

From MQ to MQQ Cryptography: Weaknesses & New Solutions

Rohit Ahlawat¹, Kanika Gupta¹ & Saibal K. Pal²

¹Department of Computer Science, University of Delhi, DELHI – 110007

²Scientific Analysis Group, DRDO, DELHI – 110054

{ahlawatrohit@yahoo.com, kanikagupta0906@gmail.com, skptech@yahoo.com}

Abstract. Public Key Cryptosystems have been in use for more than three decades. A number of schemes based on integer factorization problem, discrete log problem, residuosity problem, digital signature methods, Lucas sequence, Lattice problems, error-correcting codes, braid groups etc. have been designed. Recently, Multivariate Quadratic (MQ) Polynomials could be efficiently used for design of a number of interesting cryptosystems. However, successful attacks on some of these schemes encouraged researchers to design new trapdoor functions suitable for present cryptographic applications. Multivariate Quadratic Quasigroup (MQQ) has been one of the latest ideas in this direction but is limited to the construction of MQQ of lower orders. Our significant contribution in this direction is efficient generation of MQQs of higher order suitable for design of secure public key cryptosystems.

Keywords: Public Key Cryptosystems, Boolean Functions, Finite Fields, MQ Polynomial, Quasigroup, Multivariate Quadratic Quasigroup.

1 The Multivariate Quadratic (MQ) Problem

The MQ problem [1] over a finite field F_q (where q is a prime power) is finding a solution $x \in F_q^n$ to a given systems of m quadratic polynomial equations $y = (p_1, p_2, \dots, p_m)$ over F_q in n indeterminate. That is, we wish to solve

$$\begin{aligned} y_1 &= p_1(x_1, x_2, \dots, x_n) \\ y_2 &= p_2(x_1, x_2, \dots, x_n) \\ &\dots \\ &\dots \\ &\dots \\ y_m &= p_m(x_1, x_2, \dots, x_n) \end{aligned} \tag{1}$$

for a given $y = (y_1, \dots, y_m) \in F_q^m$ and the unknown $x = (x_1, x_2, \dots, x_n) \in F_q^n$. True to the term quadratic, in the above system of equations, the polynomials p_i have the

form

$$P_i(x_1, x_2, \dots, x_n) = \sum_{(1 \leq j \leq k \leq n)} \gamma_{i,j,k} x_j x_k + \sum_{(j=1 \text{ to } n)} \beta_{i,j} x_j + \alpha_i \quad (2)$$

for $1 \leq i \leq m$; $1 \leq j \leq k \leq n$ and $\alpha_i, \beta_{i,j}, \gamma_{i,j,k} \in F_q$ (the constant, linear and quadratic coefficients respectively) [2]. It has been shown that over a finite field, this problem is NP hard.

2 The MQ Problem in Cryptography

One proposal for secure public key scheme is based on the problem of solving Multivariate Quadratic equations (MQ-problem) over finite fields. Other proposals share the same type of public key, i.e., polynomials of degree 2 over (small) finite fields. Since MQ is NP hard problem, it was used to design secure encryption schemes. Digital signature schemes were also constructed based on MQ.

Matsumoto-Imai scheme was the first one to introduce to the world of cryptography with the new unexplored field of Multivariate Quadratic polynomials. Their key idea was to utilize both the vector space and the hidden field structure of k^n , where k is a finite field. More specifically, instead of searching for invertible maps over the vector space k^n directly, they looked for invertible maps on a field K , a degree n field extension of k , which could also be identified as an n dimensional vector space over k . This map could then be transformed into an invertible map over k^n [3]. Although this scheme was cracked by Paratin in 1995, many new variants of the same exist which have proved to be quite efficient. One of these includes the Sflash signature scheme which was accepted in 2004.

Various other schemes have been designed based on MQ, out of which four are the standards. Namely, Matsumoto and Imai scheme which was broken by Paratin, Stepwise Triangular scheme which was broken by Shamir, Hidden Field Equations which was broken up by Kipnis and Shamir, and Unbalanced Oil and Vinegar which was also successfully broken. Although multivariate quadratic shows a new light into the world of cryptography, almost all the schemes developed under it have been broken. So, we needed a new scheme which was as complex as MQ based schemes but yet difficult to break.

3 Multivariate Quadratic Quasigroups over MQ Polynomials

Public Key Cryptosystems based on Multivariate Quadratic Quasigroups (MQQ) [4, 5] were constructed to counter the weaknesses observed in the MQ based systems. As the name suggests, these are based on Quasigroups and thus combine the advantages of both the MQ polynomials and Quasigroups. Using this scheme, there will be a huge class of Quasigroups called Multivariate Quadratic Quasigroups which generates MQ polynomials using certain types of operations. It overcomes the weaknesses that existed with the MQ problem and provides a huge class of elements that are yet

unidentified with respect to the number of elements in a certain type of MQQ. This scheme would be described in detail.

4 MQQ in Cryptography

MQQ gives a new direction to the field of cryptography. MQQ generation scheme can be used for developing new MQQ based Public Key Cryptosystems as well as improving the existing schemes for encryption, hashing and digital signatures. It is not far when Quantum Computers would be designed for solving practical problems and used for cracking many existing cryptographic algorithms. By the time they arrive, it's recommended that we design stronger schemes based on new hard problems.

For a MQQ of order d , we use a Latin Square of order 2^d from which unique values are picked up randomly for generation of MQQs. The earlier scheme used to generate MQQs of order d were limited to $d=5$. We have designed a new algorithm to generate Multivariate Quadratic Quasigroups of higher order using basic concepts of Quasigroup string transformations using a Latin Square, and vector-valued Boolean function representation of Quasigroups and their operations. The vector-valued Boolean function representation is limited to a maximum degree 2 so as to give quadratic polynomials which can then be classified into MQQ or not MQQ. Our algorithm efficiently generates MQQs of higher orders, thereby providing a new and faster method of generating public and private keys from the derived equations. We would be reporting the scheme in detail, computations required for generation of different MQQs and time comparison with the existing scheme.

References

1. Wolf, C., Preneel, B.: Taxonomy of Public Key Schemes based on Problem of Multivariate Quadratic Equations, <http://eprint.iacr.org/2005/077> (2005)
2. Feldmann, A. T.: A Survey of Attacks on Multivariate Cryptosystems, Waterloo, Ontario, Canada, A Thesis presented to the University of Waterloo in fulfillment of the thesis requirement for the Degree of Master of Mathematics in Combinatorics & Optimization (2005)
3. Ding, J., Jason, E. G. and Schmidt D. S.: Multivariate Public Key Cryptosystems, Springer (2006)
4. Gligoroski, D., Markovski S. and Knapskog S. J.: A Public Key Block Cipher Based on Multivariate Quadratic Quasigroups, Cryptography and Security, <http://arxiv.org/abs/0808.0247> (2008)
5. Gupta K., Ahlawat R.: Design of Public Key Block Ciphers based on Multivariate Quadratic Quasigroups, Technical Report, Department of Computer Science, University of Delhi (2008)