorates when $|\mathbb{F}|$ increases. Finally, they show that the cost of Statistical Decoding is much higher than claimed in [18]. In particular, this is no longer the best attack even by taking into account the most recent development of [23] since the latter does not seem to perform well in this regime.

We remark that the use of a regular distribution is not seen as a clear weakness by the community [31,18,19,42,44,34], meaning that RSD is not believed to be particularly easier than SD in this PCG-relevant parameter zone. Thus, regular LPN instances are treated as random LPN instances to derive parameters. The only extensive survey about the cryptanalysis of RSD in all weight regimes was given in [31, Appendix B]. They conclude that ISD algorithms are the best attack on both SD and RSD when there is a unique solution. They also try to adapt the ISD algorithms to the regular structure [31, Appendix B.3] but the improvement does not seem apparent[4]. Finally, we have not found similar attempts to enhance LPN or SD attacks by exploiting the regular distribution and there does not seem to be any RSD-specific attack described in the literature.

Contribution. In this paper, we show that the regular noise distribution used in LPN may indeed be exploited by an attacker by presenting a new algebraic

[4] "ISD is always the most efficient attack and has roughly the same cost when considering SD and RSD" [31, p. 49]

attack on the Regular Syndrome Decoding Problem. Contrary to known attacks, it is not an adaptation of SD techniques to solve RSD as it crucially benefits from the regular structure. It also differs in nature from the previous attacks (Gaussian Elimination, ISD and Statistical Decoding) which all boil down to exploiting a set of linear equations. More importantly, this allows us to identify a parameter range (relevant to cryptography) where algebraic attacks are not only competitive, but also outperform these algorithms.

Our attack is based on solving a polynomial system in the coordinates of the error $\boldsymbol{e}$ by combining the set of $n-k$ parity-check equations $\boldsymbol{H}\boldsymbol{e}^{\mathsf{T}} = \boldsymbol{0}$ with another quadratic system which encodes the regular structure and which does not depend on the particular RSD instance. More precisely, for each block $\boldsymbol{e}_i := (e_{i,1}, \ldots, e_{i,\beta}) \in \mathbb{F}^{\beta}$ for $1 \leq i \leq h$, we consider all equations of the form $e_{i,j_1} e_{i,j_2} = 0$ for $j_1 < j_2$. Over $\mathbb{F}_2$, we consider a variant of this combined system by adding extra structural equations of the same type. We then apply standard algorithms, e.g. XL/Gröbner bases, but a first theoretical contribution lies in the complexity analysis to estimate the degree at which the system is solved and which is always a challenge in algebraic cryptanalysis. For that purpose, we proceed by isolating the structural part of the system that we analyze on its own. Then, we formalize the assumption that the parity-check equations behave nicely in the quotient ring formed by the structural part, mimicking Bardet's definitions of semi-regularity [7]. In cases when the predicted solving degree is too large, we also propose a hybrid approach to decrease the complexity by fixing zero coordinates in the error $\boldsymbol{e}$ in the style of the regular version of Prange's algorithm given in [31, Appendix B.3].

In the same way as the Arora-Gê attack [5] takes advantage of a large number of LWE samples, our attack performs best on RSD instances where there are many parity-check equations (*i.e.* with smaller code rate R). This is typically the case for the parameter sets used to instantiate the primal LPN formulation. Under similar assumptions on our specialized systems, this hybrid technique allows us to obtain very competitive complexities for several parameters of this kind, see Table 1. Note that these various assumptions have been extensively tested. In Table 1, we also notice that the attack seems to suffer less than linear

n	k	h	Best $\mathbb{F}_2$ [34]	This work $\mathbb{F}_2$	Best $\mathbb{F}_{2^{128}}$ [34]	This work $\mathbb{F}_{2^{128}}$
2^{22}	64770	4788	147	<u>103</u>	156	<u>111</u>
2^{20}	32771	2467	143	<u>126</u>	155	<u>131</u>
2^{18}	15336	1312	139	<u>123</u>	153	<u>133</u>
2^{16}	7391	667	135	141	151	151
2^{14}	3482	338	132	140	150	152
2^{12}	1589	172	131	136	155	<u>152</u>
2^{10}	652	106	176	<u>146</u>	194	<u>180</u>

Table 1. Time complexity over $\mathbb{F}_2$ and $\mathbb{F}_{2^{128}}$ on parameter sets from [18],[34]

algebra-based techniques – Gaussian elimination or ISD algorithms – when the field size is increased. Indeed, for all but the last parameter set, the increase in complexity when going from $\mathbb{F}_2$ to $\mathbb{F}_{2^{128}}$ is smaller for our attack than for the previously best known algorithms. Our method also seems to perform better in some regimes compared to others. In particular, we try to strengthen these initial intuitions by providing a sketch of asymptotic analysis of the complexity of solving our plain systems.

2 Preliminaries

2.1 Algebraic background

Let A denote a polynomial ring over a field $\mathbb{F}$ in n variables. A polynomial $f \in A$ is *homogeneous* if all its monomials have the same degree and *affine* otherwise. There are two standard methods for turning an affine polynomial into a homogeneous polynomial that we will use in our analysis. For an affine polynomial f, the first one considers the polynomial $f^{(h)}$ which only consists of the terms in f of degree $\deg(f)$ (i.e., discarding all lower degree terms). The second method is to *homogenize* f by expanding the polynomial ring with a homogenization variable y and by defining $f^{(y)}(x_1, \ldots, x_n, y) := (1/y)^{\deg(f)} f(x_1/y, \ldots, x_n/y)$.

An ideal is homogeneous if there exists a set of homogeneous generators. We will turn an affine ideal $I \subset A$ into a homogeneous ideal $I^{(h)}$ (resp. $I^{(y)}$) by applying $f^{(h)}$ (resp. $f^{(y)}$) to each of its generators. When I is homogeneous, the set $I_d := \{f \in I,\ \deg(f) = d\} = I \cap A_d$ is a subspace of A_d the vector space of homogeneous polynomials of total degree d.

Hilbert function and Hilbert series. For a homogeneous ideal $I \subset A$, we consider the *Hilbert function*:

$$\begin{aligned} \mathcal{HF}_{A/I} : \mathbb{N} &\longrightarrow \mathbb{N} \\ d &\longmapsto \dim_{\mathbb{F}}(A_d/I_d). \end{aligned}$$

The Hilbert series is a convenient tool to study the combinatorial structure of homogeneous ideals.

Definition 3 (Hilbert series). *Let $I \subset A$ be a homogeneous ideal. The Hilbert series of the quotient ring A/I is defined by*

$$\mathcal{H}_{A/I}(z) := \sum_{d=0}^{\infty} \mathcal{HF}_{A/I}(d) \cdot z^d. \tag{1}$$

Over a finite field $\mathbb{F}$, we implicitly add all the *field equations* of the form $x_i^{|\mathbb{F}|} - x_i = 0$ for $1 \leq i \leq n$. Therefore, we will study zero-dimensional ideals, *i.e.*, ideals I such that the quotient A/I is a finite dimensional vector space. For such ideals, we call *degree of regularity* d_{reg} the smallest integer d such that $I_d = A_d$. In this particular case, the Hilbert series is a polynomial.

Regular and semi-regular sequences. Unfortunately, Hilbert series are difficult to compute in general. Still, there is a known expression for the series of a subclass of systems whose definition is related to the notion of zero-divisor. When $m \leq n$, we say that a homogeneous system $\mathcal{F} := \{f_1, \ldots, f_m\}$ is *regular* if f_i is not a zero divisor in $A/\langle f_1, \ldots, f_{i-1}\rangle$ for any $1 \leq i \leq m$. The Hilbert series of such a system is given by

Proposition 1. *Let $\mathcal{F} := \{f_1, \ldots, f_m\}$ be a homogeneous regular system such that $\deg(f_i) = d_i$ for $1 \leq i \leq m$. We have*

$$\mathcal{H}_{A/\langle \mathcal{F}\rangle}(z) = \frac{\prod_{i=1}^{m}(1 - z^{d_i})}{(1-z)^n}.$$

This definition has been extended to the overdetermined case, $m > n$, with the notion of *semi-regular* sequences introduced by Bardet.

Definition 4 (Semi-regular sequence, [7]). *Consider $\mathcal{F} := \{f_1, \ldots, f_m\}$ a homogeneous sequence such that $I := \langle \mathcal{F}\rangle$ is zero-dimensional with degree of regularity d_{reg}. The sequence $\mathcal{F}$ is said to be semi-regular if $I \neq A$ and if for $1 \leq i \leq m$, $g_i f_i = 0$ in $A/\langle f_1, \ldots, f_{i-1}\rangle$ with $\deg(g_i f_i) < d_{reg}$ implies $g_i = 0$ in $A/\langle f_1, \ldots, f_{i-1}\rangle$.*

Over $\mathbb{F}_2$, there is a similar definition but which needs to take the Frobenius morphism into account:

Definition 5 (Semi-regular sequence over $\mathbb{F}_2$, [7]). *Let S denote the quotient ring $\mathbb{F}_2[\boldsymbol{x}]/\langle x_1^2, \ldots, x_n^2\rangle$. A homogeneous sequence $\mathcal{F} := \{f_1, \ldots, f_m\}$ with degree of regularity d_{reg} is semi regular over $\mathbb{F}_2$ if $I \neq S$ and if for $1 \leq i \leq m$, $g_i f_i = 0$ in $S/\langle f_1, \ldots, f_{i-1}\rangle$ with $\deg(g_i f_i) < d_{reg}$ implies $g_i = 0$ in $S/\langle f_1, \ldots, f_i\rangle$.*

The Hilbert series is also known for such systems. In particular, it is a polynomial since the corresponding ideal is zero-dimensional.

Proposition 2 ([7]). *Let $\mathcal{F} := \{f_1, \ldots, f_m\}$ be a homogeneous semi-regular system where $\deg(f_i) = d_i$ for $1 \leq i \leq m$ and let $S_{m,n,\boldsymbol{d}}(z) = \frac{\prod_{i=1}^{m}(1-z^{d_i})}{(1-z)^n}$. We have*

$$\mathcal{H}_{A/\langle \mathcal{F}\rangle}(z) = \left[S_{m,n,\boldsymbol{d}}(z)\right]^+,$$

where $[\cdot]^+$ means truncation after the first non-positive coefficient.

Proposition 3 ([7]). *Let $\mathcal{F} := \{f_1, \ldots, f_m\}$ be a homogeneous semi-regular system over $\mathbb{F}_2$ where $\deg(f_i) = d_i$ for $1 \leq i \leq m$ and let $T_{m,n,\boldsymbol{d}}(z) = \frac{(1+z)^n}{\prod_{i=1}^{m}(1+z^{d_i})}$. We have*

$$\mathcal{H}_{A/\langle \mathcal{F}\rangle}(z) = \left[T_{m,n,\boldsymbol{d}}(z)\right]^+.$$

Finally, an affine sequence $\mathcal{F} := \{f_1, \ldots, f_m\}$ is said to be semi-regular in [7, Def. 3.5.1] if the homogeneous sequence $\mathcal{F}^{(h)} := \{f_1^{(h)}, \ldots, f_m^{(h)}\}$ is semi-regular in the sense of Definition 4. Interestingly, it turns out that this subclass of systems is somehow large since it is conjectured that most systems behave as

such (this is related to the Fröberg conjecture [30]). In simpler terms, we may say that randomly chosen polynomial systems with $m \leq n$ (resp. $m > n$) have an overwhelming probability of being regular (resp. semi-regular).

