Discrete Mathematics 309 (2009) 5527–5534

Contents lists available at ScienceDirect

Discrete Mathematics

journal homepage: www.elsevier.com/locate/disc

On complexity of round transformations

Otokar Grošek [a], Peter Horák [b,*], Pavol Zajac [a]

[a] Department of Applied Informatics and Information Technology, Slovak University of Technology, Bratislava, Slovakia
[b] IAS, University of Washington, Tacoma, USA

ARTICLE INFO

Article history:
Received 29 October 2006
Received in revised form 4 May 2007
Accepted 21 March 2008
Available online 9 May 2008

Keywords:
Block ciphers design
Round function

ABSTRACT

A modern block cipher consists of round transformations, which are obtained by alternatively applying permutations (P-boxes) and substitutions (S-boxes). Clearly, the most important attribute of a block cipher is its security. However, with respect to the hardware implementation, a good block cipher has to have a reasonable complexity as well. In this paper, we study complexity of round transformations satisfying some basic security criteria. There are several ways to define the complexity of a round transformation, and to choose "necessary" security criteria. It turns out, that for our purpose, it is suitable to view a round transformation as a single Boolean function, not separating it into S-boxes and P-boxes. We require that the Boolean function F possesses some fundamental properties imposed on each block cipher for security reasons; namely, we require that the function is a strictly non-linear bijection and that it has a good diffusion. The total number of variables in the normal algebraic form of the component functions of F is taken as its complexity. We find the minimum complexity of such functions, and this way we establish a lower bound on complexity of all round transformations. To show that the lower bound is the best possible, we construct a round transformation F' attaining the bound. We stress that it is not an aspiration of this paper to construct a round transformation which would be of practical use; F' is useful only from the theoretical point of view.

1. Introduction

The idea of a modern block cipher goes back to 1949, when Shannon introduced round transformations [10]. 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 is a single large permutation used to mix these parts together. Design of good S-boxes is well understood [1–3,5,7,9,12]. An alternative construction by means of coordinate functions is suggested in e.g. [11,13]. Much work on an efficient P-box has been done by designers of AES [5]. They call it wide trail strategy, and the main goal is to prevent a cryptosystem against differential and linear cryptanalysis.

Clearly, the most important attribute of a block cipher is its security. However, with respect to the hardware implementation, a good block cipher has to have a reasonable complexity as well. Therefore, in this paper, we study complexity of round transformations satisfying some basic security criteria. Clearly, there are several ways how to define the complexity of a round transformation, and how to choose "necessary" security criteria. It turns out, that for our purpose, it is suitable to

* Corresponding author.
E-mail addresses: otokar.grosek@stuba.sk (O. Grošek), horak@u.washington.edu (P. Horák), pavol.zajac@stuba.sk (P. Zajac).

0012-365X/$ – see front matter © 2008 Elsevier B.V. All rights reserved.
doi:10.1016/j.disc.2008.03.020

view a round transformation as a single Boolean function, not separating it into S-boxes and P-boxes. We will call such a function the mixing transformation. So, we require that the Boolean function F possesses some fundamental properties imposed on each block cipher for security reasons; namely, we require that F is a strictly non-linear bijection and that it has a good diffusion. The total number of variables in the normal algebraic form of the component functions of F (i.e. the number of so called active variables) is taken as its complexity. We find the minimum complexity of such functions, and this way we establish a lower bound on complexity of all round transformations. To show that the lower bound is the best possible, we construct a round transformation F' attaining the bound. Of course, F' does not have to have good security, but it will provide a lower bound on complexity of all round transformations used in real life applications. We stress once more, that it is not an aspiration of the paper to construct a round transformation which would be of practical use; F' is useful only from the theoretical point of view.

We point out that Boolean functions that are strictly non-linear bijections achieving a complete diffusion in one round have already been studied in [8] from the S-box design point of view. However, the functions constructed there have a large number of active variables and therefore they are difficult to implement in some architectures; hence they are used only in constructions of S-boxes for small n, usually $n = 8$.

The notion of a non-linear function is standard through the literature. However, we are very well aware that the manner how we define the notions of good diffusion and the complexity of a mixing transformation is only one of many possible ways. We hope that this paper will initiate study in this direction.

Now we will formally define how we understand good diffusion and the complexity of a mixing transformation. Let $F \in \mathcal{F}_n$, where $\mathcal{F}_n$ is the family of all Boolean functions on Z_2^n, that is, $F = (f_1, f_2, \ldots, f_n)$, where $f_i : Z_2^n \to Z_2$, $i = 1, \ldots, n$, are called component functions. In order to be able to define the complexity of 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

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

where the symbol $\oplus$ represents *XOR*, and $e^{(i)}$ stands for the word with the only 1 in the ith position. Further, we set $\delta(F) = \sum_{i=1}^{n} \sum_{j=1}^{n} a_{ij}$.

We point out that, in other words, $a_{ij} = 1$ if and only if the variable x_i occurs in the normal algebraic form of f_j. Therefore, $\delta(F)$ is the total number of active variables in component functions of F.

It can be shown that the minimal number of wires connecting inputs and outputs of the hardware realization of F is proportional to $\delta(F)$. As a natural criterion for hardware implementation, we would like to minimize $\delta(F)$. Therefore we set the complexity of F to equal $\delta(F)$.

On the other hand, as the round function has to guarantee that each output bit depends on all input bits (= the complete diffusion), 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 $\Phi(F \circ F \circ \cdots \circ F) = J_n$. That is, the first application of the round function F, a change of an input bit x_i affects only few output bits, but the remaining output bits will be affected in the following iterations of the transformation. With respect to time needed for encryption the ideal situation occurs if the required property of F is obtained after two rounds, that is, if $\Phi(F \circ F) = J_n$. Thus, in this paper, by a good diffusion we mean the property that $\Phi(F \circ F) = J_n$. We are very well aware that is a typical trade-off situation. One would be able to further decrease $\delta(F)$ by allowing more iterations of F before reaching the complete diffusion, but more time would be needed for encryption. If the approach to measuring complexity introduced in the paper will attract some interest, one can consider in the future studying the minimum complexity of block ciphers where three or more iterations are needed for the complete diffusion.

As aforementioned, we require that mixing transformation is non-linear because a cipher with linear round function can be broken by linear algebra. In fact, we impose a stronger condition on F. We will require that F is strictly non-linear, that is, any linear combination of component functions is nonlinear in order not to compromise any part of the key. In addition, for obvious reasons, a mixing transformation has to be a bijection.

The main result of this paper claims that if F is strictly non-linear bijection in $\mathcal{F}_n$, and $\Phi(F \circ F) = J_n$, then $\delta(F) \geq 4n - 4$, and by a construction of a suitable function F we show that this bound is best possible. Of course, imposing further security criteria (e.g. propagation criteria, [8]) on our mixing transformation would increase its complexity. An interesting open question is whether then there exists such mixing transformation F having linear complexity $\delta(F) = cn$ with small c. The positive answer might lead to strong scalable block ciphers and hash functions.

The paper is organized as follows. In the next section we introduce the notion of an ideal mixing transformation. Section 3 contains the main result of the paper, while in the last section we compare the round functions of well known ciphers DES and Rijndael with the ideal mixing transformation defined in this paper.

2. Ideal mixing transformations

Let Z_2^n be the set of binary words of length n. The elements of Z_2^n will be denoted by small letters in the standard font, while by $\mathbf{x}$, $\mathbf{x} = (x_1, \ldots, x_n)$, in the bold font we will denote a variable from Z_2^n.