Ciencias Matemáticas, Vol. 32, No. 1, 2018, Pag. 45-50
Recibido 11-2017

Permutaciones Aleatorias con Óptima Difusión con una Mirada en Rijndael Dinámico
Random Diffusion Optimal Permutations with a Look in Dynamic Rijndael

Adrián Alfonso Peñate[1] and Pablo Freyre Arrozarena[1]*

Resumen El algoritmo criptográfico Rijndael ha sufrido en los últimos tiempos disímiles modificaciones. Uno de los principales cambios que se aprecian en la literatura pública es la sustitución de sus transformaciones internas por funciones similares, de forma tal que las mismas dependan de la llave secreta. Siguiendo esta tendencia propondremos en este trabajo una algoritmo para generar de forma aleatoria permutaciones con óptima difusión, de forma tal que las mismas puedan utilizarse en el lugar de la transformación ShiftRows.

Abstract The cryptographic algorithm Rijndael has suffered in the last times many modifications. One of the main changes that are appreciated in the public literature is the substitution of their internal transformations for similar functions, in such way that the same ones depend on the secret key. Following this tendency we will propose in this work one algorithm to generate diffusion optimal permutations in a random way, such that the same ones can be used in the place of the transformation ShiftRows.

Palabras Clave
ShiftRows, Rijndael, Difusión

Keywords
ShiftRows, Rijndael, Diffusion

[1] *Institute of Cryptography, Faculty of Mathematic and Computer Science, University of Havana, Cuba.*
[*] *pfreyre@matcom.uh.cu*

Introduction

The cryptographic algorithm Rijndael was accepted as the AES (Advanced Encryption Standard) in 2001 [8], since it was submitted to the AES competition proposed by NIST (National Institute of Standards and Technology).

Their designers, the belgians Joan Daemen and Vincent Rijmen, construct a very strong cryptographic algorithm with a simple algebraic structure. One of the hits of Rijndael is the good diffusion properties that it possesses [6] and one of the internal transformations that allows to reach the full diffusion is SiftRows.

In the section 1 we will carry out the analysis of how it is obtained the full diffusion in Rijndael and how the transformation ShiftRows acts in this process. In section 2 we will leave clear what is the real mathematical function behind the transformation ShiftRows and which have been the main intents of modifying the same one. Finally in section 3 we will give or construction for this kind of transformation explaining which it is the importance of the same one.

The advisements exposed as the result of this investigation can be applied in the design of a dynamic variant of Rijndael for a practical purpose, this task is our future work proposition.

1. The Aim of ShiftRows for Diffusion

The algorithm Rijndael operates over $4N_b$ bytes input $(N_b = 4,5,6,7,8)$ arranged as a matrix, calling state, with 4 rows and N_b columns. It is a iterated cipher with a variable number of rounds, in the which ones four transformation are applied on the state matrix. We are talking about two of them only, because the remaining transformations do not provide diffusion at all [6].

The transformation ShiftRows is applied on the state matrix displacing every row cyclically to left certain quantity N_b-dependent as is shown in the table 1.

Row	$N_b = 4$	$N_b = 5$	$N_b = 6$	$N_b = 7$	$N_b = 8$
1	0	0	0	0	0
2	1	1	1	1	1
3	2	2	2	2	3
4	3	3	3	4	4

Table 1. Rows displacement in Rijndael

ShiftRows offer high dispersion of the bytes in the state matrix, in the sense that, in each column of the state matrix after ShiftRows all the bytes belong to different columns of the state matrix before ShiftRows. For example, if $N_b = 4$ the matrix of the index position of the bytes in the state matrix are transformed by ShiftRows as following.

$$\begin{array}{|c|c|c|c|}\hline 1 & 5 & 9 & 13 \\ \hline 2 & 6 & 10 & 14 \\ \hline 3 & 7 & 11 & 15 \\ \hline 4 & 8 & 12 & 16 \\ \hline \end{array} \longmapsto \begin{array}{|c|c|c|c|}\hline 1 & 5 & 9 & 13 \\ \hline 6 & 10 & 14 & 2 \\ \hline 11 & 15 & 3 & 7 \\ \hline 16 & 4 & 8 & 12 \\ \hline \end{array}$$

The transformation MixColumns is applied on the state matrix post-multiplying every column of the same one for a fixed MDS matrix. MixColumns offer local full diffusion, in the sense that, in each column of the state matrix after MixColumns all the bits depends of every bit of the same column of the state matrix before MixColumns.