Unfortunately, we will see that the polynomial systems considered in this work cannot be directly analyzed by these tools. This issue is uniquely related to structural equations inherent in the systems. It is then possible to split the polynomial system in two: the first part can be treated in a prior analysis, and the second part can be assumed to be *generic*. At this stage, we will be able to rely on the same algebraic tools as used in proofs of Proposition 2 and Proposition 3 to derive our final Hilbert series, up to minor technical amendments.

2.2 Solving polynomial systems

Gröbner basis techniques are generally used to solve cryptographically relevant polynomial systems, keeping in mind that this approach is closely related to the XL algorithm [26]. Both approaches typically depend on the notion of *Macaulay matrix*. If $\mathcal{F}$ is homogeneous, the (homogenous) Macaulay matrix $\boldsymbol{M}_d(\mathcal{F})$ is defined as the coefficient matrix of $(\mu_{i,j} \cdot f_j)_{i,\ 1 \leq j \leq m}$ where $\mu_{i,j}$ is any monomial of degree $d - \deg(f_i)$. If $\mathcal{F}$ is affine, we prefer to consider $\boldsymbol{M}_{\leq d}(\mathcal{F})$ where now $\deg(\mu_{i,j}) \leq d - \deg(f_i)$ and where the columns are indexed by all monomials of degree $\leq d$.

XL Wiedemann. The main idea of XL is to solve by linearization an augmented system in degree $\leq d$ obtained from $\mathcal{F}$ by multiplying the initial polynomials by all monomials of the suitable degree. The value of d is chosen such that there are enough linearly independent equations compared to the number of monomials and the matrix of the linearized system is simply the Macaulay matrix $\boldsymbol{M}_{\leq d}(\mathcal{F})$. In the particular case when the linear system in degree d has a unique solution and is sparse enough, this approach may greatly benefit from the use of the Wiedemann algorithm [43] or its further improvements [25,41]. The application of the Wiedemann algorithm to solve Macaulay matrices has been implemented and studied in [24]. In our setting, we can estimate the cost of this approach to find the solution of the linear system to be

$$3 \cdot n_\mu \cdot \mathcal{M}_{\leq d}^2, \tag{2}$$

where n_μ is the number of terms in the polynomials of $\mathcal{F}$ (*i.e.* the row weight of $\boldsymbol{M}_{\leq d}(\mathcal{F})$), where $\mathcal{M}_{\leq d}$ is the number of columns in $\boldsymbol{M}_{\leq d}(\mathcal{F})$ and where the choice of a hidden constant equal to 3 is very standard in the literature on multivariate cryptography, see for example [13, Prop 3 p. 219],[17].

Witness degree. While the degree of regularity d_{reg} is usually employed as the main parameter to estimate the complexity of Gröbner basis algorithms on homogeneous systems, we will require a related, though slightly different notion in the case of XL Wiedemann. A first reason is that we have just defined d_{reg} for

homogeneous systems whereas we will typically apply this algorithm on *affine* equations. To this end, let us recall the *witness degree* d_{wit}, originally introduced in [8, Definition 2] for the binary case. For an ideal I, the notation $\text{LM}(I)$ denotes the monomial ideal generated by the leading monomials of all polynomials in I for an arbitrary graded ordering.

Definition 6 (Witness degree). *Let $\mathcal{F} := \{f_1, \dots f_m\}$ be an affine polynomial system over $\mathbb{F}_q$, and $I := \langle \mathcal{F} \rangle$ its associated ideal. Define the $\mathbb{F}_q$-vector spaces*

$$I_{\leq d} := \{p \in I \mid \deg(p) \leq d\},$$
$$J_{\leq d} := \left\{ p \in I \mid p = \sum_{i=1}^{m} g_i f_i, \text{ and } \deg(g_i) \leq d - \deg(f_i) \text{ for } 1 \leq i \leq m \right\}.$$

The witness degree d_{wit} *of $\mathcal{F}$ is defined as the smallest integer d_0 such that $I_{\leq d_0} = J_{\leq d_0}$ and $LM(I_{\leq d_0}) = LM(I)$.*

We will be interested in cases where $\mathcal{F}$ contains fewer than n affine polynomials, whereas its Gröbner basis is either $\{1\}$, or a set of n affine polynomials. Thus there are non-trivial polynomials $\sum g_i f_i \in I$ where the coefficients of the higher degree terms sum to zero. It follows that if $\mathcal{F}$ is also semi-regular, then d_{reg} is a lower bound on the degree d such that $J_{\leq d} = I_{\leq d}$. This ensures $d_{\text{wit}} \geq d_{\text{reg}}$. Even under these assumptions, we remark that d_{reg} is only attached to $\mathcal{F}^{(h)}$, whereas the purpose of d_{wit} is precisely to analyze the lower degree parts of $\mathcal{F}$ as well.

We will later see examples where d_{wit} is strictly larger than d_{reg}, so we need a more accurate estimate of the former than this lower bound. If the input polynomial system admits no solutions (i.e., $\langle \mathcal{F} \rangle = \langle 1 \rangle$), its witness degree can be upper bounded by the degree of regularity of the corresponding homogenized system by adding an extra homogenization variable y (see beginning of Section 2.1). In other words, we have

Proposition 4. *Let $\mathcal{F} = \{f_1, \dots, f_m, x_1^q - x_1, \dots, x_n^q - x_n\}$ be a sequence of polynomials in $\mathbb{F}_q[x_1, \dots, x_n]$ that admits no solutions, and let $I^{(y)}$ be its associated homogenized ideal. Then $d_{wit}(\mathcal{F}) \leq d_{reg}\left(I^{(y)}\right)$.*

This statement is shown[5] in [8, Proposition 5]. Note that the requirement of $\mathcal{F}$ being non-consistent makes sense since the BooleanSolve algorithm presented in [8] is a hybrid algorithm, and the majority of calls to a polynomial system solver is made for systems without any solutions. We will indeed follow the same strategy for the hybrid systems considered in Section 4. However, on the plain system, Proposition 4 cannot be applied readily to bound d_{wit}. Instead, we will propose a more direct approach of inspecting affine Macaulay matrices in Section 3.2.

[5] The statement in [8, Proposition 5] is only for $\mathbb{F}_2$, but we note that the same proof also works for the case of $\mathbb{F}_q$.

3 Algebraic modeling of the RSD problem

In this section, we introduce the polynomial systems that we consider for the RSD problem. We will work over a polynomial ring $A = \mathbb{F}[\boldsymbol{e}]$, where each error vector entry $e_{i,j}$ is treated as an indeterminate to be solved for. The equations of the polynomial systems are obtained from the $n-k$ parity-check equations $\boldsymbol{s}^\mathsf{T} = \boldsymbol{H}\boldsymbol{e}^\mathsf{T}$ to which we add constraints coming from the regular structure. Modeling 1 is used to solve RSD over an arbitrary (large) field $\mathbb{F}$ while Modeling 2 is specific to the binary case.

Modeling 1 (Over a large field) *For a given RSD instance $(\boldsymbol{H}, \boldsymbol{s}^\mathsf{T})$ over $\mathbb{F}$, Modeling 1 is the sequence of polynomials $\mathcal{F} := \mathcal{P} \cup \mathcal{B}$, where*

i) $\mathcal{P}$ is the set of the $n-k$ linear polynomials given by the parity-check equations $\boldsymbol{s}^\mathsf{T} = \boldsymbol{H}\boldsymbol{e}^\mathsf{T}$;
ii) $\mathcal{B}$ is the set of quadratic polynomials that describe the regular form of the error vector $\boldsymbol{e}$, namely $e_{i,j_1}e_{i,j_2} = 0$ for $1 \leq i \leq h$ and $1 \leq j_1 < j_2 \leq \beta$.

We also include the so-called field equations $e_{i,j}^{|\mathbb{F}|} - e_{i,j} = 0$, so that the ideal generated by Modeling 1 is zero-dimensional. However, these equations will not be useful for the computation due to their large degree and thus the situation is completely different over $\mathbb{F}_2$ in that respect. Also, note that Modeling 1 only captures the fact that the Hamming weight in each block is at most 1 since we have no information on the non-zero coordinate. Over $\mathbb{F}_2$ however, we know that this non-zero component is equal to 1.

Modeling 2 (Over $\mathbb{F}_2$) *For a given binary RSD instance $(\boldsymbol{H}, \boldsymbol{s}^\mathsf{T})$, Modeling 2 is the sequence of polynomials $\mathcal{F}_{\mathbb{F}_2} = \mathcal{P} \cup \mathcal{B} \cup \mathcal{Q}_{\mathbb{F}_2} \cup \mathcal{L}_{\mathbb{F}_2}$, where $\mathcal{P}$ and $\mathcal{B}$ are as in Modeling 1 and where:*

i) $\mathcal{Q}_{\mathbb{F}_2}$ is the set of field equations $e_{i,j}^2 - e_{i,j} = 0$ for $1 \leq i \leq h$ and $1 \leq j \leq \beta$;
ii) $\mathcal{L}_{\mathbb{F}_2}$ is the set of h linear equations $1 - \sum_{j=1}^{\beta} e_{i,j} = 0$ for $1 \leq i \leq h$ which express the fact that each block has a unique non-zero coordinate.

In both cases, the main contribution is the set $\mathcal{P}$ containing $n-k = n(1-R)$ parity-check equations. Therefore, this approach is expected to be relevant for instances with non-constant rate. This is the case of the parameter sets used to instantiate primal LPN, see [18,44,42,34]. From the public generator matrix $\boldsymbol{G}$, we trivially construct the equivalent dual LPN instance and we then use Modeling 1 or 2 on this dual problem. Finally, we see that the unknowns are merely the coordinates of the error vector $\boldsymbol{e}$. In particular, we expect as many solutions as the initial RSD instance, *i.e.* 1, for the range of parameters of interest[6]. This will be needed to justify the use of the XL algorithm later.

[6] Even though the weight h is slightly larger than the Gilbert-Varshamov distance, the regular structure is a much stronger requirement.

3.1 Deriving Hilbert series

The goal of this section is to compute the Hilbert series (Definition 3) of the homogeneous ideals $I := \langle \mathcal{F}^{(h)} \rangle$ and $I_{\mathbb{F}_2} := \langle \mathcal{F}_{\mathbb{F}_2}^{(h)} \rangle$ associated to Modeling 1 and Modeling 2 respectively. We start by observing that these sequences cannot be analyzed as semi-regular systems. Indeed, consider the equations $f_1 := e_{1,1}e_{1,2}$ and $f_2 := e_{1,2}e_{1,3}$. Since $e_{1,1}f_2 = 0$ in $A/\langle f_1 \rangle$, the polynomial f_2 is a non-trivial zero divisor in $A/\langle f_1 \rangle$. Note that this type of cancellation does not depend on the particular RSD instance, but rather comes from the regular structure of $\boldsymbol{e}$. Thus, it still makes sense to compute Hilbert series that will be valid for generic instances of the RSD problem.

Hilbert series for Modeling 1. Recall that Modeling 1 is the sequence $\mathcal{F} = \mathcal{P} \cup \mathcal{B}$, where $\mathcal{P}$ are the parity-check equations and where $\mathcal{B}$ describes the regular structure of the error vector. The first step will be to compute the Hilbert series $\mathcal{H}_S(z)$ by monomial counting, for $S := A/\langle \mathcal{B}^{(h)} \rangle$. Since S is not a polynomial ring, we will not formally speak about (semi-)regular sequences over S. Yet, we still want to capture the core idea of the remaining parity-check equations behaving nicely, by introducing the following assumption for Modeling 1.

