Proceedings of the 4th WSEAS Int. Conf. on Information Security, Communications and Computers, Tenerife, Spain, December 16-18, 2005 (pp147-151)

Graphs connected with block ciphers

OTOKAR GROŠEK
Slovak University of Technology
Department of Applied Informatics
Ilkovičova 3, 812 19 Bratislava
SLOVAKIA

PAVOL ZAJAC
Slovak University of Technology
Department of Applied Informatics
Ilkovičova 3, 812 19 Bratislava
SLOVAKIA

Abstract: A block cipher consists of round transformations. Each round transformation contains a mixing layer to create diffusion, that is, to have each output bit dependent on all input bits. Such a transformation can also be described by means of graph theory language. Here we generalize a partial result from our two previous papers. The main result of this paper claims that for an oriented graph G with n vertices, satisfying for all $u, v \in V(G)$ special conditions, there exists n_0 such that for all $n > n_0$ the number of arcs $e(G) \geq (n-1)(k+1)$. We also discuss a relation to the problem of an ideal round transformation.

Key–Words: Graphs with oriented path of length 2, Efficient design of block cipher.

1 Introduction

Conditions to design a good block cipher are still under careful investigation of researchers. They include security, versatility, hardware, etc. A good reference can be found in [2]. Any block cipher consists of transformations commonly called round transformations. These transformations are obtained by alternatively applying permutations, P-boxes, and substitutions, S-boxes. The role of an S-box is to create confusion, that is, to have the relation between the key and the cipher text as complex as possible. The role of a P-box is to create diffusion, that is, to have each output bit dependent on all input bits. In the ideal case, flipping an input bit should change each output bit with the probability of one half. A product cipher is a composition of round transformations, and is often called substitution-permutation network (SPN).

A common strategy is to have substitutions carried out over small disjoint parts of the input, while the P-box permutation is a single large permutation, so called global mixing transformation, used to mix these parts together. In paper [4] we suggest criteria which should be satisfied by an efficient P-box, and then we study P-boxes satisfying those criteria. It turns out that it is very handy to see the mixing transformation as a function $F \in \mathcal{F}_n$, where $\mathcal{F}_n$ is the family of all Boolean functions on Z_2^n, that is, $F = (f_1, f_2, ..., f_n)$, where $f_i : Z_2^n \to Z_2, i = 1, ..., n$, are called component functions. For obvious reasons, F has to be a bijection, and in order not to compromise the key, any linear combination of component functions $f_i^{'}$s has to be non-linear[1]. To be able to define the optimality criterion put on the mixing transformation we introduce a notion of a matrix Φ associated with the function F.

Definition 1 *Let $F = (f_1, \ldots, f_n) \in \mathcal{F}_n$. Then $\Phi(F)$ will stand for a $0-1$ matrix $A = (a_{ij})$ of order n, where a_{ij} is given by*

$$a_{ij} = \begin{cases} 1, & \text{if there exists } x \in Z_2^n \text{ such that} \\ & f_j(x \oplus e^{(i)}) \oplus f_j(x) = 1; \\ 0, & \text{otherwise,} \end{cases} \tag{1}$$

where the symbol $\oplus$ represents the Boolean sum of two words, and $e^{(i)}$ stands for the word with the only 1 in the i-th position. Further, we set $\delta(F) = \sum_{i=1}^{n} \sum_{j=1}^{n} a_{ij}$.

Clearly, because of the hardware implementation of F, we would like to minimize $\delta(F)$. On the other hand, as the mixing transformation has to guarantee that each output bit depends on all input bits, it must be $\delta(F) = n^2$, or, equivalently, $\Phi(F) = J_n$, where J_n is the matrix of order n with all elements equal to 1. One way how to deal with the two contradictory requirements is to adopt the following strategy. We seek a function $F \in \mathcal{F}_n$ with $\delta(F)$ being as small as possible but $\Phi(F \circ F \circ ... \circ F) = J_n$, That is, in the first round of the mixing transformation F, the change of an input bit x_i affects only few outputs bits, but the remaining output bits will be affected in the following rounds of the transformation. With respect to time

[1] Function $f : Z_2^n \to Z_2$ is said to be non-linear if the algebraic normal form of f contains at least one term of order 2, or more.

needed for ciphering the ideal situation occurs if the required property of F is obtained after two rounds, that is, if $\Phi(F \circ F) = J_n$.
The main result of [4] claims that if F is a bijection in $\mathcal{F}_n, n \geq 64$ so that all linear combinations of its components are non-linear functions, and $\Phi(F \circ F) = J_n$, then $\delta(F) \geq 4n - 4$, and by a construction of a suitable function F we showed that this bound is best possible.

