Reduction of Key Sizes on Rainbow-like Multivariate Signature Schemes*

Gustavo Zambonin[1]

[1]Departamento de Informática e Estatística
Universidade Federal de Santa Catarina
88040-900, Florianópolis, Brazil

gustavo.zambonin@posgrad.ufsc.br

1. Research Subject

The amount of data transmitted through digital means has grown exponentially in the last decades. Advances in engineering have provided smaller and cheaper devices, usually integrated with wireless capabilities, facilitating heterogeneous communications. Still, the matter of trusting data received from another, possibly unknown machine, is highly important. Digital signatures are cryptographic frameworks employed to solve matters of authenticity, integrity and non-repudiation of messages. Protecting information with this method is sufficient to prevent malicious actors from forging a message or reading private matters, according to Goldreich [Goldreich 2004].

Nonetheless, current digital signature schemes are proven to be secure only under the assumption that there are no quantum adversaries. Unlike classical computers, quantum machines can execute Shor's algorithm [Shor 1997] to efficiently solve problems such as integer factorisation or discrete logarithm. Ergo, it is imperative to study cryptography that is quantum-resistant, *i.e.* post-quantum, even if classical machines are still the norm. One of the main approaches for instantiating post-quantum digital signature schemes is based on multivariate quadratic equations. The problems upon which these are based are not known to be solved more efficiently with a quantum computer [Bernstein et al. 2008]. Ergo, these schemes appear to be good candidates for replacing currently used ones.

Multivariate cryptography provides a variety of signature schemes, categorised by their underlying mathematical structures. They are extremely efficient when signing and verifying messages [Ding et al. 2006], since most computations are based on finite field arithmetic. Still, schemes are highly distinct with respect to the balance between security parameters, signature and key sizes [Ding and Petzoldt 2017]. One of the most balanced schemes in this context is called Rainbow, due to Ding and Schmidt [Ding and Schmidt 2005]. It is a generalisation of the classical Unbalanced Oil and Vinegar (UOV) scheme [Kipnis et al. 1999], featuring structures that are easy to describe and implement accurately. This is important when considering, for instance, limited environments such as smart cards and embedded devices. These still need secure communications, but are restrained with regards to memory and processing power, when operating a signed message.

Nevertheless, while signature sizes for Rainbow are already excellent, key sizes are orders of magnitude greater than currently used schemes (*e.g.* RSA has 512 bytes keys). This may be addressed by means of employing special structures into its public

*As submitted to the INE410111 class (Research Methodology in Computer Science).

and private keys. Since these can be stored as matrices, sparseness and cyclic approaches are common strategies. However, it is important to note that the restriction of key pairs to matrices with these characteristics may negatively impact the overall security of the scheme. Thus, we will focus on the creation of secure methods for the reduction of public and private keys on the Rainbow signature scheme.

2. Related Works

There has been a considerable amount of work done when dealing with reduction of private and public keys on the Rainbow signature scheme. Still, not all of the published works maintain the security of their common predecessor. A scheme based on non-commutative rings due to Yasuda *et al.* [Yasuda et al. 2012] reduces private keys by up to 75%, but was broken by independent researchers [Hashimoto 2013, Thomae 2012]. A scheme based on circulant matrices by Peng and Tang [Peng and Tang 2017] gives secure parameters for other works of Yasuda *et al.* [Yasuda et al. 2013, Yasuda et al. 2014b]. Yet, its 45% private key reduction was deemed insecure by Hashimoto [Hashimoto 2018].

Still, there are various examples of schemes that resist currently known cryptanalysis. Petzoldt *et al.* suggest a scheme based on cyclic matrices [Petzoldt et al. 2010] that reduces the public key size by as much as 62%. A scheme due to Yasuda *et al.* [Yasuda et al. 2014a] uses sparse matrices to reduce private key sizes by up to 76%. Petzoldt [Petzoldt 2013] also uses linear recurring sequences to reduce the public key size by a factor of 7.5.

