SCIS 2022 2022 Symposium on
Cryptography and Information Security
Osaka, Japan & Online, Jan. 18 – 21, 2022
The Institute of Electronics,
Information and Communication Engineers

A New Efficient Variant of the XL Algorithm Using the Arithmetic over Polynomial Matrices

Hiroki Furue * Momonari Kudo *

Keywords: $\mathcal{MQ}$ problem, MPKC, XL, hybrid approach, Macaulay matrices

Abstract

Solving a system over a finite field is one of the most major problems in the field of computer science. Especially, the problem of solving a quadratic system (the $\mathcal{MQ}$ problem) is used to construct various cryptographic systems such as Rainbow and GeMSS. Given a quadratic polynomial system $\mathcal{F}$ in n variables $\mathbf{x}$ over a finite field $\mathbb{F}_q$ of q elements, the purpose of this research is to find a solution to $\mathcal{F}(\mathbf{x}) = \mathbf{0} \in \mathbb{F}_q^m$.

One of major strategies to solve the $\mathcal{MQ}$ problem is linearization, and the most basic linearization-based algorithm is the *XL algorithm* proposed by Courtois et al. [2]. XL finds a solution by generating a Macaulay matrix at certain degree and performing Gaussian elimination on the matrix. Furthermore, Yang et al. [5] analyzed a variant of the XL algorithm called *Wiedemann XL (WXL)*, which adopts Wiedemann's algorithm [3] instead of the Gaussian elimination in the XL framework.

The hybrid approach [1, 4] is an approach applying XL efficiently, which mixes exhaustive search and an $\mathcal{MQ}$ solver. In the hybrid approach, k variables are fixed, and the remaining system in $n-k$ variables are solved by an $\mathcal{MQ}$ solver. These processes are iterated until a solution is found. In the case of $n \approx m$, the hybrid approach may be effective, since the gain obtained by working on systems with less variables may overcome the loss due to the exhaustive search on the fixed variables. In this paper, we call the hybrid approach with XL (resp. WXL) *h-XL* (resp. *h-WXL*).

In this study, we propose a new variant of the XL algorithm, which we call the *polynomial XL* (PXL). PXL is constructed by improving h-XL. For the $\mathcal{MQ}$ system $\mathcal{F}$ of m equations in n variables $\mathbf{x} = (x_1, \ldots, x_n)$ over $\mathbb{F}_q$, PXL first sets the number k of guessed variables as in the hybrid approach. We then regard the given system as a system in $n-k$ variables $x_{k+1}, \ldots, x_n$, whose coefficients belong to the polynomial ring $\mathbb{F}_q[x_1, \ldots, x_k]$, and generate the Macaulay matrix over $\mathbb{F}_q[x_1, \ldots, x_k]$. The main idea of PXL is to partly perform Gaussian elimination on the matrix over the polynomial ring before fixing the k variables and complete the elimination after fixing. By doing so, we can reduce the amount of manipulations for each guessed value compared with h-XL. This enables us to solve the system more efficiently for some parameters.

We also discuss the estimation of the time and space complexities and compare them with those of h-XL and h-WXL. Comparing the time complexities, we show that the proposed algorithm is more efficient in the case of $n \approx m$. For example, on the system over $\mathbb{F}_{2^8}$ with $n = m = 80$, the number of manipulations in $\mathbb{F}_q$ required by h-XL, h-WXL, and PXL is estimated as 2^{252}, 2^{234}, and 2^{220}, respectively. On the other hand, in terms of the space complexity, the proposed algorithm is not well compared to WXL. Therefore, the relationship between PXL and WXL can be seen as a trade-off between time and memory.

References

[1] Bettale, L., Faugère, J.-C., Perret, L., "Hybrid approach for solving multivariate systems over finite fields," J. Math. Cryptol. **3**, pp. 177–197 (2009)

[2] Courtois, N., Klimov, A., Patarin, J., Shamir, A., "Efficient algorithms for solving overdefined systems of multivariate polynomial equations," EUROCRYPT 2000, pp. 392–407 (2000)

[3] Wiedemann, D. H., "Solving sparse linear equations over finite fields," IEEE Trans. Inf. Theor. **32**(1), pp. 54–62 (1986)

[4] Yang, B.-Y., Chen, J.-M., Courtois, N., "On asymptotic security estimates in XL and Gröbner bases-related algebraic cryptanalysis," ICICS 2004, pp. 401–413 (2004)

[5] Yang, B.-Y., Chen, O.C.-H., Bernstein, D.J., Chen, J.-M., "Analysis of QUAD," FSE 2007, pp. 290–308 (2007)

* Department of Mathematical Informatics, Graduate School of Information Science and Technology, The University of Tokyo, 7-3-1, Hongo, Bunkyo-ku, Tokyo, 113-8656, Japan, (furue-hiroki261@g.ecc.u-tokyo.ac.jp, kudo@mist.i.u-tokyo.ac.jp)