基于SM4轮函数设计的认证加密算法

张 建[1,2],吴文玲[1,2]
(1. 中国科学院软件研究所可信计算与信息保障实验室,北京 100190;
2. 中国科学院大学,北京 100190)

摘 要: 认证加密算法,作为一种对称密码算法,能够同时保护数据的机密性和完整性,在信息安全领域有着重要作用. 现有的认证加密算法大多是基于分组密码的工作模式设计的,底层需要调用全轮的分组密码,效率受到很大限制. 本文主要考虑从基本部件出发直接设计一个高效的认证加密算法. 首先结合国产分组密码标准SM4与广义Feistel结构给出了一种通用的结构设计. 然后以抵抗碰撞攻击为安全性目标,利用混合整数规划(MILP)方法搜索得到了一些状态大小和效率各不相同的结构,这些结构可以被用来构造消息认证码和认证加密算法. 最后,利用目前搜索得到的状态大小和效率较优的结构设计了一个认证加密算法,并进行了初步的安全性分析和软件实现,其速度约为SM4-GCM速度的10倍.

关键词: 认证加密算法; 算法设计; 广义Feistel结构; 混合整数规划(MILP); SM4算法; SM4-GCM
中图分类号: TP391 **文献标识码:** A **文章编号:** 0372-2112 (2018)06-1294-06
电子学报URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2018.06.003

Authenticated Encryption Based on SM4 Round Function

ZHANG Jian[1,2], WU Wen-ling[1,2]
(1. *Institute of Software, Chinese Academy of Sciences, TCA Lab, Beijing* 100190, *China*;
2. *University of Chinese Academy of Sciences, Beijing* 100190, *China*)

Abstract: Authenticated encryption, as a symmetric cryptographic primitive, can protect privacy and integrity simultaneously, which plays an important role in information security. Most of the existing authenticated encryption algorithms are designed based on the working mode of block cipher, which needs to call full round of block cipher. Thus the efficiency is quite limited. This paper considers to construct an efficient authenticated encryption algorithm dedicatedly using basic components. We first present a general structure by combining Chinese block cipher standard SM4 and the general Feistel structure. With the mixed integer linear programming (MILP) method, we find several secure structures against the collision attacks with different sate size and efficiency, which can be used as building blocks for MACs and authenticated encryption. Then we design an authenticated encryption using the structure with good state size and efficiency, and give the corresponding security analysis and implemention. Our benchmarks show that it runs about 10 times faster than SM4-GCM.

Key words: authenticated encryption; design; general Feistel structure; MILP; SM4 cipher; SM4-GCM

1 引言

认证加密(authenticated encryption)算法能够同时满足信息的机密性和完整性两个基本的密码学需求,兼具了加密算法和消息认证码的功能,受到了密码学界的广泛关注. 特别是受到2014年发起的CAESAR竞赛的驱动,认证加密算法的设计与分析成为了密码学的一大研究热点. 认证加密算法的设计主要可以分为两类,一类是从分组密码工作模式出发,设计安全的认证加密模式,比如OCB[1],GCM[2],CCM[3]等. 基于分组密码工作模式的认证加密算法一般都是可证明安全的,但是由于底层需要随机函数的假设,往往采用全轮的分组密码,因此效率受到了很大的限制. 另外一类主要从密码部件出发,设计安全高效的认证加密算法,比如AEGIS[4],Tiaoxin[5],ALE[6]等. 从底层部件出发设计算法具有很高的灵活性,可以使算法达到很高的效率,

收稿日期:2017-01-17;修回日期:2017-6-19;责任编辑:覃怀银
基金项目:国家自然科学基金(No. 61672509);国家密码学发展基金会(No. MMJJ20170101)

受到了设计者的青睐. 其中,借助已有的分组密码,特别是密码算法标准来进行设计,是一种常见的设计思路. 密码算法标准经过了长期大量的研究,安全性具有一定的可靠性,算法的实现也进行了各种优化,这些都会给新算法的评估和优化实现带来方便. 例如,自从高级加密标准 AES 确定以后,出现了大量的基于 AES 的设计,比如 MAC 算法 Pelican-MAC、Alpha-MAC,流密码算法 LEX、ASC-1,认证加密算法 ALE 等. 特别是近两年,由于 AES 指令的高效性,出现了很多基于 AES 轮函数设计的算法[4~8].