In the algorithm Rijndael, the round transformation

$$MixColumns(ShiftRows(state))$$

provide full diffusion in 2 rounds if $N_b = 4$ or 3 rounds if $N_b = 5, 6, 7, 8$, in the sense that, the change of one single bit in the state matrix rebounds in the change of the half of the bits after 2 or 3 rounds if $N_b = 4$ or $N_b \neq 4$ respectively. This is another measure of the diffusion in a block cipher algorithm, similar to the measure given before when we talk about the aim of MixColumns.

2. ShiftRows Like a Permutation

As we show in the previous section, in the algorithm Rijndael the state matrix is transformed by the transformation ShiftRows by means of the rule

- Row i is cyclically moved C_i position to left.

where C_i is a different value N_b-dependent for every different row $1 \leq i \leq 4$. If we consider the bijective application

$$t : M_{4\times N_b}(\mathrm{GF}(2^8)) \longrightarrow \mathrm{GF}(2^8)^{4\times N_b}$$

such that

$$t(state)_{4(j-1)+i} = state_{i,j}$$

were $\mathrm{GF}(2^8)$ is the Finite Galois Field of 256 elements and $M_{4\times N_b}(\mathrm{GF}(2^8))$ is the set of all the matrices of 4 rows and N_b columns, it is possible to see that

$$ShiftRows(state) = t^{-1}(\Pi(t(state))) \qquad (1)$$

where Π is a permutation of $4N_b$ elements defined for every $1 \leq i \leq 4$ and every $1 \leq j \leq N_b$ as

$$\Pi[4(j-1)+i] = 4(j - C_i - 1 \mod N_b) + i$$

2.1 Objective and Related Work

The permutation Π, just as we previously show it, has been defined in [6, Definition 9.4.1] like a diffusion optimal permutation. A permutation Π is diffusion optimal if all elements in each column are distributed over all different columns under the action of Π, so, the search of diffusion optimal permutations is related to one specific rectangular matrix with at least as many columns as rows [6].

This relationship is given by the bijective function t, we mean, if $B = \Pi(A)$ then the matrices $t^{-1}(A)$ and $t^{-1}(B)$ are related by means of Π. For example, if $N_b = 4$ from the matrix of the index position of the bytes in the state matrix we are able to see the permutation Π of the equation (1).

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1	6	11	16	5	10	15	4	9	14	3	8	13	2	7	12

About the replacing of the permutation Π there are some works in the public literature, most of them focused on a random row displacement for the transformation ShiftRows, forgetting the dispersion properties that Π should offer. Some attempts to change ShiftRows by replacing of the permutation Π are the following [5, 4, 1, 3].

The first real approach to replace Π in a random way is proposed in [2, 7]. In [2] is possible to construct diffusion optimal permutations related with square matrices of any size, and [7] utilizes the same idea to construct diffusion optimal permutations related with 4 × 4 square matrices only, like in the AES algorithm. In the next section we will see how this construct works and we will give a generalization of the same one for rectangular matrices.

Our contribution: We provide a set of diffusion optimal permutations with a look in dynamic Rijndael, in such way that the same ones may be used to replace the permutation Π of the equation (1). These permutations can have any size desired, except a prime number, and our construction allows to choose one of them at random. On the other hand, we enunciate a theorem related with the minimal number of rounds required to reach the full diffusion, and then we show how this construction is better than Rijndael's construction.

