Proc. of the Fifth International Conference on Advances in Computing, Electronics and Communication - ACEC 2017.

ISBN: 978-1-63248-121-4 doi: 10.15224/ 978-1-63248-121-4-28

New efficient techniques to catch lowest weights in large Quadratic Residue codes

Issam Abderrahman JOUNDAN, Said NOUH and Abdelwahed NAMIR

***Abstract*—For a large Quadratic Residue (QR) code C, the problem of finding the minimum weight d is NP-hard and many research techniques have been developed to attack its hardness such as simulated annealing, Multiple Impulse Method, Ant Colony Optimization, Zimmermann algorithms and MIM-FSI method. The true value of the minimum weight in QR codes is known for only lengths less than or equal to 223. In this work, we propose new efficient schemes to catch lowest weights codewords in QR codes. The first proposed scheme Zimmermann-FSI uses the Zimmermann algorithm for searching lowest weights in the sub code SubEQR fixed by a self invertible element of the projective special linear group. The code SubEQR has a small dimension comparing to C itself. This reduction of the dimension permits to reduce considerably the research space size and it is behind the success of the Zimmermann-FSI scheme. This good result has encourages us to continue on reducing again the dimension of SubEQR and to propose the second scheme Zimmermann-FSI-RSC which uses the Zimmermann algorithm to catch lowest weights in a list of sub codes of small dimensions randomly extracted from the sub code SubEQR. The two proposed schemes are validated on all QR codes of known minimum weight. The comparison between MIM-FSI, Zimmermann-FSI and Zimmermann-FSI-RSC on many large QR codes proves the efficiency of the two latest ones in terms of run time reduction and the results quality. The proposed methods performed very well in comparison to previously known results and they yield to some new ones for lengths up to 601.**

***Keywords*—Automorphism group, projective special linear group, Quadratic Residue codes, minimum distance, minimum weight, Multiple Impulse Method, Zimmermann's algorithm, MIM-FSI method.**

I. Introduction

The channel coding technique permits to detect and correct errors by adding redundancy in original data before transmission. In reception, the selected decoder uses the added information in correction. Each linear error correcting code C(n,k,d) can be generated by a binary generator matrix of k rows and n columns. k is called the dimension and n is the length of C.

Issam Abderrahman JOUNDAN, Said NOUH and Abdelwahed NAMIR.
TIM LAB, Faculty of Science Ben M'SIK , University Hassan II, Morocco

The weight of a word is the number of ones it contains. The error-correcting capability of a linear code is equal to its lowest non-zero weight.

For each prime n of the form: $n \equiv \pm 1 (mod\ 8)$, the Quadratic Residue code QR(n)=QR(n,(n+1)/2,d) of length n is generated by the polynomial $g(x) = \prod_{i \in Q} (x - \beta^i)$ where Q is the collection of all nonzero quadratic residue integers modulo n : $Q = \{ j^2 \ mod\ n : 1 \le j \le n-1 \}$ and β is a primitive n^{th} root of unity in GF(2^m), where m is the smallest positive integer such that n divides 2^m - 1. Each QR code can be extended to a EQR(n+1,(n+1)/2,d+1) code whose codewords are obtained by adjoining a parity-check bit to a fixed position ∞ of every codeword of the QR(n) code.

QR codes are a family of powerful error correcting codes, they have potential applications in modern communication systems and digital signal processing systems and they are recently decoded by fast and efficient methods [1-5]. They are used to construct quantum synchronizable codes [6]. In [7], authors have generalized QR codes over Galois rings using the Galois Theory. In [8], a self-dual code and a formally self-dual code are obtained from extended QR codes.

In this paper our work will focused on finding the minimum distance of large Quadratic Residue codes which is a NP-complete problem as proved in [9].

The Pless identity [10] permits to write the following equality:

$$\text{for j} \le \text{(n-1)/2} : 2j.A_{2j} = \left(n - \left(2j-1\right)\right).A_{2j-1} \qquad (2)$$

With A_i denotes the number of codewords of weight i in QR(n) code and E_i denotes the number of codewords of weight i in EQR(n).

The definition of EQR codes and (2) permit to write the following equality:

$$\text{for j} \le \frac{n-1}{2} : E_{2j} = \frac{n+1}{n+1-2j} A_{2j} = \frac{n+1}{2j} A_{2j-1} \qquad (3)$$

The formula (2) proves that:

$$d\left(QR(n)\right) = d\left(EQR(n)\right) - 1 \qquad (4)$$

PSL_2 is a part of the automorphism group of Quadratic Residue codes. It is the set of permutations over {0,1,2,…,n-1,∞}, of the form $y \to (ay+b)/cy+d$ where a, b, c and d are elements of GF(n) verifying : ad-bc=1. For all values of n, the binary EQR(n) code is invariant under PSL_2 [11].