2 Problem Formulation

Our solution presented in [4] is the best possible in the sense of minimum hardware connections for a good round transformation. Unfortunately, each but one component function f_i have only three active variables. To gain better properties, e.g. general nonlinearity, we may need more active variables per each component function. This leads to a generalization of a problem from graph theory which we used in papers [7, 4]. In this section we recall some notions and notation from graph theory, and explain the problem we solve.
Let G be an oriented graph, and (u, v) be an arc of G. Then the vertex v is said to be adjacent from u and a u is said to be adjacent to v. The number of vertices adjacent from v is called the outdegree of v and is denoted by $od(v)$, the number of vertices adjacent to v is called the indegree of v and is denoted by $id(v)$. Further, we denote by $N_{od}(v)$ and the $N_{id}(v)$ the set of vertices of G that are adjacent from v and to v, respectively; $N^2_{id}(v)$ will stand for the set of vertices of G from which v can be reached by an oriented path of length 2. Finally, by $e(G)$ we denote the number of arcs of G.
In the case that F is a mixing transformation, each input bit has to affect each output bit. Hence, translated into terms of the matrix $\Phi(F)$, the mixing transformation F satisfies the condition $\Phi(F) = J_n$, where J_n is the matrix of order n with all elements equal to 1. However, as mentioned in Introduction, the implementation of a function F with $\Phi(F) = J_n$ would be very inefficient from the hardware point of view. Therefore we seek for a function $F \in \mathcal{F}_n$ with $\delta(F)$ being small but $\Phi(F \circ F) = J_n$. Now we are ready to define the concept of the paper [4].

Definition 2 *Ideal non-linear mixing transformation. Let $\mathcal{C}_n$ be the set of all functions $F = (f_1, f_2, \ldots, f_n) : Z_2^n \to Z_2^n$ satisfying conditions:*

1. *F is a bijection;*
2. *For each $c = (c_1, ..., c_n) \in Z_2^n$, $c \neq (0, 0, ..., 0)$, the function $\bigoplus_{j=1}^n c_j f_j$ is non-linear;*
3. *$\Phi(F \circ F) = J_n$.*

We set $\delta_n = \min\{\delta(F) : F \in \mathcal{C}_n\}$, and each function $F \in \mathcal{C}_n$ with $\delta(F) = \delta_n$ will be called an ideal non-linear mixing transformation.

Theorem 3 *If $\Phi(F \circ F) = J_n$ then $\Phi(F) \odot \Phi(F) = J_n$, where $\odot$ denotes matrix multiplication with Boolean OR instead of XOR.*

We introduce two more notations which will be frequently used throughout the paper. Let $F = (f_1, ..., f_n)$ be an ideal non-linear mixing transformation, $\Phi(F) = A = (a_{ij})$. Let $R(f_i)$ is the set of all active variables of f_i, i.e. the set of all variables which appear in the algebraic normal form of f_i. Further, let $H_{u,v}$ be a subset of component functions $\{f_1, ..., f_n\}$ so that if $f \in H_{u,v}$ then $|R(f)| = k$, and both $u, v \in R(f)$.
As A is a $0 - 1$ matrix, A can be understood as the incidence matrix of an oriented graph G on n vertices $v_1, ..., v_n$, where an oriented arc $(v_i, v_j) \in G$ if $a_{ij} = 1$. Clearly, if $|R(f_j)| = k$ for a function $f_j, 1 \leq j \leq n$, then the number of $1'$s in the j-th column of A equals k, that is, $id(v_j) = k$. It is easy to check that no non-linear function with two active variables is balanced. Therefore, for each vertex $v \in G$, we have