3. Generating a Random Diffusion Optimal Permutation

It is well known that one permutation of length N acts over any finite and orientated set of N elements, independently of its nature, shuffling all the positions into de the same one. In the following we assume that one permutation of length N acts over the set of the index positions $I = \{1, 2, \ldots, N\}$.

Just as we cite above, to construct one diffusion optimal permutation, N may be a composite number kn such that k is the number of elements in every column and $n \geq k$ is the number of columns of the associated matrix. The previous facts guide the search of a random diffusion optimal permutation Π through their associated matrix $t^{-1}(\Pi(I))$.

3.1 Our Construction in the Square Case

For to generate all the diffusion optimal permutations when there are as many columns as rows, we can start with the next proposition about the cardinal.

Proposition 1 *For any $k \geq 2$, the amount of diffusion optimal permutations of length k^2 and associated matrix with k rows and k columns is $(k!)^{2k}$.*

Demonstration 1 *Let $I = \{1,2,\ldots,k^2\}$ be the set of the index positions, then we may analyze how the elements into every column of $t^{-1}(I)$ should be distributed over $t^{-1}(\Pi(I))$ in order to Π be diffusion optimal.*

Column 1: *In the first column of $t^{-1}(I)$ there are k elements and every one of them should be distributed in a different column of $t^{-1}(\Pi(I))$, so we have*

$$[k \cdot k][k \cdot (k-1)] \cdots [k \cdot 1]$$

possibilities for this, keeping in mind that the same ones can be located in any position inside the respective column of $t^{-1}(\Pi(I))$.

Column 2: *In the second column of $t^{-1}(I)$ there are k elements and every one of them should be distributed in a different column of $t^{-1}(\Pi(I))$, so we have*

$$[(k-1) \cdot k][(k-1) \cdot (k-1)] \cdots [(k-1) \cdot 1]$$

possibilities for this, keeping in mind that the same ones can be located in any position inside the respective column of $t^{-1}(\Pi(I))$, but one of these position is busy for one element of the first column of $t^{-1}(I)$.

$\vdots$

Column k: *In the $k-$th column of $t^{-1}(I)$ there are k elements and every one of them should be distributed in a different column of $t^{-1}(\Pi(I))$, so we have*

$$[1 \cdot k][1 \cdot (k-1)] \cdots [1 \cdot 1]$$

possibilities for this, keeping in mind that the same ones can be located in any position inside the respective column of $t^{-1}(\Pi(I))$, but $k-1$ of these position are busy for one element of the previous columns of $t^{-1}(I)$.

Made this analysis we get the cardinal of all the diffusion optimal permutations

$$\prod_{i=1}^{k} \prod_{j=0}^{k-1} i(k-j)$$

and improving these products the proposed number is hold. ■

In [2] is presented one algorithm for the random generation of all the diffusion optimal permutations of this size. In practical way, we are able to obtain random diffusion optimal permutations if we change the positions of the elements inside every column of the matrix

$$t^{-1}(I) = \begin{array}{|c|c|c|c|} \hline 1 & k+1 & \cdots & (k-1)k+1 \\ \hline 2 & k+2 & \cdots & (k-1)k+2 \\ \hline \vdots & \vdots & \ddots & \vdots \\ \hline k & k+k & \vdots & (k-1)k+k \\ \hline \end{array}$$

through a random permutation of k elements, transpose this matrix, and we change again the positions of the elements inside every column of this new matrix.

For example, if the next permutations of S_4 are used in the respective order

$$\begin{aligned} \tau_1 &= [1,4,3,2] \\ \tau_2 &= [2,1,4,3] \\ \tau_3 &= [3,2,1,4] \\ \tau_4 &= [4,3,2,1] \\ \tau_5 &= [1,2,3,4] \\ \tau_6 &= [2,3,4,1] \\ \tau_7 &= [3,4,1,2] \\ \tau_8 &= [4,1,2,3] \end{aligned}$$

the matrix of the index position of the bytes in the state matrix (for the case of Rijndael with $N_b = 4$) is transformed according to the previous idea until obtaining the same output of ShiftRows, as is showing next.

