Differential fault analysis about feistel block cipher

Boliang Zhang[1.a], Dong Li [2, b]

[1] Electrinic Technology Department in Engineering University of CAPF,Xi'an,710086,China;

[2] Information engineering department, Engineering College of CAPF,Xi'an,710086,China

[a] triple1991@qq.com, [b]563783912@qq.com

Keywords: Light-weight block cipher,feistel,differential fault analysis,attack modle

Abstract. Light-weight block cipher is the protection of RDIF label and smart card in communication of Internet of things.It's safty is very important..The article analyzes the fault propagation of the traditional light-weight block cipher with feistel structure and proposing a deep differential fault analysis straregy. The method based on half byte fault attack principle, for the feistel light-weight block cipher, can get the corresponding key information according to the fault and correct ciphertext's difference. establishing single round half byte fault injection model, multiple-rounds half byte fault injection model, multiple-rounds of two half byte fault injection model these three different attack models for specific cryptographic algorithms can obtain the most efficient way to attack algorithm. At the same time, giving the experimental results of the l feistel algorithms LBlock.

1 Introduction

Internet of things [1] was formally put forward by the international telecommunication union (ITU) since 2005, making a big step forward for network technology. The Internet of things technology includes radio frequency identification technology (RFID), smart card, etc. These technologies allow people to things, thing to thing communication become possible, and provides a platform for Human, material, information space fusion to fusion Because of this Internet of things's security issues become very important. For the Internet of things, traditional block cipher algorithm can not solve the problem very well, because Internet of things uses the computer and hardware processing with limited storage capacity. So, in this case, the emergence of lightweight block cipher has received great attention. Compared to the traditional block cipher, lightweight block cipher has low resource consumption, high efficiency advantages,is very suitable for the safety guarantee of RFID tags, smart card equipment in the environment of Internet of things. MIBS cipher was put forward in meeting CANS2009, LED cipher was proposed by Guo[2] in 2011 CHES meeting, 2011, Chinese scholars wen-ling wu et al[3] proposed LBlock cipher in ANCS meeting is very representative in lightweight block cipher algorithm.

In the environment of Internet of things, lightweight cipher algorithm implementation in hardware, such as RFID, smart card, often brings attackers more convenient conditions.than traditional cipher attack By directly contact with the hardware, the way of circuit analysis, software analysis and a series of side channel attack methods, an attacker can decode algorithm and it brings security threats.to the Internet of things.Especially through failure analysis to decode is very efficient.

The earlist idea of using the fault information to decode the cipher algorithm is proposed by Boneh [4] in 1996, E.Biham and A.S hamir [5] improved it in 1997, put forward the idea that analyzing the difference between right ciphertext and wrong ciphertext to decode the cipher algorithm. Now many lightweight block cipher is seriously in the threat of differential fault attack. Xin-jie zhao et al. [6] analyzed MIBS using differential fault, in the 30th round left register inject half byte unknown fault, 64bit main key space can be reduced to 224. Li Wei and others [7] analyzed LED with differential fault and got through three wrong ciphertext can recover original 64 - bit key; Xu Peng et al. [8] analyzed TWINE with differential fault got in the 35 rounds inject four fault The key space can be reduced to 220 injecting an average of 13.15 times of failure can recover 80 - bit key. But from now differential fault analysis for lightweight block cipher methods is still limited to inject half byte a time, and the efficiency has much space to improve, in addition makeing deep differencial fault analysis for lightweight block cipher is very meaningful

This paper puts forward a deep differencial fault analysis method about feistel structure block cipher. Through the establishment of half byte fault attack with single round;half byte fault attack with rounds;and two half byte fault attack with rounds these three kinds of model to ananlyze the feistel structure block cipher.At the same time, analyzing the feistel structure light-weight block cipher LBlock by deep differencial fault attack. The best results show that in 30th round injecte two half byte fault that the location is known, the size is unknown we can recovery a round key with totally four faults. In 29th round inject half byte fault that location and size is unknown can recovery a round key by approximatly 12.3 faults and 4.1 times injection.

2 Definition and notation

2.1 notation illustration

L_{r-1}: r round left half ciphertext

R_{r-1}: r round right half ciphertext

$\vartriangle L_{r-1}$: r round left differencial input

$\vartriangle R_{r-1}$: r round right differencial input

$\vartriangle L_r$: r round left differencial output

$\vartriangle R_r$: r round right differencial output

$\vartriangle S_r$: r round S box difference

NS_r^i: the i -th half byte in S_r

2.2 definitions

Block cipher with feistel structure has R rounds operation, each round (remove the last round) operation including round keys, nonlinear transform (S box), ambiguity function (M), the replacement function (P). According to the different cipher algorithm, some of the link is not same, but is essentially same. We can define each round (remove the last round) as:

$$P \{ M [S (L_{r-1} \oplus K_r)] \} \qquad (1)$$

S denote $8*n$ bits nonlinear transform: $\{1,\dots,n\} \to \{1,\dots,n\}$; M denote ambiguity function, different M has different diffusance. In traditional feistel structure block cipher, ambiguity function may not exist; P denote the replacement function.

3. The differential fault analysis

3.1 attack thinking

The basic idea of attacking as follows:

1. The attacker choose plaintext to encrypt and get correct cipher; making multiple encryption, get a lot of cipher.

2. Select the last round to inject fault, once inject half byte fault, location is random, size is unknown. Select eligible ciphertext to analyze; Using differential fault analysis method, analyze the last round key information; Then ,inject fault in last but one round, analyze the last but one round key information; Inject fault in antepenultimate round, analyze it's key information; Simultaneous the last three round key, work out the master key.

