Explicit Bounds on the Existence Probability of Random Multivariate Quadratic Systems over Finite Fields

Michiya Iwata, Ryomei Sugai, Kosuke Sakata, and Tsuyoshi Takagi

The University of Tokyo, Department of Mathematical Informatics, Japan

Abstract. The security of multivariate public-key cryptography, a major approach to post-quantum cryptography, is based on the computational hardness of solving systems of multivariate quadratic equations over finite fields (the MQ problem). The MQ problem consists of solving a system of quadratic equations over a finite field of size q, with n variables and m polynomials. The existence probability of solutions to the MQ problem plays a central role in analyzing the security of multivariate cryptography. However, explicit bounds for fixed parameters (q, n, m) have not been sufficiently studied. In this work, we evaluate the existence probability for randomly generated MQ systems with fixed parameters by analyzing the coefficient space arising from the MQ system. Using the inclusion–exclusion principle, we obtain a lower bound (approximately 0.625) and an upper bound (approximately 0.667) on the existence probability, focusing on the case $m = n$. We also derive upper and lower bounds on the probability that the number of solutions is exactly one in the case $m = n$. Finally, we analyze the existence probability of solutions to the MQ problem in the case $m \neq n$.

Keywords: post-quantum cryptography, multivariate public-key cryptography, MQ problem

1 Introduction

Multivariate public-key cryptography is a well-established approach to post-quantum cryptography, originating with the proposal of Matsumoto and Imai in 1988 [15]. Representative signature schemes include UOV [11], MAYO [3], and QR-UOV [6].

The MQ problem (Multivariate Quadratic Problem) is the problem of finding solutions to a system of m quadratic polynomials in n variables over a finite field $\mathbb{F}_q$ of size q. The security of multivariate public-key cryptography is based on the computational hardness of the MQ problem. Various algorithms for solving the MQ problem have been proposed, including Gröbner basis methods [5] and hybrid methods [2]. On the other hand, a satisfactory theoretical understanding of the solution existence probability remains limited.

Various classical theories are known for the number of solutions to polynomial systems over finite fields. When the number of variables is large compared

with the degrees, results of Warning [17] and refinements by Ax and Katz [1, 10] provide nontrivial information on the number of zeros. For a fixed system, evaluations via character sums [18] and algebraic-geometric estimates of rational points [12] are also available. For a single polynomial, the Schwartz–Zippel lemma [16, 19] gives an upper bound on the probability that a random evaluation yields zero. These existing studies do not necessarily fit the choice of parameters assumed in the MQ problem, and they do not provide the distributional behavior of MQ problems.

Among probabilistic approaches, inclusion–exclusion has played a central role. For a single *univariate* polynomial of fixed degree, the number of polynomials with no zeros can be computed explicitly by the inclusion–exclusion principle [14]. More recently, Fusco and Bach [7] derived the *asymptotic* distribution of the number of solutions for systems of multivariate polynomials of degree at least two, using inequalities based on inclusion–exclusion.

Our contributions. We provide explicit finite-parameter bounds on the solution existence probability P_{exist} for random systems of m quadratic equations in n variables over $\mathbb{F}_q$, extending the inclusion–exclusion analysis for univariate polynomials [14] to multivariate quadratic polynomial systems over finite fields.

- In the case $m = n$, we derive bounds $R^{(2)}_{\text{lower}}$ and $R^{(3)}_{\text{upper}}$ (Theorem 1), and an improved lower bound $R^{(4)}_{\text{lower}}$ by analyzing rank drops (Theorem 2).
- We analyze the solution-count distribution by computing the expectation and the variance, and we bound the probability that the MQ system has exactly one solution when $m = n$ (Theorem 4).
- We provide explicit bounds on P_{exist} in the overdetermined case $m > n$ and the underdetermined case $m < n$ (Theorem 5,6).
- As an application to cryptanalysis, we revisit the analysis of Hashimoto's algorithm by replacing the commonly used heuristic assumption on P_{exist} with our provable bounds (Section 7).

These results provide theoretical foundations for security analyses in multivariate public-key cryptography and offer further insight into the probabilistic behavior of random quadratic systems over finite fields.

Organization of the paper. Section 2 defines the solution existence probability P_{exist} for the MQ problem, and reviews related work. Section 3 presents our estimation framework based on inclusion–exclusion inequalities and introduces the basic bounds. Section 4 improves the lower bound by analyzing rank drops through affine invariance. Section 5 studies the distribution of the number of solutions and derives upper and lower bounds on the probability that the MQ system has exactly one solution. Section 6 extends the existence-probability analysis to the case $m \neq n$. Finally, Section 7 discusses an application to cryptanalysis.

2 The MQ Problem and the Existence Probability

In this section, we define the MQ problem, introduce the solution existence probability P_{exist}, and review related work.

2.1 The Solution-Existence Probability for the MQ Problem

The MQ problem (Multivariate Quadratic Problem) can be defined as follows.

Definition 1 (MQ problem). *The* MQ *problem over a finite field $\mathbb{F}_q$ is the following. Let $n, m \in \mathbb{N}$, and let $f_1, \ldots, f_m \in \mathbb{F}_q[x_1, \ldots, x_n]$ be m quadratic polynomials in n variables $x_1, \ldots, x_n \in \mathbb{F}_q$. The problem is to find $x_1, \ldots, x_n \in \mathbb{F}_q$ satisfying $f_1 = \cdots = f_m = 0$.*

More explicitly, each f_k can be written as follows.

$$\begin{cases} f_1(x_1, \ldots, x_n) = \displaystyle\sum_{1 \le i \le j \le n} a_{ij}^{(1)} x_i x_j + \sum_{1 \le i \le n} b_i^{(1)} x_i + c^{(1)} = 0, \\ \qquad\qquad \vdots \\ f_m(x_1, \ldots, x_n) = \displaystyle\sum_{1 \le i \le j \le n} a_{ij}^{(m)} x_i x_j + \sum_{1 \le i \le n} b_i^{(m)} x_i + c^{(m)} = 0. \end{cases} \tag{1}$$

The system is called underdetermined if $n > m$ and overdetermined if $m > n$.

For the subsequent discussion, we introduce notation and definitions.

- We represent an n-tuple of variables by a vector $\boldsymbol{x} = (x_1, \ldots, x_n) \in \mathbb{F}_q^n$.
- Each polynomial $f_k \in \mathbb{F}_q[x_1, \ldots, x_n]$ in an MQ system has $N = \frac{(n+2)(n+1)}{2}$ coefficients. Writing $f_k(x_1, \ldots, x_n) = \sum_{1 \le i \le j \le n} a_{ij}^{(k)} x_i x_j + \sum_{1 \le i \le n} b_i^{(k)} x_i + c^{(k)}$, we define the column vector obtained by listing all coefficients as $\boldsymbol{\theta}^{(k)} = \left(a_{11}^{(k)}, a_{12}^{(k)}, \ldots, a_{nn}^{(k)}, b_1^{(k)}, \ldots, b_n^{(k)}, c^{(k)}\right)^\top \in \mathbb{F}_q^N$. Here, $a_{ij}^{(k)}$ $(1 \le i \le j \le n)$ are ordered lexicographically with respect to the pair (i, j).
- We denote by $\boldsymbol{\theta} = \left(\boldsymbol{\theta}^{(1)}, \boldsymbol{\theta}^{(2)}, \ldots, \boldsymbol{\theta}^{(m)}\right)^\top \in \mathbb{F}_q^{mN}$ the column vector obtained by listing all mN coefficients of $f_1, \ldots, f_m$, and call it the coefficient vector. The tuple $(f_1, \ldots, f_m)$ is in one-to-one correspondence with $\boldsymbol{\theta} \in \mathbb{F}_q^{mN}$.
- For $\boldsymbol{\theta} \in \mathbb{F}_q^{mN}$, we let $f^{(\boldsymbol{\theta})}$ denote the tuple $(f_1, \ldots, f_m)$ determined by $\boldsymbol{\theta}$, and we write the system $f_1(\boldsymbol{x}) = \cdots = f_m(\boldsymbol{x}) = 0$ as $f^{(\boldsymbol{\theta})}(\boldsymbol{x}) = 0$.

Definition 2 (Existence probability of solutions to the MQ problem). *Define the probability space $(\Omega, \mathcal{F}, P)$ by $\Omega = \mathbb{F}_q^{mN}$, $\mathcal{F} = 2^\Omega$, and $P(A) = \frac{|A|}{|\Omega|}$ for $A \subset \Omega$. The existence probability of solutions to the* MQ *problem is the probability P_{exist} that, when a coefficient vector $\boldsymbol{\theta} \in \mathbb{F}_q^{mN}$ is chosen uniformly at random, the system $f^{(\boldsymbol{\theta})}(\boldsymbol{x}) = 0$ has at least one solution $\boldsymbol{x} \in \mathbb{F}_q^n$, defined by*

$$P_{\text{exist}} = P\left(\left\{\boldsymbol{\theta} \in \mathbb{F}_q^{mN} \mid \exists \boldsymbol{x} \in \mathbb{F}_q^n,\ f^{(\boldsymbol{\theta})}(\boldsymbol{x}) = 0\right\}\right).$$

2.2 Probability Evaluations and the Inclusion–Exclusion Principle

For a single univariate polynomial, the number of monic polynomials with a root can be computed explicitly via inclusion–exclusion [14]. For multivariate systems, Fusco and Bach [7] derived asymptotic estimates for the probability of having no solution using inclusion–exclusion inequalities.