1	5	9	13
2	6	10	14
3	7	11	15
4	8	12	16

1	6	11	16
4	5	10	15
3	8	9	14
2	7	12	13

1	4	3	2
6	5	8	7
11	10	9	12
16	15	14	13

1	5	9	13
6	10	14	2
11	15	3	7
16	4	8	12

3.2 Our Construction in the Rectangular Case

To find all the diffusion optimal permutations when there are more columns than rows is a very difficult task. We can prove that the amount of all the diffusion optimal permutations when the number of columns surpasses in one the number of rows is $(k+1)!(k!)^{2(k+1)}$ with a similar thought of the demonstration 1.

However, when the number of columns surpasses in more than one the number of rows, we are in front of an interesting mathematical problem, not solved yet. In this work we offer a partial solution for this problem, but for our practical purpose of diffusion this is the best solution that anyone can find. In the next subsection we will argue this affirmation.

In this case we are applying the same construction of the square case, but a transpose matrix can't be used. In their place we are considering another matrix, the which one allows to obtain diffusion optimal permutations. Our procedure is presented next.

1. Change the positions of the elements inside every column of the matrix

$$t^{-1}(I) = \begin{array}{|c|c|c|c|}\hline 1 & k+1 & \cdots & (n-1)k+1 \\ \hline 2 & k+2 & \cdots & (n-1)k+2 \\ \hline \vdots & \vdots & \ddots & \vdots \\ \hline k & k+k & \vdots & (n-1)k+k \\ \hline \end{array}$$

   through a random permutation of k elements.

2. Call $t^{-1}(\Pi_1(I))$ to the previous matrix and form, starting from the same one, a new matrix $t^{-1}(\Pi_1(\mathrm{Tr}(I)))$ in the which one the elements of $t^{-1}(\Pi_1(I))$ are placed completing the rows.

3. Change again the positions of the elements inside every column and call $t^{-1}(\Pi_1(\mathrm{Tr}(\Pi_2(I))))$ this last matrix, then a diffusion optimal permutation $\Pi = \Pi_2 o \mathrm{Tr} o \Pi_1$ has been obtained.

Using this method we can built $(k!)^{2n}$ different diffusion optimal permutations, taken all the possibles choices in S_k^{2n}. The prove of this result and at the same time the prove of randomness of the proposed algorithm is given below.

Demonstration 2 *Let $\phi : S_k^{2n} \longrightarrow S_{kn}$ be the function defined for all $\tau = (\tau_1, \ldots, \tau_{2n})$ as $\phi(\tau) = \Pi_\tau$ where τ_i is a random permutation of S_k for all $1 \leq i \leq 2n$ and Π_τ is one diffusion optimal permutation generated through the previous method by τ. Then we must see that ϕ already defined is a bijective application.*

Let us consider τ and γ two elements of S_k^{2n} such that $\tau \neq \gamma$, then exists at less $1 \leq j \leq 2n$ for the which one $\tau_j[i] \neq \gamma_j[i]$ for some $1 \leq i \leq k$. Now only two things can happen in the way that Π is formed.

For $1 \leq j \leq n$ and $1 \leq i \leq k$ the element $k(j-1)+i$ is located in a different column of Π_τ with respect to Π_γ, and therefore both are different.

On the other hand if $\tau_1 = \gamma_1, \ldots, \tau_n = \gamma_n$ happens, for $n+1 \leq j \leq 2n$ and $1 \leq i \leq k$ the $i-$th element of the $j-$th column of Π_τ will be different from the $i-$th element of the $j-$th column of Π_γ, and therefore both are different. ■

We show how taking $2n$ random permutations of S_k we are able to generate a random diffusion optimal permutation of size kn. For a practical purpose this method is used over matrices, without calculating the diffusion optimal permutations for anything, even so the algorithm to generate the same ones is presented.

