Not Easy to Prepare a Pesto: Cryptanalysis of a Multivariate Public-Key Scheme from CCZ Equivalence

Christof Beierle[1] and Patrick Felke[2]

[1] Faculty of Computer Science, Ruhr University Bochum, Bochum, Germany
christof.beierle@rub.de
[2] University of Applied Sciences Emden/Leer, Emden, Germany
patrick.felke@hs-emden-leer.de

Abstract. Multivariate cryptography is one of the challenging candidates for post-quantum cryptography. There exists a huge variety of proposals, most of them have been broken substantially. Multivariate schemes are usually constructed by applying two secret affine invertible transformations $\mathcal{S}, \mathcal{T}$ to a set of multivariate polynomials $\mathcal{F}$ (often quadratic). The secret polynomials $\mathcal{F}$ possess a trapdoor that allows the legitimate user to find a solution of the corresponding system, while the public polynomials $\mathcal{G} = \mathcal{S} \circ \mathcal{F} \circ \mathcal{T}$ look like random polynomials. In [Calderini, M., Caminata, A., Villa, I. A New Multivariate Primitive from CCZ Equivalence. J. Cryptol. 38, 25 (2025)], the authors presented a promising new way of constructing a multivariate scheme by considering the CCZ equivalence, which has been introduced and studied in the context of vectorial Boolean functions. The resulting proposal is called `Pesto`.
We present an attack against `Pesto` by constructing an equivalent secret key from the public key. We provide a reference implementation of our attack, which allows to break all the instances of the `Pesto` signature scheme proposed by the designers in practical time.

Keywords: Multivariate Cryptography · Oil-and-Vinegar Polynomials · CCZ Equivalence · `Pesto`

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 [29], Shor showed 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 available 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 on mathematical problems believed to be hard even for quantum computers, so-called *post-quantum cryptography*. In 2016, the National Institute of Standards and Technology (NIST) launched a project aimed at standardizing post-quantum public-key primitives [22]. A call for proposals was made, many candidate schemes were proposed, some winners identified and finally standardized. 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 multivariate schemes based on the MQ problem is to construct them around an easy to invert central mapping

$$\mathcal{F} = (f_1(x_1, \ldots, x_n), \ldots, f_m(x_1, \ldots, x_n)),$$

where $f_i(x_1, \ldots, x_n)$ denote multivariate quadratic polynomials in $\mathbb{F}_q[x_1, \ldots, x_n]$ and $\mathbb{F}_q$ a finite field of q elements. The mapping $\mathcal{F}$ is masked with secret and randomly chosen affine bijective mappings $\mathcal{S} : \mathbb{F}_q^m \to \mathbb{F}_q^m$ and $\mathcal{T} : \mathbb{F}_q^n \to \mathbb{F}_q^n$. The public key is $\mathcal{G} = \mathcal{S} \circ \mathcal{F} \circ \mathcal{T}$ and assumed to be hard to invert and thus in particular assumed to be a hard instance of the MQ problem. The first encryption scheme based on the MQ problem, named C^*, was proposed in [20] and was broken by Patarin in [26]. Since then, several multivariate encryption and signature schemes have been proposed, for instance [8,18,14,9,30]. The papers [11,24,2,23,21] all present attacks on MQ-based schemes, and as of now we are only aware of a few (e.g. [31,3]) that remain unbroken. Hence, designing secure multivariate cryptosystems is intriguing and of high interest.

In [5] this problem is addressed and a new kind of central mapping is deployed, which can be used to construct both encryption and signature schemes. The novel feature of the central mapping is that it is based on CCZ equivalence, which has been studied in the context of vectorial Boolean functions [7]. This central mapping is of degree 4 and not 2, where the latter is the standard case for multivariate cryptography. Their concrete construction is called `Pesto`.

Recently, it was shown in [6] that the multivariate system of degree 4 in `Pesto` can be reduced to a quadratic system, where the reduction has complexity of $\mathcal{O}(mn^6)$ if $m \leq n$. This analysis suggested that the degree-4 system obtained via the CCZ equivalence is not more secure than a quadratic multivariate scheme. Although the authors of [6] acknowledged that the quadratic system obtained after the reduction *"can be solved by using general quadratic solving methods or any OV solving methods, if it has the structure of an Oil and Vinegar (OV) scheme"*, they did not outline an actual attack on the system. However, it seems reasonable that the remaining system is efficiently solvable.

In this work, we are tackling the decomposition problem to recover an equivalent secret key that allows to decrypt or sign any message with the same complexity as for the owner of the corresponding legitimate key. The decomposition problem aims to find $\mathcal{S}', \mathcal{F}', \mathcal{T}'$ such that $\mathcal{G} = \mathcal{S}' \circ \mathcal{F}' \circ \mathcal{T}'$ and the complexity to invert $\mathcal{F}'$ is of the same magnitude as inverting $\mathcal{F}$. Since $\mathcal{F}' = \mathcal{S}'^{-1} \circ \mathcal{S} \circ \mathcal{F} \circ \mathcal{T} \circ \mathcal{T}'^{-1}$, the keys $(\mathcal{S}, \mathcal{T}, \mathcal{F})$ and $(\mathcal{S}', \mathcal{T}', \mathcal{F}')$ are called *equivalent*.

Our Contribution

We present an attack against `Pesto` with security parameters n, m, s, t, q by constructing an equivalent secret key, with a complexity of

$$\max\left\{\mathcal{O}\left(n^6(m-t)\right), \mathcal{O}\left(\frac{(m-t)(n-t)^2(n-t-s)q^s}{\mathcal{P}(q, n-t-s)}\right)\right\}$$

base field operations on average, where $\mathcal{P}(q,k) \coloneqq \prod_{i=1}^{k}(1-1/q^i)$, and an online complexity of

$$\mathcal{O}(q^s(m-t)(n-t-s)\cdot\min(m-t, n-t-s) + q^s t(n-t)^2 + q^s t^3)$$

base field operations. Thereby $t \leq \min(n, m)$ and $1 \leq s \leq n-t$. The definition of `Pesto` is recalled in Section 3. The concrete parameter proposals by the designers for the signature scheme are given in Table 1. In opposite to the attack given in [6], which only gives a reduction to an OV scheme, we present the first complete attack, together with a proof-of-concept implementation, against all proposed parameters.

Our attack makes use of the theory of quadratic forms, outlined in the next section, tailored to the new central mapping used in `Pesto`. This theory has already been used in other attacks against (UOV) multivariate cryptosystems (see e.g. [28],[1] for examples). Moreover, we make use of the standard algebraic approach of decomposing the composition $h \circ g$ of polynomial mappings if g is known, by solving linear equations gained by comparison of coefficients with the composition. The whole approach gives a new way of computing an equivalent key for multivariate cryptosystems based on CCZ equivalence. Being able to compute an equivalent key is considered a full break of the cryptosystem.

Table 1. `Pesto` parameters for the signature scheme proposed by the designers [5]. NIST I – V refers to the security levels for post-quantum signature schemes defined by NIST within the Post-Quantum Cryptography Project. The column "security" gives the equivalent security level for exhaustive key search on a block cipher.

	security	q	n	m	t	s	public key size	secret key size
NIST I	128 bit	2^6	27	25	10	2	357 MB	5.5 MB
NIST III	192 bit	2^6	40	38	14	2	2,453 MB	16.5 MB
NIST V	256 bit	2^6	57	55	20	2	13,725 MB	43.8 MB

In all the proposed instances, s is equal to 2, so the exponential factor of q^s in the formulas for the attack complexity is not problematic.

Further, note that we have the approximation

$$\mathcal{P}(q,k) \approx \exp\left(\frac{1}{1-q}\right)$$

by writing $\ln(\mathcal{P}(q,k)) = \sum_{i=1}^{k} \ln(1-1/q^i) \approx \sum_{i=1}^{k} -(1/q)^i$ and using the limit of the geometric series as well as the approximation $\ln(1-\left(\frac{1}{q}\right)^i) \approx -\left(\frac{1}{q}\right)^i$ since $\left(\frac{1}{q}\right)^i$ is small enough (see [12, pp. 99–100]). Hence, the term $\mathcal{P}(q, n-t-s)$ is close to 1 for the instances of `Pesto` we are investigating. For example, for the parameter set corresponding to the NIST I instance, we get $\mathcal{P}(q,15) \approx 0.9841$ and $\exp(1/(1-q)) \approx 0.98425$.

We practically verified and executed the attack on the parameter sets proposed by the designers using a reference implementation in Magma [4] (version V2.29-6). The execution times are given in Table 2. The code is available at `https://doi.org/10.5281/zenodo.21642070`.

Table 2. The execution times of our attack using a machine with 40 x Intel(R) Xeon(R) Silver 4114 CPU @ 2.20GHz (2 sockets) and 300 GB RAM, 20 threads.

	compressed version (w.o. Step 1)	full version (with Step 1)	decrypting
NIST I	$\approx$ 3 min	$\approx$ 3.5 min	$<$ 1 min
NIST III	$\approx$ 35 min	$\approx$ 40 min	$\approx$ 2 min
NIST V	$\approx$ 8 hrs	$\approx$ 11 hrs	$\approx$ 30 min

Organization

In Section 2 we introduce the notation used, recall some facts from the theory of quadratic forms and develop the theory for our attack. In Section 3 we give a description of `Pesto`. We outline our attack in Section 4.