The case of a single polynomial in one variable [14] For $x \in \mathbb{F}_q$, let $W_x^d \subset \mathbb{F}_q[x]$ be

$$W_x^d = \{f \mid f(x) = 0,\ f \text{ is monic},\ \deg f = d\}.$$

Then the number of monic degree-d polynomials having a root is $\left|\bigcup_{x\in\mathbb{F}_q} W_x^d\right|$. By the inclusion–exclusion principle,

$$\left|\bigcup_{x\in\mathbb{F}_q} W_x^d\right| = \sum_{k=1}^{q} \sum_{x_1<\cdots<x_k} (-1)^{k+1} \left|W_{x_1}^d \cap \cdots \cap W_{x_k}^d\right|$$

holds. When $k > d$, since a monic degree-d polynomial $f(x) \in \mathbb{F}_q[x]$ has at most d roots, we have $\left|W_{x_1}^d \cap \cdots \cap W_{x_k}^d\right| = 0$. When $k \leq d$, if a monic degree-d polynomial $f(x) \in \mathbb{F}_q[x]$ has k roots $x_1, \ldots, x_k$, then it can be written as $f(x) = (x - x_1)\ldots(x - x_k)\phi(x)$ using an arbitrary monic polynomial $\phi(x)$ of degree $d - k$, and hence $\left|W_{x_1}^d \cap \cdots \cap W_{x_k}^d\right| = q^{d-k}$. Therefore, the number of monic degree-d polynomials having a root is given by $\sum_{k=1}^{d}(-1)^{k+1}\binom{q}{k}q^{d-k}$. Then, the existence probability of solutions to a single monic degree-d univariate polynomial is $\sum_{k=1}^{d}(-1)^{k+1}\binom{q}{k}q^{-k}$. We aim to extend this work to MQ systems.

The case of asymptotic distributions of the number of solutions [7] Let $d \geq 2$ and let p be a prime. For a system with m equations in n variables, let $\alpha = m - n$. For each sufficiently large n, choose $f_1, \ldots, f_{n+\alpha} \in \mathbb{F}_p[x_1, \ldots, x_n]$ uniformly at random among degree-d polynomials. Then, as $n \to \infty$, the probability that the system $f_1 = \cdots = f_{n+\alpha} = 0$ has no solution converges to $\mathrm{e}^{-p^{-\alpha}}$. Moreover, the number of solutions in $\mathbb{F}_p^n$ converges in distribution to the Poisson law with parameter $\lambda = p^{-\alpha}$.

In particular, when $\alpha = 0$, i.e., when $m = n$, the probability of having no solution is asymptotically e^{-1}. In the proofs of these theorems, one sets $I_{\boldsymbol{x}} = \begin{cases} 1 & (f_1(\boldsymbol{x}) = \cdots = f_{n+\alpha}(\boldsymbol{x}) = 0), \\ 0 & (\text{otherwise}), \end{cases}$ and uses the fact that the probability of having no solution can be written as

$$\mathrm{E}\left[\prod_{\boldsymbol{x}}(1 - I_{\boldsymbol{x}})\right] = \sum_{k=0}^{p^n}(-1)^k \sum_{\boldsymbol{x}^{(1)}<\cdots<\boldsymbol{x}^{(k)}} \mathrm{E}\left[\prod I_{\boldsymbol{x}^{(i)}}\right].$$

For sufficiently large n, one uses that $\sum_{\boldsymbol{x}^{(1)}<\cdots<\boldsymbol{x}^{(k)}} \mathrm{E}\left[\prod I_{\boldsymbol{x}^{(i)}}\right] \approx \frac{p^{-\alpha k}}{k!}$, and from inclusion–exclusion inequalities one obtains, for odd K,

$$-\frac{p^{-\alpha K}}{K!}(1 + o(1)) \leq \mathrm{E}\left[\prod_{\boldsymbol{x}}(1 - I_{\boldsymbol{x}})\right] - \sum_{k=0}^{K-1}(-1)^k \frac{p^{-\alpha k}}{k!} \leq \frac{p^{-\alpha(K+1)}}{(K+1)!}(1 + o(1)).$$

Hence, as $n \to \infty$, the probability of having no solution converges to $\mathrm{e}^{-p^{-\alpha}}$.

This prior work focuses on the asymptotic behavior of the solution-count distribution, and does not provide an evaluation for fixed parameters. Therefore, in this work we aim to give explicit upper and lower bounds on the existence probability of solutions for a fixed n.

2.3 Related Work

Let p be the characteristic of the finite field $\mathbb{F}_q$. Refining Chevalley's theorem [4], Warning proved that, when $n > \sum_i \deg f_i$, the number of solutions to $f_1 = \cdots = f_m = 0$ satisfies (number of solutions) $\equiv 0 \mod p$ [17]. Later, Ax and Katz extended this theorem [1, 10].

On the other hand, it is known that the number of solutions can be expressed using character sums. Using a nontrivial additive character ψ, the number of solutions can be written as $q^{-m} \sum_{y \in \mathbb{F}_q^m} \sum_{x \in \mathbb{F}_q^n} \psi\Big(\sum_{i=1}^m y_i f_i(x)\Big)$ [18, 13]. Moreover, from algebraic-geometric methods, for an algebraic irreducible variety V in projective space P^n with $\dim V = r$ and $\deg V = d$, one can obtain an estimate of the form $|(\text{number of rational points of } V) - q^r| \le (d-1)(d-2)q^{r-\frac{1}{2}} + \Lambda q^{r-1}$, where Λ is a constant depending on (n, r, d) [12].

For randomly chosen $f_1, \ldots, f_m \in U \subseteq \mathbb{F}_q[x_1, \ldots, x_n]$, the expected number of solutions is q^{n-m}, and if every function $\mathbb{F}_q^n \to \mathbb{F}_q$ can be represented by a polynomial in U, the number of solutions follows $\mathrm{Bin}(q^n, q^{-m})$.

For a single polynomial, Schwartz–Zippel lemma states that for any nonzero $f \in \mathbb{F}_q[x_1, \ldots, x_n]$ and uniformly random $r_1, \ldots, r_n \in \mathbb{F}_q$, $\Pr[f(r_1, \ldots, r_n) = 0] \le \frac{\deg f}{q}$ [16, 19].

3 A Proposal for Estimating the Existence Probability of Solutions to the MQ Problem

In this section, we derive an estimate of the existence probability of solutions to the MQ problem by using inequalities from the inclusion–exclusion principle.

3.1 Inclusion–Exclusion Inequalities and the Proposed Method for Probability Estimation

In the proposed method, we extend the inclusion–exclusion analysis for a single univariate polynomial to MQ systems. The choice of order on $\mathbb{F}_q$ and the induced order $\mathbb{F}_q^n$ is arbitrary, as long as it is fixed throughout the argument. For convenience, we assume that the order on $\mathbb{F}_q^n$ is given by $\boldsymbol{x} < \boldsymbol{y} \iff \exists j \in \{1, \ldots, n\} \quad x_1 = y_1,\ \ldots,\ x_{j-1} = y_{j-1},\ x_j < y_j$.

Definition 3 (Definitions of $Z_{\boldsymbol{x}}$ and S_k). *For a given $\boldsymbol{x} = (x_1, \ldots, x_n) \in \mathbb{F}_q^n$, $k = 1, \ldots, q^n$ let $Z_{\boldsymbol{x}} \subseteq \mathbb{F}_q^{mN}$ and S_k be defined by*

$$Z_{\boldsymbol{x}} = \{\boldsymbol{\theta} \in \mathbb{F}_q^{mN} \mid f^{\boldsymbol{\theta}}(\boldsymbol{x}) = 0\}, \quad S_k = \sum_{\boldsymbol{x}^{(1)} < \cdots < \boldsymbol{x}^{(k)}} \left| Z_{\boldsymbol{x}^{(1)}} \cap \cdots \cap Z_{\boldsymbol{x}^{(k)}} \right|. \tag{2}$$

By the inclusion–exclusion principle, $\left|\bigcup_{\boldsymbol{x}\in\mathbb{F}_q^n} Z_{\boldsymbol{x}}\right| = \sum_{k=1}^{q^n}(-1)^{k+1}S_k$ follows. As an inclusion–exclusion inequality, truncating the sum $\sum_{k=1}^{q^n}(-1)^{k+1}S_k$ after an even number of terms gives a lower bound for $\left|\bigcup_{\boldsymbol{x}\in\mathbb{F}_q^n} Z_{\boldsymbol{x}}\right|$, and truncating it after an odd number of terms gives an upper bound, by the classical Bonferroni inequalities [8]. Therefore,

$$\sum_{k=1}^{K:\,\text{even}} (-1)^{k+1}S_k \le \left|\bigcup_{\boldsymbol{x}\in\mathbb{F}_q^n} Z_{\boldsymbol{x}}\right| \le \sum_{k=1}^{K':\,\text{odd}} (-1)^{k+1}S_k.$$

From the definition of $Z_{\boldsymbol{x}}$, the set $\bigcup_{\boldsymbol{x}\in\mathbb{F}_q^n} Z_{\boldsymbol{x}}$ is the set of coefficients of MQ systems that have at least one solution. Therefore,

$$P_{\text{exist}} = \frac{\left|\bigcup_{\boldsymbol{x}\in\mathbb{F}_q^n} Z_{\boldsymbol{x}}\right|}{\left|\mathbb{F}_q^{mN}\right|} = \frac{\sum_{k=1}^{q^n}(-1)^{k+1}S_k}{q^{mN}}$$

holds. Here, let

$$R_{\text{lower}}^{(K)} = \sum_{k=1}^{K:\,\text{even}} (-1)^{k+1}\frac{S_k}{q^{mN}}, \quad R_{\text{upper}}^{(K')} = \sum_{k=1}^{K':\,\text{odd}} (-1)^{k+1}\frac{S_k}{q^{mN}}. \tag{3}$$

Then, by the inclusion–exclusion inequalities, the existence probability can be evaluated as

$$R_{\text{lower}}^{(K)} \le P_{\text{exist}} \le R_{\text{upper}}^{(K')}.$$

In the case of a single univariate polynomial with $m = n = 1$ discussed in Section 2.2, we were able to compute $S_k = \sum_{\boldsymbol{x}^{(1)}<\cdots<\boldsymbol{x}^{(k)}} |Z_{\boldsymbol{x}^{(1)}} \cap \cdots \cap Z_{\boldsymbol{x}^{(k)}}|$ for any k. However, for general n, m, while S_k can be computed for small k, it becomes challenging as k grows. Therefore, in what follows, we aim to derive the lower bound $R_{\text{lower}}^{(K)}$ and the upper bound $R_{\text{upper}}^{(K')}$ by computing S_k for small k.