3. Select the appropriate round to inject fault, once inject half byte fault, location is random, size is unknown. Select eligible ciphertext to analyze; Using differential fault analysis method, analyze the last round key information; In the last but one round to inject fault, analyze it's key information; Inject fault in antepenultimate round, analyze it's key information; Simultaneous last three round keys, work out master key.

4. Select the appropriate round to inject fault .Once inject two half byte fault, position is known, the size is unknown. This is because once if inject fault that position is unkown It will cause high repetitive rate,decrease the efficience of attack. Select eligible ciphertext to analyze; Using differential fault analysis method, analyze the last round key information; In the last but one round to inject fault, analyze it’s key information; Inject fault in antepenultimate round, analyze it’s key information; Simultaneous last three round keys, work out master key.

3.2 analysis principle

Add keys, ambiguity function (M), the replacement function (P) is a linear transformation in feistel structure block cipher, only the S box operation is nonlinear transform. But because of S box has not perfect properties making it under the threat of fault attack. Therefore, the difference analysis is carried out on the box. The r thround S box input difference $\vartriangle L_{r-1}$ is equal to the output $\vartriangle R_r$, S box output difference is :

$$\vartriangle S_r = m^{-1}(p^{-1}(\vartriangle L_r)) \qquad (2)$$

After getting S box input and output difference, we can compute the box parts information injected faults:

$$S_r[NS_r^i] \oplus S_r[NS_r^i \oplus \vartriangle_{in}] = \vartriangle_{out} \qquad (3)$$

$\vartriangle_{in}$ is the inout difference of S box after injecting fault. $\vartriangle_{out}$ is the output difference of S box after injecting fault Every combination $(\vartriangle_{in} \vartriangle_{out})$ can make sure several candidate of NS_r^i, so that inject fault repetely in the same position we can get the single NS_r^i.

4. Attack instances

LBlock adopts Feistel structure, its length is 64 bits, master key length is 80 bits, iterative round number is 32. We adopt ordinary PC, a 32-bit system, 4G RAM, Intel (R) Core (TM) 2.4 GHz i5 processor to be experimental platform. Using Microsoft Visual C + + 6.0 C language programming to realize LBlock algorithm.

Inject random half byte fault before S box in 31 round. 1000 times experiments.See table 1:

Table 1 the fault need in half byte fault attack of LBlock in a round

Sbox index	2times fault （2）	3times fault （3）	4times fault （4）	More than4 （>4）
0	949	33	18	10
1	938	30	20	12
2	944	36	13	7
3	941	41	10	8
4	937	47	10	6
5	946	35	11	8
6	938	46	9	7
7	931	47	15	7

Inject random half byte fault before S box in 29 round. 1000 times experiments shown in table 2:

Table 2: the fault need in half byte fault attack of LBlock in rounds

fault number	Occurance number	proportion（%）
4	908	90.8%
5	78	7.8%
6	11	1.1%
>6	3	0.3%

Inject two half byte fault before S box in 29 round.The position is known ,value is random. 100 times experiments.

Table 3 :the fault need in two half byte fault attack of LBlock in rounds

fault number	Inject times	Occurance number	proportion（%）
4	2	100	100%
6	3	0	0%
>6	>3	0	0%

5. Conclusion

This paper focuses on feistel structure of lightweight block cipher in Internet of things environment and proposed a deep difference fault analysis method, analyzed the LBlock cipher through the experiment. Theoretical analysis and experimental results show that, through establishing half byte fault attack of single round, half byte fault attack of rounds, two half byte fault attack of rounds these three models can deeply analyzing feistel structure block cipher algorithm,evaluate it's safty The next step we will study how to protect feistel structure block cipher algorithm from differential fault attack .

References

[1]Chen HaiMing.Cui Li.Xie KaiBin.Structure and Realization Research about Internet of Things [J].Computer Journal，2013，36（1）：168-188

[2]Guo J ,Peyin T,Poschmann A et al.The LED block cipher // Proceedings of the International Workshop of Cryptographic Hardware and Embedded Systems (CHES2011). Nara, Japan, 2011: 326-341

[3]Wu W L ,Zhang L.lblock:a lightweight block cipher[A].ANCS2011[C].Nerja,Spain,LNCS 6715,2011.327-344

[4]BONEH D，DEM1LLO R，LIPTON R． On the importance ofchecking cryptographic protocols for faults[A]． Eurocrypt 1997[C1． Konstanz, Germany,1997 37—51．

[5]BIHAM E，SHAMIR A． Diferential fault analysis of sceret key cryptosystems[A] CRYFI~ 1997[C]． Santa Barbara,California,USA,1997． 513-525．

[6]Zhao XinJie， Wang Tao， Wang SuZhen. Deep Differencial Fault Analysis of MIBS [J]Communication Journal，2010，31（12）：82-89

[7]Li Wei， Gu DaWu，Zhao Chen.Safty Analysis of Lingt-Weight Block Cipher LED in Internet of Things[J].Computer Journal，2012，35（3）：434-445

[8] Xu Peng． Wei YueChuan.Pan XiaoZhong.Differencial Fault Analysis of Light-Weight Block Cipher TWINE[J]． Application Research of Computer，2O15，32（6）：1796-1800