# A reduced set of submatrices for a faster evaluation of the MDS property of a circulant matrix with entries that are powers of two

Dragan Lambić

Ponos Technology (Switzerland)
University of Novi Sad, Faculty of Education, Sombor (Serbia)
email: dragan.lambic@pef.uns.ac.rs

**Abstract.** In this paper a reduced set of submatrices for a faster evaluation of the MDS property of a circulant matrix, with entries that are powers of two, is proposed. A proposition is made that under the condition that all entries of a $t \times t$ circulant matrix are powers of 2, it is sufficient to check only its 2x2 submatrices in order to evaluate the MDS property in a prime field. Although there is no theoretical proof to support this proposition at this point, the experimental results conducted on a sample of 100 thousand randomly generated matrices indicate that this proposition is true. There are benefits of the proposed MDS test on the efficiency of search methods for the generation of circulant MDS matrices, regardless of the correctness of this proposition. However, if this proposition is correct, its impact on the speed of search methods for circulant MDS matrices will be huge, which will enable generation of MDS matrices of large sizes. Also, a modified version of the make_binary_powers function is presented. Based on this modified function and the proposed MDS test, some examples of efficient 16 x 16 MDS matrices are presented. Also, an examples of efficient 24 x 24 matrices are generated, whose MDS property should be further validated.

## 1 Introduction

The basic feature of cryptographic systems is the resistance against differential and linear cryptanalysis. Such feature can be achieved by using the linear diffusion layer which is based on a matrix with optimal diffusion property, a Maximum Distance Separable (MDS) matrix [1]. However, the multiplication with MDS matrix is expensive in general, so matrices with small elements in the time and frequency domain should be used [2]. An MDS matrix whose all elements are powers of 2 could be particularly useful because the left shift operation could be used instead of the multiplication. In this way the implementation cost could be significantly reduced from the perspective of lightweight cryptography.

In the previous period, a significant effort was made to construct or find MDS matrices with a low software and hardware implementation cost [3-16]. Some approaches for obtaining MDS matrices, such as Cauchy and Vandermonde matrices, have the advantage of being provably MDS [17]. On the other hand, matrices obtained by circulant, Hadamard, or Toeplitz approach need to be checked for the MDS condition, but such approaches reduce the search space significantly by restricting the

number of submatrices [17]. Although such approaches can provide efficient MDS matrices of a moderate size, search for larger MDS matrices is not feasible due to large search space [12].

Another limitation in the search for a efficient MDS matrix is the complexity of the MDS test. Bearing in mind that a matrix is MDS if and only if all its square submatrices are invertible [18], the MDS test [19] should check $(2^t-1)^2$ minors in order to confirm that some $t \times t$ matrix is MDS. Such complexity requires a lot of time and memory for larger dimensions of matrix, which makes search methods inefficient for larger $t$. For this reason, more efficient ways of evaluating the MDS property of a matrix are needed in order to facilitate the search for MDS matrices of a larger size.

A circulant matrix is defined by the elements of its first row and each subsequent row is a right rotation of the previous row [9]. Circulant matrices could be also obtained by using left rotation instead of right. Due to such construction, circulant matrices have many repeated submatrices [17], and a large number of equivalent submatrices [20]. The MDS test for such matrices could be performed on the reduced set which is estimated at $(2^{t-2}-1)^2$ submatrices for a $t \times t$ matrix [20]. This approach significantly reduce the complexity of the test, but such reduction is not sufficient to enable feasibility of the MDS test of circulant matrices of a larger size.

In this paper, a reduced set of matrices, which enables very fast evaluation of the MDS property of a circulant matrix with entries that are powers of 2, is proposed. Although at this point there is no theoretical proof that the evaluation of this set is sufficient in order to confirm MDS property of such matrix, the experimental results show that by using the proposed set, search methods can become much faster. The experimental results are obtained by using the random method and the modified method from the function make_binary_powers [19], which will be also presented in this paper.

## 2 The proposed MDS test for circulant matrices with entries that are powers of 2

The MDS test for circulant matrices could be performed on the reduced set, due to a large number of equivalent submatrices [20]. However, if we consider only circulant matrices whose all elements are powers of 2, the set of submatrices, which needs to be tested in order to evaluate the MDS property in a prime field, could be further reduced. In such case an assumption is made that only the set of all 2x2 submatrices should be tested in order to check whether the matrix is MDS or not. Based on the above, the following proposition is made:

**Proposition:** Under the condition that all entries of a $t \times t$ circulant matrix are powers of 2, it is sufficient to check only its 2x2 submatrices in order to evaluate the MDS property in a prime field.

