Minor improvements of algorithm to solve under-defined systems of multivariate quadratic equations

Yasufumi Hashimoto *

Abstract

There have been several works on solving an under-defined system of multivariate quadratic equations over a finite field, e.g. Kipnis et al. (Eurocrypt'98), Courtois et al. (PKC'02), Tomae-Wolf (PKC'12), Miura et al. (PQC'13), Cheng et al. (PQC'14) and Furue et al. (PQC'21). This paper presents two minor improvements of Furue's aproach.

Keywords. under-defined multivariate quadratic equations

1 Introduction

Solving a system of multivariate non-linear polynomial equations over a finite field is known to be a hard problem [5, 3]. Until now, there have been several algorithms to solve an under-defined system of multivariate quadratic equations over a finite field, i.e. the number n of variables is larger than the number m of equations. For example, the algorithms of Kipnis et al. [7], Courtois et al. [2], Miura et al. [6] and Cheng et al. [1] solve it in polynomial time but n must be much larger than m, and the algorithms of Tomae-Wolf [8], Cheng et al. [1] and Furue et al. [4] do not require too much larger n but do not solve in polynomial time.

Table 1: Algorithms of solving under-defined multivariate quadratic equations

	q	n	Complexity
Kipnis et al. [7]	even	$m(m+1)$	polyn.
Courtois et al. [2]	any	$2^{m/7}(m+1)$	polyn.
Miura et al. [6]	even	$\frac{1}{2}m(m+1)$	polyn.
Cheng et al. [1]	any	$\frac{1}{2}m(m+1)$	polyn.
Tomae-Wolf [8]	even	$m(m-a+1)$	$\mathrm{MQ}(q,a,a)$
Cheng et al. [1]	any	$\frac{1}{2}m(m+1)-\frac{1}{2}a(a-1)$	$\mathrm{MQ}(q,a,a)$
Furue et al. [4]	even	$(m-a)(m-k)+m$	$q^k\cdot\mathrm{MQ}(q,a-k,a)$
Alg. 1 ($a\gg\frac{m}{2}$)	any	$(m-a+1)(m-k)$	$q^k\cdot\mathrm{MQ}(q,a-k,a)$
Alg. 2 ($a\gg\frac{m}{2}$)	any	$(a-k)(m-a)+m$	$q^k\cdot\mathrm{MQ}(q,a-k,a)$

In the present paper, we propose two minor improvements of the most recent Furue's approach at PQCrypto 2021 [4]. Table 1 summarizes the contributions of the previous and the present works. In this Table 1, "q" is the order of the finite field, "n" is the least of required

*Department of Mathematical Science, University of the Ryukyus, hashimoto@math.u-ryukyu.ac.jp

n and "Complexity" is the complexity of the corresponding algorithm, where MQ(q, a, b) is the complexity of solving b quadratic equations of a variables over a finite field of order q. We also summarize the required n in Table 2 when a is close to m.

Table 2: Comparison of required n

a	TW [8]	C. [1]	F. [4]	Alg. 1	Alg.2
$m-1$	$2m$	$2m-1$	$2m-k$	$2m-2k$	$2m-k-1$
$m-2$	$3m$	$3m-3$	$3m-2k$	$3m-3k$	$3m-2k-4$
$m-3$	$4m$	$4m-6$	$4m-3k$	$4m-4k$	$4m-3k-9$
$m-4$	$5m$	$5m-10$	$5m-4k$	$5m-5k$	$5m-4k-16$
$m-5$	$6m$	$6m-15$	$6m-5k$	$6m-6k$	$6m-5k-25$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$

2 Furue's approach

We first describe Furue's approach [4].

Let $n, m, k, a \geq 1$ be integers, q a power of 2, $\mathbf{F}_q$ a finite field of order q and $f_1(\mathbf{x}), \ldots, f_m(\mathbf{x})$ quadratic polynomials of n variables $\mathbf{x} = {}^t(x_1, \ldots, x_n)$. Furue's approach is as follows.

Step 1. Find an $(n-m+k) \times (m-k)$ matrix M such that

$$\begin{aligned}\bar{f}_l(\mathbf{x}) :=& f_l\left(\begin{pmatrix} I_{m-k} & \\ M & I_{n-m+k}\end{pmatrix}\mathbf{x}\right)\\ =& K_l(x_1^2, \ldots, x_{m-k}^2) + \sum_{i=1}^{m-k} x_i \cdot L_{li}(x_{m-k+1}, \ldots, x_n) + Q_l(x_{m-k+1}, \ldots, x_n)\\ =& {}^t\mathbf{x}\left(\begin{array}{ccc|c} * & & & \\ & \ddots & & * \\ & & * & \\ \hline & * & & *_{n-m+k}\end{array}\right)\mathbf{x} + (\text{linear form of } \mathbf{x})\end{aligned}$$

for $1 \leq l \leq m-a$, where K_l, L_{li} are linear forms and Q_l is a quadratic form.

