

# Analysis of Multivariate Encryption Schemes: Application to Dob and $C^*$

Morten Øygaard<sup>1</sup>, Patrick Felke<sup>2</sup>, and Håvard Raddum<sup>1</sup>

<sup>1</sup> Simula UiB, Bergen, Norway

<sup>2</sup> University of Applied Sciences Emden/Leer, Emden, Germany  
{morten.oygarden,haavardr}@simula.no,  
patrick.felke@hs-emden-leer.de,

**Abstract.** A common strategy for constructing multivariate encryption schemes is to use a central map that is easy to invert over an extension field, along with a small number of modifications to thwart potential attacks. In this work we study the effectiveness of these modifications, by deriving estimates for the number of degree fall polynomials. After developing the necessary tools, we focus on encryption schemes using the  $C^*$  and Dobbertin central maps, with the internal perturbation (*ip*), and  $Q_+$  modifications. For these constructions we are able to accurately predict the number of degree fall polynomials produced in a Gröbner basis attack, up to and including degree five for the Dob encryption scheme and four for  $C^*$ . The predictions remain accurate even when fixing variables. Based on this new theory we design a novel attack on Dob, which completely recovers the secret key for the parameters suggested by its designers. Due to the generality of the presented techniques, we also believe that they are of interest to the analysis of other big field schemes.

## 1 Introduction

Public key cryptography has played a vital role in securing services on the internet that we take for granted today. The security of schemes based on integer factorization and the discrete logarithm problem (DLP) is now well understood, and the related encryption algorithms have served us well over several decades.

In [32] it was shown that quantum computers can solve both integer factorization and DLP in polynomial time. While large scale quantum computers that break the actual implementations of secure internet communication are not here yet, progress is being made in constructing them. This has led the community for cryptographic research to look for new public key primitives that are based

---

© IACR 2024. This article is the final version submitted by the authors to the IACR and to Springer-Verlag on 15.03.2024. The version published by Springer-Verlag is available at DOI: 10.1007/s00145-024-09501-w. The article is a substantially extended version of [44] (PKC 2021), where the differences are summarized at page three.

on mathematical problems believed to be hard even for quantum computers, so called *post-quantum cryptography*.

In 2016 NIST launched a project aimed at standardizing post-quantum public key primitives [29]. A call for proposals was made and many candidate schemes were proposed. The candidates are based on a variety of problems, including the shortest vector problem for lattices, the problem of decoding a random linear code, or the problem of solving a system of multivariate quadratic equations over a finite field (the MQ problem).

The basic idea for big-field encryption schemes based on the MQ problem is to construct them around a central mapping  $F(X)$  defined over a large finite field  $\mathbb{F}_{q^d}$  that is easy to invert. By using a vector space isomorphism between  $\mathbb{F}_{q^d}$  and  $\mathbb{F}_q^d$ , the mapping  $F$  can be masked with secret invertible matrices  $S$  and  $T$  from  $\mathbb{F}_q^{d \times d}$ . The public key  $P$  of the scheme then essentially consists of the composition  $P = T \circ F \circ S$  and the secret key consists of the pair  $(S, T)$ . By choosing  $F$  appropriately  $P$  can be given as a set of quadratic polynomials in  $\mathbb{F}_q[x_1, \dots, x_d]$ . The first encryption scheme based on the MQ problem, named  $C^*$ , was proposed in [28] and was broken by Patarin in [30]. Since then, several multivariate encryption schemes have been proposed, for instance [31, 9, 34, 36, 14]. One typically modifies the original  $C^*$  scheme to resist certain attacks, as in [9, 14, 15], or uses a different central map altogether, e.g., [31, 34]. While some schemes for *digital signatures* based on the MQ problem seem to be secure, it has been much harder to construct encryption schemes that are both efficient and secure. The papers [22, 45, 37, 33, 1, 24] all present attacks on MQ-based public key encryption schemes, and as of now we are only aware of a few (e.g. [41]) that remain unbroken.

In [27] a new kind of central mapping is introduced, which can be used to construct both encryption and signature schemes. The novel feature of the central mapping is that it is a polynomial that has a high degree over an extension field, while still being easy to invert. The encryption variant proposed in [27] is called Dob and uses two types of modifications to its basic construction.

## Our Contribution

The initial part of our work provides a theoretical analysis of (combinations of) two modifications for multivariate cryptosystems. The  $Q_+$ -modification was (to the best of our knowledge) first proposed in [27], while the second, internal perturbation (*ip*), has been in use in earlier schemes [18, 14, 15]. More specifically, we develop tools for computing the dimension of the ideal associated with these modifications at different degrees, and a theory for how this relates to first fall polynomials. This in turn provides key insights into the complexity of algebraic attacks based on Gröbner basis techniques.

As an application, we focus on the Dob encryption scheme proposed in [27], and  $C^*$  variants using the aforementioned modifications (examples include [14, 15]). In all cases we are able to deduce formulas that predict the exact number of first fall polynomials for degrees 3 and 4, as well as degree 5 for the Dob encryption scheme. These formulas furthermore capture how the number of degree

fall polynomials changes as an attacker fixes variables, which also allows for the analysis of hybrid methods (see e.g. [5]).

Finally, the newfound understanding allows us to develop a novel attack on the Dob encryption scheme. Through analyzing and manipulating smaller, projected polynomial systems, we are able to extract and isolate a basis of the secret modifiers, breaking the scheme. While the details of the attack have only been worked out for the Dob encryption scheme, we believe the techniques themselves could also be applied to the  $C^*$  variants, as well as generalised to other central maps and modifications.

### Relation to Previous Work

This paper is based upon [44] from PKC 2021, and its extended version [43]. We now include numerous changes and improvements over these previous works, but will limit ourselves to point out the three most significant improvements here. Firstly, the fundamental theory presented in section 4.1 has been reformulated. It is now more rigorous, and should be easier to apply in practice. Secondly, estimates and experiments for variants of  $C^*$  have been included. This also gives credence to the claim from [44] that the theory can indeed be applied to constructions beyond Dob. Thirdly, the new attack presented in [44] crucially relied on heuristic arguments for solving a certain polynomial system. This is now bypassed using MinRank techniques, which enables the attacker to recover the final linear forms of the key. This strengthens the attack by turning it into a key-recovery attack that is reliant on fewer heuristics, and has a significantly smaller estimated complexity.

### Organisation

The paper is organized as follows. In section 2 we recall the relation between  $\mathbb{F}_2^d$  and  $\mathbb{F}_{2^d}$ , as well as the necessary background for solving multivariate systems over  $\mathbb{F}_2$ . In section 4 we develop the general theory that explores the effectiveness of the modifications  $Q_+$  and  $ip$ . Section 3 studies the behaviour of Dob and  $C^*$  without modifiers, which will be used in section 5 where formulas predicting the number of degree fall polynomials for the modified variants are deduced. Experimental data verifying the accuracy of these formulas are presented in section 6. In section 7 we develop the novel attack on the Dob encryption scheme, using the information learned from the previous sections. Finally, Section 8 discusses and concludes the work.

### Notation and Definitions

Multivariate big-field encryption schemes are defined using the field  $\mathbb{F}_{q^n}$  and the  $n$ -dimensional vector space over the base field,  $\mathbb{F}_q^n$ . In practical implementations,  $q = 2$  is very often used, and we restrict ourselves to only consider this case in the paper. The polynomial systems we work with will either be over the boolean

ring  $B(n) = \mathbb{F}_2[x_1, \dots, x_n]/\langle x_1^2 + x_1, \dots, x_n^2 + x_n \rangle$ , or over the quotient ring  $\overline{B}(n) = \mathbb{F}_2[x_1, \dots, x_n]/\langle x_1^2, \dots, x_n^2 \rangle$ . These polynomial systems will at various places also be considered as polynomial maps.

Throughout the paper  $\mathcal{P}$  and  $\mathcal{F}$  will refer to the modified and unmodified polynomial systems of a multivariate scheme (see Eq. (4.1)), over  $B(n)$ . This scheme will sometimes be particular variants  $C^*$  or Dob; we trust this will be clear from the context. With the superscript  $h$ ,  $\mathcal{P}^h$  (resp.  $\mathcal{F}^h$ ) denotes the system consisting of the homogeneous quadratic forms of the polynomials in  $\mathcal{P}$  (resp.  $\mathcal{F}$ ), over  $\overline{B}(n)$ .

Table 1 contains more information on terminology that will be used throughout the paper. We list it here for easy reference.

Term	Meaning
$B(n)$	$B(n) = \mathbb{F}_2[x_1, \dots, x_n]/\langle x_1^2 + x_1, \dots, x_n^2 + x_n \rangle$
$\overline{B}(n)$	$\overline{B}(n) = \mathbb{F}_2[x_1, \dots, x_n]/\langle x_1^2, \dots, x_n^2 \rangle$
$\overline{B}(n)_\nu$	The set of homogeneous polynomials of degree $\nu$ in $n$ variables.
$\langle \mathcal{R} \rangle$	The ideal associated with the set of polynomials $\mathcal{R}$ .
$\langle \mathcal{R} \rangle_\nu$	The $\nu$ -th degree part of a graded ideal $\langle \mathcal{R} \rangle$ .
$\dim_\nu(\langle \mathcal{R} \rangle)$	The dimension of $\langle \mathcal{R} \rangle_\nu$ as an $\mathbb{F}_2$ -vector space.
$\text{Syz}(\mathcal{F})$	The (first) syzygy module of $\mathcal{F}^h$ . (See Section 2)
$\text{Triv}(\mathcal{F})$	The trivial syzygy module of $\mathcal{F}^h$ . (See Section 2)
$\mathcal{S}(\mathcal{F})$	$\mathcal{S}(\mathcal{F}) = \text{Syz}(\mathcal{F})/\text{Triv}(\mathcal{F})$ .
$\mathcal{S}^I(\mathcal{F})$	$I \cdot \text{Syz}(\mathcal{F})/I \cdot \text{Triv}(\mathcal{F})$ (see Section 4.1)
$\psi, \underline{\psi}$	Maps defined in Eq. (2.4) and Lemma 2 respectively.
$Q_+, q_i, t$	The $Q_+$ modifier, with $q_1, \dots, q_t$ added quadratic polynomials.
$(ip), v_i, k$	The <i>internal perturbation</i> modifier with $v_1, \dots, v_k$ linear forms.
$N_\nu^{(\alpha, \beta)}$	Estimate of the number of degree fall polynomials at degree $\nu$ .

Table 1: Notation used in the paper

## 2 Polynomial System Solving

Let  $\mathcal{P} = (p_1, \dots, p_m)$  be the public key of a multivariate encryption system, and  $y_1, \dots, y_m$  a fixed ciphertext. A standard technique used in the cryptanalysis of multivariate schemes, is to compute a Gröbner basis associated with the ideal  $\langle p_i + y_i \rangle_{1 \leq i \leq m}$  (see for example [12] for more information on Gröbner bases). As we are interested in an encryption system, we can reasonably expect a unique solution in the Boolean polynomial ring  $B(n)$ . In this setting the solution can be read directly from a Gröbner basis of any order. An essential tool for Gröbner basis computation is the Macaulay matrix, which is defined as follows.

**Definition 1.** *Let  $\mathcal{P}$  be an (inhomogeneous) polynomial system in  $B(n)$ , of degree two. An (inhomogeneous) Macaulay matrix of  $\mathcal{P}$  at degree  $D$ ,  $\mathcal{M}_D(\mathcal{P})$ , is a matrix with entries in  $\mathbb{F}_2$ , such that:*

1. The columns are indexed by the monomials of degree  $\leq D$  in  $B(n)$  according to a graded monomial order  $\sigma$ .
2. The rows are indexed by the possible combinations  $x^\alpha p_i$ , where  $1 \leq i \leq n$  and  $x^\alpha \in B(n)$  is a monomial of degree  $\leq D - 2$ . The entries in one row corresponds to the coefficients of the associated polynomial.

Similarly, we define the homogeneous Macaulay matrix of  $\mathcal{P}$  at degree  $D$ ,  $\overline{\mathcal{M}}_D(\mathcal{P})$ , by considering  $\mathcal{P}^h \in \overline{B}(n)$ , only including monomials of degree  $D$  in the columns, and rows associated to combinations  $x^\alpha p_i^h$ ,  $\deg(x^\alpha) = D - 2$ .

Some of the most efficient algorithms for computing Gröbner bases are based on linear algebra, such as  $F_4$  [21]. In the usual setting, this algorithm proceeds in a step-wise manner; each step has an associated degree,  $D$ , where all the polynomial pairs of degree  $D$  are reduced simultaneously using linear algebra techniques on a submatrix of a Macaulay matrix. This step-wise procedure motivates the definition of the *solving degree*<sup>3</sup>, which we define for the inhomogeneous case in the following. Consider the Macaulay matrix  $\mathcal{M}_D(\mathcal{P})$ , w.r.t. a graded monomial order  $\sigma$ , in its row echelon form. Some of its low-end rows may correspond to polynomials of degree  $< D$ . Suppose there is such a polynomial  $g$ , and a monomial  $h$  of degree  $\leq D - \deg(g)$  such that  $hg$  corresponds to a row that is not in the row space of  $\mathcal{M}_D(\mathcal{P})$ . Then a new row  $hg$  is concatenated to the matrix and the process is repeated. Let  $\text{Mat}_D$  denote matrix at the termination of this routine. It is clear that for a sufficiently large  $D$ , the rowspace of  $\text{Mat}_D$  will contain a Gröbner basis of  $\langle \mathcal{P} \rangle$  w.r.t.  $\sigma$ .

**Definition 2 (Solving Degree).** *The solving degree,  $D_{\text{solv}}$ , of the polynomial system  $\mathcal{P}$  w.r.t. a graded monomial order  $\sigma$  is the smallest integer  $D$  such that the rowspace of  $\text{Mat}_D$  contains a Gröbner basis of  $\langle \mathcal{P} \rangle$ .*

The time complexity for computing a Gröbner basis of  $\mathcal{P}$  can now be upper bounded by:

$$\text{Complexity}_{\text{GB}} = \mathcal{O}\left(\left(\sum_{i=0}^{D_{\text{solv}}} \binom{n}{i}\right)^\omega\right), \quad (2.1)$$

where  $2 \leq \omega \leq 3$  denotes the linear algebra constant. Determining  $D_{\text{solv}}$  is in general difficult, but there is an important class of polynomial systems that is well understood. Recall that a homogeneous polynomial system,  $\mathcal{F}^h = (f_1^h, \dots, f_m^h) \in \overline{B}(n)^m$ , is said to be *semi-regular* if the following holds; for all  $1 \leq i \leq m$  and any  $g \in \overline{B}(n)$  satisfying

$$gf_i^h \in \langle f_1^h, \dots, f_{i-1}^h \rangle \text{ and } \deg(gf_i^h) < D_{\text{reg}}, \quad (2.2)$$

then  $g \in \langle f_1^h, \dots, f_i^h \rangle$  (note that  $f_i^h$  is included since we are over  $\mathbb{F}_2$ ). Here  $D_{\text{reg}}$  is the *degree of regularity* as defined in [4], (for  $i = 1$  the ideal generated by

<sup>3</sup> There have been different definitions for the solving degree in the literature. Here we follow the definition of [7] (adapted to the Boolean ring).

$\emptyset$  is the 0-ideal). We will also need a weaker version of this definition, where we say that  $\mathcal{F}^h$  is  $D_0$ -semi-regular, if the same condition holds, but for  $D_0 < D_{reg}$  in place of  $D_{reg}$  in Eq. (2.2). An inhomogeneous system  $\mathcal{F}$  is said to be  $(D_0^-)$ semi-regular if its upper homogeneous part is. Define the series

$$T_{m,n}(z) = \frac{(1+z)^n}{(1+z^2)^m}. \quad (2.3)$$

The Hilbert series of  $\overline{B}(n)/\langle \mathcal{F} \rangle$  for a quadratic, semi-regular system  $\mathcal{F}$  over  $\overline{B}(n)$ , is given by  $[T_{m,n}(z)]^+$ , where  $[\cdot]^+$  means truncation after the first non-positive coefficient (Corollary 7 in [4]). Moreover, the degree of regularity can be computed explicitly as the degree of the first non-positive term in this series. Determining whether a given polynomial system is semi-regular may, in general, be as hard as computing a Gröbner basis for it. Nevertheless, experiments seem to suggest that randomly generated polynomial systems behave as semi-regular sequences with a high probability [4], and the degree of regularity can in practice be used as the solving degree in Eq. (2.1). We will denote the degree of regularity for a semi-regular sequence of  $m$  polynomials in  $n$  variables as  $D_{reg}(m, n)$ . On the other hand, it is well known that many big-field multivariate schemes are not semi-regular (e.g., [22][9]). In these cases the *first fall degree* is often used to estimate the solving degree ([16][45]).

**Syzygies and Degree Fall Polynomials.** Fix a homogeneous quadratic polynomial system  $\mathcal{P}^h = (p_1^h, \dots, p_m^h) \in \overline{B}(n)^m$ , which induces a map:

$$\begin{aligned} \psi^{\mathcal{P}^h} : \overline{B}(n)^m &\longrightarrow \overline{B}(n) \\ (b_1, \dots, b_m) &\longmapsto \sum_{i=1}^m b_i p_i^h. \end{aligned} \quad (2.4)$$

In the following we will also simply write  $\psi$  for this map whenever the underlying polynomial system is clear from the context. The kernel of  $\psi$  forms the first syzygy module of  $\mathcal{P}^h$ . In the following, we will simply refer to this module as the syzygies of  $\mathcal{P}^h$ , and denote it  $\text{Syz}(\mathcal{P}^h) = \text{Ker}(\psi)$ . Moreover,  $\psi$  splits into graded maps  $\psi_{\nu-2} : \overline{B}(n)_{\nu-2}^m \longrightarrow \overline{B}(n)_{\nu}$  and we define the  $\overline{B}(n)$ -modules  $\text{Syz}(\mathcal{P}^h)_{\nu} = \text{Ker}(\psi_{\nu-2})$ , i.e., the  $\nu$ -th grade of the (first) syzygy module of  $\mathcal{P}^h$ . When  $\nu = 4$ ,  $\text{Syz}(\mathcal{P}^h)_4$  will contain the *Koszul Syzygies*<sup>4</sup>, which are generated by  $(0, \dots, 0, p_j^h, 0, \dots, 0, p_i^h, 0, \dots, 0)$  where  $p_j^h$  is in position  $i$  and  $p_i^h$  is in position  $j$ , and the *field syzygies*, which are generated by  $(0, \dots, 0, p_i^h, 0, \dots, 0)$  with  $p_i^h$  in position  $i$ . These syzygies correspond to the cancellations  $p_j^h p_i^h + p_i^h p_j^h = 0$  and  $(p_i^h)^2 = 0$ . As they are always present, and not dependent of the structure of  $\mathcal{P}^h$ , they are known as *trivial syzygies*. In particular, for a semi-regular system these are the only types of syzygies that will occur at dimensions strictly smaller than  $D_{reg}$ . We write  $\text{Triv}(\mathcal{P}^h)$  to denote the module generated by these trivial syzygies. Being a submodule of  $\text{Syz}(\mathcal{P}^h)$ , we write  $\mathcal{S}(\mathcal{P}^h) = \text{Syz}(\mathcal{P}^h)/\text{Triv}(\mathcal{P}^h)$  for the resulting quotient module.  $\text{Triv}(\mathcal{P}^h)_{\nu}$  is the  $\nu$ -th graded component of

<sup>4</sup> Here we follow the nomenclature used, for instance, in [25].

the trivial syzygies, and the aforementioned constructions respect this grading, in the sense that  $\text{Triv}(\mathcal{P}^h)_\nu \subseteq \text{Syz}(\mathcal{P}^h)_\nu$ , and  $\mathcal{S}(\mathcal{P})_\nu = \text{Syz}(\mathcal{P}^h)_\nu / \text{Triv}(\mathcal{P}^h)_\nu$  (for an explanation why these syzygies do not yield any useful information when considered over the affine ring  $B(n)$ , see [45], p. 6). We now have the tools to define the first fall degree for a polynomial system  $\mathcal{P}$ .

**Definition 3.** *The first fall degree associated with the quadratic polynomial system  $\mathcal{P}$  is the natural number*

$$D_{ff} = \min\{ D \geq 2 \mid \mathcal{S}(\mathcal{P}^h)_D \neq 0 \}.$$

The inhomogeneous polynomials (considered over  $B(n)$ ) that are associated with  $\mathcal{S}(\mathcal{P}^h)_{D_{ff}}$  will be called *first fall polynomials*. We will, more generally, refer to the inhomogeneous polynomials associated with  $\mathcal{S}(\mathcal{P}^h)$  as *degree fall polynomials*. Note that earlier works that focuses on the first fall degree relies on the usefulness of degree fall polynomials for computing Gröbner bases. While  $D_{ff}$  is measured by syzygies over  $\overline{B}(n)$ , it is implicitly assumed that their inhomogeneous counterparts will be non-zero over  $B(n)$ , and can contribute to the Gröbner basis computation. Such a degree fall polynomial will in particular correspond to a polynomial  $hg$ , as described in the lead up to Definition 2. Our use of  $D_{ff}$  and first fall polynomials will differ significantly from this use. Indeed, in Section 7 we will see how the modifiers of a big-field scheme can be recovered from the syzygies over  $\overline{B}(n)$ , without any assumption on their impact on Gröbner basis algorithms.

**Representations over base and extension fields** For any fixed isomorphism  $\mathbb{F}_2^d \simeq \mathbb{F}_{2^d}$ , there is a one-to-one correspondence between  $d$  polynomials in  $B(d)$  and a univariate polynomial in  $\mathbb{F}_{2^d}[X]/\langle X^{2^d} + X \rangle$  (see 9.2.2.2 in [8] for more details). For an integer  $j$ , let  $w_2(j)$  denote the number of nonzero coefficients in the binary expansion of  $j$ . For a univariate polynomial  $H(X)$ , we define  $\max_{w_2}(H)$  as the maximal  $w_2(j)$  where  $j$  is the degree of a term occurring in  $H$ .

**Lemma 1.** *Let  $P(X)$  be the univariate representation of the public key of a multivariate scheme, and suppose there exists a polynomial  $H(X)$  such that*

$$\max_{w_2}(H(X)P(X)) < \max_{w_2}(H(X)) + \max_{w_2}(P(X)).$$

*Then the multivariate polynomials corresponding to the product  $H(X)P(X)$  will yield degree fall polynomials from (multivariate) degree  $\max_{w_2}(H) + \max_{w_2}(P)$  down to degree  $\max_{w_2}(HP)$ .*

It was mentioned in [22] that the presence of polynomials satisfying the condition in Lemma 1 was the reason for Gröbner basis algorithms to perform exceptionally well on HFE-systems. Constructing particular polynomials that satisfy this condition has also been a central component in the security analyzes found in [16] and [45].

