AEGIS算法的弱状态分析

施泰荣[1],关 杰[1],刘文哲[2]
(1. 信息工程大学,河南郑州 450001;2. 61415部队,内蒙古呼伦贝尔 021009)

摘 要: AEGIS算法是进入CAESAR竞赛(Competition for Authenticated Encryption:Security,Applicability,and Robustness)第三轮评选的认证加密算法.根据内部状态和密钥长度的不同,设计者推荐了三个AEGIS系列算法:AEGIS-128、AEGIS-256和AEGIS-128L.本文分别给出AEGIS-256和AEGIS-128L算法一组新的弱状态,对应出现的概率远优于现有分析结果.在此基础上,针对AEGIS-256算法,本文实现了对算法的伪造攻击,并给出内部状态与各自的明文对应,使得产生的认证标签为全0;针对AEGIS-128L算法,本文得到了算法在弱状态下的信息泄漏规律.最后对AEGIS系列算法弱状态的成因进行分析,给出了具体的设计及使用建议.目前,除设计报告外尚无对AEGIS算法的弱状态的分析,因此该文对CAESAR竞选有重要意义.

关键词: CAESAR竞赛;AEGIS算法;弱状态;伪造攻击
中图分类号: TN918.1 **文献标识码:** A **文章编号:** 0372-2112 (2018)09-2102-06
电子学报URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2018.09.009

Analysis on the Weak States of AEGIS

SHI Tai-rong[1],GUAN Jie[1],LIU Wen-zhe[2]
(1. *Information Engineering University*,*Zhengzhou*,*Henan* 450001,*China*;
2. *No.* 61415 *Troops*,*Hulunbuir*,*Inner Mongolia* 021009,*China*)

Abstract: AEGIS,an authenticated stream cipher,is one of fifteen third-round candidates of CAESAR competition (Competition for Authenticated Encryption:Security,Applicability,and Robustness). Three AEGIS versions:AEGIS-128、AEGIS-256 and AEGIS-128L are recommended in different internal state and key sizes. This paper proposes two types of weak state for AEGIS-256 and AEGIS-128L respectively. The probabilities of these types of weak state are greater than the existing results. And based on those analyses,a forgery attack on AEGIS-256 is introduced. Indeed,we present internal states with the corresponding plaintexts,in which the tags are 0. As for AEGIS-128L,we attain the information leakage of encryption. Finally,we give brief analysis of what is responsible for weak states. To the best of our knowledge,except for design document,there is no cryptanalysis on weak state of AEGIS proposed until now. Therefore,our work is significant for CAESAR competition.

Key words: CAESAR;AEGIS;weak states;forgery attack

1 引言

认证加密算法[1],指能同时实现数据加密和真实性认证功能的算法,弥补了单一加密方案不能保障完整性或单一认证方案不能保障机密性的缺憾,已经广泛应用于SSL/TLS[2]等密码协议中.为了加速认证加密理论的发展,CAESAR竞赛[3]应运而生.CAESAR竞赛由美国标准技术研究所(NIST)专门资助,继AES[4]、eSTREAM[5]之后又一次大规模的密码算法设计竞赛.随着CAESAR竞赛的推动,对于认证加密算法的安全性分析成为密码学界的研究热点[6,7,8].

AEGIS算法[9]是由Wu和Preneel设计的一类基于AES轮函数的认证加密算法,目前已进入CAESAR竞赛第二轮评选.算法的设计采用了分组密码的思想,使用若干个128比特分组作为内部状态,依次对各内部状态分组进行运算.根据内部状态和密钥长度的不同,设计者推荐了3个AEGIS系列算法:AEGIS-128、AEGIS-256、AEGIS-128L.

针对AEGIS系列算法,Minaud对AEGIS-128、AEGIS-256算法进行了线性分析[10],线性偏差为2^{-77}和

收稿日期:2016-08-16;修回日期2018-02-17;责任编辑:梅志强
基金项目:国家自然科学基金(No.61572516,No.61602514)

2^{-89},数据复杂度分别为 2^{140} 和 2^{188},这是目前除设计报告外唯一的分析结果. 事实上,设计者已经在设计报告中对线性攻击进行了评估,文献[10]的分析结果并没有超出设计者的评估结果.

对于任何一个密码算法,找到其潜在的弱状态对算法的安全性分析来说是十分必要的. 设计者在设计报告中给出 AEGIS 算法的两类弱状态:第一类弱状态是各状态值全部相等,若当前明文 $\boldsymbol{m}_i$ 为全 0,下一步内部状态仍然全部相等,这类弱状态共有 2^{128} 种情况,因此对于 AEGIS-128、AEGIS-256、AEGIS-128L,这类弱状态出现的概率分别为 2^{-512}、2^{-640} 和 2^{-896};第二类弱状态是每个内部状态 128 比特分组的各列相等,若当前明文 m_i 也具有这种形式,下一步的内部状态仍然是各列对应相等,因此对于 AEGIS-128、AEGIS-256、AEGIS-128L 算法分别有 $2^{32\times5}=2^{160}$,$2^{32\times6}=2^{192}$ 和 $2^{32\times8}=2^{256}$ 种情况,对应出现的概率分别为 2^{-480}、2^{-608} 和 2^{-768},具体分析见文献[9].

本文分别给出 AEGIS-256 及 AEGIS-128L 算法的一种新的弱状态,并计算相应的出现概率分别为 2^{-384}(设计者为 2^{-512}),2^{-512}(设计者为 2^{-768}),其结果均优于设计者现有弱状态分析结果. 在此基础上,对 AEGIS-256 进行的弱状态下的伪造攻击;给出 AEGIS-128L 算法的一个弱状态实例及在加密过程中的信息泄漏.

2　AEGIS 算法描述

AEGIS 算法分为初始化、关联数据处理、加密、认证码生成和解密与验证共五个阶段. 在本文中,主要考虑 AEGIS-256 及 AEGIS-128L 算法. 下面首先说明本文所使用符号的意义.

2.1　符号说明

$\boldsymbol{S}_i$:第 i 步更新的内部状态;

$\boldsymbol{S}_{i,j}$:第 i 步更新内部状态第 j 块 128 比特分组;

$\oplus$:按位异或运算;

&:按位与运算;

$\|$:级联;

$\lceil x\rceil$:不小于 x 的最小的整数;

$(\,)_4$:十六进制表示;

$\boldsymbol{const}0$:128 比特常数,$(000101020305080d1522375990e97962)_4$;

$\boldsymbol{const}1$:128 比特常数,$(db3d18556dc22ff12011314273b528dd)_4$;

$adlen$:关联数据长度;

$msglen$:明文分组长度;

$AESRound(\boldsymbol{S})$:对长度为 128 比特的 $\boldsymbol{S}$ 进行一轮 AES 运算(除密钥加).

