Analysis of Efficiency and Security of Signature Schemes based on Multivariate Quadratic Polynomial Problem
（多変数多項式問題に基づく署名方式の効率性と安全性の解析）

Dept. of Mathematical Informatics 48196228 Hiroki Furue
Supervisor Prof. Tsuyoshi Takagi

1 Background

Public key cryptosystem is a cryptographic system that uses pairs of keys: public keys, which may be disseminated widely, and private keys, which are known only to the owner. Multivariate public key cryptography, which is based on the multivariate quadratic polynomial ($\mathcal{MQ}$) problem, is regarded as a strong candidate for post-quantum cryptography (PQC). It is commonly admitted that MPKC is more suitable as an approach to build signature schemes. In MPKC, analyzing their efficiency and security is one of the important problems.

2 Motivation

2.1 MQDSS and SOFIA

At AsiaCrypt 2016, Chen et al. proposed MQDSS [1], the first multivariate signature scheme whose security is proven to be based solely on the $\mathcal{MQ}$-problem. This scheme is obtained by applying an extended version of the Fiat-Shamir transform to the $\mathcal{MQ}$-based 5-pass IDS proposed by Sakumoto et al. [7]. MQDSS is an $\mathcal{MQ}$-based signature scheme that has passed into the second round of NIST call for post-quantum proposals. In [1], Chen et al. prove that MQDSS is EU-CMA secure in the random oracle model (ROM), whereas, in 2020, Don et al. prove the security of MQDSS in the quantum random oracle model (QROM), where QROM means that a quantum adversary can access the random oracle in superposition. However, one problem with MQDSS is that the security reduction of MQDSS in the QROM is not tight. In the thesis, we use the definition of tight security reduction as follows: for any attackers on the target security (e.g. EU-CMA security) with a success probability ϵ, there is an attacker on the underlying mathematical problem (e.g. $\mathcal{MQ}$ problem) with a success probability ϵ' satisfying $\epsilon' \geq \epsilon - \mathsf{negl}(k)$, where $\mathsf{negl}(k)$ is a negligible function for the security parameter k.

At PKC 2018, Chen et al. [2] proposed a signature scheme called SOFIA obtained by applying the Unruh transform to the $\mathcal{MQ}$-based 5-pass IDS proposed by Sakumoto et al. [7]. This signature scheme is proven secure in the QROM, and the security reduction is tight. However, one problem with SOFIA is that SOFIA loses its effectiveness: its signature is about three times larger than that of MQDSS.

2.2 UOV and Block Anti Circulant UOV

The unbalanced oil and vinegar signature scheme (UOV) [4], a multivariate signature scheme proposed by Kipnis et al. at EUROCRYPT 1999, has withstood various types of attacks for about 20 years. UOV is a well-established signature scheme due to its short signature and short execution time. Rainbow [3], a multi-layer UOV variant, was selected as a third-round finalist in the NIST PQC project. However, both UOV and Rainbow have public keys that are much larger than those of other PQC candidates, e.g., lattice-based signature schemes. Indeed, Rainbow has the largest public key among the third-round-finalist signature schemes, and NIST's report states that Rainbow is not suitable as a general-purpose signature scheme due to this problem.

At SAC 2019, Szepieniec and Preneel [8] proposed a new variant of UOV called block-anti-circulant UOV (BAC-UOV). In this scheme, the matrices representing the quadratic part of polynomials of the public key are block-anti-circulant matrices (block matrices whose every block is an anti-circulant matrix where each row vector is rotated one element to the left relative to the preceding row vector). By using this construction, they succeed in reducing the public key size, because every block of a block-anti-circulant matrix can be represented by using its first row. Additionally, by combining the block-anti-circulant construction with other compression techniques such as the field lifting used in LUOV, the public key size of BAC-UOV decreases by about $30 \sim 40\%$ compared with LUOV, and the signature size of BAC-UOV also slightly decreases compared with LUOV.

3 Contributions

3.1 Efficient $\mathcal{MQ}$-based Signature Scheme with Tight Security Proof

In the thesis, we first propose a more efficient $\mathcal{MQ}$-based signature scheme with tight security proof in the QROM. Our approach is to propose a novel 3-pass IDS with impersonation probability of $\frac{1}{2}$ which is more optimal with the Unruh transform. We also apply the Unruh transform to other 3-pass IDSs proposed by Sakumoto et al. [7] and Monteiro et al. [6] to obtain two other $\mathcal{MQ}$-based signatures, and compare these signatures with SOFIA at the security level I of NIST PQC (see Table 1). As a result, our scheme is the most efficient among all other signa-

tures constructed by applying the Unruh transform, and so our scheme has the shortest signature among the $\mathcal{MQ}$-based signatures with the tight security in the QROM. In particular, the signature size of our scheme is decreased by about 35% compared with SOFIA.