2 Preliminaries

We assume that the reader is familiar with basic facts on finite fields. For more details, [17] is a suitable reference. Throughout this work, let n and m be positive integers. The finite field with q elements, q a prime power is denoted by $\mathbb{F}_q$. With $\mathbb{F}_q^n$ we denote the vector space of dimension n over $\mathbb{F}_q$ and with $|\cdot|$ the cardinality of a set. If not stated otherwise an element of $\mathbb{F}_q^n$ is a column vector. The canonical unit basis of $\mathbb{F}_q^n$ is denoted with

$$e_1 = (1,0,\ldots,0)^T, \ldots, e_n = (0,\ldots,0,1)^T,$$

for T denoting the transpose. The subspace generated by elements $v_1,\ldots,v_l \in \mathbb{F}_q^n$ is denoted by $< v_1,\ldots,v_l >$. Note that these vectors do not need to be linearly independent. The multivariate polynomial ring in n unknowns over $\mathbb{F}_q$ is denoted by $\mathbb{F}_q[x_1,\ldots,x_n]$. By $M(n\times m, \mathbb{F}_q)$, we denote the set of $n\times m$ matrices and by Id the identity matrix in case of $n=m$.

The following well known lemma states the probability that m uniformly chosen vectors in $\mathbb{F}_q^n$ are linearly independent. For the proof, see, e.g., [13, Thm. 7.1.5] for the number of $n \times m$ matrices with entries in $\mathbb{F}_q$ of fixed rank k. The probability is obtained by dividing by q^{mn}, i.e., the the size of $M(n \times m, \mathbb{F}_q)$.

Lemma 1. *For $m \leq n$, the probability that a uniformly chosen matrix in $M(n \times m, \mathbb{F}_q)$ has full rank is*

$$\prod_{i=0}^{m-1} (1 - q^{-(n-i)}).$$

For two sets X, Y, the relation $X \subset Y$ also includes equality. With $a \ll b$ for $a, b \in \mathbb{R}$ we denote that a is much smaller than b, where it will be always clear from that context what being "much smaller" means.

Let F be a function $F\colon \mathbb{F}_q^n \to \mathbb{F}_q^m$. Notice that F can be represented as $F = (f_1, \ldots, f_m)$ with $f_i\colon \mathbb{F}_q^n \to \mathbb{F}_q, 1 \leq i \leq m$. We call f_i the *i-th coordinate* of F and denote it also by F_i. To represent F we can extend the so-called algebraic normal form (ANF) as follows: Any function $f\colon \mathbb{F}_q^n \to \mathbb{F}_q$ has a unique representation of the form

$$f(x) = \sum_{u \in \mathbb{N}^n} a_u x_1^{u_1} \cdots x_n^{u_n} \bmod (x_1^q - x_1, \ldots, x_n^q - x_n)$$

with $a_u \in \mathbb{F}_q$. The unique polynomial representation of f with all $u_1, \ldots, u_n$ less than q is called the *algebraic normal form (ANF)*. This can be extended to an ANF for $F\colon \mathbb{F}_q^n \to \mathbb{F}_q^m$ by setting $F(x) = \sum_{u \in \mathbb{N}^n} a_u x_1^{u_1} \cdots x_n^{u_n}$ with $a_u \in \mathbb{F}_q^m$ and all $u_1, \ldots, u_n$ less than q. The monomial $x_1^{u_1} \cdots x_n^{u_n}$ belongs to a *term* of F if and only if $a_u \neq 0$. If F is non-zero, the *degree* of F is defined as

$$\deg(F) = \max\{\sum_{i=1}^{n} u_i \mid u \in \{0, \ldots, q-1\}^n, a_u \neq 0\}.$$

If $F = 0$, we define $\deg(F) = -\infty$. We call F *affine* if $\deg(F) \leq 1$, *linear* if additionally $F(0) = 0$, and *quadratic* if $\deg(F) = 2$. If all terms have the same degree then F is called *homogeneous*. If a function S is linear or affine it can be written as $S(x) = Ax$ or $S(x) = Ax + d$ respectively, where $A \in M(n \times m, \mathbb{F}_q)$ and $d \in \mathbb{F}_q^m$.

To keep the article self contained, we will now give some well-known results about quadratic forms necessary for our attacks. For readers who are interested in gaining more knowledge about the theory of quadratic forms we refer to [16] and [17].

Definition 2.1 *A function $\mathfrak{q}\colon \mathbb{F}_q^n \to \mathbb{F}_q$ is called a* quadratic form *if*

1. *$\mathfrak{q}(ax) = a^2\mathfrak{q}(x)$ holds for any scalar $a \in \mathbb{F}_q$, and*
2. *the function*

$$\begin{aligned} \mathfrak{B}_\mathfrak{q}\colon \mathbb{F}_q^n \times \mathbb{F}_q^n &\to \mathbb{F}_q \\ (x, y) &\mapsto \mathfrak{q}(x + y) - \mathfrak{q}(x) - \mathfrak{q}(y) \end{aligned}$$

is a symmetric bilinear form.

Remark 2.1 *The ANF of a quadratic form* $\mathfrak{q} \neq 0$ *is a homogeneous quadratic polynomial. In case of* $\mathbb{F}_q = \mathbb{F}_2$ *we have, by abuse of notation, to set* $x_i = x_i^2$ *in* $\mathfrak{q}$ *for the above statement to become true.*

Definition 2.2 *Given a quadratic form* $\mathfrak{q}\colon \mathbb{F}_q^n \to \mathbb{F}_q$.

1. *Two vectors* $x, y \in \mathbb{F}_q^n$ *are called* orthogonal *if* $\mathfrak{B}_\mathfrak{q}(x, y) = 0$.
2. *For* $X \subset \mathbb{F}_q^n$, *we set* $X^\perp \coloneqq \{y \in \mathbb{F}_q^n \mid \mathfrak{B}_\mathfrak{q}(x, y) = 0 \text{ for all } x \in X\}$ *and* $X^\perp$ *is called the* orthogonal complement *of* X *in* $\mathbb{F}_q^n$.
3. *If* q *is even we always have* $\mathfrak{B}_\mathfrak{q}(x, x) = 0$. *Such a form is called* skew-symmetric.
4. *The* radical *of* $\mathfrak{B}_\mathfrak{q}$ *is defined as* $\mathrm{rad}(\mathfrak{B}_\mathfrak{q}) \coloneqq \mathbb{F}_q^{n\perp}$.
5. *The* rank *of* $\mathfrak{B}_\mathfrak{q}$ *is defined as* $\mathrm{rank}(\mathfrak{B}_\mathfrak{q}) \coloneqq n - \dim(\mathrm{rad}(\mathfrak{B}_\mathfrak{q}))$. *The* rank *of* $\mathfrak{q}$ *is defined as* $\mathrm{rank}(\mathfrak{q}) \coloneqq \mathrm{rank}(\mathfrak{B}_\mathfrak{q})$
6. $\mathfrak{q}$ *is called* isotropic *if there exists a non-zero vector* $v \in \mathbb{F}_q^n$ *with* $\mathfrak{q}(v) = 0$. *Such* v *is called an* isotropic vector.

Remark 2.2 *We have* $\mathfrak{q}(x + y) = \mathfrak{q}(x) + \mathfrak{q}(y)$ *for all* $x \in \mathbb{F}_q^n$ *and* $y \in \mathrm{rad}(\mathfrak{B}_\mathfrak{q})$. *In particular,* $\mathfrak{q}$ *is a linear form when restricted to* $\mathrm{rad}(\mathfrak{B}_\mathfrak{q})$. *The radical will play a crucial role in our attack.*

Two quadratic forms $\mathfrak{q}, \mathfrak{q}'$ over $\mathbb{F}_q^n$ are called *isometric* if there exists a bijective linear mapping L with $\mathfrak{q}(x) = \mathfrak{q}'(L(x))$. In the same vein isometry between symmetric bilinear forms is defined. Isometry yields an equivalence relation for quadratic forms and its associated bilinear forms. We have the following obvious lemma.

Lemma 2.3 *Given two isometric quadratic forms* $\mathfrak{q}$ *and* $\mathfrak{q}'$ *with* $\mathfrak{q} = \mathfrak{q}'(L(x))$, *we have* $\mathrm{rad}(\mathfrak{B}_{\mathfrak{q}'}) = L(\mathrm{rad}(\mathfrak{B}_\mathfrak{q}))$.

The following corollary will be crucial for our attack.

Corollary 2.4 *Let* $\mathfrak{q}'_1, \ldots, \mathfrak{q}'_l$ *be quadratic forms over* $\mathbb{F}_q^n$, *where each form has at most* r *indeterminates* $x_1, \ldots, x_r$. *For a bijective linear mapping* L, *consider the isometric forms*

$$\mathfrak{q}_1(x) = \mathfrak{q}'_1(L(x)), \ldots, \mathfrak{q}_l(x) = \mathfrak{q}'_l(L(x)).$$

Let $\alpha_1, \ldots, \alpha_l \in \mathbb{F}_q$. *Then,*

1. $\mathrm{rad}(\mathfrak{B}_{\mathfrak{q}_i}) \supset L^{-1}(< e_{r+1}, \ldots, e_n >)$ *for* $i = 1, \ldots, l$.
2. $\cap_{i=1}^{l} \mathrm{rad}(\mathfrak{B}_{\mathfrak{q}_i}) \subset \mathrm{rad}(\mathfrak{B}_{\alpha_1\mathfrak{q}_1 + \cdots + \alpha_l\mathfrak{q}_l})$.
3. $L^{-1}(< e_{r+1}, \ldots, e_n >) \subset \mathrm{rad}(\mathfrak{B}_{\alpha_1\mathfrak{q}_1 + \cdots + \alpha_l\mathfrak{q}_l})$.
4. $\mathrm{rank}(\mathfrak{B}_{\alpha_1\mathfrak{q}_1 + \cdots + \alpha_l\mathfrak{q}_l}) \leq r$.