本文主要考虑基于 SM4[9] 轮函数设计认证加密算法. 分组密码算法 SM4 是中国第一个分组密码标准,整体采用非平衡的广义 Feistel 结构,通过迭代 32 轮完成加密过程. 那么目前使用 SM4 来实现信息的机密性和完整性保护,只能将 SM4 与认证加密模式结合起来使用,可以采用先加密后认证(encrypt-then-MAC)[10] 的方法,或者将 SM4 与已有的成熟的认证加密模式特别是国际标准结合起来,比如 SM4-GCM. 这两种方法底层都需要使用 32 轮的 SM4,效率受到了很大的限制. 本文将首先给出一个基于 SM4 轮函数的通用结构;然后针对不同的参数,利用混合线性整数规划方法搜索出一些安全的结构;最后,利用找到的结构给出了一个具体的认证加密算法 SMAE,并进行了简单的安全性分析和效率评估.

2　预备知识

本文用 $<<<i$ 表示 32bit 左循环移 i 位;Z_2^{32} 表示 32bit 的整数构成的集合;S^i 表示第 i 轮状态,且 $S^i=(S_0^i,\cdots,S_{15}^i)$,$S_j^i\in Z_2^{32}$;adlen 表示辅助数据的长度;msglen 表示消息的长度;$|A|_{64}$ 为整数 A 对应的 64 位表示.

2.1　SM4 轮函数

SM4 分组长度为 128bit,由 4 个 32bit 的字构成,整体采用了非平衡的广义 Feistel 结构. 轮函数如图 1 所示,首先 3 个字与轮密钥进行异或,然后经过函数 T,再与剩下的一个字异或得到新的状态.

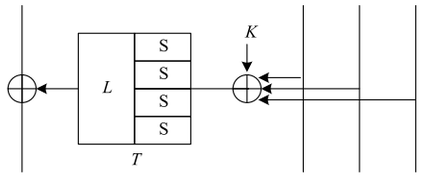

图1　SM4的轮函数结构图

T 函数由并置的 4 个完全相同的 8bit 的 S 盒和一个 32bit 的线性变换 L 构成. 对于输入 $X\in Z_2^{32}$,线性变换 $L:Z_2^{32}\to Z_2^{32}$ 为:

$$L(X)=X\oplus(X<<<2)\oplus(X<<<10)\oplus(X<<<18)\oplus(X<<<24)$$

容易通过计算机验证得到 L 的线性分支数为 5.

2.2　MILP 方法

混合线性整数规划(MILP)是一种常见的最优化模型,主要是求目标函数在一些线性约束条件下的最大或者最小值. 自从 Mouha 等人[11] 形式化地将 MILP 方法应用到密码学,MILP 方法已经成为了密码安全性分析的一种常用方法,在认证加密、分组密码、hash 函数等各类密码算法的安全性分析中得到了大量应用[12~14].

MILP 方法在密码分析中应用最多的就是用来确定差分(线性)活跃 S 盒个数的下界,从而得到差分特征概率(线性偏差)的上界,评估算法抵抗差分(线性)分析的安全性. 一般将差分按 S 盒大小进行截断,用 z_i 表示 S 盒的输入截断差分,如果 S 盒活跃,即输入差分不为 0,则 $z_i=1$,否则 $z_i=0$,那么目标函数为:

$$\mathrm{Min}\sum_i z_i$$

然后再根据截断差分在密码算法中的传播关系,建立线性约束.