$$id(v) \geq 3. \tag{2}$$

Further, $|H_{u,v}|$ is clearly equal to the number of vertices of indegree k adjacent both from u, v. In graph theory language, $H_{u,v}$ will be the set of such vertices.
By Theorem 3, $A \odot A = J_n$ is a necessary condition for F to be an ideal non-linear mixing transformation. This condition translates into graph theory language as follows: For any two vertices $u, v \in G$ there is an oriented path of length 2 both from u to v and also from v to u, that is, $N^2(v) = V(G)$ for each vertex $v \in G$. As far as we know, oriented graphs with this property, having the minimum possible number of arcs, have not been investigated yet. Results concerned with a similar problem asking for the minimum number of arcs of an oriented graph of diameter 2 can be found in [3].
From conditions 1 and 2 in Definition 2 it follows, that each f_j must be at least of order 2, and possesses at least $k \geq 3$ active variables. If this is the case then it is possible to have ([4]) $|H_{u,v}| \leq 5$. Besides this key ingredient of the proof, the main strategy in [4] consists of two steps:

1. Find a graph with minimum arcs, such that for any vertex, except of one, $id(v) \geq 3$, and for any two vertices $u, v \in G$ there is an oriented path of length 2 both from u to v and also from v to u, that is, $N^2_{id}(v) = V(G)$.

2. Find a function F satisfying conditions 1 - 3 from Definition 2 such that $\Phi(F) = \mathbf{A}$.

This yields for the incidence matrix $\mathbf{A}$ of such a graph the following conditions:

1. Matrix $\mathbf{A}$ possesses, except of one column, three 1's in each column.
2. If $a_{uj} = a_{vj} = 1$ then $\sum_{\ell=1}^{n}(a_{u\ell}a_{v\ell}) \leq 5$.
3. $\mathbf{A} \odot \mathbf{A} = \mathbf{J}_n$.
4. $\sum_{i=1}^{n}\sum_{j=1}^{n} a_{ij}$ is as small as possible.

Obviously, if we require that each f_j possesses at least k active variables, then we will have different bounds for $id(v)$, and $|H_{u,v}|$ respectively.
The main result of this paper generalize our previous results from the graph point of view regardless of the existence of underlying ideal mixing transformations.

3 Problem Solution

We start to prove our main theorem.

Theorem 4 *Let G be an oriented graph with n vertices. Let the following conditions hold:*

(1) the number of vertices adjacent to v, $id(v) \geq k$;

(2) the number of vertices $w, id(w) = k$, adjacent from both u and v is at most h;

(3) for any two vertices $u, v \in V(G)$ there is an oriented path from u to v, and v to u.

Then there exists $n_0 = n_0(k, h)$ such that for all $n > n_0$ the number of arcs $e(G) \geq (n-1)(k+1)$, and this bound is the best possible.

Proof: Before we prove $e(G) \geq (n-1)(k+1)$ we show that the bound cannot be improved because of the following construction:
For the incidence matrix $\mathbf{A} = (a_{ij})$ of a graph G with n vertices the following is valid:

1. $a_{11} = 0$;
2. For $j = 2, 3, \ldots, n$ we have $a_{1j} = a_{j1} = 1$;
3. For $j = 2, 3, \ldots, n$ we have $a_{j(j+1 \bmod n)} = a_{j(j+2 \bmod n)} = \ldots = a_{j(k-1 \bmod n)} = 1$

Then for each vertex of G we have $id(v) = od(v) = k$, the set of vertices $w, id(w) = k$, adjacent from both u and v is $h = k$. Obviously, for any two vertices $u, v \in V(G)$ there is an oriented path from u to v, and v to u. Thus $e(G) = (n-1)(k+1)$.

Assume by contradiction that

$$e(G) < (n-1)(k+1). \tag{3}$$

We will first prove the following lemma:

Lemma 5 *Let G be an oriented graph with n vertices. Let for all $v \in V(G)$, $id(v) \geq k$, and $N_{id}^2(v) = V(G)$. Then $e(G) \geq n(k+1) - k^2$.*

As G has n vertices and by (1), there has to be in G a vertex α with $id(\alpha) = k$. Set $N_{id}(\alpha) = \{v_1, v_2, \ldots v_k\}$. Since $N_{id}^2(\alpha) = V(G)$, for each $u \in G$ there is a vertex $w \in N_{id}(\alpha)$ so that $(u, w) \in G$. Hence, $e(G) = \sum_{v \in N_{id}(\alpha)} id(v) + \sum_{v \in V(G) - N_{id}(\alpha)} id(v) \geq n + k(n-k) = n(k+1) - k^2$.

