Information Processing Letters 116 (2016) 136–143

Contents lists available at ScienceDirect

Information Processing Letters

www.elsevier.com/locate/ipl

Improved improbable differential attacks on ISO standard CLEFIA: Expansion technique revisited

Cihangir Tezcan [a,b,c,*], Ali Aydın Selçuk [d]

[a] Department of Mathematics, Middle East Technical University, Ankara, Turkey
[b] Institute of Informatics, Department of Cyber Security, CYDES Laboratory, Middle East Technical University, Ankara, Turkey
[c] Institute of Applied Mathematics, Department of Cryptography, Middle East Technical University, Ankara, Turkey
[d] Department of Computer Engineering, TOBB University of Economics and Technology, Ankara, Turkey

ARTICLE INFO

Article history:
Received 18 July 2014
Received in revised form 10 July 2015
Accepted 18 September 2015
Available online 26 September 2015
Communicated by Marc Fischlin

Keywords:
Cryptography
Analysis of algorithms
Computational complexity
Improbable differential attack
CLEFIA

ABSTRACT

Improbable differential cryptanalysis is a recent attack technique that generalizes impossible differential cryptanalysis for block ciphers. In this paper, we give the most effective attacks known to date on the CLEFIA cipher using improbable differential cryptanalysis. Moreover, we provide a general data complexity calculation that can guide the cryptanalyst to choose the optimal improbable differential. On a related account, we consider the probability calculations used for improbable differential cryptanalysis. Recently, some examples were given where certain assumptions in these calculations do not hold. Although such cases exist, especially on small toy ciphers with insufficient diffusion, we provide experimental evidence which supports that the improbable differential attacks on CLEFIA and PRESENT are valid.

1. Introduction

Differential cryptanalysis [2] and its variants exploit differentials of a cipher that are more probable than a random permutation, with the exception of impossible differential cryptanalysis [1] which exploits differentials with probability zero. Recently, Tezcan [14] introduced improbable differential cryptanalysis to bridge this gap where a differential that is less probable than a random permutation is exploited as a distinguisher.

CLEFIA [12] is a 128-bit block cipher developed by Sony Corporation in 2007. It has been internationally standardized by ISO [9] as a lightweight block cipher. Despite its relatively short history, CLEFIA has been extensively analyzed by researchers. The best impossible differential attacks the designers could find were on 10, 11, and 12 rounds of CLEFIA but in [18], Tsunoo et al. provided new impossible differentials and provided 12, 13, and 14-round attacks on CLEFIA for key sizes 128, 192, and 256, respectively. In [14], Tezcan extended the impossible differential attacks of [18] to improbable differential attacks on 13, 14, and 15-round CLEFIA for key sizes 128, 192, and 256, respectively. Later on, Mala et al. [10] provided a 13-round impossible differential attack for the 128-bit key size and Bogdanov et al. [6] provided 14 and 15-round zero-correlation linear attacks for 192 and 256-bit key sizes, respectively which have better complexities than the improbable differential attacks of [14].

In this work we improve the improbable differential attacks of [14] and provide the best known attacks on CLEFIA. Our improvements are threefold: we modify the impossible differential, we modify the characteristics (the "expansion") combined with the impossible differential, and we exploit a weakness in the key schedule of CLEFIA. Attacks on CLEFIA are summarized in Table 1.

We also deal with the success probability and data complexity of improbable differential attacks in general.

* Corresponding author.
E-mail address: cihangir@metu.edu.tr (C. Tezcan).

http://dx.doi.org/10.1016/j.ipl.2015.09.010
0020-0190/

Table 1
Comparison of our attack with the previous attacks on CLEFIA. Our attack is among the deepest penetrating attacks on all key sizes of CLEFIA. Furthermore, it has the best data and time complexities on all versions.