### 3 Degree Fall Polynomials in Unmodified Big-Field Encryption Schemes

There are several ways to construct a central map  $\mathcal{F} : \mathbb{F}_2^d \rightarrow \mathbb{F}_2^d$  to be used in a big-field scheme. A common approach is to fix an isomorphism  $\phi : \mathbb{F}_2^d \rightarrow \mathbb{F}_{2^d}$  between the vector space over the base field and the extension field, and choose two random invertible  $d \times d$ -matrices over  $\mathbb{F}_2$ , called  $S$  and  $T$ . The mapping  $\mathcal{F}$  is then constructed as the composition  $\mathcal{F} = S \circ \phi^{-1} \circ F \circ \phi \circ T$ , where  $F(X) \in \mathbb{F}_{2^d}[X]$ ,  $\max_{w_2}(F) = 2$ , and such that the equation  $F(X) = Y$  is easy to solve for any given  $Y$ . In particular, this ensures that  $\mathcal{F}$  is a system of  $d$  quadratic polynomials, and ciphertexts can easily be decrypted with the knowledge of  $F$  and the secret matrices  $S$  and  $T$ . Later we will use the notation  $\mathcal{C} = \phi^{-1} \circ F \circ \phi$  to denote only the multivariate version of the mapping  $F$ , so we can also write  $\mathcal{F} = S \circ \mathcal{C} \circ T$ .

There are two main ways in the literature to construct  $F$  with these properties:

1.  $F(X) = X^e$ , where  $w_2(e) = 2$ . This is the case for  $C^*$  [28].
2.  $F(X) = \sum_{i=0}^t c_i X^{e_i}$ , where  $w_2(e_i) \leq 2$  for all  $i$ , and each  $e_i$  is bounded by a relatively small constant. This is used in HFE [31].

Indeed, both  $C^*$  and HFE have been suggested with the  $ip$ -modification, known as PMI and ipHFE, respectively [14, 18]. These schemes were broken in [24, 20], by specialised attacks recovering the kernel of the linear forms of the  $ip$ -modification. Nevertheless, a later version of the  $C^*$  variant, PMI+ [15], also added the “+” modification in order to thwart this attack<sup>5</sup>. We note that ipHFE and PMI fits into the framework to be presented in Section 4. In the following we will first analyse  $C^*$  without any modifications. We will also introduce and analyse the Dobbertin polynomial, which can be seen as a third method for constructing  $F(X)$  and used as a basis for constructing the Dob scheme. In Section 5 we will then analyze Dob and  $C^*$  when both schemes are enhanced with modifications.

#### 3.1 The $C^*$ scheme and its syzygies

The basic  $C^*$  scheme can be seen as a variant of 1., as outlined above. The central polynomial  $F(X)$  used in  $C^*$  is often written as

$$F(X) = X^{2^\theta + 1},$$

for an integer  $0 < \theta < d$ , such that  $\gcd(2^d - 1, 2^\theta + 1) = 1$ . This monomial is then easily invertible in  $\mathbb{F}_{2^d}[X]/(X^{2^d} + X)$  and has 2-weight 2 so it is realized as  $d$

---

<sup>5</sup> While we are not aware of a comprehensive analysis of PMI+, the following is remarked in [10] p. 1026: “...the original parameters of PMI+ are easily broken by a simple modification of [6] and still larger parameters can be defeated by the new MinRank techniques developed in [17].” (The citations in the quote are changed to the enumeration used in this paper).



quadratic polynomials in  $B(n)$ . The public key of  $C^*$  consists of these  $d$  polynomials, denoted by  $\mathcal{F}$ , where  $\mathcal{F} = T \circ \phi^{-1} \circ F \circ \phi \circ S$ . In the following analysis we will also allow for cases where the number of variables in the scheme,  $n$ , is lower than the number of polynomials  $d$  which represents that some of the original  $d$  variables have been fixed to 0. Not only does this cover the projection modifier (see e.g., [9]), but we shall also see cases where fixing variables is beneficial for an attacker.

From the central mapping  $F = X^{2^\theta+1}$  it is easy to see that multiplying  $F$  with  $X$  and  $X^{2^\theta}$  (of 2-weight 1) will give polynomials of 2-weight 2:

$$\begin{aligned} XF &= X^{2^\theta+2} \\ X^{2^\theta}F &= X^{2^{\theta+1}+1} \end{aligned}$$

So over  $B(n)$  these will correspond to  $2d$  degree-fall polynomials occurring at degree 3. In addition, the linearisation equations found in [30] can be written as  $X^{2^{d-\theta}}F + X^{2^\theta}F^{2^{d-\theta}} = 0$ , which yields another set of  $d$  degree fall polynomials at degree 3. Over the ground field,  $F^{2^{d-\theta}}$  just represents a linear combination of the quadratic polynomials corresponding to  $F$  (due to  $2^{d-\theta}$  having 2-weight 1) and does not increase the degree. In our description here, we have  $X^{2^{d-\theta}}F + X^{2^\theta}F^{2^{d-\theta}} = 0$ , but in a real attack using a known ciphertext these will lead to linear polynomials over  $\mathbb{F}_2$ . All these linear polynomials have been found to be linearly independent for all but a few exceptional cases of  $\theta$  and  $d$  [13]. For the rest of the paper we assume that we do not encounter one of these cases. Extensive experiments have shown that the degree fall polynomials found above then indeed yield  $3d$  linearly independent degree fall polynomials. We therefore proceed with the assumption

$$\dim_3(\mathcal{S}(\mathcal{F})) = 3d.$$

As  $d$  of these degree fall polynomials are linear, the complete system of equations from a given ciphertext gets solved at degree 3, and it is never necessary to go to higher degrees to break a  $C^*$  scheme without any modifiers.

Even though one never needs to go to higher degrees than 3 to solve an unmodified  $C^*$  scheme, for modified versions of  $C^*$  it is still interesting to know  $\dim_\nu(\mathcal{S}(\mathcal{F}))$  for  $\nu > 3$ . As a start, we can estimate that  $\dim_4(\mathcal{S}(\mathcal{F})) \approx 3dn$ , since one can take the 3 univariate degree fall polynomials occurring at degree 3, consider them as  $3d$  polynomials over  $B(n)$ , and multiply each of them with all the variables  $x_1, \dots, x_n$  that have not been fixed to 0. A naive calculation on the number of polynomials resulting from this process will count some polynomials twice, leading to a lower number of independent degree fall polynomials actually occurring. In [45] these dependencies are explored and the corrected estimate for  $\dim_4(\mathcal{S}(\mathcal{F}))$  is found to be

$$\dim_4(\mathcal{S}(\mathcal{F})) = (3n - 9)d.$$

For higher values of  $\nu$  similar formulas may be found using  $3d\binom{n}{\nu-3}$  as a starting point, but the interplay between the three degree fall polynomials occurring at

degree 3 becomes more difficult to sort out. However, expressions for higher degrees might still be found experimentally, or through careful analysis.

### 3.2 The Dob Encryption Scheme

The *Two-Face* family, introduced in [27], presents a way to construct a function  $F(X)$  that is different from the two types of central mappings mentioned in the beginning of this section. Writing  $Y = F(X)$ , we get the polynomial equation

$$E_1(X, Y) = Y + F(X) = 0.$$

When  $F$  has the Two-Face property, it can be transformed into a different polynomial  $E_2(X, Y) = 0$ , which has low degree in  $X$  and have 2-weight at most 2 for all exponents in  $X$ . The degree of  $E_2$  in  $Y$  is arbitrary. Given  $Y$ , it is then easy to compute an  $X$  that satisfies  $E_2(X, Y) = 0$ , or equivalently,  $Y = F(X)$ .

For a concrete instantiation, the authors of [27] suggest the polynomial

$$F(X) = X^{2^m+1} + X^3 + X, \quad (3.1)$$

where  $d = 2m - 1$ . Dobbertin showed in [19] that  $F$  is a permutation polynomial. In [27], based on the results of [19], it is further pointed out that

$$E_2(X, Y) = X^9 + X^6Y + X^5 + X^4Y + X^3(Y^{2^m} + Y^2) + XY^2 + Y^3 = 0$$

holds for any pair  $Y = F(X)$ . Note that  $F$  itself has a high degree in  $X$ , but the highest exponent of  $X$  found in  $E_2$  is 9 and all exponents have 2-weight at most 2.

The public key  $\mathcal{F}$  associated with Eq. (3.1) under the composition described at the beginning of this section is called *nude Dob*, and was observed in [27] to be weak. Experiments showed that the associated multivariate system had solving degree three. Indeed, in Section 3.4 we will show that this is the case for any  $d$ .

The (full) Dob encryption scheme is made by extending nude Dob with the two modifications,  $Q_+$  and  $ip$ , to be described in Section 4.

### 3.3 Syzygies of the Unmodified Dob Scheme

The goal of this subsection is to estimate  $\dim_\nu(\mathcal{S}(\mathcal{F}))$ , for  $\nu = 3, 4, 5$ , where  $\mathcal{F}$  denotes nude Dob. We start by inspecting  $F$  (Eq. (3.1)) over the extension field  $\mathbb{F}_{2^d}[X]/\langle X^{2^d} + X \rangle$ . Note that  $\max_{w_2}(F) = 2$ , and consider the following polynomials:

$$\begin{aligned} G_1 &= XF = X^{2^m+2} + X^4 + X^2 \\ G_2 &= (X^{2^m} + X^2)F = X^{2^{m+1}+1} + X^{2^m+1} + X^5 + X^3. \end{aligned}$$

$G_1$  and  $G_2$  are both products of  $F$  and a polynomial of 2-weight one, but the resulting polynomials have  $\max_{w_2}(G_i) = 2$ . By Lemma 1 they will correspond

to  $2d$  degree fall polynomials at degree three, down to quadratic polynomials. We expect that the above degree fall polynomials form all the syzygies at degree 3 and confirmed this assumption by extensive experiments. Hence we assume

$$\dim_3(\mathcal{S}(\mathcal{F})) = 2d. \quad (3.2)$$

It was noted in [27] that experiments of nude Dob had a solving degree of three, though the authors did not provide a proof that this is always the case. The presence of  $G_1$  and  $G_2$  ensures that the first fall degree of nude Dob is three. A complete proof that the solution of nude Dob can always be found by only considering polynomials of degree three is a little more involved, and is included in Section 3.4.

Things get more complicated for dimensions  $\nu > 3$ . While we expect the two polynomials  $G_1$  and  $G_2$  to generate a significant part of the syzygies, we also expect there to be other generators, as well as cancellations to keep track of. Due to the complexity of fully characterizing the higher degree parts of  $\mathcal{S}(\mathcal{F})$ , we instead found an expression for its dimension at degrees  $\nu = 4, 5$  experimentally. The experimental setup is further described at the end of this subsection. Note that the formulas we present in this subsection will all yield numbers that are multiples of  $d$ . This strongly suggests that all the syzygies of the system come from its extension field structure. These relations could then, in principle, be written out analytically as was the case for  $\nu = 3$ . In particular, this makes it reasonable to expect the formulas to continue to hold for larger values of  $d$  (i.e., beyond our experimental capabilities).

In the subsequent formulas we will allow the number of variables  $n$  to be smaller than  $d$ , as we also did for  $C^*$ . For  $\nu = 4$ , we find the following expression:

$$\dim_4(\mathcal{S}(\mathcal{F})) = (2n - 1)d, \quad (3.3)$$

where we note that the term  $2nd$  has been generated by  $G_1$  and  $G_2$ .

For  $\nu = 5$ , we have

$$\dim_5(\mathcal{S}(\mathcal{F})) = \left( 2 \binom{n}{2} - n - 2d - 20 \right) d. \quad (3.4)$$

Once more, some of these terms can be understood from the syzygies of lower degrees. The contribution from the polynomials  $G_1$  and  $G_2$  from  $\nu = 3$  will now be the  $2 \binom{n}{2} d$  term. The term  $-d$  from  $\nu = 4$  will now cause the  $-nd$  term. We do not have any easy explanation for the remaining terms  $-2d^2 - 20d$ , but believe they have to do with inclusion/exclusion when counting the same polynomials multiple times.

**Experimental Setup.** The experiments used to test Eq. (3.3) and Eq. (3.4) have been done as follows. The public polynomials of nude Dob are first generated, and we consider their upper homogeneous part,  $\mathcal{F}^h$ , over  $\overline{B}(d)$ .  $\dim_\nu(\mathcal{S}(\mathcal{F}))$  is computed as the dimension of the kernel of the homogeneous Macaulay matrix  $\overline{\mathcal{M}}_\nu(\mathcal{F}^h)$ , minus  $\dim_\nu(\text{Triv}(\mathcal{F}^h))$ . For  $\nu = 4, 5$  we tested all odd  $d$ ,  $25 \leq d \leq 41$ , all matching the values predicted by Eq. (3.3) and Eq. (3.4).

### 3.4 Nude Dob is Fully Broken at Degree 3

In [27] it is noted that experiments indicate that nude Dob has a solving degree 3. We will now prove that this is indeed the case. Let  $c'$  denote the ciphertext of a plaintext  $m' \in \mathbb{F}_2^d$  encrypted with nude Dob and secret key  $S, T$ . We will first consider the situation over  $\mathbb{F}_{2^d}[X]/\langle X^{2^d} + X \rangle$  and then via the isomorphism  $\phi$  transfer it to  $B(d)$ . To do so we set  $C := \phi \circ T^{-1}(c')$ . Let  $F(X)$  denote the central map of nude Dob. Consider  $F(X) + C = X^{2^{m'+1}} + X^3 + X + C$  then there exists a unique  $M$  with  $F(M) = 0$  and  $m' = S^{-1} \circ \phi^{-1}(M)$ . Tedious hand calculation shows that

$$\left. \begin{aligned} & C^2 \left( (1 + X^2)(XF) \right)^{2^m} + (C^2 + X^4)F^{2^{m+1}} + X^{2^{m+1}}(C^2F^2 + F^4) \\ & + C^{2^{m+2}}F^{2^m} + C^{2^{m+2}}XF + ((X^4 + X^2)(XF) + (X^2 + X)CF)^2 \end{aligned} \right\} (I) \quad (3.5)$$

$$= \left. \begin{aligned} & X^{16} + (C^{2^{m+1}} + C^{2^{m+2}} + C^4 + C^2)X^4 \\ & + (C^2 + 1)X^8 + (C^{2^{m+2}} + C^4)X^2 + C^{2^{m+3}}X. \end{aligned} \right\} (II)$$

The polynomial (II) is linearized and of degree 16. Thus its zeros form a subspace of dimension at most 4 and  $M$  is one of the zeros as  $F(M) = 0$ . It follows that (II) will correspond to a linear system  $l_1(x_1, \dots, x_d) = \dots = l_d(x_1, \dots, x_d) = 0$  of rank at least  $d - 4$  over  $B(d)$  from which the multivariate representation of  $M$  can be computed. It follows that equation (3.5) holds for the public key  $\mathcal{F}$  as well as when modified by  $S, T$ , i.e. there exists polynomials  $l'_1(x_1, \dots, x_d) = \dots = l'_d(x_1, \dots, x_d) = 0$  from which the plaintext  $m'$  can be easily recovered from  $c'$ .

It remains to show that  $l'_1, \dots, l'_d$  can be computed from the public key  $p_1, \dots, p_d$ , using polynomials of degree at most 3. Recall from Section 3.3 that  $XF$  correspond to degree fall polynomials down to degree two in  $B(d)$ . Each such polynomial will correspond to a solution  $a_{i,j}, \gamma_{i,j}, \beta_i, \delta \in \mathbb{F}_2$ , for the equation

$$(a_{1,0} + a_{1,1}x_1 + \dots + a_{1,d}x_d)p_1 + \dots + (a_{d,0} + a_{d,1}x_1 + \dots + a_{d,d}x_d)p_d + \sum \gamma_{i,j}x_i x_j + \sum \beta_i x_i + \delta = 0$$

in  $B(d)$  (recall that we substitute  $x_i^2$  by  $x_i, i = 1, \dots, d$ , in this ring). As described in Section 3.3, we expect the solution space, w.r.t.  $a_{i,j}, \gamma_{i,j}, \beta_i$ , and  $\delta$ , to be of dimension  $2d$ . Let  $b_1, \dots, b_{2d}$  be a basis of the degree fall polynomials derived in this step, i.e., a basis of the partial polynomials  $\sum \gamma_{i,j}x_i x_j + \sum \beta_i x_i + \delta$  from this solution space. The only terms in (I) of 2-weight four are generated from  $(XF)$  and can be substituted by its degree fall polynomials. Equation (3.5) remains valid by doing so. Consequently, by employing the above degree fall polynomials, we will find non-trivial solutions  $a'_{i,j}, \beta'_i, \delta' \in \mathbb{F}_2$  for the following system of equations.

$$(a'_{1,0} + a'_{1,1}x_1 + \dots + a'_{1,d}x_d)p_1 + \dots + (a'_{d,0} + a'_{d,1}x_1 + \dots + a'_{d,d}x_d)p_d + (a'_{d+1,0} + a'_{d+1,1}x_1 + \dots + a'_{d+1,d}x_d)b_1 + \dots + (a'_{3d,0} + a'_{3d,1}x_1 + \dots + a'_{3d,d}x_d)b_{2d} + \beta'_1 x_1 + \dots + \beta'_d x_d + \delta' = 0.$$

In particular, the linear forms can be written  $l'_j = \sum \beta'_{j,i} x_i + \delta'_j$ , where the  $\beta'_{j,i}$  and  $\delta'_j$ -coefficient will be associated with solutions of this system.

Since all the systems described above only includes polynomials of degree at most three, finding a plaintext remains practical, even for  $d = 129$ . In practice one can also apply algorithms that can exploit degree fall polynomials, such as  $F_4$ . If this is the case, the polynomials associated with  $XF$  will be found in the first step of degree three, and the linear polynomials (II) will be found in the ensuing step of degree three.

### 3.5 Equivalent Keys

For multivariate schemes, the secret key is often not unique. Rather, there can be many equivalent keys associated with the same public key. This is studied by Wolf and Preneel in [40]. In this subsection we will examine the equivalent keys of  $C^*$  and nude Dob. This will be particularly useful in Section 7.5, where we will recover (equivalent) secret transformations  $S, T$  by MinRank techniques for the modified Dob encryption scheme (see [3, 23] for details on the MinRank problem). The questions arising when trying to recover  $S, T$  are how many equivalent keys one can expect, and whether the recovered triplet  $(T', C', S')$  is sufficient for our attack.

Recall that  $\mathcal{C}$  or  $\mathcal{C}'$  denotes the multivariate representation of a central mapping  $F$  or  $F'$ , respectively, with respect to the chosen isomorphism  $\phi$  for the setup of the system. The following definition from [40] (which we have generalized to include a weaker, homogeneous version) provides the means to address these questions.

**Definition 4.** *The triplets  $(T, \mathcal{C}, S)$  and  $(T', \mathcal{C}', S')$  are called equivalent if they yield the same public key, i.e. if  $T \circ \mathcal{C} \circ S = T' \circ \mathcal{C}' \circ S'$ , where  $S, S', T, T'$  are invertible matrices and  $\mathcal{C}, \mathcal{C}'$  are multivariate representation of the quadratic central maps  $F(X), F'(X)$ . We will also write that  $(T, \mathcal{C}, S)^h$  and  $(T', \mathcal{C}', S')^h$  are equivalent if their upper homogeneous part is, i.e., if  $(T \circ \mathcal{C} \circ S)^h = (T' \circ \mathcal{C}' \circ S')^h$ .*

**Equivalent Keys for  $C^*$ .** Let  $Q_i$  denote the matrix representing the linear mapping  $X \mapsto X^{2^i}, i = 0, \dots, d - 1$ , over  $\mathbb{F}_2^d$ , with respect to the fixed isomorphism  $\phi$ . Similarly, let  $\Lambda$  be the matrix representing the linear mapping  $X \mapsto \lambda X, \lambda \in \mathbb{F}_{2^d}^*$ , with respect to the same basis. It is a routine matter to show that  $Q_{d-i} \Lambda^{-(1+2^\theta)} \circ \mathcal{C} \circ \Lambda Q_i = \mathcal{C}$ , where  $\mathcal{C}$  is the multivariate representation of a  $C^*$  scheme using  $F(X) = X^{1+2^\theta}$ . Hence for a given  $T, S$  the triplet  $(T Q_{d-i} \Lambda^{-(1+2^\theta)}, \mathcal{C}, \Lambda Q_i S)$  yields an equivalent key. The following Theorem shows that this describes all the equivalent keys when we restrict the central map to  $\mathcal{C} = X^{1+2^\theta}$ , i.e., the equivalent keys of the form  $T \circ \mathcal{C} \circ S = T' \circ \mathcal{C} \circ S'$ . We use the notation  $S(\lambda)$  for  $S \in \mathbb{F}_2^{d \times d}$  and  $\lambda \in \mathbb{F}_{2^d}$  to mean the element in  $\mathbb{F}_{2^d}$  resulting from the matrix-vector multiplication between  $S$  and the vector representation of  $\lambda$ .

*Remark 1.* Combining Theorem 4.3 and Lemma 4.5 of [40] yields all equivalent keys of  $C^*$  for finite fields  $\mathbb{F}_q$ , where  $q > 2$ . Theorem 1 below completes these results by characterizing the equivalent keys for  $C^*$  with base field  $\mathbb{F}_2$ . Hence the statement in Theorem 1 holds for  $C^*$  over any binary base field.

**Theorem 1.** *Let  $\mathcal{C}$  be the multivariate representation in  $B(d)$  of the central map  $F(X) = X^{1+2^\theta} \in \mathbb{F}_{2^d}$ , where  $0 < \theta < d$  is an integer satisfying  $\gcd(2^d - 1, 2^\theta + 1) = 1$ . Furthermore, let  $S, S'$  and  $T, T'$  be invertible  $d \times d$  matrices over  $\mathbb{F}_2$ . Then the following holds for some matrices  $Q_i$  and  $\Lambda$  as defined above.*

1. If  $T \circ \mathcal{C} \circ S = T' \circ \mathcal{C} \circ S'$  then  $T' = TQ_{d-i}\Lambda^{-(1+2^\theta)}$ ,  $S' = \Lambda Q_i S$ .

*Proof.* The proof is organised as follows. We will show:

1. If  $T \circ \mathcal{C} \circ S = \mathcal{C}$  and  $S(1) = 1$  then  $T = Q_{d-i}$  and  $S = Q_i$ .

2. If  $T \circ \mathcal{C} \circ S = \mathcal{C}$  then  $T = Q_{d-i}\Lambda^{-(1+2^\theta)}$  and  $S = \Lambda Q_i$ .

3. If  $T \circ \mathcal{C} \circ S = T' \circ \mathcal{C} \circ S'$  then  $T' = TQ_{d-i}\Lambda^{-(1+2^\theta)}$ ,  $S' = \Lambda Q_i S$ .

Showing statement 1. is equivalent to consider  $T \circ \mathcal{C} = \mathcal{C} \circ S^{-1}$ . Let  $\sum_{i=0}^{d-1} t_i X^{2^i}$  and  $\sum_{i=0}^{d-1} s_i X^{2^i}$  denote the unique linearized polynomials in the quotient ring  $\mathbb{F}_2[X]/\langle X^{2^d} + X \rangle$  corresponding to  $T$  and  $S^{-1}$ , respectively. We assume that  $2\theta < d$  which is always possible, since otherwise we could consider  $X^{1+2^{d-\theta}}$  instead of  $X^{1+2^\theta}$ . Moreover,  $d \neq 2^l \theta$ ,  $l \geq 1$  as otherwise  $2^\theta + 1$  divides  $2^d - 1$  and thus  $x^{2^\theta+1}$  would not be bijective. The equality  $T \circ \mathcal{C} = \mathcal{C} \circ S^{-1}$  can now be written

$$\sum_{i=0}^{d-1} t_i X^{2^i(1+2^\theta)} = \left( \sum_{i=0}^{d-1} s_i X^{2^i} \right)^{1+2^\theta}$$

over  $\mathbb{F}_2[X]/\langle X^{2^d} + X \rangle$ . We now show that this is only possible if both linearized polynomials are of the form  $X^{2^i}$ , for some  $i$ . Expanding the left-hand side, we have

$$\sum_{i=0}^{d-1} t_i X^{2^i(1+2^\theta)} = \sum_{i=0}^{d-\theta-1} t_i X^{2^i+2^{i+\theta}} + \sum_{i=0}^{\theta-1} t_{d-\theta+i} X^{2^i+2^{d-\theta+i}}. \quad (3.6)$$

The right-hand side can be written as the product

$$\left( \sum_{i=0}^{d-1} s_i X^{2^i} \right) \left( \sum_{i=0}^{d-1} s_{d-\theta+i}^{2^\theta} X^{2^i} \right), \quad (3.7)$$

where indices are computed modulo  $d$ . Without loss of generality, we consider the case  $s_0 \neq 0$ . The other cases follow in exactly the same way as will become clear from the proof for this case. In (3.6), only the monomials  $X^{1+2^\theta}$  and  $X^{1+2^{d-\theta}}$  are of the form  $X^{1+2^j}$ , for all  $0 \leq j \leq d-1$ . On the right-hand side the sum

$$s_0 X \left( \sum_{i=0}^{d-1} s_{d-\theta+i}^{2^\theta} X^{2^i} \right) + s_{d-\theta}^{2^\theta} X \left( \sum_{i=1}^{d-1} s_i X^{2^i} \right)$$

yields all the monomials of this form. Consequently the term  $s_0 s_{d-\theta}^{2^\theta} X^2$  has to vanish. As we consider the case  $s_0 \neq 0$  it follows that  $s_{d-\theta}^{2^\theta} = 0$ . Hence only

$$s_0 X \left( \sum_{i=0}^{d-1} s_{d-\theta+i}^{2^\theta} X^{2^i} \right)$$

generates monomials of the form  $X^{1+2^j}$ . In this product all terms have to vanish except for  $s_0^{1+2^\theta} X^{1+2^\theta}$  and  $s_0 s_{d-2\theta}^{2^\theta} X^{1+2^{d-\theta}}$  since these are the only terms of this form that exist in (3.6). Thus, apart from  $s_0$ , only  $s_{d-2\theta}$  is possibly not equal to zero. Note that  $d - 2\theta > 0$  by assumption. Expanding (3.7) shows that the right-hand side contains the term  $s_{d-2\theta} s_0^{2^\theta} X^{2^{d-2\theta}+2^\theta}$ , but the monomial  $X^{2^{d-2\theta}+2^\theta}$  exists on the left-hand side (3.6) only if  $d = 4\theta$ . This is not a valid choice of  $d$ , as mentioned earlier in the proof. Thus  $s_{d-2\theta} = 0$  as well and it follows that the corresponding linearized polynomial for  $S^{-1}$  is  $s_0^{1+2^\theta} X$  by our assumption. As we further require  $S(1) = S^{-1}(1) = 1$  we get  $s_0 = 1$  and that  $S^{-1}$  simply corresponds to  $X$ , and consequently  $T$  corresponds to  $X$  as well. As stated in the beginning of the proof, the cases  $s_i \neq 0, i = 1, \dots, d-1$  follow exactly in the same way, requiring all other coefficients to be zero.

For statement 2. we now generalize and let  $S(1) = \lambda$  for some non-zero  $\lambda$ , with the corresponding matrix  $A$ . Since  $\mathcal{C}$  is the mapping that raises the input to the power  $1+2^\theta$ , we have that  $T \circ \mathcal{C} \circ S$  is equivalent to  $T A^{1+2^\theta} \circ \mathcal{C} \circ A^{-1} S$ . Now  $(A^{-1} S)(1) = 1$ , so from statement 1. we know that  $A^{-1} S = Q_i$  and  $T A^{1+2^\theta} = Q_{d-i}$ . This yields the stated expressions for  $S$  and  $T$ .

For statement 3. we know that  $T \circ \mathcal{C} \circ S = T' \circ \mathcal{C} \circ S'$  is equivalent to  $\mathcal{C} = T^{-1} T' \circ \mathcal{C} \circ S' S^{-1}$ . From 2. we then get  $T^{-1} T' = Q_{d-i} A^{-(1+2^\theta)}$  and  $S' S^{-1} = A Q_i$ , leading to the stated expressions for  $T'$  and  $S'$ . This ends our proof.  $\square$

**Equivalent Keys for Dob.** We do not know of a way to prove a similar statement on the number of equivalent keys for nude Dob, but we strongly believe that they can only be generated using the maps  $Q_i$  and  $A$  described above. This is also widely believed to hold for the similar HFE scheme, as seen e.g., in [40, 6] (note that we need not consider the “additive sustainer” mentioned in these works, as we do not allow  $S$  and  $T$  to be affine).

If we restrict ourselves to cases where the central map  $F'(X)$  has to consist of the same terms as the original map  $F(X)$  from Eq. (3.1), one can show that the triplet  $(T Q_{d-i} A^{-1}, \mathcal{C}', Q_i S)$  gives an equivalent key for a nude Dob scheme, where  $\mathcal{C}'$  denotes the multivariate representation of the altered Dob mapping  $F'(X) = \lambda(X^{2^m+1} + X^3 + X)$ . We will use this observation in Section 7.5.

## 4 Estimating the Number of Degree Fall Polynomials

We start by introducing a general setting, motivated by the Dob and  $C^*$  encryption schemes. Let  $\mathcal{F} : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^m$  be a system of  $m$  quadratic polynomials over  $B(n)$ . Furthermore, consider the following two modifiers<sup>6</sup>:

1. The *internal perturbation* (*ip*) modification chooses  $k$  linear forms  $v_1, \dots, v_k$ , and adds a random quadratic polynomial in the  $v_i$ 's to each polynomial in  $\mathcal{F}$ .
2. The  $Q_+$  modifier selects  $t$  quadratic polynomials  $q_1, \dots, q_t$ , and adds a random linear combination of them to each polynomial in  $\mathcal{F}$ .

Let  $H_{ip}$  be the random quadratic polynomials in  $v_1, \dots, v_k$  and  $H_{Q_+}$  the random linear combinations of  $q_1, \dots, q_t$ . A modification of the system  $\mathcal{F}$  can then be written as

$$\begin{aligned} \mathcal{P} : \mathbb{F}_2^n &\longrightarrow \mathbb{F}_2^m \\ x &\longmapsto \mathcal{F}(x) + H_{ip}(v_1, \dots, v_k) + H_{Q_+}(q_1, \dots, q_t). \end{aligned} \tag{4.1}$$

Recall that in order to be able to decrypt it is necessary to be able to invert the central mapping. When modifiers are added to  $\mathcal{F}$ , it can no longer be readily inverted algebraically. The polynomials  $v_1, \dots, v_k, q_1, \dots, q_t$  are considered part of the secret key and are therefore known to the party doing the decryption, but their evaluation in the plaintext is unknown to the decryptor. The only way to do decryption when modifiers are in use is to guess on their values when evaluated, and remove their effect when inverting  $\mathcal{F}$ . Each guess will give a candidate plaintext, which can be checked for correctness. For this reason the number of modifiers,  $k$  and  $t$ , must be relatively small as one must expect to try  $2^{k+t-1}$  inversions on average before the correct decryption is found.

The problem we will be concerned with in this section is the following: given full knowledge of the degree fall polynomials of the system  $\mathcal{F}$ , what can we say about the degree fall polynomials of the system  $\mathcal{P}$ ?

### 4.1 The Big Picture

Much of the following theory will be presented using ideals and modules. We start by briefly introducing some notation, as well as recalling a few fundamental concepts; for more details we refer to [2]. Let  $I$  and  $J$  be two ideals over a ring  $R$ , and  $N$  an  $R$ -module.  $I + J$  is the usual sum of ideals. We will write  $I \cap J = \{e \mid e \in I \text{ and } e \in J\}$  to denote the intersection ideal. The product ideal is written  $IJ = \{lj \mid l \in I \text{ and } j \in J\}$ . Note that  $IJ$  is always a subideal of  $I \cap J$ ,

---

<sup>6</sup> The authors of [27] named these two modifiers  $\oplus$  and “+”. Note that in earlier literature (c.f. [39]), the “+” modification refers to a different modification than what is described in [27], and the  $\oplus$  modification has been called *internal perturbation* (*ip*). To the best of our knowledge, the “+” modification from [27] has not been used in earlier work. To avoid any confusion, we have chosen to stick with the name (*ip*) and use  $Q_+$  for [27]’s “+”



but the other inclusion does not hold in general.  $I \cdot N$  will denote the module generated by the set  $\{l\mathbf{a} \mid l \in I \text{ and } \mathbf{a} \in N\}$ . When  $I$  and  $N$  are graded,  $I \cdot N$  will inherit this grading by defining  $(I \cdot N)_\nu$  as the possible sums of elements  $\{l\mathbf{a} \mid l \in I_\alpha, \mathbf{a} \in N_\beta \text{ and } \alpha + \beta = \nu\}$ . We will also write  $\mathcal{S}^I(\mathcal{F}^h) = I \cdot \text{Syz}(\mathcal{F}^h) / I \cdot \text{Triv}(\mathcal{F}^h)$  (note that  $\mathcal{S}^I(\mathcal{F}^h)$  could in general be different to  $I \cdot \mathcal{S}(\mathcal{F}^h)$ , where  $\mathcal{S}$  is the quotient module defined prior to Definition 3). If  $\mathcal{G}$  is a polynomial system, we will write  $\langle \mathcal{G} \rangle$  for the ideal generated by the polynomials of  $\mathcal{G}$ .

Let  $\mathcal{F}^h$  and  $\mathcal{P}^h$  denote the quadratic homogeneous parts of the systems  $\mathcal{F}$  and  $\mathcal{P}$  respectively, and consider them over  $\overline{B}(n)$ . For a non-negative integer  $\alpha \leq k$ , we define  $V^\alpha$  to be the homogeneous ideal in  $\overline{B}(n)$  that is generated by all possible combinations of  $\alpha$  linear forms from the  $ip$  modification, i.e.:

$$V^\alpha = \langle (v_{i_1} v_{i_2} \cdots v_{i_\alpha})^h \mid 1 \leq i_1 < i_2 < \dots < i_\alpha \leq k \rangle. \quad (4.2)$$

In other words,  $V^\alpha$  is the product ideal  $\overbrace{V^1 \cdot V^1 \cdots V^1}^\alpha$ . Similarly, for the quadratic polynomials associated with the  $Q_+$  modifier we define  $Q^\beta$  for a positive integer  $\beta \leq t$  to be the product ideal:

$$Q^\beta = \langle (q_{i_1} q_{i_2} \cdots q_{i_\beta})^h \mid 1 \leq i_1 < i_2 < \dots < i_\beta \leq t \rangle. \quad (4.3)$$

Finally, for  $0 \leq \alpha \leq k$  and  $0 \leq \beta \leq t$ , we define the ideal of different combinations of the modifiers,  $M^{(\alpha, \beta)} = (V^\alpha + Q^\beta)$ , along with the boundary cases  $M^{(\alpha, 0)} = V^\alpha$ ,  $M^{(0, \beta)} = Q^\beta$  and  $M^{(0, 0)} = \langle 1 \rangle$ .

The following result is an important first step to understand how the degree fall polynomials in  $\mathcal{F}$  behave when modifiers are introduced to the scheme. Recall the map  $\psi^{\mathcal{P}^h} : \overline{B}(n)^m \rightarrow \overline{B}(n)$  from (2.4), and its associated graded maps  $\psi_{\nu-2} : \overline{B}(n)_{\nu-2}^m \rightarrow \overline{B}(n)_\nu$ .

**Lemma 2.** *Let  $\mathcal{P}^h$ ,  $\mathcal{F}^h$ , and  $M^{(2,1)}$  be defined as above, and  $\psi^{\mathcal{P}^h}$  be as defined in Eq. (2.4), which we will abbreviate with  $\psi$  in the sequel. Then for any homogeneous ideal  $I \subseteq \overline{B}(n)$ :*

- i)  $\langle \psi(I \cdot \text{Syz}(\mathcal{F}^h)) \rangle$  is a homogeneous subideal of  $(I \langle \mathcal{P}^h \rangle) \cap (IM^{(2,1)})$ .
  - ii)  $\langle \psi(I \cdot \text{Triv}(\mathcal{F}^h)) \rangle$  is a homogeneous subideal of  $IM^{(2,1)} \langle \mathcal{P}^h \rangle$ .
- In particular,  $\psi$  induces a  $\overline{B}(n)$ -module homomorphism*

$$\underline{\psi}^I : \mathcal{S}^I(\mathcal{F}^h) \rightarrow (IM^{(2,1)}) / (IM^{(2,1)} \langle \mathcal{P}^h \rangle)$$

- iii)  $\langle \psi(IM^{(2,1)} \cdot \text{Syz}(\mathcal{F}^h)) \rangle$  is a homogeneous subideal of  $IM^{(2,1)} \langle \mathcal{P}^h \rangle$ .

*Proof.* i) Let  $f_i^h, p_i^h$  denote the polynomials of  $\mathcal{F}^h$  and  $\mathcal{P}^h$  respectively. By construction, we can write  $p_i^h = f_i^h + \sum_j c_{i,j} m_j$ , for suitable constants  $c_{i,j} \in \mathbb{F}_2$ , where  $m_j$  denote the modifiers  $q_r^h$  and  $(v_r v_l)^h$ . Let  $l\mathbf{a}$  be an element of the set generators of  $I \cdot \text{Syz}(\mathcal{F}^h)$ , such that  $l \in I$  and  $\mathbf{a} \in \text{Syz}(\mathcal{F}^h)$ . We have  $\psi(l\mathbf{a}) = l\psi(\mathbf{a})$ , where  $\psi(\mathbf{a}) \in \langle \mathcal{P}^h \rangle$  by definition of  $\psi$ . This shows the first inclusion,  $\langle \psi(I \cdot \text{Syz}(\mathcal{F}^h)) \rangle \subseteq (I \langle \mathcal{P}^h \rangle)$ . Furthermore we see that the  $f_i^h$ -parts of  $\psi(\mathbf{a})$  will

vanish. Hence  $\psi(\mathbf{a})$  will be a polynomial generated from the elements of  $V^2$  and  $Q^1$ , and the second inclusion,  $\langle \psi(I \cdot \text{Syz}(\mathcal{F}^h)) \rangle \subseteq IM^{(2,1)}$ , also follows.

ii) Let  $l$  be a generator of  $I$ , and recall from Section 2 that  $\text{Triv}(\mathcal{F}^h)$  is generated by Koszul- and field syzygies. For a Koszul syzygy the image will be

$$\begin{aligned} \psi(l(0, \dots, 0, f_{i_0}^h, 0, \dots, 0, f_{j_0}^h, 0, \dots, 0)) &= lf_{i_0}^h \left( \sum_j c_{j_0, j} m_j \right) + lf_{j_0}^h \left( \sum_j c_{i_0, j} m_j \right) \\ &= l \left( \sum_j c_{j_0, j} m_j \right) \left( p_{i_0}^h + \left( \sum_j c_{i_0, j} m_j \right) \right) + l \left( \sum_j c_{i_0, j} m_j \right) \left( p_{j_0}^h + \left( \sum_j c_{j_0, j} m_j \right) \right) \\ &= l \left( \sum_j c_{j_0, j} m_j \right) p_{i_0}^h + l \left( \sum_j c_{i_0, j} m_j \right) p_{j_0}^h. \end{aligned}$$

The image of a field syzygy can be written as

$$\begin{aligned} \psi(l(0, \dots, 0, f_{i_0}^h, 0, \dots, 0)) &= lf_{i_0}^h p_{i_0}^h = l \left( p_{i_0}^h + \left( \sum_j c_{i_0, j} m_j \right) \right) p_{i_0}^h \\ &= l \left( \sum_j c_{i_0, j} m_j \right) p_{i_0}^h, \end{aligned}$$

which shows  $\langle \psi(I \cdot \text{Triv}(\mathcal{F}^h)) \rangle \subseteq I \cdot M^{(2,1)} \langle \mathcal{P}^h \rangle$ .

For the map  $\underline{\psi}^I$ , note that  $(IM^{(2,1)}) / (IM^{(2,1)} \langle \mathcal{P}^h \rangle)$  is a quotient  $\overline{B}(n)$ -module, and let  $\pi$  denote the quotient map

$$\pi : (IM^{(2,1)}) \longrightarrow (IM^{(2,1)}) / (IM^{(2,1)} \langle \mathcal{P}^h \rangle).$$

For an equivalence class  $[a] \in \mathcal{S}^I(\mathcal{F}^h)$ , the map  $\underline{\psi}^I([a])$  is given by applying  $\pi \circ \psi$  to any representative of  $[a]$ . This is well-defined due to *i*) and *ii*), and  $\underline{\psi}^I$  inherits the properties of a  $\overline{B}(n)$ -module homomorphism from  $\psi$  and  $\pi$ . Finally, *iii*) follows from *i*), using the ideal  $IM^{(2,1)}$ .  $\square$

As before,  $\underline{\psi}^I$  naturally splits into graded maps  $\underline{\psi}_\nu^I$ ,  $\nu \geq 0$ , and we will simply write  $\underline{\psi}$  in cases where  $I = \langle 1 \rangle$ .

We now focus on how this relates to the encryption schemes we are interested in. In the previous section we noticed that (unmodified)  $C^*$  and Dob have degree fall polynomials at degree 3, meaning that  $\mathcal{S}_\nu(\mathcal{F})$  is non-trivial for these schemes when  $\nu \geq 3$ . The effect of adding modifiers to the polynomial system can be seen as mapping  $\mathcal{S}_\nu(\mathcal{F})$  under  $\underline{\psi}$ . In general, an element of  $\text{Syz}(\mathcal{F}^h)$  is not trivial under  $\psi$ , and will thus not correspond to syzygies in  $\mathcal{P}^h$ . However, consider two distinct classes  $[a], [b] \in \mathcal{S}_\nu(\mathcal{F})$  such that  $\underline{\psi}_\nu([a]) = \underline{\psi}_\nu([b])$ , and fix a pair of representatives  $a = (a_1, \dots, a_d)$  and  $b = (b_1, \dots, b_d)$  of the classes  $[a]$  and  $[b]$  respectively. Then, by Lemma 2 *ii*) there is a tuple  $(m_1, \dots, m_d)$ , with  $m_i \in$

$M^{(2,1)}$ , satisfying

$$\psi(a_1 - b_1 + m_1, \dots, a_d - b_d + m_d) = \sum_{i=1}^d (a_i - b_i + m_i) p_i = 0.$$

Hence  $(a_1 - b_1 + m_1, \dots, a_d - b_d + m_d)$  is a syzygy in  $\mathcal{P}^h$ , which is moreover a nontrivial syzygy if at least one of the polynomials  $a_i - b_i$  is not an element of  $M^{(2,1)}$ .

Lemma 2 contains information on when we can expect such syzygies to occur. If the dimension of the domain of  $\underline{\psi}_\nu$  exceeds the dimension of its codomain, then  $\underline{\psi}_\nu$  cannot be injective, and collisions of the form  $\underline{\psi}_\nu([a]) = \underline{\psi}_\nu([b])$  are guaranteed to occur. Lemma 2 *iii*) moreover implies that the elements in  $\mathcal{S}^{M^{(2,1)}}(\mathcal{F}^h)$  should be deducted when counting the dimensions of the domain. Indeed, any representative of an element  $[a] \in \mathcal{S}^{M^{(2,1)}}(\mathcal{F}^h)$  will consist of polynomials  $a_i \in M^{(2,1)}$ . This argument of counting dimensions can be made more explicit. In the previous section we did indeed give concrete estimates for the dimension of the domain, i.e.,  $\dim_\nu(\mathcal{S}(\mathcal{F}^h))$ , for certain degrees  $\nu$  when  $\mathcal{F}$  is either  $C^*$  or Dob. The dimensions  $\dim_\nu(M^{(2,1)})$ ,  $\dim_\nu(M^{(2,1)}\langle\mathcal{P}^h\rangle)$ , and  $\dim_\nu(\mathcal{S}^{M^{(2,1)}}(\mathcal{F}^h))$  will be studied in later sections.

As we consider  $\underline{\psi}_\nu^I$  using  $I = M^{(0,0)} = \langle 1 \rangle$  for our first estimate for number of degree fall polynomials at degree  $\nu$ , we denote the estimate  $N_\nu^{(0,0)}$ :

$$\begin{aligned} N_\nu^{(0,0)} &= \dim_\nu(\mathcal{S}(\mathcal{F}^h)) - \dim_\nu(M^{(2,1)}) \\ &\quad + \dim_\nu(M^{(2,1)}\langle\mathcal{P}^h\rangle) - \dim_\nu(\mathcal{S}^{M^{(2,1)}}(\mathcal{F}^h)). \end{aligned} \tag{4.4}$$

When  $N_\nu^{(0,0)}$  is a positive number, this is the number of degree fall polynomials we expect to find based on restrictions posed by  $\underline{\psi}_\nu$ . If  $N_\nu^{(0,0)}$  is non-positive we do not expect any degree fall polynomials at degree  $\nu$ . The benefits of having the expression in Eq. (4.4) is that the study of the relatively complex polynomial system  $\mathcal{P}^h$  can be broken down to studying simpler systems. The dimensions of  $M^{(2,1)}$  can, in particular, be further studied under the assumptions that the modifiers form a semi-regular system. In addition to being a reasonable assumption as the modifiers are randomly chosen, this is also the ideal situation for the legitimate user, as this maximizes the dimension of  $M^{(2,1)}$ . We will now generalise the ideas presented so far, arriving at several expressions that can be used to estimate the number of degree fall polynomials.