Assumption 1 *Consider an instance $\mathcal{F}$ of Modeling 1 and let d_{reg} be the degree of regularity of $I := \langle \mathcal{F}^{(h)} \rangle$. Define the quotient ring $S := A/\langle \mathcal{B}^{(h)} \rangle$ and let $\mathcal{P}^{(h)} = \{p_1^{(h)}, \ldots, p_{n-k}^{(h)}\}$ denote the set of linear parity-check equations. We assume that for $1 \leq i \leq n-k$, $g_i p_i = 0$ in $S/\langle p_1, \ldots, p_{i-1} \rangle$ with $\deg(g_i p_i) < d_{reg}$ implies $g_i = 0$ in $S/\langle p_1, \ldots, p_{i-1} \rangle$.*

Relying on this assumption, we can obtain the final Hilbert series for $I := \langle \mathcal{F}^{(h)} \rangle$:

Theorem 1. *Under Assumption 1, the Hilbert series of the homogeneous ideal $I := \langle \mathcal{F}^{(h)} \rangle$ associated with Modeling 1 is given by*

$$\mathcal{H}_{A/I}(z) = \left[(1-z)^{n-k} \cdot \left(1 + \beta \cdot \tfrac{z}{1-z}\right)^h \right]_+ , \tag{3}$$

where $[.]_+$ means truncation after the first non-positive coefficient, and where we call $(1-z)^{n-k} \cdot \left(1 + \beta \cdot \frac{z}{1-z}\right)^h$ the generating series *of I.*

Proof. The proof can be found in Appendix A.1. □

Hilbert series for Modeling 2. Modeling 2 contains extra structural equations, starting from the field equations in $\mathcal{Q}_{\mathbb{F}_2}$. A difficulty arises when adding the last set of equations $\mathcal{L}_{\mathbb{F}_2}$ since it yields another type of cancellation. For $1 \leq i \leq h$ and $1 \leq j_0 \leq \beta$, we indeed have:

$$e_{i,j_0} \cdot \left(-\sum_{j=1}^{\beta} e_{i,j} \right) = 0 \bmod \left\{ e_{i,j_0}^2, \{ e_{i,j_1} e_{i,j_2} \}_{j_1 < j_2} \right\}. \tag{4}$$

In other words, any polynomial in $\mathcal{L}_{\mathbb{F}_2}^{(h)}$ is a zero divisor in $A/\langle \mathcal{B}^{(h)} \cup \mathcal{Q}_{\mathbb{F}_2}^{(h)} \rangle$. To keep the same type of analysis as with Modeling 1, we may use $\mathcal{L}_{\mathbb{F}_2}$ to remove h variables. More formally, we define the graded ring homomorphism

$$\begin{aligned} \mathcal{L} : \mathbb{F}_2[\boldsymbol{e}] &\longrightarrow \mathbb{F}_2[\boldsymbol{x}] \\ e_{i,j} &\longmapsto x_{i,j}, \text{ for } 1 \leq i \leq h \text{ and } 1 \leq j < \beta \\ e_{i,\beta} &\longmapsto \sum_{j=1}^{\beta-1} x_{i,j} \text{ for } 1 \leq i \leq h. \end{aligned}$$

Definition 7. *Consider an instance of Modeling 2, and $\mathcal{L}$ be as detailed above. We then define $A' := \mathcal{L}(A)$, $I' := \mathcal{L}(I^{(h)})$, $\mathcal{B}' := \mathcal{L}(\mathcal{B}^{(h)})$, $\mathcal{Q}' := \mathcal{L}(\mathcal{Q}_{\mathbb{F}_2}^{(h)})$ and $S' := A'/\langle \mathcal{B}' \cup \mathcal{Q}' \rangle$.*

The following lemma shows that A' is a polynomial ring and describes the structure of S'.

Lemma 1. *A' is isomorphic to $\mathbb{F}_2[x_1, \ldots, x_{h(\beta-1)}]$. Moreover, the ideal $\langle \mathcal{B}' \cup \mathcal{Q}' \rangle$ is generated by $\mathcal{G} = \{x_{i,j}x_{i,l} \mid 1 \leq i \leq h \text{ and } 1 \leq j, l < \beta\}$.*

Proof. The first statement is immediate from the definition of $\mathcal{L}$. For the second statement, we note that $\mathcal{G}$ is exactly the image of generators of $\mathcal{B}^{(h)} \cup \mathcal{Q}_{\mathbb{F}_2}^{(h)}$ that does not contain an element $e_{i,\beta}$. To see that the image of the remaining generators of $\mathcal{Q}_{\mathbb{F}_2}^{(h)}$ does not add anything new, we get

$$\mathcal{L}(e_{i,\beta}^2) = \left(\sum_{j=1}^{\beta-1} x_{i,j}^2 \right) = 0 \bmod \mathcal{G}.$$

The cancellations of the remaining generators of $\mathcal{B}^{(h)}$ were already pointed out by (4). □

We can furthermore use Lemma 1 to count the number of monomials in S'. Indeed, the possible monomials are squarefree and contain only one variable per block due to the shape of $\mathcal{G}$. In particular, a degree d monomial defines a set of d blocks. Then, each block contains $\beta - 1$ relevant variables instead of β since we reduce modulo $\mathcal{L}_{\mathbb{F}_2}$. This shows that there are $\binom{h}{d}(\beta-1)^d$ degree d monomials in S'.

We now need to adopt a similar assumption as with Modeling 1. Note the strong similarity between Definition 5 and the following Assumption 2:

Assumption 2 *Consider an instance of Modeling 2 with degree of regularity d_{reg}, and let S' be as defined in Definition 7. For every parity-check equation, p_i, write $p_i' = \mathcal{L}(p_i^{(h)})$. We assume that for $1 \leq i \leq n-k$, $g_i p_i' = 0$ in $S'/\langle p_1', \ldots, p_{i-1}' \rangle$ with $\deg(g_i) + \deg(p_i') < d_{reg}$ implies $g_i = 0$ in $S'/\langle p_1', \ldots, p_i' \rangle$.*

Theorem 2. *Under Assumption 2, the Hilbert series of the homogeneous ideal* $I_{\mathbb{F}_2} := \langle \mathcal{F}_{\mathbb{F}_2}^{(h)} \rangle$ *associated to Modeling 2 is given by*

$$\mathcal{H}_{A/I_{\mathbb{F}_2}}(z) = \left[\frac{(1+(\beta-1)\cdot z)^h}{(1+z)^{n-k}} \right]_+ . \tag{5}$$

Proof. The proof can be found in Appendix A.2. □

3.2 Estimating the witness degree

As explained at the end of Section 2, we will use the witness degree d_{wit} of the input polynomial system (see Definition 6) to estimate the cost of the XL Wiedemann approach.

By definition, the system $\mathcal{F}$ of Modeling 1 (resp. Modeling 2) admits at least one solution and we will assume that it is unique for the range of parameters of interest. Note that a polynomial system that includes field equations[7] and admits a unique solution $(a_1, \ldots, a_n)$ has reduced Gröbner basis $\{x_1 - a_1, \ldots, x_n - a_n\}$. Recalling the conditions in Definition 6 and if $I := \langle \mathcal{F} \rangle$, we have $\text{LM}(I_{\leq 1}) = \text{LM}(I)$ and $\dim(I_{\leq d}) = \dim(A_{\leq d}) - 1$. In particular, we can say that $d_{\text{wit}}(\mathcal{F})$ is the smallest degree such that the rank of the associated affine Macaulay matrix is equal to the number of columns minus one.

We will use this observation to provide an estimate of the witness degree. Note that semi-regularity can be seen as the assumption that the *homogeneous* Macaulay matrices have maximal rank; we now adopt the assumption that the *affine* Macaulay matrices achieve maximal rank. With this assumption, we can reuse the Hilbert Series machinery we have developed in this section. Consider the untruncated version of the series in Equations (3) and (5). The coefficient in a term of degree $d < d_{\text{reg}}$ is positive and it coincides with the number of columns that cannot be reduced in the homogeneous Macaulay matrix of degree d. When $d \geq d_{\text{reg}}$, the coefficient is non-positive and measures the number of "excess" rows after full reduction of this matrix. When these rows are considered in their full affine form they will, in general, not sum to zero. Coming back to the polynomial representation, they yield what we typically call *degree falls* or *degree fall polynomials* in the literature.

Finally, we arrive at the following estimate for the witness degree by summing these coefficients.

Estimate (Plain witness degree) *Let $\mathcal{F}$ be the polynomial system of Modeling 1 (resp. Modeling 2) and let $\mathcal{H}$ denote the untruncated series of Equation (3) (resp. Equation (5)). Then we estimate $d_{wit}(\mathcal{F})$ to be*

$$d_{wit,(0,0)} := \min \left\{ d \in \mathbb{Z}_{\geq 1} \;\middle|\; \sum_{j=0}^{d} [z^j] \left(\mathcal{H}(z) \right) \leq 0 \right\}, \tag{6}$$

[7] The field equations ensure that the ideal is radical, and the result follows from Hilbert's Nullstellensatz. In practice, the reliance on field equations can typically be eased for sufficiently overdetermined systems. Thus we will assume that this also holds for Modeling 1, even when the field equations are not explicitly included in $\mathcal{F}$.

where $[z^j]\,(\mathcal{H}(z))$ *denotes the coefficient of the monomial* z^j *in* $\mathcal{H}$.

We have found this estimate to be accurate in all our experiments, which are further reported in Appendix C.

4 Hybrid approach

As is standard in algebraic cryptanalysis, the complexity of our approach essentially depends on the value of d_{reg} or d_{wit}. However, for most of the parameter sets that we have studied, these degrees seem too high for straightforward algebraic techniques to be competitive with other types of attacks.

To decrease these degrees and possibly improve the overall complexity, we propose to add new equations in the same $\boldsymbol{e}$ variables which may hold with probability $0 < \mathcal{P} < 1$. The idea is the same as in a standard hybrid approach [16]: we hope that the complexity gain in solving the resulting system may supersede the loss coming from adding these equations since we have to repeat the process $\mathcal{O}(\mathcal{P}^{-1})$ times on average to find a solution. Due to the nature of the RSD problem, a natural idea is to fix linear constraints of the form $e_{i',j'} = 0$. Note that this is exactly what the Prange algorithm does by picking an information set I and then assuming that $\boldsymbol{e}_I = \mathbf{0}$. In our case, these constraints reduce the number of non-zero monomials in degree $d \geq 1$ (even though the number of equations at hand also decreases) and thus we hope that the specialized system with these constraints will be solved at a smaller degree. In the following, we develop this hybrid approach for Modeling 1, noting that the case of Modeling 2 works in the same way.