#Rounds	Attack	Key size	Data	Time	Memory	Reference
12	Impossible	All	$2^{118.9}$ CP	2^{119} En	2^{73} blocks	[18]
12	Impossible	All	2^{108} CP	2^{108} En	2^{99} blocks	[17]
13	Improbable	All	$2^{126.83}$ CP	$2^{126.83}$ En	$2^{101.32}$ blocks	[14]
13	Impossible	128	$2^{119.4}$ CP	$2^{125.52}$ En	$2^{119.4}$ blocks	[13]
13	Impossible	128	$2^{117.8}$ CP	$2^{121.2}$ En	$2^{86.8}$ blocks	[10]
13	**Improbable**	**All**	$\mathbf{2^{118.39}}$ **CP**	$\mathbf{2^{118.39}}$ **En**	$\mathbf{2^{109.46}}$ **blocks**	**This paper**
13	**Improbable**	**128**	$\mathbf{2^{116.78}}$ **CP**	$\mathbf{2^{116.98}}$ **En**	$\mathbf{2^{87.32}}$ **blocks**	**This paper**
13	Impossible	192, 256	$2^{119.8}$ CP	2^{146} En	2^{120} blocks	[18]
14	Improbable[a]	192, 256	$2^{127.43}$ CP	$2^{183.17}$ En	$2^{127.43}$ blocks	[14]
14	Multidim. ZC	192, 256	$2^{127.5}$ KP	$2^{180.2}$ En	2^{111} blocks	[6]
14	**Improbable**	**192, 256**	$\mathbf{2^{118.95}}$ **CP**	$\mathbf{2^{177.68}}$ **En**	$\mathbf{2^{118.95}}$ **blocks**	**This paper**
14	Impossible	256	$2^{120.3}$ CP	2^{212} En	2^{121} blocks	[18]
15	Improbable[b]	256	$2^{127.85}$ CP	$2^{247.49}$ En	$2^{127.85}$ blocks	[14]
15	Multidim. ZC	256	$2^{127.5}$ KP	$2^{244.08}$ En	2^{111} blocks	[6]
15	**Improbable**	**256**	$\mathbf{2^{119.35}}$ **CP**	$\mathbf{2^{242.08}}$ **En**	$\mathbf{2^{119.35}}$ **blocks**	**This paper**

[a] Due to a calculation error, in [14] the data and memory complexities of this attack were reported as $2^{126.98}$ instead of $2^{127.43}$.
[b] Due to a calculation error, in [14] the data and memory complexities of this attack were reported as $2^{127.40}$ instead of $2^{127.85}$.

Following the work of Blondeau et al. [4,5], we give a calculation for the data complexity of improbable differential attacks which can guide the cryptanalyst to choose the optimal improbable differential.

As a final note, we look into some recent studies [15,3] on improbable differential attacks where certain assumptions were shown not to hold in practice. We present experimental results which suggest that the same assumptions are mostly valid in our attack as well as Tezcan's previous attack on PRESENT [15].

2. Improbable differential cryptanalysis

Improbable differential attack [14] is a statistical differential attack where a given differential of a cipher is less probable than a random permutation. That is, we aim to find a differential with α input difference and β output difference so that these differences are observed with probability p_0 for the cipher and with probability p for a random permutation where $p_0 < p$. The impossible differential attacks can be seen as a special case of improbable differential cryptanalysis with $p_0 = 0$.

One way of obtaining an improbable differential is the *expansion method* [14], where a differential (or two) is combined with an impossible differential. Let $\delta \nrightarrow \beta$ be an impossible differential (i.e., $Pr(\delta \rightarrow \beta) = 0$), and $\alpha \rightarrow \delta$ be a differential with probability p'. By combining these two, we can construct the improbable differential $\alpha \rightarrow \beta$. Given that the output difference β has a probability of p for a random permutation, and assuming p is also the probability of β given $\alpha \nrightarrow \delta$, the combined differential $\alpha \rightarrow \beta$ has a probability $p_0 = (1 - p')p$, which is less than p. Although the difference between p_0 and p may seem tiny, as we will show, it can be used effectively to distinguish the right subkey.

As p_0 is less than p, the attack will use N plaintext pairs, count the hits each subkey value gets, and expect that the counter for the right subkey to be less than a threshold T. The number of hits a wrong (right) subkey gets can be seen as a random variable of a binomial distribution with parameters N and p (p_0). We denote the *non-detection* error probability, which is the probability of the counter for the right subkey to be higher than T, by p_{nd}; and the *false alarm* error probability, which is the probability of the counter for a wrong subkey to be less than or equal to T, by p_{fa}.

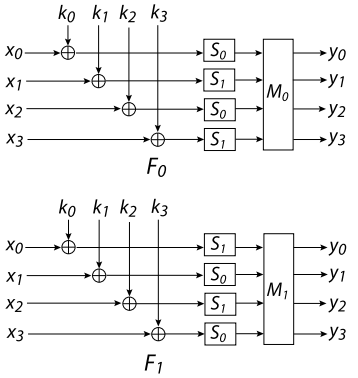

Fig. 1. F_0 and F_1 functions.

3. CLEFIA

CLEFIA [12] is a prominent cipher designed by Sony Corporation in 2007 and adopted as an international standard by ISO/IEC 29192-2:2012 [9] for lightweight cryptography, along with PRESENT [7].

CLEFIA has a 128-bit block size and a generalized Feistel structure with four data lines. It has 18, 22, and 26 rounds for the key lengths k of 128, 192, and 256 bits, respectively. Each round contains two parallel F functions, F_0 and F_1 as shown in Fig. 1, where S_0 and S_1 are 8×8-bit S-boxes. The two matrices M_0 and M_1 used in the F functions are defined as follows: