Reducing Public Key Size on the Rainbow Signature Scheme with Cyclic Structures*

Gustavo Zambonin[1], **Albrecht Petzoldt**[2], **Johannes Buchmann**[2]

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

gustavo.zambonin@posgrad.ufsc.br

[2] Department of Computer Science
Technische Universität Darmstadt
Hochschulstraße 10, 64289 Darmstadt, Germany

{apetzoldt,buchmann}@cdc.informatik.tu-darmstadt.de

Abstract. *Cryptography based on multivariate equations is one of the main approaches for creating algorithms that are quantum-resistant. Nonetheless, digital signature schemes based on these concepts feature impractical key pair sizes, orders of magnitude greater than commonly-used schemes. We identify a special structure on components of the Rainbow signature scheme that allows for the creation of public keys with a partially cyclic construction, reducing storage requirements by up to approximately a factor of three.*

1. Introduction

Security in communications is necessary to ensure trust between parties. For example, a handwritten signature may be placed on a document to attest that the signer is in agreement with its contents. This is no exception when considering digital transit of data, for instance electronic mail or messages between devices. In this context, cryptographic techniques such as digital signature schemes must be employed to ensure desirable properties, namely authenticity, integrity and non-repudiation. These mathematical frameworks permit a signer to hold a private key and a correspondent public key, uniquely related in the sense that one can decode only what its dual has encoded.

Furthermore, to prevent forgery of signatures by any malicious actor, schemes are naturally bound to computational problems, virtually unsolvable without the private key. Integer factorisation and discrete logarithm are the most common examples, related respectively to the RSA and ECDSA schemes. Yet, such problems are provably computable in polynomial time by a quantum computer [Shor 1997]. Ergo, post-quantum digital signature schemes are paramount in maintaining secure inter-communications.

One of the approaches for constructing post-quantum schemes is based on systems of linear equations with multiple variables, and is appropriately called multivariate cryptography. Performing computations with these equations is generally very efficient, suitable for performance-, energy-constrained devices. Still, considering common key

*Written for the INE410111 class (Research Methodology in Computer Science), based on [Petzoldt et al. 2010b] from [Petzoldt 2013], Qualis of B1. **This is not a real paper.**

sizes of at most 512 bits for elliptic curve cryptography, the size of keys for multivariate schemes is prohibitive, as seen in [Petzoldt 2013, Table 6.4] and [Ding and Petzoldt 2017, Table 1]. Naturally, it is imperative to research strategies with the intent of reducing these keys, which are at least a few KB in size.

We focus on reducing the public key size of the Rainbow scheme due to Ding and Schmidt [Ding and Schmidt 2005], a generalised version of the Unbalanced Oil and Vinegar (UOV) scheme by Kipnis *et al.* [Kipnis et al. 1999], that itself already reduces key sizes and signature length. We apply the strategy described in [Petzoldt 2013, Chapter 7], namely choosing part of the public key instead of a central map, and generating remaining elements as needed.

1.1. Related Works

Reduction of private keys is featured much more commonly in the literature, as seen in the works of Yasuda *et al.* [Yasuda et al. 2013, Yasuda et al. 2014b, Yasuda et al. 2014a] and, more recently, Peng and Tang [Peng and Tang 2017], through the use of clever matrix representations. While these approaches cut up to 80% of the private key, we note that public keys are (evidently) more frequently distributed and stored throughout various devices, creating additional limitations for devices that sign or verify messages with various public keys. Hence, it is compelling to elaborate strategies to reduce these.

1.2. Organization

In Section 2, a straightforward description of the Rainbow signature scheme is given. Afterwards, the rationale behind generating a public key with a special structure is explained in Section 3. A comparison between practical instances of the new and old schemes is given in Section 4. Finally, Section 5 concludes the paper and suggests future works.

2. Classic Rainbow Signature Scheme

We describe below the Rainbow digital signature scheme, that consists of several "oil and vinegar" layers. Consider a finite field $\mathbb{F}_q$, and a sequence of integers $0 = v_0 < v_1 < v_2 < \cdots < v_{u+1} = n$, with $m = n - v_1$. For $i = \{1, \ldots, u\}$, let the vinegar variables be $V_i = \{1, \ldots, v_i\}$ and oil variables be $O_i = \{v_i + 1, \ldots, v_{i+1}\}$, with $o_i = |O_i|$. Denote an instance of the scheme by Rainbow$(\mathbb{F}_q, v_1, o_1, \ldots, o_u)$. Note that when $u = 1$, we get the UOV scheme.