3.2 A Lower Bound $R_{\text{lower}}^{(2)}$ and an Upper Bound $R_{\text{upper}}^{(3)}$ for the Existence Probability

In practice, by computing S_1, S_2, S_3 in Definition 3, we derive $R_{\text{lower}}^{(2)}$ and $R_{\text{upper}}^{(3)}$ for the case $m = n$, by taking $K = 2$ and $K' = 3$ in (3).

As preparation for evaluating $|Z_{\boldsymbol{x}^{(1)}} \cap \cdots \cap Z_{\boldsymbol{x}^{(k)}}|$, we define,

$$\Phi_{\boldsymbol{x}} = \left(x_1^2,\, x_1x_2,\, \ldots,\, x_n^2,\, x_1,\, \ldots,\, x_n,\, 1\right) \in \mathbb{F}_q^{1\times N}$$

for $\boldsymbol{x} \in \mathbb{F}_q^n$. Here, the quadratic terms x_ix_j are arranged for $1 \le i \le j \le n$ in lexicographic order with respect to the index pair (i, j). Using $\Phi_{\boldsymbol{x}}$, we can write $f_k(\boldsymbol{x}) = \Phi_{\boldsymbol{x}}\boldsymbol{\theta}^{(k)}$, and so on.

Proposition 1. *$S_1 = \sum_{\boldsymbol{x}} |Z_{\boldsymbol{x}}|$ satisfies $S_1 = q^{mN-m+n}$. In particular, when $m = n$, we have $S_1 = q^{nN}$.*

Proof. Fix $\boldsymbol{x} \in \mathbb{F}_q^n$, and define a linear map from the coefficient space $\mathbb{F}_q^{mN}$ to $\mathbb{F}_q^m$ by $F_1 : \boldsymbol{\theta} \longmapsto \big(f_1(\boldsymbol{x}), \ldots, f_m(\boldsymbol{x})\big)^\top$. In matrix form, F_1 is represented by $A_1 = \operatorname{diag}(\boldsymbol{\Phi}_{\boldsymbol{x}}, \ldots, \boldsymbol{\Phi}_{\boldsymbol{x}}) \in \mathbb{F}_q^{m \times mN}$. Each row $\boldsymbol{\Phi}_{\boldsymbol{x}}$ of A_1 contains the constant term 1, and hence $\operatorname{rank}(A_1) = m$. Since $|Z_{\boldsymbol{x}}|$ equals the number of $\boldsymbol{\theta}$ such that $F_1(\boldsymbol{\theta}) = 0$, the dimension theorem implies $\dim \operatorname{Ker} F_1 = mN - m$, and $|Z_{\boldsymbol{x}}| = q^{mN-m}$. Thus,

$$S_1 = \sum_{\boldsymbol{x} \in \mathbb{F}_q^n} |Z_{\boldsymbol{x}}| = q^n \cdot q^{mN-m} = q^{n+m(N-1)}.$$

In particular, when $m = n$, we obtain $S_1 = q^{nN}$.

Proposition 2. *$S_2 = \sum_{\boldsymbol{x}<\boldsymbol{y}} |Z_{\boldsymbol{x}} \cap Z_{\boldsymbol{y}}|$ satisfies $S_2 = \dfrac{q^{n+m(N-2)}(q^n-1)}{2}$. In particular, when $m = n$, we have $S_2 = \frac{q^{nN}(1-q^{-n})}{2}$.*

Proof. Fix distinct $\boldsymbol{x}, \boldsymbol{y} \in \mathbb{F}_q^n$, and define a linear map from the coefficient space $\mathbb{F}_q^{mN}$ to $\mathbb{F}_q^{2m}$ by $F_2 : \boldsymbol{\theta} \longmapsto \big(f_1(\boldsymbol{x}), f_1(\boldsymbol{y}), \ldots, f_m(\boldsymbol{x}), f_m(\boldsymbol{y})\big)^\top$. In matrix form, F_2 is represented by $A_2 = \operatorname{diag}(B_2, \ldots, B_2) \in \mathbb{F}_q^{2m \times mN}$, $B_2 = \begin{pmatrix} \boldsymbol{\Phi}_{\boldsymbol{x}} \\ \boldsymbol{\Phi}_{\boldsymbol{y}} \end{pmatrix} \in \mathbb{F}_q^{2 \times N}$. Hence, $\operatorname{rank}(A_2) = m \cdot \operatorname{rank}(B_2)$.

Let $\alpha, \beta \in \mathbb{F}_q$ and assume $\alpha\boldsymbol{\Phi}_{\boldsymbol{x}} + \beta\boldsymbol{\Phi}_{\boldsymbol{y}} = 0$. From the constant-term component we obtain $\alpha + \beta = 0$. From the linear-term components we obtain $\alpha(x_i - y_i) = 0$ for all i. Since $\boldsymbol{x} \neq \boldsymbol{y}$, there exists j such that $x_j \neq y_j$, which implies $\alpha = 0$, and hence $\beta = 0$. Then, $\boldsymbol{\Phi}_{\boldsymbol{x}}$ and $\boldsymbol{\Phi}_{\boldsymbol{y}}$ are linearly independent, and thus $\operatorname{rank}(B_2) = 2$. Consequently, $\operatorname{rank}(A_2) = 2m$, and by the dimension theorem $\dim \operatorname{Ker} F_2 = mN - 2m$. Hence, $|Z_{\boldsymbol{x}} \cap Z_{\boldsymbol{y}}| = q^{mN-2m}$. Therefore,

$$S_2 = \sum_{\boldsymbol{x}<\boldsymbol{y}} |Z_{\boldsymbol{x}} \cap Z_{\boldsymbol{y}}| = \binom{q^n}{2} q^{mN-2m} = \frac{q^{n+m(N-2)}(q^n-1)}{2}.$$

In particular, when $m = n$, we obtain $S_2 = \frac{q^{nN}(1-q^{-n})}{2}$.

Proposition 3. *$S_3 = \sum_{\boldsymbol{x}<\boldsymbol{y}<\boldsymbol{z}} |Z_{\boldsymbol{x}} \cap Z_{\boldsymbol{y}} \cap Z_{\boldsymbol{z}}|$ satisfies $S_3 = \frac{q^{n+m(N-3)}(q^n-1)(q^n-2)}{6}$. In particular, when $m = n$, $S_3 = \frac{q^{nN}(1-3q^{-n}+2q^{-2n})}{6}$.*

Proof. Fix distinct $\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z} \in \mathbb{F}_q^n$, and define a linear map $F_3 : \mathbb{F}_q^{mN} \to \mathbb{F}_q^{3m}$ by $\boldsymbol{\theta} \longmapsto \big(f_1(\boldsymbol{x}), f_1(\boldsymbol{y}), f_1(\boldsymbol{z}), \ldots, f_m(\boldsymbol{x}), f_m(\boldsymbol{y}), f_m(\boldsymbol{z})\big)^\top$. In matrix form, F_3 is represented by $A_3 = \operatorname{diag}(B_3, \ldots, B_3) \in \mathbb{F}_q^{3m \times mN}$, $B_3 = \begin{pmatrix} \boldsymbol{\Phi}_{\boldsymbol{x}} \\ \boldsymbol{\Phi}_{\boldsymbol{y}} \\ \boldsymbol{\Phi}_{\boldsymbol{z}} \end{pmatrix} \in \mathbb{F}_q^{3 \times N}$. Hence $\operatorname{rank}(A_3) = m \cdot \operatorname{rank}(B_3)$.

Below, let $\alpha, \beta, \gamma \in \mathbb{F}_q$ and show that if $\alpha\boldsymbol{\Phi}_{\boldsymbol{x}} + \beta\boldsymbol{\Phi}_{\boldsymbol{y}} + \gamma\boldsymbol{\Phi}_{\boldsymbol{z}} = 0$, then $\alpha = \beta = \gamma = 0$.

(i) Consider the case where $(x_1, \ldots, x_n, 1), (y_1, \ldots, y_n, 1), (z_1, \ldots, z_n, 1) \in \mathbb{F}_q^{n+1}$ are linearly independent over $\mathbb{F}_q^{n+1}$. Looking at the constant-term and linear-term components of $\alpha \Phi_{\boldsymbol{x}} + \beta \Phi_{\boldsymbol{y}} + \gamma \Phi_{\boldsymbol{z}} = 0$, it follows that $\alpha = \beta = \gamma = 0$. Hence $\Phi_{\boldsymbol{x}}, \Phi_{\boldsymbol{y}}, \Phi_{\boldsymbol{z}}$ are linearly independent. Since the case distinction in **(i)** exhausts all possibilities when $q = 2$, we assume $q \geq 3$ in what follows.