2.2　AEGIS-128 算法

AEGIS-128 算法密钥长度为 128 比特,初始向量长度为 128 比特,认证码长度为 128 比特,内部状态规模为 640 比特. 在 AEGIS 算法的每一步利用 128 比特消息分组 $\boldsymbol{m}_i$,并行 5 个 AES 轮函数运算 $AESRound$(不包括密钥加)来更新状态 $\boldsymbol{S}_i$. 下面给出 AEGIS-128 算法的状态更新函数 $\boldsymbol{S}_{i+1}=StateUpdate128(\boldsymbol{S}_i,\boldsymbol{m}_i)$:

$$\boldsymbol{S}_{i+1,0}=\boldsymbol{S}_{i,0}\oplus AESRound(\boldsymbol{S}_{i,4})\oplus\boldsymbol{m}_i$$
$$\boldsymbol{S}_{i+1,1}=\boldsymbol{S}_{i,1}\oplus AESRound(\boldsymbol{S}_{i,0})$$
$$\boldsymbol{S}_{i+1,2}=\boldsymbol{S}_{i,2}\oplus AESRound(\boldsymbol{S}_{i,1})$$
$$\boldsymbol{S}_{i+1,3}=\boldsymbol{S}_{i,3}\oplus AESRound(\boldsymbol{S}_{i,2})$$
$$\boldsymbol{S}_{i+1,4}=\boldsymbol{S}_{i,4}\oplus AESRound(\boldsymbol{S}_{i,3})$$

算法的内部状态更新过程如图 1 所示.

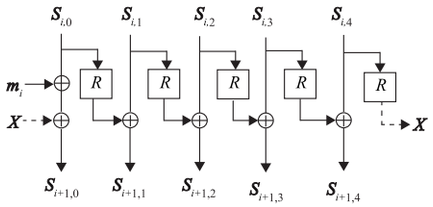

图1　AEGIS-128的内部状态更新函数

图 1 中,$\boldsymbol{X}$ 指一个临时 128 比特分组,用于 $\boldsymbol{S}_{i,0}$ 的更新,R 指 $AESRound(\boldsymbol{S})$.

2.3　AEGIS-256 算法

AEGIS-256 算法密钥长度为 256 比特,初始向量长度为 256 比特,认证码长度为 128 比特,内部状态规模为 768 比特. 在 AEGIS 算法的每一步利用 128 比特消息分组 $\boldsymbol{m}_i$,并行 6 个 AES 轮函数运算(不包括密钥加)来更新状态 $\boldsymbol{S}_i$. 下面给出 AEGIS-256 算法的状态更新函数 $\boldsymbol{S}_{i+1}=StateUpdate256(\boldsymbol{S}_i,\boldsymbol{m}_i)$:

$$\boldsymbol{S}_{i+1,0}=\boldsymbol{S}_{i,0}\oplus AESRound(\boldsymbol{S}_{i,5})\oplus\boldsymbol{m}_i$$
$$\boldsymbol{S}_{i+1,1}=\boldsymbol{S}_{i,1}\oplus AESRound(\boldsymbol{S}_{i,0})$$
$$\boldsymbol{S}_{i+1,2}=\boldsymbol{S}_{i,2}\oplus AESRound(\boldsymbol{S}_{i,1})$$
$$\boldsymbol{S}_{i+1,3}=\boldsymbol{S}_{i,3}\oplus AESRound(\boldsymbol{S}_{i,2})$$
$$\boldsymbol{S}_{i+1,4}=\boldsymbol{S}_{i,4}\oplus AESRound(\boldsymbol{S}_{i,3})$$
$$\boldsymbol{S}_{i+1,5}=\boldsymbol{S}_{i,5}\oplus AESRound(\boldsymbol{S}_{i,4})$$

(1)初始化过程

AEGIS-256 算法的初始化过程包括将密钥和初始向量注入到内部状态中,并将密钥和初始向量作为消息分组对算法进行 16 步状态更新. 密钥和初始向量注入方式如下:

$$\boldsymbol{S}_{-16,0}=\boldsymbol{K}_{256,0}\oplus\boldsymbol{IV}_{256,0};$$
$$\boldsymbol{S}_{-16,1}=\boldsymbol{K}_{256,1}\oplus\boldsymbol{IV}_{256,1};$$
$$\boldsymbol{S}_{-16,2}=\boldsymbol{const}1;$$
$$\boldsymbol{S}_{-16,3}=\boldsymbol{const}0;$$
$$\boldsymbol{S}_{-16,4}=\boldsymbol{K}_{256,0}\oplus\boldsymbol{const}0;$$
$$\boldsymbol{S}_{-16,5}=\boldsymbol{K}_{256,1}\oplus\boldsymbol{const}1;$$

将密钥和初始向量注入后,使用以下消息分组对内部状态进行16步更新:

For $i=-4$ to -1

$\boldsymbol{m}_{4i}=\boldsymbol{K}_{256,0}$;

$\boldsymbol{m}_{4i+1}=\boldsymbol{K}_{256,1}$;

$\boldsymbol{m}_{4i+2}=\boldsymbol{K}_{256,0}\oplus\boldsymbol{IV}_{256,0}$;

$\boldsymbol{m}_{4i+3}=\boldsymbol{K}_{256,1}\oplus\boldsymbol{IV}_{256,1}$;

End for

For $i=-16$ to -1

$\boldsymbol{S}_{i+1}=StateUpdate256(\boldsymbol{S}_i,\boldsymbol{m}_i)$;

End for

(2)关联数据处理过程

For $i=0$ to $\left\lceil\frac{adlen}{128}\right\rceil-1$

$\boldsymbol{S}_{i+1}=StateUpdate256(\boldsymbol{S}_i,\boldsymbol{A}\boldsymbol{D}_i)$;

End for

(3)加密过程

令 $u=\left\lceil\frac{adlen}{128}\right\rceil$,$v=\left\lceil\frac{msglen}{128}\right\rceil$

For $i=0$ to $v-1$:

$\boldsymbol{C}_{u+i}=\boldsymbol{S}_{u+i,1}\oplus\boldsymbol{S}_{u+i,4}\oplus\boldsymbol{S}_{u+i,5}\oplus(\boldsymbol{S}_{u+i,2}\&\boldsymbol{S}_{u+i,3})\oplus\boldsymbol{m}_i$;

$\boldsymbol{S}_{u+i+1}=StateUpdate256(\boldsymbol{S}_{u+i},\boldsymbol{m}_i)$;

End for

(4)认证过程

在加密阶段结束后,算法运行7步状态更新函数来产生认证标签,令 $\boldsymbol{tmp}=\boldsymbol{S}_{u+v,3}\oplus(adlen\parallel msglen)$,其中 $adlen$ 和 $msglen$ 均为64比特二进制表示.