对于异或运算 $y=x_1\oplus x_2$,$x_1,x_2\in\{0,1\}$ 为截断差分变量,可以通过四个不等式来刻画:

$$\begin{cases} y+x_1+x_2-2t\geqslant 0\\ v-t\leqslant 0, v\in\{x_1,x_2,y\}\end{cases}$$

其中 t 为引入的临时二元变量,$t=0$ 时,$y=x_1=x_2=0$,$t=1$ 时,$y+x_1+x_2\geqslant 2$,与异或运算的结果相对应. 需要特别注意的是,由于利用的是截断差分,丢失了大量的信息,当 $x_1=x_2=1$ 时,y 的值并不唯一确定,该性质使得 MILP 方法得到的活跃 S 盒个数的下界并不紧.

对于线性变换 L,如果输入为 (x_1,x_2,x_3,x_4),输出为 (y_1,y_2,y_3,y_4),那么由于线性分支数为 5,可以得到 9 个线性不等式,

$$\begin{cases} x_1+x_2+x_3+x_4+y_1+y_2+y_3+y_4\geqslant 5t\\ v\leqslant t, v\in\{x_1,x_2,x_3,x_4,y_1,y_2,y_3,y_4\}\end{cases}$$

其中 $x_i,y_i,i\in\{1,2,3,4\}$ 为截断差分变量,t 为临时变量. 如果 $t=0$,则所有变量取值为 0;否则,受到线性变换 L 分支数为 5 的约束.

有了目标函数和线性约束,就可以直接利用已有的优化模型求解工具进行求解,比如 CPLEX、Gurobi 等. 但是需要注意的是,如果我们要求所有的变量都是二元变量,那么整个问题变成了 0-1 规划问题,求解速度会大大降低,所以正如 Borghoff[15] 等人建议,只要求输入截断差分变量和所有临时变量为二元变量,可以极大地提高求解速度.

3　基于 SM4 轮函数结构的设计

3.1　通用结构 R_s^t

利用 SM4 的轮函数结合广义 Feistel 结构,定义了一

种迭代型的结构 R_s^t,其中 t 表示每轮使用 SM4 轮函数的个数(状态大小),s 表示每轮打入 32bit 消息的块数(如没有特别说明,假设从左到右依次打入消息块),每一轮的结构如图 2 所示,其中 $M_i \in Z_2^{32}$,P 是一个向量置换.

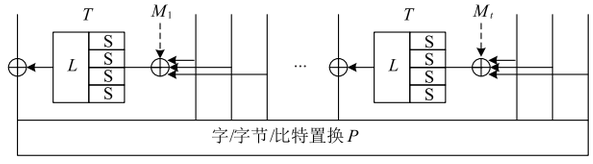

图2 R_s^t 一轮的结构图,虚线表示具有可选择性

对于结构 R_s^t,状态大小相同的情况下,每轮处理的消息块越多,那么结构的效率越高. 定义一个衡量效率的指标 rate.

定义 1 结构 R_s^t 的效率可以通过处理 32bit 的消息块需要的 SM4 轮函数的个数来衡量,即 rate = t/s.

那么 rate 越小,对应结构的效率越高. 容易知道 SM4 与认证加密模式结合使用,rate 至少为 8,比如 SM4-GCM. 我们的目标是以 SM4 的轮函数作为基本部件设计一个结构(算法),与 SM4-GCM 相比具有更高的效率.

3.2 安全性目标

R_s^t 作为一个通用结构,可以通过添加初始化等过程构造完整的 MAC 算法、hash 算法和认证加密算法. 假设密钥长度为 128bit,那么对基于 R_s^t 的算法进行攻击时,只有当复杂度小于 128bit 时,攻击才是有效的.