The arcs of the subgraph induced by $N_{id}(\alpha)$ will be called blue arcs. Each vertex in $N_{id}(\alpha)$ is a initial vertex of a blue arc, thus there are at least k of them. Let $X'_i = N_{id}(v_i) - N_{id}(\alpha)$. If $e(G) = n(k+1) - k^2$, then X'_i are pairwise disjoint, $id(v) = k$ for each vertex in $V(G) - N_{id}(\alpha)$, and there are exactly k blue arcs in G.

Put $e(G) = n(k+1) - k^2 + \delta$. Then under supposition (3), $0 \leq \delta \leq k^2 - (k+1)$. If there is a vertex $v \in V(G) - N_{id}(\alpha)$ with $id(v) = k + \varepsilon$, $\varepsilon > 0$, then we choose arbitrarily ε arcs with the initial vertex v and color them red. Further, every arc (v, v_i), $v \in X'_j$, $j < i$, will be color red as well. Clearly, the total number of red and blue arcs is $k + \delta$. Thus, there are at most δ red arcs in G. In what follows red will stand for the number of the red arcs in G.

Set, $X_1 = X'_1, X_2 = X'_2 - X_1, \ldots X_k = X'_k - \{X_1 \cup X_2 \ldots \cup X_{k-1}\}$. We assume that $|X_1| \geq |X_2| \geq \ldots |X_k|$. Thus, $|X_1| \geq \frac{n-k}{k}$.

First of all we show

Claim 1. If $v \in G$, and $id(v) = k$, then $(v_1, v) \in G$.

Proof of the Claim 1. Suppose by contradiction that there is a vertex $v, id(v) = k$, in G so that $(v_1, v) \notin G$. Since $N_{id}^2(v) = V(G)$, there is a path of length 2 from each vertex in X_1 to v. Let $u \in N_{id}(v)$. Then the number of vertices in X_1 adjacent to u equals at most $id(u)$ for $u \in V(G) - N_{id}(\alpha)$, and equals at most the number of red arcs whose terminal vertex is u, for $u \in N_{id}(\alpha)$. As $red \leq \delta$, $|X_1| \leq red + k \times k \leq \delta + k^2 < \frac{n-k}{k} \leq |X_1|$ for $n \geq 2k^3 - k^2$. The proof of Claim 1 is complete.

The following statement is essential for the proof of the theorem.

Claim 2. For each $v \in V(G) - \{v_1\}$, $(v, v_1) \in G$.

Proof of Claim 2. First of all we point out that there are in G at least $n-k-\delta$ vertices of indegree k. To see this we recall that $\sum\limits_{v\in N_{id}(\alpha)} id(v) \geq n.$

Assume by contradiction that there is a vertex $\beta \in G, \beta \neq v_1$, so that $(\beta, v_1) \notin G$. With respect to (2), and Claim 1, the vertex β is adjacent to at most h vertices v of indegree k.
Further, β might be adjacent to vertices of indegree more than k. There are at most δ of them. Indeed, each vertex $w, id(w) > k$, and $w \in V(G) - N_{id}(\alpha)$ is incident with a red arc. Also, there are at most $k-1$ vertices of $N_{id}(\alpha)$ adjacent to β as $(\beta, v_1) \notin G$. However, if some vertices of $N_{id}(\alpha)$ are adjacent to β, then either some of them is adjacent to β by a red arc (if $\beta \in V(G) - N_{id}(\alpha)$ or there are at least $k+1$ blue arcs in G, i.e. at most $\delta - 1$ red arcs, if $\beta \in N_{id}(\alpha)$. To see this we recall that each vertex in $N_{id}(\alpha)$ is a terminal vertex of a blue arc.
Thus, $od(\beta) \leq h + \delta$. Taking into account that there are at least $n-k-\delta-h$ vertices of outdegree k that are not adjacent from β, and that to each $v \in G$ there is a vertex $u \in N_{id}(v)$ so that $(\beta, u) \in G$, the pigeon hole principle guaranties that there is a vertex $\gamma \in N_{od}(\beta)$ that is adjacent to at least $\left\lceil \frac{n-k-\delta-h}{h+\delta} \right\rceil$, vertices of indegree k. However, $\left\lceil \frac{n-k-\delta-h}{h+\delta} \right\rceil > h$, for $n \geq h^2 + h + (h+1)(k^2-k-1) + k$, which contradicts (2), because each of those vertices would be adjacent from both v_1 and γ. The proof of Claim 2 is complete.