Proof. The first statement is a direct consequence of Lemma 2.3 and the second statement follows from the definition of the radical. The last two statements follow easily from the first two. □

If q is odd, then for any quadratic form $\mathfrak{q}$ there exists a unique symmetric matrix $A \in M(n \times n, \mathbb{F}_q)$ such that $\mathfrak{q}(x) = x^\top Ax$. More precisely, for $\mathfrak{q}(x) = \sum_{i,j} \alpha_{ij} x_i x_j$, the entries a_{ij} of A are defined by $a_{ij} = a_{ji} = \frac{\alpha_{ij}+\alpha_{ji}}{2}, i \neq j$, and $a_{ii} = \alpha_{ii}$. We have $\mathfrak{B}_\mathfrak{q}(x, y) = 2 \cdot x^T Ay$ and thus $\operatorname{rank}(\mathfrak{B}_\mathfrak{q}) = \operatorname{rank}(A)$.

For q even, the situation is different because any symmetric matrix A yields $x^T Ax = \sum_i a_{i,i} x_i^2$. Hence, it is not possible to represent $\mathfrak{q}(x) = \sum_{i,j} \alpha_{ij} x_i x_j$ as $x^T Ax$ for a symmetric representative matrix A in general. Still, $\mathfrak{B}_\mathfrak{q}(x, y)$ allows such a representation similarly to the case of odd q. More precisely, there exists a unique matrix C defined by $C = A + A^\top$ for any A that represents $\mathfrak{q}$. For instance, A could be chosen to be an upper triangular matrix U starting with $\alpha_{1,1}, \alpha_{1,2}, \ldots$ in the first row, $0, \alpha_{2,2}, \ldots$ in the second row and so forth, but also as the lower triangular matrix $A = U^T$. Importantly, such C does not depend on the choice of the representing matrix A. We then have $\mathfrak{B}_\mathfrak{q}(x, y) = x^T Cy$ so that $\operatorname{rank}(\mathfrak{B}_\mathfrak{q}) = \operatorname{rank}(C)$.

We get the following as a consequence.

Theorem 2.5 *Let $\mathfrak{q}$ be a quadratic form over $\mathbb{F}_q^n$ chosen uniformly at random. The probability that $\mathfrak{q}$ has rank n is bounded from below by*

$$\mathcal{P}(q, n) = \prod_{i=1}^{n} (1 - 1/q^i),$$

unless q is even and n is odd.

If q is even and n is odd, $\operatorname{rank}(\mathfrak{q})$ is always even and the probability that $\mathfrak{q}$ has rank $n-1$ is at least $\prod_{i=2}^{n}(1 - 1/q^i)$.

Proof. For a quadratic form $\mathfrak{q}$ over $\mathbb{F}_q^n$ chosen uniformly at random, $\operatorname{rank}(\mathfrak{B}_\mathfrak{q})$ is distributed as the rank of a uniformly at random chosen symmetric matrix in $M(n \times n, \mathbb{F}_q)$, with zero diagonal in case of q even. The number of such matrices is known [19, Thm. 2 and Thm. 3]. More precisely, let $0 \leq k \leq n$ and denote the number of symmetric matrices in $M(n \times n, \mathbb{F}_q)$ of rank k by $N(n, k)$. We have

$$N(n, k) = \prod_{i=1}^{\lfloor \frac{k}{2} \rfloor} \frac{q^{2i}}{q^{2i} - 1} \cdot \prod_{i=0}^{k-1} (q^{n-i} - 1).$$

For q even, let $N_0(n, k)$ denote the number of symmetric matrices in $M(n \times n, \mathbb{F}_q)$ with zero diagonal. Then,

$$N_0(n, 2s) = q^{-2s} N(n, 2s), \quad N_0(n, 2s+1) = 0.$$

In particular, if q is even, the rank of a quadratic form is always even.

The total number of symmetric matrices in $M(n \times n, \mathbb{F}_q)$, and of those with zero diagonal, is given by

$$T(n) = q^{\frac{n^2+n}{2}} = \prod_{i=0}^{n-1} q^{n-i} \quad \text{and} \quad T_0(n) = q^{\frac{n^2-n}{2}} = \prod_{i=1}^{n-1} q^{n-i},$$

respectively.

The probabilities are then obtained by taking the ratio $N(n,n)/T(n)$ in case of q odd, $N_0(n,n)/T_0(n)$ in case of q even and n even, and $N_0(n,n-1)/T_0(n)$ in case of q even and n odd. We obtain the stated lower bounds by bounding $\prod_{i=1}^{\lfloor k/2 \rfloor} \frac{q^{2i}}{q^{2i}-1}$ from below by 1. □

Remark 2.3 *In our attack, we will assume that the rank of a uniformly chosen quadratic form over $\mathbb{F}_q^n$ is n, resp., $n-1$ in case of both q even and n odd, with high probability. Indeed, Theorem 2.5 yields that these probabilities are at least the probability that an element in $M(n \times n, \mathbb{F}_q)$ is invertible, which is equal to $\mathcal{P}(q,n)$.*

We are now interested in a polynomial with a special shape.

Definition 2.6 *Let $V = \{x_1, \ldots, x_v\}$ and $O = \{x_{v+1}, \ldots, x_n\}$. A polynomial P_{OV} of the shape*

$$\sum_{1 \leq i,j \leq v} \alpha_{ij} x_i x_j + \sum_{\substack{1 \leq i \leq v \\ v+1 \leq j \leq n}} \beta_{ij} x_i x_j + \sum_{j=1}^{n} \gamma_j x_j + \delta,$$

$\alpha_{ij}, \beta_{ij}, \gamma_j, \delta \in \mathbb{F}_q$, is called an Oil and Vinegar (OV) polynomial *or* polynomial in OV form.

V is called the set of vinegar variables *and O the set of* oil variables. *If $|V| > |O|$, the OV polynomial is also referred to as an* unbalanced OV (UOV) polynomial.

Remark 2.4 *When fixing the vinegar variables, an OV polynomial is affine in the oil variables. Therefore, if $|V|$ is small enough, we can find the zeros efficiently by first guessing the vinegar variables and then applying Gaussian elimination.*

Given an OV polynomial P_{OV} as in Definition 2.6. We refer to the subspace

$$\underbrace{\{0\} \times \cdots \times \{0\}}_{\times v} \times \underbrace{\mathbb{F}_q \times \cdots \times \mathbb{F}_q}_{\times n-v}$$

as the oil space. *Note that the oil space is a subspace of the variety of $P_{OV} - P_{OV}(0, 0, \ldots, 0, x_{v+1}, \ldots, x_n)$. In the same vein,*

$$\underbrace{\mathbb{F}_q \times \cdots \times \mathbb{F}_q}_{\times v} \times \underbrace{\{0\} \times \cdots \times \{0\}}_{\times n-v}$$

is referred to as the vinegar space. *In case of multivariate cryptosystems build on OV polynomials, the central map is an OV polynomial where the affine part is zero. For more details on OV polynomials and early approaches to build cryptosystems with them, see e.g., [25],[14],[15].*

The next lemma, which gives some standard results in OV/UOV cryptanalysis (see e.g. [28]), and the subsequent theorem, which deals with a special case of OV polynomials, will be of importance in Subsection 4.3. Note that the subspace of isotropic vectors I_0 together with 0 in Lemma 2.7 is what is referred to as an oil space in the remark above.

Lemma 2.7 *Let L be a bijective linear mapping on $\mathbb{F}_q^n$ and $\mathfrak{q}_\nu \colon \mathbb{F}_q^n \to \mathbb{F}_q$ be uniformly chosen quadratic forms in OV form*

$$\sum_{1\leq i\leq j\leq v} \alpha_{ij}^{(\nu)} x_i x_j + \sum_{\substack{1\leq i\leq v \\ v+1\leq j\leq n}} \beta_{ij}^{(\nu)} x_i x_j =$$

$$\sum_{1\leq i\leq j\leq v} \alpha_{ij}^{(\nu)} x_i x_j + \sum_{1\leq i\leq v} x_i \ell_i^{(\nu)}(x_{v+1},\ldots,x_n), \tag{1}$$

where $1 \leq \nu \leq m$. Further, we are given the corresponding isometric forms $\mathfrak{q}'_\nu(x) \coloneqq \mathfrak{q}_\nu(L(x))$. We have:

1. *$I_0 \coloneqq \underbrace{\{0\}\times\cdots\times\{0\}}_{\times v} \times \underbrace{\mathbb{F}_q\times\cdots\times\mathbb{F}_q}_{\times n-v} \subset I_{\mathfrak{q}_\nu}$ for $1 \leq \nu \leq m$, where $I_{\mathfrak{q}_\nu}$ denotes the union of $\{0\}$ and the set of isotropic vectors of $\mathfrak{q}_\nu$.*
2. *If $n - v \leq m$, then for $u \in \mathbb{F}_q^v \setminus \{0\}$ the number of isotropic vectors $(u, w) \in \cap_{\nu=1}^m I_{\mathfrak{q}_\nu}$ is less than one with high probability. More precisely, this probability is at least $\prod_{i=0}^{n-v-1}(1 - q^{-(m-i)})$.*
3. *Let $\mathcal{B} = \{b_1, \ldots, b_{n-v}\}$ be a linear independent subset contained in $L^{-1}(I_0)$ and $u_1, \ldots, u_v$ an extension of $\mathcal{B}$ to a basis of $\mathbb{F}_q^n$. Then for the linear mapping L' defined by the matrix $(u_1, \ldots, u_v, b_1, \ldots, b_{n-v})$, the composition $L \circ L'$ has the representation matrix*

$$\begin{pmatrix} A & 0 \\ B & C \end{pmatrix}$$

with respect to the canonical basis. Thereby,

$$A \in M(v \times v, \mathbb{F}_q), B \in M((n-v)\times v, \mathbb{F}_q), C \in M((n-v)\times(n-v), \mathbb{F}_q).$$