For $i=u+v$ to $u+v+6$

$\boldsymbol{S}_{i+1}=StateUpdate256(\boldsymbol{S}_i,\boldsymbol{tmp})$;

End for

$\boldsymbol{T}=\oplus_{i=0}^{5}\boldsymbol{S}_{u+v+7,i}$

2.4 AEGIS-128L 算法

AEGIS-128L算法密钥长度为128比特,初始向量长度为128比特,认证码长度为128比特,内部状态规模为1024比特. 在每一步运算中,AEGIS-128L算法使用两个128比特的明文分组 $\boldsymbol{m}_{2i}$ 和 $\boldsymbol{m}_{2i+1}$ 来更新状态 $\boldsymbol{S}_i$,经过8轮AES轮函数来更新状态 $\boldsymbol{S}_i$. 状态更新函数 $\boldsymbol{S}_{i+1}=StateUpdate128\mathrm{L}(\boldsymbol{S}_i,\boldsymbol{m}_{2i},\boldsymbol{m}_{2i+1})$:

$$\begin{aligned}
\boldsymbol{S}_{i+1,0}&=\boldsymbol{S}_{i,0}\oplus AESRound(\boldsymbol{S}_{i,7})\oplus\boldsymbol{m}_{2i}\\
\boldsymbol{S}_{i+1,1}&=\boldsymbol{S}_{i,1}\oplus AESRound(\boldsymbol{S}_{i,0})\\
\boldsymbol{S}_{i+1,2}&=\boldsymbol{S}_{i,2}\oplus AESRound(\boldsymbol{S}_{i,1})\\
\boldsymbol{S}_{i+1,3}&=\boldsymbol{S}_{i,3}\oplus AESRound(\boldsymbol{S}_{i,2})\\
\boldsymbol{S}_{i+1,4}&=\boldsymbol{S}_{i,4}\oplus AESRound(\boldsymbol{S}_{i,3})\oplus\boldsymbol{m}_{2i+1}\\
\boldsymbol{S}_{i+1,5}&=\boldsymbol{S}_{i,5}\oplus AESRound(\boldsymbol{S}_{i,4})\\
\boldsymbol{S}_{i+1,6}&=\boldsymbol{S}_{i,6}\oplus AESRound(\boldsymbol{S}_{i,5})\\
\boldsymbol{S}_{i+1,7}&=\boldsymbol{S}_{i,7}\oplus AESRound(\boldsymbol{S}_{i,6})
\end{aligned}$$

(1)初始化过程

AEGIS-128L算法的初始化过程包括将密钥 $\boldsymbol{K}_{128}$ 和初始向量 $\boldsymbol{IV}_{128}$ 注入到内部状态中,并将密钥和 $\boldsymbol{IV}_{128}$ 作为消息分组对算法进行10步状态更新. 密钥和 $\boldsymbol{IV}_{128}$ 注入方式如下:

$$\begin{aligned}
\boldsymbol{S}_{-10,0}&=\boldsymbol{K}_{128}\oplus\boldsymbol{IV}_{128};\\
\boldsymbol{S}_{-10,1}&=\boldsymbol{const}1;\\
\boldsymbol{S}_{-10,2}&=\boldsymbol{const}0;\\
\boldsymbol{S}_{-10,3}&=\boldsymbol{const}1;\\
\boldsymbol{S}_{-10,4}&=\boldsymbol{K}_{128}\oplus\boldsymbol{IV}_{128};\\
\boldsymbol{S}_{-10,5}&=\boldsymbol{K}_{128}\oplus\boldsymbol{const}0;\\
\boldsymbol{S}_{-10,6}&=\boldsymbol{K}_{128}\oplus\boldsymbol{const}1;\\
\boldsymbol{S}_{-10,7}&=\boldsymbol{K}_{128}\oplus\boldsymbol{const}0;
\end{aligned}$$

将密钥 $\boldsymbol{K}_{128}$ 和 $\boldsymbol{IV}_{128}$ 注入后,使用状态更新函数对内部状态进行10步更新:

For $i=0$ to $\left\lceil\frac{adlen}{256}\right\rceil-1$:

$\boldsymbol{S}_{i+1}=StateUpdate128L(\boldsymbol{S}_i,\boldsymbol{IV}_{128},\boldsymbol{K}_{128})$

End for

(2)加密过程

令 $u_L=\left\lceil\frac{adlen}{256}\right\rceil$,$v_L=\left\lceil\frac{msglen}{256}\right\rceil$,加密过程如下:

For $i=u_L$ to v_L-1,

$\boldsymbol{C}_{2i}=\boldsymbol{S}_{i,1}\oplus\boldsymbol{S}_{i,6}\oplus(\boldsymbol{S}_{i,2}\&\boldsymbol{S}_{i,3})\oplus\boldsymbol{m}_{2i}$;

$\boldsymbol{C}_{2i+1}=\boldsymbol{S}_{i,2}\oplus\boldsymbol{S}_{i,5}\oplus(\boldsymbol{S}_{i,6}\&\boldsymbol{S}_{i,7})\oplus\boldsymbol{m}_{2i+1}$;

$\boldsymbol{S}_{i+1}=StateUpdate128L(\boldsymbol{S}_i,\boldsymbol{m}_{2i},\boldsymbol{m}_{2i+1})$;

End for

3 AEGIS-256 算法的弱状态及伪造攻击

本节中,我们将给出AEGIS-256算法的一种新的弱状态,并对这种弱状态的总数及出现概率进行评估. 在此基础上对算法进行伪造攻击,找出了算法的 2^{512} 个内部状态并证明其均存在一组对应的明文,使得产生的认证标签以概率 2^{-128} 为全0,并给出这样的内部状态与明文对应方式,从而实现对算法的伪造攻击.

3.1 AEGIS-256 算法的弱状态

定理1 AEGIS-256算法在加密阶段第 i 步的内部状态为 $\boldsymbol{S}_i=(\boldsymbol{S}_{i,0},\boldsymbol{S}_{i,1},\boldsymbol{S}_{i,2},\boldsymbol{S}_{i,3},\boldsymbol{S}_{i,4},\boldsymbol{S}_{i,5})$,其中 $\boldsymbol{S}_{i,0}=\boldsymbol{S}_{i,3}$,$\boldsymbol{S}_{i,1}=\boldsymbol{S}_{i,4}$,$\boldsymbol{S}_{i,2}=\boldsymbol{S}_{i,5}$,如果 $\boldsymbol{m}_i=0$,则下一步的内部状态仍有这一性质,即 $\boldsymbol{S}_{i+1,0}=\boldsymbol{S}_{i+1,3}$,$\boldsymbol{S}_{i+1,1}=\boldsymbol{S}_{i+1,4}$,$\boldsymbol{S}_{i+1,2}=\boldsymbol{S}_{i+1,5}$,因此 $\boldsymbol{S}_i$ 是AEGIS-256算法的一种弱状态.