Table 1. Size of signature obtained by applying the Unruh transform to $\mathcal{MQ}$-based identification schemes in level I of NIST PQC security category

Unruh transform + $\mathcal{MQ}$-based IDS	|sig| (KB)
Sakumoto et al.'s 5-pass IDS [7]	46.8
Sakumoto et al.'s 3-pass IDS [7]	34.8
Monteiro et al.'s 3-pass IDS [6]	33.3
our proposed 3-pass IDS	**29.6**

Our technique in designing a new 3-pass IDS combines both IDSs of Sakumoto et al. [7] and Monteiro et al. [6]. As a result, it has impersonation probability of $\frac{1}{2}$, which is the same as that in the 3-pass IDS by Monteiro et al., whereas that in the 3-pass IDS by Sakumoto et al. is $\frac{2}{3}$. One drawback of our IDS is that the response size is larger than that in the 3-pass IDS by Sakumoto et al. and comparable with that in the 3-pass IDS by Monteiro et al. However, if we construct an $\mathcal{MQ}$-based signature scheme by applying the Unruh transform to our IDS, then the signature size of our scheme is smaller than those of signature schemes using the previous 3-pass IDSs. We stress that the signature size of our proposed scheme is not shorter than that of MQDSS. We can also construct a signature scheme by applying the Fiat-Shamir transform to our proposed IDS, but this scheme is not effective than MQDSS and not tightly secure. Therefore, in the thesis, we consider only our scheme from the Unruh transform.

3.2 Attack on Block Anti Circulant UOV

In the thesis, we propose a new attack against the BAC-UOV scheme, that is composed of three steps.

First, we utilize the property of an anti-circulant matrix that the sum of the elements of one row is the same as those of other rows. By using this property, we can transform a block-anti-circulant matrix into the following form:

$$\overbrace{}^{N}\overbrace{}^{(\ell-1)N}$$

$$\begin{array}{|c|c|}\hline A & 0 \\ \hline 0 & B \\ \hline \end{array}, \qquad (1)$$

where A and B are an $N \times N$ matrix and an $(\ell-1)N \times (\ell-1)N$ matrix, respectively ($N := n/\ell$, n is the number of variables, and ℓ is the block size). The matrices associated with the quadratic forms of the public key polynomials can all be transformed into the form of (1) by multiplying a special invertible matrix on the right and its transpose on the left. Second, we execute the UOV attack [5] on the upper-left $N \times N$ submatrices of the obtained matrices, which only requires very little complexity, and we can change those submatrices into the form of the matrix representing the quadratic parts of the central map of UOV. By this operation, we can reduce the number of variables that appear in the quadratic terms of the public key polynomials. Finally, we execute the direct attack on the transformed polynomial system.

From our analysis, the complexity of our attack decreases by about 20% compared with the best existing attack on UOV (see Table 2). As a result, we consider that the secure parameters of BAC-UOV need to be modified.

Table 2. Comparison complexity of existing attacks and our proposed attack on BAC-UOV

security level	security parameter in [8]	our proposed attack
NIST II	2^{147}	$\mathbf{2^{119}}$
NIST IV	2^{210}	$\mathbf{2^{171}}$
NIST V	2^{257}	$\mathbf{2^{219}}$

Bibliography

[1] Chen, M. S., Hülsing, A., Rijneveld, J., Samardjiska, S., Schwabe, P.: From 5-pass MQ-based identification to MQ-based signatures. In: ASIACRYPT 2016, LNCS, vol. 10032, pp. 135–165. Springer (2016)

[2] Chen, M. S., Hülsing, A., Rijneveld, J., Samardjiska, S., Schwabe, P.: SOFIA: MQ-based signature in the QROM. In: PKC 2018, LNCS, vol. 10770, pp. 3-33. Springer (2018)

[3] Ding, J., Schmidt, D.: Rainbow, a New Multivariable Polynomial Signature Scheme. In: ACNS 2005, LNCS, vol. 3531, pp. 164–175. Springer (2005)

[4] Kipnis, A., Patarin, J., Goubin, L.: Unbalanced oil and vinegar signature schemes. In: EUROCRYPT 1999, LNCS, vol. 1592, pp. 206–222. Springer (1999)

[5] Kipnis, A., Shamir, A.: Cryptanalysis of the oil and vinegar signature scheme. In: CRYPTO 1998, LNCS, vol. 1462, pp. 257–266. Springer (1998)

[6] Monteiro, F. S., Goya, D. H., Terada, R.: Improved identification protocol based on the MQ problem. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, **98**-A(6), 1255–1265 (2015)

[7] Sakumoto, K., Shirai, T., Hiwatari, H.: Public-key identification scheme based on multivariate quadratic polynomials. In: CRYPTO 2011, LNCS, vol. 6841, pp. 706–723. Springer (2011)

[8] Szepieniec, A., Preneel, B.: Block-anti-circulant unbalanced oil and vinegar. In: SAC 2019, LNCS, vol. 11959, pp. 574–588. Springer (2019)