Malaysian Journal of Computing and Applied Mathematics 2019, Vol 2(2): 25-31

(Online)

MALAYSIAN JOURNAL OF COMPUTING AND APPLIED MATHEMATICS

New Signature Algorithm Based on Concatenated Rank Codes

Roumaissa Mahdjoubi[a], Sedat Akleylek[b], Guenda Kenza[c]

[a,c] Faculty of Mathematics, *Univesity of Science and Technology Houari Boumedien*, Algiers, Algeria
[b] Ondokuz Mayis University, Samsun, Turkey

*Corresponding author: mahdjoubi.roumaissa@gmail.com

Received: 06/05/2019, Accepted: 22/10/2019

Abstract

In this paper we propose a new rank code based signature scheme that used a concatenation of the LRPC and the λ-Gabidulin codes. Our construction benefits from the decoding algorithm of both of codes a considerable security levels with a moderate public key size.

Keywords: Rank metric, Signature algorithm, λ-Ganidulin code, LRPC codes.

Introduction

In 1978, McEliece introduced the code based cryptography and opened the problem of finding an efficient signature scheme to solve. Until now, there is no efficient algorithm known due to the large public key of CFS scheme (Courtois et al, 2001) and the large signature size of Fiat-Shamir heuristic (Stern, 1996) and a slow signing algorithm of them. In Santini et al. (2018) there was proposed an algorithm which provided a reduced key size from the structure of the codes used but it had a large signature size. Those schemes are not practical since they have to repeat the protocol many times in order to guarantee the correctness and security of the message, and they are vulnerable to attacks such as key recovery and reaction attacks.

In 1991, Gabidulin introduced an analogue to the code based cryptography called rank based cryptography. The main advantage is the reduction of key size of the public key but these codes are very structured. Recently Gaborit et al. (2015) proposed a new rank signature algorithm based on LRPC codes similar to NTRU in Hamming metric. It was submitted to the NIST call but it has been withdrawn due to an attack which recover its drawback; the very low weight of the public code's codewords (Debris-Alazard and Tillich, 2018). The main problem that the signatures scheme are based is the Syndrome Decoding problem (SD) which is NP-complete in Hamming metric, while in the rank metric, this problem is proved to be hard in Gaborit et al. (2014). Many attacks were developed to solve this problem and classified into combinatorial and algebraic attack which are both feasible for specific parameters.

Many Attacks on the signatures schemes were developed such as the information leakage attack and the forgery information attack. They are efficient since they can recover the hidden structure of the public key by the information leaking from real signatures, and the reaction attack that recover the reaction of Bob to recover the structure of the code.

Most efforts in the rank-based cryptography were based on constructing new public key cryptosystems (PKCs) to countering attacks. Recently, Jon-Lark et al (2018) proposed McNie as a new PKC that submitted to the NIST call (NIST, 2019) and consisted in combining the McElice and the Niederreiter cryptosystems, using parity check matrix of an [*n,k*] codes in the private key and the generator matrix of an [*n,l*] linear code in the public key. It benefited from the construction of 3-QC-LRPC and 4-QC-LRPC a major reduction of the key with high security level. Another proposition on a new signature and identification scheme was given by Bellini et al (2018), it consisted of two signatures which reduce the public and private keys. But it has a large signature size. In addition with a new Identification scheme that resisted to an attack that was proposed also by the authors which made the Stern and Veron Identification scheme broken. Beside to this, the rank metric code has been enriched with the new construction code named *λ*-Gabidulin codes proposed by Lau and Tan (2019), they used such a code in the McEliece-like cryptosystem such that the generator matrix of the public code is multiplied with a scrambler matrix associated to $\lambda \in \mathbb{F}_{q^m}^n$. It is proved to be secure against attacks Overbeck's, anulator polynomial and Frobenious weak attacks (Overbeck, 2008; Horlemann-Trautmann et al., 2016; Otmani et al., 2018).

Our contribution is to provide a new rank signature in code-based cryptography for the *λ*-Gabidulin code and the LRPC codes by their concatenation. The robustness becomes from the hardness of the rank syndrome decoding (RSD) problem and the efficient decoding algorithm of their concatenation.

This paper is organized as follows: Section 2 we introduce an overview on signature schemes and some definitions on the rank metric with the RSD problem. Then in section 3, we describe the suggested signature scheme based on the RSD problem with the desired concatenation code. The security analysis is studied in section 4. Finally, we conclude our work.

Preliminary

A. Overview on signatures schemes

Generally, all signatures schemes consist of three steps or more precisely algorithms:

a. Generation of pair of keys : public and secret.
b. Construction of the signature using a cryptosystem (McEliece or Niederreiter) with the secret key and a hash function on message *M*.
c. Verification of the signature if it is valid using the public key.

The conditions that every signature should achieve are as follows:

d. Message authentication: The sender of the message is authentic.
e. Integrity of the message: Message has not been modified during transmission.
f. Non repudiation: The sender of a message cannot deny the creation of the message.

B. Background on rank metric codes

Let F*q* be a finite field of *q* elements and let F*qm* be an extension field of degree *m*. Let $x = (x_1,...,x_n)$ be a vector over F*qm* and $(a_1,...,a_m)$ be a basis of F*qm* over F*q* such that $a_i \in$ F*q* for $i = \{1,...,m\}$ and $x_j = \sum_{i=1}^{m} \alpha_{ij} a_i$ for $j = \{1,...,n\}$.

The maximal number of elements x_j that are linearly independent over F*q* define the rank of *x* over F*q* which denoted by *rk*(*x*|F*q*). The rank distance between two vectors *x* and $y \text{ in } \mathbb{F}_{q^m}^n$ is : $d_r(x,y) = \text{rank}(x - y|\text{F}q)$.

Any code *C* of length *n* and dimension *k* over F*qm* has a minimum rank distance $d_r(C) = d_r = min\{d_r(x,y)|x,y \in C, x \neq y\}$ is a rank metric code, verifying the Singleton bound $d \leq n - k + 1$.

If this inequality is achieved the code will be a Maximum rank distance (MRD) codes for $m \geq n$. Therefore, we say that the code correct *t* errors if t= $\lfloor \frac{d-1}{2} \rfloor$.

The *k* × *n* generator matrix *G* of a MRD code is defined for any set of elements $g_1,...,g_n$ from F*qm* that are linearly independent over F*q* and its parity check matrix *H* which has for any elements from F*qm* linearly independents over F*q* the following definition

$$G = \begin{bmatrix} g_1 & g_2 & \dots & g_n \\ g_1^{[1]} & g_2^{[1]} & \dots & g_n^{[1]} \\ \vdots & \vdots & \ddots & \vdots \\ g_1^{[k-1]} & g_2^{[k-1]} & \dots & g_n^{[k-1]} \end{bmatrix} \quad (1)$$

and

$$H = \begin{bmatrix} h_1 & h_2 & \dots & h_n \\ h_1^{[1]} & h_2^{[1]} & \dots & h_n^{[1]} \\ \vdots & \vdots & \ddots & \vdots \\ h_1^{[d-2]} & h_2^{[d-2]} & \dots & h_n^{[d-2]} \end{bmatrix} \quad (2)$$

where $g^{[i]} = g^{q^i \bmod n}$ (respectively $h^{[j]} = h^{q^j \bmod n}$is the *i*-th Frobenius power of *g* with *i* = 1*...n*. (respectively the *j*-th Frobenius power of *h* with *j* = 1*...d* − 1).

Definition 1: The F*q*-sub vector space of F*qm* generated by {$g_1,...,g_n$} denoted by *E* is the support of *g* of dimension *r* (where *r* = rank(*g*|F*q*)).
The number of possible supports of length *n* and dimension *r* over F*qm* can be calculated by the Gaussian binomial
$\begin{bmatrix} n \\ r \end{bmatrix}_q \sim (q^{rn})$. This notion is very interesting in the RSD problem to recover the complete coordinates of *g*. In the sequel, we define two known codes in order to construct another one to analyze our application to cryptography. Gaborit et al. (2013) proposed a new codes that are analogy to the LDPC codes as given in the following definition:

Definition 2: The LRPC codes of rank *d*, length *n* and dimension *k* over F*qm*, has $H(h_{i,j})$ as a (*n* − *k*) × *n* paritycheck matrix of weight *d* which represents the dimension of *F* the subspace of F*qm* generated by coefficients of *H*, ie: we write$h_{i,j} = \sum_{l=1}^{d} h_{i,j,l} F_l$. Where {$F_1,...,F_d$} form a basis of *F*.
Recently, a new code had been proposed by Lau and Tan (2019) defined in the rank metric in analogy to the Generalized ReedSlomone codes. A definition of such codes is given as follows:

Definition 3: (*λ*-Gabidulin codes (Lau and Tan, 2019)) Let *g* = $(g_1, \dots, g_n) \in \mathbb{F}_{q^m}^n$ be linearly independent over F*q* and
$\lambda = (\lambda_1, \dots, \lambda_n) \in \mathbb{F}_{q^m}^n$. The *λ*-Gabidlin code over F*qm* of dimension *k* associated with vector *g* and *λ* is the code generated by a matrix G_λ of the form

$$G_\lambda = \begin{bmatrix} \lambda_1 g_1 & \lambda_2 g_2 & \dots & \lambda_n g_n \\ \lambda_1 g_1^{[1]} & \lambda_2 g_2^{[1]} & \dots & \lambda_n g_n^{[1]} \\ \vdots & \vdots & \ddots & \vdots \\ \lambda_1 g_1^{[k-1]} & \lambda_2 g_2^{[k-1]} & \dots & \lambda_n g_n^{[k-1]} \end{bmatrix} \quad (3)$$

and its parity check matrix is given by

$$H_\lambda = \begin{bmatrix} \lambda_1^{-1} h_1 & \lambda_2^{-1} h_2 & \dots & \lambda_n^{-1} h_n \\ \lambda_1^{-1} h_1^{[1]} & \lambda_2^{-1} h_2^{[1]} & \dots & \lambda_n^{-1} h_n^{[1]} \\ \vdots & \vdots & \ddots & \vdots \\ \lambda_1^{-1} h_1^{[n-k-1]} & \lambda_2^{-1} h_2^{[n-k-1]} & \dots & \lambda_n^{-1} h_n^{[n-k-1]} \end{bmatrix} \quad (4)$$

Such codes had been selected in the application of cryptography; the McEliece like cryptosystem and proved out that it can be resistant for the rank syndrome decoding problem (RSD) to known attacks for well chosen parameters.

The Rank Syndrome Decoding problem (RSD) was the most interesting problem studied for more than 20 years ago, to find the codeword x which satisfies the two conditions:
The rank(x|Fq) = r and $Hx^t = s$, with a given integer r, $s \in \mathbb{F}_{q^m}^k$ and H is a $(n-k)\times n$ matrix over Fqm with $k < n$. This problem is NP-hard with a randomized reduction in Gaborit and Zemor (2016) and is proved to be hard in Gaborit et al. (2014) which is convenient for decoding algorithm security.

Proposition 1: Let C_1 and C_2 be a $[n,k_1,d_2]$ LRPC code and a $[n,k_2,d_2]$ λ-Gabidulin code respectively. The concatenation of these two codes is defined as a code $C = (C_1|C_2)$, with parameters $[n = n_1 \cdot n_2, k = k_1 \cdot k_2, d]$ where $d \geq d_1 \cdot d_2$. The code C consists of vectors $v = (v_1, v_2)$ where $v_1 \in C_1$ and $v_2 = \lambda v_1 \in C_2$ with $\lambda \in \mathbb{F}_{q^m}^n$.

This construction increases all the parameters of the code and its decoding algorithm will consider first the decoding algorithm D_1 (Gaborit et al., 2014) of the LRPC code C_1 as the inner code and then the decoding algorithm D_2 (Lau and Tan, 2019) of the λ-Gabidulin C_2 as the outer code. Such decoding algorithm is an error/erasure decoder which can correct r errors and r' erasures only when $2r + r' < d$.

New Rank Signature Scheme

For the construction of the scheme, we define the subspace $E = E' + T$ of dimension $t = 2r + r'$ over Fqm such that E' is the subspace of errors of dimension $2r$ and $T \subset E'$ is the subspace of erasures of dimension r'.

a. Key generation:

i) Input

- Invertible matrix S of order $(n - k)$ over Fqm.
- Invertible matrix P of order $(n + r')$ over Fqm as given in Gabidulin (2008).
- A concatenated code over Fqm between LRPC and λ-Gabidulin code with parity check matrix H of size $(n - k) \times n$. Which can decode t errors.

Choose at random a matrix R of size $(n - k) \times r'$ and compute $H_{pub} = S[H|R]P$.

ii) Output : A pair of keys (*pk,sk*) such that
- *pk*: H_{pub}, hash function hash and an integer *l*.
- *sk*: *S*, *P*, *H* and *R* with D_1 and D_2.

b. Signature of message M:

i) Input : A message *M* and *sk*.
- Pick randomly $b \in \{0,1\}^l$.
- Choose r' random independent elements $(e_1,...,e_r') = e$ of Fq^m.
- Compute h = hash($M|b$).
- Decode $h' = S^{-1}h^{\mathsf{T}} - Re^{\mathsf{T}}$ by the decoding algorithms D_1 and then by D_2.
- If the decoding algorithm works and outputs $e' = (e_{r'+1},...,e_{n+r}')$ with rank$(e'|F_q) = 2r+r'$ then the signature outputs $\sigma(e''(P^{\mathsf{T}})^{-1},b)$ where $e'' = (e_1,...,e_{n+r}')$. Else return step 1.

ii) Output : The signature $\sigma = (e''(P^{\mathsf{T}})^{-1},b)$.

c. Verifying of validity:

i) Input : *pk* and σ.
- Check if rank$(e'') \leq t$.
- Check if $H_{pub}e''^{\mathsf{T}} = h$ then h = hash($M|b$).

ii) Output : ”Valid” if $H_{pub}e''^{\mathsf{T}}$ = hash($M|b$), else ”Invalid”.

After generating the pair of keys, the signer initialized small vector *b* over F*q* in order to compute it with the hash of the message *M*, and choose randomly a vector $(e_1,...,e_r') = e$ in a random support *T* over F*qm*. Then, the signer decode the hash value by performing the decoding algorithm of the dual matrix of the public code using D_1 and D_2 with *t* errors. If such decoding returned to give $(e_1,...,e_n)$ of rank weight $t = 2r + r'$ then the signature will be transmitted to the verifier as a couple of $(e''(P^{>})^{-1})$ with $e'' = (e_1,...,e_{n+t1})$ which will assure that the number of errors/erasures is exactly *t* and that the $H_{pub}e'^{\mathsf{T}}$ = hash($M|b$). If the decoding does not work or the verification is not valid then it will outputs ”Invalid”, else output will be ”Valid”. Since this signature presents a variant of the RankSign (Lau and Tan, 2019) we set the complexity of the signature and the verification algorithm about $(n - k)(n + r')\log_2(q)$ and the public key size of about $(n - k)(k + r')m\log_2(q)$ while the signature size equals $(m + n + r')t\log_2(q)$.

To ensure the correctness of the signature we check the decoding capability of e''^{-1} and the output $e' = (e'_1, \ldots, e'_{n+r'})$. Hence, we decode first by $D_1 : D_1(h') = C(h'')$ then by $D_2 : D_2(h'') = e'$ for an output e' of rank weight less than or equal to *t* and the verifier should obtain $H_{pub}e''^{\mathsf{T}} = H_{pub}h'^{\mathsf{T}} = H_{pub}(S^{-1}h - Re'^{\mathsf{T}})^{\mathsf{T}} = e'$. We can write $H_{pub}e''^{\mathsf{T}} = h \Rightarrow [R|H\}Pe^{\mathsf{T}} = S^{-1}h^{\mathsf{T}} \Rightarrow [HP_1e'^{\mathsf{T}}|\ RP_2e^{\mathsf{T}}] = S^{-1}h^{\mathsf{T}}$ where P_1 and P_2 are sub-blocks of *P*. By applying the decoding algorithm we get the output of decoding for $S^{-1}h^{\mathsf{T}} - RP_2e'^{\mathsf{T}}$ which is e'. Therefore, we can decode correctly only when the rank weight of e'' and $S^{-1}h - Re'^{\mathsf{T}}$ is less or equal to the decoding capability *t*.

Security Analysis

The security of this signature algorithm is based on the difficulty of RSD problem, it can benefits from such a problem to withstand existed attack. Which has been developed over the years and categorized as attacks; on the PKC like the *message recover* which used the decoding attack and like the *public key recover* which used the algebraic attack. Rather than this, they used the attacks of Rank Syndrome Decoding problem and classified into combinatorial and algebraic attacks. Attacks on the message like the *information set decoding* which was developed in 1962 by Prange (1962) as a technique of direct attack on the message. It is enough to find a set of *k* information positions with no errors. In the rank metric, it has been converted into the error support attack (Gaborit, Ruatta and Schrek, 2016). Another type which attack directly on the signature like the forgery attack which also proposed to forge the real signature algorithm and

consists in generating the valid signature of a message M that has not been signed by the right person.

The proposed signature has the property of mixing two interested codes from the rank metric. The application of the LRPC codes had a moderate public key size. While the λ-Gabidulin code had for chosen parameters a fast run time and resistant to Overbeck attack. In the attack of Otmani et al. (2018), it was given a particular case for which their attack can't be feasible on RankSign; if the minimum distance of the public code is not too small ($d \geq 3$) and $(n-k)d$ is not too close too n. Roughly speaking, this attack can be feasible when it is provided 3 condition naturally given by the RankSign; $m = (r - t')(d + 1)$, $n - k = d(r - t - t')$ and $n = (n - k)d$ with t' is the dimension of subspace T' for which the attacker choose the matrix H' for decoding algorithm. With respect to these conditions we choose parameters to withstand such an attack.

Table 1 we suggest a set of parameters for LRPC (Gaborit et al., 2014) and λ-Gabidulin (Lau and Tan, 2019). Their public key sizes (bits) with a moderate public key size of their concatenation.

Table 1. Public Key Sizes with Security Level 120

Type of code $[n,m,k,q,t,r^0,r]$	Public key size
[16,18,8,216,2,4,6] LRPC	23040
[79,83,31,2,8 = a] λ-Gab	15430
[1264,83,248,2,48,8,20] Concatenation	21587968

In Table 2 we compare the sizes of signature, secret key and public key with our variant in security level 128. Our variant has larger public key size and secret key size while it is moderate in the signature size.

Table 2. Comparison of Sizes of Our Case with Ranksign, Rank Veron and Rank CVE Signature In Security Level 128

SIGNATURE Scheme (parameters)	$\|sign\|$	$\|sk\|$	$\|pk\|$
RankSign $(n,n-k,m,q,t,r,r^0)$ $(16,8,18,2^{16},2,4,6)$	3456	41472	23040
Rank Veron (q,m,n,k,r,σ,h) $(2,80,64,30,9,219,256)$	1719296	7520	77124
Rank CVE (q,m,n,k,r,σ,h) $(2,80,64,30,9,128,256)$	27389952	5120	310084
Concatenation (n,m,k,q,t,r^0,r) $[1264,83,248,2,48,8,20]$	65040	107265216	21587968

Conclusion

We proposed a concatenation code from LRPC and λ-Gabidulin codes and gave new version of RankSign: signature algorithm which had a moderate public key size and signature size with a considerably high level security. The art of having an efficient and fast signature scheme is an attractive subject to study in the future work.

Acknowledgments

Sedat Akleylek was partially supported by TUBITAK under grant no. EEEAG-117E636.

References

NIST Post-quantum cryptography standardization. (2019). Available from https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Round-1-Submissions.

Lau T.S.C., Tan C.H. (2019). A New Gabidulin-Like Code and Its Application in Cryptography. In: Carlet C., Guilley S., Nitaj A., Souidi E. (eds) Codes, Cryptology and Information Security. C2SI 2019. *Lecture Notes in Computer Science*, vol 11445. Springer, Cham.

Courtois, N, M. Finiasz and N. Sendrier. (2011). How to achieve a McEliece based digital signature scheme, Proc. of Asiacrypt 2001, *Lecture Notes in Computer Science, vol. 2248*, pp. 157-174.

Gabidulin,E. M. (2008). Attacks and counter-attacks on GPT public key cryptosystem. *Designs, Codes and Cryptography*, pp. 171-177.

Gaborit, P., and G. Zémor. (2016). On the Hardness of the Decoding and the Minimum Distance Problems for Rank Codes, *IEEE Transactions on Information Theory*, 62(12), 7245-7252.

Gaborit, P., O. Ruatta, J. Schrek, J. P. Tillich and G. Zemor. (2015). Rank based cryptography: a credible post-quantum alternative to classical. *NIST Workshop on Cybersecurity in a Post - Quantum World*.

Gaborit P., Ruatta O., Schrek J., Zémor G. (2014) RankSign: An Efficient Signature Algorithm Based on the Rank Metric. In: Mosca M. (eds) Post-Quantum Cryptography. PQCrypto 2014. *Lecture Notes in Computer Science*, vol 8772. Springer, Cham.

Gaborit, P., O. Ruatta and J. Schrek. (2016). On the Complexity of the Rank Syndrome Decoding Problem, in IEEE Transactions on Information Theory, 62(2), 1006-1019.

Gaborit, P., G. Murat, O. Ruatta and G. Zmor. (2013). Low Rank Parity Check Codes and their application in cryptography, *in Workshop Codes and Cryptography* (WCC 2013), Bergen.

Prange, E. (1962). The Use of Information Sets in Decoding Cyclic Codes, *IRE Trans.Inform. Theory,* 8(5), 5-9, 1962.

Stern, J. (1996). A new paradigm for public key identification, *IEEE Transactions on Information Theory*, 42(6), 2757-2768.

Santini, P. M. Baldi, G. Cancellieri and F. Chiaraluce. (2018). Hindering reaction attacks by using monomial codes in the McEliece cryptosystem, Available at https://arxiv.org/abs/1805.04722.

Jon-Lark, K., K Young-Sik, G. Lucky, J.K. Myeong and L. Nari. (2018). McNie: A code-based public key cryptosystem, Available at https://arxiv.org/abs/1812.05008.

Bellini, E., F. Caullery, A. Hasikos, M. Manzano, and V. Mateu. (2018). Code-based signature schemes from Identification protocols in the rank metric, *International Conference on Cryptology and Network Security, CANS 2018: Cryptology and Network Security*, pp. 277-298.

Overbeck, R. (2008). Structural attacks for public key cryptosystems based on Gabidulin codes, *Journal of Cryptology*, 21(2), 280-301.

Horlemann-Trautmann, A., K. Marshall and J. Rosenthal. (2016). Considerations for Rank-based Cryptosystems, *In IEEE International Symposium on Information Theory*, pp. 2544-2548.

Otmani, A., H. T. Kalachi and S. Ndjeya. (2018). Improved Cryptanalysis of Rank Metric Schemes Based on Gabidulin Codes. *Designs, Codes and Cryptography*, 86(9), 1983-1996.

Debris-Alazard, T., and J.P. Tillich. (2018). An attack on a NIST proposal: RankSign, a codebased signature in rank metric, Available at https://eprint.iacr.org/2018/339.pdf.