由于 R_s^t 仅仅是一个通用结构,而不是一个具体的算法,因此想要全面的分析其抵抗各种攻击的安全性是不可能的. 本文主要考虑 R_s^t 抵抗内部碰撞攻击的安全性. 内部碰撞攻击是一种分析 MAC 算法、hash 算法和认证加密算法的一种最为常见的分析方法,很容易转化成伪造攻击,比如对 ALE 的攻击[17],主要利用两次不同消息的处理过程中,通过消息的打入引入初始差分,然后在后面的消息引入差分使得内部状态发生碰撞,即内部状态差分为 0. 我们将这种通过消息引入初始差分,再通过消息差分使得内部状态差分为 0 的攻击方法称为内部碰撞攻击.

由于 SM4 的 S 盒最大差分概率为 2^{-6},考虑到 128bit 的安全性假设,那么碰撞攻击的差分传播过程中活跃 S 盒的个数不能小于 22 个. 我们将活跃 S 盒个数不少于 22 作为搜索安全的结构 R_s^t 时,确定参数 s,t 和 P 的依据.

3.3 实验结果

我们的目标是通过搜索得到一些高效的安全的结构. 首先假设 P 为基于字(32bit)的向量置换,一方面能够大大减少搜索量,另外一方面也能简化安全性的分析过程. 然后给定 s,t,利用 MILP 方法搜索 P,使得内部碰撞发生时,活跃 S 盒个数的下界至少为 22.

首先,有如下定理:

定理 1 对于 R_s^t,当 rate = 1,即 $s = t$ 时,存在只有 1 个活跃 S 盒的差分路径使得状态差分为 0,即发生内部碰撞.

定理 1 很容易证明,假设在 M_1 引入差分 δ_1,经过一个轮函数传播为 δ_2,那么因为 P 是基于字的向量置换,所以一定能在 δ_2 进入 S 盒前,通过消息差分的引入使得内部差分为 0. 定理 1 说明 rate 至少为 2 时结构 R_s^t 才有可能安全.

对于 R_1^2,我们穷搜了所有 8! 种置换,并没有找到安全的结构,又因为定理 1,R_2^2 和 R_1^1 一定是不安全的. 所以有,

定理 2 参数 t 至少为 3 时,结构 R_s^t 才有可能安全,即抵抗内部碰撞攻击.

当 $t \geqslant 3$ 时,要穷尽搜索所有的置换 P,搜索量太大. 因此我们每次随机生成一个 P,再检验结构是否安全. 通过这样的方式,搜索得到一些使得结构安全的置换 P.

对于 R_1^3,我们找到了很多可用的 P,图 3 给出了一个简单的例子,此时 P 是一个循环移位,类似于 SM4 算法的向量置换,整个结构 rate = 3,在第 1 轮引入差分,经过 15 轮之后差分消掉,总共需要至少 25 个活跃 S 盒.

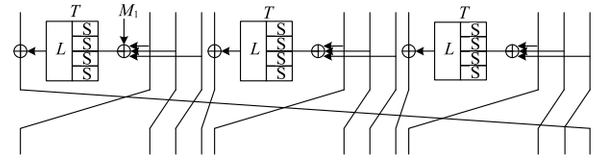

图3 R_1^3 中 P 为循环移位时结构图

然后,我们考虑搜索 rate 更小的结构. 我们对 R_2^3 进行了部分搜索,这时候 rate = 1.5,然而令我们失望的是并没有找到可用的 P,因此我们推测 R_2^3 是不安全的.

我们对 R_2^4 进行了搜索,得到了大量可用的 P,表 1 中列出了一部分 P 以及对应的活跃 S 盒个数的下界. 我们将用 P_5 在第 4 节中构造具体的认证加密算法.

我们对 R_4^6,R_3^5 等一些 rate 更小的结构进行了部分搜索,都没有找到安全的结构.