证明 将 $\boldsymbol{m}_i=0$ 以及 $\boldsymbol{S}_{i,0}=\boldsymbol{S}_{i,3}$,$\boldsymbol{S}_{i,1}=\boldsymbol{S}_{i,4}$,$\boldsymbol{S}_{i,2}=\boldsymbol{S}_{i,5}$ 代入AEGIS-256算法的状态更新函数 $\boldsymbol{S}_{i+1}=StateUpdate256(\boldsymbol{S}_i,\boldsymbol{m}_i)$.

由 $\boldsymbol{S}_{i+1,0}=\boldsymbol{S}_{i,0}\oplus AESRound(\boldsymbol{S}_{i,5})\oplus\boldsymbol{m}_i$, $\boldsymbol{S}_{i+1,3}=\boldsymbol{S}_{i,3}\oplus AESRound(\boldsymbol{S}_{i,2})$ 得到 $\boldsymbol{S}_{i+1,0}=\boldsymbol{S}_{i+1,3}$;

由 $\boldsymbol{S}_{i+1,1}=\boldsymbol{S}_{i,1}\oplus AESRound(\boldsymbol{S}_{i,0})$, $\boldsymbol{S}_{i+1,4}=\boldsymbol{S}_{i,4}\oplus AESRound(\boldsymbol{S}_{i,3})$ 得到 $\boldsymbol{S}_{i+1,1}=\boldsymbol{S}_{i+1,4}$;

由 $\boldsymbol{S}_{i+1,2}=\boldsymbol{S}_{i,2}\oplus AESRound(\boldsymbol{S}_{i,1})$, $\boldsymbol{S}_{i+1,5}=\boldsymbol{S}_{i,5}\oplus AESRound(\boldsymbol{S}_{i,4})$ 得到 $\boldsymbol{S}_{i+1,2}=\boldsymbol{S}_{i+1,5}$;

故新的内部状态 $\boldsymbol{S}_{i+1}=(\boldsymbol{S}_{i+1,0},\boldsymbol{S}_{i+1,1},\boldsymbol{S}_{i+1,2},\boldsymbol{S}_{i+1,3},\boldsymbol{S}_{i+1,4},\boldsymbol{S}_{i+1,5})$ 仍具有内部状态值对称相等的性质 $\boldsymbol{S}_{i+1,0}=\boldsymbol{S}_{i+1,3}$, $\boldsymbol{S}_{i+1,1}=\boldsymbol{S}_{i+1,4}$, $\boldsymbol{S}_{i+1,2}=\boldsymbol{S}_{i+1,5}$, 因此 $\boldsymbol{S}_i$ 是 AEGIS-256 算法的一种弱状态.

证毕

由于 $\boldsymbol{S}_{i,0}=\boldsymbol{S}_{i,3}$, $\boldsymbol{S}_{i,1}=\boldsymbol{S}_{i,4}$, $\boldsymbol{S}_{i,2}=\boldsymbol{S}_{i,5}$, 且每一个 128 比特分组有 2^{128} 种选择,故这类弱状态共有 $2^{128\times3}=2^{384}$ 种取值,算法内部状态规模为 768 比特,所以出现概率为 2^{-384}.

3.2　AEGIS-256 算法的伪造攻击

针对 AEGIS-256 算法的加密过程,给出一种基于弱状态的伪造攻击. 具体地说,就是从任意时刻开始,改变明文输入,使得下一步的状态成为弱状态,在弱状态条件下,生成的认证标签以概率 2^{-128} 为全 0,因此我们可以以成功率 2^{-128} 实现伪造攻击. 在进行伪造攻击时,我们需要用到以下定理.

定理 2　对于 AEGIS-256 算法,若在加密过程结束后其内部状态(即认证过程的初态) $\boldsymbol{S}_{u+v}$ 是弱状态且 $\boldsymbol{tmp}=0$,那么生成的认证标签以概率 1 为全 0.

证明　由于 $\boldsymbol{S}_{u+v}$ 是弱状态,故 $\boldsymbol{S}_{u+v}=(\boldsymbol{S}_{u+v,0},\boldsymbol{S}_{u+v,1},\boldsymbol{S}_{u+v,2},\boldsymbol{S}_{u+v,3},\boldsymbol{S}_{u+v,4},\boldsymbol{S}_{u+v,5})$, 满足 $\boldsymbol{S}_{u+v,0}=\boldsymbol{S}_{u+v,3}$, $\boldsymbol{S}_{u+v,1}=\boldsymbol{S}_{u+v,4}$, $\boldsymbol{S}_{u+v,2}=\boldsymbol{S}_{u+v,5}$

由认证过程的状态更新函数 $\boldsymbol{S}_{i+1}=StateUpdate256(\boldsymbol{S}_i,\boldsymbol{tmp})$ 以及 $\boldsymbol{tmp}=0$ 可知 $\boldsymbol{S}_{u+v+1}=(\boldsymbol{S}_{u+v+1,0},\boldsymbol{S}_{u+v+1,1},\boldsymbol{S}_{u+v+1,2},\boldsymbol{S}_{u+v+1,3},\boldsymbol{S}_{u+v+1,4},\boldsymbol{S}_{u+v+1,5})$ 依然是弱状态,即 $\boldsymbol{S}_{u+v+1,0}=\boldsymbol{S}_{u+v+1,3}$, $\boldsymbol{S}_{u+v+1,1}=\boldsymbol{S}_{u+v+1,4}$, $\boldsymbol{S}_{u+v+1,2}=\boldsymbol{S}_{u+v+1,5}$, 经过七步更新之后,再由内部状态 $\boldsymbol{S}_{u+v+7}$ 生成认证标签: $T=\oplus_{i=0}^{5}\boldsymbol{S}_{u+v+7,i}$. 由于 $\boldsymbol{S}_{u+v+7,0}=\boldsymbol{S}_{u+v+7,3}$, $\boldsymbol{S}_{u+v+7,1}=\boldsymbol{S}_{u+v+7,4}$, $\boldsymbol{S}_{u+v+7,2}=\boldsymbol{S}_{u+v+7,5}$, 故 $T=0$ 以概率 1 成立.

