The Journal of Systems and Software 84 (2011) 1685–1692

Contents lists available at ScienceDirect

The Journal of Systems and Software

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

A meet-in-the-middle attack on reduced-round ARIA

Xuehai Tang[a,*], Bing Sun[a,b], Ruilin Li[a], Chao Li[a], Juhua Yin[c]

[a] Department of Mathematics and System Science, Science College of National University of Defense Technology, Changsha, Hunan, P.R. China
[b] State Key Laboratory of Information Security, Graduate University of Chinese Academy of Sciences, Beijing, P.R. China
[c] Bayinguoleng Vocational and Technical College, Korla, Xinjiang, P.R. China

ARTICLE INFO

Article history:
Received 29 November 2010
Received in revised form 4 March 2011
Accepted 18 April 2011
Available online 30 April 2011

Keywords:
Block cipher
ARIA
Meet-in-the-middle

ABSTRACT

In this paper, the meet-in-the-middle attack against block cipher ARIA is presented for the first time. Some new 3-round and 4-round distinguishing properties of ARIA are found. Based on the 3-round distinguishing property, we can apply the meet-in-the-middle attack with up to 6 rounds for all versions of ARIA. Based on the 4-round distinguishing property, we can mount a successful attack on 8-round ARIA-256 for the first time. Furthermore, the 4-round distinguishing property could be improved which leads to a 7-round attack on ARIA-192. Compared with the existing cryptanalytic results on ARIA, the meet-in-the-middle attack has a huge precomputation and memory complexities. However, we can do the precomputation once and for all. These results show that 8-round ARIA-256 is not immune to the meet-in-the-middle attack.

1. Introduction

ARIA (Kwon et al., 2004) is a 128-bit block cipher designed by a group of Korean experts in 2003. Its design adopts the same idea (wide trail strategy) of the Advanced Encryption Standard (AES). It was later established as a Korean Standard by the Ministry of Commerce, Industry and Energy in 2004. ARIA supports key length of 128, 192 and 256 bits, these versions of ARIA are denoted as ARIA-128, ARIA-192 and ARIA-256. The number of rounds for these three versions is 12, 14 and 16, respectively.

The security of ARIA was analyzed by many cryptographers. The designers of ARIA, Kwon et al. (2004) presented some cryptanalysis including both differential cryptanalysis, linear cryptanalysis, and some other known attacks. Later, Biryukov et al. (2004) performed an evaluation of ARIA, however, they especially focused on truncated differential cryptanalysis and dedicated linear cryptanalysis. Wu et al. (2007) firstly found some non-trivial 4-round impossible differentials which led to a 6-round attack of ARIA. Li et al. (2008) presented an algorithm to find many new 4-round impossible differentials which can improve the 6-round impossible differential attack. The security of ARIA against boomerang attack was presented by Fleischmann et al. (2009). And recently, Li et al. (2009, 2010) studied the integral attack of ARIA. The meet-in-the-middle attack on AES was firstly introduced by Demirci and Selçuk (2008). Inspired by their work, we construct some new 3/4-round distinguishing properties of ARIA and use them to apply the meet-in-the-middle attack against reduced-round ARIA. Based on the 3-round distinguishing property, we can attack all versions of ARIA with up to 6 rounds. Based on the 4-round distinguishing property, we can mount a successful attack on 8-round ARIA-256 for the first time. Furthermore, we improve the 4-round distinguishing property and use it to attack 7-round ARIA-192. Although this kind of attack has a huge precomputation and memory complexity, we do the precomputation once and for all. To validate the correctness of the meet-in-the-middle attack, we also do some experiments on 3-round ARIA.

The rest of this paper is organized as follows: We describe the meet-in-the-middle attack on block ciphers in Section 2 and give a brief description of ARIA in Section 3. In Section 4, we construct some 3/4-round distinguishing properties of ARIA and present the meet-in-the-middle attacks on reduced-round ARIA. We show some experimental results of the meet-in-the-middle attack on 3-round ARIA in Section 5. Finally, Section 6 summarizes this paper.

2. The meet-in-the-middle attack on block ciphers

The idea of meet-in-the-middle attack on block ciphers was firstly introduced by Diffie and Hellman (1977) in cryptanalysis of Two-DES. Recently, Demirci and Selçuk (2008) and Demirci et al. (2009) extended the meet-in-the-middle attack in a more generalized case and applied it to attack 8-round AES-256 based on some 5-round distinguishing property, which originates from an early 4-round distinguishing property constructed by Henri and Minier (2000).

In this section, we describe in detail the generalized meet-in-the-middle attack against iterative block ciphers.

* Corresponding author. Tel.: +86 13755054594; fax: +86 073184574234.
E-mail address: txh0203@163.com (X. Tang).

0164-1212/$ – see front matter © 2011 Elsevier Inc. All rights reserved.
doi:10.1016/j.jss.2011.04.053