表 1 部分使得 R_2^4 安全的置换 P

No.	置换 P	活跃 S 盒个数
P_0	11,5,7,9,14,8,12,1,15,0,3,2,10,6,13,4	22
P_1	10,2,7,5,11,12,8,13,3,4,1,14,15,6,0,9	23
P_2	14,10,1,12,9,4,11,6,3,7,15,0,2,5,13,8	24
P_3	8,4,3,13,7,15,5,10,14,12,9,6,11,1,2,0	22
P_4	9,7,4,10,11,12,5,14,13,6,15,0,3,2,8,1	23
P_5	5,11,12,7,8,10,15,6,13,4,1,2,14,3,9,0	23

这一节中我们给出了两类结构 R_1^3 和 R_2^4. R_1^3 具有更小的状态,R_2^4 具有更高的效率,可以根据应用环境的不同选择一个设计认证加密算法. 需要特别注意的是,我们只是使用了一些最基本的约束条件进行搜索,再结合 MILP 方法本身的特点,我们得到的 S 盒个数的下界可能是非常不紧的. 对于特殊的 P,通过添加一些额外的约束条件,或许能够找到 rate 更小的结构. 另外,我们限制了 P 是基于字的置换,如果 P 是基于字节甚至是比特的置换,也可能得到 rate 更小的结构.

4　认证加密算法 SMAE

本节中我们利用结构 R_2^4 设计一个安全的认证加密算法 SMAE,并进行初步的安全性分析和效率评估.

4.1　算法描述

SMAE 的输入包含:长度为 128bit 的密钥 $K\in\{0,1\}^{128}$,初始向量(也称为 nonce)$N\in\{0,1\}^{128}$,辅助数据 A 和消息 M;输出密文 C 和 128bit 的标签 $T\in\{0,1\}^{128}$. 首先将辅助数据和消息进行填充(用 1 连接上多个 0),使得其长度为 64bit 的整数倍,对于已经是 64bit 整数倍的消息,也需要进行填充. 填充过后的辅助数据和消息分别记为 $A=(A_0,\cdots,A_{2d-1})$,$M=(M_0,\cdots,M_{2t-1})$,其中 $A_i,M_j\in\{0,1\}^{32}$. 算法一轮结构如图 4 所示,每轮处理两个消息块,我们将一轮的更新函数记为 Round(M_1,M_2). 第 i 轮状态由 16 个 32bit 的字构成,记为 $S^i=(S_0^i,\cdots,S_{15}^i)\in(Z_2^{32})^{16}$,向量置换采用表 1 中的 P_5.

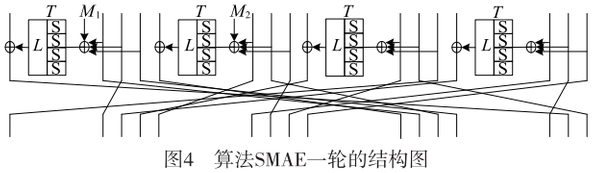

图4　算法SMAE一轮的结构图

4.1.1　初始化

初始化过程主要完成密钥 K 和初始化向量 N 的混合,整个过程分为两步:

(1)初始状态装载密钥 K 和 N:

$(S_0^0,S_1^0,S_2^0,S_3^0)=K$;$(S_4^0,S_5^0,S_6^0,S_7^0)=N$;

$(S_8^0,S_9^0,S_{10}^0,S_{11}^0)=\mathrm{cst}_1$;$(S_{12}^0,S_{13}^0,S_{14}^0,S_{15}^0)=\mathrm{cst}_2$;

其中,cst_1,cst_2 为常数. 分别有 $\mathrm{cst}_1=0\times31415926$,$\mathrm{cst}_2=0\times53589793$.