证毕

伪造攻击　假设在第 i 时刻,AEGIS-256 算法的内部状态值为 $\boldsymbol{S}_i=(\boldsymbol{S}_{i,0},\boldsymbol{S}_{i,1},\boldsymbol{S}_{i,2},\boldsymbol{S}_{i,3},\boldsymbol{S}_{i,4},\boldsymbol{S}_{i,5})$, 明文为 $\boldsymbol{m}_i$, 此时可以修改明文使得下一步的内部状态成为弱状态,具体的明文形式推导如下:

令 $\boldsymbol{S}_i=(\boldsymbol{S}_{i,0},\boldsymbol{S}_{i,1},\boldsymbol{S}_{i,2},\boldsymbol{S}_{i,3},\boldsymbol{S}_{i,4},\boldsymbol{S}_{i,5})=(\boldsymbol{A},\boldsymbol{B},\boldsymbol{C},\boldsymbol{D},\boldsymbol{E},\boldsymbol{F})$, 若下一步的内部状态成为弱状态,根据弱状态的形式及状态更新函数,则下列方程组一定成立

$$\begin{cases}\boldsymbol{A}\oplus AESRound(\boldsymbol{F})\oplus\boldsymbol{m}_i=\boldsymbol{D}\oplus AESRound(\boldsymbol{C})\\ \boldsymbol{B}\oplus AESRound(\boldsymbol{A})=\boldsymbol{E}\oplus AESRound(\boldsymbol{D})\\ \boldsymbol{C}\oplus AESRound(\boldsymbol{B})=\boldsymbol{F}\oplus AESRound(\boldsymbol{E})\end{cases}\tag{1}$$

通过解方程可以得到 $\boldsymbol{E},\boldsymbol{F}$ 的形式如下:

$$\boldsymbol{E}=\boldsymbol{B}\oplus AESRound(\boldsymbol{A})\oplus AESRound(\boldsymbol{D});$$

$$\boldsymbol{F}=\boldsymbol{C}\oplus AESRound(\boldsymbol{B})\oplus AESRound(\boldsymbol{E});$$

故若下一步达到弱状态,当前时刻的内部状态的形式为

$$(\boldsymbol{A},\boldsymbol{B},\boldsymbol{C},\boldsymbol{D},\boldsymbol{B}\oplus AESRound(\boldsymbol{A})\oplus AESRound(\boldsymbol{D}),\ \boldsymbol{C}\oplus AESRound(\boldsymbol{B})\oplus AESRound(\boldsymbol{E})).$$

此时将明文 $\boldsymbol{m}_i$ 修改为 $\boldsymbol{m}'_i=\boldsymbol{A}\oplus AESRound(\boldsymbol{F})\oplus\boldsymbol{D}\oplus AESRound(\boldsymbol{C})$, 其中 $\boldsymbol{F}=\boldsymbol{C}\oplus AESRound(\boldsymbol{B})\oplus AESRound(\boldsymbol{E})$, 则

$$\begin{cases}\boldsymbol{E}=\boldsymbol{B}\oplus AESRound(\boldsymbol{A})\oplus AESRound(\boldsymbol{D})\\ \boldsymbol{F}=\boldsymbol{C}\oplus AESRound(\boldsymbol{B})\oplus AESRound(\boldsymbol{E})\\ \boldsymbol{m}'_i=\boldsymbol{A}\oplus AESRound(\boldsymbol{F})\oplus\boldsymbol{D}\oplus AESRound(\boldsymbol{C})\end{cases}\tag{2}$$

式(2)是方程组(1)的解,容易知道 $\boldsymbol{A},\boldsymbol{B},\boldsymbol{C},\boldsymbol{D}$ 是四组规模为 128 比特的自由变量,因此具有这种形式的内部状态共有 $2^{128\times4}=2^{512}$ 种可能取值. 由 $\boldsymbol{tmp}=\boldsymbol{S}_3^{u+v+7}\oplus(adlen\parallel msglen)$, $\boldsymbol{S}_3^{u+v+7}=(adlen\parallel msglen)$ 的概率为 2^{-128}, 故 $\boldsymbol{tmp}=\boldsymbol{0}$ 的概率为 2^{-128}. 因此我们可以得到以下结论:

结论　对于 AEGIS-128-L 算法的最后一步加密,其加密前内部状态为 $\boldsymbol{S}_{u+v-1}$, 则 $\boldsymbol{S}_{u+v-1}$ 存在 2^{512} 个形式为 $(\boldsymbol{A},\boldsymbol{B},\boldsymbol{C},\boldsymbol{D},\boldsymbol{B}\oplus AESRound(\boldsymbol{A})\oplus AESRound(\boldsymbol{D}),\boldsymbol{C}\oplus AESRound(\boldsymbol{B})\oplus AESRound(\boldsymbol{E}))$ 的取值情况,当修改明文 $\boldsymbol{m}_i$ 为 $\boldsymbol{m}'_i=\boldsymbol{A}\oplus AESRound(F)\oplus\boldsymbol{D}\oplus AESRound(\boldsymbol{C})$, 使得经过一步加密后 $\boldsymbol{S}_{u+v}$ 会成为弱状态,此时生成的认证标签以概率 2^{-128} 为全 0,从而实现伪造攻击.

4　AEGIS-128L 算法的弱状态及信息泄漏

本节中,我们给出 AEGIS-128L 算法的一种新的弱状态,并对这种弱状态的总数及出现概率进行评估. 在此基础上,找到算法初始化过程弱状态的一个实例,并对加密过程中弱状态下的信息泄漏规律进行分析.

4.1　AEGIS-128L 算法的弱状态

定理 3　AEGIS-128L 算法在加密阶段第 i 步的内部状态为 $\boldsymbol{S}_i=(\boldsymbol{S}_{i,0},\boldsymbol{S}_{i,1},\boldsymbol{S}_{i,2},\boldsymbol{S}_{i,3},\boldsymbol{S}_{i,4},\boldsymbol{S}_{i,5},\boldsymbol{S}_{i,6},\boldsymbol{S}_{i,7})$, 其中 $\boldsymbol{S}_{i,0}=\boldsymbol{S}_{i,4}$, $\boldsymbol{S}_{i,1}=\boldsymbol{S}_{i,5}$, $\boldsymbol{S}_{i,2}=\boldsymbol{S}_{i,6}$, $\boldsymbol{S}_{i,3}=\boldsymbol{S}_{i,7}$, 如果 $\boldsymbol{m}_{2i}=\boldsymbol{m}_{2i+1}$, 则下一步的内部状态仍有这一性质,即 $\boldsymbol{S}_{i+1,0}=\boldsymbol{S}_{i+1,4}$, $\boldsymbol{S}_{i+1,1}=\boldsymbol{S}_{i+1,5}$, $\boldsymbol{S}_{i+1,2}=\boldsymbol{S}_{i+1,6}$, $\boldsymbol{S}_{i+1,3}=\boldsymbol{S}_{i+1,7}$, 因此 $\boldsymbol{S}_i$ 是 AEGIS-128L 算法的一种弱状态.