For a prime $n \equiv -1 (mod\ 8)$, the minimum distance d of a QR(n) code is related to its length by the following Krasikov inequality [12]:

$$d + 1 \le 0.166315\ n \qquad (5)$$

Proc. of the Fifth International Conference on Advances in Computing, Electronics and Communication - ACEC 2017.

ISBN: 978-1-63248-121-4 doi: 10.15224/ 978-1-63248-121-4-28

In [13], the likelihood weight enumerators of some quadratic residue codes are found.

The remainder of this paper is organized as follows. The next section presents some background on Quadratic Residue codes, the projective special linear group PSL_2 and the main related works. The section 3 presents the proposed schemes: Zimmermann-FSI and Zimmermann-FSI-RSC. The section 4 presents the main results. The conclusion and the possible future directions of this research are outlined in section 5.

II. Related works

The determination of the minimum weight d in a linear block code C(n,k,d) permits to know its capability in detecting and in correcting errors or erasures. When the dimension k increases, the size of the search space becomes prohibitively large and exhaustive search becomes not feasible. In [14-21] authors have used many techniques to find the true value of the minimum distances of QR codes for all lengths less than or equal to 223. For more lengths, this metric is still unknown. This section summarizes the most important previous works.

Wallis and Houghten [22] have applied many heuristic search techniques for BCH codes. They concluded that genetic algorithms with a large population size significantly outperformed hill-climbing, tabu search and hybrid techniques (GA – Hill climbing and GA - Tabu Search). In [23] the authors had improve some parameter of GA and get best result for BCH code compared to wallis and simulated Annealing [24] and applied this GA to QR codes of length up to 223.

Instead the turbo decoder used in [25], the MIM method (Multiple Impulse Method) [23] uses the OSD decoder of order 3 and injects errors in many positions. This method has permits to find good results in terms of time and precision.

Leon [26] has proposed an efficient probabilistic method based on information sets and the automorphism group and applied this method to QR codes of length up to 521.

Aylaj and Belkasmi [27] have proposed a new simulated annealing by using new mechanism of moving the search in different regions of solution space by degeneration of energy. They obtained new lower bounds for some linear codes.

Zimmerman algorithm [28] is a general algorithm for computing the minimum distance of a linear code. It is implemented in GAP (package Guava) [29] over fields F_2 and F_3. It is also implemented, in Magma over any finite field. The method by Zimmerman is outlined in Algorithm 1. It is based on the so called information sets. Given a linear code C with parameters [n, k, d] and a generator matrix G, an information set $S = \{i_1, \ldots, i_k\} \subset \{1, \ldots, n\}$ is a subset of k indices such that the corresponding columns of G are linearly independent. Therefore, after permutation of columns and elementary row operations we get a systematic matrix $\Gamma_1 = (I_k \mid A_1)$. Assume that we are able to find m−1 disjoint information sets ($S_1 \cap \cdots \cap S_{m-1} = \emptyset$), then we get m−1 different matrices $\Gamma_j = (I_k \mid A_j)$. Notice that there still may be left $n - k(m-1)$ positions, so that the corresponding columns of G do not have rank k but $k_m < k$, then after applying column permutations and row operations, one gets $\Gamma_m = \begin{pmatrix} I_{k_m} & A \\ 0 & B \end{pmatrix}$. In overall, the number of Γ matrices is m: The first m − 1 will have full rank k, and the last one will have a rank strictly smaller than k.

The idea is to consider an upper bound U, initialized to n −k+1, and a lower bound L, initialized to 1. Then, both bounds are updated after enumerating codewords, and it is checked whether L ≥ U; if so, the minimum weight is U.

The codewords are enumerated as follows: consider all the linear combinations $i \cdot \Gamma_j$ for j = 1, . . . ,m, where $i = (i_1, \ldots, i_k)$ and wt(i) = 1. After computing any linear combination, if the new weight is smaller than U, then U is updated with the new weight. Moreover, after finishing with all linear combinations $i \cdot \Gamma_j$ for j = 1, . . . ,m, the lower bound is increased in m− 1 units (actually one after each Γ_j) for the disjoint information sets. Now the same procedure is repeated for linear combinations $i \cdot \Gamma_j$ for j = 1, . . . ,m and wt(i) = 2. Then, the same is done for wt(i) = 3, and so on until L ≥ U is obtained.

Algorithm 1 (Minimum weight for a linear code C)
Input: The generator matrix G of the linear code C with parameters [n, k, d].
Output: d The minimum weight of C.

```
L := 1;
U := n − k + 1;
w := 1;
while w ≤ k and L < U do
   for j = 1, . . . ,m do
   U := min{U, min{wt(i Γ_j) : i ∈ Fk2 | wt(i) = w}} ;
   end for
   L := (m − 1)(w + 1) + max{0, w + 1 − k + k_m} ;
   w := w + 1;
end while
return U;
```

In [30], we have used an efficient scheme to compute the minimum distance for linear codes. This method is based on reduction of the code dimension and the use of the MIM method on a given sub code fixed by a self invertible permutation σ of the projective special linear group of Extended *Quadratic Residue codes*. The dimension of this sub code is very low comparing to the dimension of C itself .In the next section we will apply the Zimmermann algorithm on this sub code.

III. The proposed schemes

This section presents the Zimmermann-FSI method for finding the lowest weight in large QR codes. The first proposed scheme Zimmermann-FSI works as follows:

Inputs: - n a prime : $n \equiv \pm 1 (mod\ 8)$
- A generator matrix G of EQR(n+1)
Step 1: find an element σ∈PSL$_2$(n): σ^2=1 (self invertible)
Step 2: find the sub code:
SubEQR(n+1,σ)={c∈ EQR(n): σ(c)=c} fixed by σ by

Proc. of the Fifth International Conference on Advances in Computing, Electronics and Communication - ACEC 2017.

ISBN: 978-1-63248-121-4 doi: 10.15224/ 978-1-63248-121-4-28

solving the following system (S) of two fundamental equations:

$$(S)=\begin{cases}\sigma(c)=c\\ c=(Inf,Red)=Inf*G\end{cases}$$

Step 3: find the estimated minimum distance d of SubEQR(n+1,σ) by using the Zimmermann method.
Output: d-1 as estimated minimum distance of QR(n)

The second proposed scheme Zimmermann-FSI-RSC (on Random Sub codes) works as follows:

Inputs: - n a prime : $n \equiv \pm 1 (mod\ 8)$
- A generator matrix G of EQR(n+1)
- N, the umber of random sub codes
Step 1: find an element σ∈PSL$_2$(n): σ^2=1 (self invertible)
Step 2: find the sub code SC:
SC={c∈ EQR(n): σ(c)=c} fixed by σ by solving the following system (S) of two fundamental equations:

$$(S)=\begin{cases}\sigma(c)=c\\ c=(Inf,Red)=Inf*G\end{cases}$$

Step 3:
d←n
For i=1 to N do
- Randomly extract a sub code SSC of SC
- find the minimum distance d' of SSC by using the Zimmermann method.
- if (d'<d) then
d←d'
end If
End For
Output: d-1 as estimated minimum distance of QR(n)

IV. Results and Discussions

This section presents a validation of the proposed method on all binary quadratic residue codes of known minimum distance and its application for finding the minimum distance of some unknown minimum distance.

In the comparison of Zimmermann-FSI with other method, we define the weight gain *WG* as the difference between the lowest weight obtained by the Zimmermann-FSI scheme and that obtained by other method: WG=d(Zimmermann-FSI)-d(Other).

All results have been done using a simple configuration machine: Intel(R) Core(TM) i3-4005U CPU @1.70GHz.

A. Validation of Zimmermann-FSI Method:

In order to validate the proposed method, it is applied on all QR codes of known minimum distance presented in [14-21]. The TABLE I summarizes the obtained results, it shows that the minimum weight found by the Zimmermann-FSI method is equal to the true value of the minimum distance of all QR codes of known minimum distance. Then the Zimmermann-FSI method is validated for length less than or equal to 223. This table shows that the proposed scheme gives the lowest weight codeword in a very short time.

B. Comparison between Ant Colony Optimization (ACO) and Zimmermann-FSI:

The TABLE II compares Ant Colony Optimization (ACO) Method [21] with Zimmermann-FSI .This table shows that Zimmermann-FSI outperforms very well the ACO method in finding the true value of the minimum distance for Quadratic Residue codes of length up to 199.

C. Comparison between Aylaj's SA and Zimmermann-FSI:

The TABLE III compares Aylaj's SA algorithm [27] with Zimmermann-FSI .This table shows that Zimmermann- FSI outperforms very well the Aylaj's SA in finding lowest weight codewords in Quadratic Residue codes.

D. Comparison between MIM and Zimmermann-FSI:

The TABLE IV compares MIM Method [23] with Zimmermann-FSI .This table shows that Zimmermann- FSI outperforms MIM in finding lowest weight codewords for Quadratic Residue codes.

E. Comparison between Zimmermann-FSI scheme and Zimmermann method:

In order to compare the Zimmermann-FSI scheme with the Zimmermann method [28-29], their applications on some QR codes are made. The TABLE V gives the obtained results. It shows that the Zimmermann-FSI scheme greatly outperforms the Zimmermann method on finding lowest weight codewords. The run time of the two methods is 24 hours in the same configuration machine given above.

F. Comparison between MIM-FSI and Zimmermann-FSI:

The TABLE VI compares and summarizes the total run time and the result quality of the two methods MIM-FSI and Zimmermann-FSI. This table shows that Zimmermann-FSI outperforms MIM-FSI in both total run time and in the results quality.

G. Comparison between Zimmermann-FSI and Zimmermann-FSI-RSC methods:

The TABLE VII compares and summarizes the minimum distance found by the two methods Zimmermann-FSI and Zimmermann-FSI-RSC. This TABLE shows that Zimmermann-FSI-RSC outperforms Zimmermann-FSI especially for large codes.

Proc. of the Fifth International Conference on Advances in Computing, Electronics and Communication - ACEC 2017.

ISBN: 978-1-63248-121-4 doi: 10.15224/ 978-1-63248-121-4-28

TABLE I. Validation of Zimmermann-FSI method

QR Codes		True value of the minimum distance	d(Zimmermann-FSI)	d(Zimmermann-FSI-RSC)
n	k			
17	9	**5**	**5**	**5**
41	21	**9**	**9**	**9**
73	37	**13**	**13**	**13**
89	45	**17**	**17**	**17**
97	49	**15**	**15**	**15**
113	57	**15**	**15**	**15**
137	69	**21**	**21**	**21**
193	97	**27**	**27**	**27**
31	16	**7**	**7**	**7**
47	24	**11**	**11**	**11**
71	36	**11**	**11**	**11**
79	40	**15**	**15**	**15**
103	52	**19**	**19**	**19**
127	64	**19**	**19**	**19**
151	76	**19**	**19**	**19**
167	84	**23**	**23**	**23**
191	96	**27**	**27**	**27**
199	100	**31**	**31**	**31**
223	112	**31**	**31**	**31**

TABLE II. Comparison between Zimmermann -FSI and ant colony optimization (ACO) algorithm of Bland

Codes QR		True value of the minimum distance	d(Zimmermann-FSI)	d(ACO)	weight gain WG
n	k				
113	57	15	**15**	16	1
137	69	21	**21**	21	0
193	97	27	**27**	38	11
151	76	19	**19**	19	0
191	96	27	**27**	35	8
199	100	31	**31**	40	9

TABLE III. Comparison between Zimmermann-FSI and Aylaj's SA algorithm

Codes QR		d(SA)	d(Zimmermann-FSI)	weight gain WG
n	k			
383	192	63	**47**	**16**
431	216	75	**47**	**28**
463	232	79	**59**	**20**
479	240	83	**55**	**28**
409	205	68	**47**	**21**
433	217	76	**37**	**39**
449	225	76	**55**	**21**
439	220	72	**47**	**25**

TABLE IV. Comparison between ZIMMERMANN-FSI and MIM methods

Codes QR		d(Zimmermann-FSI)	d(MIM)	weight gain WG
n	k			
313	157	39	39	0
337	169	39	39	0
353	177	41	41	0
401	201	**41**	61	**20**
409	205	**47**	63	**16**
433	217	**37**	67	**30**
449	225	**55**	67	**12**
311	156	35	35	0
359	180	**39**	55	**16**
367	184	**47**	59	**12**
383	192	**47**	59	**12**
431	216	**47**	67	**20**
439	220	**47**	67	**20**

TABLE V. Comparison between Zimmermann-FSI and Zimmermann methods

Codes QR		d(Zimmermann - FSI)	d(Zimmermann)	Total Run Time of Zimmermann -FSI	Run Time of Zimmermann	WG
n	k					
439	220	**47**	**67**	332	2853	**20**
569	285	**59**	**91**	54268	12422	**32**
631	316	**75**	**103**	19944	48447	**28**

