ISSN 1000-9825, CODEN RUXUEW
Journal of Software, Vol.17, No.2, February 2006, pp.333−338
DOI: 10.1360/jos170333

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel/Fax: +86-10-62562563

TAE 模式的分析和改进*

王 鹏[1+], 冯登国[1,2]

[1](信息安全国家重点实验室(中国科学院 研究生院),北京 100049)

[2](信息安全国家重点实验室(中国科学院 软件研究所),北京 100080)

Cryptanalysis of the TAE Mode and Its Improvement

WANG Peng[1+], FENG Deng-Guo[1,2]

[1](State Key Laboratory of Information Security (Graduate School, The Chinese Academy of Sciences), Beijing 100049, China)

[2](State Key Laboratory of Information Security (Institution of Software, The Chinese Academy of Sciences), Beijing 100080, China)

+ Corresponding author: Phn: +86-10-88258713, Fax: +86-10-88258713, E-mail: zrockingz@yahoo.com.cn

Wang P, Feng DG. Cryptanalysis of the TAE mode and its improvement. *Journal of Software*, 2006,17(2): 333−338. http://www.jos.org.cn/1000-9825/17/333.htm

Abstract: The TAE (tweakable authenticated encryption) mode is an authenticated encryption mode which is based on a tweakable block cipher. Previous research results show that the secure tweakable block cipher is not sufficient for the security of the authenticated encryption TAE mode. Only when the tweakable block cipher is strong will the TAE be secure. Some improvements to the TAE mode are also given in this paper, resulting in a MTAE (modified tweakable authenticated encryption) mode with security proof.

Key words: authenticated encryption; block cipher; TAE (tweakable authenticated encryption) mode; tweakable block cipher

摘 要: TAE(tweakable authenticated encryption)模式是一种基于可调分组密码的加密认证模式.研究结果表明,安全的可调分组密码不是安全的 TAE 模式的充分条件.只有当可调分组密码是强安全的时候,TAE 模式才是安全的.同时,还给出了 TAE 模式的一些改进,得到模式 MTAE(modified tweakable authenticated encryption),并且证明了其安全性.

关键词: 加密认证;分组密码;TAE 模式;可调分组密码

中图法分类号: TP309 文献标识码: A

由于 NIST 对 AES 工作模式的征集和一些具体应用环境的要求,对分组密码工作模式的讨论是近几年的一个研究热点.分组密码的工作模式可以分为:加密模式,如常见的 CBC 模式、CTR 模式,、OFB 模式、CFB 模式;认证模式,如 CBC-MAC;加密认证模式,如 OCB 模式[1]、EAX 模式[2]、CWC 模式[3].与这些基于分组密码的工作模式不同,TAE(tweakable authenticated encryption)模式是一种基于可调分组密码(tweakable block cipher)的

* Supported by the National Natural Science Foundation of China under Grant No.60273027 (国家自然科学基金); the National Grand Fundamental Research 973 Program of China under Grant No.G1999035802 (国家重点基础研究发展规划(973)); the National Outstanding Young Scientists Foundation of China under Grant No.60025205 (国家杰出青年科学基金)

Received 2004-10-19; Accepted 2005-07-11

加密认证模式.可调分组密码的严格定义,最早是由 Liskov 等人在文献[4]中给出的.与分组密码相比,可调分组密码多了一个称为调柄(tweak)的输入.调柄的作用与密钥不同:密钥是秘密的,确保的是密码的机密性;调柄是公开的,增加的是密码的灵活性.每一个调柄对应于一个分组密码.对于(强)安全的可调分组密码,不同调柄对应的分组密码相当于相互独立的随机置换.调柄在文献[5]中被称为随机化子(randomiser)和多样化参数(diversification parameter).(强)安全的分组密码和可调分组密码的存在性是等价的[4].可调分组密码可以由分组密码构造得到.因为可调分组密码的灵活性,在文献[4]中,Liskov 等人建议基于分组密码的模式设计分成两个部分:首先在分组密码的基础上设计可调分组密码,然后在可调分组密码的基础上进行工作模式的设计.作为这一思想的一个例子,文献[4]给出了 TAE 模式.TAE 模式是一种加密认证模式,与 OCB 模式[1]类似.Liskov 等人认为,如果所用的可调分组密码是安全的,那么 TAE 模式也是安全的,即同时提供了机密性和完整性,并且还给出了证明.我们的研究表明,这一结论是错误的,证明是有漏洞的.我们构造一个简单的例子说明了这个问题.这个例子表明,安全的可调分组密码不能保证 TAE 模式提供的完整性.只有当可调分组密码是强安全的时候,TAE 模式才是安全的.

