

## 論文の内容の要旨

論文題目     Security Evaluation of Multivariate Public-Key Cryptography via  
Algebraic Techniques  
(代数的手法による多変数多項式暗号の安全性評価)

氏     名     王   亜 成

Public-key cryptography, as one of the most fundamental security tools in modern technology, assures secure communications and data storage on the internet. It can be commonly used on public-key encryption, signing digital signatures and key establishment. The mostly widely used modern public-key cryptosystems are RSA cryptosystem and elliptic curve cryptosystem, which are, respectively, based on large integer factorization problem and discrete logarithm problem. As trustworthy and secure they have been, various attacks are constantly been considered to test their security. With the advent of new technologies, quantum computing, new breakthrough has been found on successfully breaking those systems in polynomial time on a quantum computer running specifically designed quantum algorithm [9], which leads to the urgent task of developing new cryptography, which are commonly referred to as post-quantum cryptography.

Post-quantum cryptosystems are developed using mathematically hard problem that quantum computers have no advantages in solving compared to classical computers. Multivariate public-key cryptography, lattice-based cryptography, code-based cryptography, hash-based cryptograph and isogeny-based cryptography are commonly considered as promising candidates. In the submissions to the post-quantum cryptography standardization project started by National Institute of Standards and Technology, many of those cryptosystems are submitted. Multivariate public-key cryptography uses a set of multivariate non-linear (often quadratic) polynomials as its public key, which also realizes its high security since solving a set of non-linear multivariate polynomials is proven to be NP-complete [5]. Research topics in multivariate public-key cryptography is often orbiting around shrinking public key size, thorough security analysis and developing new cryptosystems. In this thesis, we focus on security analysis of multivariate public-key cryptography via algebraic techniques. This includes three different directions.

## 1. Algebraic cryptanalysis of multivariate public-key cryptosystems via existing algebraic techniques

On this line of research, this thesis gives a more thorough algebraic cryptanalysis of multivariate encryption schemes EFC [8] and PERN [10] using existing algebraic techniques.

A public key of a multivariate public-key cryptosystem consists of a set of multivariate quadratic polynomials. Breaking such a cryptosystem is equivalent to solving this polynomial system, which can be achieved by first computing a Gröbner basis [2] of the ideal generated by those polynomials or the extended linearization algorithm, evaluating the complexities of those solving method is crucial to understand the algebraic security of a cryptosystem. This complexity is related to the algebraic properties of the ideal generated by this polynomial system. More specifically, it is related to the degree of regularity of the ideal. In summary, learning about the degree of regularity is important to understand the algebraic security of a cryptosystem.

EFC can be considered as a variation of the classical cryptosystem HFE [7], which is relatively well-studied. Therefore, its degree of regularity was approximated by applying the results from HFE on EFC. In this thesis, we experimentally confirmed the incorrectness of this direct application and broke the proposed 80-bit and 128-bit security parameters of EFC using hybrid approach of polynomial solving and adding field equations of the based field, where EFC is constructed. Moreover, combining the experimental results, we give secure parameters of EFC for different security levels.

PERN is a multivariate encryption cryptosystem, whose public key is generated from random multivariate non-linear polynomials with integer coefficients. It is expected to have very high security as it only depends on the hardness of solving those public key polynomials. To enable efficient decryption, the plaintext and ciphertext space of PERN is manipulated. PERN has a very small plaintext space and a relatively large ciphertext, which makes the polynomial maps in PERN injective. This small plaintext space has to be considered in algebraic cryptanalysis of PERN. This thesis gives a concrete formula for estimating the degree of regularity of the ideal generated from the public key polynomials of PERN, which allows deduction of secure parameters for PERN.

## 2. Structural and algebraic combined attack on multivariate public-key cryptosystem

On this line of research, this thesis mainly focuses on the minrank problem and minrank attack related to multivariate public-key cryptography. We propose a mixed method for solving the minrank problem, that is better than existing method under some parameters. We also revisit the minrank attack on the classic multivariate signature scheme Rainbow [3] and

evaluate its security against minrank attack using all possible method.

The minrank problem is another commonly considered problem in the field of multivariate public-key cryptography. Purely random multivariate non-linear polynomials are difficult to be used directly as public keys since its efficient inversion is hard to achieve. Therefore, most multivariate cryptosystem first uses a set of multivariate non-linear polynomials with a special structure, then use change of variables and an additional linear map to mix up all polynomials to hide their special structure. This could result in vulnerabilities to some possible structural attacks like the minrank attack, which is related to the minrank problem.