(2)状态进行 32 轮迭代更新:

For $i=0$ to 31,Round(0,0);

4.1.2　辅助数据的处理

填充过后的辅助数据逐块进行处理:

For $i=0$ to $d-1$,Round(A_{2i},A_{2i+1});

4.1.3　消息的处理

填充过后的消息逐块进行处理,先用状态与明文生成密文,再更新状态:

For $i=0$ to $t-1$,

$C_{2i}=M_{2i}\oplus S_0^i\oplus S_4^i\oplus(S_3^i\wedge S_{10}^i)\oplus(S_5^i\wedge S_{14}^i)$;

$C_{2i+1}=M_{2i+1}\oplus S_8^i\oplus S_{12}^i\oplus(S_7^i\wedge S_9^i)\oplus(S_1^i\wedge S_{13}^i)$;

Round(M_{2i},M_{2i+1});

4.1.4　标签的生成

标签生成过程可以分为三步:

(1)利用辅助数据和消息的长度信息 adlen 和 msglen 更新两轮. 即:

$(M_1',M_2')=|\mathrm{adlen}|_{64}$;$(M_3',M_4')=|\mathrm{msglen}|_{64}$;

Round(M_1',M_2');Round(M_3',M_4');

(2)迭代更新 32 轮:

For $i=0$ to 31,Round(0,0);

(3)利用状态生成标签:

$$T=(S_0^i\oplus S_4^i\oplus S_8^i\oplus S_{12}^i)\,\|\,(S_1^i\oplus S_5^i\oplus S_9^i\oplus S_{13}^i)\,\|\,(S_2^i\oplus S_6^i\oplus S_{10}^i\oplus S_{14}^i)\,\|\,(S_3^i\oplus S_7^i\oplus S_{11}^i\oplus S_{15}^i)$$

算法返回 $C=(C_0,\cdots,C_{2t-1})$ 和标签 T. 解密验证的过程与加密的过程类似,这里不再描述.

4.2　安全性分析

首先,为了保证认证加密算法 SMAE 的安全性,我们做如下要求:

(1)初始向量值(nonce)不能重复使用,即每次加密必须更换初始向量值.

(2)解密验证过程中,不输出明文信息. 验证成功,输出明文;否则输出 $\perp$.

(3)同一个密钥下能够加密的辅助数据和消息的数量小于 2^{64}bit.

如果满足上述要求,SMAE 算法针对密钥恢复攻击和伪造攻击的安全性可以达到 128bit. 与基于工作模式的认证加密算法不同,我们不能对安全性进行证明,但是可以从分析的角度评估算法的安全性.

由于 SMAE 的向量置换使用的是表 1 中的 P_5,根据第 3 节中的分析,通过消息引入差分,构造内部碰撞,至少需要经过 23 个活跃 S 盒,那么 SMAE 一定抵抗内部碰撞攻击.

另外,考虑初始化阶段的差分传播的安全性. 我们同样利用 MILP 的方法搜索差分活跃 S 盒的个数,为了使得活跃 S 盒个数的下界更紧,可以利用类似文献[12]中的方法,添加更多的约束.

定理 3　如果初始状态存在差分,连续 4 轮 SMAE 至少有一个活跃 S 盒.

定理 3 可以利用反证法进行证明,假设连续 4 轮 SMAE 中所有 S 盒都不活跃,那么可以得到 16 个关于初始状态差分变量 $\Delta S_0^0,\cdots,\Delta S_{15}^0$ 的齐次线性方程,可以通过计算机验证知道系数矩阵是可逆的,那么方程组

有唯一 0 解,即初始状态差分为 0,矛盾. 因此,只要初始状态有差分,那么连续 4 轮 SMAE 至少存在一个活跃 S 盒.

定理 3 也是设计 SMAE 算法时选取置换的一个重要依据,因为并不是表 1 中的所有置换都能得到类似定理 3 的结论. 结合定理 3,利用 MILP 方法进行搜索,可以知道 25 轮的初始化结构至少有 22 个活跃 S 盒. 那么,32 轮的初始化过程和 32 轮的生成标签的过程,都足够抵抗差分攻击.

