X-Authentication-Warning: teak.ii.uib.no: larsr owned process doing -bs
Date: Fri, 7 Apr 2000 14:49:42 +0200 (MET DST)
From: Lars Ramkilde Knudsen <Lars.Knudsen@ii.uib.no>
To: AESRound2@nist.gov
cc: Lars Ramkilde Knudsen <Lars.Knudsen@ii.uib.no>
Subject: mars note

Dear Sir(s),

Please find enclosed a 2Round comment on MARS.

Best regards

Lars R. Knudsen, Assoc.Prof., Univ. of Bergen, Dept.of Informatics,
PB 7800, N-5020 Bergen, Norway +47 55 58 41 57, (fax +47 55 58 41 99),
Lars.Knudsen@ii.uib.no, http://www.ii.uib.no/~larsr/

Linear approximations to the MARS S-box

Lars R. Knudsen and Håvard Raddum
Department of Informatics, University of Bergen

April 6, 2000

Abstract

One of the components of the cipher MARS, one of the AES finalists, is a 9x32 bit S-box. The designers have conjectured that there exists no linear approximation to the S-box with a bias higher than 2^{-3}. We give several examples of approximations that exceed this bound.

1 Introduction

IBM's submission to AES is the cipher MARS. The details of the cipher can be found in [1]. One of the components of the cipher is a 9x32 bit S-box. The designers list several properties they require their S-box to have, and they have some comments on linear and differential cryptanalysis of the S-box. In [2] it is pointed out that the S-box actually fails to have all the properties the designers required. Below we will show that there are linear approximations to the S-box with biases higher than 1/8, contradicting a conjecture by the MARS designers.

2 Linear approximations

We will briefly recall the terminology used in linear cryptanalysis. A *mask* X is a bitstring of fixed length. An *approximation* to some bitstrings $w_1, \ldots, w_n$ with the masks $X_1, \ldots, X_n$ is defined as $(X_1 \bullet w_1) \oplus (X_2 \bullet w_2) \oplus \ldots \oplus (X_n \bullet w_n)$, where $X_i \bullet w_i$ is the inner product. The *bias* of an approximation is defined as $|\frac{1}{2} - Pr(\oplus_{i=1}^{n}(X_i \bullet w_i) = 0)|$ where the probability is taken over all values of w_i.

An approximation to the S-box used in MARS will consist of a mask X_1 of length 9 and a mask X_2 of length 32. We let w_1 denote the nine input bits, and w_2 denote the 32 output bits. (w_1, w_2) can take on only $2^9 = 512$ different values, so it is easy to calculate the bias to any particular approximation. In [1] it is conjectured there exists no approximation with a bias higher than 2^{-3}. We fixed X_1 to be all zeros, and let X_2 take on all 2^{32} possible values. We computed the bias to every mask, and kept a record of the masks that gave high biases. The highest biases were found for the masks $X_2 = 939092D8_x$ and $X_2 = 16220880_x$ written in hex notation. The first mask gives a probability of $\frac{324}{512}$, the second a probability of $\frac{188}{512}$. The bias is in both cases $\frac{68}{512} \approx 2^{-2.91}$. As can be seen, both of these masks gives a bias higher than the designers of MARS imagined.

We also made a search with masks where X_1 takes on different non-zero values. Doing an exhaustive search letting (X_1, X_2) take on all 2^{41} values would require too much computing power for our resources. However, by just picking random values for X_1 and X_2 we have found 871 approximations with a bias bigger than 1/8. The mask giving the highest bias we have found is $X_1 = 120_x$ and $X_2 = CC96E27E_x$ (the one in X_1 denotes that the first bit is one). This mask gives a bias of $\frac{82}{512} \approx 2^{-2.64}$.

References

[1] Carlynn Burwick et al., *MARS - a candidate cipher for AES*, http://www.research.ibm.com/security/mars.html

[2] L. Burnett, G. Carter, E. Dawson and W. Millan, *Efficient Methods for Generating MARS-like S-boxes*. Accepted for FSE'2000.