**Generalised Estimates of Degree Fall Polynomials.** Instead of considering *all* the syzygies of  $\mathcal{F}^h$ , as we did with  $\underline{\psi}$ , we can more generally focus on the maps  $\underline{\psi}^I$ , where  $I = M^{(\alpha,\beta)}$ , for some  $\alpha, \beta \geq 0$ . Observe from Lemma 2 *ii*) that this decreases both the dimension of the domain and codomain of  $\underline{\psi}^I$ , and will thus lead to different degree fall estimates. Indeed, in Section 6 we will see several

examples where this yields a better estimate than  $N_\nu^{(0,0)}$ . Following through with this idea, we arrive at the following estimate for  $\alpha, \beta \geq 0$ :

$$\begin{aligned} N_\nu^{(\alpha,\beta)} &= \dim_\nu \left( \mathcal{S}^{M^{(\alpha,\beta)}}(\mathcal{F}^h) \right) - \dim_\nu \left( M^{(\alpha,\beta)} M^{(2,1)} \right) \\ &\quad + \dim_\nu \left( M^{(\alpha,\beta)} M^{(2,1)} \langle \mathcal{P}^h \rangle \right) - \dim_\nu \left( \mathcal{S}^{M^{(\alpha,\beta)} M^{(2,1)}}(\mathcal{F}^h) \right). \end{aligned} \quad (4.5)$$

We now have several different estimates for degree fall polynomials, varying with the choice of  $\alpha, \beta$ . Any of these may be dominating, depending on the parameters of the scheme. The general estimate at degree  $\nu$  is then taken to be their maximum:

$$N_\nu = \max\{0, N_\nu^{(\alpha,\beta)} \mid 0 \leq \alpha \leq k \text{ and } 0 \leq \beta \leq t\}. \quad (4.6)$$

Note in particular that if  $N_\nu = 0$ , then all our estimates are non-positive, and we do not expect any degree fall polynomials at this degree.

We conclude this subsection by stressing that the aim of this section has been to investigate *one* of the aspects that can lead to a system exhibiting degree fall polynomials. The estimates presented should not be used without care to derive arguments about lower bounds on the first fall degree. Nevertheless, we find that in practice these estimates and their assumptions seem to be reasonable. With the exception of a slight deviation in only two cases (see Section 5.3), the estimates lead to formulas that are able to describe all our experiments for the Dob and  $C^*$  encryption schemes that will be reported in Section 6.

## 4.2 Dimension of the Modifiers

The estimate given in Equation (4.5) requires knowledge of the dimension of (products of) the ideals  $M^{(\alpha,\beta)}$ . These will in turn depend on the chosen modifications  $V^\alpha$  and  $Q^\beta$ . In this section we collect various results, largely based on the inclusion-exclusion principle, that will be needed to determine these dimensions. We start with the following elementary properties.

**Lemma 3.** *Consider  $M^{(\alpha,\beta)} = (V^\alpha + Q^\beta)$ , and positive integers  $\alpha_0, \beta_0, \nu$ . Then the following holds:*

- (i)  $V^{\alpha_0} V^\alpha = V^{\alpha_0+\alpha}$  and  $Q^{\beta_0} Q^\beta = Q^{\beta_0+\beta}$ .
- (ii)  $V^{\alpha_0} Q^{\beta_0} \subseteq V^\alpha Q^\beta$  if  $\alpha \leq \alpha_0$  and  $\beta \leq \beta_0$ .
- (iii)  $M^{(\alpha_0,\beta_0)} M^{(\alpha,\beta)} = M^{(\alpha_0+\alpha,\beta_0+\beta)} + V^{\alpha_0} Q^\beta + V^\alpha Q^{\beta_0}$ .
- (iv)  $\dim_\nu(M^{(\alpha,\beta)}) = \dim_\nu(Q^\beta) + \dim_\nu(V^\alpha) - \dim_\nu(Q^\beta \cap V^\alpha)$ .
- (v)  $\dim_\nu(M^{(\alpha_0,\beta_0)} M^{(\alpha,\beta)}) = \dim_\nu(M^{(\alpha_0+\alpha,\beta_0+\beta)}) + \dim_\nu(V^{\alpha_0} Q^\beta) + \dim_\nu(V^\alpha Q^{\beta_0}) - \dim_\nu(M^{(\alpha_0+\alpha,\beta_0+\beta)} \cap V^{\alpha_0} Q^\beta) - \dim_\nu(M^{(\alpha_0+\alpha,\beta_0+\beta)} \cap V^\alpha Q^{\beta_0}) - \dim_\nu(V^{\alpha_0} Q^\beta \cap V^\alpha Q^{\beta_0}) + \dim_\nu(M^{(\alpha_0+\alpha,\beta_0+\beta)} \cap V^{\alpha_0} Q^\beta \cap V^\alpha Q^{\beta_0})$ .

*Proof.* Properties (i) – (iv) follow from the appropriate definitions in a straightforward manner; we give a brief sketch of property (v) here. From property (iii) we know that  $M^{(\alpha_0, \beta_0)}M^{(\alpha, \beta)}$  can be written as the sum of the three ideals  $M^{(\alpha_0 + \alpha, \beta_0 + \beta)}$ ,  $V^{\alpha_0}Q^\beta$  and  $V^\alpha Q^{\beta_0}$ . We start by summing the dimension of each of these three ideals individually. Any polynomial belonging to exactly two of these subideals is now counted twice, which is why we subtract by the combinations intersecting two of these ideals. Lastly, a polynomial belonging to all three of the subideals will, at this point, have been counted thrice, and then subtracted thrice. Hence, we add the dimension of intersecting all three subideals.  $\square$

The dimension  $\dim_\nu(V^\alpha)$  can be further inspected using the following result.

**Lemma 4.** *Suppose that  $v_1, \dots, v_k$  are  $k$  linearly independent linear forms in  $\overline{B}(n)$ . Then*

$$\dim_\nu(V^\alpha) = \sum_{\substack{i \geq \alpha, j \geq 0 \\ i+j=\nu}} \binom{k}{i} \binom{n-k}{j} \quad (4.7)$$

holds under the conventions that  $\binom{a}{b} = 0$  if  $b > a$ , and  $\binom{a}{0} = 1$ .

*Proof.* As  $v_1, \dots, v_k$  are linearly independent, we can choose  $n - k$  linear forms of  $\overline{B}(n)$ ,  $w_{k+1}, \dots, w_n$ , that constitute a change of variables

$$\overline{B}(n) \simeq \overline{B}' = \mathbb{F}_2[v_1, \dots, v_k, w_{k+1}, \dots, w_n] / \langle v_1^2, \dots, w_n^2 \rangle.$$

For any monomial  $\gamma \in \overline{B}'$ , we will define  $\deg_v(\gamma)$  as its degree in the  $v_1, \dots, v_k$ -variables, and  $\deg_w(\gamma)$  as its degree in the variables  $w_{k+1}, \dots, w_n$ . The elements of  $V^\alpha$  of (total) degree  $\nu$ , is now generated (in  $\overline{B}'$  as an  $\mathbb{F}_2$ -vector space) by all monomials  $\gamma$  such that  $\deg_v(\gamma) \geq \alpha$  and  $\deg_v(\gamma) + \deg_w(\gamma) = \nu$ . The number of all such monomials are counted in Eq. (4.7).  $\square$

**Lemma 5.** *Let  $q_1^h, \dots, q_t^h$  be a  $D_0$ -semi-regular system of homogeneous quadratic polynomials over  $\overline{B}(n)$ . Then, for any  $2 \leq \nu < D_0$ , we have*

$$\dim_\nu(Q^1) = \binom{n}{\nu} - [z^\nu]T_{t,n}(z),$$

where  $[z^\nu]T_{t,n}(z)$  denotes the coefficient of the monomial  $z^\nu$  in the expansion of the series  $T_{t,n}(z)$ , as given in Eq. (2.3).

*Proof.* By assumption, the series  $T_{t,n}(z)$  coincides with the Hilbert series of  $\overline{B}(n)/Q^1$ , for the terms with degree  $2 \leq \nu < D_0$ . From the additive property of the Hilbert function, we have that  $\dim_\nu(Q^1) = \dim_\nu(\overline{B}(n)) - [z^\nu]T_{t,n}(z)$ , and it is well-known that  $\dim_\nu(\overline{B}(n)) = \binom{n}{\nu}$ .  $\square$

While Lemma 5 can be used to find  $\dim_\nu(Q^1)$  for any given  $n, t, \nu$ , we can also find closed-form expressions in  $n$  and  $t$  for small values of  $\nu$ . In particular, we get  $\dim_3(Q^1) = nt$ ,  $\dim_4(Q^1) = \binom{n}{2}t - \left(\binom{t}{2} + t^2\right)$  and  $\dim_5(Q^1) = \binom{n}{3}t - n\left(\binom{t}{2} + t^2\right)$ , which will be useful to us in later sections.

**Lemma 6.** *Suppose that  $(v_1, \dots, v_k, q_1, \dots, q_t)$  is  $D_0$ -semi-regular, and consider  $1 \leq \alpha \leq k$  and  $1 \leq \beta \leq t$ . Then*

$$(V^\alpha \cap Q^\beta)_\nu = (V^\alpha Q^\beta)_\nu,$$

holds for all  $\nu < D_0$ .

*Proof.* (Sketch) The product of any pair of ideals is contained in their intersection. For the other direction, consider a non-trivial element  $e \in (V^\alpha \cap Q^\beta)_\nu$ . Then, for some polynomials  $f_i, g_j$ , we can write  $e = \sum f_i q_{i_1}^h \cdots q_{i_\beta}^h \in Q_\nu^\beta$ , and  $e = \sum g_j (v_{j_1} \cdots v_{j_\alpha})^h \in V_\nu^\alpha$ , which yields the syzygy

$$\sum f_i (q_{i_1}^h \cdots q_{i_\beta}^h) + \sum g_j (v_{j_1} \cdots v_{j_\alpha})^h = 0.$$

By assumption, all syzygies of degree  $< D_0$  of  $(v_1, \dots, v_k, q_1^h, \dots, q_t^h)$  will be generated by the field and Koszul syzygies of the  $v_i$ - and  $q_j^h$ -polynomials. It follows that (after possibly reducing by syzygies generated by only  $q_1^h, \dots, q_t^h$ ) we have  $f_i \in V^\alpha$ . Similarly, we have  $g_j \in Q^\beta$ . In particular,  $e \in V^\alpha Q^\beta$ .  $\square$

A general characterisation of the ideal  $V^\alpha Q^\beta$  is trickier. We are content with discussing some special cases of its dimension, which will be of interest to us.

**Example 1** *Let  $1 \leq \alpha \leq k$  and  $1 \leq \beta \leq t$ .*

(a) *The generators of  $V^\alpha Q^\beta$  are of degree  $\alpha + 2\beta$ , hence  $\dim_\nu(V^\alpha Q^\beta) = 0$  for all  $\nu < \alpha + 2\beta$ .*

*Suppose furthermore that  $(v_1, \dots, v_k, q_1, \dots, q_t)$  is  $D_0$ -semi-regular.*

- (b) *If  $D_0 > \alpha + 2\beta + 1$ , then  $\dim_{(\alpha+2\beta+1)}(V^\alpha Q^\beta) = \binom{t}{\beta} \dim_{\alpha+1}(V^\alpha)$ . To see this, note that  $\langle V^\alpha Q^\beta \rangle_{\alpha+2\beta+1}$  is generated by elements of the form  $v_{l_1} \cdots v_{l_\alpha} q_{c_1} \cdots q_{c_\beta} x_r$ , where  $1 \leq l_1 < \dots < l_\alpha \leq k$ ,  $1 \leq c_1 < \dots < c_\beta \leq t$  and  $1 \leq r \leq n$ . The semi-regularity assumption assures that there will be no cancellations (save for the ones already accounted for in  $\dim_{\alpha+1}(V^\alpha)$ ).*
- (c) *If  $D_0 > \alpha + 2\beta + 2$ , then  $\dim_{(\alpha+2\beta+2)}(V^\alpha Q^\beta) = \binom{t}{\beta} \dim_{\alpha+2}(V^\alpha) - \binom{k}{\alpha} \left[ \binom{t}{\beta} t - \binom{t}{\beta+1} \right]$ . The reasoning is similar to (b), with the difference that  $\dim_{\alpha+2}(V^\alpha)$  will now count the polynomials of the form  $q_c^h (v_{l_1} \cdots v_{l_\alpha})^h$ . There are  $\binom{k}{\alpha} \left[ \binom{t}{\beta} t - \binom{t}{\beta+1} \right]$  combinations of these that will reduce to 0 over  $\overline{B}(n)$  (when multiplied with the combinations  $q_{c_1}^h \cdots q_{c_\beta}^h$ ).*

## 5 Degree Fall Polynomials in the $C^*$ and Dob Schemes with $ip$ and $Q_+$ Modifiers

In the following we apply the formulas for the number of degree fall polynomials we have derived, and consider the strength of the  $C^*$  and Dob schemes when both the  $ip$  and  $Q_+$  modifiers are in use together. We start by considering the impact of  $M^{(2,1)}\langle \mathcal{P}^h \rangle$  and  $\mathcal{S}^{M^{(2,1)}}(\mathcal{F}^h)$  for the cases we are interested in.

### 5.1 $IM^{(2,1)}\langle\mathcal{P}^h\rangle$ and $\mathcal{S}^{IM^{(2,1)}}(\mathcal{F}^h)$ for the $C^*$ and Dob Central Maps

We start with  $I = \langle 1 \rangle$ , noting that in this case  $M^{(2,1)}\langle\mathcal{P}^h\rangle$  will have degree at least 4. Since the polynomials generating  $M^{(2,1)}$  are randomly chosen, we do not expect non-trivial polynomials in the intersection of  $M^{(2,1)}$  and  $\langle\mathcal{P}^h\rangle$  at degree  $\leq 5$ . Hence the following estimate.

$$\dim_\nu \left( M^{(2,1)}\langle\mathcal{P}^h\rangle \right) = \begin{cases} 0, & \text{for } \nu = 3, \\ d \left( \dim_2(M^{(2,1)}) \right) & \text{for } \nu = 4, \\ d \left( \dim_3(M^{(2,1)}) \right) & \text{for } \nu = 5. \end{cases} \quad (5.1)$$

Multiplying with an ideal  $I \neq \langle 1 \rangle$  will increase the smallest degrees of all the involved polynomials. Among the variants we will consider throughout the paper, we only expect a non-trivial contribution when  $I = M^{(1,0)}$  and  $\nu = 5$  (see Equation (A.1), Appendix A), in which case we estimate  $\dim_5(M^{(1,0)}M^{(2,1)}\langle\mathcal{P}^h\rangle)$  to be  $d \left( \dim_3(M^{(1,0)}M^{(2,1)}) \right)$ .

For  $\mathcal{S}^{IM^{(2,1)}}(\mathcal{F}^h)$ , we note that both the unmodified Dob and  $C^*$  maps have a first fall degree of 3. Thus the non-trivial elements of  $M^{(2,1)} \cdot \text{Syz}(\mathcal{F}^h)$  are expected to be of degree at least 5 (when considered as polynomials under  $\psi$ ). For the cases we will be interested in, this term will then only have an impact for  $I = \langle 1 \rangle$ ,  $\nu = 5$ , in which case we expect it to be

$$\dim_5 \left( \mathcal{S}^{M^{(2,1)}}(\mathcal{F}^h) \right) = \dim_2(M^{(2,1)})\dim_3(\mathcal{S}(\mathcal{F}^h)). \quad (5.2)$$

### 5.2 Degree Fall Polynomials of the $C^*$ Scheme with Modifiers

Using the formulas from Section 4 we now investigate how well the  $ip$  and  $Q_+$  modifiers protect  $C^*$  against a Gröbner basis attack. The public key of  $C^*$  with the  $ip$  and  $Q_+$  modifiers is constructed as in Equation (4.1) and denoted  $\mathcal{P}$ .

Recall that  $\dim_\nu(\mathcal{S}(\mathcal{F}^h))$  is found in Section 3.1. When accounting for the modifiers, we proceed as described in Section 4.2, where in particular expressions for  $\dim_\nu(V^2)$  are given in (4.7) and  $\dim_\nu(Q^1)$  are given following Lemma 5. We will assume that the chosen modifying polynomials  $\{v_1, \dots, v_k, q_1, \dots, q_t\}$  form a  $(\nu + 1)$ -semi-regular system. The dimensions of  $IM^{(2,1)}\langle\mathcal{P}^h\rangle$  and  $\mathcal{S}^{IM^{(2,1)}}(\mathcal{F}^h)$  is estimated in Section 5.1. Plugging all this into (4.4) for  $\nu = 3$  we get

$$N_3^{(0,0)} = \underbrace{\dim_3(\mathcal{S}(\mathcal{F}^h))}_{3d} - \overbrace{\left( (n-k) \binom{k}{2} + \binom{k}{3} \right)}^{\dim_3(V^2)} - \underbrace{\dim_3(Q^1)}_{nt}. \quad (5.3)$$

We now apply (4.4) for  $\nu = 4$ . As seen in Lemma 3 *iv*), we also have a non-trivial term  $\dim_4(Q^1 \cap V^2)$ , which we compute using Lemma 6 and Example 1.

$$\begin{aligned}
N_4^{(0,0)} = & \overbrace{(3n-9)d}^{\dim_4(\mathcal{S}(\mathcal{F}^h))} - \overbrace{\left( \binom{k}{2} \binom{n-k}{2} + (n-k) \binom{k}{3} + \binom{k}{4} \right)}^{\dim_4(V^2)} - \\
& \overbrace{\left( \binom{n}{2} t - \binom{t}{2} - t \right)}^{\dim_4(Q^1)} + \overbrace{\binom{k}{2} t}^{\dim_4(V^2 \cap Q^1)} + \overbrace{\left( \binom{k}{2} + t \right) d}^{\dim_4(M^{(2,1)}(\mathcal{P}^h))}. \tag{5.4}
\end{aligned}$$

We also give the expression for  $N_4^{(1,0)}$  as this case will dominate in some of the experiments in the next section. In this case we would expect  $\dim_4(\mathcal{S}^{V^1}(\mathcal{F}^h)) = 3kd$ , but the experiments show that the true expression should be  $(3k+1)d$ . The experiments also show there should be a  $-\binom{t}{2}$  in the formula that we can not account for. The formula for  $N_4^{(1,0)}$  consistent with all experiments is given as

$$\begin{aligned}
N_4^{(1,0)} = & \overbrace{(3k+1)d}^{\dim_4(\mathcal{S}^{V^1}(\mathcal{F}^h))} - \overbrace{\left( \binom{k}{3} (n-k) + \binom{k}{4} \right)}^{\dim_4(V^3)} \\
& - \overbrace{t \left( k(n-k) + \binom{k}{2} \right)}^{\dim_4(Q^1 V^1)} - \binom{t}{2}. \tag{5.5}
\end{aligned}$$

For the  $C^*$  scheme we stop giving explicit formulas here at degree 4. To get correct formulas for degree 5, one must first compute  $\dim_5(\mathcal{S}(\mathcal{F}^h))$ . While it may be possible to find the closed expression for this via experiments, it is of less interest since the  $C^*$  encryption scheme is so weak in any case.

### 5.3 Degree Fall Polynomials of the Dob Scheme with Modifiers

We now turn to the Dob scheme, and use the tools from Section 4 to write out explicit formulas for (variants of) the estimates  $N_\nu^{(\alpha,\beta)}$ , up to degree 5. The approach for the formulas is the same as described in Section 5.2, with the difference that  $\dim_\nu(\mathcal{S}(\mathcal{F}^h))$  is now given according to Section 3.3. The dimensions that are not covered by combining results discussed so far, will be commented on separately.

$$N_3^{(0,0)} = \overbrace{2d}^{\dim_3(\mathcal{S}(\mathcal{F}^h))} - \overbrace{\left( (n-k) \binom{k}{2} + \binom{k}{3} \right)}^{\dim_3(V^2)} - \overbrace{nt}^{\dim_3(Q^1)}. \tag{5.6}$$



$$\begin{aligned}
N_4^{(0,0)} &= \overbrace{(2n-1)d}^{\dim_4(\mathcal{S}(\mathcal{F}^h))} - \overbrace{\left(t \binom{n}{2} - \binom{t}{2} - t\right)}^{\dim_4(Q^1)} + \overbrace{t \binom{k}{2}}^{\dim_4(Q^1 \cap V^2)} \\
&\quad - \overbrace{\left(\binom{k}{2} \binom{n-k}{2} + \binom{k}{3} (n-k) + \binom{k}{4}\right)}^{\dim_4(V^2)} + \overbrace{d \left(\binom{k}{2} + t\right)}^{\dim_4(M^{(2,1)}(\mathcal{P}^h))}.
\end{aligned} \tag{5.7}$$

$$\begin{aligned}
N_4^{(1,0)} &= \overbrace{2kd}^{\dim_4(\mathcal{S}^{V^1}(\mathcal{F}^h))} - \overbrace{\left(\binom{k}{3} (n-k) + \binom{k}{4}\right)}^{\dim_4(V^3)} \\
&\quad - \overbrace{t \left(k(n-k) + \binom{k}{2}\right)}^{\dim_4(Q^1 V^1)}.
\end{aligned} \tag{5.8}$$

Recall that at degree 5 we expect the dimension of  $\mathcal{S}^{M^{(2,1)}}(\mathcal{F}^h)$  to be non-trivial, and given by Equation (5.2).

$$\begin{aligned}
N_5^{(0,0)} &= \overbrace{\left(2 \binom{n}{2} - n - 2d - 20\right)d}^{\dim_5(\mathcal{S}(\mathcal{F}^h))} - \overbrace{\left(t \binom{n}{3} - n \binom{t}{2} - tn\right)}^{\dim_5(Q^1)} \\
&\quad - \overbrace{\left(\binom{k}{2} \binom{n-k}{3} + \binom{k}{3} \binom{n-k}{2} + \binom{k}{4} (n-k) + \binom{k}{5}\right)}^{\dim_5(V^2)} \\
&\quad + \overbrace{t \left(\binom{k}{2} (n-k) + \binom{k}{3}\right)}^{\dim_5(Q^1 \cap V^2)} \\
&\quad + \overbrace{d \left(nt + \left(\binom{k}{2} (n-k) + \binom{k}{3}\right)\right)}^{\dim_5(M^{(2,1)}(\mathcal{P}^h))} - \overbrace{2d \left(t + \binom{k}{2}\right)}^{\dim_5(\mathcal{S}^{M^{(2,1)}}(\mathcal{F}^h))}.
\end{aligned} \tag{5.9}$$

It is a bit more involved to derive  $N_5^{(1,1)}$  and  $N_5^{(2,1)}$ , and we will refer to Appendix A for more details. It would also appear that our assumptions are slightly off for these two estimates, as our experiments consistently yield  $4d$  more degree fall polynomials than we are able to explain (see Remark 3 for more

details). We present here the experimentally adjusted versions:

$$\begin{aligned}
N_5^{(1,1)} = & d \left( k(2n - k - 2) + t(2 + k) + \binom{k}{3} + 4 \right) - \binom{t}{2} n - \binom{k}{3} \binom{n - k}{2} \\
& - \binom{k}{5} - \binom{k}{4} (n - k) - t \left( k \binom{n - k}{2} + \binom{k}{2} (n - k) - kt \right).
\end{aligned} \tag{5.10}$$

$$\begin{aligned}
N_5^{(2,1)} = & 2d \left( \binom{k}{2} + t + 2 \right) - \left( \binom{k}{4} (n - k) + \binom{k}{5} \right) \\
& - t \left( \binom{k}{2} (n - k) + \binom{k}{3} \right) - \binom{t}{2} n.
\end{aligned} \tag{5.11}$$

We stop giving further explicit formulas for the number of degree fall polynomials occurring at various degrees when modifiers are taken into account. For degree 6 and higher, the terms in (4.4) will be less simple, complicating matters further. However, we hope that we have demonstrated that it is possible to get accurate estimates of the number of degree fall polynomials in various big-field constructions, even when modifications suggested in the literature are in use. By breaking the counting problem into smaller parts and treating each part separately, accurate (but complicated) formulas can be derived and explained.