4.1 Guessing error-free positions in all blocks

A first idea is to guess the same number of error-free positions in all blocks. A similar approach was followed in [31, B.3] to adapt ISD algorithms to a regular error distribution. Each block in the RSD problem can be seen as a random vector of length β and weight 1. The success probability of guessing u error-free positions is $\binom{\beta-1}{u}/\binom{\beta}{u}$. By exploiting the regular structure, one may guess the same number of positions in each block with probability

$$\mathcal{P}_{(u)} := \left(\frac{\binom{\beta-1}{u}}{\binom{\beta}{u}} \right)^h = (1 - u/\beta)^h. \tag{7}$$

The improvement by using Equation (7) instead of the naive probability in the Prange algorithm (or even in more involved ISD variants) was not really apparent in [31] ("ISD is always the most efficient attack and has roughly the same cost when considering SD and RSD" [31, p. 49]). Still, we can try to adopt the same technique for Modeling 1. We start by guessing that the top part of size $0 \leq u \leq \beta$ is error-free in each block, which holds with probability $(1 - u/\beta)^h$. The main difference with [31, B.3] is that we will have $uh \ll k$. Indeed, we need to guess

much fewer error-free positions to decrease the solving degree of Modeling 1 while the Prange linear system "stays" in degree 1 and needs more equations. In case of failure, we consider a permutation matrix $\boldsymbol{P}_\pi \in \mathbb{F}^{n\times n}$ which permutes the coordinates in each block (so that the regular structure is maintained) and we try again on the RSD instance $(\boldsymbol{H}\boldsymbol{P}_\pi^{-1}, \boldsymbol{s})$ which has error $\boldsymbol{\varepsilon}^\mathsf{T} = \boldsymbol{P}_\pi \boldsymbol{e}^\mathsf{T}$. By fixing the $e_{i,j}$ variables to zero for $1 \le i \le h$ and $1 \le j \le u$, the number of possible non-zero monomials in degree d is now given by the coefficient of z^d in

$$\left(1 + (\beta - u) \cdot \tfrac{z}{1-z}\right)^h.$$

To derive the Hilbert series of the specialized system, we need to adapt Assumption 1 (see Assumption 3 in Appendix B.1) to ensure that fixing variables does not introduce unexpected cancellations at higher degree among the system of $n-k$ parity-check equations $\{p_1, \dots, p_{n-k}\}$. Under this new assumption, the Hilbert series of the hybrid system is obtained by applying Theorem 1 to an RSD instance with block size $\beta - u$:

$$\mathcal{H}_{A/I,\mathrm{hyb1},u}(z) = \left[(1-z)^{n-k} \cdot \left(1 + (\beta - u) \cdot \tfrac{z}{1-z}\right)^h\right]_+ \tag{8}$$

Hence, while both the number of equations and monomials of degree $d \ge 1$ are affected by adding the zero constraints, they are still on a form that is captured by the Hilbert series studied in Section 3. In practice, we typically require a weaker form of Assumption 3. Indeed, the optimal choice of u is rather small for the parameters that we will study in Section 5. Heuristically, we have more confidence in our assumption with a smaller u as it implies less specialization of the polynomial system. Finally, we note that a similar statement for specialized systems is also present in the standard hybrid approach for semi-regular systems, see [16, Hypothesis 3.3]. Starting from a semi-regular system $\{f_1, \dots, f_m\}$, they assume that all the specialized versions

$$\{f_1(x_1, \dots, x_{n-k}, \boldsymbol{v}), \dots, f_m(x_1, \dots, x_{n-k}, \boldsymbol{v})\},\ \forall \boldsymbol{v} \in \mathbb{F}^k,\ \forall 0 \le k \le n$$

are semi-regular.

4.2 Restricting to $f \le h$ blocks

A slightly more general approach is to guess $0 \le u \le \beta$ error-free positions in only $0 \le f \le h$ blocks so that the success probability becomes $\mathcal{P}_{(f,u)} := (1 - u/\beta)^f$. Under a similar assumption (see Assumption 3 in Appendix B.1 which encompasses both strategies), we can obtain the Hilbert series

$$\mathcal{H}_{A/I,\mathrm{hyb2},f,u}(z) = \left[(1-z)^{n-k} \cdot \underbrace{\left(1 + (\beta - u) \cdot \frac{z}{1-z}\right)^f}_{\text{constraint}} \cdot \underbrace{\left(1 + \beta \cdot \frac{z}{1-z}\right)^{h-f}}_{\text{no constraint}}\right]_+ \tag{9}$$

4.3 Witness degree for the hybrid approach

Similary to what we did in Section 3.2 for the plain system, we now derive an estimate of d_{wit} for the specialized system. Since the plain system is expected to have a unique solution, the majority of guesses will be wrong, *i.e.*, resulting in polynomial systems without any solutions. In that respect, the situation is similar to that of the original BooleanSolve algorithm of [8]. We can in this case use Proposition 4 to upper bound the witness degree by the degree of regularity of the homogenized system.

We will assume that the hybrid systems form semi-regular systems with the extra variable y. Under this assumption, it is straightforward to adapt the Hilbert series given by Equation (8) and Equation (9) to the homogenized versions in the following manner:

$$\mathcal{H}_{A/I,\text{hyb}i,f,u}(z)/(1-z), \tag{10}$$

for $i \in \{1, 2\}$. For the hybrid approach on Modeling 2, we similarly divide by $(1-z)$ the series in Equation (21) Appendix B.2. The degree of regularity of the homogenized systems is then obtained in the usual manner, i.e., by computing the first non-positive coefficient in the associated series. We note that this adaptation on the Hilbert series is in line with the earlier literature (c.f. [8, Proposition 6]) and it has been accurate in our experiments (see Appendix C).

4.4 Complexity with XL Wiedemann

The cost of the hybrid approach of Section 4.2 can now be computed as follows. For each pair (f, u) where $0 \leq f \leq h$ and $0 \leq u \leq \beta$, we proceed as explained in Section 4.3 to obtain an upper-bound bound on the witness degree which we denote by $d_{\text{wit},(f,u)}$ and that we use as our estimate of the real witness degree. To apply Equation (2), we then need the value $\mathcal{M}^{(f,u)}_{\leq d_{\text{wit},(f,u)}}$ which is the number of monomials of degree $\leq d_{\text{wit},(f,u)}$ in the specialized system. It depends on both f, u and $d_{\text{wit},(f,u)}$. Indeed, let $\mathcal{H}_{(S,f,u)}(z) = \left(1 + (\beta - u) \cdot \frac{z}{1-z}\right)^f \cdot \left(1 + \beta \cdot \frac{z}{1-z}\right)^{h-f}$. We have

$$\mathcal{M}^{(f,u)}_{\leq d_{\text{wit},(f,u)}} = \sum_{j=0}^{d_{\text{wit},(f,u)}} [z^j] \left(\mathcal{H}_{(S,f,u)}(z)\right), \tag{11}$$

where we recall that $[z^j]\left(\mathcal{H}(z)\right)$ is the coefficient of the monomial z^j in the series $\mathcal{H}$. Finally, we need to estimate the quantity n_μ which is the number of non-zero terms in one row of the Macaulay matrix. This is directly related to the monomial content of the initial parity-check equations. We can assume that the matrix $\boldsymbol{H}$ is given in systematic form, so that $n_\mu \leq k + 1 = \mathcal{O}(k)$. For the specialized system, we can actually choose to fix the f bottom blocks of the

error[8] to obtain the better factor $n_{\mu,(f,u)} \leq k+1-f \cdot u$. This allows to possibly gain a few bits in the final complexity.

Proposition 5. *Under Assumption 3 and the assumptions described in Section 4.3, the time complexity in $\mathbb{F}$-operations of the hybrid approach of Section 4.2 on Modeling 1 is estimated by*

$$\mathcal{O}\left(\min_{\substack{0\leq f\leq h\\ 0\leq u\leq \beta}}\left(\mathcal{P}_{(f,u)}^{-1}\cdot 3\cdot n_{\mu,(f,u)}\cdot\left(\mathcal{M}_{\leq d_{\mathrm{wit},(f,u)}}^{(f,u)}\right)^2\right)\right),$$

where

$$\mathcal{P}_{(f,u)} := (1-u/\beta)^f,$$
$$n_{\mu,(f,u)} := k+1-f\cdot u,$$
$$\mathcal{M}_{\leq d_{\mathrm{wit},(f,u)}}^{(f,u)} \text{ is defined in Equation (11),}$$

and where $d_{\mathrm{wit},(f,u)}$ is the index of the first non-positive coefficient in the generating series given in Equation (10).

We can obtain a similar statement for Modeling 2 (see Proposition 7 in Appendix B.2). Finally, we want to stress the fact that the specializations proposed in Sections 4.1 and 4.2 are possibly the most naive ways to fix variables in the system. Even though they seem to lead the best success probability since we take advantage of the regular structure, other approaches might allow to decrease the solving degree faster.

4.5 Rationale and experimental verification

The assumptions that we use can be seen as very similar to those generally encountered in algebraic cryptanalysis. More specifically, in our systems these genericity assumptions concern the linear parts of the parity-check equations, and these polynomials simply depend on the matrix $\boldsymbol{H}$. Even though the underlying code $\mathcal{C}$ is typically chosen d-local in the primal formulation, the parity-check matrix obtained from the public matrix $\boldsymbol{G}$ has no reason to be special in a certain sense. Otherwise, such a particular property may probably be exploited by attacks or indicate that this instantiation is weaker than standard LPN.

In a very similar context, the well-known Arora-Gê system [5] to solve LWE is generally assumed to be semi-regular [2,40]. In [3], some practical experiments have been performed to confirm this hypothesis ([3, §7.1]) and we also note that they try to prove (a weaker form of) it in some particular cases ([3, A.2]). Their experiments verify that the solving degree of Arora-Gê coincides with that of a random system of the same size.

We have experimentally tested the assumptions made throughout Sections 3 and 4, the details of which are available in Appendix C. More specifically,

[8] There is no loss of generality: this can be seen as choosing a monomial ordering which favors the upper variables and then fixing somehow small variables.

we have tested Assumptions 1, 2 and their hybrid counterparts; the hybrid d_{wit} estimate for Modeling 1 and 2; and finally the plain d_{wit} estimate for Modeling 1. Assumptions 1 and 2 have been correct in all our experiments, and we have only been able to observe discrepancies for a few hybrid cases of Modeling 2 (see Appendix C.1 for further discussion). Finally, the estimates on the witness degree have been correct in all the tested cases.

5 Application to some parameters

We now estimate the complexity of the attack using the hybrid technique of Section 4.2 on some LPN parameter sets with non-constant rate taken from primal LPN instantiations. For each parameter set, we compute the optimal complexity using Proposition 5 for Modeling 1 (resp. Proposition 7 from Appendix B.2 for Modeling 2). We report the pair (f, u) that leads to the best complexity and the associated estimate on the witness degree $d_{\text{conj}} := d_{\text{wit},(f,u)}$. When f and u are positive, we use the upper bound from Section 4.3 for $d_{\text{wit},(f,u)}$, and when $f = u = 0$, we use the estimate in Equation (6). The sparsity factor is $k+1-f \cdot u$ over large fields or $\min(k+1-f \cdot u,\ k/2+1)$ over $\mathbb{F}_2$. The constant from Wiedemann's algorithm is taken equal to 3 as presented in Equation (2). For illustration, we also give the complexity of the attack without fixing any variables.

The parameters we will consider were first proposed by [18, Table 1]. Their security over $\mathbb{F}_2$ has been re-evaluated in the recent paper [34], where the same parameters are also analyzed over the larger field $\mathbb{F} = \mathbb{F}_{2^{128}}$ (see [34, Table 3]). They are presented in Table 2 and Table 3, respectively. Finally, [34, Table 1] also gives parameters whose initial security target was 128 using the analysis of [18] but which are thought to be much harder according to [34]. These parameters are presented in Tables 4 and 5. When n/h is not an integer, we set $\beta = \lfloor n/h \rfloor$ and fix the last $n - h\beta$ coordinates to zero. Note that the number of parity-check equations at hand is still $n - k$.

Small scale. In Table 2 and Table 3, "Best" refers to the best attack according to the analysis of [34]. In the binary case, the best attack according to [34] are advanced ISD algorithms. For a field size $\log_2(|\mathbb{F}|) = 128$, they note that the Pooled Gauss attack and ISD perform equally. As Gauss can be considered as a special case of ISD, this is quite reminiscent of the result of Canto-Torres [22] which states that all ISD variants converge to the same cost when $|\mathbb{F}|$ tends to infinity and which is basically the cost of Prange's algorithm.

