Cryptanalysis of Ake98

Jorge Nakahara Júnior¹ and Daniel Santana de Freitas²

¹ jorge_nakahara@yahoo.com.br
² LabSEC, Laboratório de Segurança em Computação, UFSC, Brazil santana@inf.ufsc.br

Abstract. This paper describes a linear attack on the Ake98 block cipher, an updated version of the Akelarre cipher presented by Alvarez et al. at the SAC’96 Workshop. The new attacks require the assumption of weak keys. It is demonstrated that Ake98 does not introduce enough security measures to counter cryptanalytic attacks, both in a known-plaintext and in a ciphertext-only setting. A key-recovery attack on 4.5-round Ake98, for instance, is applicable to a weak-key class of size $2^{108}$, and requires only 71 known plaintexts, with an effort of $71 \cdot 2^{71}$ half-round decryptions. Moreover, the existence of weak keys precludes the use of Ake98 as a building block for other cryptographic primitives, such as in Davies-Meyer Hash mode. Attacks using weak keys can be applied up to 11.5 rounds of Ake98 with less effort than an exhaustive key search. But, Ake98 with 8.5 rounds is already slower than IDEA, RC6 or AES, which implies that this updated version of the Akelarre cipher does not seem to provide significant advantages (security or efficiency) compared to the former, more established ciphers.

Keywords: cryptanalysis, Akelarre, Ake98, IDEA, RC5, RC6, AES.

1 Introduction

Akelarre is a block cipher designed by Alvarez et al. [4] and presented at SAC’96 Workshop. Akelarre combines design features from the IDEA [9] and RC5 [11] ciphers, and processes 128-bit text blocks, uses a 128-bit key, and iterates 4 rounds plus an output transformation (OT). The operations of modular addition, $\oplus$, and exclusive-or, $\oplus$, were inherited from IDEA, while bitwise rotation, $\ll$, came from RC5. In [8], Knudsen and Rijmen presented known-plaintext and ciphertext-only attacks on Akelarre for any number of rounds, and that are independent of the key schedule algorithm. Further attacks were also presented by Ferguson and Schneier in [6], but using chosen plaintext.

Subsequently, the designers of Akelarre presented Ake98 [3] that is claimed to avoid the previous attacks on Akelarre.

This paper is organized as follows: Sect. 2 describes briefly the Akelarre block cipher; Sect. 3 describes Ake98 and the main differences with Akelarre. Sect. 4 explains the attack on Ake98, its similarity to the attack of Knudsen-Rijmen, the attack requirements and its complexity. Subsect. 4.2 describes a ciphertext-only attack on Ake98. Sect. 5 compares the software performance of Ake98 with that of AES, IDEA and RC6. Sect. 6 concludes the paper.
2 The Akelarre Cipher

The Akelarre block cipher was presented at the SAC’96 workshop, and its design combines features from the IDEA and RC5 ciphers. Akelarre uses three operations on $w$-bit words: bitwise exclusive-or, denoted $\oplus$, addition modulo $2^w$, denoted $\boxplus$, and bitwise rotation, denoted $\ll$. The multiplication operation of IDEA is absent. A note on terminology: the notation $\text{lsb}_i(X)$ (lower case) will denote the $i$-th least significant bit(s) of $X$, while $\text{LSB}_i(X)$ (upper case) will denote the ensemble of $i$ consecutive least significant bits.

All of the internal operations in Akelarre are on $w$-bit words. Akelarre operates on variable-length words, text blocks and keys, and uses a variable number of rounds. The suggested parameter values in [4] are: 128-bit blocks, 32-bit words, 128-bit key and 4 rounds. Fig. 1 depicts the computational graph of Akelarre. The MA-box of IDEA becomes an AR-box (Addition-Rotation box). Details of the AR-box are given in the Appendix.

The key schedule algorithm of Akelarre will not be described in this paper but the interested reader can find further information in [4].

---

For example, if $X = 01101110_2$ in binary, then $\text{lsb}_1(X) = 0$, $\text{lsb}_2(X) = 1$, but $\text{LSB}_2(X) = 2$, and $\text{LSB}_3(X) = 6$. 

---

Fig. 1. Computational graph of the Akelarre block cipher