Moreover, there are also generic constructions that reduce the public key in exchange of increasing the signature. This is the case of the works of Szepieniec *et al.* [Szepieniec et al. 2017] and Beullens [Beullens 2017]. Another strategy by Beullens and Preneel [Beullens and Preneel 2017] works for any scheme based on the Oil—Vinegar principle, and is based on lifting public and central maps to an extension field. However, none of the aforementioned works deal with reduction of both keys in the key pair.

3. Hypothesis

It is evident that no works in the literature have reduced both private and public keys on the Rainbow signature scheme. Thus, our target research question asks if there are any restrictions in doing so. It is known that, in public key cryptography, codifications done by a private key will only be undone by its corresponding public key and vice-versa, *i.e.* both keys are intrinsically related. The usual procedure is to use a seeded pseudo-random number generator to create a private key, and derive the public key from that. In the case of Rainbow, we wish to know if this method can be executed using only matrices with a desirable symmetry, that may act as a key pair of this scheme.

4. Objectives

With this project, we aim to reduce the size of both private and public keys on the Rainbow signature scheme. This will be done through the introduction of a special structure into the matrix representation of both keys, allowing their compact presentation and decreasing overall storage requirements for the scheme. Based on this, the following specific objectives are presented.

a. Verify whether symmetric matrix structures (*e.g.* Hessenberg, Hankel, centrosymmetric) may be used to generate key pairs and their direct effect on the security of the scheme;
b. Establish structures that are fit to be used in the context of multivariate public key cryptography, that is, observe if public keys generated from specially composed private keys will maintain their underlying structure;
c. Development of a Rainbow signature scheme variant employing a matrix structure with the intent of reducing private and public key sizes;
d. Provide sets of parameters reasonable for environments with distinct security requirements, for instance, desktop computers, mobile and embedded devices, servers etc..

5. Methodology

We will demonstrate the previously mentioned objectives through a chronological list of activities presented below. These partial endeavours will enhance our knowledge in special matrix structures, the Oil—Vinegar principle, the Rainbow signature scheme and its modern variants, as well as new cryptanalytic methods. Furthermore, note that there are some specific literary and oral productions that must be created, as part of the master's program requirements.

a. Bibliographic review and maintenance of a database with works that are related to the Rainbow signature scheme. We will mainly focus on variations that feature reduction of public or private key sizes, and related cryptanalysis;
b. Deep study of matrix-like structures that may be represented in a compact form;
c. Creation of an algorithm that can generate a compact private-public key pair;
d. Procedure to check if the reduced key space of compact key pairs is still large enough to prevent brute-force search;
e. Apply currently known cryptanalytic methods to the new Rainbow-like signature scheme and compare it with the original method;
f. Compare the new algorithm with other schemes that also reduce key sizes through experiments;
g. At least one scientific contribution in the form of a conference paper or journal article;
h. Oral presentation about the work done so far, that will act as a qualification exam;
i. Production of a dissertation about the subject;
j. Oral presentation about the concluded work.

6. Expected Results

We wish to collaborate with individuals and institutions alike, with the intent of broadening our knowledge and push the boundaries of optimisations with regards to reducing key sizes in single-field schemes. As such, we expect the publication of scientific material on this subject, collaboration with students, professors, independent and contracted researchers. Further, we also aim to promote our university through oral presentations of this research, provide free, open-source software implementations of these algorithms, and create a breakthrough result on the relation between compact private and public keys on Rainbow.

References

Bernstein, D. J., Buchmann, J., and Dahmen, E. (2008). *Post Quantum Cryptography*. 1st edition.

Beullens, W. (2017). New signature schemes based on UOV with smaller public keys. Master's thesis, Katholieke Universiteit Leuven.

Beullens, W. and Preneel, B. (2017). Field Lifting for Smaller UOV Public Keys. In Patra, A. and Smart, N., editors, *Progress in Cryptology – INDOCRYPT 2017*, volume 10698 of *Lecture Notes in Computer Science*.