Larger scale. The parameters of [34, Table 1] are obtained simply by increasing the weight h and keeping the same triples (n, k, β) as in the original parameters from [18]. In order words, the noise rate increases but the code rate remains the same. They were chosen so that they just achieve 128 bit security according to the analysis of [18] but [34] considers them to be much harder, see Column "Best" in Tables 4 and 5.

n	k	h	Best [34]	d_{conj} plain	(f, u)	d_{conj}	XL hybrid Sec. 4.2
2^{22}	64770	2735	104	2	$(0, 0)$	2	<u>103</u>
2^{20}	32771	1419	99	3	$(1159, 2)$	2	<u>98</u>
2^{18}	15336	760	95	3	$(657, 7)$	2	104
2^{16}	7391	389	91	4	$(373, 10)$	2	108
2^{14}	3482	198	86	6	$(197, 11)$	2	106
2^{12}	1589	98	83	8	$(88, 13)$	2	103
2^{10}	652	57	94	12	$(54, 9)$	2	101

Table 2. Hybrid approach of Section 4.2 over $\mathbb{F}_2$ (Modeling 2).

n	k	h	Best [34]	d_{conj} plain	(f, u)	d_{conj}	XL hybrid Sec. 4.2
2^{22}	64770	2735	108	2	$(0, 0)$	2	<u>104</u>
2^{20}	32771	1419	107	3	$(1246, 3)$	2	<u>102</u>
2^{18}	15336	760	105	3	$(670, 8)$	2	107
2^{16}	7391	389	103	4	$(374, 11)$	2	111
2^{14}	3482	198	101	6	$(197, 12)$	2	110
2^{12}	1589	98	100	8	$(96, 13)$	2	107
2^{10}	652	57	111	14	$(55, 10)$	2	111

Table 3. Hybrid approach of Section 4.2 over $\mathbb{F}_{2^{128}}$ (Modeling 1).

Ferret and Wolverine. We have also tested our methods on the parameters from [44] and [42]. While most of them seem resistant to the attack, a notable exception is the one-time parameter set with $|\mathbb{F}| = 2^{61}-1$, $n = 642048$, $k = 19870$ and $h = 2508$ from [42, Table 2]. The authors of [42] claim to achieve 128 bits of security whereas the more recent methods of [34] would suggest that this is too conservative. More precisely, [34, Provided script] estimates 154 bit security. Four our part, we estimate that plain Modeling 1 solves the problem with 126 bit complexity in degree $d = 3$.

5.1 Comments on the results

Overall, we see the complexity of our attack is rather close to the best attack even if clearly a bit above this value for most instances in Tables 2 and 3. In a way, the high witness degree for the plain system is circumvented by the hybrid component of our attack which can be seen as an analogue of Prange's algorithm. Therefore, we should not expect a big gap between the complexities in this case because our attack is not a pure algebraic attack. Also, this difference is much reduced in the parameters from Tables 4 and 5 (Larger Scale) compared to those of Tables 2 and 3 (Smaller Scale). We also observe that our attack is extremely efficient compared to ISD when we can solve at degree $2, 3$ without fixing a lot of variables (see for instance the first three rows in Tables 4 and 5). This may suggest a weak zone of parameters which is not encompassed by former ISD algorithms.

n	k	h	Best [34]	d_{conj} plain	(f,u)	d_{conj}	XL hybrid Sec. 4.2
2^{22}	64770	4788	147	2	$(0,0)$	2	103
2^{20}	32771	2467	143	3	$(2340,4)$	2	125
2^{18}	15336	1312	139	4	$(676,1)$	3	122
2^{16}	7391	667	135	5	$(604,7)$	2	139
2^{14}	3482	338	132	7	$(322,7)$	2	138
2^{12}	1589	172	131	11	$(154,7)$	2	135
2^{10}	652	106	176	19	$(104,4)$	3	145

Table 4. Hybrid approach of Section 4.2 over $\mathbb{F}_2$ (Modeling 2).

n	k	h	Best [34]	d_{conj} plain	(f,u)	d_{conj}	XL hybrid Sec. 4.2
2^{22}	64770	4788	156	3	$(4237,1)$	2	110
2^{20}	32771	2467	155	3	$(0,0)$	3	131
2^{18}	15336	1312	153	4	$(995,2)$	3	133
2^{16}	7391	667	151	6	$(613,8)$	2	150
2^{14}	3482	338	150	8	$(324,8)$	2	150
2^{12}	1589	172	155	12	$(157,8)$	2	150
2^{10}	652	106	194	24	$(105,5)$	3	179

Table 5. Hybrid approach of Section 4.2 over large field $\mathbb{F}_{2^{128}}$ (Modeling 1).

Secondly, the algebraic attack seems to compare better to known techniques for larger fields. As mentioned earlier, the main reason may be that the advantage of ISD algorithms over Prange/Pooled Gauss worsens when $|\mathbb{F}| \to +\infty$. In our case, even though the witness degree for plain Modeling 1 is slightly higher than the one of Modeling 2, the difference is not enough (at most 1 for all parameter sets except the last row in Tables 4 and 5) to expect a similar increase in the cost as we observe for ISD.

6 Asymptotic analysis

This section aims to illustrate the concrete results shown in Section 5 by providing a sketch of asymptotic analysis. Note that a study of convergence speed is out of the scope of this work, so the results presented here should be viewed as a purely theoretical contribution. Recall that our motivation for introducing the witness degree was to analyze the Wiedemann algorithm, which is likely to be the best tool for linear algebra for the parameters we have discussed so far. Since there are other linear algebra algorithms that may perform asymptotically better than the Wiedemann algorithm (see, e.g., [33]), we choose to focus on the degree of regularity for the remainder of this section. We start by exploring a potentially weak range of parameters where the RSD problem can be solved at degree 2. Then we go on to obtain an asymptotic equivalent of the degree of regularity in Section 6.2 for the plain system. All cases are considered over $\mathbb{F}_2$ using Modeling 2.

From this partial analysis, the next natural question would be to perform a broader comparison to known attacks, in particular to ISD algorithms. There is also the question of analyzing and comparing the hybrid versions of our attack. We leave both questions for future work.

6.1 Solving at low degree

First, note that the number of monomials in degree $\leq d$ in Modeling 2 can be well approximated by $\binom{h}{d}(\beta-1)^d$ which is the number of exact degree d monomials (see the discussion right after Lemma 1). Using Proposition 7 Appendix B.2, we see that the complexity is polynomial in the degree of regularity d_{reg}. In particular, having a constant d_{reg} is a sufficient condition for the algorithm to run in polynomial time. Moreover, we noted in Section 5.1 that our techniques proved especially effective when plain RSD was close to being solved at a small degree. Thus, we start our analysis by exploring the potentially weak zone of parameters where Modeling 2 meets the strong condition being solved at degree 2. This will happen whenever the coefficient in front of z^2 in the series $\mathcal{H}_{A/I_{\mathbb{F}_2}}(z)$ given in Equation (5) is non-positive. This coefficient reads

$$\kappa_2 := \tbinom{n-k+1}{2} + (\beta-1)^2\tbinom{h}{2} - (n-k)h(\beta-1).$$

In all generality, we can view this coefficient as a function of the length n, the code rate R and the error rate ρ and study the behaviour when $n \to +\infty$. More precisely, we get

$$\kappa_2 = \frac{n \cdot \left(\rho^3 n - 2nR\rho^2 + R^2\rho n - 1 + 3\rho - R\rho - \rho^2\right)}{2\rho}.$$

Note that if the code rate R dominates over ρ, the possibly dominant term in the numerator is either $R^2\rho n$ or -1. If the term $R^2\rho n$ tends to zero, the main contribution in the numerator comes from the -1 term and κ_2 is asymptotically negative. Note also that we can find such a zone which is non-trivial in a cryptographic sense. Indeed, recall that the standard adaptation of Prange's algorithm to the regular case would be to guess k/h error-free coordinates per block. The success probability of this approach is then $(1-k/h/n/h)^h = (1-R)^h$. This gives a complexity of $e^{-h\cdot\ln(1-R)}$, and assuming that $R = o(1)$ the main term in the exponent $-h\cdot\ln(1-R)$ is $hR = n\rho R$. If for instance $hR = n\rho R \sim n^\alpha$ for $0 < \alpha < 1$, it may give a subexponential algorithm. On the contrary, we can clearly find code rates for which $R^2\rho n \to 0$ under this condition.

To simplify the analysis even further, we consider particular functions $R = \phi(n)$ and $\rho = \psi(n)$ and view $\kappa_2 := \kappa(n)$ as a function of n. Upon inspection of Table 6, it seems relevant to study a regime of the form $\rho := n^{-a}$ and $R := \log(n)\cdot n^{-a}$ for some $0 < a < 1$ even if we extrapolate from a very small number of values. With this particular choice, we obtain

$$\kappa_2(n) = -\frac{n^{a+1}}{2} + \frac{(\log(n)-1)^2 n^{2-2a}}{2} + \frac{3n}{2} - \frac{(\log(n)+1)n^{1-a}}{2}. \tag{12}$$

Lemma 2. *Under Assumption 2, the degree of regularity of plain Modeling 2 for an RSD instance with $\rho := n^{-a}$ and $R := \log(n) \cdot n^{-a}$ is asymptotically equal to 2 when $a > 1/3$.* □

Proof. In Equation (12), the term $-\frac{n^{1+a}}{2}$ dominates when $a+1 > 2-2a$, hence $a > 1/3$. □

Recall that the Prange exponent is $nR\rho = n^{1-2a}\log(n)$ in this case, which leaves a possibly relevant zone for our attack when $1/3 < a < 1/2$.

Another choice of interest from Table 6 is $\rho := n^{-a}$ and $R := n^{-b}$ for some $0 < b < a$. In this case, we have

$$\kappa := \frac{n^{2-2a}}{2} + \frac{n^{2-2b}}{2} - n^{2-a-b} - \frac{n^{1+a}}{2} + \frac{3n}{2} - \frac{n^{1-a}}{2} - \frac{n^{1-b}}{2}. \tag{13}$$

Lemma 3. *Under Assumption 2, the degree of regularity of plain Modeling 2 for an RSD instance with $\rho := n^{-a}$ and $R := n^{-b}$ for some $0 < b < a$ is asymptotically equal to 2 when $a + 2b > 1$.*

Proof. In Equation (13), the dominant term is either $\frac{n^{2-2b}}{2}$ or $-\frac{n^{1+a}}{2}$. The second dominates when $1 + a > 2 - 2b$, that is, $a + 2b > 1$. □

In this case the Prange exponent is $nR\rho = n^{1-a-b}$, and there is a possibly relevant zone for our attack when $1 - b < a + b < 1$.

n	k	h	$b := 1 - \frac{\log(k)}{\log(n)}$	$a := 1 - \frac{\log(h)}{\log(n)}$	$R/(\log_2(n)\rho)$
2^{22}	64770	2735	0.27	0.48	1.08
2^{20}	32771	1419	0.25	0.48	1.15
2^{18}	15336	760	0.23	0.47	1.12
2^{16}	7391	389	0.20	0.46	1.19
2^{14}	3482	198	0.16	0.46	1.26
2^{12}	1589	98	0.11	0.45	1.35
2^{10}	652	57	0.07	0.42	1.14
2^{22}	64770	4788	0.27	0.44	0.61
2^{20}	32771	2467	0.25	0.44	0.66
2^{18}	15336	1312	0.23	0.42	0.65
2^{16}	7391	667	0.20	0.41	0.69
2^{14}	3482	338	0.16	0.40	0.74
2^{12}	1589	172	0.11	0.38	0.77
2^{10}	652	106	0.07	0.33	0.62

Table 6. General trends for the parameters of Section 5

6.2 Asymptotic analysis of $d_{\mathbf{reg}}$

A more accurate complexity analysis requires to estimate the degree of regularity d_{reg}, which is done in the following Proposition 6:

Proposition 6. *When $n \to +\infty$, the degree of regularity d_{reg} of Modeling 2 behaves asymptotically as follows:*

1. *For constant code rate R and noise rate $\rho = o(1)$, let $\kappa_R := 2-R-2\sqrt{1-R} > 0$. We have*

$$d_{reg} \sim \kappa_R h.$$

2. *For $R = o(1)$ and $\rho = o(1)$ such that $\rho = o(R)$, we have*

$$d_{reg} + 1 \sim \frac{R^2}{4} h.$$

3. *Finally, for $R = o(1)$ and $\rho = o(1)$ such that $\rho = \lambda R$ is linear in R with $\lambda < 1$, we have*

$$d_{reg} + 1 \sim \frac{(1-\lambda)^2 R^2}{4} h. \tag{14}$$

The main tool for the proof is the so-called saddle-point method. A detailed account of this approach in the context of Hilbert series can be found in [7, Chap. 4]. Each coefficient in the series can be obtained as a Cauchy integral, namely

$$[z^d]\mathcal{H}_{A/I_{\mathbb{F}_2}}(z) = \frac{1}{2i\pi} \oint \frac{1}{z^{d+1}} \mathcal{H}_{A/I_{\mathbb{F}_2}}(z) dz.$$

The saddle-point method allows to study the asymptotic behaviour of this integral for fixed d. Since we are interested in the value of d such that the integral vanishes when $n \to +\infty$, we then cancel the main term in the resulting development in order to obtain the first term in the development of d_{reg}. The full proof can be found in Appendix D.