证明　将 $\boldsymbol{S}_{i,0}=\boldsymbol{S}_{i,4}$, $\boldsymbol{S}_{i,1}=\boldsymbol{S}_{i,5}$, $\boldsymbol{S}_{i,2}=\boldsymbol{S}_{i,6}$, $\boldsymbol{S}_{i,3}=\boldsymbol{S}_{i,7}$ 以及 $\boldsymbol{m}_{2i}=\boldsymbol{m}_{2i+1}$ 代入 AEGIS-128L 算法的状态更新函数.

由 $\boldsymbol{S}_{i+1,0}=\boldsymbol{S}_{i,0}\oplus AESRound(\boldsymbol{S}_{i,7})\oplus\boldsymbol{m}_{2i}$, $\boldsymbol{S}_{i+1,4}=\boldsymbol{S}_{i,4}\oplus AESRound(\boldsymbol{S}_{i,3})\oplus\boldsymbol{m}_{2i+1}$ 得到 $\boldsymbol{S}_{i+1,0}=\boldsymbol{S}_{i+1,4}$;

由 $\boldsymbol{S}_{i+1,1}=\boldsymbol{S}_{i,1}\oplus AESRound(\boldsymbol{S}_{i,0})$, $\boldsymbol{S}_{i+1,5}=\boldsymbol{S}_{i,5}\oplus AESRound(\boldsymbol{S}_{i,4})$ 得到 $\boldsymbol{S}_{i+1,1}=\boldsymbol{S}_{i+1,5}$;

由 $\boldsymbol{S}_{i+1,2}=\boldsymbol{S}_{i,2}\oplus AESRound(\boldsymbol{S}_{i,1})$, $\boldsymbol{S}_{i+1,6}=\boldsymbol{S}_{i,6}\oplus$

$AESRound(\boldsymbol{S}_{i,5})$得到$\boldsymbol{S}_{i+1,2}=\boldsymbol{S}_{i+1,6}$;

由$\boldsymbol{S}_{i+1,3}=\boldsymbol{S}_{i,3}\oplus AESRound(\boldsymbol{S}_{i,2})$,$\boldsymbol{S}_{i+1,7}=\boldsymbol{S}_{i,7}\oplus AESRound(\boldsymbol{S}_{i,6})$得到$\boldsymbol{S}_{i+1,3}=\boldsymbol{S}_{i+1,7}$.

故$\boldsymbol{S}_{i+1,0}=\boldsymbol{S}_{i+1,4}$,$\boldsymbol{S}_{i+1,1}=\boldsymbol{S}_{i+1,5}$,$\boldsymbol{S}_{i+1,2}=\boldsymbol{S}_{i+1,6}$,$\boldsymbol{S}_{i+1,3}=\boldsymbol{S}_{i+1,7}$,因此$\boldsymbol{S}_i$是 AEGIS-128L 算法的一种弱状态.

证毕

由于$\boldsymbol{S}_{i+1,0}=\boldsymbol{S}_{i+1,4}$,$\boldsymbol{S}_{i+1,1}=\boldsymbol{S}_{i+1,5}$,$\boldsymbol{S}_{i+1,2}=\boldsymbol{S}_{i+1,6}$,$\boldsymbol{S}_{i+1,3}=\boldsymbol{S}_{i+1,7}$,且每一个 128 比特分组有$2^{128}$种选择,故这类弱状态共有$2^{128\times4}=2^{512}$种取值,算法内部状态规模为 1024 比特,所以出现概率为2^{-512}.

4.2 AEGIS-128L 弱状态实例

由 4.1 节中 AEGIS-128L 算法的弱状态描述可知当$\boldsymbol{S}_{i,0}=\boldsymbol{S}_{i,4}$,$\boldsymbol{S}_{i,1}=\boldsymbol{S}_{i,5}$,$\boldsymbol{S}_{i,2}=\boldsymbol{S}_{i,6}$,$\boldsymbol{S}_{i,3}=\boldsymbol{S}_{i,7}$时,$\boldsymbol{S}_i=(\boldsymbol{S}_{i,0},\boldsymbol{S}_{i,1},\boldsymbol{S}_{i,2},\boldsymbol{S}_{i,3},\boldsymbol{S}_{i,4},\boldsymbol{S}_{i,5},\boldsymbol{S}_{i,6},\boldsymbol{S}_{i,7})$是算法的一个弱状态.结合 AEGIS-128L 算法的初始化过程,找到了算法应用中的一个弱状态实例.

结合密钥$\boldsymbol{K}_{128}$、$\boldsymbol{IV}_{128}$的加载过程及上述弱状态的形式,进行以下分析:

由$\boldsymbol{S}_{-10,0}$和$\boldsymbol{S}_{-10,4}$的表达式:$\boldsymbol{S}_{-10,0}=\boldsymbol{K}_{128}\oplus\boldsymbol{IV}_{128}$,$\boldsymbol{S}_{-10,4}=\boldsymbol{K}_{128}\oplus\boldsymbol{IV}_{128}$,可知$\boldsymbol{S}_{i,0}=\boldsymbol{S}_{i,4}$是自然成立的.

由$\boldsymbol{S}_{-10,1}$和$\boldsymbol{S}_{-10,5}$的表达式:$\boldsymbol{S}_{-10,1}=\boldsymbol{const}1$,$\boldsymbol{S}_{-10,5}=\boldsymbol{K}_{128}\oplus\boldsymbol{const}0$,根据$\boldsymbol{S}_{i,1}=\boldsymbol{S}_{i,5}$可知$\boldsymbol{K}_{128}=\boldsymbol{const}0\oplus\boldsymbol{const}1$.

由$\boldsymbol{S}_{-10,2}$和$\boldsymbol{S}_{-10,6}$的表达式:$\boldsymbol{S}_{-10,2}=\boldsymbol{const}0$,$\boldsymbol{S}_{-10,6}=\boldsymbol{K}_{128}\oplus\boldsymbol{const}1$,根据$\boldsymbol{S}_{i,2}=\boldsymbol{S}_{i,6}$可知$\boldsymbol{K}_{128}=\boldsymbol{const}0\oplus\boldsymbol{const}1$.

由$\boldsymbol{S}_{-10,3}$和$\boldsymbol{S}_{-10,7}$的表达式:$\boldsymbol{S}_{-10,3}=\boldsymbol{const}1$,$\boldsymbol{S}_{-10,7}=\boldsymbol{K}_{128}\oplus\boldsymbol{const}0$,根据$\boldsymbol{S}_{i,3}=\boldsymbol{S}_{i,7}$可知$\boldsymbol{K}_{128}=\boldsymbol{const}0\oplus\boldsymbol{const}1$.