TABLE VI. Comparison between Zimmermann-FSI and MIM-FSI methods

QR Codes		d(Zimmermann-FSI)	d(MIM-FSI)	Total Run Time of MIM-FSI	Total Run Time of Zimmermann –FSI
n	k				
439	220	**47**	**47**	438	332
487	244	**55**	**55**	86672	553
503	252	**55**	**55**	42084	9084
521	261	**53**	**53**	226045	709
569	285	**59**	**75**	88518	54268
607	304	**83**	**83**	129550	1384
631	316	**75**	**87**	732833	19944

TABLE VII. Comparison between Zimmermann-FSI and Zimmermann-FSI-RSC methods

QR Codes		d(Zimmermann-FSI)	d(Zimmermann--FSI-RSC)
n	k		
463	232	**55**	**55**
487	244	**55**	**55**
503	252	**55**	**55**
521	261	**53**	**53**
569	290	**59**	**59**
601	301	**79**	**77**

V. Conclusion and perspectives

In this paper we have proposed new efficient schemes to find the minimum weight in large Quadratic Residue codes. These schemes permits to catch codewords of very smallest weight comparing to other known powerful methods. In the perspectives we have to adapt and use these methods to find the minimum weight in other linear codes like BCH codes, Low Density Parity Check codes (LDPC) and convolutional codes.

References

[1] Huang CF., Cheng WR., Yu C. “A Novel Approach to the Quadratic Residue Code”. in Intelligent Information Hiding and Multimedia Signal Processing. Smart Innovation, Systems and Technologies, Springer, vol 64. , 2017.

[2] Yani Zhang, Xiaomin Bao, Zhihua Yuan, Xusheng Wu. “Decoding of the Five-Error-Correcting Binary Quadratic Residue Codes”. American Journal of Mathematical and Computer Modelling. Vol. 2, No. 1, 2017, pp. 6-12.

[3] Yan-Haw Chen, Jack Chang, Ching-Fu Huang, “Decoding of binary quadratic residue codes with hash table”, IET Communications, Vol 10 , No 1 , 2016.

ISBN: 978-1-63248-121-4 doi: 10.15224/ 978-1-63248-121-4-28

[4] Chong-Dao Lee, Yan-Haw Chen, Trieu-Kien Truong, Yaotsu Chang "Algebraic Decoding of Some Quadratic Residue Codes With Weak Locators", IEEE Transactions on Information Theory, Vol 61, No 3, 2015.

[5] Saïd Nouh, Idriss Chana and Mostafa Belkasmi, " Decoding of Block Codes by using Genetic Algorithms and Permutations Set", *International Journal of Communication Networks and Information Security*, Vol. 5, No. 3, 2013.

[6] Xie Y;Yuan J;Fujiwara Y, 2014, 'Quantum synchronizable codes from quadratic residue codes and their supercodes', IEEE Information Theory Workshop, ITW 2014, pp. 172 – 176.

[7] Young Ho Park, Quadratic residue codes over Galois rings, The Korean Journal of Mathematics, Vol 24, No 3 , 2016.

[8] Jian Gao and Fanghui Ma, "Some results on quadratic residue codes over the ring Fp+vFp+v2Fp+v3Fp" , Discrete Mathematics, Algorithms and Applications, Vol 9, No 3, 2017.

[9] A. Vardy, The intractability of Computing the Minimum distance of a Code, *IEEE Transaction on Information Theory*, vol. 43, No. 6, 1997, pp.1757–1766.

[10] V. Pless et al., *Handbook of Coding Theory* (North Holland, 1998).

[11] F.J.MacWilliams and N.J.A.Sloane. *The theory of Error-Correcting Codes (* North-Holland, 1977).

[12] Krasikov, I. and Litsyn, S. 'An improved upper bound on the minimum distance of doubly-even self-dual codes', *IEEE-IT*, Vol. 46, No. 1, 2000,pp.274–278

[13] S. Nouh and M. Belkasmi, "Genetic algorithms for finding the weight enumerator of binary linear block codes", *International Journal of Applied Research on Information Technology and Computing IJARITAC*, N°3, Vol 2, 2011.

[14] D. Coppersmith and G. Seroussi, "On the Minimum Distance of some Quadratic Residue Codes," *IEEE Trans. Inform. Theory*, vol. 30, no. 2,pp. 407-411, Mar. 1984.

[15] N. Boston, "The Minimum Distance of the [137, 69] Quadratic Residue Code," *IEEE Trans. Inform. Theory*, vol. 45, no. 1, pp. 282, Jan. 1999.