Asymptotics with hybrid approach. It is possible to carry out the same analysis for the system obtained after hybrid approach but this is more technical. We leave this problem as a future work. In this case, the relevant question would be to find the best asymptotic trade-off between the cost coming from the fixed variables and the one of the solving step. This has already been studied in the case of quadratic semi-regular systems, see for instance [15, §4.3].

Acknowledgments. We express our warm gratitude to the Eurocrypt23' reviewers for their suggestion to analyze the witness degree. We also thank Geoffroy Couteau for motivating the study of this problem and for insightful discussions.

References

1. Aguilar-Melchor, C., Blazy, O., Deneuville, J.C., Gaborit, P., Zémor, G.: Efficient Encryption From Random Quasi-Cyclic Codes. IEEE Transactions on Information Theory **64**(5), 3927–3943 (2018). https://doi.org/10.1109/TIT.2018.2804444
2. Albrecht, M., Cid, C., Faugère, J.C., Fitzpatrick, R., Perret, L.: On the complexity of the Arora-Ge Algorithm against LWE. In: SCC 2012 – Third international conference on Symbolic Computation and Cryptography. pp. 93–99. Castro Urdiales, Spain (Jul 2012), https://hal.inria.fr/hal-00776434
3. Albrecht, M.R., Cid, C., Faugère, J.C., Perret, L.: Algebraic Algorithms for LWE. Cryptology ePrint Archive, Paper 2014/1018 (2014), https://eprint.iacr.org/2014/1018
4. Applebaum, B., Damgård, I., Ishai, Y., Nielsen, M., Zichron, L.: Secure Arithmetic Computation with Constant Computational Overhead. In: Katz, J., Shacham, H. (eds.) Advances in Cryptology – CRYPTO 2017. pp. 223–254. Springer International Publishing, Cham (2017)
5. Arora, S., Ge, R.: New Algorithms for Learning in Presence of Errors. In: Aceto, L., Henzinger, M., Sgall, J. (eds.) Automata, Languages and Programming. pp. 403–415. Springer Berlin Heidelberg, Berlin, Heidelberg (2011)
6. Augot, D., Finiasz, M., Sendrier, N.: A Family of Fast Syndrome Based Cryptographic Hash Functions. In: Dwason, Ed, Vaudenay, Serge (eds.) MYCRYPT 2005 : First International Conference on Cryptology in Malaysia. Lecture Notes in Computer Science, vol. 3715, pp. 64–83. Springer, Kuala Lumpur, Malaysia (Sep 2005). https://doi.org/10.1007/11554868_6, https://hal.inria.fr/inria-00509188
7. Bardet, M.: Étude des systèmes algébriques surdéterminés. Applications aux codes correcteurs et à la cryptographie. Theses, Université Pierre et Marie Curie - Paris VI (Dec 2004), https://tel.archives-ouvertes.fr/tel-00449609
8. Bardet, M., Faugère, J.C., Salvy, B., Spaenlehauer, P.J.: On the complexity of solving quadratic Boolean systems. Journal of Complexity **29**(1), 53–75 (2013)
9. Bardet, M., Faugère, J.C., Salvy, B., Yang, B.Y.: Asymptotic behaviour of the index of regularity of quadratic semi-regular polynomial systems. In: The Effective Methods in Algebraic Geometry Conference (MEGA'05)(P. Gianni, ed.). pp. 1–14 (2005)
10. Baum, C., Braun, L., Munch-Hansen, A., Razet, B., Scholl, P.: Appenzeller to Brie: Efficient Zero-Knowledge Proofs for Mixed-Mode Arithmetic and Z2k. In: Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security. p. 192–211. CCS '21, Association for Computing Machinery, New York, NY, USA (2021), https://doi.org/10.1145/3460120.3484812
11. Baum, C., Braun, L., Munch-Hansen, A., Scholl, P.: Moz$\mathbb{Z}_{2^k}$arella: Efficient Vector-OLE and Zero-Knowledge Proofs Over $\mathbb{Z}_{2^k}$. In: Dodis, Y., Shrimpton, T. (eds.) Advances in Cryptology – CRYPTO 2022. pp. 329–358. Springer Nature Switzerland, Cham (2022)
12. Becker, A., Joux, A., May, A., Meurer, A.: Decoding Random Binary Linear Codes in 2n/20: How $1+1=0$ Improves Information Set Decoding. In: Pointcheval, D., Johansson, T. (eds.) Advances in Cryptology – EUROCRYPT 2012. pp. 520–536. Springer Berlin Heidelberg, Berlin, Heidelberg (2012)
13. Bernstein, D.J., Buchmann, J., Dahmen, E.: Post-Quantum Cryptography. Springer, Dordrecht (2008). https://doi.org/10.1007/978-3-540-88702-7, https://cds.cern.ch/record/1253241

14. Bernstein, D.J., Lange, T., Peters, C.: Smaller Decoding Exponents: Ball-Collision Decoding. In: Rogaway, P. (ed.) Advances in Cryptology – CRYPTO 2011. pp. 743–760. Springer Berlin Heidelberg, Berlin, Heidelberg (2011)
15. Bettale, L.: Cryptanalyse algébrique : outils et applications. Ph.D. thesis, Université Pierre et Marie Curie - Paris 6 (2012)
16. Bettale, L., Faugère, J.C., Perret, L.: Hybrid approach for solving multivariate systems over finite fields. Journal of Mathematical Cryptology **3**(3), 177–197 (Jan 2010). https://doi.org/10.1515/jmc.2009.009, https://hal.archives-ouvertes.fr/hal-01148127
17. Beullens, W.: Improved Cryptanalysis of UOV and Rainbow. In: Canteaut, A., Standaert, F.X. (eds.) Advances in Cryptology – EUROCRYPT 2021. pp. 348–373. Springer International Publishing, Cham (2021)
18. Boyle, E., Couteau, G., Gilboa, N., Ishai, Y.: Compressing Vector OLE. In: Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security. p. 896–912. CCS '18, Association for Computing Machinery, New York, NY, USA (2018), https://doi.org/10.1145/3243734.3243868
19. Boyle, E., Couteau, G., Gilboa, N., Ishai, Y., Kohl, L., Rindal, P., Scholl, P.: Efficient Two-Round OT Extension and Silent Non-Interactive Secure Computation. In: Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security. p. 291–308. CCS '19, Association for Computing Machinery, New York, NY, USA (2019), https://doi.org/10.1145/3319535.3354255
20. Boyle, E., Couteau, G., Gilboa, N., Ishai, Y., Kohl, L., Scholl, P.: Efficient Pseudorandom Correlation Generators: Silent OT Extension and More. In: Boldyreva, A., Micciancio, D. (eds.) Advances in Cryptology – CRYPTO 2019. pp. 489–518. Springer International Publishing, Cham (2019)
21. Boyle, E., Couteau, G., Gilboa, N., Ishai, Y., Kohl, L., Scholl, P.: Efficient Pseudorandom Correlation Generators from Ring-LPN. In: Micciancio, D., Ristenpart, T. (eds.) Advances in Cryptology – CRYPTO 2020. pp. 387–416. Springer International Publishing, Cham (2020)
22. Canto Torres, R.: Asymptotic analysis of ISD algorithms for the $q-$ary case. In: Proceedings of the Tenth International Workshop on Coding and Cryptography WCC 2017 (Sep 2017), http://wcc2017.suai.ru/Proceedings{_}WCC2017.zip
23. Carrier, K., Debris-Alazard, T., Meyer-Hilfiger, C., Tillich, J.P.: Statistical decoding 2.0: Reducing decoding to LPN. In: Advances in Cryptology–ASIACRYPT 2022: 28th International Conference on the Theory and Application of Cryptology and Information Security, Taipei, Taiwan, December 5–9, 2022, Proceedings, Part IV. pp. 477–507. Springer (2022)
24. Cheng, C.M., Chou, T., Niederhagen, R., Yang, B.Y.: Solving Quadratic Equations with XL on Parallel Architectures. In: Proceedings of the 14th International Conference on Cryptographic Hardware and Embedded Systems. p. 356–373. CHES'12, Springer-Verlag, Berlin, Heidelberg (2012), https://doi.org/10.1007/978-3-642-33027-8_21
25. Coppersmith, D.: Solving Homogeneous Linear Equations over GF(2) via Block Wiedemann Algorithm. Mathematics of Computation **62**(205), 333–350 (jan 1994), https://doi.org/10.2307/2153413
26. Courtois, N., Klimov, A., Patarin, J., Shamir, A.: Efficient Algorithms for Solving Overdefined Systems of Multivariate Polynomial Equations. In: Preneel, B. (ed.) Advances in Cryptology — EUROCRYPT 2000. pp. 392–407. Springer Berlin Heidelberg, Berlin, Heidelberg (2000)