从整个分析过程可知,密钥$\boldsymbol{K}_{128}$并没有矛盾的取值,因此$\boldsymbol{K}_{128}=\boldsymbol{const}0\oplus\boldsymbol{const}1$是造成弱状态的一个密钥;接下来,根据算法初始化阶段密钥$\boldsymbol{K}_{128}$,$\boldsymbol{IV}_{128}$加载过后的 10 步更新

$$\boldsymbol{S}_{i+1}=StateUpdate128L(\boldsymbol{S}_i,\boldsymbol{IV}_{128},\boldsymbol{K}_{128}).$$

如果取$\boldsymbol{IV}_{128}=\boldsymbol{K}_{128}$,根据弱状态的传递性质,在初始化结束之后,内部状态仍是弱状态. 即

$$\boldsymbol{S}_{i,0}=\boldsymbol{S}_{i,4},\boldsymbol{S}_{i,1}=\boldsymbol{S}_{i,5},\boldsymbol{S}_{i,2}=\boldsymbol{S}_{i,6},\boldsymbol{S}_{i,3}=\boldsymbol{S}_{i,7}.$$

由 4.1 节分析可知,对于这种弱状态,其产生概率是2^{-384},然而当算法使用这种$(\boldsymbol{K}_{128},\boldsymbol{IV}_{128})$时,弱状态的产生概率成为 1.

4.3 AEGIS-128L 算法弱状态下的信息泄漏

假设在 AEGIS-128L 算法在第i步加密时,内部状态为$\boldsymbol{S}_i$为弱状态,当前时刻进行加密的两组明文为$(\boldsymbol{m}_{2i},\boldsymbol{m}_{2i+1})$,两者的差为$\Delta\boldsymbol{m}_{2i}=\boldsymbol{m}_{2i}\oplus\boldsymbol{m}_{2i+1}$,密文为$(\boldsymbol{C}_{2i},\boldsymbol{C}_{2i+1})$,密文的差为$\Delta\boldsymbol{C}_{2i}=\boldsymbol{C}_{2i}\oplus\boldsymbol{C}_{2i+1}$,根据加密过程:

$$\boldsymbol{C}_{2i}=\boldsymbol{S}_{i,1}\oplus\boldsymbol{S}_{i,6}\oplus(\boldsymbol{S}_{i,2}\&\boldsymbol{S}_{i,3})\oplus\boldsymbol{m}_{2i} \quad (3)$$

$$\boldsymbol{C}_{2i+1}=\boldsymbol{S}_{i,2}\oplus\boldsymbol{S}_{i,5}\oplus(\boldsymbol{S}_{i,6}\&\boldsymbol{S}_{i,7})\oplus\boldsymbol{m}_{2i+1} \quad (4)$$

由于$\boldsymbol{S}_i$为弱状态,$\boldsymbol{S}_{i,0}=\boldsymbol{S}_{i,4}$,$\boldsymbol{S}_{i,1}=\boldsymbol{S}_{i,5}$,$\boldsymbol{S}_{i,2}=\boldsymbol{S}_{i,6}$,$\boldsymbol{S}_{i,3}=\boldsymbol{S}_{i,7}$,将(3)、(4)两式等号左右两边相加再移位,故得到$\Delta\boldsymbol{m}_{2i}=\Delta\boldsymbol{C}_{2i}$.

此时进行一步状态更新$\boldsymbol{S}_{i+1}=StateUpdate128L(\boldsymbol{S}_i,\boldsymbol{m}_{2i},\boldsymbol{m}_{2i+1})$,由$\boldsymbol{S}_{i+1,1}=\boldsymbol{S}_{i,1}\oplus AESRound(\boldsymbol{S}_{i,0})$,$\boldsymbol{S}_{i+1,5}=\boldsymbol{S}_{i,5}\oplus AESRound(\boldsymbol{S}_{i,4})$得到$\boldsymbol{S}_{i+1,1}=\boldsymbol{S}_{i+1,5}$;由$\boldsymbol{S}_{i+1,2}=\boldsymbol{S}_{i,2}\oplus AESRound(\boldsymbol{S}_{i,1})$,$\boldsymbol{S}_{i+1,6}=\boldsymbol{S}_{i,6}\oplus AESRound(\boldsymbol{S}_{i,5})$得到$\boldsymbol{S}_{i+1,2}=\boldsymbol{S}_{i+1,6}$;由$\boldsymbol{S}_{i+1,3}=\boldsymbol{S}_{i,3}\oplus AESRound(\boldsymbol{S}_{i,2})$,$\boldsymbol{S}_{i+1,7}=\boldsymbol{S}_{i,7}\oplus AES\ Round(\boldsymbol{S}_{i,6})$得到$\boldsymbol{S}_{i+1,3}=\boldsymbol{S}_{i+1,7}$. 此时对下一组明文进行加密.

$$\boldsymbol{C}_{2i+2}=\boldsymbol{S}_{i,1}\oplus\boldsymbol{S}_{i,6}\oplus(\boldsymbol{S}_{i,2}\&\boldsymbol{S}_{i,3})\oplus\boldsymbol{m}_{2i+2};$$

$$\boldsymbol{C}_{2i+3}=\boldsymbol{S}_{i+1,2}\oplus\boldsymbol{S}_{i+1,5}\oplus(\boldsymbol{S}_{i+1,6}\&\boldsymbol{S}_{i+1,7})\oplus\boldsymbol{m}_{2i+3};$$

同理可以得到$\Delta\boldsymbol{m}_{2i+2}=\Delta\boldsymbol{C}_{2i+2}$.

记$\boldsymbol{m}_{2i}=(\boldsymbol{m}_{2i,1},\boldsymbol{m}_{2i,2},\cdots,\boldsymbol{m}_{2i,128})$,$\boldsymbol{m}_{2i+1}=(\boldsymbol{m}_{2i+1,1},\boldsymbol{m}_{2i+1,2},\cdots,\boldsymbol{m}_{2i+1,128})$各自有 128 比特,若我们知道$\boldsymbol{m}_{2i,j}$,由$\Delta\boldsymbol{m}_{2i+2}=\Delta\boldsymbol{C}_{2i+2}$,得到$\boldsymbol{m}_{2i+1,j}\oplus\boldsymbol{m}_{2i,j}=C_{2i+1,j}\oplus C_{2i,j}$,从而求出$\boldsymbol{m}_{2i+1,j}=\boldsymbol{m}_{2i,j}\oplus C_{2i+1,j}\oplus C_{2i,j}$. 因此如果知道 256 比特密文$(\boldsymbol{m}_{2i},\boldsymbol{m}_{2i+1})$中 128 比特任意位于不同比特位(即若任意两比特取自不同分组$\boldsymbol{m}_{2i,j}$,$\boldsymbol{m}_{2i+1,k}$,须满足$j\neq k$)的明文对应,就能恢复其余 128 比特明文.