Algorithm 1: Random generation of Π.

```
Input: Random permutations $\tau_1, \tau_2, \ldots, \tau_{2n} \in S_k$.
begin
    for $j = 1 \cdots n$ do
        for $i = 1 \cdots k$ do
            $\Pi_1[k(j-1)+i] = k(j-1)+\tau_j[i]$.
            $\mathrm{Tr}[k(j-1)+i] = n(i-1)+j$.
            $\Pi_2[k(j-1)+i] = k(j-1)+\tau_{n+j}[i]$.
        end for
    end for
    for $j = 1 \cdots n$ do
        for $i = 1 \cdots k$ do
            $\Pi[k(j-1)+i] = \Pi_1[\mathrm{Tr}[\Pi_2[k(j-1)+i]]]$.
        end for
    end for
end
Output: Random diffusion optimal permutation $\Pi$.
```

3.3 The Advantages of Our Construction

It is clear that this construction is not so fast as Rijndael's construction, where only displacements are applied from one state matrix to another, even so, the speed is not a priority in our approach.

The first advantage of our construction is the amount of variants generated by means of the algorithm 1. If we do all the possibles row displacements, to obtain the diffusion optimal every one of this displacements should be different, and for this reason there are only V_k^n variants. There is an obvious difference between both methods, for example, for diffusion optimal permutations acting in matrices of 4 rows and 4 columns, our construction offer 24^8 variants in the meantime that Rijndael's construction offer only 24 variants.

The second advantage that we can appreciate is the minimality of the full diffusion, in the sense of the minimal number of rounds required to allows the same one. The theorem 1 will be enunciate for this reason, but before seeing the same one let us consider some important aspects.

1. Let $M_{k \times n}(\mathrm{GF}(2^8))$ be the set of all the matrices with k rows and n columns with entries in the Galois Field $\mathrm{GF}(2^8)$, as always $k \leq n$. For similarity with Rijndael we will be calling state to any matrix of this set.

2. Keep in mind a transformations like MixColumns, that operate independently over all the columns of the state providing local full diffusion. It can be reached by multiplication of one MDS matrix of size $k \times k$, and we will be calling this transformation θ.

3. For each diffusion optimal permutation given in our construction we replace the permutation Π of the equation (1), and we will be calling this transformation π.

Theorem 1 *The round transformation $\theta(\pi(state))$ provides full diffusion in 2 round if $n = k$ or $i+1$ round if $k^{i-1} < n \leq k^i$ for some $i \geq 2$.*

Demonstration 3 *We analyze the dependence of one byte of the state $\xi \in \mathrm{GF}(2^8)$, without loss generality we can assume that byte as the first, through the round transformation already defined.*

If $n = k$, then all the bytes in the first column of the state after the application of θ at the first round are $\xi-$dependent. In the second round, in the way that Π are constructed, all the columns of the state after the application of π have one element $\xi-$dependent, and then, whit the transformation θ in the second round all the elements of the state are $\xi-$dependent.

When $k^{i-1} < n \leq k^i$ for some $i \geq 2$ the prove of the theorem is similar. How $n \leq k^i$, and in the way that Π are constructed, the following is expected.

Round 1: *When applying π and then θ all the elements on the first column of the state are $\xi-$dependent.*

Round 2: *When applying π the first k columns of the state have at less one element $\xi-$dependent, then after the application of θ all the elements on the first k columns of the state are $\xi-$dependent.*

Round 3: *When applying π the first k^2 columns of the state have at less one element $\xi-$dependent, then after the application of θ all the elements on the first k^2 columns of the state are $\xi-$dependent.*

$\vdots$

Round $i+1$: *When applying π all the columns of the state hold have at less one element $\xi-$dependent, then after the application of θ all the elements of the state are $\xi-$dependent.* ■

Corollary 1 *The number of rounds necessary to reach the full diffusion by the round transformation $\theta(\pi(state))$ in minimal.*