27. Esser, A., Kübler, R., May, A.: LPN decoded. In: Katz, J., Shacham, H. (eds.) Advances in Cryptology - CRYPTO 2017 - 37th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 20-24, 2017, Proceedings, Part II. Lecture Notes in Computer Science, vol. 10402, pp. 486–514. Springer (2017). https://doi.org/10.1007/978-3-319-63715-0_17
28. Finiasz, M., Sendrier, N.: Security Bounds for the Design of Code-Based Cryptosystems. In: Advances in Cryptology - ASIACRYPT 2009, 15th International Conference on the Theory and Application of Cryptology and Information Security, Tokyo, Japan, December 6-10, 2009. Proceedings. Lecture Notes in Computer Science, vol. 5912, pp. 88–105. Springer (2009), https://www.iacr.org/archive/asiacrypt2009/59120082/59120082.pdf
29. Flajolet, P., Sedgewick, R.: Analytic Combinatorics. Cambridge University Press (2009), http://www.cambridge.org/uk/catalogue/catalogue.asp?isbn=9780521898065
30. Fröberg, R.: An inequality for Hilbert series of graded algebras. MATHEMATICA SCANDINAVICA **56**, 117–144 (Dec 1985). https://doi.org/10.7146/math.scand.a-12092, https://www.mscand.dk/article/view/12092
31. Hazay, C., Orsini, E., Scholl, P., Soria-Vazquez, E.: TinyKeys: A New Approach to Efficient Multi-Party Computation. In: Advances in Cryptology – CRYPTO 2018. Lecture Notes in Computer Science, vol. 10993, pp. 3–33. Springer (2018)
32. Jabri, A.K.A.: A Statistical Decoding Algorithm for General Linear Block Codes. In: Honary, B. (ed.) Cryptography and Coding, 8th IMA International Conference, Cirencester, UK, December 17-19, 2001, Proceedings. Lecture Notes in Computer Science, vol. 2260, pp. 1–8. Springer (2001), https://doi.org/10.1007/3-540-45325-3_1
33. Le Gall, F.: Powers of Tensors and Fast Matrix Multiplication. In: Proceedings of the 39th international symposium on symbolic and algebraic computation. pp. 296–303 (2014)
34. Liu, H., Wang, X., Yang, K., Yu, Y.: The Hardness of LPN over Any Integer Ring and Field for PCG Applications. Cryptology ePrint Archive, Paper 2022/712 (2022), https://eprint.iacr.org/2022/712
35. May, A., Meurer, A., Thomae, E.: Decoding Random Linear Codes in $\tilde{\mathcal{O}}(2^{0.054n})$. In: ASIACRYPT. Lecture Notes in Computer Science, vol. 7073, pp. 107–124. Springer (2011), https://www.iacr.org/archive/asiacrypt2011/70730106/70730106.pdf
36. May, A., Ozerov, I.: On Computing Nearest Neighbors with Applications to Decoding of Binary Linear Codes. In: Oswald, E., Fischlin, M. (eds.) Advances in Cryptology – EUROCRYPT 2015. pp. 203–228. Springer Berlin Heidelberg, Berlin, Heidelberg (2015)
37. Misoczki, R., Tillich, J.P., Sendrier, N., Barreto, P.S.L.M.: MDPC-McEliece: New McEliece variants from Moderate Density Parity-Check codes. In: 2013 IEEE International Symposium on Information Theory. pp. 2069–2073 (2013). https://doi.org/10.1109/ISIT.2013.6620590
38. Prange, E.: The use of information sets in decoding cyclic codes. IRE Transactions on Information Theory **8**(5), 5–9 (1962). https://doi.org/10.1109/TIT.1962.1057777
39. Stern, J.: A method for finding codewords of small weight. In: Cohen, G., Wolfmann, J. (eds.) Coding Theory and Applications. pp. 106–113. Springer Berlin Heidelberg, Berlin, Heidelberg (1989)

40. Sun, C., Tibouchi, M., Abe, M.: Revisiting the Hardness of Binary Error LWE. In: Liu, J.K., Cui, H. (eds.) Information Security and Privacy. pp. 425–444. Springer International Publishing, Cham (2020)
41. Thomé, E.: Subquadratic Computation of Vector Generating Polynomials and Improvement of the Block Wiedemann Algorithm. Journal of symbolic computation **33**(5), 757–775 (2002), https://doi.org/10.1006/jsco.2002.0533
42. Weng, C., Yang, K., Katz, J., Wang, X.: Wolverine: Fast, Scalable, and Communication-Efficient Zero-Knowledge Proofs for Boolean and Arithmetic Circuits. In: 42nd IEEE Symposium on Security and Privacy, SP 2021, San Francisco, CA, USA, 24-27 May 2021. pp. 1074–1091. IEEE (2021), https://doi.org/10.1109/SP40001.2021.00056
43. Wiedemann, D.: Solving sparse linear equations over finite fields. IEEE Transactions on Information Theory **32**(1), 54–62 (1986). https://doi.org/10.1109/TIT.1986.1057137
44. Yang, K., Weng, C., Lan, X., Zhang, J., Wang, X.: Ferret: Fast Extension for Correlated OT with Small Communication. In: Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security. p. 1607–1626. CCS '20, Association for Computing Machinery, New York, NY, USA (2020), https://doi.org/10.1145/3372297.3417276

A Proof of Theorems 1 and 2

This section contains the proofs of Theorem 1 and Theorem 2. Our main contribution is the strategy of splitting the system into two parts as described above. The structural part requires to compute some Hilbert series $\mathcal{H}_S(z)$ (resp. $\mathcal{H}_{S'}(z)$). On the rest of the equations, most of the technical work as explained in the main text was to state Assumption 1 (resp. Assumption 2) in order to mimick Bardet's definitions of semi-regularity (resp. semi-regularity over $\mathbb{F}_2$). From there, this structure of the proof is exactly the same as in [7, §3.3.2,§3.3.3].

A.1 Proof of Theorem 1

The theorem easily follows from the following lemmata.

Lemma 4. *Let S denote the quotient ring $A/\langle \mathcal{B}^{(h)} \rangle$, where $\mathcal{B}^{(h)}$ consists of the quadratic parts of the structural equations from Modeling 1. We have*

$$\mathcal{H}_S(z) = \left(1 + \beta \cdot \tfrac{z}{1-z}\right)^h. \tag{15}$$

Proof. The quotient S can be seen as the set of polynomials whose monomials involve at most one $e_{i,j}$ variable in each block $1 \leq i \leq h$. For a given block, admissible monomials have only one variable but their degree can be arbitrary. Therefore, the Hilbert series "for one block" will be $1+\beta\cdot\frac{z}{1-z}$. Finally, a general d monomial is a product of such monomials for distinct blocks and such that the sum of their degrees is equal to d. Relying on the same symbolic argument as presented in [29] which gives the generating series of a Cartesian product, we finally obtain the series in (15). □

Lemma 5. *Let I denote the homogeneous ideal associated to Modeling 1. Under Assumption 1, we have*

$$\mathcal{H}_{A/I}(z) = \left[(1-z)^{n-k} \cdot \mathcal{H}_S(z)\right]^+ .$$

Proof. This may be seen as a particular case of [7, §3.3.2]. We give the proof here for the sake of completeness. To simplify notation, we write $\{f_1, \ldots, f_{n-k}\}$ for the set of homogeneous parity-check equations $\mathcal{P}^{(h)}$. For $1 \leq j \leq n-k$, we denote by $I(j)$ the ideal $\langle \mathcal{B}^{(h)}, f_1, \ldots, f_j \rangle$ in A and $I(0) = \langle \mathcal{B}^{(h)} \rangle$. For $1 \leq j \leq n-k$ and up to the degree of regularity of I, Assumption 1 states that we have the exact sequence of vector spaces when $d < d_{\text{reg}}$:

$$0 \to (A/I(j-1))_{d-1} \to (A/I(j-1))_d \to (A/I(j))_d \to 0$$

This gives the following equality between Hilbert functions

$$\mathcal{HF}_{A/I(j-1)}(d-1) - \mathcal{HF}_{A/I(j-1)}(d) + \mathcal{HF}_{A/I(j)}(d) = 0. \tag{16}$$

Consider now the abstract sequence $h_{d,j}$ defined by $h_{d,j} = \dim_{\mathbb{F}}(S_d)$ if $j = 0$ or $d = 0$ and the induction relation

$$h_{d,j} = h_{d,j-1} - h_{d-1,j-1}. \tag{17}$$

Let $\mathcal{G}_j$ denote the generating series for $(h_{d,j})_{d \geq 0}$. From Equation (17) and by multiplying by z we easily obtain $\mathcal{G}_j(z) = (1-z)\mathcal{G}_{j-1}(z)$. The generating series for $(h_{d,0})_{d \geq 0}$ being $\mathcal{G}_0(z) := \mathcal{H}_S(z)$ we get $\mathcal{G}_{n-k}(z) = (1-z)^{n-k}\mathcal{H}_S(z)$. As long as the involved quantities are positive, Equation (16) and Equation (17) may be seen as the same relation. Therefore, the final Hilbert series is

$$\mathcal{H}_{A/I}(z) = \left[(1-z)^{n-k} \cdot \mathcal{H}_S(z)\right]_+ .$$

□

A.2 Proof of Theorem 2

Recall A' and S' from Definition 7. Theorem 2 easily follows from the following lemmata.

Lemma 6. *We have*

$$\mathcal{H}_{S'}(z) = (1 + (\beta - 1) \cdot z)^h . \tag{18}$$

Proof. From the set of generators $\mathcal{G}$ described in Lemma 1, we observe that the admissible monomials of S' involve at most one variable from each block, with degree at most 1. The result follows by reasoning in a similar way as in the proof of Lemma 4. □

Lemma 7. *Let I denote the homogeneous ideal associated to Modeling 2. Under Assumption 2, we have*

$$\mathcal{H}_{A/I}(z) = \left[\mathcal{H}_{S'}(z)/(1+z)^{n-k}\right]_+ .$$

Proof (sketch). By construction, we clearly have $\mathcal{H}_{A/I}(z) = \mathcal{H}_{A'/I'}(z)$, for the ideal I' introduced in Definition 7. As in the proof of Lemma 5, we simplify notation by writing $\{f_1, \ldots, f_{n-k}\}$ for the set of homogeneous parity-check equations $\mathcal{L}(\mathcal{P}^{(h)})$, and for $1 \leq j \leq n-k$, we denote by $I'(j)$ the ideal $\langle \mathcal{B}', \mathcal{Q}', f_1, \ldots, f_j \rangle$ in A' and $I'(0) = \langle \mathcal{B}', \mathcal{Q}' \rangle$. Assumption 2 ensures that the following sequence is exact for $d < d_{\text{reg}}$.

$$0 \to (A'/I'(j))_{d-1} \xrightarrow{\times f_j} (A'/I'(j-1))_d \xrightarrow{\pi} (A'/I'(j))_d \to 0.$$

The rest of the proof now proceeds in the same way as [9, proof of Proposition 9], starting from the equality between Hilbert functions

$$\mathcal{HF}_{A'/I'(j)}(d-1) - \mathcal{HF}_{A'/I'(j-1)}(d) + \mathcal{HF}_{A'/I'(j)}(d) = 0. \tag{19}$$

Similarly, we consider the sequence $c_{d,j}$ defined by $c_{d,j} = \dim_{\mathbb{F}}(S'_d)$ if $j = 0$ or $d = 0$ and the recurrent formula

$$c_{d,j} = c_{d,j-1} - c_{d-1,j}. \tag{20}$$

Let $\mathcal{C}_j$ denote the generating series for $(c_{d,j})_{d \geq 0}$. Multiplying by z in Equation (20) yields $(1+z)\mathcal{C}_j(z) = \mathcal{C}_{j-1}(z)$ and we have the border condition $\mathcal{C}_0(z) = \mathcal{H}_{A'/I'(0)}(z) = \mathcal{H}_{S'}(z)$. This finally gives

$$\mathcal{H}_{A/I}(z) = \mathcal{H}_{A'/I'}(z) = \left[\frac{\mathcal{H}_{S'}(z)}{(1+z)^{n-k}} \right]_+ .$$

□

B Missing details in Section 4

B.1 Regularity assumption for specialized Modeling 1

For any invertible matrix $\boldsymbol{P}$, for $0 \leq f \leq h$ and for $0 \leq u \leq \beta$, let $\overline{\mathbf{P}^{-1}_{u,f}}$ denote the map that applies $\mathbf{P}^{-1}$ and then fixes the initial u variables to 0 in the last f blocks of the error.

Assumption 3 *Let $\mathcal{P}$ be the set of parity-check equations from an instance of Modeling 1. For every permutation matrix $\mathbf{P}$ which stabilizes each block of the error, for $0 \leq f \leq h$ and for $0 \leq u \leq \beta$, we assume $\mathcal{P}^{(h)} \circ \overline{\mathbf{P}^{-1}_{u,f}}$ satisfies Assumption 1 with ring $A \circ \overline{\mathbf{P}^{-1}_{u,f}}$ and quotient ring $S \circ \overline{\mathbf{P}^{-1}_{u,f}}$.*

We need the full version of this assumption for the approach of Section 4.2 while only the particular case $f = h$ is required for Section 4.1.