(ii) Consider the case where $(x_1, \ldots, x_n, 1), (y_1, \ldots, y_n, 1), (z_1, \ldots, z_n, 1) \in \mathbb{F}_q^{n+1}$ are not linearly independent over $\mathbb{F}_q^{n+1}$. $\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z}$ lie on the same line in $\mathbb{F}_q^n$. Thus we can write $\boldsymbol{x} = \tau_x \boldsymbol{v} + \boldsymbol{a}$, $\boldsymbol{y} = \tau_y \boldsymbol{v} + \boldsymbol{a}$, $\boldsymbol{z} = \tau_z \boldsymbol{v} + \boldsymbol{a}$, where $\tau_x, \tau_y, \tau_z \in \mathbb{F}_q$ are pairwise distinct, $\boldsymbol{v} \in \mathbb{F}_q^n \setminus \{0\}$, and $\boldsymbol{a} \in \mathbb{F}_q^n$. For $\alpha \Phi_{\boldsymbol{x}} + \beta \Phi_{\boldsymbol{y}} + \gamma \Phi_{\boldsymbol{z}} = 0$, combining the relation from constant, linear, and quadratic terms, we have $\begin{pmatrix} 1 & 1 & 1 \\ \tau_x & \tau_y & \tau_z \\ \tau_x^2 & \tau_y^2 & \tau_z^2 \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \\ \gamma \end{pmatrix} = 0$. However, $\det \begin{pmatrix} 1 & 1 & 1 \\ \tau_x & \tau_y & \tau_z \\ \tau_x^2 & \tau_y^2 & \tau_z^2 \end{pmatrix} = (\tau_x - \tau_y)(\tau_y - \tau_z)(\tau_z - \tau_x)$, and since τ_x, τ_y, τ_z are pairwise distinct when $\boldsymbol{x} < \boldsymbol{y} < \boldsymbol{z}$, this determinant is nonzero. Then, $\alpha = \beta = \gamma = 0$, and hence $\Phi_{\boldsymbol{x}}, \Phi_{\boldsymbol{y}}, \Phi_{\boldsymbol{z}}$ are linearly independent.

From the above, in both **(i)** and **(ii)** we have $\operatorname{rank}(B_3) = 3$, and hence $\operatorname{rank}(A_3) = 3m$. Therefore, by the dimension theorem, $\dim \operatorname{Ker} F_3 = mN - 3m$, and thus $|Z_{\boldsymbol{x}} \cap Z_{\boldsymbol{y}} \cap Z_{\boldsymbol{z}}| = q^{mN-3m}$. Consequently,

$$S_3 = \sum_{\boldsymbol{x}<\boldsymbol{y}<\boldsymbol{z}} |Z_{\boldsymbol{x}} \cap Z_{\boldsymbol{y}} \cap Z_{\boldsymbol{z}}| = \binom{q^n}{3} q^{mN-3m} = \frac{q^{n+m(N-3)}(q^n-1)(q^n-2)}{6}.$$

In particular, when $m = n$, we obtain $S_3 = \frac{q^{nN}(1-3q^{-n}+2q^{-2n})}{6}$.

When $m = n$, Propositions 1, 2, and 3 yield the following lower and upper bounds $R_{\text{lower}}^{(2)}$ and $R_{\text{upper}}^{(3)}$ for the existence probability:

$$R_{\text{lower}}^{(2)} = \sum_{k=1}^{2} (-1)^{k+1} \frac{S_k}{q^{mN}} = \frac{1}{2}\left(1 + \frac{1}{q^n}\right),$$

$$R_{\text{upper}}^{(3)} = \sum_{k=1}^{3} (-1)^{k+1} \frac{S_k}{q^{mN}} = \frac{2}{3}\left(1 + \frac{1}{2q^{2n}}\right).$$

We thus obtain the following theorem.

Theorem 1 (Lower and upper bounds on the existence probability for the MQ problem with $m = n$). *When $m = n$, the existence probability P_{exist} of solutions for the* MQ *problem satisfies*

$$\frac{1}{2}\left(1 + \frac{1}{q^n}\right) \leq P_{\text{exist}} \leq \frac{2}{3}\left(1 + \frac{1}{2q^{2n}}\right).$$

Since $\frac{1}{2}\left(1 + \frac{1}{q^n}\right) \geq \frac{1}{2}$ and, for $q \geq 2$ and $n \geq 1$, $\frac{2}{3}\left(1 + \frac{1}{2q^{2n}}\right) \leq \frac{2}{3}\left(1 + \frac{1}{8}\right) = \frac{3}{4}$, the following corollary holds.

Corollary 1. *When $m = n$, the existence probability P_{exist} of solutions for the* MQ *problem satisfies* $\frac{1}{2} \leq P_{\text{exist}} \leq \frac{3}{4}$.

4 Improved Lower Bound $R^{(4)}_{\mathrm{lower}}$ for the Existence Probability

In this section, we compute $R^{(4)}_{\mathrm{lower}}$ when $m = n$, i.e., the quantity in (3) with $K = 4$, by evaluating S_4 in Definition 3.

For $k \geq 4$, in evaluating S_k we must take into account that there exist tuples $\boldsymbol{x}^{(1)}, \ldots, \boldsymbol{x}^{(k)}$ for which a rank drop occurs in $B_k = \begin{pmatrix} \Phi_{\boldsymbol{x}^{(1)}} \\ \vdots \\ \Phi_{\boldsymbol{x}^{(k)}} \end{pmatrix} \in \mathbb{F}_q^{k \times N}$. To study the rank drop of B_k, we first confirm properties satisfied by $\Phi_{\boldsymbol{x}}$ and B_k.

Lemma 1 (Invariance of $\Phi_{\boldsymbol{x}}$ under affine transformations). *Let $T : \mathbb{F}_q^n \to \mathbb{F}_q^n$ be an affine transformation. If $\boldsymbol{x}, \boldsymbol{x}' \in \mathbb{F}_q^n$ satisfy $\boldsymbol{x} = T(\boldsymbol{x}')$, then there exists an invertible matrix $P_T \in \mathbb{F}_q^{N \times N}$ such that $\Phi_{\boldsymbol{x}} = \Phi_{\boldsymbol{x}'} P_T$.*

Proof. An affine transformation T can be written as $\boldsymbol{x} = T(\boldsymbol{x}') = A\boldsymbol{x}' + \boldsymbol{c}$ for a nonsingular matrix $A \in \mathbb{F}_q^{n \times n}$ and a vector $\boldsymbol{c} \in \mathbb{F}_q^n$. Each component of $\Phi_{\boldsymbol{x}}$ can be expressed in terms of A, $\boldsymbol{c}$, and $\boldsymbol{x}'$ as follows:

$$
\begin{aligned}
1 &= 1 \quad \text{(constant term)}, \\
x_i &= \sum_k A_{ik} x'_k + c_i \quad \text{(linear terms)}, \\
x_i x_j &= \sum_{k,\ell} A_{ik} A_{j\ell} x'_k x'_\ell + \sum_s \big(A_{is} c_j + A_{js} c_i\big) x'_s + c_i c_j \quad \text{(quadratic terms)}.
\end{aligned}
$$

By arranging the corresponding coefficients into columns, we can construct a matrix $P_T \in \mathbb{F}_q^{N \times N}$ such that $\Phi_{\boldsymbol{x}} = \Phi_{\boldsymbol{x}'} P_T$.

Moreover, for affine transformations S and T, consider their composition $S \circ T$. Then $\Phi_{S \circ T(\boldsymbol{x})} = \Phi_{T(\boldsymbol{x})} P_S = \Phi_{\boldsymbol{x}} P_T P_S = \Phi_{\boldsymbol{x}} P_{S \circ T}$, and hence $P_T P_S = P_{S \circ T}$. Taking $S = T^{-1}$ yields $P_T P_S = P_T P_{T^{-1}} = P_{T^{-1} \circ T} = P_{I_n} = I_N$, and thus $P_T^{-1} = P_{T^{-1}}$. Therefore, P_T is invertible.

Corollary 2. *Let $T : \mathbb{F}_q^n \to \mathbb{F}_q^n$ be an affine transformation, and suppose that $\boldsymbol{x}_i = T(\boldsymbol{x}'_i)$ holds for $i = 1, \ldots, k$. If $\alpha_i \in \mathbb{F}_q$ and $\sum_{i=1}^k \alpha_i \Phi_{\boldsymbol{x}_i} = 0$, then $\sum_{i=1}^k \alpha_i \Phi_{\boldsymbol{x}'_i} = 0$.*

Proof. By Lemma 1, $\sum_{i=1}^k \alpha_i \Phi_{\boldsymbol{x}_i} = \sum_{i=1}^k \alpha_i \Phi_{\boldsymbol{x}'_i} P_T = \left(\sum_{i=1}^k \alpha_i \Phi_{\boldsymbol{x}'_i}\right) P_T = 0$. Since P_T is invertible, the claim follows.

Corollary 3. *Let $\boldsymbol{x}^{(1)}, \ldots, \boldsymbol{x}^{(k)} \in \mathbb{F}_q^n$ be distinct points. Let $T : \mathbb{F}_q^n \to \mathbb{F}_q^n$ be an affine transformation, and suppose that $\boldsymbol{x}_i = T(\boldsymbol{x}'_i)$ holds for $i = 1, \ldots, k$. If we define*

$$
B_k = \begin{pmatrix} \Phi_{\boldsymbol{x}^{(1)}} \\ \vdots \\ \Phi_{\boldsymbol{x}^{(k)}} \end{pmatrix} \in \mathbb{F}_q^{k \times N}, \quad B'_k = \begin{pmatrix} \Phi_{\boldsymbol{x}^{(1)\prime}} \\ \vdots \\ \Phi_{\boldsymbol{x}^{(k)\prime}} \end{pmatrix} \in \mathbb{F}_q^{k \times N},
$$

then $\mathrm{rank}(B_k) = \mathrm{rank}(B'_k)$.