[16] D. Kuhlmann, "The Minimum Distance of the [83, 42] Quadratic Residue Code," *IEEE Trans. Inform. Theory*, vol. 45, no. 1, pp. 282, Jan. 1999.

[17] Markus Grassl, "On the Minimum Distance of some Quadratic Residue Codes," *Proc. IEEE Int'l Symp. on Inform. Theory(ISIT)*, Sorrento, Italy, June, 2000.

[18] Wen-Ku Su ,Pei-Yu Shih ,Tsung-Ching Lin ,Trieu-Kien Truong "On the minimum weights of binary extended quadratic residue codes", *ICACT'09 Proceedings of the 11th international conference on Advanced Communication Technology* - Volume 3 IEEE Press Piscataway, NJ, ISBN: 978-8-9551-9138-7

[19] Saouter, Y., Mestre, G. LE. A FPGA implementation of Chen's algorithm *35th International Symposium on Symbolic and Algebraic Computation*, July 2010, Munich, Germany, 2010.

[20] J.A. Bland, D.J. Baylis, A tabu search approach to the minimum distance of error-correcting codes, Int. J. Electron. 79 , 1995, pp. 829–837.

[21] J.A. Bland. Local search optimisation applied to the minimum distance problem. *Advanced Engineering Informatics*, 21, 2007

[22] J. Wallis and K. Houghten, "A Comparative Study of Search Techniques Applied tothe Minumum Distance of BCH Codes," *Conference on Artificial Intelligence and Soft Computing*, Banff, 17-19 July 2002.

[23] Askali M., Azouaoui A., Nouh S., Belkasmi M. "On the Computing of the Minimum Distance of Linear Block Codes by Heuristic Methods", *International Journal of Communications, Network and System Sciences*, 5(11), 2012, pp. 774-784

[24] M. Zhang, F. Ma, Simulated annealing approach to the minimum distance of error-correcting codes, Int. J. Electron. 76, 1994, pp. 377–384.

[25] C. Berrou, S. Vaton, M. Jezequel and C. Douillard, "Computing the Minimum Distance of Linear Codes by the Error Impulse Method," Proceedings of IEEE Globecom, Taipei, 17-21 November 2002, pp. 10-14.

[26] J. Leon, "A probabilistic algorithm for computing minimum weights of large error-correcting codes,"*IEEE Trans. Inform. Theory*, vol. 34, pp.1354–1359, 1988.

[27] Bouchaib AYLAJ and Mostafa BELKASMI, New Simulated Annealing Algorithm for Computing the Minimum Distance of Linear Block Codes. *Advances in Computational Research*, indexed Google Scholar ISSN : 0975-3273, E-ISSN : 0975-9085, Volume 6, Issue 1, pp.-153-158, 2014.

[28] Zimmermann K.-H., Integral Hecke Modules, Integral Generalized Reed-Muller Codes, *and Linear Codes* Technische Universitat HamburgHarburg, Tech. Rep. 3-96, 1996.

[29] The GAP Group. "GAP–Groups, Algorithms, and Programming, Version 4.7.9". 2015. http://www.gap-system.org.

[30] S. NOUH, I. A. Joundan, B. Aylaj, M. Belkasmi, A. Namir "New Efficient Scheme Based on Reduction of the Dimension in the Multiple Impulse Method to Find the Minimum Distance of Linear Codes", International Review on Computers and Software IRECOS, Vol 11, No 9, 2016, pages 742-751.

Issam Abderrahman JOUNDAN received his Master in networks and telecommunications in 2011 from University of Chouaib Doukkali, El Jadida, Morocco. Currently he is doing his PhD in Computer Science at TIM Lab, Faculty of sciences Ben M'Sik, Hassan II university, Casablanca, Morocco. His areas of interest are Information and Coding Theory.

Said NOUH is associate professor at Faculty of sciences Ben M'Sik, Hassan II university, Casablanca, Morocco. He had PhD in computer sciences at ENSIAS (National School of Computer Science and Systems Analysis), Rabat, Morocco in 2014. His current research interests telecommunications, Information and Coding Theory.

Abdelwahed NAMIR is a Professor at Faculty of Sciences Ben M'Sik, Hassan II University of Casablanca, Morocco. He obtained his Doctoral Thesis of State in Digital Methods of the Engineer at EMI (school Engineer's Mohammedia) of Rabat in 1993. His current research interests :Decision-making mathematics, decision-making Computing,Telecommunication.