Similar Keys of Multivariate Quadratic Public Key Cryptosystems

Yuh-Hua Hu[1], Lih-Chung Wang[2], Chun-Yen Chou[3], and Feipei Lai[4]

[1] Department of Computer Science and Information Engineering,
National Taiwan University, Taipei 106, Taiwan
d92015@csie.ntu.edu.tw
[2] Department of Applied Mathematics,
National Donghwa University,
Hualien 974, Taiwan
lcwang@mail.ndhu.edu.tw
[3] Department of Mathematical Education,
National Hualien University of Education,
Hualien 970, Taiwan
choucy@mail.nhlue.edu.tw
[4] Departments of Electrical Engineering & of Computer Science
and Information Engineering,
National Taiwan University, Taipei 106, Taiwan
flai@ntu.edu.tw

Abstract. Most multivariate schemes have potentially much higher performance than other public key cryptosystems [15] [4] [1] [2]. Wolf and Preneel [16] show multivariate quadratic public key schemes have many equivalent keys and provide some transformations to identify the keys. In this paper, we propose the idea of similar keys of MQ-based public key cryptosystems(PKCs) and provide a method to reduce the size of private key in MQ-based PKCs to 50% $\sim$ 70% of its original size. And our method is generic for most MQ-based PKCs except for UOV-like and STS-like schemes. Moreover, our method remains the equivalent security and efficiency with original MQ-based PKCs.

Keywords: MQ, multivariate, public key cryptosystem, digital signature, similar key.

1 Introduction

Public key cryptography is involving the use of two separate keys, and the use of two keys has profound consequences in the areas of non-repudiation, confidentiality, and authentication. For example, on-line transactions need the digital signature schemes to verify the validness, the e-mail security application like PGP[18] needs the public key cryptosystem to protect the session key, and the heart of the authentication service X.509[18] is public key certificate. Finding a efficient, secure and easy to implement PKC is helpful to the network security

Y.G. Desmedt et al. (Eds.): CANS 2005, LNCS 3810, pp. 211–222, 2005.

application. Most MQ-based PKCs are faster than other PKCs in key generation/signing or decrypting/verifying or encrypting [15] [4] [1] [2]. Hence, they may be applied in more occasions. However, the key size of MQ-based PKCs is their drawback.

Number-theoretical PKCs have relatively small private key size, for example RSA-1024 bits, ECC-163bits [7] [5]. MQ-based PKCs have a large size of private key, such as C*[8], HFE[11], QUARTZ[12], SFLASH^{v3}[2], TRMS[15], TTS[1] and UOV[6]. The reason is that most MQ-based PKCs need to store the affine transformations, consisting of an invertible matrix and constant offset, and the coefficients of polynomials in φ_2. The coefficients of the affine transformations are the major parts of the private key.

Changing the affine transformation is an intuitive way to reduce the size of private key. Wang et al. [15] used the extension field instead of the ground field and Hu et al. [4] used the elementary row operations to reduce the size of private key, and both of them speeded up the signing or decrypting time. Though there is still no attack to these specific affine transformations, they did not prove that the specific affine transformation has the same security with arbitrary invertible matrix.

Wolf and Preneel[16] showed some systematic schemes to analyze the equivalent keys. And they provide the concept and the normal forms to reduce the private key. In this paper we introduce the idea of similar keys of MQ-based PKCs, and give a model for most MQ-based PKCs that can reduce the size of the private key to 50% $\sim$ 70% of original size except for UOV-like and STS-like [17] schemes, and we sketch that the new model has the same security as the original model.

In Section 2, we describe the model of MQ-based public key scheme. In Section 3, we define the similar key of MQ-based PKCs. In Section 4, we give our model to reduce the keys and the performance. In Section 5, we discuss and analyze our model. And our conclusion is in Section 6.

2 MQ-Based PKCs

For a typical MQ-based PKC, they operate on a base field $\mathbb{K}$. And its public key is composed of three maps, $\varphi_3 \circ \varphi_2 \circ \varphi_1$, and its private key is the triple $(\varphi_1^{-1}, \varphi_2, \varphi_3^{-1})$. φ_1 and φ_3 are affine transformations in $\mathbb{K}^n$ and $\mathbb{K}^m$ respectively and φ_1^{-1} and φ_3^{-1} are their inverse transformations. The φ_2 is a quadratic transformation and the structure of φ_2 in each MQ-based PKC is different (HFE, SFLASH^{v3}, C*, QUARTZ, TTS, TRMS, UOV). We illustrate the idea of similar keys with TRMS. The following example is revised in the workshop of PKC2005 [13].

2.1 Structure of TRMS

There are a variety of schemes of TRMS which are all based on tractable rational maps. Tractable rational maps on $\mathbb{K}^n$ are invertible affine transformations or, after a rearrangement of indices if necessary, functions of the following form $\varphi : \mathbb{K}^n \to \mathbb{K}^n$,