2.1. Key Generation

We randomly generate linear or affine maps $\mathcal{S} : \mathbb{F}_q^m \to \mathbb{F}_q^m$ and $\mathcal{T} : \mathbb{F}_q^n \to \mathbb{F}_q^n$. The central map $\mathcal{F} : \mathbb{F}_q^m \to \mathbb{F}_q^n$ has a special structure. It consists of m quadratic polynomials of the form

$$f^{(k)} = \sum_{i,j \in V_\ell, i \le j} a_{ij}^{(k)} x_i x_j + \sum_{i \in V_\ell, j \in O_\ell} b_{ij}^{(k)} x_i x_j + \sum_{i \in V_\ell \cup O_\ell} c_i^{(k)} x_i + d^{(k)}, \tag{1}$$

with $k \in \{v_1 + 1, \ldots, n\}$, where ℓ is the only integer such that $k \in O_\ell$. The private key is the triple $(\mathcal{S}, \mathcal{F}, \mathcal{T})$. We hide the structure of $\mathcal{F}$ in the public key through its composition with the other maps. Hence, the public key is the map $\mathcal{P} = \mathcal{S} \circ \mathcal{F} \circ \mathcal{T} : \mathbb{F}_q^n \to \mathbb{F}_q^m$.

2.2. Signature Generation

To sign a message α, consider a cryptographic hash function $\mathcal{H} : \{0,1\}^* \to \mathbb{F}_q^m$, and obtain the digest $d = \mathcal{H}(\alpha)$. Compute $x = \mathcal{S}^{-1}(d)$. To compute $y = \mathcal{F}^{-1}(x)$, every UOV layer must be inverted recursively. Randomly choose values of $x_1, \ldots, x_{v_1}$ and substitute them into $\mathcal{F}$. Due to its construction, assigning values to the vinegar variables will lead to a system of linear equations formed by the first o_1 polynomials in $x_{v_1+1}, \ldots, x_{v_2}$, that may be solvable through Gaussian elimination. If the system does not have a solution, the vinegar variables need to be randomly chosen again. The newly-obtained variables may then be substituted into the remaining polynomials. This process can be repeated for all layers, resulting in $y = (x_1, \ldots, x_n)$. Finally, compute $\sigma = \mathcal{T}^{-1}(y)$.

2.3. Signature Verification

To verify a signature, compute $d' = \mathcal{P}(\sigma)$. If $d = d'$, then the signature is accepted, and otherwise rejected.

3. Obtaining a Cyclical Structure

We apply the rationale given by Petzoldt *et al.* in [Petzoldt et al. 2010a] to the key generation step of the Rainbow scheme. We restrict ourselves to the case of $u = 2$, but the generalised process is akin [Petzoldt 2013, Section 7.2]. Recall that the public key of Rainbow is the composition of three maps, $\mathcal{P} = \mathcal{S} \circ \mathcal{F} \circ \mathcal{T}$. Let $\mathcal{Q} = \mathcal{F} \circ \mathcal{T}$.

If we fix coefficients $t_{ij} \in \mathcal{T}$, the public key composition represents a linear relation between coefficients $q_{ij}^{(k)}, f_{ij}^{(k)}$ of the monomial $x_i x_j$ in the k-th component of $\mathcal{Q}$ and $\mathcal{F}$ respectively, with the form

$$q_{ij}^{(k)} = \sum_{r=1}^{n} \sum_{s=r}^{n} \alpha_{ij}^{rs} f_{rs}^{(k)}, \quad \alpha_{ij}^{rs} = \begin{cases} t_{ri} t_{si} & \text{if } i = j, \\ t_{ri} t_{sj} + t_{rj} t_{si} & \text{otherwise} \end{cases}, \tag{2}$$