Step 2. Choose $u_1, \ldots, u_{n-m+k} \in \mathbf{F}_q$ such that

$$L_{li}(u_1, \ldots, u_{n-m+k}) = 0$$

for $1 \leq l \leq m-a$ and $1 \leq i \leq m-k$.

Step 3. Solve the system

$$\left\{\bar{f}_l(x_1, \ldots, x_{m-k}, u_1, \ldots, u_{n-m+k}) = 0\right\}_{1 \leq l \leq m} \tag{1}$$

of m equations of $m-k$ variables $(x_1, \ldots, x_{m-k})$. If there exists a solution of (1), output $\begin{pmatrix} I & \\ -M & I\end{pmatrix}{}^t(x_1, \ldots, x_{m-k}, u_1, \ldots, u_{n-m+k})$ as a solution of $\{f_l(\mathbf{x}) = 0\}_{1 \leq l \leq m}$. If not, go back to Step 2 and choose another $(u_1, \ldots, u_{n-m+k})$.

Condition of (n, m) and Complexity. In Step 1, one solves the systems of at most $(m-k-1)(m-a)$ linear equations of $n-m+k$ variables. Step 2 is to solve $(m-k)(m-a)$ linear equations of $n-m+k$ variables. In Step 3, one solves the system of $m-a$ quadratic equations in the forms

$$K_l(x_1^2, \ldots, x_{m-k}^2) = (\text{const.}) \tag{2}$$

and a random quadratic equations of $m-k$ variables. When q is even, (2) is equivalent to a linear equation of $x_1, \ldots, x_{m-k}$ (see e.g. [8, 4]). Then solving (1) is reduced to solving the system of a quadratic equations of $a-k$ variables. Remark that, since the probability that (1) has a solution is considered to be about q^{-k}, there should be additional k variables in Step 2. We thus conclude that $n \geq m + (m-k)(m-a)$ is required in this approach and the complexity is $q^k \cdot \mathrm{MQ}(q, a-k, a)$.

3 New algorithms

We propose two minor improvements of Furue's approach given in the previous section. Remark that q does not have to be even.

3.1 Algorithm 1

Step 1. Find an $(n-m+k) \times (m-k)$ matrix M such that

$$\begin{aligned}
\bar{f}_l(\mathbf{x}) :=& f_l\left(\begin{pmatrix} I_{m-k} & \\ M & I_{n-m+k} \end{pmatrix} \mathbf{x}\right) \\
=& \sum_{i=1}^{m-k} x_i \cdot L_{li}(x_{m-k+1}, \ldots, x_n) + Q_l(x_{m-k+1}, \ldots, x_n) \\
=& {}^t\mathbf{x} \left(\begin{array}{c|c} 0_{m-k} & * \\ \hline * & *_{n-m+k} \end{array}\right) \mathbf{x} + (\text{linear form of } \mathbf{x})
\end{aligned}$$

for $1 \leq l \leq m-a$, where L_{li} is a linear form and Q_l is a quadratic form.

Step 2. Choose $u_1, \ldots, u_{n-m+k} \in \mathbf{F}_q$ arbitrary.

Step 3. Solve the system

$$\left\{\bar{f}_l(x_1, \ldots, x_{m-k}, u_1, \ldots, u_{n-m+k}) = 0\right\}_{1 \leq l \leq m} \tag{3}$$

of m equations of $m-k$ variables $(x_1, \ldots, x_{m-k})$. If there exists a solution of (3), output $\begin{pmatrix} I & \\ -M & I \end{pmatrix} {}^t(x_1, \ldots, x_{m-k}, u_1, \ldots, u_{n-m+k})$ as a solution of $\{f_l(\mathbf{x}) = 0\}_{1 \leq l \leq m}$. If not, go back to Step 2 and choose another $(u_1, \ldots, u_{n-m+k})$.

Condition of (n, m) and Complexity. In Step 1, one solves the systems of at most $(m-k-1)(m-a)$ linear equations and $m-a$ quadratic equations of $n-m+k$ variables. Step 2 is to choose parameters arbitrary. In Step 3, one solves the system of $m-a$ linear equations and a random quadratic equations of $m-k$ variables. Since the probability that (3) has a solution is considered to be about q^{-k}, we can conclude that we need $n \geq (m-k)(m-a+1)$ and the complexity is $\mathrm{MQ}(q, m-a, m-a) + q^k \cdot \mathrm{MQ}(q, a-k, a)$.

