Introduction to Multivariate Public Key Cryptography

Hyunsuk Moon [1]

1) *National Institute for Mathematical Sciences.*

Corresponding Author : Hyunsuk Moon, hsmoon@nims.re.kr

ABSTRACT

Nowadays, RSA and ECC are the major public key cryptography algorithm. According to Shor's algorithm [1][2], they will be broken eventually after the quantum computer is fully developed. Also, to embed into lightweight equipment, such as self-driving car and IoT(internet of things), the current cryptography systems require too heavy calculation. So we need an alternative of RSA that is safe against the quantum attack with light calculation. Multivariate public key cryptography (MPKC) is one of the promising candidates. Its research started from the work of Matsumoto and Imai [3][4]. A MPKC schemes security relies on the complexity theory that solving a set of randomly chosen quadratic polynomial equations over a finite field is NP-hard. The major idea is to find a good multivariate system F, called a central map, which can be easily inverted with appropriate method. Then two affine linear invertible maps S and T, working as a private key, need to be chosen randomly to mix the special structure of central map F. The public key is calculated as $P = S \circ F \circ T$ which is hard to distinguish from random polynomial system. MPKCs are usually highly efficient in computation to fit into the lightweight equipment, and it is safe from the quantum attacks. However, many of them have been proved to be insecure, such as MatsumotoImai scheme [3][4], balanced oil and vinegar (OV) [5]. Among them, Rainbow [6], an improvement of the unbalanced oil and vinegar scheme(UOV) [5], is regarded as a relatively effective and secure scheme. Since it was proposed, a lot of attacks have been applied to evaluate its security, such as MinRank attack [7], HighRank attack [8], UOV reconciliation and Rainbow Band Separation (RBS) attack [9] and so on. To resist all these attacks, its parameters need to be adjusted very carefully.

In this talk, I will introduce basic ideas of Multivariate Public Key Cryptography and several famous schemes. And I will show that what kind of attacks threaten the security and how it is related to the algebraic geometry problems.

REFERENCES

1. Shor, P., "Algorithms for quantum computation: discrete logarithms and factoring", 1994 Proc. 35th Annual Symp. Foundations of Computer Science, 1994, pp. 124-134
2. Shor, P. "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer", SIAM J. Comput., 1996, 26, pp. 1484-1509
3. Imai, H., Matsumoto, T., "Algebraic methods for constructing asymmetric cryptosystems", Algebraic Algorithms and Error-Correcting Codes, 1986, pp. 108-119
4. Matsumoto, T., Imai, H., "Public quadratic polynomial-tuples for efficient signature-verification and message-encryption", Advances in Cryptology-EUROCRYPT, 1988, pp. 419-453

5. Kipnis, A., Patarin, J., Goubin, L., “Unbalanced Oil and Vinegar signature schemes”, Advances in Cryptology-EUROCRYPT99, 1999, pp. 206-222

6. Ding, J., Schmidt, D., “Rainbow, a new multivariable polynomial signature scheme”, Appl. Cryptography Netw. Secur., 2005, pp. 317-366

7. Billet, O., Gilbert, H. “Cryptanalysis of Rainbow”, Secur. Cryptography Netw., 2006, pp. 336-347

8. Yang, B., Chen, J., “Building secure tame-like multivariate public-key cryptosystems: The new tts” Inf. Sec. Priv., 2005, pp. 518-531

9. Ding, J., Yang, B., Chen, C. et al., “New differential-algebraic attacks and reparametrization of Rainbow”, Proc. of the Sixth Int. Conf. on Applied Cryptography and Network Security, 2008, pp. 242-257