This proposition is based on the fact that by reducing the set of possible elements of a matrix to only powers of 2, the conditions required for all 2x2 submatrices to be invertible will have a greater impact on the invertibility of larger submatrices. The total number of 2x2 submatrices of $t \times t$ matrix is $(t(t-1)/2)^2$ which is significantly smaller than the number of all submatrices $(2^t-1)^2$. This difference in complexity enables much faster evaluation of MDS property, especially for larger matrices.

At this point there is no theoretical proof to support this proposition, but the experimental results conducted so far indicate that this proposition is true. The experiment conducted on a sample of 100 thousand randomly generated $t \times t$ circulant MDS matrices whose all elements are powers of 2 (for 8

≤ $t$ ≤ 12) shows that results of the full MDS test and the proposed reduced MDS test are the same for each tested matrix. The reason why the experiment with large sample is not conducted on larger matrices is the complexity of the full MDS test which makes difficult to conduct mass testing. For this reason, for $t > 12$, the experiment was conducted only on the limited number of matrices.

The examples of larger matrices included in the experiment are two 16 x 16 circulant matrices for the Goldilocks field ($p = 2^{64}-2^{32}+1$), circ(8388608, 2, 1, 1, 131072, 1, 2048, 4, 32768, 1, 64, 8, 2, 16, 512, 524288) obtained by the modified function make_binary_powers and circ(1, 1, 2, 1, 8, 32, 2, 256, 4096, 8, 65536, 512, 8388608, 268435456, 128, 8192) obtained by the original function make_binary_powers from the reference [19]. Both matrices are confirmed to be MDS by the proposed test and by the full MDS test from the reference [19]. The modified function make_binary_powers will be presented in the next section.

The generation of an efficient 24 x 24 MDS matrix is still an open problem [2]. By using the proposed MDS test, a 24 x 24 circulant matrix circ(67108864, 8388608, 131072, 256, 8, 2, 1, 1, 1048576, 1, 17179869184, 2, 2048, 8192, 1, 2, 16, 1024, 4, 64, 68719476736, 2199023255552, 4503599627370496, 4096) for Goldilocks field ($p = 2^{64}-2^{32}+1$) is obtained, whose all entries are power of 2. This matrix passed the proposed MDS test, but confirmation with full MDS test was not possible due to its complexity for such a large matrix.

When the generation of efficient 16 x 16 MDS matrices over the Mersenne field ($p = 2^{31}-1$) is in question, some advanced search method based on heuristics should be applied, because the original and the modified versions of make_binary_powers function were not able to obtain MDS with all entries that are powers of 2. After several attempts, the modified function generated a 16 x 16 matrix in which one random element remained. By applying another modification of make_binary_powers function which replaces random numbers with numbers such as $2^x \pm 1$ (instead of powers of 2) a matrix circ(2097152, 2, 1, 1, 131072, 1, 2, 512, 16, 1, 32768, 4, 2048, 8, 32, 3) is obtained. The MDS property of this matrix is confirmed by the full MDS test.

The generation of a 24 x 24 MDS matrix with entries that are powers of 2 for the Mersenne field is even more complicated task due to the small size of the field. By using the modified function make_binary_powers a circulant matrix is obtained, which do not have all entries equal to some power of 2. Seven elements remained random. By applying another modification of the make_binary_powers function which replaces random numbers with numbers such as $2^x \pm 2^y$, where $x \neq y$ (instead of powers of 2), a circulant matrix circ(1, 2, 1, 1, 4, 3, 5, 1, 4096, 8, 8192, 65536, 32, 7, 9, 12, 1, 16384, 1024, 128, 15, 16, 4, 17) is obtained.

Because this matrix do not have all entries that are powers of 2, it is not suitable for the proposed test. For this reason, further confirmation is needed to confirm its MDS property. Besides confirming the MDS property of the examples of matrices, future research should focus on finding a theoretical proof for this proposition, or on conducting an experiment on a larger sample for various sizes of matrices.

Because of the difference in the complexity of testing between the proposed and full MDS test, even in the case that this proposition is not correct (or conditions for its use are not satisfied), the application of the proposed test in the search methods for MDS matrices significantly reduces their

complexity. The proposed MDS test should be used in the search phase, while the full MDS test should be used on the final result of the search in order to confirm that a matrix is MDS. Due to fact that the complexity of the proposed MDS test is almost negligible compared to the complexity of the full MDS test, by using the aforementioned approach, the complexity of the search method such as the one described in [19] is reduced approximately to the complexity of one full MDS test. In the case that this proposition is correct, and the experimental results imply that it is, the proposed MDS test could enable very fast generation of such $t \times t$ circulant MDS matrices of large sizes, even for t bigger than 32.