**Note on EFLASH.** In [45] the cipher EFLASH [9], an encryption scheme using  $C^*$  with the minus and projection modifiers, was broken using similar techniques as described here. In particular, formulas were derived that predicts the number of degree fall polynomials for degrees  $\nu = 3, 4$ , for this construction. We note that removing a *small* number of public polynomials (i.e., the minus modification) behaves very similarly to the  $Q_+$  modifier. It follows that the formulas in [45] can easily be derived from the framework presented in Section 4 (see Section 4.1 in [42] for more details). While a thorough examination of the minus modifier is beyond the scope of this work, we believe this observation strongly suggests that the framework introduced in Section 4 can be expanded to include other modifiers.

## 6 Experimental Results on Degree Fall Polynomials

In the previous section we developed the theory on how to estimate the number of first fall polynomials, ending up with several formulas. This section is focused on the accuracy of these formulas, and how they can be used by an attacker. Note that since we are interested in the unique structure of the encryption schemes, we will always assume that ‘generic’ degree fall polynomials do not interfere. More specifically, when inspecting a system of  $d$  polynomials in  $n$  variables at degree  $\nu$ , we assume that  $d$  and  $n$  is chosen such that  $D_{reg}(d, n) > \nu$ .

## 6.1 Fixing Variables

The formulas separate  $d$ , the size of the field extension, and  $n$ , the number of variables. While the Dob and  $C^*$  encryption schemes uses  $d = n$ , an attacker can easily create an overdetermined system with  $n < d$  by fixing some variables. This approach, known as the hybrid method, can be viewed as a trade-off between exhaustive search and Gröbner basis techniques, and its benefits are well-known for semi-regular sequences [5]. From Eqs. (5.3) to (5.11), we find that for the relevant choices of parameters  $(d, t, k)$ , a greater difference between  $n$  and  $d$  can increase the number of degree fall polynomials. This means that a hybrid method will have a more intricate effect on the Dob and  $C^*$  systems, than what we would expect from random systems. To a certain extent, an attacker can “tune” the number of degree fall polynomials, by choosing the amount of variables to fix. Of course, if the intent is to find a solution of the polynomial system through a Gröbner basis, this comes at the added cost of solving the system  $2^r$  times, where  $r$  is the number of fixed variables, but in Section 7 we will present a different attack that circumvents this exponential factor.

Finally, one could ask whether it is reasonable to expect Eqs. (5.3) to (5.11) to be accurate after fixing a certain number of variables. It is, for instance, possible that different degree fall polynomials will cancel out, as certain variables are fixed. However, this has not occurred in the experiments we have performed (see Section 6.3), where the formulas remain precise as  $n$  is varied.

## 6.2 Using the Degree Fall Formulas

We briefly recall how the formulas found in Section 5 relate to the public polynomials of a  $C^*$  or Dob encryption scheme. Let  $\mathcal{P}$  be the polynomial system associated with a Dob or  $C^*$  scheme of fixed parameters  $(d, n, t, k)$  (where  $n$  is as described in Section 6.1). We expect the non-trivial dimension (i.e., the dimension of the part that is not generated by  $\text{Triv}(\mathcal{F}^h)$ ) of the kernel of  $\overline{\mathcal{M}}_\nu(\mathcal{P}^h)$  to be given by the maximum of the formulas  $N_\nu^{(\alpha, \beta)}$ , for  $\nu = 3, 4, 5$ .

If a step-wise algorithm such as  $F_4$  is used, we expect the formulas to predict the number of degree falls polynomials, but *only* at the first fall degree. Suppose, for instance, that  $N_3 = 0$ , but  $N_4 > 0$ . Then this algorithm runs a second step at degree 4, using the newly found degree fall polynomials. This means that there are effectively more available polynomials in the system when (if) a step of degree 5 is performed, and in this case we do not expect the formulas we have for  $N_5$  to be accurate.

Note in particular that if all the formulas we have are non-positive, an attacker is likely required to go up to step degree  $\geq 6$  in order to observe first fall polynomials.

### 6.3 Experimental Results

We have run a number of experiments with the Dob and  $C^*$  systems of varying parameters  $(d, n, t, k)$ . A subset<sup>7</sup> of them is presented in Table 2 and Table 3. Gröbner bases of the systems were found using the  $F_4$  algorithm implemented in the computational algebra system Magma. The script used for the experiments is available at [26].

In Table 2 and Table 3 we use the following notation. ‘ $D_{ff}$ ’ is the experimentally found first fall degree. ‘ $N$  (predicted)’ is the number of first fall polynomials as predicted by the equations in Section 5. ‘ $N$  (Magma)’ is the number of first fall polynomials read from the verbose output of Magma, written as ‘degree : {# of degree fall polynomials at this degree}’.

The solving degree  $D_{solv}$  (Definition 2) was found experimentally by Magma. In the instances where the algorithm did not run to completion due to memory constraints, we give  $D_{solv}$  as  $\geq Z$ , where  $Z$  is the degree of the step where termination occurred. The degree of regularity for semi-regular systems of the same size,  $D_{reg}(d, n)$ , is also given. ‘Step Degrees’ lists the degrees of the steps that are being performed by  $F_4$  up until linear relations are found. Once a sufficient number of linear relations are found, Magma restarts  $F_4$  with the original system, as well as these linear relations. This restart typically needs a few rounds before the entire basis is found, but its impact on the running time of the algorithm is negligible, which is why we have chosen to exclude it when listing the step degrees. For convenience, the step where first fall polynomials are found is marked in blue and the most time consuming step is marked in red. The color purple is used to mark the steps where these two coincide.

Table 2: Number of degree fall polynomials for  $C^*$  with  $ip$  and  $Q_+$  modifiers

$d$	$n$	$t$	$k$	$\theta$	$D_{ff}$	$N$ (predicted)	$N$ (Magma)	$D_{solv}$ ( $D_{reg}(d, n)$ )	Step Degrees
35	30	1	3	13	4	$N_4^{(0,0)} : 1464, N_4^{(1,0)} : 204$	3:1464	4 (6)	2,3,4,4
45	42	2	4	13	4	$N_4^{(0,0)} : -453, N_4^{(1,0)} : 115$	3:115	5 (7)	2,3,4,4,4,5
45	42	1	5	13	4	$N_4^{(0,0)} : -2125, N_4^{(1,0)} : 150$	3:150	5 (7)	2,3,4,4,5
65	40	2	4	11	4	$N_4^{(0,0)} : 2265, N_4^{(1,0)} : 335$	3:2265	4 (6)	2,3,4,4
65	40	2	6	11	4	$N_4^{(0,0)} : -2317, N_4^{(1,0)} : 101$	3:101	5 (6)	2,3,4,4,5,4
65	40	1	6	11	4	$N_4^{(0,0)} : -1619, N_4^{(1,0)} : 321$	3:321	5 (6)	2,3,4,4,4,5
65	40	3	5	11	4	$N_4^{(0,0)} : -549, N_4^{(1,0)} : 127$	3:127	5 (6)	2,3,4,4,5
77	41	4	5	17	4	$N_4^{(0,0)} : -39, N_4^{(1,0)} : 101$	3:101	5 (6)	2,3,4,4,4,5
136	60	0	6	24	4	$N_4^{(0,0)} : 2736, N_4^{(1,0)} : 1353$	3:2736	4 (6)	2,3,4,4

<sup>7</sup> Table 3 is just a small sample of the experiments we have run for the Dob encryption scheme. More experiments, covering a total of four pages, is available in Appendix G of [43], all of which are consistent with the formulas presented in Section 5.3.

Table 3: Number of degree fall polynomials for Dob with  $ip$  and  $Q_+$  modifiers.

$d$	$n$	$t$ ( $Q_+$ )	$k$ ( $ip$ )	$D_{ff}$	$N$ (predicted)	$N$ (Magma)	$D_{solv}$ ( $D_{reg}(d, n)$ )	Step Degrees
53	53	0	0	3	$N_3^{(0,0)} : 106$	2:106	3 (9)	2,3,3
53	53	0	3	4	$N_4^{(0,0)} : 1999$	3:1999	4 (9)	2,3,4,4
53	53	3	0	4	$N_4^{(0,0)} : 1596$	3:1596	4 (9)	2,3,4,4
59	29	0	7	4	$N_4^{(1,0)} : 21$	3:21	5 (5)	2,3,4,4,5
37	25	2	3	4	$N_4^{(0,0)} : 692$	3:692	4 (5)	2,3,4,4
31	29	0	8	5	$N_5^{(1,1)} : 478$	4:478	5 (6)	2,3,4,5,5,5
31	30	0	8	5	$N_5^{(2,1)} : 264$	4:264	5 (6)	2,3,4,5,5,5,4
39	37	1	7	5	$N_5^{(2,1)} : 136$	4:136	$\geq 6$ (7)	2,3,4,5,5,5,6...
57	38	4	6	5	$N_5^{(1,1)} : 2086$	4:2086	$\geq 6$ (6)	2,3,4,5,5,6...
57	37	4	6	5	$N_5^{(1,1)} : 2847$	4:2847	5 (6)	2,3,4,5,5
129	50	6	6	5	$N_5^{(0,0)} : 64024$	4:64024	$\geq 5$ (6)	2,3,4,5,5...

A first observation is that in all experiments we find that ‘ $N$  (predicted)’ matches ‘ $N$  (Magma)’. We also find that fixing variables affects the cross-over point between the formulas  $N_\nu^{(\alpha,\beta)}$ , as for instance seen in the rows 6 and 7 of Table 3. We note that  $N_\nu^{(0,0)}$  tend to be dominant when  $n \ll d$ , and that  $N_5^{(2,1)}$  in Table 3 only seems to have an impact when  $k$  is large and  $t$  is small. For the majority of cases we observe that  $D_{ff} = D_{solv}$  or  $D_{solv} + 1$ , but one should be careful in drawing any conclusions from this, seeing that our experiments are in practice limited to computations of  $D < 6$ . The relation between  $n$  and  $D_{solv}$  is also noteworthy. For instance, in row 9 of Table 3 we have  $d = 57$  and  $n = 38$ ;  $D_{ff}$  is 5, but  $D_{solv} \geq 6$ . In row 10 we fix one more variable,  $n = 37$  (while keeping everything else as before), and find  $D_{solv} = 5$ .

In Table 2 we have put emphasis on examples where  $N_4^{(1,0)}$  dominates, to show the terms in (5.5) we can not explain are consistently present. One of the exception is the last row, where  $d = 136$  and  $k = 6$  was suggested parameters in [14] (the same choice of parameters, along with the “+” modifier, is suggested for 80-bit security in [15]). The experiment in the last row of Table 3,  $d = 129$ ,  $t = k = 6$ , is suggested for 80-bit security in [27]. Thus, our formulas are also exact for parameters suggested for use in practice.

**Impact on Known Attacks.** The solving degree of big field schemes are often estimated using the first fall degree. In cases where  $D_{solv} > D_{ff}$ , we observed instances where it is beneficial for an attacker to fix (a few) variables in order to lower the  $D_{solv}$  for each guess. Without a better understanding of  $D_{solv}$  and how it is affected by fixing variables, it seems that the approximation  $D_{ff} \approx D_{solv}$  is conservative, yet reasonable, when estimating the complexity of direct/hybrid attacks against big-field encryption systems.

Another attack that may greatly benefit from the detailed formulas for degree fall polynomials obtained here is an adapted version of the distinguishing attack that was proposed for HFEv- (Section 5 in [17]). An attacker fixes random linear forms, and distinguishes between the cases where (some of) the fixed linear forms are in the span of  $(v_1, \dots, v_k)$ , and when none of them are, by the use of Gröbner basis techniques. Indeed, if *one* of the fixed linear forms are in this span, the number of degree fall polynomials will be the same as for a system with  $k - 1$  *ip* linear forms. Hence, a distinguisher based on the formulas presented here will work even without a drop in first fall degree, making the attack more versatile.

The deeper understanding for how the modifiers work allows for an even more efficient attack. We present it in the next section for the Dob encryption scheme.

## 7 A New Attack on the Dob Encryption Scheme

In the previous two sections we have studied how degree fall polynomials can occur in the Dob scheme, and have verified the accuracy of our resulting formulas through experiments. In this section we will show how all these insights can be combined into a novel attack. In Section 7.1, we shall see that adding an extra polynomial to the system can leak information about the modification polynomials. We will use this information to retrieve (linear combinations of) the secret *ip* linear forms and the homogeneous quadratic part of the  $Q_+$  modification in Sections 7.2 and 7.3. The remaining linear parts of  $Q_+$  as well as an equivalent description for the underlying nude Dob scheme is described in Section 7.5 and Section 7.6. This results in an equivalent key, which allows an attacker to decrypt just as easily as the legitimate user. Experiments on toy examples are described in Section 7.7, and we finally discuss the complexity of the attack in Section 7.8.

### 7.1 Adding an Extra Polynomial

In Section 4.1 we discussed how products of the modifiers and public polynomials affect the number of degree fall polynomials, through  $M^{(2,1)}\langle \mathcal{P}^h \rangle$ . One would also expect a similar effect to take place when adding a random polynomial to the system.

Consider a set of parameters for the Dob scheme, where the number of first fall polynomials is determined by  $N_\nu^{(0,0)}$ , for some  $\nu > 3$ . Again we denote by  $\mathcal{P}$  be the public key of this scheme, and consider a randomly chosen homogeneous polynomial  $p_R$  of degree  $\nu - 2$ . As it is unlikely that the randomly chosen  $p_R$  has any distinct interference with  $\mathcal{P}$ , we expect  $(\langle p_R \rangle \cap M^{(2,1)})_\nu$  to be generated by the  $t$  possible combinations  $p_R q_i^h$ , and  $\binom{k}{2}$  different combinations  $p_R (v_j v_l)^h$ . Furthermore, the non-zero elements of  $\psi(\text{Syz}(\mathcal{F}^h))$  have degree at least 3 so we expect that  $\langle \psi(\text{Syz}(\mathcal{F}^h)) \rangle_\nu \cap \langle p_R \rangle_\nu = \emptyset$ , since  $\langle p_R \rangle_\nu$  is generated by multiplying  $p_R$  only with quadratic polynomials.

From these considerations, we estimate the number of degree fall polynomials for the system  $\{\mathcal{P}, p_R\}$  at degree  $\nu$  to be:

$$N_\nu(\{\mathcal{P}, p_R\}) = N_\nu^{(0,0)}(\mathcal{P}) + t + \binom{k}{2}. \quad (7.1)$$

We ran a few experiments that confirm this intuition, the details are given in Table 4. First, we confirmed that the number of degree fall polynomials of  $\mathcal{P}$  were indeed given by  $N_\nu^{(0,0)}(\mathcal{P})$ , before applying Magma's implementation of the  $F_4$  algorithm on the system  $\{\mathcal{P}, p_R\}$ . Recall also our convention that  $\binom{0}{2} = \binom{1}{2} = 0$  when applying Eq. (7.1).

Table 4: First fall polynomials of Dob encryption schemes with an added, randomly chosen polynomial  $p_R$ .

$d$	$n$	$\deg(p_R)$	$t$ ( $Q_+$ )	$k$ ( $ip$ )	$D_{ff}$	$N$ (predicted)	$N$ (Magma)
31	29	2	2	2	4	$N_4 : 705$	3:705
45	30	2	6	0	4	$N_4 : 342$	3:342
75	39	3	6	6	5	$N_5 : 4695$	4:4695
39	37	3	6	0	5	$N_5 : 9036$	4:9036

With all this in mind, assume for the moment that  $d = n$ , and consider a homogeneous Macaulay matrix of  $\{\mathcal{P}^h, p_R\}$  at degree  $\nu$ ,  $\overline{\mathcal{M}}_\nu(\{\mathcal{P}^h, p_R\})$ . Any element in the (left) kernel of this matrix corresponds to a syzygy:

$$h_R p_R + \sum_{i=1}^d h_i p_i^h = 0, \quad (7.2)$$

for some homogeneous polynomials  $h_i \in \overline{B}(d)_{\nu-2}$ ,  $1 \leq i \leq d$ , and  $h_R \in \overline{B}(d)_2$ . In the following we will focus only on the polynomials  $h_R$  in this expression, and knowing the order of the polynomials in  $\overline{\mathcal{M}}_\nu(\{\mathcal{P}^h, p_R\})$  allows us to easily extract only the  $h_R$  polynomials from the kernel. From the discussion above, we expect that the only way  $p_R$  contributes to these kernel elements is through the trivial syzygies, i.e. multiplications with  $p_i^h$  or  $p_R$ , and through multiplying with the generators of  $M^{(2,1)}$ . It follows that any polynomial  $h_R$ , from Eq. (7.2), will be in the span of<sup>8</sup>

$$\mathcal{H} := \{p_1^h, \dots, p_d^h, p_R, q_1^h, \dots, q_t^h, (v_1 v_2)^h, \dots, (v_{k-1} v_k)^h\}. \quad (7.3)$$

<sup>8</sup> If  $p_R$  has degree  $\geq 3$ , then the syzygy  $p_R^2 + p_R = 0$  will be of degree  $> \nu$ . In this case  $p_R$  will not be among the generators of  $\mathcal{H}$ . This matters little, as  $p_R$  will be removed in the degree 2 case anyway in Section 7.4.

Hence, given more than  $|\mathcal{H}| = d + t + \binom{k}{2} + 1$  linearly independent kernel elements of  $\overline{\mathcal{M}}_\nu(\{\mathcal{P}^h, p_R\})$ , a set of generators of  $\text{Span}(\mathcal{H})$  can likely be found. In the next subsection we will generalise this observation to the case where we fix a number of variables to 0, making  $n$  smaller than  $d$ .

## 7.2 Gluing Polynomials

Let  $W_\eta$  denote a non-empty subset of  $r$  variables, i.e.  $W_\eta = \{x_{i_{\eta,1}}, \dots, x_{i_{\eta,r}}\}$  for integers  $1 \leq i_{\eta,1} < \dots < i_{\eta,r} \leq d$ . For  $n = d - r$ , there is a natural projection map associated to  $W_\eta$ , namely  $\pi_{W_\eta} : B(d) \rightarrow B(d)/W_\eta \simeq B(n)$ , that sets the variables in  $W_\eta$  to 0. For any polynomial system  $\mathcal{R}$  over  $B(d)$ , we write  $\pi_{W_\eta}(\mathcal{R})$  to mean the system consisting of all polynomials in  $\mathcal{R}$  under  $\pi_{W_\eta}$ .

Suppose now that the number of first fall polynomials of a Dob system  $\pi_{W_\eta}(\mathcal{P}^h)$  is given by  $N_\nu^{(0,0)}$ , after fixing the  $r$  variables in  $W_\eta$  to 0. Following a similar line of reasoning as in Section 7.1, we find that  $\pi_{W_\eta}(h_R)$  from a kernel element of the Macaulay matrix associated with  $\pi_{W_\eta}(\{\mathcal{P}^h, p_R\})$  will no longer be in the span of  $\mathcal{H}$ , but rather lie in the span of  $\pi_{W_\eta}(\mathcal{H})$ . To ease notation, we will write  $\mathcal{H}_\eta = \pi_{W_\eta}(\mathcal{H})$ .

We show in the following that we can recover a basis for  $\mathcal{H}$  by defining  $\rho$  different variable sets  $W_1, \dots, W_\rho$ , and finding generators for the associated polynomial sets  $\mathcal{H}_1, \dots, \mathcal{H}_\rho$ . The idea is that each  $\mathcal{H}_i$  reveals a piece of the picture of the full  $\mathcal{H}$ , and we will see that these pieces are partially overlapping. By aligning the overlapping parts we can “glue” all the pieces together to reveal the full picture, which in our case is a basis for the space spanned by the full  $\mathcal{H}$  where no variables have been set to 0.

Let  $\widetilde{W}_\eta := \{x_1, \dots, x_d\} \setminus W_\eta$  denote the complement of  $W_\eta$ , and note that  $\mathcal{H}_\eta$  only contains information about the set of quadratic monomials where both variables in the monomial are in  $\widetilde{W}_\eta$ . Denote the set of monomials not eliminated by  $W_\eta$  as

$$A(W_\eta) := \{x_i x_j \mid x_i, x_j \in \widetilde{W}_\eta\}.$$

In order to guarantee that the family  $\mathcal{H}_1, \dots, \mathcal{H}_\rho$  can give complete information about  $\mathcal{H}$  we need to ensure that for any choice of  $1 \leq i < j \leq d$ , we have  $x_i x_j \in A(W_\eta)$  for at least one  $1 \leq \eta \leq \rho$ .

In practice,  $d$  will be determined by the chosen Dob parameters, but the attacker is free to choose the size and construction of the sets  $W_\eta$  himself. There are a few trade-offs when it comes to choosing the size  $r$  of the variable sets  $W_\eta$ . On the one hand, we want  $r$  to be big, giving small  $n$  compared to  $d$ , so we get many degree fall polynomials in  $\mathcal{M}_\nu$  for a low degree  $\nu$ . On the other hand,  $r$  can not be so big that  $\pi_{W_\eta}(\mathcal{P}^h)$  becomes so degenerate that we get more syzygies than the ones coming from  $\mathcal{H}$ . For instance, we expect this to be the case if  $r$  is chosen such that  $d_{reg}(\pi_{W_\eta}(\mathcal{P}^h)) \leq \nu$  (see Eq. (2.3)). This degeneration is possible to check since we know that the dimension of the basis for  $\mathcal{H}_\eta$  that we recover from  $\overline{\mathcal{M}}_\nu(\pi_{W_\eta}(\{\mathcal{P}^h, p_R\}))$  should have dimension  $d + t + \binom{k}{2} + 1$ . If we get a different number,  $r$  must be decreased. As will become clear below,



$r$  can also not be so big that the  $\widetilde{W}_\eta$  become too small. Essentially, we need  $A(W_{\eta_1}) \cap A(W_{\eta_2}) > |\mathcal{H}|$  for different  $\eta_1$  and  $\eta_2$ . From our experience with the Dob system, these condition are easy to fulfill, and there is a rather large span of suitable  $r$ -values we can choose.