B.2 XL Wiedemann complexity for Modeling 2

The success probability $\mathcal{P}_{(f,u)} := (1-u/\beta)^f$ is independent of the algebraic system. Over $\mathbb{F}_2$, we may consider that $n_\mu \approx \frac{k}{2}+1$ in general instead of simply $n_\mu \leq k+1$ for the number of non-zero terms per equation. We leave it to the reader to state the equivalent of Assumption 3 for Modeling 2. All the following results are under this assumption, as well as the assumptions noted in Section 4.3. We now give the complexity of the hybrid approach of Section 4.2 on Modeling 2. The degree of regularity $d_{\mathrm{reg},(f,u)}$ is obtained as the index of the first non-positive coefficient in the series

$$\frac{(1+(\beta-1-u)\cdot z)^f \cdot (1+(\beta-1)\cdot z)^{h-f}}{(1+z)^{n-k}} \tag{21}$$

As noted in Section 4.3, this series is divided by $(1-z)$, to derive an upper bound, $d_{\mathrm{wit},(f,u)}$, on the witness degree. Finally, the analogue of Equation (11) is

$$\mathcal{M}^{(f,u)}_{\leq d_{\mathrm{wit},(f,u)}} = \sum_{j=0}^{d_{\mathrm{wit},(f,u)}} [z^j]\left(\mathcal{H}_{(S',f,u)}(z)\right),$$

where $\mathcal{H}_{(S',f,u)}(z) := (1+(\beta-1-u)\cdot z)^f \cdot (1+(\beta-1)\cdot z)^{h-f}$.

Proposition 7. *The time complexity in $\mathbb{F}_2$ operations of the hybrid approach of Section 4.2 on Modeling 2 is estimated by*

$$\mathcal{O}\left(\min_{\substack{0\leq f\leq h\\ 0\leq u\leq \beta}}\left(\mathcal{P}^{-1}_{(f,u)}\cdot 3\cdot n_{\mu,(f,u)}\cdot\left(\mathcal{M}^{(f,u)}_{\leq d_{\mathrm{wit},(f,u)}}\right)^2\right)\right).$$

C Experiments

In this section, we present experiments that we have run on randomly generated instances of the RSD problem in order to check the validity of the assumptions from Section 3 and 4.

C.1 Hilbert series

We give the parameter sets as $(h,\beta,k,f,u)_t$, where h,β and k describe the RSD problem, where f,u are the parameters for the hybrid approach of Section 4.2 and where t is the number of times that we have repeated the experiment. For an affine ideal I, we compute the Hilbert series of the ideal $I^{(h)}$ associated with the homogeneous upper part of I. For some of the hybrid systems, we have also computed the Hilbert series of the *homogenized* ideal $I^{(y)}$ (see Section 2.1 for the difference between these two notions). The tests have been run using the computer algebra system Magma V2.27-1 and the built-in command `HilbertSeries`$(\cdot)$.

Experiments for Modeling 1. The systems we have tested for Modeling 1 are listed in Table 7, where we also give the associated degree of regularity d_{reg}. In all tests, the experimentally found Hilbert series is equal to the Hilbert series of Equation (9), meaning, in particular, that Assumption 1 and 3 have been true in all our experiments. For most of the hybrid systems, we have also computed the Hilbert series of the homogenized ideals $I^{(y)}$ and given the associated degree of regularity $d_{\text{reg}}^{(y)}$. The Hilbert series in all of these tests have been equal to (the truncation of) those predicted by Equation (10).

System	d_{reg}	$d_{\text{reg}}^{(y)}$	System	d_{reg}	$d_{\text{reg}}^{(y)}$	System	d_{reg}	$d_{\text{reg}}^{(y)}$
$(5,6,15,0,0)_5$	3	-	$(5,6,20,0,0)_5$	4	-	$(5,8,20,0,0)_5$	3	-
$(5,8,30,0,0)_5$	4	-	$(7,7,30,0,0)_5$	4	-	$(8,6,30,0,0)_5$	5	-
$(10,4,25,0,0)_5$	6	-	$(12,7,50,3,2)_1$	5	-	$(7,8,30,2,3)_{10}$	3	3
$(7,8,30,6,3)_{10}$	2	3	$(10,7,40,5,2)_{10}$	4	4	$(10,7,40,5,3)_{10}$	3	4

Table 7. Tested Hilbert Series from Hybrid Modeling 1 systems over $\mathbb{F}_{101}$.

Experiments for Modeling 2. Table 8 contains tests for Hilbert series on Modeling 2. The experimental Hilbert series of the plain cases ($f = u = 0$) are all described by our theory. While the majority of *hybrid* cases we have tested are accurately described by (21), we have been able to find a few discrepancy with the theoretical values. The systems marked by † both included a single case where the experimental Hilbert series deviated slightly from (21) in one of its terms. The system marked by ‡ was another type of outlier, where the quotient A/I contained a few cubic elements in half of the tested cases. We note that for the system marked by ‡, the corresponding (untruncated) series (21) is exactly zero at term z^2. Thus the homogeneous Macaulay matrix of degree 2 will be a square matrix over $\mathbb{F}_2$ (after removing trivial syzygies), and the quotient A/I will contain cubic terms whenever this matrix fails to be of full rank. For the other tested cases, the series have a *negative* coefficient at the term corresponding to the degree of regularity, indicating that the homogeneous Macaulay matrices will be rectangular. We believe that this difference explains the peculiar behaviour observed for case ‡. Finally, we have performed the same experiments as in Modeling 1 for the ideals $I^{(y)}$ and we obtained the same conclusive results regarding Equation (10).

C.2 Witness degree for plain systems

We have also tested the witness degree for (non-hybrid) systems of Modeling 1. In these tests, we have created the affine Macaulay matrix of degree 2 or 3 and then computed its rank to check if it has a unique solution. The witness degree in all these tests was the same as the value estimated by Equation (6) in Section 3.2. Details are given in Table 9, where the systems are denoted (h, β, k).

System	d_{reg}	$d_{\text{reg}}^{(y)}$	System	d_{reg}	$d_{\text{reg}}^{(y)}$	System	d_{reg}	$d_{\text{reg}}^{(y)}$
$(10,6,30,0,0)_{10}$	3	-	$(10,6,30,3,3)_{10}$	2	2	$(10,6,40,0,0)_{10}$	4	-
$(10,6,40,6,2)_{10}^{\dagger}$	3	-	$(14,7,50,0,0)_{10}$	4	-	$(14,7,50,2,2)_{10}$	3	4
$(14,7,50,10,2)_{10}$	$2^{\ddagger}$	3	$(15,6,70,10,3)_{10}^{\dagger}$	5	-	$(20,6,70,5,3)_{10}$	4	4
$(20,6,70,10,3)_{10}$	3	3	$(15,6,60,2,1)_{1}$	5	-	$(20,20,150,0,0)_{1}$	3	-
$(20,20,150,15,4)_{10}$	2	3	$(20,20,100,0,0)_{10}$	2	-			

Table 8. Tested Hilbert Series from Hybrid Modeling 2 systems over $\mathbb{F}_2$.

System	d_{wit}	System	d_{wit}	System	d_{wit}	System	d_{wit}
$(8,8,18)$	2	$(4,12,21)$	2	$(15,8,27)$	2	$(12,7,20)$	2
$(7,5,16)$	3	$(8,4,13)$	3	$(4,8,20)$	3	$(8,5,18)$	3

Table 9. Witness degree for Modeling 1 systems over $\mathbb{F}_{101}$.

D Proof of Proposition 6

Proof. The starting point is the Cauchy integral

$$\mathcal{I}_d(n) := \frac{1}{2i\pi}\int \underbrace{\frac{1}{z^{d+1}}\frac{(1+(\beta-1)\cdot z)^h}{(1+z)^{n-k}}}_{=e^{n\cdot f(z)}} dz,$$

where we set $f(z) := -\dfrac{d+1}{n}\cdot\log(z)-(1-R)\cdot\log(1+z)+\rho\cdot\log(1+(\rho^{-1}-1)\cdot z)$.

We study the behaviour of this integral when n grows. Using Cauchy's integral theorem, we can make the path of integration to meet the saddle points so that the integral concentrates in the neighborhood of these saddle points when n tends to $+\infty$. These saddle points are solutions to the equation

$$zf'(z) = -\frac{d+1}{n} - (1-R)\cdot\frac{z}{1+z} + (1-\rho)\,\frac{z}{1+(\rho^{-1}-1)\cdot z} = 0.$$

It may be be rewritten as a quadratic equation $P(z) = p_2\cdot z^2 + p_1\cdot z + p_0 = 0$, where

$$\begin{aligned} p_2 &:= (\rho-1)\cdot(d+1+(1-R-\rho)n)\,,\\ p_1 &:= \rho R n - n\rho^2 - d - 1,\\ p_0 &:= -\rho\cdot(d+1). \end{aligned}$$

Then, the standard argument is that P must have a double root, *i.e.* the saddle points have to *coalesce* (otherwise the integral is exponential, see for example [7, p. 94], [3, A.1.] for details). Writing that the discriminant $\Delta(P)$ is equal to zero

yields a quadratic equation $A \cdot d^2 + B \cdot d + C = 0$, where

$$A := (2\rho - 1)^2,$$
$$B := -4R\rho^2 n - 4\rho^3 n + 2R\rho n + 10n\rho^2 - 4\rho n + 8\rho^2 - 8\rho + 2,$$
$$C := R^2\rho^2 n^2 + \rho^4 n^2 - 2R\rho^3 n^2 - 4R\rho^2 n - 4\rho^3 n + 2R\rho n + 10n\rho^2 - 4n\rho + (2\rho - 1)^2.$$

Solving for d gives

$$\begin{aligned} d &= \frac{-R\rho n - \rho^2 n + 2n\rho - 2\rho + 1 \pm \sqrt{\delta}}{1 - 2\rho} \\ &= -1 + \frac{\rho n \left(\pm 2\sqrt{1-R}\sqrt{1-\rho} + 2 - \rho - R\right)}{1 - 2\rho}, \end{aligned} \tag{22}$$

where $\sqrt{\delta} := 2n\sqrt{R\rho^3 - R\rho^2 - \rho^3 + \rho^2} = 2n\rho\sqrt{1-R}\sqrt{1-\rho}$. We want the smallest positive root which is given by the minus case of $\pm\sqrt{\delta}$, in the equation above. The end of the proof then consists in studying Equation (22) in the different regimes:

- For constant code rate R and $\rho = o(1)$, we obtain

$$-2\sqrt{1-R}\sqrt{1-\rho} + 2 - \rho - R = (2 - R) - 2\sqrt{1-R} + o(1),$$

  hence $d_{\text{reg}} \sim \kappa_R h$, where $\kappa_R := (2 - R) - 2\sqrt{1-R} > 0$.
- For $R = o(1)$ and $\rho = o(1)$ we have

$$\begin{aligned} -2\sqrt{1-R}\sqrt{1-\rho} &= -2\left(1 - \tfrac{R}{2} - \tfrac{R^2}{8} + o(R^2)\right)\left(1 - \tfrac{\rho}{2} - \tfrac{\rho^2}{8} + o(\rho^2)\right) \\ &= -2 + R + \rho + \tfrac{R^2}{4} + \tfrac{\rho^2}{4} - \tfrac{R\rho}{2} + o(R\rho), \end{aligned}$$

  hence $-2\sqrt{1-R}\sqrt{1-\rho} + 2 - \rho - R = \frac{R^2}{4} + \frac{\rho^2}{4} - \frac{R\rho}{2} + o(R\rho)$. This gives us $d_{\text{reg}} + 1 \sim \frac{R^2}{4} h$ if $r = o(R)$ and $d_{\text{reg}} + 1 \sim \frac{R^2}{4}(1-\lambda)^2 h$ if $\rho = \lambda R$ is linear in R with $\lambda < 1$.

□