The minrank problem finds a linear combination of a given set of matrices that has a low target rank, methods for solving it includes minors modeling [1] and Kipnis-Shamir method [6]. In this thesis, we propose a combined method from those existing method and experimentally show this new method can be better for some minrank problem instances. Moreover, we revisit the minrank problem from the classic Rainbow signature scheme and give a more thorough security of Rainbow against the minrank attack using all the existing and proposed methods. As a result, we conclude Rainbow is not as strong as claimed against the minrank attack, but we could not break the proposed parameters.

### 3. New techniques for polynomial solving and its complexity

On this line of research, this thesis mainly focuses on the Weil descent method [4]. It is a method for transforming a set of polynomials over an extension field to a new set of polynomials over its subfield. This thesis approximates the degree of regularity of the ideal of the polynomial system from the Weil descent method using the first fall degree and gives a concrete formula for estimating this first fall degree.

The Weil descent method was first proposed to break the discrete logarithm problem on algebraic curve over composite fields and it can also be applied to solving a set of multivariate quadratic polynomials. When a set of polynomials over an extension field are given, after the Weil descent method, a new set of polynomials over its subfield can be obtained. Considering the subfield is usually small, field equations and hybrid approach of polynomial solving can be used. We are interested in the complexity of solving this new polynomial system, which means we have to learn about its degree of regularity. We approximate this value by the first fall degree. The first fall degree is also related to the algebraic properties of an ideal and can be obtained by analyzing the non-trivial syzygies of polynomial system. By analyzing the non-trivial syzygies of the polynomial system from the Weil descent method using linear algebra techniques, we give a concrete formula for this first fall degree, and we experimentally verified the correctness of this formula.

To conclude, this thesis focuses on the algebraic cryptanalysis of multivariate public-key

cryptography. When analyzing the algebraic security of a cryptosystem, we first consider all existing algebraic techniques, then we analyze the special structure hidden in the cryptosystem and see if it can be used to transform breaking a system into solving a set of multivariate polynomials. Finally, we consider new method for solving the given multivariate polynomials and analyze its complexity. There are still many research topics left open in this thesis. Especially regarding the minrank related research and the Weil descent method, we would like to continue exploring.

## Bibliography

- [1] Luk Bettale, Jean-Charles Faugère, and Ludovic Perret. Cryptanalysis of HFE, multi-HFE and Variants for odd and even characteristic. *Designs, Codes and Cryptography*, 69(1):1-52, 2013.
- [2] Bruno Buchberger. *Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal*. PhD thesis, Universität Innsbruck, 1995.
- [3] Jintai Ding and Dieter Schmidt. Rainbow, a new multivariate polynomial signature scheme. In *Applied Cryptography and Network Security – ACNS 2005*, vol.3531, LNCS, pp.164-175. Springer, 2005.
- [4] Gerhard Frey and Hans-Georg Rück. A remark concerning m-divisibility and the discrete logarithm in the divisor class group of curves. *Math. Comp.*, 62:865-874,1994.
- [5] Michael R. Garey and David S. Johnson. Computers and Intractability: *A Guide to the Thoery of NP-Completeness*. W. H. Freeman and Company, 1979.
- [6] Aviad Kipnis and Adi Shamir. Cryptanalysis of the HFE public key cryptosystem by relinearization. In *Advances in Cryptology – CRYPTO99*, vol.1666, LNCS, pp.19-30. Springer, 1999.
- [7] Jacques Patarin. Hidden fields equations (HFE) and isomorphisms of polynomials (IP): Two new families of asymmetric algorithms. In *Advances in Cryptology – EUROCRYPT96*, vol.1070, LNCS, pp.33-48. Springer, 1996.
- [8] Alan Szepieniec, Jintai Ding, and Bart Preneel. Extension Field Cancellation: A new central trapdoor for multivariate quadratic systems. In *Post-Quantum Cryptography – PQCrypto 2016*, vol.9606, LNCS, pp.182-196. Springer, 2016.
- [9] Peter Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Journal on Computing*, 26(5):1484-1509, 1997.
- [10] Takanori Yasuda, Yacheng Wang, and Tsuyoshi Takagi. Multivariate encryption schemes based on polynomial equations over real numbers. In *Post-Quantum Cryptography – PQCrypto 2020*, vol.12100, LNCS, pp.402-421. Springer, 2020.