New Multiset Attacks on Rijndael with Large Blocks

Jorge Nakahara Jr.[1], Daniel Santana de Freitas[2], and Raphael C.-W. Phan[3]

[1] UniSantos, Brazil
jorge_nakahara@yahoo.com.br
[2] LabSEC, INE, Federal University of Santa Catarina, Brazil
santana@inf.ufsc.br
[3] iSECURES Lab, Swinburne University of Technology (Sarawak Campus), Malaysia
rphan@swinburne.edu.my

Abstract. This paper presents the first security evaluation of the **Rijndael cipher with block sizes larger than 128 bits**. We describe new higher-order multiset distinguishers for such large-block instances of Rijndael. Both Rijndael and the AES were designed to resist differential and linear cryptanalysis, which is indicated by the number of active S-boxes (minimum of 25 for 4-round AES) for the best differential and linear distinguishers, for which the probability and correlation values are estimated as 2^{-150} and 2^{-75}. All of these Rijndael variants have been formally defined by their designers as extensions of the AES. We describe new 5-round distinguishers for Rijndael with 160 up to 256-bit blocks, all holding with certainty, and with many more than 25 active S-boxes.

Keywords: Rijndael, higher-order multiset attacks, cryptanalysis.

1 Introduction

Rijndael is an SPN-type cipher designed by J. Daemen and V. Rijmen for the AES Development Process [17]. Both the block and key sizes can range from 128 up to 256 bits in steps of 32 bits [6, p.42]. The number of rounds is variable, depending on the block and key lengths. There are 25 instances of Rijndael formally defined by their designers [6,13] for all possible combinations of key and block sizes (Table 1). The 128-bit block version of Rijndael is officially known as the AES [17]. The other variants will be denoted Rijndael-160, Rijndael-192, Rijndael-224 and Rijndael-256, with the suffix indicating the block size in bits. The text and key blocks are usually represented by a $4 \times t$ state matrix of bytes, $4 \leq t \leq 8$. For instance, the state matrix for a $4t$-byte ($32t$-bit) text block, $A = (a_0, a_1, a_2, a_3, a_4, \ldots, a_{4t-1})$, is

$$\text{State} = \begin{pmatrix} a_0 & a_4 & \ldots & a_{4t-4} \\ a_1 & a_5 & \ldots & a_{4t-3} \\ a_2 & a_6 & \ldots & a_{4t-2} \\ a_3 & a_7 & \ldots & a_{4t-1} \end{pmatrix}, \tag{1}$$

E. Dawson and S. Vaudenay (Eds.): Mycrypt 2005, LNCS 3715, pp. 277–295, 2005.

namely, with the bytes filled columnwise. The AES has been extensively analyzed since 1997 but the same cannot be said of the other variants, most probably because they were not standardized as the AES. Rijndael-256, with a 256-bit key, had its software performance evaluated in the NESSIE Project [16], but there was no security analysis. However, analysis of these sisters of the AES may shed further light into the design of the AES and its structure as well as resistance against cryptanalysis.

This paper describes higher-order multiset distinguishers that consist, and therefore trace, the status of 128-bit words, instead of bytes as in [5]. Since our attacks require sets of 2^{128} chosen plaintexts at a time, the attacks do not apply to the AES, whose codebook size is 2^{128}. Nonetheless, this paper presents the first security evaluation of Rijndael with block sizes larger than 128 bits.

Table 1. Parameters of the Rijndael block cipher [6]

		Cipher				
		AES	**Rijndael-160**	**Rijndael-192**	**Rijndael-224**	**Rijndael-256**
Nr (# rounds)		Nb (# 32-bit words)				
		4	5	6	7	8
Nk (# 32-bit words)	4	10	11	12	13	14
	5	11	11	12	13	14
	6	12	12	12	13	14
	7	13	13	13	13	14
	8	14	14	14	14	14
ShiftRows Offsets	C_1	1	1	1	1	1
	C_2	2	2	2	2	3
	C_3	3	3	3	4	4

There are four layers in a full round transformation in Rijndael: AddRoundKey ($\mathbf{AK}_i$), SubBytes ($\mathbf{SB}_i$), ShiftRows ($\mathbf{SR}_i$) and MixColumns ($\mathbf{MC}_i$), all of which will be referred to as quarters of a round, or 0.25-round, so that distinguishers and attacks can be described more precisely. The subscripts i indicate the round number. One full round of Rijndael consists of $\mathrm{AK}_i \circ \mathrm{MC}_i \circ \mathrm{SR}_i \circ \mathrm{SB}_i(X) = \mathrm{AK}_i(\mathrm{MC}_i(\mathrm{SR}_i(\mathrm{SB}_i(X))))$, namely instantiation is in right-to-left order. There is an input transformation, AK_0 prior to the first round, and the last round does not include MC_i. For further details about Rijndael components refer to [6].

The paper is organized as follows: Sect. 2 gives basic definitions for the multiset attack. Sect. 3.1 describes attacks on Rijndael-160. Sect. 3.2 describes attacks on Rijndael-192. Sect. 3.3 describes attacks on Rijndael-224. Sect. 3.4 describes attacks on Rijndael-256. Sect. 4 concludes the paper.

2 Preliminaries

The multiset technique [2] has similarities with the Square attack [5], the saturation attack [14] and with integral cryptanalysis [10,12]. All of these techniques