Apart from setting the largest possible  $r$ , there is the question of how to actually construct the sets  $W_1, \dots, W_\rho$  in the most efficient way. In order not to do more gluing than necessary, we want  $\rho$  to be as small as possible for a given  $r$ . For the gluing operation that follows, there is the requirement that every quadratic monomial in  $\overline{B}(d)_2$  must be included in at least one  $A(W_\eta)$ . This naturally leads to the following problem:

**Definition 5 (The quadratic  $(r, d)$ -Covering Problem).** *For integers  $1 < r < d - 1$ , find the smallest number  $\rho$  of variable sets, each of size  $r$ , such that*

$$A(W_1) \cup \dots \cup A(W_\rho) = \{x_i x_j \mid 1 \leq i < j \leq d\}.$$

In Appendix B we present a constructive solution to this problem, which provides a good upper bound for  $\rho$  that is sufficient for our case. The upper bound is given by the following lemma

**Lemma 7.** *The quadratic  $(r, d)$ -Covering Problem is upper bounded by*

$$\rho \leq \binom{\left\lceil \frac{d}{\lfloor (d-r)/2 \rfloor} \right\rceil}{2}.$$

**Gluing.** We are now ready to explain how the gluing process works. Assume that we have defined  $W_1, \dots, W_\rho$  such that  $\dim(\mathcal{H}_i) = d + t + \binom{k}{2} + 1$  for  $1 \leq i \leq \rho$  and  $\cup_{i=1}^\rho A(W_i) = \{x_i x_j \mid 1 \leq i < j \leq d\}$ . Let  $H_i$  be the part of the kernel of  $\overline{\mathcal{M}}_\nu(\pi_{W_i}(\{\mathcal{P}^h, p_R\}))$  that forms a basis for  $\mathcal{H}_i$ , i.e.  $H_i$  is a matrix with  $d + t + \binom{k}{2} + 1$  linearly independent rows and  $\binom{d}{2}$  columns representing all monomials in  $\overline{B}(d)_2$ . As attackers we can generate and store all matrices  $H_i$  for  $i = 1, \dots, \rho$ . Recall also that each  $H_i$  contains information on the monomials appearing in  $A(W_i)$ .

We now explain in detail how we can glue together  $H_1$  and  $H_2$ , to make a new matrix  $H_{1,2}$  that reveals the monomials in  $A(W_1) \cup A(W_2)$  appearing in a basis for  $\mathcal{H}$ . First split the quadratic monomials in  $\overline{B}(d)_2$  into four disjoint sets  $U_{1,2}, U_{\overline{1},2}, U_{1,\overline{2}}$  and  $U_{\overline{1},\overline{2}}$  as follows:

- $U_{1,2} = \{\text{monomials set to 0 by both } W_1 \text{ and } W_2\}$ .
- $U_{\overline{1},2} = \{\text{monomials set to 0 by } W_2, \text{ but not by } W_1\}$ .
- $U_{1,\overline{2}} = \{\text{monomials set to 0 by } W_1, \text{ but not by } W_2\}$ .
- $U_{\overline{1},\overline{2}} = \{\text{monomials not set to 0 by either } W_1 \text{ or } W_2\}$ .

Sort the monomials in  $\overline{B}(d)_2$  according to these sets, and create the matrix  $H_2^1$  containing the rows of both  $H_1$  and  $H_2$ :

$$H_2^1 = \begin{matrix} & U_{1,2} & U_{\overline{1},2} & U_{1,\overline{2}} & U_{\overline{1},\overline{2}} \\ \begin{matrix} H_1 \\ H_2 \end{matrix} & \left( \begin{array}{cccc} 0 & * & 0 & * \\ 0 & 0 & * & * \end{array} \right) \end{matrix}$$

A zero indicates all coefficients in this part of the matrix are 0 because these monomials have been eliminated by setting all variables in  $W_1$  or  $W_2$  to zero. A \* indicates that the coefficients in that part of the matrix have not been lost due to fixing variables in  $W_1$  and  $W_2$  to zero.

For a matrix  $H$  and a set of monomials  $U$ , let  $H|_U$  denote the submatrix of  $H$  restricted to columns indexed by monomials in  $U$ , and let  $[H]$  denote the  $\mathbb{F}_2$ -space spanned by  $H$ . Both  $H_1$  and  $H_2$  are projections of a basis for the space spanned by the polynomials in  $\mathcal{H}$ . Since none of the monomials in  $U_{\bar{1},\bar{2}}$  have been set to zero by either  $W_1$  or  $W_2$  we expect that  $[H_1|_{U_{\bar{1},\bar{2}}}] = [H_2|_{U_{\bar{1},\bar{2}}}]$ . This fact comes with the caveat that  $r$  was chosen small enough such that the ranks of  $H_1|_{U_{\bar{1},\bar{2}}}$  and  $H_2|_{U_{\bar{1},\bar{2}}}$  are both  $d+t+\binom{k}{2}+1$ . This can be checked during the attack, and if it fails the attacker just reduces  $r$ . Referring back to the overall idea of gluing, these two bases for the same space are the overlapping parts of the pieces given by  $H_1$  and  $H_2$ .

Let  $Z$  be a basis for the kernel of  $H_2^1|_{U_{\bar{1},\bar{2}}}$ , with kernel elements written as  $z = (z_1, z_2)$  such that  $zH_2^1 = z_1H_1 + z_2H_2$ . We know that  $\dim(Z) = d+t+\binom{k}{2}+1$  since  $H_1|_{U_{\bar{1},\bar{2}}}$  and  $H_2|_{U_{\bar{1},\bar{2}}}$  are bases for the same space. Finally, create the matrix  $H_{1,2}$  by computing the following rows for each element  $(z_1, z_2) \in Z$  and adding them as rows to  $H_{1,2}$ :

$$(0 \quad z_1H_1|_{U_{\bar{1},2}} \quad z_2H_2|_{U_{1,\bar{2}}} \quad z_1H_1|_{U_{\bar{1},\bar{2}}})$$

The matrix  $H_{1,2}$  is then a projected basis for  $\mathcal{H}$ , where only monomials that get eliminated by both  $W_1$  and  $W_2$  are missing. In the comparison with pieces of a picture, the two pieces given by  $H_1$  and  $H_2$  have now been glued together along their overlapping part  $U_{\bar{1},\bar{2}}$  to form one larger piece  $H_{1,2}$ . The general gluing of two matrices like this is given in Algorithm 1.

---

**Algorithm 1**  $\text{Glue}(H_1, H_2, U_1, U_2, U_3, U_4)$

---

**Require:** Matrices  $H_1$  and  $H_2$  plus four disjoint sets  $U_1, U_2, U_3, U_4$  of column indices, such that  $[H_1|_{U_4}] = [H_2|_{U_4}]$ ,  $H_1|_{U_1 \cup U_3} = 0$ , and  $H_2|_{U_1 \cup U_2} = 0$ .

**Ensure:** Matrix  $H_{1,2}$  where  $[H_{1,2}|_{U_4}] = [H_1|_{U_4}] = [H_2|_{U_4}]$ ,  $[H_{1,2}|_{U_2}] = [H_1|_{U_2}]$ , and  $[H_{1,2}|_{U_3}] = [H_2|_{U_3}]$ .

$$H_2^1 \leftarrow \begin{pmatrix} H_1 \\ H_2 \end{pmatrix}$$

$$Z \leftarrow \ker(H_2^1)$$

$$H_{1,2} \leftarrow \emptyset$$

**for**  $(z_1, z_2) \in Z$  **do**

Add  $(0 \quad z_1H_1|_{U_2} \quad z_2H_2|_{U_3} \quad z_1H_1|_{U_4})$  as row in  $H_{1,2}$

**end for**

Return  $H_{1,2}$ .

---

To glue the next piece  $H_3$  onto  $H_{1,2}$ , we proceed by dividing the set of quadratic monomials into the following four disjoint sets:

- $U_{1,2,3} = \{\text{monomials set to 0 by } W_1, W_2, \text{ and } W_3\}$ .
- $U_{\overline{1},2,3} = \{\text{monomials set to 0 by } W_3, \text{ but not by both } W_1 \text{ and } W_2\}$ .
- $U_{1,2,\overline{3}} = \{\text{monomials set to 0 by both } W_1 \text{ and } W_2, \text{ but not by } W_3\}$ .
- $U_{\overline{1},\overline{2},\overline{3}} = \{\text{monomials not set to 0 by both } W_1 \text{ and } W_2, \text{ and not set to 0 by } W_3\}$ .

Then we call Algorithm 1 to compute  $H_{1,2,3}$ :

$$H_{1,2,3} = \text{Glue}(H_{1,2}, H_3, U_{1,2,3}, U_{\overline{1},2,3}, U_{1,2,\overline{3}}, U_{\overline{1},\overline{2},\overline{3}}).$$

Note that we can expect  $|U_{\overline{1},\overline{2},\overline{3}}| > |U_{\overline{1},\overline{2}}|$ , as  $U_{\overline{1},\overline{2},\overline{3}}$  contains all monomials from the three sets  $U_{\overline{1},2}, U_{1,\overline{2}}$ , and  $U_{\overline{1},\overline{2}}$  that are not set to zero by  $W_3$ . So the requirement that the ranks of  $H_{1,2}$  and  $H_3$  are  $d + t + \binom{k}{2} + 1$  in the overlapping part we glue along is more likely to be satisfied the more pieces are already glued.

We continue like this, re-dividing the set of all monomials in  $\overline{B}(d)_2$  into four disjoint subsets and recursively computing

$$H_{1,\dots,i} = \text{Glue}(H_{1,\dots,i-1}, H_i, U_{1,\dots,i}, U_{\overline{1},\dots,i-1,i}, U_{1,\dots,i-1,\overline{i}}, U_{\overline{1},\dots,i-1,\overline{i}}),$$

for  $i = 2, \dots, \rho$ . When we glue the last time, the set  $U_{1,\dots,\rho}$  will be empty since the sets  $W_1, \dots, W_\rho$  have been constructed such that there is at least one  $W_\eta$  that does not set  $x_i x_j$  to zero, for all pairs  $(i, j)$ . So there is no monomial that gets set to zero by all of  $W_1, \dots, W_\rho$ . This means that  $H_{1,\dots,\rho}$  will show the complete picture, namely a basis for the full, unprojected,  $\mathcal{H}$ .

### 7.3 Retrieving the Linear Forms from $ip$

The rows of  $H_{1,\dots,\rho}$  give a set of generators (polynomials) for the space spanned by  $\mathcal{H}$ . These polynomials will in general form a different basis than the polynomials given as  $\mathcal{H}$ , so we will label them  $\mathcal{G}$ . The next goal is to recover the  $k$  linear forms that are generators for  $\langle v_1, \dots, v_k \rangle$ . In order to simplify our arguments we will assume  $k \geq 5$ . The cases  $2 \leq k \leq 4$  will be discussed in Remark 2.

Consider the kernel of the homogeneous Macaulay matrix  $\overline{\mathcal{M}}_3(\mathcal{G})$ . From the definition of  $\mathcal{H}$  (Eq. (7.3)), we find that the space spanned by  $\mathcal{H}$  (and  $\mathcal{G}$ ) contains all the homogeneous nude Dob-polynomials  $f_1^h, \dots, f_d^h$ , as well as all the combinations  $(v_i v_j)^h$ ,  $1 \leq i < j \leq k$ . Note that  $v_i (v_i v_j)^h = 0$ , and  $v_j (v_i v_j)^h = 0$  in  $\overline{B}(d)$ . Hence each polynomial  $(v_i v_j)^h$  generates two syzygies of degree 3 in this ring. The nude Dob-polynomials will also generate the  $2d$  kernel elements associated with the degree fall polynomials discussed in Section 3.3. We would like to separate these two types of kernel elements. To this end, we construct a smaller system,  $\mathcal{G}'$ , by removing three polynomials from  $\mathcal{G}$  that are in the span of  $\{p_1^h, \dots, p_d^h\}$ . It is easy to find three such polynomials to remove, since  $\{p_1^h, \dots, p_d^h\}$  are fully known. We noted in Section 5.2 that removing a small number of  $s$  public polynomials has similar behaviour to applying  $Q_+$  with  $s = t$ . Eq. (5.3) then yields  $N_3^{(0,0)} = 2d - 3d$ , and hence that there will be no contribution to the kernel of  $\overline{\mathcal{M}}_3(\mathcal{G}')$  from the nude Dob polynomials.

On the other hand, some of the kernel elements generated by combinations of the  $(v_i v_j)^h$ -elements can still be observed for  $\mathcal{G}'$  at degree 3. More specifically, suppose  $\mathcal{G}'$  was created from  $\mathcal{G}$  by removing  $p_1^h, p_2^h$  and  $p_3^h$ . Then  $\text{Span}(\mathcal{G}')$  may not necessarily contain  $(v_1 v_j)^h$  itself, for any  $2 \leq j \leq k$ , but it will contain the combination  $(v_1 v_j)^h + b_{1,j} p_1^h + b_{2,j} p_2^h + b_{3,j} p_3^h$ , for some  $b_{1,j}, b_{2,j}, b_{3,j} \in \mathbb{F}_2$ . By considering these equations for  $j = 2, \dots, k$ , we see it is possible to eliminate the terms containing  $p_1^h, p_2^h$  and  $p_3^h$  by adding together appropriate polynomials on the form  $(v_1 v_j)^h + b_{1,j} p_1^h + b_{2,j} p_2^h + b_{3,j} p_3^h$ . Here we use the assumption that  $k \geq 5$ . We therefore find that  $\text{Span}(\mathcal{G}')$  will contain a polynomial  $z_1 = \sum_{j=2}^k a_j (v_1 v_j)^h$ , where  $a_2, \dots, a_k \in \mathbb{F}_2$  are not all 0. The polynomial  $v_1 z_1$  will subsequently be reduced to 0 over  $\overline{B}(d)$ . Similarly, we are guaranteed to find polynomials  $z_2, \dots, z_k$  which can be given as sums of pure  $(v_i v_j)^h$ -polynomials, which will be reduced to zero when multiplied with  $v_2, \dots, v_k$ , respectively.

We expect that these are the only contributors to the kernel of  $\mathcal{G}'$  and that they only become 0 when multiplied with their corresponding  $v_i$ . The attacker can compute the kernel of  $\overline{\mathcal{M}}_3(\mathcal{G}')$ , and write each of the kernel elements as  $\sum l_i g_i = 0$ , where  $g_i \in \mathcal{G}'$ , and each  $l_i$  is a known linear combination of  $\{x_1, \dots, x_d\}$ . We know that  $z_i = \sum d_{i,j} g_j$ , for some unknown  $d_{i,j} \in \mathbb{F}_2$ , and therefore we also know that all the known  $l_i$ -polynomials must lie in  $\text{Span}(\{v_1, \dots, v_k\})$ . It follows that an attacker can retrieve a basis  $v_1^*, \dots, v_k^*$  of  $\langle v_1, \dots, v_k \rangle$ , by choosing  $k$  linearly independent polynomials among these  $l_i$ 's.

*Remark 2.* In the text above, we remove 3 polynomials from  $\mathcal{G}$ , and assumed  $k \geq 5$  in order to guarantee the existence of the polynomials  $z_i$ .

When  $k = 4$ , we know we will have the polynomials  $(v_1 v_j)^h + b_{1,j} p_1^h + b_{2,j} p_2^h + b_{3,j} p_3^h$  in  $\text{Span}(\mathcal{G}')$ , for  $j = 2, 3, 4$  and some random values  $b_{i,j} \in \mathbb{F}_2$ . If the  $3 \times 3$  matrix

$$\begin{pmatrix} b_{1,2} & b_{2,2} & b_{3,2} \\ b_{1,3} & b_{2,3} & b_{3,3} \\ b_{1,4} & b_{2,4} & b_{3,4} \end{pmatrix}$$

has full rank, it is not possible to find a polynomial in  $\text{Span}(\mathcal{G}')$  that is a non-trivial sum of pure  $(v_1 v_j)^h$ -terms, and hence not possible to create  $z_1$  as described above. Likewise,  $z_2, z_3, z_4$  will not exist in  $\text{Span}(\mathcal{G}')$  if their corresponding  $3 \times 3$  matrices have full rank. However, the number of  $3 \times 3$  matrices over  $\mathbb{F}_2$  with rank 3 is only 168 out of the 512 possible matrices. So the probability that all four matrices concerning  $z_1, z_2, z_3, z_4$  have full rank is only  $(168/512)^4 \approx 0.0116$ . In other words, just following the procedure given for  $k \geq 5$  will also succeed in finding at least one kernel element for  $k = 4$  with probability greater than 98.8%. Finding a single kernel element is enough to recover all of  $\{v_1^*, v_2^*, v_3^*, v_4^*\}$ , since the space spanned by them is only of dimension 4. From one kernel element we get at least  $d + t + \binom{4}{2} - 3$  linear combinations in  $\text{Span}(\{v_1, v_2, v_3, v_4\})$ , making it likely that a basis can be found. In the unlikely case that this fails, the attacker can always remove a different set of three polynomials instead of  $p_1^h, p_2^h, p_3^h$  and try the whole procedure again.

If  $k = 2, 3$  the attacker can try finding non-trivial elements in the kernel of  $\overline{\mathcal{M}}_3(\mathcal{G}')$  by removing different sets of three polynomials from  $\{p_1^h, \dots, p_d^h\}$ .

Even for  $k = 2$  the attacker will succeed in finding the single kernel element generated by  $(v_1 v_2)^h$  with more than 95% probability after 23 tries. Moreover, for  $k \leq 3$  we have  $\binom{k}{2} \leq k$ , so we can alternatively just treat the unknown  $(v_i v_j)^h$ -polynomials as belonging to the polynomials in  $Q_+$  in this case. That is, for  $k = 2, 3$  we can just as well assume we have  $t + k$  polynomials in  $Q_+$  and no *ip* modifier. We conclude that an attacker will not have any problems recovering a basis for  $\langle v_1, \dots, v_k \rangle$  in the cases  $k \leq 4$ .

The attacker has now recovered the quadratic part of the secret modifiers, but lacks any information about the linear part from the  $Q_+$  modifier. A natural way to decrypt might now be to guess the values of  $v_1^*, \dots, v_k^*, q_1^*, \dots, q_t^*$  when evaluated in the plaintext, and try to solve the resulting system by Gröbner basis computation. A heuristic analysis of this strategy can be found in sections 6.4 and 6.5 in [43]. While this is a great improvement over a straightforward Gröbner basis attack on the Dob encryption system, the presence of the linear forms from  $Q_+$  increases the complexity compared to nude Dob. This is especially true for larger  $t$ . In the following subsections we suggest a stronger version of the attack that recovers an equivalent key for the Dob encryption schemes. The total complexity is also greatly reduced when compared to the approach of [43].

#### 7.4 Retrieving the Quadratic Forms of $\mathcal{F}$

Next, we want to recover a system of  $d$  homogeneous quadratic polynomials  $\mathcal{F}'$ , such that  $\text{Span}(\mathcal{F}') = \text{Span}(\mathcal{F}^h)$ . This is a non-trivial step, even with all the information recovered so far, since it is not a priori clear how the polynomials  $(v_i^* v_j^*)^h$  and  $q_l^*$  have been added to the nude Dob polynomials.

Recall from the previous subsection that the kernel of  $\overline{\mathcal{M}}_3(\mathcal{G})$  will be generated by the  $2d$  degree fall polynomials from nude Dob, as well as the combinations  $(v_i v_j)^h$ . If we are able to separate these effects, we can learn combinations of the nude Dob polynomials from the first set of generators. To this end, we start by fixing a change of variables, such that the first  $k$  variables correspond to the linear combinations  $v_1^*, \dots, v_k^*$ . More precisely, fix a linear, invertible mapping  $L^*$  sending the variables  $x_1, \dots, x_d$  to  $x_1^*, \dots, x_d^*$ , with the property that  $v_i^*(x_1, \dots, x_d) \mapsto x_i^*$ , for  $1 \leq i \leq k$ . Apart from the restriction that  $L^*$  must be invertible and linear combinations  $v_i^*$  must be mapped to the single variables  $x_i^*$ , the rest of  $L^*$  can be chosen arbitrarily.

We define  $\mathcal{G}^*$  to be the polynomial system  $\mathcal{G}$  under this change of variables, i.e., the system consisting of the polynomials

$$g_i^* = g_i(x_1^*, \dots, x_d^*) = g_i \circ L^*(x_1, \dots, x_d), \quad \text{for } 1 \leq i \leq d + t + \binom{k}{2} + 1.$$

Note that fixing one of the first  $k$  variables  $x_i^*$  to zero amounts to a projection along  $v_i^* = 0$ . It follows that fixing all but one of the  $k$  first  $x_i^*$  variables is sufficient to ensure that all combinations  $(v_i v_j)^*$  will vanish. For each  $1 \leq i \leq k$ , we define the variable set  $W_i = \{x_1^*, \dots, x_{i-1}^*, x_{i+1}^*, \dots, x_k^*\}$ , i.e., the set containing

the  $k$  first  $x^*$ -variables, with the exception of  $x_i^*$ . By construction of  $\mathcal{G}$ , and due to the remark outlined above, the projected system  $\pi_{W_i}(\mathcal{G}^*)$ , for  $1 \leq i \leq k$ , will only contain  $d+1+t$  linearly independent polynomials. By a slight abuse of notation we will let  $\pi_{W_i}(\mathcal{G}^*)$  denote any fixed basis for these linearly independent polynomials.

Without the influence of the  $(v_i^* v_j^*)^h$  polynomials, the matrix  $\overline{\mathcal{M}}_3(\pi_{W_1}(\mathcal{G}^*))$  will now have a kernel of size  $2d$ , caused by the projected nude Dob polynomials. Each such kernel element can be written as

$$x_1^* \left( \sum_{i=1}^{d+1+t} a_{1,i} \pi_{W_1}(g_i^*) \right) + \dots + x_d^* \left( \sum_{i=1}^{d+1+t} a_{d,i} \pi_{W_1}(g_i^*) \right) = 0, \quad (7.4)$$

for constants  $a_{j,i} \in \mathbb{F}_2$ . Recall that  $f_i$  denotes a nude Dob polynomial, and write  $f_i^* = f_i^h \circ L^*(x_1, \dots, x_d)$ . Since the kernel elements come from the nude Dob polynomials, each combination  $\left( \sum_{i=1}^{d+1+t} a_{j,i} \pi_{W_1}(g_i^*) \right)$  in Eq. (7.4) will lie in the span of  $\{\pi_{W_1}(f_1^*), \dots, \pi_{W_1}(f_d^*)\}$ . It follows that an attacker is able to recover a basis for  $\text{Span}(\{\pi_{W_1}(f_1^*), \dots, \pi_{W_1}(f_d^*)\})$ , from the kernel of  $\overline{\mathcal{M}}_3(\pi_{W_1}(\mathcal{G}^*))$ . This procedure is repeated for the variable sets  $W_i$ ,  $1 \leq i \leq k$ , and the resulting bases are glued together using the procedure described in Section 7.2.

One drawback of using the variable sets  $W_i$  is that the gluing procedure does not give information about the monomials  $x_i^* x_j^*$ ,  $1 \leq i, j \leq k$ . Indeed, at this point we have recovered  $d$  polynomials of the form

$$z_i = h_i^*(x_{k+1}^*, \dots, x_d^*) + u_i^*(x_{k+1}^*, \dots, x_d^*) s_i^*(x_1^*, \dots, x_k^*) + \sum_{1 \leq l < j \leq k} y_{l,j}^i x_l^* x_j^*,$$

where  $h_i^*$  is a known quadratic polynomial,  $u_i^*$  and  $s_i^*$  are known linear polynomials, but the  $y_{l,j}^i$ 's are unknown constants in  $\mathbb{F}_2$ . The polynomials  $z_1, \dots, z_d$  will only form a basis for  $\text{Span}(\{f_1^*, \dots, f_d^*\})$  if the  $y_{l,j}^i$ 's are chosen correctly. We will once more rely on the fact that the degree fall polynomials from nude Dob will yield distinguishable polynomials. Indeed, there will now be  $2d$  combinations

$$\begin{aligned} \sum_{r=1}^d \sum_{i=1}^d a_{r,s} x_r^* z_i = \sum_{r=1}^d \sum_{1 \leq l < j \leq k} x_l^* x_j^* x_r^* \left( \sum_{i=1}^d a_{r,i} y_{l,j}^i + c_{l,j,r} \right) \\ + \{\text{Quadratic terms in the } x^*\text{-variables}\}, \end{aligned} \quad (7.5)$$

where  $a_{r,s}$  and  $c_{l,j,r}$  are constants in  $\mathbb{F}_2$  ( $c_{l,j,r}$  is in turn determined by the contribution of the  $a_{r,s}$ 's and the  $u_i^* s_i^*$  part of the various  $z_i$ 's). Said differently, all monomials of degree 3 (in the  $x^*$ -variables) contains at least 2 variables in  $\{x_1^*, \dots, x_k^*\}$ . These  $2d$  combinations can easily be found by constructing the matrix  $\overline{\mathcal{M}}_3(\{z_1, \dots, z_d\})$ , remove the columns associated with the aforementioned monomials, and find a basis for the resulting kernel. In particular, this recovers the constants  $a_{r,s}$  and  $c_{l,j,r}$  in Eq. (7.5). Since each of the cubic terms will cancel out for the correct choice of  $y_{l,j}^i$ -variables, we can set up linear equations of the form  $\sum_{i=1}^d a_{r,i} y_{l,j}^i + c_{l,j,r} = 0$ . There are  $2d$  equations of the form in (7.5), each

having  $\binom{k}{2}(d-k) + \binom{k}{3}$  cubic terms, which gives a total of  $2d \left( \binom{k}{2}(d-k) + \binom{k}{3} \right)$  linear equations. As there are only  $d \binom{k}{2}$   $y$ -variables, we expect a unique solution for this system. Once a basis for  $\text{Span}(\{f_1^*, \dots, f_d^*\})$  is recovered, we can transform it back to the original variable basis using  $(L^*)^{-1}$ , which yields  $\mathcal{F}^b$ , a basis for  $\text{Span}(\mathcal{F}^h)$ . We want to use this to fix another basis  $\mathcal{F}'$  for  $\text{Span}(\mathcal{F}^h)$ , a quadratic map  $H'_{ip} : \mathbb{F}_2^k \rightarrow \mathbb{F}_2^d$  and a linear map  $H'_{Q_+} : \mathbb{F}_2^t \rightarrow \mathbb{F}_2^d$ , such that the equality of the form

$$\mathcal{P}^h = \mathcal{F}' + H'_{ip}(v_1^*, \dots, v_k^*) + H'_{Q_+}(q_1^*, \dots, q_t^*), \quad (7.6)$$

holds. Recall that at this point in the attack,  $q_1^*, \dots, q_t^*$  may still depend on the random polynomial  $p_R$  (if  $p_R$  is quadratic). We remove this dependency by going through the possible tuples  $(e_1, \dots, e_t) \in \mathbb{F}_2^t$  until each polynomial in  $\mathcal{P}^h$  can be written as a linear combination of the polynomials in  $\mathcal{F}^b$ , the combinations  $(v_i^* v_j^*)^h$ , and  $q_1^* + e_1 p_R, \dots, q_t^* + e_t p_R$ , that yields a valid choice of  $\mathcal{F}'$ ,  $H'_{ip}$  and  $H'_{Q_+}$ . Since  $2^t$  is small for the Dob scheme, and each step is checked by linear algebra, recovering the description in Eq. (7.6) is fast. From here on, we will write  $q_1^*, \dots, q_t^*$  to mean the polynomials where the effect of  $p_R$  has been removed.

## 7.5 Retrieving Equivalent Matrices for $S$ and $T$

The attacker has now recovered a system of homogeneous quadratic polynomials  $\mathcal{F}'$ , with the knowledge that  $T^b \circ \mathcal{F}' = (T \circ \mathcal{C} \circ S)^h = \mathcal{F}^h$ , for some invertible linear map  $T^b$ . We now want to use rank techniques in order to recover matrices for  $S'$  and  $T'$  such that the triplets  $(T, \mathcal{C}, S)^h$  and  $(T', \mathcal{C}', S')^h$  are equivalent, in the sense of Definition 4. Moreover, defining  $F^h$  as  $F^h = X^{2^m+1} + X^3$ ,  $\mathcal{C}'$  will be the multivariate representation of a univariate polynomial  $F'(X)$ , such that  $F'(X) = \lambda F^h(X)$  for some  $\lambda \in \mathbb{F}_{2^d}$ .

To this end, we will closely follow the analysis of the HFE system by Bettale, Faugère and Perret [6], and we refer to this work for much of the underlying details. As a consequence, the following subsection will only provide a brief overview of the theory, as well as a discussion of the parts where a rank attack on the Dobbertin system differs from that of a HFE system. To avoid confusion with other notation used throughout the paper, we will write all matrices introduced in this subsection in boldface.

Consider the basis  $\underline{X} = (X, X^2, \dots, X^{2^d-1})$ , and let  $\mathbf{A}$  be any  $d \times d$  matrix over  $\mathbb{F}_{2^d}$  representing the quadratic form of  $F = X^{2^m+1} + X^3 + X$ , i.e.,  $F^h(X) = \underline{X} \mathbf{A} \underline{X}^\top$ . We then define the symmetric matrix associated to  $F^h$ , to be  $(\mathbf{F}^h)^{*0} = \mathbf{A} + \mathbf{A}^\top$ , which will be the  $d \times d$  matrix given by:

$$\begin{cases} 1, & \text{for entries } (1, 2), (1, m+1), (2, 1), (m+1, 1) \\ 0, & \text{otherwise.} \end{cases} \quad (7.7)$$

In a similar manner, we define  $(\mathbf{F}^h)^{*i}$  to be the symmetric matrix associated with  $(F^h(X))^{2^i}$ . This can be seen as the matrix described in (7.7), where all

entries are shifted  $i$  places to the right and  $i$  places down (wrapping around when necessary). In particular, all matrices  $(\mathbf{F}^h)^{*i}$  will have rank 2 for  $0 \leq i \leq d-1$ . Let  $f'_1, \dots, f'_d$  be the homogeneous quadratic system  $\mathcal{F}'$ , that was recovered in section 7.4. We similarly consider the associated symmetric matrices, over the multivariate basis  $\underline{x} = (x_1, \dots, x_d)$ , as any  $d \times d$  matrix  $\mathbf{B}_i$  over  $\mathbb{F}_2$ , satisfying  $f'_i = \underline{x}\mathbf{B}_i\underline{x}^\top$ . Moreover, we write  $(\mathbf{f}'_i)^* = \mathbf{B}_i + \mathbf{B}_i^\top$ .

Let  $\mathbf{M}$  be an invertible  $d \times d$  matrix over  $\mathbb{F}_{2^d}$ , that is associated with the fixed vector basis of  $\mathbb{F}_{2^d}$  over  $\mathbb{F}_2$  (see Proposition 2 in [6]), and write  $\mathbf{W} = \mathbf{S}\mathbf{M}$ . Moreover, define  $\mathbf{U} = ((T^b)^{-1}T^{-1}\mathbf{M}) \otimes \mathbf{I}_d$ , where  $\mathbf{I}_d$  is the  $d \times d$  identity matrix,  $\otimes$  is the Kronecker product, and  $T^b$  the invertible matrix such that  $\mathcal{F}^h = T^b \circ \mathcal{F}'$ . In particular,  $\mathbf{U}$  is an invertible  $d^2 \times d^2$  matrix over  $\mathbb{F}_{2^d}$  such that the following equation holds:

$$((\mathbf{f}'_1)^* | \dots | (\mathbf{f}'_d)^*) \mathbf{U} = \left( \mathbf{W} (\mathbf{F}^h)^{*0} \mathbf{W}^\top | \dots | \mathbf{W} (\mathbf{F}^h)^{*d-1} \mathbf{W}^\top \right), \quad (7.8)$$

where  $|$  denotes horizontal concatenation (this follows from the same arguments leading up to Equation (3) in [6], using  $TT^b$  in place of the matrix  $\mathbf{T}$ ). Since  $\mathbf{W}$  is invertible, it follows that  $\mathbf{W} (\mathbf{F}^h)^{*i} \mathbf{W}^\top$  will have rank 2 for  $0 \leq i \leq d-1$ , and an attacker can now learn information about the secret matrix  $\mathbf{U}$  by solving a MinRank problem of rank 2 using the known matrices  $(\mathbf{f}'_i)^*$ ,  $0 \leq i \leq d-1$ . More specifically, we wish to find a tuple  $(z_1, \dots, z_d) \in \mathbb{F}_{2^d}^d$ , such that the matrix  $\sum_{i=1}^d z_i (\mathbf{f}'_i)^*$  has rank 2. Efficient methods for solving this problem include the minors modelling [23], and support minors modelling [3]. Due to the equivalent keys predicted in section 3.5, we expect many different solutions to the MinRank problem. As is common practice for HFE (see e.g. Section 5 of [6]), we suggest fixing  $z_1 = 1$ , and solve for the remaining  $z_i$ 's. Once a solution to the MinRank problem has been found, we let it form the first column of a matrix  $\mathbf{T}'^{-1}\mathbf{M} \in \mathbb{F}_{2^d}^{d \times d}$ , and construct the remaining columns by iterative Frobenius transforms, as described in Proposition 3 of [6]. We expect this matrix  $\mathbf{T}$  is part of an equivalent key for the Dob system, and write  $(\mathbf{T}', \mathcal{C}', \mathbf{S}')^h$  for a triplet that is equivalent to  $(T, \mathcal{C}, S)^h$ . We also write  $\mathbf{W}' = \mathbf{S}'\mathbf{M}$ , and  $F'(X)$  for the univariate polynomial associated with  $\mathcal{C}'$ . Let  $\mathbf{T}'^{-1}\mathbf{M}[i]$  denote the  $i$ -th column of  $\mathbf{T}'^{-1}\mathbf{M}$ . Then

$$((\mathbf{f}'_1)^* | \dots | (\mathbf{f}'_d)^*) (\mathbf{T}'^{-1}\mathbf{M}[i] \otimes \mathbf{I}_d) = \mathbf{W}' (\mathbf{F}')^{*i} \mathbf{W}'^\top,$$

follows from Eq. (7.8), and the definition of equivalent triplets. Moreover, the attacker can in particular easily compute

$$\mathbf{K} = \text{Ker} \left( ((\mathbf{f}'_1)^* | \dots | (\mathbf{f}'_d)^*) (\mathbf{T}'^{-1}\mathbf{M}[1] \otimes \mathbf{I}_d) \right) = \text{Ker} \left( \mathbf{W}' (\mathbf{F}')^{*0} \right), \quad (7.9)$$

where we let  $\mathbf{K}$  be the matrix of a fixed basis for the left kernel  $\text{Ker}$ . Since  $(\mathbf{F}')^{*0}$  has rank 2,  $\mathbf{K}$  is a  $(d-2) \times d$  matrix over  $\mathbb{F}_{2^d}$ . From Eq. (7.9) it also follows that  $\mathbf{K}\mathbf{W}' = \text{Ker} \left( (\mathbf{F}')^{*0} \right)$ . Recall from section 3.5 that we now expect the equivalent central map to be of the form  $F'(X) = \gamma F^h(X)$ , for some  $\gamma \in \mathbb{F}_{2^d}$ . Upon inspection of (7.7), we then note that there are two restrictions on the



columns of  $\mathbf{KW}'$ . Firstly, column 1 is zero and secondly, column 2 is equal to column  $m + 1$ . The same restrictions are generalised to the kernel of  $(\mathbf{F}')^{*i}$ , by shifting the entries  $i$  places to the right (with wrap-around). In the same manner as Lemma 7 in [6],  $\mathbf{K}$  is related to these latter kernels through Frobenius transforms<sup>9</sup>, in the sense that

$$\text{Frob}_i(\mathbf{K})\mathbf{W}' = \text{Ker}\left((\mathbf{F}')^{*i}\right), \text{ for } 0 \leq i \leq d - 1, \quad (7.10)$$

where  $\text{Frob}_i(\mathbf{K})$  raises all the entries in  $\mathbf{K}$  to the power  $2^i$ . If we treat each entry of  $\mathbf{W}'$  as a variable, we find that the restrictions on the columns, applied to the various  $\text{Frob}_i(\mathbf{K})\mathbf{W}'$   $0 \leq i \leq d - 1$  from Eq. (7.10), yields a total of  $2d(d - 2)$  linear equations in the  $d^2$   $\mathbf{W}'$ -variables. In addition, any column of  $\mathbf{W}'$  is equal to applying the Frobenius to each entry of the previous column (Proposition 3 in [6]). In our experiments, we find that these conditions are sufficient to recover a unique  $\mathbf{W}'$ , and hence also  $\mathbf{S}'$ .

## 7.6 Retrieving the Linear Forms of the Key

Up until this point of the attack, we have been focusing on the homogeneous quadratic parts of the key. We are now in a position to address the question of recovering the linear parts as well. We will approach this through finding the linear parts of the maps  $H'_{ip}$ ,  $H'_{Q+}$  and  $\mathcal{F}'$ , from Eq. (7.6).

Let  $\mathcal{L}'$  denote the  $d$  linear forms satisfying  $\mathcal{F} = T^b \circ (\mathcal{F}' + \mathcal{L}')$ . Recall that the central map we have recovered for  $\mathcal{F}'$ , will have a univariate polynomial on the form  $\gamma F^h(X)$ , for some non zero  $\gamma \in \mathbb{F}_{2^d}$ . Hence, we have

$$\mathcal{F}' + \mathcal{L}' = T' \circ \phi^{-1} \circ \left( \lambda(X^{2^m+1} + X^3 + X) \right) \circ \phi \circ S',$$

where  $T'$  and  $S'$  are the linear maps associated with the matrices  $\mathbf{T}'$  and  $\mathbf{S}'$  recovered in the previous subsection. Since the monomials  $X^{2^m+1}$  and  $X^3$  only depend on the known homogeneous quadratic  $\mathcal{F}'$  we can, using Eq. (7.6), find  $\lambda$  as the coefficient of these two terms in the univariate polynomial

$$\phi \circ T'^{-1} \circ \left( \mathcal{P}^h - H'_{ip}(v_1^*, \dots, v_k^*) - H'_{Q+}(q_1^*, \dots, q_t^*) \right) \circ S'^{-1} \circ \phi^{-1}. \quad (7.11)$$

We remark that the action of  $\phi \circ (\cdot) \circ \phi^{-1}$ , i.e. lifting the multivariate polynomial system to a univariate polynomial over the extension field, can easily be done by an interpolation step once the multivariate polynomials in the middle of (7.11) have been computed. Indeed, since the potentially non-zero terms of the

<sup>9</sup> Eq. (7.10) can be derived by adapting the proof of Lemma 7 in [6] to the case of the Dobbartin permutation. Indeed, to adapt this proof we need only check that the entries of  $\text{Ker}\left((\mathbf{F}')^{*0}\right)$  can be chosen in  $\mathbb{F}_2$ , and that the kernel of  $(\mathbf{F}')^{*i}$  can be obtained by shifting the columns of  $\text{Ker}\left((\mathbf{F}')^{*0}\right)$   $i$  places to the right. This follows from our recent discussion in the text.

resulting univariate polynomial will only be the  $d$  linear monomials on the form  $X^{2^i}$ , as well as  $X^{2^m+1}$  and  $X^3$ , we need only consider  $d + 2$  data points. These data points are constructed through evaluation of the multivariate system, and then mapped to the extension field by  $\phi$ . The interpolation itself now reduces to solving a linear system of  $d + 2$  variables and equations over  $\mathbb{F}_{2^d}$ .

The remaining linear part is now generated by  $t + k$  linear forms; the known  $v_1^*, \dots, v_k^*$ , as well as the unknown  $l_1^*, \dots, l_t^*$ , which are the linear parts belonging to  $q_1^*, \dots, q_t^*$ . Once  $\lambda$  has been found, we can set up the following equality

$$\begin{aligned} (H'_{ip})^l(v_1^*, \dots, v_k^*) + H_{Q_+}^*(l_1^*, \dots, l_t^*) &= \mathcal{P} - H'_{ip}(v_1^*, \dots, v_k^*) - H'_{Q_+}(q_1^*, \dots, q_t^*) \\ &\quad - T' \circ \phi^{-1} \circ \left( \lambda(X^{2^m+1} + X^3 + X) \right) \circ \phi \circ S', \end{aligned} \tag{7.12}$$

where  $(H'_{ip})^l$  is an unknown linear map  $\mathbb{F}_2^k \rightarrow \mathbb{F}_2^d$ . Note that  $l_1^*, \dots, l_t^*$  are mixed using the linear map  $H_{Q_+}^*$  that was found in Section 7.4. The right hand side of Eq. (7.12) are  $d$  known linear forms in the  $x$ -variables. On the left hand side the unknown map  $(H'_{ip})^l$  can be described using  $dk$  constants in  $\mathbb{F}_2$ . While the map  $H'_{Q_+}$  is known, the unknown linear forms  $l_1^*, \dots, l_t^*$  can be described using  $dt$  constants in  $\mathbb{F}_2$ . Since the coefficient of each of the  $x_i$ -terms on the right hand side yields a constraint on these constants, Eq. (7.12) can be used to set up a system of  $d(t + k)$  variables in  $d^2$  linear equations. Despite having  $d > t + k$  in the Dob encryption scheme, we did not get a unique solution for  $(H'_{ip})^l$  and  $l_1^*, \dots, l_t^*$  in the experiments we have run. This matters little for the attack, as the attacker can simply fix any of the valid solutions of this system.

**An Equivalent Dob Key** The attacker has now recovered a description for the Dob scheme that allows to decrypt as efficiently as the legitimate user, which is

$$\mathcal{P} = \mathcal{F}' + \mathcal{L}' + \left( H'_{ip} + (H'_{ip})^l \right) (v_1^*, \dots, v_k^*) + H'_{Q_+}(q_1^* + l_1^*, \dots, q_t^* + l_t^*).$$

For an intercepted ciphertext, the attacker goes through the possible values for  $v_1^*, v_k^*, q_1^* + l_1^*, \dots, q_t^* + l_t^*$ , and inverts  $\mathcal{F}' + \mathcal{L}'$  as described in Section 3.2 (adapted to  $\lambda F(X)$ ).

## 7.7 Practical Verification of the Attack

We implemented and tested the attack in the computational algebra system Magma for the two toy examples outlined below. The implementation uses Magma's standard kernel method for finding the kernel of the Macaulay matrices described in Section 7.2, and solves the MinRank problem using the minors modelling with Magma's  $F_4$ . The implementation is available at [26].

**Example 2** *In the first toy example we consider an instance of the Dob encryption scheme with  $d = 45$ ,  $t = 1$  and  $k = 4$ . When fixing 15 variables,  $n = 30$ ,*

we find that no degree fall polynomials at degree 3, and at degree 4 we have  $N_4 = N_4^{(0,0)} = 487$ , as predicted by Eq. (5.7). When adding a randomly chosen homogeneous quadratic polynomial  $p_R$  to this system, we got 494 degree fall polynomials at degree 4, as predicted in Eq. (7.1). For simplicity, we used the three disjoint sets:  $W_1 = \{x_1, \dots, x_{15}\}$ ,  $W_2 = \{x_{16}, \dots, x_{30}\}$  and  $W_3 = \{x_{31}, \dots, x_{45}\}$ , to perform the gluing step detailed in Section 7.2.

We ran and verified the entirety of the attack as described in sections 7.1 – 7.6 for this case, and indeed found a working equivalent key.

**Example 3** In the second toy example we used parameters  $d = 63$ ,  $t = 1$  and  $k = 4$ . Fixing 21 variables, we find no degree fall polynomials at degree 3, and  $N_4 = N_4^{(0,0)} = 445$  degree fall polynomials at degree 4. Adding a random quadratic polynomial yields 452 degree fall polynomials at degree 4, as predicted in Eq. (7.1). As in Example 2, we divide into three equal sets:  $W_1 = \{x_1, \dots, x_{21}\}$ ,  $W_2 = \{x_{22}, \dots, x_{42}\}$  and  $W_3 = \{x_{43}, \dots, x_{63}\}$ .

For this instance we ran the steps described in sections 7.1 – 7.3, successfully finding the homogeneous quadratic polynomial  $q_1^*$ , as well as the linear forms  $v_1^*, \dots, v_4^*$ . However, we ran out of memory ( $\approx 256$  GB) when attempting to solve the MinRank problem described in Section 7.5.

## 7.8 Attack Complexity

We now analyze the complexity of performing the attack described in this section. Suppose an attacker fixes  $d - n$  variables in order to find  $\rho$  polynomial systems  $\mathcal{H}_1, \dots, \mathcal{H}_\rho$  from the kernel elements of Macaulay matrices of degree  $D_0 \geq 3$ . The gluing operations, determining the linear forms  $v_1^*, \dots, v_k^*$ , and the quadratic forms  $q_1^*, \dots, q_t^*$  only involve Macaulay matrices of degree at most three, and will hence be comparatively cheap. This is also the case when recovering  $\mathcal{F}^h$ , as described in Section 7.4. We assume that solving the MinRank problem described in Section 7.5 is comparable to solving a MinRank problem from an HFE system with extension field degree  $d$  and rank 2. Section 7 of [6] estimates the complexity of solving this problem using Minors Modelling to be  $\mathcal{O}\left(\left(\sum_{i=0}^3 \binom{d}{i}\right)^\omega\right)$ , where  $2 \leq \omega \leq 3$  is the linear algebra constant. The remainder of the attack described in sections 7.5 and 7.6 only involves solving linear equations systems whose complexities are negligible when compared to the previous steps.

We thus expect the complexity of the entire attack to be dominated by recovering generators for the polynomial systems  $\mathcal{H}_i$ . While the optimal choice of attack parameters may depend on the parameters of the Dob encryption scheme, as a rule of thumb it seems best to first minimize  $D_0$ , then  $n$ , and lastly  $\rho$ . In practice, minimizing  $n$  involves choosing the smallest  $n$  such that  $D_{reg}(d, n) > D_0$ , for a fixed  $d$ . Kernel elements of the resulting sparse, homogeneous Macaulay matrix can be found using a variant of the Wiedemann algorithm [38] (see also [11] for an implementation of a version adapted to the XL algorithm). Section VI of [38] shows that one kernel vector can be retrieved after three iterations

with probability  $> 0.7$ , and as a simplification we estimate the complexity of finding a sufficient number of kernel elements of the  $\rho$  Macaulay matrices, and hence also the total attack complexity, as

$$\rho \frac{3}{0.7} \left( t + \binom{k}{2} \right) \binom{n}{D_0}^2 \binom{n}{2}. \quad (7.13)$$

We discuss in greater detail how to estimate the attack complexity in the case of the 80-bit secure parameter set proposed in Section 2.4 of [27], in the following.

**Security of the Suggested Parameters.** Let  $d = 129$ , and  $t = k = 6$  for the Dob encryption scheme. Using equations (2.3) and (5.7) we find that it is not possible to choose an  $n$  such that  $N_4^{(0,0)}$  is positive, and  $D_{reg}(129, n) > 4$ . For degree 5, we find that  $n = 50$  is the smallest number such that  $N_5^{(0,0)}$  is positive, and  $D_{reg}(129, 50) > 5$ . Indeed, for this choice of parameters, we get:

$$N_5^{(0,0)} = 64024,$$

which is exactly the number of degree fall polynomials observed in the last row of Table 3. For this choice of parameters,  $\rho$  is upper bounded by 15, due to Lemma 7. In this case we can do even better, and use  $\rho = 11$ , as described in Appendix B. By the estimate given in (7.13) we find that the attack requires about  $2^{62}$  operations.

## 8 Conclusions

We have presented an analysis of the effectiveness the  $Q_+$  and  $ip$  modifications against algebraic attacks on big-field encryption schemes. The theory was applied to the  $C^*$  and Dob encryption schemes, along with a novel attack on the Dob construction. A natural question to ask is whether it is possible to find parameters for an efficient and secure version of the Dob encryption scheme. We have seen that the modifications of the Dob encryption scheme is not as effective as initially hoped in hiding the degree fall polynomials of nude Dob. Furthermore, an attacker has a lot of flexibility in fixing variables, and gluing together polynomials that reveals information about the secret modifications. Even if secure parameters could be found for degree five, there is always the question of how the number of degree fall polynomials grows for larger degrees, i.e., determining  $N_\nu$  for  $\nu > 5$ . For these reasons it seems likely that a significant increase to  $t, k$ , and/or  $d$  is needed, which would in turn have a large negative impact on decryption time and/or public key size.

Due to the similarities between the  $C^*$  and Dobbertin central map, our new attack can likely be generalized to variants of  $C^*$  using a combination of the  $ip$  and  $Q_+$  modifier. The  $C^*$  central map yields an even higher number of degree fall polynomials than the Dobbertin polynomial, making these variants likely less secure than the Dob encryption scheme. This is noteworthy, as  $ip$  has been

discussed in the literature as a possible tool to secure the basic  $C^*$  scheme. Adding the “plus” modifier, as in PMI+, only gives more degree fall polynomials and likely enhances the attack in this work. This is best seen in Eq. (7.1), where adding the single random polynomial  $p_R$  increases the number of degree fall polynomials by  $t + \binom{k}{2}$  compared to not adding  $p_R$ . We also noted at the end of Section 5.2, that the attack on another  $C^*$  encryption variant, EFLASH, can be understood using the framework presented in this paper. In conclusion we believe it will be very hard to find big-field multivariate encryption schemes that are both efficient and secure.

On the other hand, the analysis presented in this work may not prove much of a threat to the security of multivariate *signature* schemes, where the minus modifier can remove a large number of the public key. For instance, in [27] a version of the Dob signature scheme is suggested using  $d = 257$ , and removing 129 polynomials for 128-bit security. While we have noted that the minus modifier behaves similarly to  $Q_+$ , it seems unlikely that our techniques will be successful when such a large number of modifications are in place, even when degrees  $> 5$  are taken into account. It should be noted that signature schemes cannot rely on the minus modifier alone, as shown in [35]. Indeed, the Dob signature scheme is likely vulnerable to a version of this attack.

There are several directions where the ideas presented here may inspire future work. Firstly, the modifications are treated as ideals, whose dimensions can be examined. If different types of modifications, such as minus and vinegar, can be rigorously included in this framework, it could lead to a deeper understanding of the security of an even larger subclass of big-field schemes. Secondly, the attack introduces new tools for the cryptanalysis of multivariate schemes. The gluing technique allows an attacker to collect useful information after fixing a number of variables. As there is no need for correct guesses, the exponential factor usually associated with hybrid methods is avoided. Furthermore, the technique does not rely on heuristic assumptions on the relation between the first fall and solving degrees. It would be interesting to see if the gluing technique can be used in other attacks.

In light of this, we believe that security analyses of big-field multivariate schemes ought not only focus on the first fall degree directly, but also how this degree changes when fixing variables. Cryptographers wishing to design encryption schemes by adding limited modification to an otherwise weak polynomial system should be particularly aware of the effect presented in this work.

## Acknowledgements

Morten Øygarden has been funded by The Research Council of Norway through the project “qsIoT: Quantum safe cryptography for the Internet of Things”. The authors would like to thank Carlos Cid for useful discussions on this work. We are also grateful to the reviewers at the Journal of Cryptology for suggesting numerous improvements.

## References

1. D. Apon, D. Moody, R. Perlner, D. Smith-Tone, and J. Verbel. Combinatorial rank attacks against the rectangular simple matrix encryption scheme. In *International Conference on Post-Quantum Cryptography*, pages 307–322. Springer, 2020.
2. M. F. Atiyah and I. G. Macdonald. *Introduction to commutative algebra*. CRC Press, 2016.
3. M. Bardet, M. Bros, D. Cabarcas, P. Gaborit, R. Perlner, D. Smith-Tone, J.-P. Tillich, and J. Verbel. Improvements of Algebraic Attacks for solving the Rank Decoding and MinRank problems. In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 507–536. Springer, 2020.
4. M. Bardet, J.-C. Faugère, and B. Salvy. Complexity of Gröbner basis computation for Semi-regular Overdetermined sequences over  $\mathbb{F}_2$  with solutions in  $\mathbb{F}_2$ . 2003. [Research Report] RR-5049, INRIA, inria-00071534.
5. L. Bettale, J.-C. Faugère, and L. Perret. Hybrid approach for solving multivariate systems over finite fields. *Journal of Mathematical Cryptology*, 3(3):177–197, 2009.
6. L. Bettale, J.-C. Faugère, and L. Perret. Cryptanalysis of HFE, multi-HFE and variants for odd and even characteristic. *Designs, Codes and Cryptography*, 69(1):1–52, 2013.
7. A. Caminata and E. Gorla. Solving degree, last fall degree, and related invariants. *Journal of Symbolic Computation*, 114:322–335, 2023.
8. C. Carlet. Vectorial boolean functions for cryptography. In Y. Crama and P. L. Hammer, editors, *Boolean Models and Methods in Mathematics, Computer Science, and Engineering*, pages 398–469. Cambridge University Press, 2010.
9. R. Cartor and D. Smith-Tone. EFLASH: A New Multivariate Encryption Scheme. In C. Cid and M. Jacobson Jr., editors, *Selected Areas in Cryptography – SAC 2018*, volume 11349 of *Lecture Notes in Computer Science*, pages 281–299. Springer International Publishing, 2019.
10. R. Cartor and D. Smith-Tone. All in the  $C^*$  family. *Designs, Codes and Cryptography*, 88(6):1023–1036, 2020.
11. C.-M. Cheng, T. Chou, R. Niederhagen, and B.-Y. Yang. Solving quadratic equations with XL on parallel architectures. In *International Workshop on Cryptographic Hardware and Embedded Systems*, pages 356–373. Springer, 2012.
12. D. A. Cox, J. Little, and D. O’Shea. *Using algebraic geometry*, volume 185. Springer Science & Business Media, 2006.
13. A. Diene, J. Ding, J. E. Gower, T. J. Hodges, and Z. Yin. Dimension of the linearization equations of the matsumoto-imai cryptosystems. In Ø. Ytrehus, editor, *Coding and Cryptography*, pages 242–251, Berlin, Heidelberg, 2006. Springer Berlin Heidelberg.
14. J. Ding. A new variant of the Matsumoto-Imai cryptosystem through perturbation. In *International Workshop on Public Key Cryptography*, pages 305–318. Springer, 2004.
15. J. Ding and J. E. Gower. Inoculating multivariate schemes against differential attacks. In *International Workshop on Public Key Cryptography*, pages 290–301. Springer, 2006.
16. J. Ding and T. J. Hodges. Inverting HFE systems is quasi-polynomial for all fields. In *Annual Cryptology Conference*, pages 724–742. Springer, 2011.
17. J. Ding, R. Perlner, A. Petzoldt, and D. Smith-Tone. Improved cryptanalysis of HFEv- via projection. In *International Conference on Post-Quantum Cryptography*, pages 375–395. Springer, 2018.

18. J. Ding and D. Schmidt. Cryptanalysis of HFEv and internal perturbation of HFE. In *International Workshop on Public Key Cryptography*, pages 288–301. Springer, 2005.
19. H. Dobbertin. Almost perfect nonlinear power functions on  $\text{GF}(2^n)$ : the Welch case. *IEEE Transactions on Information Theory*, 45(4):1271–1275, 1999.
20. V. Dubois, L. Granboulan, and J. Stern. Cryptanalysis of HFE with internal perturbation. In *International Workshop on Public Key Cryptography*, pages 249–265. Springer, 2007.
21. J.-C. Faugère. A new efficient algorithm for computing Gröbner bases (F4). *Journal of pure and applied algebra*, 139(1-3):61–88, 1999.
22. J.-C. Faugère and A. Joux. Algebraic cryptanalysis of hidden field equation (HFE) cryptosystems using Gröbner bases. In *Annual International Cryptology Conference*, pages 44–60. Springer, 2003.
23. J.-C. Faugère, F. Levy-dit Vehel, and L. Perret. Cryptanalysis of MinRank. In *Annual International Cryptology Conference*, pages 280–296. Springer, 2008.
24. P.-A. Fouque, L. Granboulan, and J. Stern. Differential cryptanalysis for multivariate schemes. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 341–353. Springer, 2005.
25. J. W. Hoffman, X. Jia, and H. Wang. *Commutative Algebra: An Introduction*. Stylus Publishing, LLC, 2016.
26. <https://github.com/Simula-UiB/Attack-On-The-Dob-Encryption-Scheme>.
27. G. Macario-Rat and J. Patarin. Two-face: New public key multivariate schemes. In *International Conference on Cryptology in Africa*, pages 252–265. Springer, 2018.
28. T. Matsumoto and H. Imai. Public quadratic polynomial-tuples for efficient signature-verification and message-encryption. In D. Barstow, W. Brauer, P. Brinch Hansen, D. Gries, D. Luckham, C. Moler, A. Pnueli, G. Seegmüller, J. Stoer, N. Wirth, and C. G. Günther, editors, *Advances in Cryptology — EUROCRYPT '88*, pages 419–453, Berlin, Heidelberg, 1988. Springer Berlin Heidelberg.
29. National Institute for Standards and Technology. Post-Quantum Cryptography Standardization, 2017. <https://csrc.nist.gov/Projects/post-quantum-cryptography/post-quantum-cryptography-standardization>.
30. J. Patarin. Cryptanalysis of the Matsumoto and Imai public key scheme of Eurocrypt'88. In *Annual International Cryptology Conference*, pages 248–261. Springer, 1995.
31. J. Patarin. Hidden fields equations (HFE) and isomorphisms of polynomials (IP): Two new families of asymmetric algorithms. In *International Conference on the Theory and Applications of Cryptographic Techniques*, pages 33–48. Springer, 1996.
32. P. W. Shor. Algorithms for quantum computation: discrete logarithms and factoring. In *Proceedings 35th annual symposium on foundations of computer science*, pages 124–134. Ieee, 1994.
33. D. Smith-Tone and J. Verbel. A rank attack against extension field cancellation. In *International Conference on Post-Quantum Cryptography*, pages 381–401. Springer, 2020.
34. A. Szepieniec, J. Ding, and B. Preneel. Extension field cancellation: A new central trapdoor for multivariate quadratic systems. In *Post-Quantum Cryptography*, pages 182–196. Springer, 2016.
35. C. Tao, A. Petzoldt, and J. Ding. Efficient Key Recovery for All HFE Signature Variants. In *Annual International Cryptology Conference*, pages 70–93. Springer, 2021.

36. C. Tao, H. Xiang, A. Petzoldt, and J. Ding. Simple matrix–a multivariate public key cryptosystem (MPKC) for encryption. *Finite Fields and Their Applications*, 35:352–368, 2015.
37. Y. Wang, Y. Ikematsu, D. H. Duong, and T. Takagi. The secure parameters and efficient decryption algorithm for multivariate public key cryptosystem EFC. *IE-ICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, 102(9):1028–1036, 2019.
38. D. Wiedemann. Solving sparse linear equations over finite fields. *IEEE transactions on information theory*, 32(1):54–62, 1986.
39. C. Wolf and B. Preneel. Taxonomy of public key schemes based on the problem of multivariate quadratic equations. Cryptology ePrint Archive, Report 2005/077, 2005. <https://eprint.iacr.org/2005/077>.
40. C. Wolf and B. Preneel. Equivalent keys in Multivariate Quadratic public key systems. *Journal of Mathematical Cryptology*, 4(4):375–415, 2011.
41. T. Yasuda, Y. Wang, and T. Takagi. Multivariate encryption schemes based on polynomial equations over real numbers. In *International Conference on Post-Quantum Cryptography*, pages 402–421. Springer, 2020.
42. M. Øygarden. *Algebraic Cryptanalysis of Cryptographic Schemes with Extension Field Structure*. PhD thesis, University of Bergen, 2021. <https://hdl.handle.net/11250/2771891>.
43. M. Øygarden, P. Felke, and H. Raddum. Analysis of multivariate encryption schemes: Application to dob. Cryptology ePrint Archive, Report 2020/1442, 2020. <https://ia.cr/2020/1442>.
44. M. Øygarden, P. Felke, and H. Raddum. Analysis of Multivariate Encryption Schemes: Application to Dob. In *IACR International Conference on Public-Key Cryptography*, pages 155–183. Springer, 2021.
45. M. Øygarden, P. Felke, H. Raddum, and C. Cid. Cryptanalysis of the multivariate encryption scheme EFLASH. In *Cryptographers’ Track at the RSA Conference*, pages 85–105. Springer, 2020.

## A Formulas for Dob Degree Fall Polynomials at $\nu = 5$

$\mathbf{N}_5^{(1,1)}$ : Let us start by examining  $(S^{M^{(1,1)}}(\mathcal{F}^h))_5$ . The polynomials involving the quadratic polynomials from  $Q_+$ , namely the  $q_i^h$ , are easy to classify as they would only appear as products with the  $2d$  degree fall polynomials at  $\nu = 3$  (from Section 3.3). The elements containing the  $ip$  linear forms are slightly more involved. At first glance, the  $\nu = 3$  syzygies will generate  $2d \cdot \dim_2(V^1)$ , but we also need to take into consideration the cancellations appearing at  $\nu = 4$  (which sums up to the  $-d$  term in Eq. (3.3)). Assuming that none of these cancellations can be factorized by a linear form in  $\text{Span}(v_1, \dots, v_k)$  (which is highly likely when  $n \gg k$ ), we will need to subtract  $kd$  to account for these cancellations.

Turning our attention to the modifiers, we can combine (v) and (ii) from Lemma 3, to get

$$\dim_5(M^{(2,1)}M^{(1,1)}) = \dim_5(M^{(3,2)}) + \dim_5(V^1Q^1) - \dim_5(M^{(3,2)} \cap V^1Q^1).$$



Expecting that  $(Q^2 \cap V^3)_5$  is empty, and using Lemma 3 (iv), we can further rewrite this as

$$\begin{aligned} \dim_5(M^{(2,1)}M^{(1,1)}) &= \dim_5(Q^2) + \dim_5(V^3) + \dim_5(V^1Q^1) \\ &\quad - \dim_5(Q^2 \cap V^1Q^1) - \dim_5(V^3 \cap V^1Q^1). \end{aligned}$$

Example 1 1 covers  $\dim_5(V^1Q^1)$ , and we will deal with the intersections through ad hoc arguments. We expect  $\langle Q^2 \cap V^1Q^1 \rangle_5$  to be generated by the possible combinations  $q_iq_jv_l$ , so we estimate its dimension to be  $k\binom{t}{2}$ . Similarly,  $\langle V^3 \cap V^1Q^1 \rangle_5$  is expected to be generated by the combinations  $v_iv_jv_rq_l$ , and its dimension is expected to be  $t\binom{k}{3}$ .

Lastly, we examine  $M^{(1,1)}M^{(2,1)}\langle \mathcal{P}^h \rangle$ . At degree 5 the only possible combinations are  $v_iv_jv_rq_l$ , and  $v_iq_jp_l$ . All this information sums up to the following:

$$\begin{aligned} (N_5^{(1,1)})' &= d \overbrace{\left( 2k(n-k) + 2\binom{k}{2} + 2t - k \right)}^{\dim_5(\mathcal{S}^{M^{(1,1)}}(\mathcal{F}^h))} - \overbrace{\binom{t}{2}n}^{\dim_5(Q^2)} \\ &\quad - \overbrace{\left( \binom{k}{3}\binom{n-k}{2} + \binom{k}{4}(n-k) + \binom{k}{5} \right)}^{\dim_5(V^3)} \\ &\quad - t \overbrace{\left( k\binom{n-k}{2} + \binom{k}{2}(n-k) + \binom{k}{3} \right)}^{\dim_5(Q^1V^1)} + k \left( t^2 - \binom{t}{2} \right) \tag{A.1} \\ &\quad + \overbrace{\binom{t}{2}k}^{\dim_5(Q^2 \cap V^1Q^1)} + \overbrace{\binom{k}{3}t}^{\dim_5(V^3 \cap V^1Q^1)} \\ &\quad + \overbrace{d \left( kt + \binom{k}{3} \right)}^{\dim_5(M^{(1,1)}M^{(2,1)}\langle \mathcal{P}^h \rangle)}. \end{aligned}$$

*Remark 3.* We have run tests for  $\dim_5(\mathcal{S}^{M^{(1,1)}}(\mathcal{F}^h))$ ,  $\dim_5(M^{(1,1)}M^{(2,1)})$  and  $\dim_5(M^{(1,1)}M^{(2,1)}\langle \mathcal{P}^h \rangle)$ , and separately they agree with what we have counted above. However, when running tests for  $(N_5^{(1,1)})'$  as a whole, we find that the theoretical formula presented in Eq. (A.1) consistently undershoots the number of degree fall polynomials by  $4d$ . Hence there is some interplay between the separate parts making up the formula that we do not yet understand. For this reason, we adjust Eq. (5.10) in the main part of the text by this value, i.e.,  $N_5^{(1,1)} = (N_5^{(1,1)})' + 4d$ .

$\mathbf{N}_5^{(2,1)}$ : The degree five part of  $\mathcal{S}^{M^{(2,1)}}(\mathcal{F}^h)$  is given by Equation (5.2). An application of Lemma 3 (iv) and (v) leads to

$$\dim_5(M^{(2,1)}M^{(2,1)}) = \dim_5(V^4) + \dim_5(Q^2) + \dim_5(V^2Q^1).$$

Example 1 (b) is used to compute  $\dim_5(V^2Q^1)$ , and we furthermore expect no polynomials of degree five in  $M^{(2,1)}M^{(2,1)}\langle\mathcal{P}^h\rangle$ . All this sums up to the following estimate:

$$\begin{aligned} (N_5^{(2,1)})' &= \overbrace{2d\left(\binom{k}{2} + t\right)}^{\dim_5(S^{M^{(2,1)}}(\mathcal{F}^h))} - \overbrace{\left(\binom{k}{4}(n-k) + \binom{k}{5}\right)}^{\dim_5(V^4)} \\ &\quad - \overbrace{t\left(\binom{k}{2}(n-k) + \binom{k}{3}\right)}^{\dim_5(Q^1V^2)} - \overbrace{\binom{t}{2}n}^{\dim_5(Q^2)}. \end{aligned} \tag{A.2}$$

Similarly to what was discussed in Remark 3, we also find that the theoretically predicted  $(N_5^{(2,1)})'$  is off by  $4d$  in experiments. Hence, we adjust for this in Eq. (5.11) by setting  $N_5^{(2,1)} = (N_5^{(2,1)})' + 4d$ .

## B Proof of Lemma 7

By a slight abuse of notation we will consider  $\widetilde{W}_\eta$  to include integers, by listing the index of the variables it contains. Recall the  $(r, d)$  covering problem, which can be stated as follows: for given  $d$  and  $r < d-1$ , find  $\rho$  subsets  $\widetilde{W}_\eta \subset \{1, \dots, d\}$  of size  $d-r$ , such that for any pair  $(i, j)$  where  $1 \leq i < j \leq d$ ,  $\{i, j\} \subset \widetilde{W}_\eta$  for at least one  $\eta$ .

*Proof (of Lemma 7).* Let  $s = \lfloor (d-r)/2 \rfloor$ . We divide  $\{1, \dots, d\}$  into blocks of size  $s$ :

$$C_b = \{(b-1)s + 1, \dots, bs\}, \text{ for } 1 \leq b \leq \lfloor d/s \rfloor$$

Let the sets  $\widetilde{W}_\eta$  for  $1 \leq \eta \leq \binom{\lfloor d/s \rfloor}{2}$  be defined as the union of  $C_a$  and  $C_b$ , for all choices of  $1 \leq a < b \leq \lfloor d/s \rfloor$ . In the case  $d-r$  is odd, we also add one arbitrary extra number to each set to make sure that each  $\widetilde{W}_\eta$  contains exactly  $d-r$  numbers.

Any  $\{i, j\} \subset \{1, \dots, s\lfloor d/s \rfloor\}$  will then be contained in at least one  $\widetilde{W}_\eta$ . If both  $i$  and  $j$  belong to the same block  $C_b$ , then all  $\widetilde{W}_\eta$  involving  $C_b$  will contain  $\{i, j\}$ . If  $i \in C_a$  and  $j \in C_b$  for  $a \neq b$ , then the set  $\widetilde{W}_\eta = C_a \cup C_b$  will contain  $\{i, j\}$ . Hence the  $\binom{\lfloor d/s \rfloor}{2}$  sets constructed will cover all pairs from  $\{1, \dots, s\lfloor d/s \rfloor\}$ .

If  $s$  divides  $d$  we are done. Otherwise, to cover all pairs of numbers in  $\{1, \dots, d\}$  it is sufficient to create  $\lfloor d/s \rfloor$  new  $\widetilde{W}$ -sets consisting of  $\{s\lfloor d/s \rfloor + 1, \dots, d\} \cup C_b \cup \{s - (d - s\lfloor d/s \rfloor) \text{ extra numbers}\}$ , where  $1 \leq b \leq \lfloor d/s \rfloor$ , and the extra numbers are arbitrary. The total number of sets will then be  $\binom{\lfloor d/s \rfloor}{2}$ , and replacing  $s$  with  $\lfloor (d-r)/2 \rfloor$  we get Lemma 7.

For the particular case  $d = 129, r = 79$  (which is used in Section 7.8) we get  $\rho \leq 15$ . Doing the exercise in practice we find that  $\rho = 11$  is sufficient to solve the problem by extending the block  $C_5$  to cover all numbers  $101, \dots, 129$ , and modifying slightly the sets involving  $C_5$ .