Proof. By Lemma 1, there exists an invertible matrix P_T such that $B_k = B'_k P_T$. Right multiplication by an invertible matrix only changes a basis of the column space, and hence $\mathrm{rank}(B_k) = \mathrm{rank}(B'_k P_T) = \mathrm{rank}(B'_k)$.

4.1 Derivation of S_4 and improvement of the lower bound

Using the affine invariance derived in the previous subsection, we compute S_4.

Proposition 4. $S_4 = \sum_{\boldsymbol{x}<\boldsymbol{y}<\boldsymbol{z}<\boldsymbol{w}} |Z_{\boldsymbol{x}} \cap Z_{\boldsymbol{y}} \cap Z_{\boldsymbol{z}} \cap Z_{\boldsymbol{w}}|$ *satisfies*

$$S_4 = \left(\binom{q^n}{4} + \binom{q}{4} \frac{q^n - 1}{q - 1} q^{n-1}(q^m - 1) \right) q^{mN-4m}.$$

In particular, when $m = n$, $S_4 = \frac{q^{nN}}{24} \left(1 + \frac{q(q-5)}{q^n} + \frac{-2q^2+10q-1}{q^{2n}} + \frac{q(q-5)}{q^{3n}}\right)$.

Proof. Fix distinct points $\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z}, \boldsymbol{w}$, and define the map from $\mathbb{F}_q^{mN}$ to $\mathbb{F}_q^{4m}$ by $F_4 : \boldsymbol{\theta} \mapsto \big(f_1(\boldsymbol{x}), \ldots, f_1(\boldsymbol{w}), \ldots, f_m(\boldsymbol{x}), \ldots, f_m(\boldsymbol{w})\big)^\top$. The map F_4 can be represented by the matrix $A_4 = \mathrm{diag}(B_4, \ldots, B_4) \in \mathbb{F}_q^{4m \times mN}$, whose block diagonal consists of $B_4 = (\boldsymbol{\Phi}_{\boldsymbol{x}}, \boldsymbol{\Phi}_{\boldsymbol{y}}, \boldsymbol{\Phi}_{\boldsymbol{z}}, \boldsymbol{\Phi}_{\boldsymbol{w}})^\top \in \mathbb{F}_q^{4 \times N}$. Hence, $\mathrm{rank}(A_4) = m \times \mathrm{rank}(B_4)$. Let $\alpha, \beta, \gamma, \delta \in \mathbb{F}_q$ and suppose that $\alpha\boldsymbol{\Phi}_{\boldsymbol{x}} + \beta\boldsymbol{\Phi}_{\boldsymbol{y}} + \gamma\boldsymbol{\Phi}_{\boldsymbol{z}} + \delta\boldsymbol{\Phi}_{\boldsymbol{w}} = 0$.

(i) Let $n \geq 2$. Consider the case where $\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z}, \boldsymbol{w}$ are such that no three of them are collinear in $\mathbb{F}_q^n$. By Corollary 3, we may assume $\boldsymbol{x} = 0$, $\boldsymbol{y} = \boldsymbol{e}_1$, and $\boldsymbol{z} = \boldsymbol{e}_2$. Comparing components in the identity $\alpha\boldsymbol{\Phi}_{\boldsymbol{x}} + \beta\boldsymbol{\Phi}_{\boldsymbol{y}} + \gamma\boldsymbol{\Phi}_{\boldsymbol{z}} + \delta\boldsymbol{\Phi}_{\boldsymbol{w}} = 0$, we first obtain, for the quadratic components, $\beta + \delta w_1 w_1 = 0$, $\gamma + \delta w_2 w_2 = 0$ and $\delta w_i w_j = 0$. Since no three points are collinear, there exist indices $\{i, j\}$ other than $\{1, 1\}$ and $\{2, 2\}$ such that $w_i w_j \neq 0$, and hence $\delta = 0$ follows. Then, $\beta = 0$ and $\gamma = 0$, and from the constant-term component $\alpha + \beta + \gamma + \delta = 0$ we obtain $\alpha = 0$. Thus $\boldsymbol{\Phi}_{\boldsymbol{x}}, \boldsymbol{\Phi}_{\boldsymbol{y}}, \boldsymbol{\Phi}_{\boldsymbol{z}}, \boldsymbol{\Phi}_{\boldsymbol{w}}$ are linearly independent, and hence $\mathrm{rank}(B_4) = 4$. Note that when $q = 2$, any three distinct points are not collinear, so the case distinction is complete with **(i)**. In what follows, we assume $q \geq 3$.

(ii) Let $n \geq 2$. Consider the case where, among $\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z}, \boldsymbol{w}$ in $\mathbb{F}_q^n$ for $n \geq 2$, three points are collinear and the remaining point is not on that line. We may assume without loss of generality that $\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z}$ are collinear. By Corollary 3, we may assume $\boldsymbol{x} = \tau_x \boldsymbol{e}_1$, $\boldsymbol{y} = \tau_y \boldsymbol{e}_1$, $\boldsymbol{z} = \tau_z \boldsymbol{e}_1$. Then, under $\alpha\boldsymbol{\Phi}_{\boldsymbol{x}} + \beta\boldsymbol{\Phi}_{\boldsymbol{y}} + \gamma\boldsymbol{\Phi}_{\boldsymbol{z}} + \delta\boldsymbol{\Phi}_{\boldsymbol{w}} = 0$, we have $\alpha\tau_x + \beta\tau_y + \gamma\tau_z + \delta w_1 = 0$ and $\delta w_j = 0$ for $j \geq 2$. Since $\boldsymbol{w}$ is not on the same line as the other three points, there exist indices $j \geq 2$ such that $w_j \neq 0$, and hence $\delta = 0$. Combining the constant-term component $\alpha + \beta + \gamma = 0$ and the quadratic-term component $\alpha\tau_x^2 + \beta\tau_y^2 + \gamma\tau_z^2 = 0$, we obtain $\begin{pmatrix} 1 & 1 & 1 \\ \tau_x & \tau_y & \tau_z \\ \tau_x^2 & \tau_y^2 & \tau_z^2 \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \\ \gamma \end{pmatrix} = 0$, and $\alpha = \beta = \gamma = 0$ follows. Thus $\boldsymbol{\Phi}_{\boldsymbol{x}}, \boldsymbol{\Phi}_{\boldsymbol{y}}, \boldsymbol{\Phi}_{\boldsymbol{z}}, \boldsymbol{\Phi}_{\boldsymbol{w}}$ are linearly independent, and hence $\mathrm{rank}(B_4) = 4$. Note that when $q = 3$, four distinct points cannot all lie on the same line, so the case distinction is complete with **(i)** and **(ii)**. In what follows, we assume $q > 3$.

(iii) Let $n \geq 1$. Consider the case where all four points $\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z}, \boldsymbol{w}$ are collinear in $\mathbb{F}_q^n$. When $n = 1$ we only need to consider this case. By Corollary 3, we may

assume $\boldsymbol{x} = \tau_x \boldsymbol{e}_1$, $\boldsymbol{y} = \tau_y \boldsymbol{e}_1$, $\boldsymbol{z} = \tau_z \boldsymbol{e}_1$, $\boldsymbol{w} = \tau_w \boldsymbol{e}_1$. In this case, the only nonzero column vectors of B_4 are $(\tau_x^2, \tau_y^2, \tau_z^2, \tau_w^2)^\top$, $(\tau_x, \tau_y, \tau_z, \tau_w)^\top$, $(1,1,1,1)^\top$, so $\mathrm{rank}(B_4) \leq 3$. Since the minor determinants are nonzero, we have $\mathrm{rank}(B_4) = 3$.

In cases **(i)** and **(ii)**, by the dimension theorem, we have $\mathrm{rank}(A_4) = 4m$, and thus $\dim \mathrm{Ker}\, F_4 = mN - 4m$. Therefore, $|Z_{\boldsymbol{x}} \cap Z_{\boldsymbol{y}} \cap Z_{\boldsymbol{z}} \cap Z_{\boldsymbol{w}}| = q^{mN-4m}$.

In case **(iii)**, by the dimension theorem, we have $\mathrm{rank}(A_4) = 3m$, and thus $|Z_{\boldsymbol{x}} \cap Z_{\boldsymbol{y}} \cap Z_{\boldsymbol{z}} \cap Z_{\boldsymbol{w}}| = q^{mN-3m}$. As for the number of quadruples yielding case **(iii)**, the number of distinct lines in $\mathbb{F}_q^n$ is $\frac{q^n-1}{q-1} \cdot \frac{q^n}{q}$, and hence the number of tuples $(\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z}, \boldsymbol{w})$ with $\boldsymbol{x} < \boldsymbol{y} < \boldsymbol{z} < \boldsymbol{w}$ lying on the same line is $\binom{q}{4} \frac{q^n-1}{q-1} q^{n-1}$. Therefore,

$$S_4 = \sum |Z_{\boldsymbol{x}} \cap Z_{\boldsymbol{y}} \cap Z_{\boldsymbol{z}} \cap Z_{\boldsymbol{w}}| = \left(\binom{q^n}{4} + \binom{q}{4} \frac{q^n - 1}{q-1} q^{n-1} (q^m - 1) \right) q^{mN-4m}.$$

Note that this formula also holds for $n = 1$ and for$q \leq 3$. Moreover, when $m = n$, S_4 is given by

$$S_4 = \frac{q^{nN}}{24} \left(1 + \frac{q(q-5)}{q^n} + \frac{-2q^2 + 10q - 1}{q^{2n}} + \frac{q(q-5)}{q^{3n}} \right).$$

As seen above, in order to compute S_k for general k, it is necessary to take into account rank drops of B_k. Since this requires understanding the k-tuples of points in $\mathbb{F}_q^n$ for which B_k loses rank, it is not easy to derive S_k in general.