4. *The forms $\mathfrak{q}'_\nu(L'(x))$ contain no quadratic monomials of the form $x_i x_j$ with $x_i, x_j \in O$.*

Proof. The first statement is obvious due to the special shape of each $\mathfrak{q}_\nu$. The second statement can be seen as follows: Fixing the first v variables conforming to u in each $\mathfrak{q}_\nu$ yields m uniformly random linear equations in the remaining $n - v$ variables, which readily becomes apparent from Expression 1 and the choice of $\mathfrak{q}_\nu$. As $u \neq 0$, the system has rank $n - v$ and thus at most one solution if the row space spanned by $\ell_i^{(\nu)}$ contains a basis of $\mathbb{F}_q^{n-v}$. By Lemma 1 this probability is at least $\prod_{i=0}^{n-v-1}(1 - q^{-(m-i)})$. Hence, the amount of isotropic vectors $(u, w) \in \cap_{\nu=1}^m I_{\mathfrak{q}_\nu}$ for fixed non-zero u is at most one with high probability as the above product becomes close to 1 very quickly.

Since L maps $\mathcal{B}$ into I_0, the third statement follows immediately. The fourth statement follows from the shape of the representation matrix of $L \circ L'$. □

Remark 2.5 *Note that we expect* $|\cap_{\nu=1}^{m} (I_{\mathfrak{q}_\nu} \setminus I_0)| \leq q^v - 1$ *with high probability by 1 and 2.*

The next theorem, which will be of importance in Section 4.3, shows a naive algorithm to compute L'. Observe that many attacks on UOV apply here. Given our parameters, the naive attack presented in Theorem 2.8 seems optimal to compute L' (see also Remark 2.6).

Theorem 2.8 *Given* $\mathfrak{q}_\nu(L(x)), 1 \leq \nu \leq m$ *as in Lemma 2.7 with* $n - v \leq m$. *If* $\left(\frac{q^v-1}{q^n}\right)\left(\frac{(n-v)q^v}{\mathcal{P}(q,n-v)}\right) \ll 1$, *then* L' *as in Lemma 2.7 can be computed with* $\mathcal{O}\left(\frac{m(n-v)q^v}{\mathcal{P}(q,n-v)}\right)$ *quadratic form evaluations.*

Proof. To compute L' one chooses b uniformly at random from $\mathbb{F}_q^n$ and checks whether $\mathfrak{q}_\nu(L(b)) = 0$ for all $1 \leq \nu \leq m$. Repeating this approximately $(n - v)q^v \cdot \mathcal{P}(q, n - v)^{-1}$ times yields $n - v$ linearly independent isotropic vectors $b_1, \ldots, b_{n-v}$ contained in $L^{-1}(I_0)$ on average, as long as

$$((q^v - 1)/q^n)\left((n - v)q^v\mathcal{P}(q, n - v)^{-1}\right) \ll 1.$$

This can be seen as follows. The probability that $\{b_1, \ldots, b_{n-v}\} \subset L^{-1}(I_0)$ is linear independent is equivalent to randomly choosing a basis in $\mathbb{F}_q^{n-v}$ due to the shape of I_0. The latter is equivalent to randomly choosing an invertible $(n - v) \times (n - v)$-matrix over $\mathbb{F}_q$; the probability for this is $\mathcal{P}(q, n - v) = (1 - \frac{1}{q})(1 - \frac{1}{q^2}) \cdots (1 - \frac{1}{q^{n-v}})$. It could have happened that some b was chosen from $L^{-1}(I_{\mathfrak{q}_\nu} \setminus I_0)$ for $1 \leq \nu \leq n-v$. Such an isotropic vector is chosen with probability at most $\frac{q^v-1}{q^n}$ by Remark 2.5. Since by assumption

$$((q^v - 1)/q^n)\left((n - v)q^v\mathcal{P}(q, n - v)^{-1}\right) \ll 1,$$

this is not expected to happen at all on average.

Thus, after $(n-v)q^v\mathcal{P}(q, n-v)^{-1}$ trials, $\mathcal{B}$ and finally L' is found on average. Since the check if $b \in L^{-1}(I_0)$ is carried out by checking that b is isotropic for all m forms, we get the desired number of evaluations and the theorem follows. Note that the cost for checking the linear independence of the found isotropic vectors is dominated by the quadratic form evaluations; each of them being in $\mathcal{O}(n^2)$. □

Remark 2.6 *More sophisticated approaches like the reconciliation attack (see [10] or [1] for a brief description) are not more efficient. The main reason is that, in our case,* v *and thus the resulting system of quadratic equations is so small for practical instances of* `Pesto` *that these are most efficiently solved by exhaustive search. Hence, the main complexity is in finding proper positions for the constraints, which is as complex as in our approach, and there is no gain in making use of Gröbner basis algorithms to solve the resulting restricted system of quadratic equations. Moreover, the check for orthogonality, which usually additionally speeds up the attack, makes it even slower as our approach.*

For estimating the complexity of our attack, similarly as in [5], we use that solving a linear system of m equations in n unknowns can be performed in $\mathcal{O}(mn\min(m,n))$ base field operations.
In the subsequent sections, by abuse of notation, $\mathfrak{q}$ will sometimes denote a quadratic map and not a quadratic form (i.e., $\mathfrak{q}$ could contain affine terms). The meaning will always be clear from the context.

3 A Description of Pesto

In this section we describe the design of Pesto. The approach makes use of CCZ equivalence. As this fact is neither of importance for our attack nor for understanding Pesto we refer for the details to [5]. We mainly follow the notation from the designers' work.

We now fix positive integers n, m, t, s with $t \leq \min(n, m)$ and $s \leq n - t$. We work with polynomials in n indeterminates $x_1, \ldots, x_t, y_1, \ldots, y_{n-t}$. The central map is based on the following maps:

- For a randomly chosen quadratic map $\mathfrak{q}\colon \mathbb{F}_q^{n-t} \to \mathbb{F}_q^t$, set
$$x - \mathfrak{q}(y) \coloneqq (x_1 - \mathfrak{q}_1(y), \ldots, x_t - \mathfrak{q}_t(y)).$$
Note that using $-$ instead of $+$ is due to the notation in [5]. We stress that, compared to a quadratic form, the ANF of the quadratic map $\mathfrak{q}$ could now consist of linear or constant terms.
- $U\colon \mathbb{F}_q^n \to \mathbb{F}_q^{m-t}$ is a mapping in which the $m - t$ coordinates consist of randomly chosen OV polynomials conforming Definition 2.6, where from now on $V = \{x_1, \ldots, x_t, y_1, \ldots, y_s\}$ and $O = \{y_{s+1}, \ldots, y_{n-t}\}$.

Let

- $A_1\colon \mathbb{F}_q^m \to \mathbb{F}_q^m, x \mapsto S(x) + c, S \in M(m \times m, \mathbb{F}_q), c \in \mathbb{F}_q^m$ be a randomly chosen affine bijection.
- $A_2\colon \mathbb{F}_q^n \to \mathbb{F}_q^n, x \mapsto T(x) + d, T \in M(n \times n, \mathbb{F}_q), d \in \mathbb{F}_q^n$ be a randomly chosen affine bijection.

Set $G \coloneqq (x - \mathfrak{q}(y), U(x - \mathfrak{q}(y), y))$. The map
$$G_{\text{pub}} \coloneqq A_1 \circ G \circ A_2$$
is the public key, and the tuple $(A_1, A_2, \mathfrak{q}, U)$ is the secret key.

Pesto Encryption Scheme *Encryption.*

1. The sender would like to encrypt the message $\mathtt{m}$. To do so, some redundancy r has to be added, such that the actual message to be encrypted is $z = (\mathtt{m}||r) \in \mathbb{F}_q^n$ with $||$ denoting the concatenation. The necessity for the redundancy r will become clear during the decryption process. For more details on how to choose the redundancy see, e.g., [27].

2. The sender encrypts z by computing $c = G_{\text{pub}}(z) \in \mathbb{F}_q^m$.

Decryption.

1. From $c \in \mathbb{F}_q^m$ compute $c' = A_1^{-1}(c)$.
2. For simplicity, set $z' = A_2(z)$ where z is the sought for plaintext. So $c' = G(z')$. This c' can be decomposed into $c' = (c'_Q, c'_U) \in \mathbb{F}_q^t \times \mathbb{F}_q^{m-t}$. Similarly $z' = (x', y') \in \mathbb{F}_q^t \times \mathbb{F}_q^{n-t}$. It holds

$$\begin{aligned} c'_Q &= x' - \mathfrak{q}(y') \\ c'_U &= U(x' - \mathfrak{q}(y'), y') = U(c'_Q, y'). \end{aligned}$$

   For fixed values $y'_1, \ldots, y'_s$, the system of equations $c'_U = U(c'_Q, y')$ becomes linear in $y'_{s+1}, \ldots, y'_{n-t}$ as the coordinates of U are OV polynomials. By exhaustive search over (possibly) all $(y'_1, \ldots, y'_s) \in \mathbb{F}_q^s$, a set of values $\mathcal{Y}' \subset \mathbb{F}_q^{n-t}$ is computed by solving the resulting linear system of equations.
3. For all $y \in \mathcal{Y}'$, the corresponding value x' is easily computed from $x' - \mathfrak{q}(y')$ and finally all possible plaintexts $z = A_2^{-1}(z') = A_2^{-1}((x', y'))$. The correct plaintext is identified by the redundancy r.