## 3 The modification of the make_binary_powers function

In reference [19], resources for finding and testing circulant $t \times t$ MDS matrices, with entries that are powers of 2, are provided. The function make_binary_powers represents a very efficient search method for such matrices. In the first phase of this method a random circulant MDS matrix is obtained by the random generation of its first row. Afterwards, three random entries from the first row are replaced with ones, and the other random entries are replaced with the smallest power of two that maintains the MDS property.

Although the proposed MDS test is intended only for matrices whose all elements are powers of 2, it can be used in the methods such as the make_binary_powers function which uses matrices with random elements in the search stage in order to find the final matrix with entries that are powers of 2. The proposed MDS test can not confirm that initial and intermediate matrices in this method are MDS, except for the final matrix, but that is not necessary in order for this method to work. The ability to evaluate the MDS property of the final matrix, whose all elements are powers of 2, is sufficient.

However there are some features of the make_binary_powers function which could be improved in order to facilitate the search for the more efficient MDS matrices of the larger sizes. For this reason the modified version of this function is made, which is mentioned in previous sections. The fact that only three ones are inserted into the first row of a circulant matrix, indicates that this function is intended for the generation of smaller $t \times t$ MDS matrices, where $t \leq 12$. The maximum number of ones, in the first row of a circulant MDS matrix, is bigger than three for $t > 12$. For example, 13 x 13 MDS matrix circ(32, 8, 1, 1, 128, 1, 2, 64, 16384, 512, 8192, 1, 4) has 4 ones. For this reason, in the modified version of this function, part of the code which insert ones in the first row is omitted. Instead, all random entries are replaced with the smallest power of two starting from the number 2. In this way final matrix consists of exclusively even numbers so all the elements of the final matrix can be divided by 2 in order to get smaller values of a matrix.

Although initial MDS is generated in a random manner, all resulting MDS matrices of the same dimension for the same field are the same. This happens because random entries are always replaced by the powers of 2 in the same order (from the first to the last). In the modified version of this function, random entries are replaced in the sequence which corresponds to their value. The random numbers are replaced from the smallest one to the biggest one. In this way, the output MDS matrix depends on the random input and therefore different MDS matrices of various quality could be generated.

The last modification of this function is based on the search method used. In the make_binary_powers function, search is only made for the appropriate value of a power of 2, while the position of that number is not changed in the search. In the modified version, after the new element is inserted in the first row, circulant matrix is generated and check for the MDS condition is performed. The new element is checked at each position in the first row and if none of matrices generated by such first rows are MDS, next power of 2 is checked. Although this change could lead to a greater complexity of this method (in worse cases), such modification enables more freedom in the search which could result in better output MDS matrix.

For example, by using make_binary_powers function for the generation of 16 x 16 MDS matrix in the Mersenne prime field ($p = 2^{31}-1$), matrix with 3 random elements is obtained. With the proposed modification, matrix with only one random element could be obtained after several attempts. For the above mentioned reasons, modified version of the make_binary_powers function is used in this research. In the next subsection an example of modified function is provided.

### 3.1 An example of using the modified make_binary_powers function

In this subsection an example of obtaining $12 \times 12$ circulant MDS matrix in the field defined over the 31-bit Mersenne prime $p = 2^{31}-1$ is presented. In the first step of this function a random sequence 1033412, 1526990061, 1001410421, 1461020265, 998857270, 1967061242, 765393048, 1466034474, 1786802793, 892566188, 559843044, 1525817832 is obtained which will be used as a first row of the circulant matrix. In the step 2, the circulant matrix is generated and in the step 3 it is confirmed that it is MDS.

In the step 4, one element of the random sequence should be discarded. In this example, the smallest random number will be discarded in each iteration of the proposed approach, although any method for choosing element to be discarded should provide satisfactory output for the next step. Smallest element (which is discarded) is 1033412, so the reduced sequence 1526990061, 1001410421, 1461020265, 998857270, 1967061242, 765393048, 1466034474, 1786802793, 892566188, 559843044, 1525817832 is obtained.

In step 5, number 2 is added to the sequence at the first position so the first row of the circulant matrix is 2, 1526990061, 1001410421, 1461020265, 998857270, 1967061242, 765393048, 1466034474, 1786802793, 892566188, 559843044, 1525817832. After generating a circulant matrix, the test confirmed that this matrix is MDS. For this reason the proposed approach can go to the step 4 in the next iteration.

In the case that matrix failed the MDS test, search would be continued with number 2 on the second position in the first row, and so on until the last position $t$ is checked. If none of these matrices is MDS, search is continued with the next power of 2, which is the number 4.

In the second iteration in the step 4, one of the remaining random numbers should be discarded from the first row of the current MDS matrix. Smallest remaining random number 559843044 is discarded so the reduced sequence 2, 1526990061, 1001410421, 1461020265, 998857270, 1967061242, 765393048, 1466034474, 1786802793, 892566188, 1525817832 is obtained.

