Quadratic relations in Khazad and Whirlpool *[*]
NES/DOC/UIB/WP5/017/1

Lars R. Knudsen, UiB etc.

June 27, 2002

Abstract

In this note it is examined whether there exist quadratic relations with certainty over the input and output bits of the S-boxes of Khazad and Whirlpool. The answer is negative.

1 Introduction

Whirlpool is a (conjectured) one-way, collision-resistant hash function, which produces a 512-bit hash result. Khazad is a 64-bit block cipher with a 128-bit key. Both Khazad and Whirlpool have been submitted to NESSIE.

2 Quadratic relations

In [3] it is shown that for the S-boxes of Rijndael and Serpent there exist quadratic equations in the input and outputs bits which hold with probability one. Such equations always exist for n-bit to n-bit S-boxes, where $n \leq 6$, but not in general for $n > 6$. Therefore, for Serpent versions with four-bit S-boxes, such equations would always exist, while for versions of Rijndael they would not, e.g., with a randomly chosen 8-bit S-box such equations are unlikely to exist.

It is shown [3] that these equations can be used to describe a system of multivariate equations in the input and output bits of the entire encryption engines of Rijndael and Serpent. It is further conjectured that these systems of equations can be solved in time faster than the time of an exhaustive search for the key for some versions of the ciphers. The conjecture is still unproven.

In this note, we investigate whether such quadratic relations exist for the S-box of Khazad and and for S-box of Whirlpool. Both S-boxes are permutations of eight bits. Let the input be $x = x_0, \ldots, x_7$ and the corresponding output $y = y_0, \ldots, y_7$. Then we are looking for equations

$$p(x_0, \ldots, x_7, y_0, \ldots, y_7) = 0,$$

where the degrees of the terms in p are at most two. There are

$$\left(\begin{array}{c} 8 \\ 0 \end{array}\right) + 2\left(\begin{array}{c} 8 \\ 1 \end{array}\right) + 2\left(\begin{array}{c} 8 \\ 2 \end{array}\right) + \left(\begin{array}{c} 8 \\ 1 \end{array}\right)\left(\begin{array}{c} 8 \\ 1 \end{array}\right) = 137$$

[*] This work was supported by the European Union fund IST-1999-12324 - Nessie. The information in this document is provided as is, and no warranty is given or implied that the information is fit for any particular purpose. The user thereof uses the information at its sole risk and liability.

possible terms of degree at most two in a multivariate expression of the eight input and output bits. It is a simple matter to check whether such equations exist simply by computing the kernel of a 256 times 137 binary matrix. We implemented this in Maple. It was found that for the Khazad and Whirlpool S-boxes there are no quadratic equations which hold with certainty, while for the Rijndael S-box there are 39 (independent ones).

References

[1] Paulo S.L.M. Barreto and Vincent Rijmen. The KHAZAD Legacy-Level Block Cipher. Submission to NESSIE. See www.cryptonessie.org.

[2] Paulo S.L.M. Barreto and Vincent Rijmen. The WHIRLPOOL Hashing Function. Submission to NESSIE. See www.cryptonessie.org.

[3] N.T.Courtois and Josef Pieprzyk. Cryptanalysis of Block Ciphers with Overdefined Systems of Equations. Available at http://eprint.iacr.org, 2002/044.