`Pesto` **Signature Scheme** This scheme can easily be turned into a signature scheme. The hash value $H(\mathtt{m})$ of the message $\mathtt{m}$ to be signed gets the role of c. From this all solutions z with $H(\mathtt{m}) = G_{\text{pub}}(z)$ are computed and one is chosen. Checking the signature is done by verifying that $H(\mathtt{m}) = G_{\text{pub}}(z)$.

To ensure that $H(\mathtt{m}) = G_{\text{pub}}(z)$ has a solution, one approach is for instance to consider $\mathtt{m}' = (\mathtt{m}||r)$, where r is a random value. By this variation, the system is expected to become solvable at some point.

Parameter Choices The designers of `Pesto` proposed three parameter sets for the signature scheme, which we list in Table 1. Their security analysis advises that in general s has to be chosen such that $s > 0$ and $t \approx \frac{n}{3}$. For more details on that parameter choices see [5]. Note that the designers did not provide a concrete proposal of parameters for the encryption scheme.

The designers also discussed a compressed variant of `Pesto`, where the linear part of A_1 is of the form

$$\begin{pmatrix} A & 0 \\ B & C \end{pmatrix}$$

$A \in M(t \times t, \mathbb{F}_q), B \in M((n-t) \times t, \mathbb{F}_q), C \in M((n-t) \times (n-t), \mathbb{F}_q)$. This leads to a reduction in the key size by not changing the security (see Remark 5 in [5]).

4 The Attack

The attack exploits the fact that it is possible to transform G_{pub} into a set of polynomials, which is equally easy to invert as the central map. To simplify the notation, let (x, y) denote the vector of indeterminates $(x_1, \ldots, x_t, y_1, \ldots, y_{n-t})$

or an element of $\mathbb{F}_q^n$. The meaning will always be clear from the context. Let $q'_i(x,y)$ denote the i-th coordinate of $(x - \mathfrak{q}(y)) \circ A_2(x,y)$ and

$$Q' \coloneqq < q'_1(x,y), \ldots, q'_t(x,y) >$$

the subspace of $\mathbb{F}_q[x_1, \ldots, x_n]$ considered as a vector space.

The general outline of the attack is as follows: If the public key is not compressed, then at first a basis of Q' is recovered. How to recover Q' is also given in [5] but to keep the paper self contained, we will show it here as well and additionally give more rigorous arguments why this approach indeed recovers Q' uniquely and does not give invalid solutions. This yields a transformation S'^{-1} applied to the public key. Note that S'^{-1} is the identity for compressed keys.

After that, the recovered basis of Q' is transformed into polynomials of the form $\mathfrak{l}_i(x) - \mathfrak{q}''_i(y)$, where $\mathfrak{l}_i$ corresponds to a linear and $\mathfrak{q}''_i$ to a quadratic mapping, by making use of radicals of quadratic forms. This steps yields another transformation T'^{-1} applied to the whole key. Then the $m-t$ degree-four polynomials of this transformed key are decomposed into $U'(\mathfrak{l}(x) - \mathfrak{q}''(y), y)$, where we skip the indices here to ease notation. After this step, U' has not yet exactly the shape of U, as the quadratic part purely in y has still more than s terms. Recall that $U \colon \mathbb{F}_q^n \to \mathbb{F}_q^{m-t}$ is a mapping in which the $m-t$ coordinates consist of OV polynomials with $V = \{x_1, \ldots, x_t, y_1, \ldots y_s\}$. By applying another transformation, one obtains $\mathfrak{l}'_i(x) - \mathfrak{q}'''_i(y)$, i.e., the desired U'', which is of the shape of U. By composing of all these linear transformations together with U'' and $\mathfrak{l}'_i(x) - \mathfrak{q}'''_i(y)$, the attacker is equipped with an equivalent key which allows to decrypt or sign any message with the same complexity as the owner of the legitimate key.

4.1 Step 1: Recover the Space Q'

Let $G' \coloneqq G \circ A_2$ and g'_i its coordinates. Similarly, let $g_{\text{pub},i}$ denote the coordinates of the public key. With this notation, $Q' =< g'_1, \ldots, g'_t >$. As mentioned above, Step 1 can be omitted for the compressed version as in this case we have

$$Q' =< g_{\text{pub},1}, \ldots, g_{\text{pub},t} >$$

already. To recover Q' we compute all linear combinations

$$\sum_{i=1}^{m} \alpha_i g_{\text{pub},i} = \sum_{i=1}^{m} \alpha_i \left(A_1 \circ G'\right)_i$$

such that the sum has degree at most 2. We use the following, assuming $q > 4$ to avoid exceptions when considering $G \circ A_2$ and counting monomials due to $x_i^q = x_i$.

Assumption. The polynomials $g'_{t+1}, \ldots, g'_m$ can be considered as randomly chosen polynomials of degree 4. Hence any linear combination has still degree 4 with high probability.

The second part of this assumption is justified by the following argument. There are

$$K(n) \coloneqq \binom{4+n-1}{n-1} + \binom{3+n-1}{n-1} = \binom{4+n-1}{4} + \binom{3+n-1}{3} \in \mathcal{O}(n^4)$$

monomials of degree 3 and 4 in n variables. We have

$$\sum_{i=1}^{m} \alpha_i \left(A_1 \circ G'\right)_i = \sum_{i=1}^{m} \alpha'_i g'_i,$$

for properly chosen α'_i. Hence, the sum can only have a degree of at most 2 if the terms of degree 3 and 4 in the partial sum $\sum_{t+1}^{m} \alpha'_i g'_i$ cancel out. Since these are assumed to behave like randomly chosen and m is much lower than $K(n)$ for values m, n that lead to practical instances of `Pesto`, the parts of degree 3 and 4 of $g'_{t+1}, \ldots, g'_m$ will be linear independent with very high probability, see Lemma 1. From this we get that $\alpha = (\alpha_1, \ldots, \alpha_m)$ is a solution if and only if $\alpha S \in \mathbb{F}_q^t \times \{0\} \times \cdots \times \{0\} \subset \mathbb{F}_q^m$. Thus, the solution space is generated by the first t rows of S^{-1} and will therefore be denoted by $S^{-1}_{Q'}$. We denote a basis of $S^{-1}_{Q'}$ by $\alpha_{Q',1}, \ldots, \alpha_{Q',t} \in \mathbb{F}_q^m$. Such a basis can be computed by solving a system of linear equations with m unknowns and at most $K(n)$ equations, i.e. one equation for each monomial of degree 4 and 3 occurring in at least one of the $g_{\mathrm{pub},i}$.

Let S'^{-1} denote the matrix, where the first rows are $\alpha_{Q',1}, \ldots, \alpha_{Q',t}$ and the last $m-t$ rows are the vectors $e_{t+1}, \ldots, e_m$. Then we denote the first t components of $S'^{-1} \circ G_{\mathrm{pub}}$ by $q'_{\alpha_{Q',1}}, \ldots, q'_{\alpha_{Q',t}}$, and we have

$$Q' = < q'_{\alpha_{Q',1}}, \ldots, q'_{\alpha_{Q',t}} > .$$

For the compressed version, we can simply take $S'^{-1} = Id$.

This step is dominated by the complexity of computing $\alpha_{Q',1}, \ldots, \alpha_{Q',t}$ by Gaussian elimination and has therefore a worst-case complexity of

$$\mathcal{O}\left(m^2 K(n)\right) = \mathcal{O}(m^2 n^4).$$

4.2 Step 2: Transform $q'_{\alpha_{Q',i}}$ Into $\mathfrak{l}_i(x) - \mathfrak{q}''_i(y)$

Recall that T denotes the linear part of A_2. Consider the homogeneous part of each $q'_{\alpha_{Q',i}}$ of degree 2, denoted $q'_{h,\alpha_{Q',i}}$. These are linear combinations of the homogeneous parts of $q'_i(x,y)$, which are equal to the homogeneous parts of degree 2 of $\mathfrak{q}_i(T(x,y)), i = 1, \ldots, t$. So, each $q'_{h,\alpha_{Q,i}}$ is isometric to a linear combination of $\mathfrak{q}_{h,1}, \ldots, \mathfrak{q}_{h,t}$, where $\mathfrak{q}_{h,i}$ denotes the homogeneous part of $\mathfrak{q}_i$. Note that we have a slight abuse of notation here, as by definition the $\mathfrak{q}_i$ are mappings from $\mathbb{F}_q^{n-t}$ to $\mathbb{F}_q$ and we now interpret them as mappings from $\mathbb{F}_q^n$ to $\mathbb{F}_q$ by setting the first t indeterminates to zero. In particular, $< e_1, \ldots, e_t > \subset \mathrm{rad}(\mathfrak{B}_{\mathfrak{q}_{h,i}})$. Crucially, we expect that

$$\cap_{i=1}^{t} \mathrm{rad}(\mathfrak{B}_{\mathfrak{q}_{h,i}}) = < e_1, \ldots, e_t >$$

holds with high probability. We give the reasoning below.