From Propositions 1, 2, 3, and 4, we obtain the lower bound $R^{(4)}_{\mathrm{lower}}$ by evaluating the partial sum $\frac{1}{q^{mN}} (S_1 - S_2 + S_3 - S_4)$.

Theorem 2 (A lower bound on the existence probability for the MQ problem with $m = n$). *When $m = n$, a lower bound $R^{(4)}_{\mathrm{lower}}$ on the existence probability for the* MQ *problem is given by*

$$\frac{5}{8} \left(1 - \frac{q(q-5)}{15q^n} + \frac{(2q^2 - 10q + 9)}{15q^{2n}} - \frac{q(q-5)}{15q^{3n}} \right).$$

Corollary 4 ($R^{(4)}_{\mathrm{lower}}$ improves $R^{(2)}_{\mathrm{lower}}$ for $n \geq 2$). *For $n \geq 2$, for the* MQ *problem with $m = n$, the lower bounds $R^{(2)}_{\mathrm{lower}}$ and $R^{(4)}_{\mathrm{lower}}$ satisfy $R^{(4)}_{\mathrm{lower}} > R^{(2)}_{\mathrm{lower}}$.*

Corollary 5 (Improved constant lower bounds on P_{exist} for $n \geq 2$). *Assume that $m = n$ and $n \geq 2$. Then*

$$P_{\mathrm{exist}} > \frac{7}{12}.$$

Proof. By Theorem 2, $P_{\mathrm{exist}} \geq R^{(4)}_{\mathrm{lower}}$. Hence it suffices to show that $R^{(4)}_{\mathrm{lower}} > \frac{7}{12}$. From the explicit formula for $R^{(4)}_{\mathrm{lower}}$, we obtain

$$24 \left(R^{(4)}_{\mathrm{lower}} - \frac{7}{12} \right) = 1 - \frac{q(q-5)}{q^n} + \frac{2q^2 - 10q + 9}{q^{2n}} - \frac{q(q-5)}{q^{3n}}.$$

Set $E_{q,n} := 1 - \frac{q(q-5)}{q^n} + \frac{2q^2-10q+9}{q^{2n}} - \frac{q(q-5)}{q^{3n}}$. It is enough to prove that $E_{q,n} > 0$.

If $q = 2$ or $q = 3$, then $q(q-5) < 0$ and $2q^2 - 10q + 9 = -3$, so $E_{q,n} = 1 + \frac{q(5-q)}{q^n} - \frac{3}{q^{2n}} + \frac{q(5-q)}{q^{3n}} \geq 1 - \frac{3}{q^{2n}} > 0$. If $q = 4$, then $E_{4,n} = 1 + \frac{4}{4^n} + \frac{1}{4^{2n}} + \frac{4}{4^{3n}} > 0$. If $q = 5$, then $E_{5,n} = 1 + \frac{9}{5^{2n}} > 0$.

Assume now that $q \geq 6$, and put $x = q^{-n}$. Since $n \geq 2$, we have $0 < x \leq q^{-2}$. Define

$$F(x) := 1 - q(q-5)x + (2q^2 - 10q + 9)x^2 - q(q-5)x^3.$$

Then $E_{q,n} = F(q^{-n})$, and $F'(x) = -q(q-5) + 2(2q^2 - 10q + 9)x - 3q(q-5)x^2$. For $0 < x \leq q^{-2}$, we have

$$F'(x) \leq -q(q-5) + \frac{2(2q^2 - 10q + 9)}{q^2} = -q(q-5) + 4 - \frac{20}{q} + \frac{18}{q^2} < 0.$$

Hence F is decreasing on $(0, q^{-2}]$, and therefore,

$$\begin{aligned} E_{q,n} = F(q^{-n}) \geq F(q^{-2}) &= 1 - \frac{q(q-5)}{q^2} + \frac{2q^2 - 10q + 9}{q^4} - \frac{q(q-5)}{q^6} \\ &= \frac{5}{q} + \frac{2q^2 - 10q + 9}{q^4} - \frac{q-5}{q^5} > \frac{5}{q} - \frac{q-5}{q^5} > 0. \end{aligned}$$

Thus $E_{q,n} > 0$ for all $q \geq 6$ as well.

5 On the distribution of the number of solutions of MQ systems

In this section, we investigate properties of the distribution of the number of solutions of MQ systems.

5.1 Expectation and variance of the number of solutions

Using the results on S_1 and S_2 obtained in the previous sections, we can prove the following theorem.

Let $Y(\boldsymbol{\theta})$ be the random variable representing the number of solutions of the MQ system determined by the coefficient vector $\boldsymbol{\theta} \in \Omega$. That is, we define

$$Y(\boldsymbol{\theta}) = \left| \left\{ \boldsymbol{x} \in \mathbb{F}_q^n \;\middle|\; f^{\boldsymbol{\theta}}(\boldsymbol{x}) = 0 \right\} \right|.$$

Theorem 3 (Expectation and variance of the number of solutions). *The expectation* $\mathrm{E}[Y(\boldsymbol{\theta})]$ *and the variance* $\mathrm{Var}[Y(\boldsymbol{\theta})]$ *are given by*

$$\mathrm{E}[Y(\boldsymbol{\theta})] = q^{n-m}, \quad \mathrm{Var}[Y(\boldsymbol{\theta})] = q^{n-m} - q^{n-2m}.$$

In particular, when $m = n$, *we have* $\mathrm{E}[Y(\boldsymbol{\theta})] = 1$ *and* $\mathrm{Var}[Y(\boldsymbol{\theta})] = 1 - \frac{1}{q^n}$.

Proof. For a fixed $\boldsymbol{x} \in \mathbb{F}_q^n$, define $I_{\boldsymbol{x}}^{\boldsymbol{\theta}} = \begin{cases} 1 & (f^{\boldsymbol{\theta}}(\boldsymbol{x}) = 0) \\ 0 & (f^{\boldsymbol{\theta}}(\boldsymbol{x}) \neq 0) \end{cases}$. By the definition of expectation, $\mathrm{E}[Y(\boldsymbol{\theta})] = \sum_{\boldsymbol{\theta}\in\Omega} Y(\boldsymbol{\theta}) \frac{1}{|\Omega|} = \frac{1}{|\Omega|} \sum_{\boldsymbol{\theta}\in\Omega} \sum_{\boldsymbol{x}\in\mathbb{F}_q^n} I_{\boldsymbol{x}}^{\boldsymbol{\theta}}$. By exchanging the order of the finite sums and using that $\sum_{\boldsymbol{\theta}\in\Omega} I_{\boldsymbol{x}}^{\boldsymbol{\theta}} = |Z_{\boldsymbol{x}}| = q^{mN-m}$, which follows from the computation of S_1 in the previous section, we obtain

$$\mathrm{E}[Y(\boldsymbol{\theta})] = \frac{1}{|\Omega|} \sum_{\boldsymbol{x}\in\mathbb{F}_q^n} \sum_{\boldsymbol{\theta}\in\Omega} I_{\boldsymbol{x}}^{\boldsymbol{\theta}} = \frac{1}{q^{mN}} \sum_{\boldsymbol{x}\in\mathbb{F}_q^n} q^{mN-m} = \frac{1}{q^{mN}} q^n q^{mN-m} = q^{n-m}.$$

The variance can also be computed using sums of indicator variables. First,

$$\mathrm{E}[Y(\boldsymbol{\theta})^2] = \sum_{\boldsymbol{\theta}\in\Omega} Y(\boldsymbol{\theta})^2 \frac{1}{|\Omega|} = \frac{1}{|\Omega|} \sum_{\boldsymbol{\theta}\in\Omega} \left(\sum_{\boldsymbol{x}\in\mathbb{F}_q^n} I_{\boldsymbol{x}}^{\boldsymbol{\theta}} + \sum_{\boldsymbol{x}\neq\boldsymbol{y}} I_{\boldsymbol{x}}^{\boldsymbol{\theta}} I_{\boldsymbol{y}}^{\boldsymbol{\theta}} \right),$$

where we used $I_{\boldsymbol{x}}^{\boldsymbol{\theta}} I_{\boldsymbol{x}}^{\boldsymbol{\theta}} = I_{\boldsymbol{x}}^{\boldsymbol{\theta}}$. By exchanging the order of the finite sums and using the computation of S_2 in the previous section, which implies $|Z_{\boldsymbol{x}} \cap Z_{\boldsymbol{y}}| = \sum_{\boldsymbol{\theta}\in\Omega} I_{\boldsymbol{x}}^{\boldsymbol{\theta}} I_{\boldsymbol{y}}^{\boldsymbol{\theta}} = q^{mN-2m}$, we obtain

$$\mathrm{E}[Y(\boldsymbol{\theta})^2] = \frac{1}{|\Omega|} \left(\sum_{\boldsymbol{x}\in\mathbb{F}_q^n} |Z_{\boldsymbol{x}}| + \sum_{\boldsymbol{x}\neq\boldsymbol{y}} |Z_{\boldsymbol{x}} \cap Z_{\boldsymbol{y}}| \right) = q^{n-m} + q^{2(n-m)} - q^{n-2m}.$$

Therefore, $\mathrm{Var}[Y(\boldsymbol{\theta})] = \mathrm{E}[Y(\boldsymbol{\theta})^2] - \mathrm{E}[Y(\boldsymbol{\theta})]^2 = q^{n-m} - q^{n-2m}$.