猜测确定攻击[18]主要通过猜测一些变量,利用轮函数的传播得到一些新的变量,从而恢复出所有状态变量. 我们分析了 SMAE 算法针对猜测确定攻击的安全性. 由于 SMAE 中线性变换 L 的分支数为 5,那么 L 的输入输出字节中,至少已知 4 个字节(32bit)才能得到新的字节的值. 又因为向量置换和异或运算都是基于 32bit 的字的运算. 所以,整个猜测确定过程可以看做是以 32bit 的字为变量进行猜测,那么要想通过猜测至多 3 个变量(否则超过 128bit 的密钥穷搜的复杂度)恢复所有状态是不可能的,因此 SMAE 抵抗猜测确定攻击.

线性攻击[19]主要利用密文之间高概率的线性关系,与随机函数进行区分. 我们分析了 SMAE 算法针对线性攻击的安全性. 首先,利用各轮状态之间存在的相等关系,比如 $S_{10}^0 = S_1^1$,再对轮函数和生成密文的"与"运算进行线性化,可以得到下面的线性逼近等式:

$$\lambda \cdot C_1 \oplus \lambda \cdot C_2 \oplus \lambda \cdot C_3 \oplus \lambda \cdot C_4 \oplus \lambda \cdot C_5 \oplus \lambda \cdot C_6 = 0,$$

其中 $\lambda \in Z_2^{32}$ 为线性掩码,$C_1, \cdots, C_6$ 为连续三轮的密文. 通过计算机搜索得到当线性掩码 $\lambda = 0 \times 10104$ 时,等式成立的最优偏差为 $2^{-92.43}$. 根据线性分析[19]的原理,进行区分攻击和明文恢复攻击需要的数据复杂度大约为 2^{184},因此 SMAE 算法针对线性攻击是安全的.

4.3 实现效率

我们在个人计算机上对 SMAE 进行了实现,采用的处理器是 intel core i3-2120. 表 3 给出了实验结果与其它一些结果的对比,其中软件速度以 Gb/s 来衡量.

表 2 不同算法的软件速度

算法	SMAE	SM4-GCM	AES-CTR
速度(Gb/s)	3.8	0.28	2.52[20]

需要注意的是我们对 SMAE 和 SM4-GCM 的实现,采用的是最基本的查表方式,可以通过并行实现或者使用 CPU 指令来进行加速. 通过表 3 可以看到,SMAE 的速度大约为 SM4-GCM 速度的 10 倍,与利用 AES 指令实现的 AES-CTR 的速度相当.

5 总结

本文首先研究了基于 SM4 轮函数设计认证加密算法的通用结构,然后利用 MILP 方法搜索给出了两种抵抗碰撞攻击的结构 R_2^4 和 R_1^3. 进一步,利用结构 R_2^4 设计了一个高效的认证加密算法 SMAE. 与 SM4-GCM 相比,SMAE 算法具有明显的性能优势,速度大约为 SM4-GCM 的 10 倍. SMAE 算法是一个直接设计的认证加密算法,没有可证明安全性,我们初步评估了其针对几种分析方法的安全性,欢迎有兴趣的同行继续深入分析评估其安全性.

参考文献

[1] Rogaway P, Bellare M, et al. OCB: a block-cipher mode of operation for efficient authenticated encryption[J]. ACM Transactions on Information and System Security (TISSEC), 2003. 6(3): 365 – 403.

[2] McGrew D, Viega J. The Galois/Counter Mode of Operation (GCM)[EB/OL]. http://nvlpubs. nist. gov/nistpubs/Legacy/SP/nistspecialpublication800 – 38d. pdf, 2004.

[3] Whiting D, Housley R, Ferguson N. Counter with CBC-MAC (CCM)[EB/OL]. http://csrc. nist. gov/encryption/modes/proposedmodes, 2003.

[4] Wub H, Preneel B. AEGIS: a fast authenticated encryption algorithm[A]. Lange T. Selected Areas in Cryptography—SAC[C]. Berlin: Springer, 2014. 185 – 201.