In case of q odd or both q and n even, since $\mathfrak{q}_i$ are randomly chosen mappings over $\mathbb{F}_q^{n-t}$, we expect the corresponding quadratic forms to have rank $n-t$ with a high probability by Theorem 2.5 and Remark 2.3. As t is large enough, we obtain $\cap_{i=1}^{t}\mathrm{rad}(\mathfrak{B}_{\mathfrak{q}_{h,i}}) =< e_1,\ldots,e_t >$ with high probability.

In case of q even and n odd, we first note that the probability that t' uniformly chosen vectors $v_1,\ldots,v_{t'} \in \mathbb{F}_q^{n-t}$ satisfy $\cap_{i=1}^{t'} < v_i >= \{0\}$ is

$$\left(1-\frac{(q^{n-t}-1)(q-1)^{t'-1}}{(q^{n-t})^{t'}}\right).$$

Now let t' be the number of quadratic forms among the $\mathfrak{q}_i$ having rank $n-t-1$. Each of them has a radical of dimension 1. This yields t' uniformly chosen vectors $r_1,\ldots,r_{t'} \in \underbrace{\{0\}\times\cdots\times\{0\}}_{\times t}\times\mathbb{F}_q^{n-t}$ generating the radicals. Hence, the probability that $\cap_{i=1}^{t'} < r_i >= \{0\}$ is $\left(1-\frac{(q^{n-t}-1)(q-1)^{t'-1}}{(q^{n-t})^{t'}}\right)$. Again by Theorem 2.5, Remark 2.3 and the size of t, this value will be close to 1 with a high probability.

At first the radical of $\mathfrak{B}_{q'_{h,\alpha_{Q',1}}}$ is computed. Since $q'_{h,\alpha_{Q',1}}$ is isometric to a linear combination of $\mathfrak{q}_{h,1},\ldots,\mathfrak{q}_{h,t}$, we expect by Corollary 2.4 and by what we have discussed so far that $\mathrm{rad}(\mathfrak{B}_{h,q'_{\alpha_{Q,1}}}) =< T^{-1}(e_1),\ldots,T^{-1}(e_t) >$ and thus to have dimension t. If the dimension is higher, it will be intersected with $\mathrm{rad}(\mathfrak{B}_{q'_{h,\alpha_{Q',2}}})$, and so on. If we proceed in this manner, we expect due to the above mentioned isometry that

$$\cap_{i=1}^{t}\mathrm{rad}(\mathfrak{B}_{q'_{h,\alpha_{Q',i}}}) =< T^{-1}(e_1),\ldots,T^{-1}(e_t) >$$

with high probability.

To compute the radical of $\mathfrak{B}_{q'_{h,\alpha_{Q',i}}}$ one has to solve the system of linear equations

$$\begin{aligned}\mathfrak{B}_{q'_{h,\alpha_{Q',i}}}(e_1,y) &= 0\\ &\vdots\\ \mathfrak{B}_{q'_{h,\alpha_{Q',i}}}(e_n,y) &= 0.\end{aligned}$$

Hence in the worst-case, i.e., one has to compute the complete intersection, a system of tn equations in n unknowns has to be solved. We conclude that this part has complexity $\mathcal{O}(tn^3)$.

Once a basis $t'_1,\ldots,t'_t$ of $< T^{-1}(e_1),\ldots,T^{-1}(e_t) >$ is recovered we generate a matrix T'^{-1}, where the t first columns are $t'_1,\ldots,t'_t$ and the last $n-t$ columns $t'_{t+1},\ldots,t'_n$ are chosen such that $t'_1,\ldots,t'_n$ form as basis of $\mathbb{F}_q^n$. Then the composition TT'^{-1} has the shape

$$\begin{pmatrix} A & B\\ 0 & C\end{pmatrix},$$

where $A \in M(t \times t, \mathbb{F}_q), B \in M(t \times (n-t), \mathbb{F}_q), C \in M((n-t) \times (n-t), \mathbb{F}_q)$. The composition $g_i'' \coloneqq q'_{\alpha_{Q',i}} \circ T'^{-1}$ has the shape $\mathfrak{l}_i(x) - \mathfrak{q}_i''(y)$, where $\mathfrak{q}_i''(y)$ is a quadratic mapping from $\mathbb{F}_q^{n-t}$ to $\mathbb{F}_q$ and $\mathfrak{l}_i$ a linear mapping from $\mathbb{F}_q^t$ to $\mathbb{F}_q$. Note that A is necessarily invertible and thus given $y = (y_1, \ldots, y_{n-t})$ and $c_1'', \ldots c_t''$ there always exists $x = (x_1, \ldots, x_t)$ such that $g_1''(x,y) = c_1'', \ldots, g_t''(x,y) = c_t''$. In other words $(g_1''(\cdot, y), \ldots, g_t''(\cdot, y))$ is still a bijection over $\mathbb{F}_q^t$ for any $y \in \mathbb{F}_q^{n-t}$. This fact is of importance later.

Then $S'^{-1} \circ G_{\text{pub}} \circ T'^{-1}$ is equal to

$$G'' \coloneqq \begin{pmatrix} g_1'' \\ \vdots \\ g_t'' \\ g_{t+1}'' \\ \vdots \\ g_m'' \end{pmatrix} = \begin{pmatrix} g_1'' \\ \vdots \\ g_t'' \\ g_{\text{pub},t+1} \circ T'^{-1} \\ \vdots \\ g_{\text{pub},m} \circ T'^{-1} \end{pmatrix}.$$

The current step is dominated by computing the radical(s) and thus has a complexity of $\mathcal{O}(tn^3)$.

Remark 4.1 *This step already reduces the entropy of the system by t. Indeed, let $c' \coloneqq S'^{-1}(c)$ for an intercepted ciphertext c. For the first t entries one gets the equations $c_i' = g_i'' = \mathfrak{l}_i(x) - \mathfrak{q}_i''(y)$. Exhaustive search over the $n-t$ variables y yields a linear system of equations in the remaining t variables x. Solving it and checking the result against the whole ciphertext yields the message after applying T'^{-1} to the remaining solution.*

In the next step we will transform $g_{\text{pub},t+1} \circ T'^{-1}, \ldots, g_{\text{pub},m} \circ T'^{-1}$ into polynomials such that, combined with g_i'', decryption will be as easy as with the knowledge of A_1, A_2.

4.3 Step 3: Transform the Lower Part of G''

Since the $q'_{\alpha_{Q',i}}$ generate Q' and thus especially the elements $q_i'(x,y)$, we have, for properly chosen elements $\alpha_{jkl}, \beta_{jkl}, \gamma_{ijl}, \delta_{il}, \nu_{jl}, \mu_l$, the identity

$$\begin{aligned} &\left(U(x - \mathfrak{q}(y), y) \circ A_2 \circ T'^{-1}\right)_l = \\ &\textstyle\sum_{1 \le j \le k \le t} \alpha_{jkl} g_j'' g_k'' + \\ &\textstyle\sum_{j \in \{1,\ldots,t\}, k \in \{1,\ldots,n-t\}} \beta_{jkl} g_j'' y_k + \\ &\textstyle\sum_{1 \le i \le j \le n-t} \gamma_{ijl} y_i y_j + \\ &\textstyle\sum_{i=1}^{t} \delta_{il} g_i'' + \\ &\textstyle\sum_{j=1}^{n-t} \nu_{jl} y_j + \mu_l, \end{aligned}$$

where l denotes the l-th coordinate for $l = 1, \ldots, t$. As $g_{t+1}'', \ldots, g_m''$ are linear combinations of $\left(U(x - \mathfrak{q}(y), y) \circ A_2 \circ T'^{-1}\right)_l$ and $g_1'', \ldots, g_t''$ due to the compo-

sition with A_1, we get from the above identity that

$$\begin{array}{l} g_l'' = \\ \sum_{1\le j\le k\le t} \alpha'_{jkl} g_j'' g_k'' + \\ \sum_{j\in\{1,\ldots,t\},k\in\{1,\ldots,n-t\}} \beta'_{jkl} g_j'' y_k + \\ \sum_{1\le i\le j\le n-t} \gamma'_{ijl} y_i y_j + \\ \sum_{i=1}^{t} \delta'_{il} g_i'' + \\ \sum_{j=1}^{n-t} \nu'_{jl} y_j + \mu'_l, \end{array} \tag{2}$$

for $l = t+1, \ldots, m$ and properly chosen $\alpha'_{jkl}, \beta'_{jkl}, \gamma'_{ijl}, \delta'_{il}, \nu'_{jl}, \mu'_l$.

This solution is unique if we exclude exceptional cases over $\mathbb{F}_2$, which are not of interest for this paper. This can be seen as follows: Consider the difference for two different solutions, i.e.,

$$\begin{array}{l} 0 = \\ \sum_{1\le i\le j\le t} (\alpha^{'(1)}_{jkl} - \alpha^{'(2)}_{jkl}) g_j'' g_k'' + \\ \sum_{j\in\{1,\ldots,t\},k\in\{1,\ldots,n-t\}} (\beta^{'(1)}_{jkl} - \beta^{'(2)}_{jkl}) g_j'' y_k + \\ \sum_{1\le i\le j\le n-t} (\gamma^{'(1)}_{ijl} - \gamma^{'(2)}_{ijl}) y_i y_j + \\ \sum_{i=1}^{t} (\delta^{'(1)}_{il} - \delta^{'(2)}_{il}) g_i'' + \\ \sum_{j=1}^{n-t} (\nu^{'(1)}_{jl} - \nu^{'(2)}_{jl}) y_j + (\mu^{'(1)}_{l} - \mu^{'(2)}_{l}). \end{array}$$

Recall that $(g_1''(\cdot, y), \ldots, g_t''(\cdot, y))$ is bijective over $\mathbb{F}_q^t$. Hence, each g_j'' can be considered as an independent variable in the above equation. Since a quadratic polynomial induces the zero-mapping under evaluation if and only if it is zero itself, the claim follows if we exclude exceptional cases over the field $\mathbb{F}_2$.