$k \in \{v_1 + 1, \ldots, n\}$ and $i, j \in \{1, \ldots, n\}$. Eq. 2 can be reduced if we consider that $\mathcal{F}$ does not allow quadratic monomials with only oil variables. Hence,

$$q_{ij}^{(k)} = \sum_{r=1}^{v_1} \sum_{s=r}^{v_2} \alpha_{ij}^{rs} f_{rs}^{(k)}, \ k \in O_1, \quad q_{ij}^{(k)} = \sum_{r=1}^{v_2} \sum_{s=r}^{n} \alpha_{ij}^{rs} f_{rs}^{(k)}, \ k \in O_2. \tag{3}$$

Operating on these coefficients will lead us to useful relations. Let $D_w = v_w(v_w + 1)/2 + v_w o_w$ be the number of quadratic terms in the central polynomials of the w-th layer, and $D = n(n+1)/2$ be the number of quadratic terms in the public polynomials. Further, define a monomial ordering that acts as following. The D_w monomials that appear only in the central polynomials of the w-th layer shall appear before the D_{w+1} monomials, with $w \in \{1, \ldots, u\}$. The remaining $D - D_u$ quadratic monomials come after all layers. The linear and constant monomials come last. Lexicographic ordering is used to order the elements inside of these "blocks".

These definitions enable us to represent Eq. 3 in a more compact form. Define a $D_2 \times D_2$ matrix as $A = (\alpha_{ij}^{rs}),\ 1 \le i \le v_2, i \le j \le n$ (rows), $1 \le r \le v_2, r \le s \le n$ (columns), with the above ordering. Additionally, you can create similar matrices for the coefficients of $\mathcal{P}$, $\mathcal{Q}$ and $\mathcal{F}$, as pictured in [Petzoldt 2013, Figure 7.5]. By contemplating only the coefficients of quadratic terms, we have matrices P, Q, F with D_2 columns. Let A_{11} be the upper left $D_1 \times D_1$ sub-matrix of A, S_{22} be the lower right $o_2 \times o_2$ sub-matrix of S, and other sub-matrices defined analogously. By also specifically partitioning P and F, we get the following relations:

$$P = S \cdot Q \rightarrow \begin{pmatrix} B_1 & C_1 \\ & B_2 \end{pmatrix} = \begin{pmatrix} S_{11} & S_{12} \\ S_{21} & S_{22} \end{pmatrix} \cdot \begin{pmatrix} Q_{11} & Q_{12} \\ Q_{21} & Q_{22} \end{pmatrix}, \tag{4}$$

$$Q = F \cdot A^T \rightarrow \begin{pmatrix} Q_{11} & Q_{12} \\ Q_{21} & Q_{22} \end{pmatrix} = \begin{pmatrix} F_1 & 0 \\ \multicolumn{2}{c}{F_2} \end{pmatrix} \cdot \begin{pmatrix} A_{11}^T & A_{12}^T \\ A_{21}^T & A_{22}^T \end{pmatrix}. \tag{5}$$

With this strategy, we can configure the $m \times D_1$ matrix B_1 and the $o_2 \times (D_2 - D_1)$ matrix B_2 with elements that generate a small structure, deriving the central map from $\mathcal{P}$.

3.1. Key Generation

Randomly choose vectors $a^{(1)} \in \mathbb{F}_q^{D_1}, a^{(2)} \in \mathbb{F}_q^{D_2 - D_1}$, and set

$$b_{ij}^{(1)} = a^{(1)}_{((j-i) \pmod{D_1})+1}, \qquad b_{ij}^{(2)} = a^{(2)}_{((j-i) \pmod{D_2 - D_1})+1}. \tag{6}$$

Choose at random a map $\mathcal{S}$ with the additional restriction that S_{22} must be invertible. Also generate randomly a map $\mathcal{T}$ and compute A through Eq. 3. If A or A_{11} are not invertible, choose another $\mathcal{T}$. To obtain $\mathcal{F}$, by Eq. 4, compute $(Q_{11}\ Q_{21})^T = S^{-1} \cdot B_1$, and obtain the quadratic coefficients of the central polynomials for the first Rainbow layer through Eq. 5, with $F_1 = Q_{11} \cdot (A_{11}^{-1})^T$. Again, by Eq. 5, compute $Q_{12} = F_1 \cdot A_{21}^T$ and by Eq. 4, $Q_{22} = S_{22}^{-1} \cdot (B_2 - S_{21} \cdot Q_{12})$. Obtain the quadratic coefficients for the second layer by Eq. 5 with $F_2 = (Q_{21}\ Q_{22}) \cdot (A^{-1})^T$. Choose linear and constant terms of the central polynomials randomly. Finally, the private key is the triple $(\mathcal{S}, \mathcal{Q}, \mathcal{T})$, and the public key is composed of the vectors $a^{(1)}, a^{(2)}$, the sub-matrix $C_{11} = S_{11} \cdot Q_{12} + S_{12} \cdot Q_{22}$, and the last $(n+1)(n+2)/2 - D_2$ columns of the matrix P.

