Malaysian Journal of Computing and Applied Mathematics 2020, Vol 3(1): 35-39

(Online)

MALAYSIAN JOURNAL OF COMPUTING AND APPLIED MATHEMATICS

Efficient GeMSS Based Ring Signature Scheme

Murat Demircioglu[a], *Sedat Akleylek[b], Murat Cenk[c]

[a,c]Institute of Applied Mathematics, Middle East Technical University, Ankara, Turkey
[b]Computer Engineering, Ondokuz Mayis University Samsun, Turkey

*Corresponding author: sedat.akleylek@bil.omu.edu.tr

Received: 12/12/2019, Accepted: 11/03/2020
http://dx.doi.org/10.37231/myjcam.2020.3.1.41

Abstract

The ring signature scheme has an important usage area of public key crypto-system. It can be used for e-voting, as well as leaking information without revealing identity within a group. However, most of these systems relies on traditional crypto-systems which are not secure against quantum computing related attacks. Multivariate cryptography is one of the most popular research areas on quantum resilient crypto-systems. In this work, we propose an efficient ring signature scheme based on GeMSS, where we achieve smaller signature size and faster verification time with respect to other alternatives.

Keywords: post-quantum cryptography, multivariate, GeMSS, ring signature

INTRODUCTION

The security of modern public-key crypto-systems are mainly based on the difficulty of mathematical problems; such as integer factorization problem, discrete log problem, etc. However, these systems will become insecure as the large-scale quantum computers are built. Shor's algorithm Shor, (1999) solves these number theoretic problems on quantum computers in polynomial time. Therefore, there arises a need for alternative public-key systems that will be secure against quantum computer related attacks. This new area of study is called Post-Quantum Cryptography. Multivariate, lattice, isogeny, code and hash based crypto-systems are the candidates for it (Bernstein et al., 2002). Among these, Multivariate crypto-systems are very fast and require modest computational power. Their security is based on *MQ Problem*. Although there exist many signature schemes such as Gui; Petzoldt et al., (2015), Rainbow; Ding and Schmidt, (2005), and UOV Rivest et al., (2001), there is a lack of signature schemes with special properties such as ring signature, bling signature, threshold signature, etc.

In a ring signature scheme, a user in a group is able to sign a message anonymously on behalf of the group, and nobody including the group members cannot reveal the true identity of the signer. This scheme can be used in leaking secrets, e-voting, electronic cash, etc. There are many ring signature schemes based on traditional public-key crypto- systems. The idea of the ring signature was firstly introduced by Rivest et al. (2001) and they proposed the first ring signature scheme based on RSA algorithm. After that, a number of ring signature schemes that are based on multivariate cryptography have been proposed (Petzoldt et al., 2012; Wang et al., 2011; Wang, 2013; Zhang and Zhao, 2014).

In this paper, we propose an efficient multivariate ring signature scheme that is based on GeMSS; Casanova et al., (2017) which is one of the Round 2 candidates in Post-Quantum Standardization Call of NIST.

This paper is organized as follows. In Section II, we introduce the concept of ring signature scheme and multi- variate crypto-system. A brief introduction to GeMSS is also given in this section. In Section III, we propose our ring signature algorithm. The public key and signature sizes, and the computation times of the proposed scheme are given in Section IV. We conclude the paper in Section V

PRELIMINARIES

A. Ring Signatures

In a group $\mathcal{R} = \{u_1, \dots, u_1\}$ consisting of t −many possible signers, Ring signature schemes allow a member to sign a message anonymously on behalf of the group. The verifier can easily check if the message is signed by a member of the group. However, nobody including the group members can reveal the identity of the actual signer. A ring signature scheme consists of three algorithms **Key-Gen**, **RingSign**, and **Verify.**

- Keygen (1^{λ}) is a probabilistic algorithm that takes a security parameter λ as an input, and then generates a public and private key pair (sk, pk). By using this algorithm, each user $u_1 \in \mathcal{R}$ generates their own key pairs to be used in a ring signature scheme.
- RingSign $((d, sk_i, \{pk_1, \dots, pk_t\})$ is a probabilistic algorithm where the user $u_1 \in \mathcal{R}$ signs the message d, and output is the signature σ.
- Verify$(d, \sigma), \{pk_1, \dots, pk_t\})$ is a deterministic algorithm that returns true only if the signature is valid.

A ring signature is assumed to be correct if the following equation holds

$$Pr[Verify((d, RingSign((d, sk_i, \{pk_1, \dots, pk_t\})), \{pk_1, \dots, pk_t\})] \quad (1)$$

for all $i = \{1, \dots, t\}$.