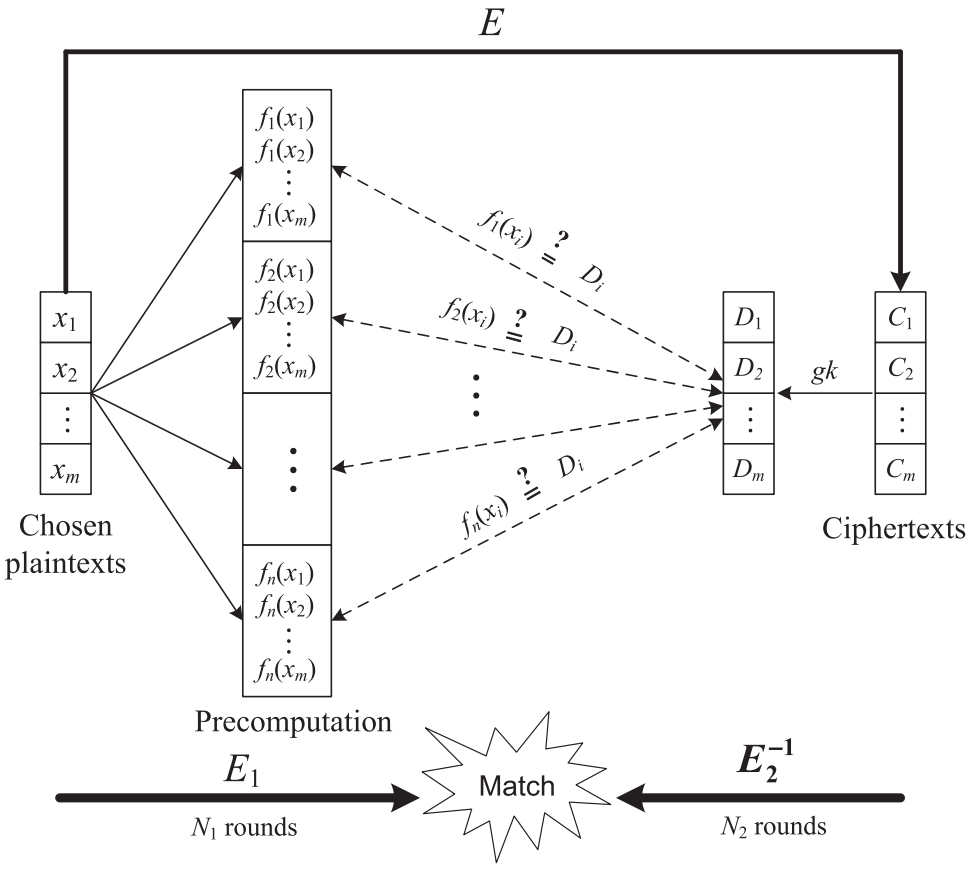

Fig. 1. The meet-in-the-middle attack on block ciphers.

Let an N-round block cipher be

$$C = E(P, K), \tag{1}$$

where C, P and K denote ciphertext, plaintext and the user key, respectively. The encryption procedure is treated as a concatenation of two consecutive encryptions, namely E_1 and E_2, i.e. $E = E_2 \circ E_1$, where E_1 is the first N_1 rounds encryption and E_2 the last $N_2 = N - N_1$ rounds encryption, thus

$$C = E_2(E_1(P, K_1), K_2), \tag{2}$$

where K_1 and K_2 are the subkeys of the first N_1 and the last N_2 rounds, respectively.

If we consider m different plaintexts with the feature that they are different at some fixed bits(denoted as x) only and the rest bits are constant values. Denote the m plaintexts as $x_1, x_2, \ldots, x_m$, encrypt the m plaintexts with the first N_1 rounds, we can compute the ciphertexts $C_i^* = E(x_i, K_1)$, where $1 \le i \le m$. Usually, we consider a partial bits of C_i^*, denoted as c_i. Note that the constant values in the plaintexts and K_1 are fixed for each ciphertext c_i, then c_i can be expressed as the function with the variable x_i:

$$c_i = f(x_i) \tag{3}$$

where f is determined by some parameters and the subkey K_1 is included in the parameters. If the number of parameters in $f(x)$ is small enough, we can search exhaustively all the parameters and the right subkey K_1 must be included. In other words, for each possible parameter, we can obtain a mapping $f(x_i) : x_i \to c_i$, thus we can obtain many mappings and only one mapping is correct.

The attack procedure is described in Fig. 1:

Firstly, choose a set of m suitable plaintexts which are different at some fixed bits (denoted as $x_1, x_2, \ldots, x_m$), compute and store $f(x_i)$ for each possible f. This step is called the precomputation phase. Assume that there are n possible parameters for the function f, then there are n possible functions f, denoted as $f_1, f_2, \ldots, f_n$.

Secondly, encrypt the m plaintexts with N rounds and the ciphertexts are denoted as $C_1, C_2, \ldots, C_m$, then search certain subkey gk, do a partial N_2 rounds decryption and obtain $D_i = E_2^{-1}(C_i, gk)$, note that the position of D_i in the data state is the same as c_i, so they have the same length.

Thirdly, check whether $D_i = f_j(x_i)(1 \le i \le m)$ hold for some $f_j(1 \le j \le n)$, once an f_j is found so that $D_i = f_j(x_i)(1 \le i \le m)$, we call a match is found and the guessed subkey gk is most likely correct since the probability of having a match for a wrong key is approximately $n \times 2^{-k \times m}$, where k is the length of D_i, i.e. D_i is k-bit length. Then if m is big enough, all wrong keys can be excluded.

Note that in the precomputation phase, the number of the parameters in f cannot be too large since the precomputation complexity would exceed the exhaustive search attack if n is too large. On the other hand, in the attack phases, sometimes we filtrate the wrong subkeys according to checking whether $f_j(x_i) \oplus f_j(x_{i'}) = D_i \oplus D_{i'}$ holds, because in this way we can reduce the precomputation complexity or guess less subkeys in the partial decryption phase. For the first case, we give an example: Assume that the function $f(x) = g(x) \oplus c$, where c is a parameter, then $f(x_i) \oplus f(x_{i'}) = g(x_i) \oplus g(x_{i'})$ and the parameter c can be ignored in the precomputation phase. For the second case, one will see it be used in our attacks on reduced-round ARIA in Section 4.

3. Description of ARIA

ARIA adopts a substitution-permutation network (SPN) and employs an involutional binary 16×16 matrix over $GF(2^8)$ in its diffusion layer. The substitution layer consists of sixteen 8×8-bit S-boxes based on the inversion in $GF(2^8)$. The 128-bit plain-