3.2 Algorithm 2

Step 1. Find an $(n-m+k)\times(m-k)$ matrix M such that

$$\begin{aligned}\bar{f}_l(\mathbf{x}) :=& f_l\left(\begin{pmatrix} I_{m-k} & \\ M & I_{n-m+k}\end{pmatrix}\mathbf{x}\right)\\ =& P_l(x_{a-k+1},\dots,x_{m-k})+\sum_{i=1}^{m-k} x_i\cdot L_{li}(x_{m-k+1},\dots,x_n)+Q_l(x_{m-k+1},\dots,x_n)\\ =& {}^t\mathbf{x}\left(\begin{array}{cc|c} 0_{a-k} & 0 & * \\ 0 & *_{m-a} & * \\ \hline * & * & *_{n-m+k}\end{array}\right)\mathbf{x} + (\text{linear form of } \mathbf{x})\end{aligned}$$

for $1\le l\le m-a$, where L_{li} is a linear forms and P_l, Q_l are quadratic forms.
Step 2. Choose $u_1,\dots,u_{n-m+k}\in\mathbf{F}_q$ such that

$$L_{li}(u_1,\dots,u_{n-m+k})=0$$

for $1\le l\le m-a$ and $1\le i\le a-k$.
Step 3. Solve the system

$$\left\{\bar{f}_l(x_1,\dots,x_{m-k},u_1,\dots,u_{n-m+k})=0\right\}_{1\le l\le m} \tag{4}$$

of m equations of $m-k$ variables $(x_1,\dots,x_{m-k})$. If there exists a solution of (4), output $\begin{pmatrix} I & \\ -M & I\end{pmatrix}{}^t(x_1,\dots,x_{m-k},u_1,\dots,u_{n-m+k})$ as a solution of $\{f_l(\mathbf{x})=0\}_{1\le l\le m}$. If not, go back to Step 2 and choose another $(u_1,\dots,u_{n-m+k})$.

Condition of (n,m) and Complexity. In Step 1, one solves the systems of at most $(a-k-1)(m-a)$ linear equations and $m-a$ quadratic equations of $n-m+k$ variables, and the systems of $(a-k)(m-a)$ linear equations of $n-m+k$ variables. Step 2 is to solve $(a-k)(m-a)$ linear equations of $n-m+k$ variables. In Step 3, one solves the system of $m-a$ quadratic equations of $m-a$ variables $x_{a-k+1},\dots,x_{m-k}$ and a random quadratic equations of $m-k$ variables $x_1,\dots,x_{m-k}$. Since the probability that (4) has a solution is considered to be about q^{-k}, there should be additional k variables in Step 2. We thus conclude that we need $n\ge m+(a-k)(m-a)$ and the complexity is $\mathrm{MQ}(q,m-a,m-a)+q^k\cdot\mathrm{MQ}(q,a-k,a)$.

Acknowledgment. The author was supported by JST Crest no.JPMJCR14D6 and JSPS Grant-in-Aid for Scientific Research (C) no.17K05181.

References

[1] C.M. Cheng, Y. Hashimoto, H. Miura and T. Takagi, A polynomial-time algorithm for solving a class of underdetermined multivariate quadratic equations over fields of odd characteristics, PQCrypto'14, LNCS **8772** (2014), pp.40–58.

[2] N. Courtois, L. Goubin, W. Meier, J.-D. Tacier, Solving underdefined systems of multivariate quadratic equations, PKC'02, LNCS **2274** (2002), pp.211–227.

[3] A.S. Fraenkel, Y. Yesha, Complexity of problems in games, graphs and algebraic equations. Discrete Appl. Math. **1** (1979), pp.15–30.

[4] H. Furue, S. Nakamura, T. Takagi, Improving Thomae-Wolf algorithm for solving underdetermined multivariate quadratic polynomial problem, PQC'21, LNCS **12841** (2021), pp.65–78.

[5] M.R. Garey, D.S. Johnson, Computers and Intractability, A Guide to the Theory of NP-completeness, W.H. Freeman, 1979.

[6] H. Miura, Y. Hashimoto, T. Takagi, Extended algorithm for solving underdefined multivariate quadratic equations, PQCryoto'13, LNCS **7932** (2013), pp.118–135.

[7] A. Kipnis, J. Patarin, L. Goubin, Unbalanced oil and vinegar signature schemes, Eurocrypt'99, LNCS **1592** (1999), pp.206–222, extended in `http://www.goubin.fr/papers/OILLONG.PDF`, 2003.

[8] E. Thomae, C. Wolf, Solving underdetermined systems of multivariate quadratic equations revisited, PKC'12, LNCS **7293** (2012), pp.156–171.