Ding, J., Gower, J., and Schmidt, D. (2006). *Multivariate Public Key Cryptosystems*. 1st edition.

Ding, J. and Petzoldt, A. (2017). Current State of Multivariate Cryptography. *IEEE Security & Privacy*, 15(4):28–36.

Ding, J. and Schmidt, D. (2005). Rainbow, a New Multivariable Polynomial Signature Scheme. In Ioannidis, J., Keromytis, A., and Yung, M., editors, *Applied Cryptography and Network Security*, volume 3531 of *Lecture Notes in Computer Science*, pages 164–175.

Goldreich, O. (2004). *Foundations of Cryptography: Volume 2, Basic Applications*. 1st edition.

Hashimoto, Y. (2013). Cryptanalysis of the Quaternion Rainbow. In Sakiyama, K. and Terada, M., editors, *Advances in Information and Computer Security*, volume 8231 of *Lecture Notes in Computer Science*, pages 244–257.

Hashimoto, Y. (2018). On the security of Circulant UOV/Rainbow. Cryptology ePrint Archive, Report 2018/847.

Kipnis, A., Patarin, J., and Goubin, L. (1999). Unbalanced Oil and Vinegar Signature Schemes. In Stern, J., editor, *Advances in Cryptology – EUROCRYPT '99*, volume 1592 of *Lecture Notes in Computer Science*, pages 206–222.

Peng, Z. and Tang, S. (2017). Circulant Rainbow: A New Rainbow Variant With Shorter Private Key and Faster Signature Generation. *IEEE Access*, 5:11877–11886.

Petzoldt, A. (2013). *Selecting and Reducing Key Sizes for Multivariate Cryptography*. PhD thesis, Technische Universität Darmstadt.

Petzoldt, A., Bulygin, S., and Buchmann, J. (2010). CyclicRainbow – A Multivariate Signature Scheme with a Partially Cyclic Public Key. In Gong, G. and Gupta, K. C., editors, *Progress in Cryptology – INDOCRYPT 2010*, volume 6498 of *Lecture Notes in Computer Science*, pages 33–48.

Shor, P. W. (1997). Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. *SIAM Journal on Computing*, 26(5):1484–1509.

Szepieniec, A., Beullens, W., and Preneel, B. (2017). MQ Signatures for PKI. In Lange, T. and Takagi, T., editors, *Post Quantum Cryptography*, volume 10346 of *Lecture Notes in Computer Science*, pages 224–240.

Thomae, E. (2012). Quo Vadis Quaternion? Cryptanalysis of Rainbow over Non-commutative Rings. In Visconti, I. and de Prisco, R., editors, *Security and Cryptography for Networks*, volume 7485 of *Lecture Notes in Computer Science*, pages 361–373.

Yasuda, T., Ding, J., Takagi, T., and Sakurai, K. (2013). A Variant of Rainbow with Shorter Secret Key and Faster Signature Generation. In Chen, K., Xie, Q., Qiu, W., Xu, S., and Zhao, Y., editors, *ACM Workshop on Asia Public-Key Cryptography*, pages 57–62.

Yasuda, T., Sakurai, K., and Takagi, T. (2012). Reducing the Key Size of Rainbow Using Non-commutative Rings. In Dunkelman, O., editor, *Topics in Cryptology – CT-RSA 2012*, volume 7178 of *Lecture Notes in Computer Science*, pages 68–83.

Yasuda, T., Takagi, T., and Sakurai, K. (2014a). Efficient variant of Rainbow using sparse secret keys. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*, 5(3):3–13.

Yasuda, T., Takagi, T., and Sakurai, K. (2014b). Efficient Variant of Rainbow without Triangular Matrix Representation. In Mahendra, M. S., Neuhold, E. J., Tjoa, M. A., and You, I., editors, *Information and Communication Technology*, volume 8407 of *Lecture Notes in Computer Science*, pages 532–541.