5 AEGIS 算法弱状态原因分析及设计建议

观察上述两类弱状态,本文分析出弱状态的成因如下:

(1)AEGIS-256 和 AEGIS-128L 算法的内部状态具有一定的对称性.

对于 AEGIS-256 算法的内部状态$\boldsymbol{S}_i=(\boldsymbol{S}_{i,0},\boldsymbol{S}_{i,1},\boldsymbol{S}_{i,2},\boldsymbol{S}_{i,3},\boldsymbol{S}_{i,4},\boldsymbol{S}_{i,5})$,前三个 128 比特分组和对应后三个 128 比特分组分别取值相同时,则成为弱状态.

对于 AEGIS-128L 算法的内部状态$\boldsymbol{S}_i=(\boldsymbol{S}_{i,0},\boldsymbol{S}_{i,1},\boldsymbol{S}_{i,2},\boldsymbol{S}_{i,3},\boldsymbol{S}_{i,4},\boldsymbol{S}_{i,5},\boldsymbol{S}_{i,6},\boldsymbol{S}_{i,7})$,前四个 128 比特分组和后四个 128 比特分组取值相同时,则成为弱状态.

(2)AEGIS 系列算法的状态更新函数对于每个 128 比特分组具有相似性.

除了明文参与的更新,其他状态分组均以$\boldsymbol{S}_{i+1,j+1}=\boldsymbol{S}_{i,j+1}\oplus AESRound(\boldsymbol{S}_{i,j})$的更新方式进行运算.

AEGIS-256 和 AEGIS-128L 算法具备了以上两个条件,因此形成此类弱状态,对比 AEGIS-128 算法,虽然具备了比特分组更新的相似性,但其内部状态采用奇数个 128 比特分组,因此不存在此类弱状态.

在设计算法时,应适当考虑以上两个因素,据此我们提出以下三种方法来避免弱状态带来的危害:

(1)认证码检测技术:当对一组明文$\boldsymbol{m}$进行加密并认证得到$(\boldsymbol{C},\boldsymbol{T})$,对认证码进行检测,若$\boldsymbol{T}=\boldsymbol{0}$,则可以抛弃$(\boldsymbol{C},\boldsymbol{T})$,重新选取初始向量$\boldsymbol{IV}$进行加密认证;

(2)状态检测技术:在算法运行过程中,对内部状态进行检测,若符合弱状态的性质,则重新选择$\boldsymbol{IV}$,进

行认证加密.

(3)修改算法,打破算法更新的相似性. 可以在算法每步更新后增加变换(例如任意两个分组进行比特乘或模 2 加),使得弱状态不能传递下去.

其中修改算法是可以从根本上避免算法产生弱状态,然而这种方式可能会影响算法原本的安全性及效率. 认证码检测技术适用于 AEGIS-128L,状态检测技术适用于 AEGIS-256 和 AEGIS-128L,除外之外,对于 AEGIS-128L 算法,要避免使用造成弱状态的密钥.

6　结束语

本文对 AEGIS 算法的安全性进行了分析,针对算法的弱状态,主要做出了以下几方面工作:

(1)针对 AEGIS-256 算法提出了一种新的弱状态,对应出现的概率分别为 2^{-384};给出伪造攻击,证明了该算法存在 2^{512} 个内部状态,每个内部状态都存在一组明文,并给出这样的内部状态与明文对应方式,使得产生的认证标签以概率 1 为全 0,从而我们可以实现对 AEGIS-256 算法的伪造攻击;

(2)针对 AEGIS-128L 算法提出了一种新的弱状态,对应出现的概率分别为 2^{-512};分析得到算法在弱状态下的信息泄漏,并给出造成弱状态的一个密钥实例 $\boldsymbol{K}_{128}$;

(3)根据本文的弱状态分析结果,提出了一些算法的使用及设计建议.

本文的分析内容并没有威胁到算法的安全性,但是首次改进了设计报告中的分析结果,对算法设计及使用有一定的参考价值,为 AEGIS 算法的安全性评估提供了基础. 接下来,我们将对弱状态做更深入的研究,并对 AEGIS 算法抵抗其他攻击的能力进行分析.

参考文献

[1] Bellare M, Namprempre C. Authenticated encryption: relations among notions and analysis of the generic composition paradigm[J]. Journal of Cryptology, 2008, 21(4): 469-491.

[2] Hickman K, Elgamal T. The SSL protocol[DB/OL]. http://www. webstart. com/jed/papers/HRM/references/ssl. html, 2016.

[3] Bernstein D J. CAESAR call for submissions[EB/OL]. http://competitions:cr:yp:to/caesar-call:html. 2014.

[4] Daemen J, Rijmen V. The Design of Rijndael[M]. Berlin: Springer-Verlag, 2002. 31-51.

[5] Preneel B. eSTREAM: ECRYPT Stream Cipher Project [EB/OL]. http://www. ecrypt. eu. org/stream, 2006.

[6] Abed F, Forler C, Lucks S. General Overview of the Authenticated Schemes for the First Round of the CAESAR Competition [EB/OL]. https://eprint. iacr. org /2014/792. pdf, 2014.

[7] Fuhr T, Leurent G, Suder V. Collision attacks against CAESAR candidates [A]. ASIACRYPT 2015 [C]. Berlin: Springer-Verlag, 2015. 510-532.

[8] Schroé W, Mennink B, Andreeva E, et al. Forgery and subkey recovery on CAESAR candidate iFeed[A]. SAC 2015 [C]. Sackville, NB, Cauada: Springer International Publishing, 2015. 197-204.

[9] Wu H, Preneel B. AEGIS: A Fast Authenticated Encryption Algorithm (v1) [EB/OL]. https://competitions. cr. yp. to/round1/aegisv1. pdf, 2015

[10] Minaud B. Linear biases in AEGIS keystream[A]. SAC 2014[C]. Montreal, QC, Canada: Springer International Publishing, 2014. 290-305.

作者简介

施泰荣　女,1992 年生于山东临沂. 信息工程大学硕士研究生. 研究方向为对称密码设计与分析.

E-mail: strwanzi@163. com

关　杰　女,1974 年生于河南郑州,信息工程大学教授、博士生导师,研究方向为密码学与信息安全.

E-mail: guanjie007@163. com

刘文哲　男,1992 年生于内蒙古赤峰,研究方向为密码学.