To compute the coefficients in Equation (2) one simply has to evaluate $g_1'', \ldots, g_m''$. Plugging the resulting values for $y_1, \ldots, y_{n-t}, g_1'', \ldots, g_m''$ into the equation yields linear equations in $\alpha'_{jkl}, \beta'_{jkl}, \gamma'_{ijl}, \delta'_{il}, \nu'_{jl}, \mu'_l$. Since the solution is unique we expect this system to have full rank after having generated $\mathcal{O}(n^2)$ equations this way for different inputs. Hence, this step has a complexity of $\mathcal{O}((m-t)n^6)$.

Since the solution is unique, it follows that the forms

$$\sum_{1\le i\le j\le n-t} \gamma'_{ijl} y_i y_j$$

are linear combinations of those quadratic parts of the OV polynomials from U, which are isometric to OV polynomials in $y_1, \ldots, y_{n-t}$ as in Lemma 2.7, where $v = s$. Thereby, the isometry L is defined by the representation matrix of $T \circ T'^{-1}$ restricted to the lower right $n-t$ rows and columns, which is given by C. Assuming that $\frac{q^s-1}{q^{n-t}} \left((n-t-s)q^s \cdot \mathcal{P}(q, n-t-s)^{-1}\right) \ll 1$, which is the case for the practical instances proposed by the designers, Theorem 2.8 can be applied to these forms. Extending the resulting isometry $\widetilde{C}^{-1}$ in $n-t$ to

$$C'^{-1} = \begin{pmatrix} E_t & 0 \\ 0 & \widetilde{C}^{-1} \end{pmatrix} \in M(n \times n, \mathbb{F}_q),$$

where E_t is the $t \times t$ identity matrix, and composing the latter with G'' yields $m - t$ polynomials of the form

$$\begin{array}{l} g_l''' = \\ \sum_{1 \le j \le k \le t} \alpha''_{jkl} g_j''' g_k''' + \\ \sum_{j \in \{1,\ldots,t\}, k \in \{1,\ldots,n-t\}} \beta''_{jkl} g_j''' y_k + \\ \sum_{1 \le i \le j \le s} \gamma''_{ijl} y_i y_j + \\ \sum_{1 \le i \le s} y_i \ell_{il}(y_{s+1}, \ldots, y_{n-t}) \\ \sum_{i=1}^{t} \delta''_{il} g_i''' + \\ \sum_{j=1}^{n-t} \nu''_{jl} y_j + \mu''_l, \end{array}$$

for properly chosen $\alpha''_{jkl}, \beta''_{jkl}, \gamma''_{ijl}, \delta''_{il}, \nu''_{jl}, \mu''_l$. Thereby, $g_1''', \ldots, g_t'''$ remains of the shape $\mathfrak{l}'_i(x) - \mathfrak{q}'''_i(y)$ for a linear mapping $\mathfrak{l}'_i$ and quadratic mapping $\mathfrak{q}'''_i$.

Obviously, Step 3 is dominated by the first part, which is in $\mathcal{O}\left(n^6(m-t)\right)$, or the last part, which needs $\mathcal{O}\left((m-t)(n-t-s)q^s \cdot \mathcal{P}(q, n-t-s)^{-1}\right)$ quadratic form evaluations by Theorem 2.8. Since each quadratic form evaluation costs $(n-t)^2$ base field operations, this step has overall complexity of

$$\max\left\{\mathcal{O}\left(n^6(m-t)\right), \mathcal{O}\left((m-t)(n-t)^2(n-t-s)q^s \cdot \mathcal{P}(q, n-t-s)^{-1}\right)\right\}$$

base field operations on average.

4.4 Decrypting Any Ciphertext or Forging Any Signature

Without loss of generality, we restrict to show how to attack the encryption algorithm. For an intercepted c, the mapping S'^{-1} is applied resulting in $c' = (c'_1, \ldots, c'_m)$. For each $l = t+1, \ldots, m$, the polynomials $g_1''', \ldots, g_t'''$ in the equation

$$\begin{array}{l} c'_l = \\ \sum_{1 \le i \le j \le t} \alpha''_{jkl} g_j''' g_k''' + \\ \sum_{j \in \{1,\ldots,t\}, k \in \{1,\ldots,n-t\}} \beta''_{jkl} g_j''' y_k + \\ \sum_{1 \le i \le j \le s} \gamma''_{ijl} y_i y_j + \\ \sum_{1 \le i \le s} y_i \ell_{il}(y_{s+1}, \ldots, y_{n-t}) \\ \sum_{i=1}^{t} \delta''_{il} g_i''' + \\ \sum_{j=1}^{n-t} \nu''_{jl} y_j + \mu''_l \end{array}$$

are substituted by $c'_1, \ldots, c'_t$. After that, a brute-force step is conducted for all values $y_1, \ldots, y_s$. For each candidate, the resulting linear system of equations in $y_{s+1}, \ldots, y_{n-t}$ is solved. The corresponding solution $y_1, \ldots, y_{n-t}$ is plugged into $g_1''', \ldots, g_t'''$ and the remaining system of linear equations in $x_1, \ldots, x_t$ is solved. This step has a complexity of

$$\mathcal{O}(q^s(m-t)(n-t-s) \cdot \min(m-t, n-t-s) + q^s t(n-t)^2 + q^s t^3)$$

base field operations. Applying $T'^{-1}C'^{-1}$ to the resulting vector in $\mathbb{F}_q^n$ and checking if the result is a correct message conforming to the redundancy r yields finally the plaintext and we are done.

The overall attack complexity for $m \le n, t, s \le n$ (the typical case) is summarized in the following theorem.

Theorem 4.1 *For* `Pesto` *with parameters* $m \leq n, t, s \leq n$ *and*

$$\frac{q^s - 1}{q^{n-t}} \left((n-t-s) q^s \cdot \mathcal{P}(q, n-t-s)^{-1} \right) \ll 1,$$

one can generate an equivalent secret key from the public key with a precomputation of a worst-case complexity of

$$\max \left\{ \mathcal{O}\left(n^6(m-t)\right), \mathcal{O}\left((m-t)(n-t)^2(n-t-s)q^s \cdot \mathcal{P}(q, n-t-s)^{-1}\right) \right\}$$

base field operations. Deciphering an intercepted message or forging a signature has an online complexity of

$$\mathcal{O}(q^s(m-t)(n-t-s) \cdot \min(m-t, n-t-s) + q^s t(n-t)^2 + q^s t^3)$$

base field operations.

Proof. Obviously, the complexity of Step 3 dominates the precomputation (note that we assume $m \leq n$). Moreover, deciphering or forging a signature is carried out with the substitute key almost as fast as with the original key. The additional matrix multiplications with $S'^{-1}, T'^{-1}C'^{-1}$ do not increase the overall cost, as it is dominated by solving q^s times a system in initially $n-t-s$ and then in t indeterminates. □

Remark 4.2 *Note that the online phase of our attack is about as fast as using the legitimate key for practical choices of* n, t, s.

4.5 Implementation of the Attack

We prepared a proof-of-concept implementation of our attack in Magma [4]. We run the attack on all three instances of the signature scheme proposed by the designers on a machine with 40 x Intel(R) Xeon(R) Silver 4114 CPU @ 2.20GHz (2 sockets) and 300 GB RAM using 20 threads. To have more benchmarks, we also conducted the attack on the compressed variant of `Pesto` (omitting Step 1 of the attack, see Subsection 4.1), where the linear part of A_1 is already of the form

$$\begin{pmatrix} A & 0 \\ B & C \end{pmatrix}.$$

Note that the designers already acknowledged that the reduction from the full variant of `Pesto` to the compressed version is of complexity $\mathcal{O}(n^6)$ (note that $m \leq n$ for their parameter proposals), so that the former may not offer additional security over the latter, see [5, Remark 5].

The execution times are given in Table 2. For instance, for the NIST I instance, we were able to recover an equivalent secret key for a compressed instance in about 3 minutes, for the full version in about 3.5 minutes, and to decrypt an intercepted ciphertext in less than a minute. Note that, for simplicity, we did not add any redundancy to the plaintexts.

5 Conclusion

We presented an attack against `Pesto` by targeting the decomposition problem to recover an equivalent secret key.

To build possibly secure systems based on the idea introduced in [5], one has to remove the separation of variables induced by $x - \mathtt{q}(y)$ and the OV polynomials. The challenge is then to find a way to get an easy-to-invert mapping by maintaining cryptosystems with practical key sizes. Despite the attack presented here, we think it is valuable to conduct further research in this direction. Having secure multivariate cryptosystems is an important cornerstone in post-quantum cryptography.

Acknowledgments

We thank the anonymous reviewers for their detailed and helpful comments, which allowed us to improve the editorial and technical quality of the article. We thank Frederik Gosewehr for testing the Magma code.

Use of generative AI. We used *Google Gemini 3.1 Pro* to optimize the Magma implementation of our attack, leaving the overall algorithmic design and theoretical framework unchanged.