There are two basic security criteria for a ring signature scheme. These are anonymity and unforgeability.

- **Anonymity:** The verifier should not be able to find the actual signer of the given message.
- **Unforgeability:** An adversary not belonging to the group $\mathcal{R}$ should not be able to forge a valid signature on behalf of the group $\mathcal{R}$.

B. Multivariate Cryptography

The basic objects of multivariate cryptography are systems of multivariate quadratic polynomials in (2).

$$\begin{aligned} f^{(1)}(x_1, \dots, x_n) &= \sum_{i=1}^{n}\sum_{j=1}^{n} f_{ij}^{(1)} \cdot \sum_{i=1}^{n} f_i^{(1)} \cdot x_i + f_0^{(1)} \\ f^{(2)}(x_1, \dots, x_n) &= \sum_{i=1}^{n}\sum_{j=1}^{n} f_{ij}^{(2)} \cdot \sum_{i=1}^{n} f_i^{(2)} \cdot x_i + f_0^{(2)} \\ &\vdots \qquad\qquad\qquad \vdots \\ f^{(m)}(x_1, \dots, x_n) &= \sum_{i=1}^{n}\sum_{j=1}^{n} f_{ij}^{(m)} \cdot \sum_{i=1}^{n} f_i^{(m)} \cdot x_i + f_0^{(m)} \end{aligned} \quad (2)$$

Let F be a finite field. The main idea is to choose the central map $\mathcal{F}: F^m \to F^n$ which is a multivariate system of easily invertible quadratic polynomials. After the choice of $\mathcal{F}$, two affine linear invertible maps $\mathcal{S}: F^m \to F^m$ and $\mathcal{T}: F^n \to F^n$ are chosen to hide the structure of the central map. Therefore, public-key is $\mathcal{P} = \mathcal{S} \circ \mathcal{F} \circ \mathcal{T}: F^m \to F^n$, and private key is $(\mathcal{S}, \mathcal{F}, \mathcal{T})$.

The security is based on the **MQ Problem**: Given m multivariate quadratic polynomials $f^{(1)}(x), \dots, f^{(m)}(x)$ in n variables $x_1, \dots, x_n$ as stated in (2), find a vector $\bar{x} = (x_1, \dots, x_n)$ such that $f^{(1)}(\bar{x}) =$

$\cdots = f^{(m)}(\bar{x}) = 0$. The MQ problem (for $m \approx n$) is proven to be NP-hard even for quadratic polynomials over F_2 (Garey & Johnson, 1979). The generic multivariate signature scheme consists of:

- **Signature Generation:** In order to sign a message M, the signer uses a hash function $\mathcal{H}: \{0,1\} \rightarrow F^m$: to compute $h = \mathcal{H}(M) \in F^m$. Then he calculates computes recursively $x = \mathcal{S}^{-1}(h) \in F^m, y = \mathcal{F}^{-1}(x) \in F^n$ and $z = \mathcal{S}^{-1}(y) \in F^n$. At the end, the signature of the message M is $\sigma = \mathcal{S}^{-1}$ σ = $\mathcal{T}^{-1}(\mathcal{F}^{-1}(\mathcal{S}^{-1}(h)))$.
- **Signature Verification**: In order to check if the signature σ is valid for the message M, the verifies computes $h = \mathcal{H}(M)$ and $h' = \mathcal{P}(\sigma)$. If they are same, then the signature is valid, otherwise not.

C. GeMSS

GeMSS Casanova et al., (2017) (Great Multivariate Short Signature) is a multivariate-based signature scheme with small signature size, fast verification process and medium/large public-key size. It is one of the Round 2 candidates in the NIST's Post-Quantum Cryptography Standardization. As well as being in direct lineage from QUARTZ; Patarin et al., (2001), GeMSS borrows some design rationale of the Gui multivariate signature scheme (Ding and Yang, 2013). The main parameters of GeMSS are:

- D, a positive integer that is the degree of a secret polynomial,
- K, the output size in bits of the hash function,
- λ, the security level of GeMSS,
- m, number of equations in the public-key,
- $nb_{ite} > 1$, number of iterations in the public-key,
- n, the degree of a field extension,
- v, the number of vinegar variables,
- Δ, the number of minus, where $m = n - \Delta$.

The public-key in GeMSS is a set $P = (f_1, \dots, f_m) \in F^2[x_1, \dots, x_{n+v}]^m$ of m quadratic equations in $n + v$ variables. The secret-key is composed of a couple of invertible matrices $(\mathcal{S}, \mathcal{T}) \in GL_{n+v}(F_2) \times GL_n(F_2)$ and a polynomial $\mathcal{F} \in F_{2^n}[X, v_1, \dots, v_v]$.

There are three main algorithms of GeMSS; key generation, signing and verification processes. Let $F = F_2$ and choose $nb\_ite = 4$ as in QUARTZ (Patarin, 2001).

1) Let *GKeyGen* be the function to generate GeMSS keypair (pk, sk).
   - Input: GeMSS parameters (λ, D, n, v, m)
   - Output: GeMSS keypair $(sk, pk) = (\mathcal{S}, \mathcal{F}, \mathcal{T}(\mathcal{P}))$.
2) Let *GSign* be the function to generate a GeMSS signature σ for a given message M.
   - Input: GeMSS private-key $sk = (\mathcal{S}, \mathcal{F}, \mathcal{T})$., message M, repetition factor nb_ite.
   - Output: Signature σ = $(\mathcal{S}nb\_ite, X\, nb\_ite, \dots, X_1) \in F^{m+nb\_ite(n+v-m)}$.
3) Let *GVer* be the function to verify if the given GeMSS signature is valid.
   - Input: Signature σ, GeMSS public key sk, message M, repetition factor nb_ite
   - Output:$\mathcal{S}_0 \in F^m$. If it is equal to zero, then the signature is valid. Otherwise, it is not valid.

GEMSS BASED RING SIGNATURE SCHEME

In this section, we propose a new multivariate ring signature scheme based on GeMSS signature algorithm. Since the propose scheme is mainly based on the verification algorithm, GeMSS is a perfect choice with its fast verification time and small signature size.

Let $\mathcal{R} = (u_1, \dots, u_t)$ be a group of t users.

Key Generation: Each user $u_i \in \mathcal{R}$ generates a key pair $(sk_i, pk_i) = ((\mathcal{S}_i, \mathcal{F}_i, \mathcal{T}_i), \mathcal{P}_i)$ by using the key generation function *GKeyGen* of GeMSS, where

$$\begin{matrix}(\mathcal{S}_i, \mathcal{T}_i) \in GL_{n+v}(F_2) \times GL_n(F_2) \\ \mathcal{F}_i \in F_{2^n}[X, v_1, \dots, v_v] \\ \mathcal{P}_i = F^2[x_1, \dots, x_{n+v}]^m\end{matrix} \quad (3)$$

The group public key is the concatenation of the public keys of all users, i.e. $\mathcal{P} = \mathcal{P}_1 \| \mathcal{P}_2 \| \dots \mathcal{P}_i$. Each user ui keeps their private key $sk_i = (\mathcal{S}_i, \mathcal{F}_i, \mathcal{T}_i)$ as secret.

Signature Generation: In order to sign a message M on behalf of the group $\mathcal{R}$, a user u_i should follow the following steps:

1) Compute the hash of the message M and take first m-bits

$$h = \mathcal{H} \in F_2^m \quad (4)$$

2) Choose random vectors $\sigma_1, \dots, \sigma_{i-1}, \sigma_{i+1}, \sigma_t \in F_2^{[m+nb\_ite(n+v-m]t}$, and then compute

$$\bar{h} = h - \sum_{j=1, j\neq i}^{t} GVer(\sigma_j, pk_j, M, nb\_ite) \quad (5)$$

3) Use private key sk_j to compute a vector σ_i such that $GVer(\sigma_j, pk_j, M, nb\_ite) = \bar{h}$.

The ring signature for the message M is $\sigma = (\sigma_1, \dots, \sigma_t) \in F_2^{[m+nb\_ite(n+v-m]t}$

Signature Verification: In order to check if the given signature σ is valid for the message M, the verifier follows the following steps:

1) Compute the hash of the message M and take first m-bits:

$$h = \mathcal{H} \in F_2^m \quad (6)$$

2) Use the group public key and compute

$$\bar{h} = \sum_{j=1}^{t} GVer(\sigma_j, pk_j, M, nb\_ite) \quad (7)$$

If $\bar{h} = h$ holds, then the signature is valid. Otherwise, the given signature for the message M is not valid.

PERFORMANCE ANALYSIS

Table 1 shows the parameters for different security levels of GeMSS that are given in (Casanova et al., (2017) Section 3).

Table 1: Performance Analysis of GeMSS

	pk size (kB)	Sign. size (bit)	sign (ms)	verify (ms)
GeMSS128	352.18	258	260	0.041
GeMSS192	1,237,960	411	694	0.117
GeMSS256	3,040,690	576	1,090	0.336

We use this table to calculate the signature size and approximate calculation time of our proposed ring signature scheme. Size of the group public key $\mathcal{P}$ can be calculated by simply multiplying the number of group members with the size of a public key for the chosen security level. In order to calculate the size of the ring signature, we sum up m-bits from the hash of the message, size of the *nb_ite* (which is taken constant 4 ≈3-bits), and t −many sizes of signatures where t is the number of group members. In order to sign a message on behalf of the group, a user u_i will perform $t-1$ evaluations of $GVer$, and 1 evaluation of *GSign* functions. The verification can be done by t evaluations of *GVer* function.

CONCLUSION

GeMSS, GUI and Rainbow algorithms are multivariate based cryptosystems that are proposed in the NIST's competition. If we compare the size of their key and signature, and performance on their reference implementation results under the same security levels, one can see that the GeMSS and GUI provides smaller signature sizes and faster verification times with respect to Rainbow. If we compare GeMSS and GUI, we will find that GeMSS provide smaller public key and signature sizes, and much faster verification time. Furthermore, as the security level increases, GeMSS achieves faster signature generation time. Since our ring signature scheme mainly based on signature verification algorithm as stated above, using GeMSS as a signature algorithm in a ring signature scheme will result in a faster evaluation time and smaller signature sizes with respect to the ring signature schemes; Akleylek et al., (2018) and Mohamed & Petzoldt, (2017) that are based on GUI and Rainbow, respectively.

References

Akleylek S, Demircioglu M and Cenk M. (2018). GUI Based Ring Signature Scheme, *proceedings of the 18th Central European Conference on Cryptology (CECC 2018), Smolenice*.

Bernstein D J. Buchmann J. and Dahmen E. (2002). Post Quantum Cryptography, Springer, 2009 *Berlin: Springer-Verlag*, 533–547.

Casanova A, Faugere J, MacarioRat G, Patarin J, Perret L and Ryckeghem J. (2017). GeMSS: A Great Multivariate Short Signature, *Research Report*, Available at https://hal.inria.fr/hal-01662158.

Ding J, and Schmidt D S. (2005). Rainbow, a new multivariate polynomial signature scheme, *ACNS, LNCS, 3531,* 164-175. Springer.

Ding J and Yang B. (2013). Degree of regularity for HFEv and HFEv-, In Philippe Gaborit, editor, Post-Quantum Cryptography - 5th International Workshop, PQCrypto 2013, Limoges, France, June 4-7, 2013. *Proceedings, 7932 of Lecture Notes in Computer Science*, 52-66. Springer.

Garey M R, and Johnson D S. (1979). *Computers and Intractability:* A Guide to the Theory of NP-Completeness, W.H. Freeman and Company.

Kipnis A, Patarin L and Goubin L. (1999). Unbalanced Oil and Vinegar Schemes, *EUROCRYPT 1999, LNCS, 1592*, 206-222. Springer.

Mohamed M S E and Petzoldt A. (2017). RingRainbow – An Efficient Multivariate Ring Signature Scheme. *AFRICACRYPT, LNCS 10239, 3-20.* Springer, 2017.

Patarin J, Courtois N, and Goubin L. (2001). Quartz, 128-bit long digital signatures", In David Naccache, editor, Topics in Cryptology - CTRSA 2001, The Cryptographer's Track at RSA Conference 2001, San Francisco, CA, USA, April 8-12, 2001, *Proceedings, 2020 of Lecture Notes in Computer Science,* 282-297. Springer, 2001.

Petzoldt A, Bulygin S, Buchmann J. (2012). A Multivariate Threshold Ring Signature Scheme, *AAECC 24,* 255 - 275.

Petzoldt A, Chen M S, Yang Y B, Tao C, and Ding J. (2015). Design Principles for HFEv- based Signature Schemes, *ASIACRYPT 2015 - Part 1, LNCS*, *9452,* 311-334.

Rivest R L, Shamir A, and Tauman Y. (2001). How to Leak a Secret, in: Cryptology–Asiacrypt 2001, in: *LNCS, 2248, Springer-Verlag, Berlin*, 552–565.

Shor P W. (1999). Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer, *SIAM Review 41*(2): 303-332.

Wang L. (2013). A New Multivariate-based Ring Signature Scheme*, Applied Mechanics and Materials, 347-350.*

Wang S, Ma R, Zhang Y and Wang X. (2011). Ring signature scheme based on multivariate public key cryptosystems, *Computers and Mathematics with Applications 62*, 3973-3979.

Zhang J, Zhao Y. (2014). A New Multivariate Based Threshold Ring Signature Scheme, *NSS 14, LNCS, 8792*, 526 - 533. Springer.