Demonstration 4 *The minimality of the necessary rounds until obtain the complete $\xi-$dependency is obvious, since for every column that hold at less one element $\xi-$dependent in the next round there are k columns that hold at less one element $\xi-$dependent. For another one diffusion optimal permutation do not generated by the algorithm 1 the above mentioned is obtained in same or bigger number of rounds.* ■

With this property, that for every column that hold at less one element $\xi-$dependent in the next round there are k columns that hold at less one element $\xi-$dependent, we can to consider another matrices $t^{-1}(\Pi_1(\mathrm{Tr}(I)))$ and therefore to construct another permutations Tr for the which ones the diffusion optimal is expected in the minimal rounds as possible. The amount of all this possibilities is

$$\binom{n}{k}\binom{n-k}{k}\binom{n-2k}{k}\cdots\binom{n-\left\lfloor\frac{n}{k}\right\rfloor k}{k}$$

but for simplicity in our design we are considering the only one exposed above.

We can show in a simple way that Rijndael's construction is not efficient for to obtain the full diffusion in a minimal way using the round transformation $\theta(\pi(state))$, we mean, when the permutation Π of the equation (1) is built by means of rows displacement on the state. For the values $k = 4$ and $n = N_b$ of the algorithm Rijndael the number of rounds until reach the full diffusion are the same for both constructions, but if $k = 4$ and $n = 10$ using the Rijndael's construction the full diffusion in obtained in a minimal trail of 4 rounds for some displacement and using our construction the full diffusion in obtained in a minimal trail of 3 rounds since $k < n < k^2$.

This is an important property to keep in mind if we want to increase the input sizes of the algorithm Rijndael for a practical purpose. As we said at the beginning of this work, the design of a new dynamic variant of Rijndael with the reached results is a future task.

Conclusion

The cryptographic algorithm Rijndael has suffered some transformations since it was accepted as the AES in 2001. Today, there are not yet practical attacks on the Rijndael that can make it vulnerable, even so, some investigators has made dynamic their internal transformations to increase the cryptographic strength of the same one, hiding the relationships between the plain text and the cipher text.

In this work we provide a class of random diffusion optimal permutations with a look in dynamic Rijndael. The transformation ShiftRows offer high dispersion of the bytes in the state matrix by means of wows displacement and contributes with the full diffusion, we show a new construction as simple as is possible where the dispersion is equally obtained but the full diffusion is reached in a minimal number of rounds.

References

[1] Ahmad Z. Al-Wattar A., Mahmod R. and Izura N. A new dna based approach of generating key-dependent shift rows transformation. *International Journal of Network Security and Its Applications*, Vol. 7, No. 1, 2015.

[2] A. Alfonso. Random generation of diffusion optimal permutation. *Proceedings of the III National Scientific Workshop of Cryptography, Institute of Cryptography of the Havana University*, 2016.

[3] Lauridsen M. Leander G. Beierle C., Jovanovic P. and Rechberger C. Analyzing permutations for aes-like ciphers: Understanding shiftrows. *IACR Cryptology ePrint Archive*, No. 212, 2015.

[4] Mohsen A. Hussein N., Monem A. and Yousef S. A byte-oriented multi keys shift rows encryption and decryption cipher processes in modified aes. *International Journal of Scientific and Engineering Research*, Vol. 5, Issue 4, 2014.

[5] Khattab S. Ismail I., Galal-Edeen G. and Moustafa M. Performance examination of aes encryption algorithm with constant and dynamic rotation. *International Journal of Reviews in Computing*, Vol. 12, 2012.

[6] Daemen J. and Rijmen V. The design of rijndael: Aes - the advanced encryption standard. *Springer-Verlag*, 2002.

[7] Spain M. and Varia M. Diversity within the rijndael design principles for resistance to differential power analysis. *Springer-Verlag*, Proceedings of the CANS-2016, LNCS 10052:pp. 71–87, 2016.

[8] Federal Information Processing Standards. Announcing the advanced encryption standard. *FIPS Publication 197*, 2001.