In the step 5 of the second iteration, number 2 is added to the sequence at the first position so the first row of the circulant matrix is 2, 2, 1526990061, 1001410421, 1461020265, 998857270, 1967061242, 765393048, 1466034474, 1786802793, 892566188, 1525817832. After generating a circulant matrix, test confirmed that this matrix is MDS so the proposed approach can go to the step 4 in the next iteration.

After 12$^{th}$ iteration of the proposed approach, MDS matrix circ(16384, 64, 4, 2, 2, 2048, 2, 4, 32, 8, 128, 4096) is obtained. After division of all elements by 2, an MDS matrix circ(8192, 32, 2, 1, 1, 1024, 1, 2, 16, 4, 64, 2048) is obtained.

## References


1. Yang Y., Zeng X., Wang S.: Construction of lightweight involutory MDS matrices. Designs, Codes and Cryptography 89, 1453–1483 (2021).
2. Grassi L., Khovratovich D., Lüftenegger R., Rechberger C., Schoffneger M., Walch R.: Hash Functions Monolith for ZK Applications: May the Speed of SHA-3 be With You. Cryptology ePrint Archive, Paper 2023/1025 (2023).
3. Beierle C., Kranz T., Leander G.: Lightweight multiplication in GF*(*2n*)* with applications to MDS matrices. In: CRYPTO 2016, pp. 625–653. Springer (2016).
4. Duval S., Leurent G.: MDS matrices with lightweight circuits. IACR Trans. Symmetric Cryptol. **2018**(2), 48–78 (2018).
5. Guo Z., LiuR., Gao S.,WuW., Lin D.: Direct construction of optimal rotational-XOR diffusion primitives. IACR Trans. Symmetric Cryptol. **2017**(4), 169–187 (2017).
6. Gupta K.C., Ray I.G.: Cryptographically significant MDS matrices based on circulant and circulant-like matrices for lightweight applications. Cryptogr. Commun. **7**(2), 257–287 (2015).
7. Li Y., Wang M.: On the construction of lightweight circulant involutory MDS matrices. IACR Trans. Symmetric Cryptol. **2016**(1), 121–139 (2016).
8. Li S., Sun S., Li C., Wei Z., Hu L.: Constructing low-latency involutory MDS matrices with lightweight circuits. IACR Trans. Symmetric Cryptol. **2019**(1), 84–117 (2019).
9. Liu M., Sim S.M.: Lightweight MDS generalized circulant matrices. IACR Trans. Symmetric Cryptol. **2016**(1), 101–120 (2016).
10. Sarkar S., Syed H.: Lightweight diffusion layer: importance of Toeplitz matrices. IACR Trans. Symmetric Cryptol. **2016**(1), 95–113 (2016).
11. Zhou L., Wang L., Sun Y.: On efficient constructions of lightweight MDS matrices. IACR Trans. Symmetric Cryptol. **2018**(1), 180–200 (2018).
12. Gupta K.C., Pandey S.K., Ray I.G., Samanta S.: Cryptographically significant MDS matrices over finite fields: A brief survey and some generalized results. Advances in Mathematics of Communications,13(4), 779–843, (2019).
13. Lacan J., Fimes J.: Systematic MDS erasure codes based on Vandermonde matrices. IEEE Communications Letters, 8(9), 570–572, (2004).
14. Ferdaouss Mattoussi, Vincent Roca, and Bessem Sayadi. Complexity comparison of the use of Vandermonde versus Hankel matrices to build systematic MDS Reed-Solomon codes. In 2012 IEEE 13th International Workshop on Signal Processing Advances in Wireless Communications (SPAWC), pages 344–348, 2012.
15. Augot D., Finiasz M.: Direct Construction of Recursive MDS Diffusion Layers Using Shortened BCH Codes. In Carlos Cid and Christian Rechberger, editors, Fast Software Encryption, pages 3–17, Berlin, Heidelberg,2015. Springer Berlin Heidelberg.
16. Gupta K.C., Pandey S.K., Samanta S.: On the Direct Construction of MDS and Near-MDS Matrices. arXiv:2306.12848

17. Kranz T., Leander G., Stoffelen Ko., Wiemer F.: Shorter linear straight-line programs for MDS matrices. IACR Trans. Symm. Cryptol., 2017(4): 188–211, 2017.
18. MacWilliams, F.J., Sloane, N.J.A.: The Theory of Error-Correcting Codes. North-Holland Publishing Company, Amsterdam (1977)
19. https://github.com/0xPolygonZero/hash-constants/blob/master/mds_search.sage
20. Malakhov, S. S. (2021). Construction of a set of circulant matrix submatrices for faster MDS matrix verification. *arXiv preprint arXiv:2110.13325*.