To finish the proof of the theorem it suffices to recall that for each $v \in G$, $id(v) \geq k$, and by Claim 2, $id(v_1) = n-1$. Thus, the total number of arcs in G, for $n_0 = \max\{h^2+h+(h+1)(k^2-k-1)+k, 2k^3-k^2\}$, is at least $(n-1)(k+1)$.

4 Conclusions

A pertinent question for application in a design of a block cipher is to find to such a minimal graph an ideal round transformation.
For $k=2$, minimal graphs with $3n-3$ arcs are given as follows [7]:

$$\mathbf{A}_2 = \begin{pmatrix} \mathbf{0} & \mathbf{J}_{1,n-1} \\ \mathbf{J}_{n-1,1} & \mathbf{P}_{n-1} \end{pmatrix},$$

where $\mathbf{P}_n$ denotes $n \times n$ permutation matrix, and $\mathbf{J}_{m,n}$ denotes $m \times n$ matrix full of ones. In this case the bound $h=1$, and the round transformations are described in [7]. To fulfil condition $N_{id}^2(v) = V(G)$, it is not possible to remove any arc from the graph. The case $k=3, h=5$ is discussed in [4]. For $k>3$, possible minimal graphs with $(n-1)(k+1)$ arcs are given, e.g. as follows:

$$\mathbf{A}_k = \begin{pmatrix} \mathbf{0} & \mathbf{J}_{1,n-1} \\ \mathbf{J}_{n-1,1} & \mathbf{B}_{n-1,k-1,h-1} \end{pmatrix},$$

where $\mathbf{B}_{n,k,h}$ denotes $n \times n$ matrix containing k ones in each column, and at least 1 and at most h ones in each row. Summing up the number of ones by rows, and columns respectively we get condition

$$(n-1)(1+h) \geq (n-1)(k+1), \qquad (4)$$

or $h \geq k$.
For a given incidence matrix $\mathbf{A}$, one can try to find a suitable boolean function F, such that $\Phi(F) = \mathbf{A}$, and conditions from Definition 2 are satisfied. A straightforward strategy is to generate all possible component functions f_j by trying all possible algebraic normal forms yielding active variables from the set $\{x_i | \ a_{ij} = 1\}$ for the fixed j, and to test the conditions of balancedness and non-linearity of all their linear combinations. Clearly this solution is impractical even for smaller n's. A construction of F for general n, and $k = 2, 3$ has been shown in [7, 4] providing upper bound for parameter h, and thus for n_0 too.

It is still an open question, how to construct function F for both general n, and $k > 3$. We believe, that such a construction exists, and that in this construction more restrictions on the parameter h, and n_0 will be specified.

Acknowledgements: The research was supported by the Slovak National Grant Agency VEGA No. 1/0161/03.

References:

[1] R.A. Brualdi, H.J. Ryser, *Combinatorial Matrix Theory.* Cambridge University Press, Cambridge 1991.

[2] J. Daemen, V. Rijmen, *The Design of Rijndael.* Springer–Verlag, Berlin–Heidelberg–New York–Tokyo 2002.

[3] Z. Füredi, P. Horák, Xuding Zhu, *Oriented graphs of diameter 2.* Graphs and Combinatorics 14, 1998, pp. 345–350.

[4] O. Grošek, P. Horák, P. Zajac, *Efficient Mixing Transformations for Block Ciphers.* Submitted, 2005.

[5] M. Hall, Jr.: *Combinatorial Theory.* Blaisdell Pub. Comp., Waltham, 1967.

[6] M. Šimovcová, M. Vojvoda, *Symmetric and Complementary Boolean Functions.* Proceedings of Elitech 2001, STU-FEI, Bratislava, 2002, pp.89-90.

[7] P. Zajac, *Remark to the mixing layer of SPN ciphers.* Journal of Electrical Engineering. Accepted for publication, 2005.