5.2 On the probability that the solution count equals exactly 1

In this subsection, we study the distribution of the number of solutions to the MQ problem. By deriving a representation in terms of S_k, we obtain upper and lower bounds on the probability that the MQ system has exactly one solution. Throughout this section, we use the convention $\binom{a}{b} = 0$ if $a < 0$ or $a < b$.

Lemma 2 (Representation of the solution-count distribution via S_k). *Fix q and assume $m = n$. Let $\boldsymbol{\theta} \in \mathbb{F}_q^{mN}$ be uniformly random. For $i \in \mathbb{N}$, the probability that the number of solutions satisfies $Y(\boldsymbol{\theta}) = i$ is given by*

$$\Pr[Y(\boldsymbol{\theta}) = i] = \sum_{k=i}^{q^n} \frac{S_k}{q^{mN}} \binom{k}{i} (-1)^{k-i},$$

where $S_k = \sum_{\boldsymbol{x}^{(1)}<\cdots<\boldsymbol{x}^{(k)}} \left| Z_{\boldsymbol{x}^{(1)}} \cap \cdots \cap Z_{\boldsymbol{x}^{(k)}} \right|$.

Proof. Define the probability generating function $g(t) = \mathbb{E}\left[t^{Y(\boldsymbol{\theta})}\right]$. Recall $Y(\boldsymbol{\theta}) = \sum_{\boldsymbol{x}\in\mathbb{F}_q^n} I_{\boldsymbol{x}}^{\boldsymbol{\theta}}$, then $g(t) = \mathbb{E}\left[\prod_{\boldsymbol{x}\in\mathbb{F}_q^n} t^{I_{\boldsymbol{x}}^{\boldsymbol{\theta}}}\right] = \mathbb{E}\left[\prod_{\boldsymbol{x}\in\mathbb{F}_q^n} \left(1 + (t-1) I_{\boldsymbol{x}}^{\boldsymbol{\theta}}\right)\right]$. Therefore,

$$g(t) = \mathbb{E}\left[\sum_{S\subset\mathbb{F}_q^n} (t-1)^{|S|} \prod_{\boldsymbol{x}\in S} I_{\boldsymbol{x}}^{\boldsymbol{\theta}} \right] = \sum_{k=0}^{q^n} (t-1)^k \, \mathbb{E}\left[\sum_{\substack{S\subset\mathbb{F}_q^n \\ |S|=k}} \prod_{\boldsymbol{x}\in S} I_{\boldsymbol{x}}^{\boldsymbol{\theta}} \right].$$

The inner sum counts k-subsets of the solution set, hence $\sum_{\substack{S\subset\mathbb{F}_q^n\\|S|=k}}\prod_{\boldsymbol{x}\in S} I_{\boldsymbol{x}}^{\boldsymbol{\theta}} = \binom{Y(\boldsymbol{\theta})}{k}$. Therefore,

$$g(t)=\sum_{k=0}^{q^n}(t-1)^k\,\mathbb{E}\left[\binom{Y(\boldsymbol{\theta})}{k}\right]=\sum_{i=0}^{q^n}t^i\sum_{k=i}^{q^n}\mathbb{E}\left[\binom{Y(\boldsymbol{\theta})}{k}\right]\binom{k}{i}(-1)^{k-i}.$$

On the other hand, by definition of the probability generating function, $g(t)=\sum_{i=0}^{q^n}\Pr[Y(\boldsymbol{\theta})=i]\,t^i$, so comparing coefficients of t^i yields

$$\Pr[Y(\boldsymbol{\theta})=i]=\sum_{k=i}^{q^n}\mathbb{E}\left[\binom{Y(\boldsymbol{\theta})}{k}\right]\binom{k}{i}(-1)^{k-i}.$$

Since $S_k=\sum_{\boldsymbol{x}_1<\cdots<\boldsymbol{x}_k}\ \sum_{\boldsymbol{\theta}\in\mathbb{F}_q^{mN}}\mathbf{1}\{\boldsymbol{\theta}\in Z_{\boldsymbol{x}_1}\cap\cdots\cap Z_{\boldsymbol{x}_k}\}=\sum_{\boldsymbol{\theta}\in\mathbb{F}_q^{mN}}\binom{Y(\boldsymbol{\theta})}{k}$, we have $\mathbb{E}\left[\binom{Y(\boldsymbol{\theta})}{k}\right]=\frac{S_k}{q^{mN}}$. Substituting this completes the proof.

Lemma 3. *Let $M\in\mathbb{N}$ and $i\in\mathbb{N}$. Then, for $Y:=Y(\boldsymbol{\theta})$,*

$$\sum_{k=i+M+1}^{q^n}\mathbb{E}\left[\binom{Y}{k}\right]\binom{k}{i}(-1)^{k-i}=(-1)^{M+1}\mathbb{E}\left[\binom{Y}{i}\binom{Y-i-1}{M}\right].$$

Proof. By linearity of expectation,

$$\sum_{k=i+M+1}^{q^n}\mathbb{E}\left[\binom{Y}{k}\right]\binom{k}{i}(-1)^{k-i}=\mathbb{E}\left[\sum_{k=i+M+1}^{Y}\binom{Y}{k}\binom{k}{i}(-1)^{k-i}\right].$$

Put $k=i+j$, the inner sum equals $\binom{Y}{i}\sum_{j=M+1}^{Y-i}(-1)^j\binom{Y-i}{j}$. Then we have $\sum_{j=M+1}^{Y-i}(-1)^j\binom{Y-i}{j}=-\sum_{j=0}^{M}(-1)^j\binom{Y-i}{j}$. Using $\sum_{j=0}^{M}(-1)^j\binom{r}{j}=(-1)^M\binom{r-1}{M}$ with $r=Y-i$, the inner sum becomes $(-1)^{M+1}\binom{Y}{i}\binom{Y-i-1}{M}$. Taking expectation yields the claim.

Lemma 4 (Inclusion–exclusion inequalities for the solution-count distribution). *Fix q and choose the coefficient vector $\boldsymbol{\theta}\in\mathbb{F}_q^{mN}$ uniformly at random. For $i\in\mathbb{N}$, let K be even and K' be odd. Then, using S_k, we have*

$$\sum_{k=i}^{i+K'}\frac{S_k}{q^{mN}}\binom{k}{i}(-1)^{k-i}\le\Pr[Y(\boldsymbol{\theta})=i]\le\sum_{k=i}^{i+K}\frac{S_k}{q^{mN}}\binom{k}{i}(-1)^{k-i}.$$

Proof. By Lemma 2 and Lemma 3, for $M\in\mathbb{N}_0$,

$$\begin{aligned}\Pr[Y(\boldsymbol{\theta})=i]-\sum_{k=i}^{i+M}\frac{S_k}{q^{mN}}\binom{k}{i}(-1)^{k-i}&=\sum_{k=i+M+1}^{q^n}\mathbb{E}\left[\binom{Y}{k}\right]\binom{k}{i}(-1)^{k-i}\\&=(-1)^{M+1}\mathbb{E}\left[\binom{Y}{i}\binom{Y-i-1}{M}\right].\end{aligned}$$

Hence, if M is even ($M = K$), then $\Pr[Y(\boldsymbol{\theta}) = i] - \sum_{k=i}^{i+K} \frac{S_k}{q^{mN}} \binom{k}{i} (-1)^{k-i} \leq 0$, and if M is odd ($M = K'$), then $\Pr[Y(\boldsymbol{\theta}) = i] - \sum_{k=i}^{i+K'} \frac{S_k}{q^{mN}} \binom{k}{i} (-1)^{k-i} \geq 0$. This proves the desired inequalities.

Using the above lemmas, we can derive the following bounds on the probability that the MQ system has exactly one solution.

Theorem 4. *Fix q and assume $m = n$. Choose the coefficient vector $\boldsymbol{\theta} \in \mathbb{F}_q^{mN}$ uniformly at random. Then the probability that the number of solutions satisfies $Y(\boldsymbol{\theta}) = 1$ obeys*

$$\frac{1}{3}\left(1 - \frac{q^2 - 5q + 3}{2q^n} + \frac{2q^2 - 10q + 7}{2q^{2n}} - \frac{q(q-5)}{2q^{3n}}\right) \leq \Pr[Y(\boldsymbol{\theta}) = 1] \leq \frac{1}{2}\left(1 - \frac{1}{q^n} + \frac{2}{q^{2n}}\right).$$

Proof. By the inequalities in Lemma 4,

$$\frac{1}{q^{mN}}(S_1 - 2S_2 + 3S_3 - 4S_4) \leq \Pr[Y(\boldsymbol{\theta}) = 1] \leq \frac{1}{q^{mN}}(S_1 - 2S_2 + 3S_3).$$

When $m = n$, we use $S_1 = q^{nN}$, $S_2 = \frac{q^{nN}(1-q^{-n})}{2}$, $S_3 = \frac{q^{nN}(1-3q^{-n}+2q^{-2n})}{6}$, and $S_4 = \frac{q^{nN}}{24}\left(1 + \frac{q(q-5)}{q^n} + \frac{-2q^2+10q-1}{q^{2n}} + \frac{q(q-5)}{q^{3n}}\right)$. Substituting the expressions, we obtain the desired expression.

6 On the existence probability for MQ problems with $m \neq n$

In this section, we evaluate the existence probability for MQ systems with $m \neq n$. For this evaluation, we use the quantities S_k obtained in Propositions 1, 2, and 3, as well as the expectation and variance of the solution count.