[5] Nikolic I. Tiaoxin—346 [EB/OL]. CAESAR Third Round Submission. http://competitions. cr. yp. to/round3/tiaoxinv21. pdf, 2016.

[6] Bogdanov A, Mendel F, et al. ALE: AES-based lightweight authenticated encryption[A]. Moriai S. Fast Software Encryption[C]. Berlin: Springer, 2013. 447 – 466.

[7] Jean J, Nikolić I. Efficient design strategies based on the AES round function[A]. Peyrin T. Fast Software Encryption[C]. Berlin: Springer, 2016. 334 – 353.

[8] Ye D, Wang P, et al. PAES v1: Parallelizable Authenticated Encryption Schemes Based on AES Round Function[EB/OL]. CAESAR First Round Submission. http://competitions. crypto/round1/paesv1. pdf, 2014.

[9] Diffie W, Ledin G, et al. SMS4 Encryption Algorithm For Wireless Networks[EB/OL]. IACR Cryptology Eprint Archive. http://eprint. iacr. org/2008/329, 2008.

[10] Bellare M, Namprempre C. Authenticated encryption: relations among notions and analysis of the generic composition paradigm[A]. Okamoto T. Advances in Cryptology—ASIACRYPT[C]. Berlin: Springer, 2000. 531 – 545.

[11] Mouha N, Wang Q, et al. Differential and linear cryptanalysis using mixed-integer linear programming[A]. Wu CK. International Conference on Information Security and Cryptology[C]. Berlin: Springer, 2011. 57 – 76.

[12] Zhang J, Wu W, et al. Security of SM4 against (related-

key) differential cryptanalysis[A]. Bao F. Information Security Practice and Experience[C]. Cham: Springer, 2016. 65 – 78.
[13] Sun S, Hu L, et al. Automatic security evaluation and (related-key) differential characteristic search: application to Simon, Present, LBlock, DES(L) and other bit-oriented block ciphers[A]. Sarkar P. Advances in Cryptology-AsiaCrypt[C]. Berlin: Springer, 2014. 158 – 178.
[14] Sun S, Hu L, et al. Automatic security evaluation of block ciphers with s-bp structures against related-key differential attacks[A]. Lin D. Information Security and Cryptology[C]. Cham: Springer, 2014. 39 – 51.
[15] Borghoff J, Knudsen L R, et al. Bivium as a mixed-integer linear programming problem[A]. Parker M G. Ima International Conference on Cryptography and Coding[C]. Berlin: Springer, 2009. 133 – 152.
[16] Wu S, Wu H, et al. Leaked-state-forgery attack against the authenticated encryption algorithm ale[A]. Sako K. Advances in Cryptology-AsiaCrypt[C]. Berlin: Springer, 2013. 377 – 404.
[17] Dinur I, Jean J. Cryptanalysis of FIDES[A]. Cid C. Fast Software Encryption[C]. Berlin: Springer, 2014. 224 – 240.
[18] Minaud B. Linear biases in AEGIS keystream[A]. Joux A. Selected Areas in Cryptography[C]. Berlin: Springer, 2014. 290 – 305.
[19] Matsui M. Linear cryptanalysis method for DES cipher[A]. Helleseth T. Advances in Cryptology—EuroCrypt[C]. Berlin: Springer, 1994. 386 – 397.
[20] Krovetz T, Rogaway P. The software performance of authenticated encryption modes[A]. Joux A. Fast Software Encryption[C]. Berlin: Springer, 2011. 306 – 327.

作者简介

张　建　男,1988 年生于四川成都. 现为中国科学院软件研究所博士研究生. 主要研究方向为分组密码和认证加密算法.
E-mail: zhangjian@tca.iscas.ac.cn

吴文玲　女,1966 年生于陕西蒲城. 现为中国科学院软件研究所研究员、博士生导师. 主要研究方向为对称密码学.
E-mail: wwl@tca.iscas.ac.cn