References

1. Beullens, W.: Improved cryptanalysis of UOV and Rainbow. In: Canteaut, A., Standaert, F. (eds.) Advances in Cryptology - EUROCRYPT 2021, Proceedings, Part I. Lecture Notes in Computer Science, vol. 12696, pp. 348–373. Springer (2021). https://doi.org/10.1007/978-3-030-77870-5_13
2. Beullens, W.: Breaking Rainbow takes a weekend on a laptop. In: Dodis, Y., Shrimpton, T. (eds.) Advances in Cryptology - CRYPTO 2022, Proceedings, Part II. Lecture Notes in Computer Science, vol. 13508, pp. 464–479. Springer (2022). https://doi.org/10.1007/978-3-031-15979-4_16
3. Beullens, W.: MAYO: Practical post-quantum signatures from oil-and-vinegar maps. In: AlTawy, R., Hülsing, A. (eds.) Selected Areas in Cryptography. SAC 2021. Lecture Notes in Computer Science, vol. 13203, pp. 355–376. Springer, Cham (2022). https://doi.org/10.1007/978-3-030-99277-4_17
4. Bosma, W., Cannon, J., Playoust, C.: The Magma algebra system. I. The user language. J. Symbolic Comput. **24**(3-4), 235–265 (1997). https://doi.org/10.1006/jsco.1996.0125
5. Calderini, M., Caminata, A., Villa, I.: A new multivariate primitive from CCZ equivalence. J. Cryptol. **38**(3), 25 (2025). https://doi.org/10.1007/S00145-025-09544-7
6. Caminata, A., Gorla, E., Mabe, M., Vigorito, M., Villa, I.: Cryptanalysis of a multivariate CCZ scheme. Des. Codes Cryptogr. **94**(4), 75 (2026). https://doi.org/10.1007/s10623-025-01793-8

7. Carlet, C., Charpin, P., Zinoviev, V.A.: Codes, bent functions and permutations suitable for des-like cryptosystems. Des. Codes Cryptogr. **15**(2), 125–156 (1998). https://doi.org/10.1023/A:1008344232130
8. Cartor, R., Smith-Tone, D.: EFLASH: A New Multivariate Encryption Scheme. In: Cid, C., Jacobson Jr., M. (eds.) Selected Areas in Cryptography – SAC 2018. Lecture Notes in Computer Science, vol. 11349, pp. 281–299. Springer International Publishing (2019)
9. Ding, J., Schmidt, D.: Rainbow, a new multivariable polynomial signature scheme. In: Ioannidis, J., Keromytis, A.D., Yung, M. (eds.) Applied Cryptography and Network Security, Third International Conference, ACNS 2005, Proceedings. Lecture Notes in Computer Science, vol. 3531, pp. 164–175 (2005). https://doi.org/10.1007/11496137_12
10. Ding, J., Yang, B., Chen, C.O., Chen, M., Cheng, C.: New differential-algebraic attacks and reparametrization of Rainbow. In: Bellovin, S.M., Gennaro, R., Keromytis, A.D., Yung, M. (eds.) Applied Cryptography and Network Security, 6th International Conference, ACNS 2008, Proceedings. Lecture Notes in Computer Science, vol. 5037, pp. 242–257 (2008). https://doi.org/10.1007/978-3-540-68914-0_15
11. Faugère, J., Joux, A.: Algebraic cryptanalysis of hidden field equation (HFE) cryptosystems using Gröbner bases. In: Boneh, D. (ed.) Advances in Cryptology - CRYPTO 2003, Proceedings. Lecture Notes in Computer Science, vol. 2729, pp. 44–60. Springer (2003). https://doi.org/10.1007/978-3-540-45146-4_3
12. Forster, O.: Algorithmische Zahlentheorie. Springer Spektrum Wiesbaden, 2 edn. (2015)
13. Hachenberger, D., Jungnickel, D.: Topics in Galois Fields. Springer Cham (2020). https://doi.org/10.1007/978-3-030-60806-4
14. Kipnis, A., Patarin, J., Goubin, L.: Unbalanced oil and vinegar signature schemes. In: Stern, J. (ed.) Advances in Cryptology - EUROCRYPT '99, Proceeding. Lecture Notes in Computer Science, vol. 1592, pp. 206–222. Springer (1999). https://doi.org/10.1007/3-540-48910-X_15
15. Kipnis, A., Shamir, A.: Cryptanalysis of the oil & vinegar signature scheme. In: Krawczyk, H. (ed.) Advances in Cryptology - CRYPTO '98, Proceedings. Lecture Notes in Computer Science, vol. 1462, pp. 257–266. Springer (1998). https://doi.org/10.1007/BFB0055733
16. Lam, T.Y.: The algebraic theory of quadratic forms. Mathematics lecture note series, W.A. Benjamin, Reading, Mass (1973)
17. Lidl, R., Niederreiter, H.: Finite Fields. Cambridge University Press (1997)
18. Macario-Rat, G., Patarin, J.: Two-face: New public key multivariate schemes. In: Joux, A., Nitaj, A., Rachidi, T. (eds.) Progress in Cryptology - AFRICACRYPT 2018, Proceedings. Lecture Notes in Computer Science, vol. 10831, pp. 252–265. Springer (2018). https://doi.org/10.1007/978-3-319-89339-6_14
19. MacWilliams, J.: Orthogonal matrices over finite fields. Am. Math. Mon. **76**(2), 152–164 (1969)
20. Matsumoto, T., Imai, H.: Public quadratic polynominal-tuples for efficient signature-verification and message-encryption. In: Barstow, D., Brauer, W., Brinch Hansen, P., Gries, D., Luckham, D., Moler, C., Pnueli, A., Seegmüller, G., Stoer, J., Wirth, N., Günther, C.G. (eds.) Advances in Cryptology - EUROCRYPT '88, Proceedings. Lecture Notes in Computer Science, vol. 330, pp. 419–453. Springer (1988). https://doi.org/10.1007/3-540-45961-8_39

21. Moody, D., Perlner, R., Smith-Tone, D.: An asymptotically optimal structural attack on the ABC multivariate encryption scheme. In: Mosca, M. (ed.) Post-Quantum Cryptography. PQCrypto 2014. Lecture Notes in Computer Science, vol. 8772, pp. 180–196. Springer, Cham (2014). https://doi.org/10.1007/978-3-319-11659-4_11
22. National Institute for Standards and Technology: Post-Quantum Cryptography Standardization, https://csrc.nist.gov/projects/post-quantum-cryptography, accessed May 11, 2026
23. Øygarden, M., Felke, P., Raddum, H.: Analysis of multivariate encryption schemes: Application to Dob. In: Garay, J.A. (ed.) Public-Key Cryptography - PKC 2021, Proceedings, Part I. Lecture Notes in Computer Science, vol. 12710, pp. 155–183. Springer (2021). https://doi.org/10.1007/978-3-030-75245-3_7
24. Øygarden, M., Felke, P., Raddum, H., Cid, C.: Cryptanalysis of the multivariate encryption scheme EFLASH. In: Jarecki, S. (ed.) Topics in Cryptology - CT-RSA 2020, Proceedings. Lecture Notes in Computer Science, vol. 12006, pp. 85–105. Springer (2020). https://doi.org/10.1007/978-3-030-40186-3_5
25. Patarin, J.: The oil and vinegar signature scheme. Presented at Dagstuhl Workshop on Cryptography September, 1997
26. Patarin, J.: Cryptanalysis of the Matsumoto and Imai public key scheme of Eurocrypt'88. In: Coppersmith, D. (ed.) Advances in Cryptology - CRYPTO '95, Proceedings. Lecture Notes in Computer Science, vol. 963, pp. 248–261. Springer (1995). https://doi.org/10.1007/3-540-44750-4_20
27. Patarin, J.: Hidden fields equations (HFE) and isomorphisms of polynomials (IP): two new families of asymmetric algorithms. In: Maurer, U.M. (ed.) Advances in Cryptology - EUROCRYPT '96, Proceeding. Lecture Notes in Computer Science, vol. 1070, pp. 33–48. Springer (1996). https://doi.org/10.1007/3-540-68339-9_4
28. Pébereau, P.: One vector to rule them all: Key recovery from one vector in uov schemes. In: Saarinen, M.J., Smith-Tone, D. (eds.) Post-Quantum Cryptography. PQCrypto 2024. Lecture Notes in Computer Science, vol. 14772, pp. 92–108. Springer, Cham (2024). https://doi.org/10.1007/978-3-031-62746-0_5
29. Shor, P.W.: Algorithms for quantum computation: Discrete logarithms and factoring. In: 35th Annual Symposium on Foundations of Computer Science, Santa Fe, New Mexico, USA, November 20-22, 1994. pp. 124–134. IEEE Computer Society (1994). https://doi.org/10.1109/SFCS.1994.365700
30. Tao, C., Diene, A., Tang, S., Ding, J.: Simple matrix scheme for encryption. In: Gaborit, P. (ed.) Post-Quantum Cryptography. PQCrypto 2013. Lecture Notes in Computer Science, vol. 7932, pp. 231–242. Springer, Berlin, Heidelberg (2013). https://doi.org/10.1007/978-3-642-38616-9_16
31. Yasuda, T., Wang, Y., Takagi, T.: Multivariate encryption schemes based on polynomial equations over real numbers. In: Ding, J., Tillich, J. (eds.) Post-Quantum Cryptography - 11th International Conference, PQCrypto 2020, Proceedings. Lecture Notes in Computer Science, vol. 12100, pp. 402–421. Springer (2020). https://doi.org/10.1007/978-3-030-44223-1_22