The signature generation and verification steps are left unmodified. The new scheme is called CyclicRainbow.

4. Effect of the Construction

As seen in [Petzoldt 2013, Section 9.3], none of the known attacks against the classical Rainbow scheme work better against CyclicRainbow. As such, finding weaknesses in this construction remains an open question. Hence, to prevent efficient instances of these attacks, we suggest parameter sets that are similar to the original Rainbow$(\mathbb{F}_{2^8}, 17, 13, 13)$.

Deriving the size of public keys from the schemes described in Sections 2 and 3, the size for a Rainbow public key is $m \cdot (n+1)(n+2)/2$ field elements, and in the case of CyclicRainbow with two layers, the size is $(m \cdot (n+1)(n+2)/2) - o_1 D_1 - (o_2 - 1)D_2$. Table 1 compares average instances of our scheme to the original Rainbow with regards to various security levels and layer sizes. Note that the reduction factor grows with the increase in the number of polynomials and variables, varying between a half and a third of the original public key size.

Parameters	Security level (bit)	Signature size (bit)	Private key size (KB)	Public key size (KB)
$\text{R}(\mathbb{F}_{2^4}, 17, 23, 17)$ $\text{CR}(\mathbb{F}_{2^4}, 17, 23, 17)$	80	228	21.9	33.4 15.6
$\text{R}(\mathbb{F}_{2^5-1}, 14, 19, 14)$ $\text{CR}(\mathbb{F}_{2^5-1}, 14, 19, 14)$	80	256	17.1	25.3 12.0
$\text{R}(\mathbb{F}_{2^8}, 17, 17, 13)$ $\text{CR}(\mathbb{F}_{2^8}, 17, 17, 13)$	80	344	19.1	25.1 10.4
$\text{R}(\mathbb{F}_{2^8}, 26, 16, 17)$ $\text{CR}(\mathbb{F}_{2^8}, 26, 16, 17)$	100	472	45.0	59.0 21.7
$\text{R}(\mathbb{F}_{2^8}, 36, 21, 22)$ $\text{CR}(\mathbb{F}_{2^8}, 36, 21, 22)$	128	632	102.5	136.1 47.3

Table 1. Comparison between instances of the Rainbow scheme with (CR) and without (R) partially cyclic keys. Adapted from [Petzoldt 2013, Table 9.8].

5. Conclusion

By extending the approach presented in [Petzoldt et al. 2010a], we are able to introduce a cyclic structure in the public key of the Rainbow signature scheme, yielding a new scheme featuring public keys with almost a third of their original size. This scheme can be used in computational devices with constraints in storage or networking. Furthermore, it is also shown that these modifications do not impact the security of the scheme. As points of interest for future works, we suggest the inspection of characteristics in the new scheme that may introduce security weaknesses, and the use of pseudo-random number generators to construct the public key, further reducing its size.

References

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

[Ding and Schmidt 2005] 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.

[Kipnis et al. 1999] 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 and Tang 2017] 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 2013] Petzoldt, A. (2013). *Selecting and Reducing Key Sizes for Multivariate Cryptography*. PhD thesis, Technische Universität Darmstadt.

[Petzoldt et al. 2010a] Petzoldt, A., Bulygin, S., and Buchmann, J. (2010a). A Multivariate Signature Scheme with a Partially Cyclic Public Key. In Faugère, J.-C. and Cid, C., editors, *International Conference on Symbolic Computation and Cryptography*, pages 229–235.

[Petzoldt et al. 2010b] Petzoldt, A., Bulygin, S., and Buchmann, J. (2010b). 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 1997] 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.

[Yasuda et al. 2013] 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 et al. 2014a] 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 et al. 2014b] 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.