6.1 Existence probability for overdetermined MQ systems ($m > n$)

Theorem 5. *Consider an overdetermined* MQ *instance with $m > n$. Let $k = m - n$. Then the existence probability P_{exist} satisfies*

$$\frac{3}{4}q^{-k} \leq P_{\text{exist}} \leq q^{-k}.$$

Proof. By Proposition 1, 2, we have $S_1 = q^{mN-m+n}$ and $S_2 = \frac{q^{n+m(N-2)}(q^n-1)}{2}$. Hence,

$$P_{\text{exist}} \geq R^{(2)}_{\text{lower}} = \frac{1}{q^{mN}}(S_1 - S_2) = q^{n-m} - \frac{q^{n-2m}(q^n-1)}{2} \geq q^{-k}\left(1 - \frac{q^{-k}}{2}\right)$$

Since $m > n$ implies $k > 0$, we have $q^{-k} \leq 2^{-1}$, and thus $q^{-k}\left(1 - \frac{q^{-k}}{2}\right) \geq q^{-k}\left(1 - \frac{2^{-1}}{2}\right)$. Therefore, $P_{\text{exist}} \geq q^{-k}\left(1 - \frac{q^{-k}}{2}\right) \geq q^{-k}\left(1 - \frac{1}{4}\right) = \frac{3}{4}q^{-k}$.

Let Y denote the number of common zeros of the given MQ system over $\mathbb{F}_q^n$. By Theorem 3, $\mathrm{E}[Y] = q^{n-m} = q^{-k}$. Since $P_{\text{exist}} = \Pr[Y \geq 1]$, Markov's inequality yields $P_{\text{exist}} = \Pr[Y \geq 1] \leq \mathrm{E}[Y] = q^{-k}$. This proves the claim.

6.2 Existence probability for underdetermined MQ systems ($n > m$)

Theorem 6. *Consider an underdetermined* MQ *instance with $m < n$. Let $k = m - n$. Then the existence probability P_{exist} satisfies*

$$P_{\text{exist}} \geq \frac{1}{1 + q^k - q^{-n}}.$$

In particular,

$$P_{\text{exist}} \geq \frac{1}{1 + q^k}.$$

Proof. In the underdetermined case $m < n$, we have $k < 0$. By Theorem 3, the expectation and variance of the solution count $Y(\boldsymbol{\theta})$ satisfy $\mathbb{E}[Y(\boldsymbol{\theta})] = q^{n-m}$ and $\mathrm{Var}[Y(\boldsymbol{\theta})] = q^{n-m} - q^{n-2m}$. Using the Cauchy–Schwarz inequality,

$$(\mathbb{E}[Y])^2 = \left(\mathbb{E}\left[Y \cdot \mathbf{1}_{Y>0}\right]\right)^2 \leq \mathbb{E}[Y^2] \Pr[Y > 0],$$

we obtain

$$\Pr[Y > 0] \geq \frac{(\mathbb{E}[Y])^2}{\mathrm{Var}[Y] + (\mathbb{E}[Y])^2}.$$

Therefore,

$$P_{\text{exist}} = \Pr[Y > 0] \geq \frac{(q^{n-m})^2}{q^{n-m} - q^{n-2m} + (q^{n-m})^2} = \frac{1}{1 + q^k - q^{-n}}.$$

In particular, $\frac{1}{1+q^k-q^{-n}} \geq \frac{1}{1+q^k}$.

7 Applications

In this section, we illustrate how the solution existence probability of the MQ problem informs the evaluation of cryptographic attack methods.

As an efficient attack method for an underdetermined MQ system with n variables and m polynomials, Hashimoto's algorithm [9] is known. Overall, Hashimoto's algorithm consists of Steps (1)–(5), and Steps (3)–(5) are repeated until a solution is obtained.

Let a, k be nonnegative integers satisfying $a + k \leq m$, and partition the n variables into the following triple (X, Y, Z):

$$\overbrace{x_1, \ldots, x_{m-a-k+1}}^{X}, \overbrace{x_{m-a-k+2}, \ldots, x_{m-k}}^{Y}, \overbrace{x_{m-k+1}, \ldots, x_n}^{Z}.$$

(1), (2) Apply an appropriate linear transformation to the given MQ system.
(3) For Z, choose a candidate Z from the solution space of the system of linear equations obtained by the transformation, and substitute it.
(4) For Y, solve an MQ system with $a - 1$ variables and $a - 1$ polynomials, and substitute the obtained solution.
(5) For X, solve an overdetermined MQ system with $m - a - k$ variables and $m - a$ polynomials. If no solution is obtained, return to Step (3).

In evaluating such an algorithm, the following assumption is made.

Hypothesis 1 *For an* MQ *instance over* $\mathbb{F}_q$ *consisting of* n *variables and* m *polynomials, when* $n \leq m$*, the solution existence probability* P_{exist} *is assumed to satisfy* $P_{\text{exist}} = q^{n-m}$*. In particular, when* $m = n$*, it is assumed that* $P_{\text{exist}} = 1$*.*

Therefore, for Hashimoto's algorithm, it is evaluated that a solution is obtained in Step (4) with probability 1, and a solution is obtained in Step (5) with probability q^{-k}.

However, according to the theoretical estimates obtained in this work, when $n < m$, the solution existence probability P_{exist} satisfies $\frac{3}{4}q^{n-m} \leq P_{\text{exist}} \leq q^{n-m}$ by Theorem 5, and when $m = n$, we have $\frac{7}{12} \leq P_{\text{exist}} \leq \frac{3}{4} < 1$ by the Corollary 1 and Corollary 5. Hence, for Hashimoto's algorithm, if each MQ system solved in each step can be regarded as randomly given, then Step (4) yields a solution with probability between $\frac{7}{12}$ and $\frac{3}{4}$, and Step (5) yields a solution with probability between $\frac{3}{4}q^{-k}$ and q^{-k}. We note that the above discussion concerns the interpretation of Step (4) in which one solution of the $n = m$ MQ subsystem is computed and substituted into Step (5).

8 Conclusion

In this paper, we investigated the existence probability of solutions to the MQ problem, which underpins the security of multivariate public-key cryptography. By evaluating the image space of a linear map from the coefficient space to the polynomials defining an MQ system and applying the inclusion–exclusion principle, we derived explicit upper and lower bounds on the existence probability for MQ systems.

As future work, it is desirable to determine an explicit value of the existence probability for arbitrary m and n. In this study, we derived only upper and lower bounds on the existence probability. To compute the existence probability via the inclusion–exclusion principle, it is necessary to explicitly evaluate S_k for arbitrary k. However, in this study we were only able to provide explicit evaluations for $k = 1, 2, 3, 4$. The difficulty lies in analyzing the rank drop of the matrix B_k that characterizes S_k for general k, and this remains an important topic for future investigation.

Acknowledgments. This work was supported by JST K Program Grant Number JPMJKP24U2, Japan.

References

1. Ax, J.: Zeroes of polynomials over finite fields. American Journal of Mathematics **86**(2), 255–261 (1964)
2. Bettale, L., Faugere, J.C., Perret, L.: Hybrid approach for solving multivariate systems over finite fields. Journal of Mathematical Cryptology **3**(3), 177–197 (2009)
3. Beullens, W.: Mayo: Practical post-quantum signatures from oil-and-vinegar maps. In: Selected Areas in Cryptography (SAC 2021). pp. 355–376 (2021)

4. Chevalley, C.: Démonstration d'une hypothèse de M. Artin. Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg **11**, 73–75 (1935)
5. Faugère, J.C.: A new efficient algorithm for computing Gröbner bases without reduction to zero (F5). In: Proceedings of the International Symposium on Symbolic and Algebraic Computation (ISSAC '02). pp. 75–83 (2002)
6. Furue, H., Ikematsu, Y., Kiyomura, Y., Takagi, T.: A new variant of unbalanced oil and vinegar using quotient ring: QR-UOV. In: Advances in Cryptology – ASIACRYPT 2021, Part IV. pp. 187–217 (2021)
7. Fusco, G., Bach, E.: Phase transition of multivariate polynomial systems. In: Theory and Applications of Models of Computation (TAMC 2007). Lecture Notes in Computer Science, vol. 4484, pp. 79–90. Springer (2007)
8. Galambos, J., Simonelli, I.: Bonferroni-Type Inequalities with Applications. Springer, New York (1996)
9. Hashimoto, Y.: An improvement of algorithms to solve under-defined systems of multivariate quadratic equations. JSIAM Letters **15**, 53–56 (2023)
10. Katz, N.M.: On a theorem of Ax. American Journal of Mathematics **93**(2), 485–499 (1971)
11. Kipnis, A., Patarin, J., Goubin, L.: Unbalanced oil and vinegar signature schemes. In: Advances in Cryptology – EUROCRYPT '99. pp. 206–222 (1999)
12. Lang, S., Weil, A.: Number of points of varieties in finite fields. American Journal of Mathematics **76**(4), 819–827 (1954)
13. Leep, D.B., Schueller, L.M.: Zeros of a pair of quadratic forms defined over a finite field. Finite Fields and Their Applications **5**(2), 157–176 (1999)
14. Leont'ev, V.K.: Roots of random polynomials over a finite field. Mathematical Notes **80**, 300–304 (2006)
15. Matsumoto, T., Imai, H.: Public quadratic polynomial-tuples for efficient signature-verification and message-encryption. In: Advances in Cryptology – EUROCRYPT '88. pp. 419–453 (1988)
16. Schwartz, J.T.: Fast probabilistic algorithms for verification of polynomial identities. Journal of the ACM **27**(4), 701–717 (1980)
17. Warning, E.: Bemerkung zur vorstehenden arbeit von Herrn Chevalley. Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg **11**, 76–83 (1935)
18. Weil, A.: Numbers of solutions of equations in finite fields. Bulletin of the American Mathematical Society **55**(5), 497–508 (1949)
19. Zippel, R.: Probabilistic algorithms for sparse polynomials. In: Proceedings of the International Symposium on Symbolic and Algebraic Manipulation (EUROSAM '79). pp. 216–226 (1979)