本文第 1 节给出可调分组密码和加密认证模式的定义.第 2 节描述 TAE 模式的细节.第 3 节给出反例和分析.第 4 节是对 TAE 模式的改进和安全性证明.最后是结论.

1 基本概念

1.1 可调分组密码

分组密码 $E:\{0,1\}^k\times\{0,1\}^n\to\{0,1\}^n$ 是一个函数,并且对任意的 $K\in\{0,1\}^k$,$E(K,\cdot)=E_K(\cdot)$是$\{0,1\}^n$ 上的置换.可调分组密码 $\tilde{E}:\{0,1\}^k\times\{0,1\}^t\times\{0,1\}^n\to\{0,1\}^n$ 是一个函数,并且对任意的 $K\in\{0,1\}^k$ 和 $T\in\{0,1\}^t$,$\tilde{E}(K,T)=\tilde{E}(T,\cdot)=\tilde{E}_K^T(\cdot)$ 是$\{0,1\}^n$ 上的置换.分别称$\{0,1\}^k$,$\{0,1\}^t$ 和$\{0,1\}^n$ 为密钥空间、调柄空间和明文空间(密文空间).由定义可知,对任意固定的调柄 T, $\tilde{E}_K^T(\cdot)$ 是一个分组密码,可调分组密码可以看作是以调柄为索引的分组密码的集合.$perm(n)$表示$\{0,1\}^n$ 上的所有置换的集合,$perm(t,n)$表示所有$\{0,1\}^t$到 $perm(n)$上的映射的集合.$a\leftarrow S$ 表示从集合 S 随机选取元素 a,如果集合只有一个元素则表示赋值.如果$\Pi\leftarrow perm(n)$,则称Π是$\{0,1\}^n$上的随机置换;如果 $\tilde{\Pi}\leftarrow perm(t,n)$,则称 $\tilde{\Pi}$ 为$\{0,1\}^n$ 上的调柄空间为$\{0,1\}^t$的可调随机置换.由定义可知,对于任意固定的 $T\in\{0,1\}^t$,$\tilde{\Pi}(T,\cdot)$ 是一个随机置换.

我们将分组密码的安全性定义为敌手(adversary)区分分组密码和随机置换的优势;将可调分组密码的安全性定义为敌手区分可调分组密码和可调随机置换的优势.敌手攻击的方式分为选择明文攻击和选择密文攻击,对于可调分组密码,敌手还可以选择调柄.下面给出精确的定义.

敌手是一种可询问若干个预言机(oracle)的概率算法,敌手在攻击的过程中,可以任意询问预言机,最后输出比特 0 或者 1.不失一般性,假设敌手不询问已知的信息.例如敌手不重复已询问过的明文加密.我们用 $A\Rightarrow 1$ 表示敌手 A 输出比特 1,将 A 所询问的预言机写在其右上角.A 在对可调分组密码进行攻击时,不但可以选择明(密)文,而且可以选择调柄.分组密码和可调分组密码的安全性是由下列优势函数定义的:

$$\mathrm{Adv}_E^{prp}(A)=\Pr[A^{E_K(\cdot)}\Rightarrow 1]-\Pr[A^{\Pi(\cdot)}\Rightarrow 1];\quad \mathrm{Adv}_E^{sprp}(A)=\Pr[A^{E_K(\cdot)E_K^{-1}(\cdot)}\Rightarrow 1]-\Pr[A^{\Pi(\cdot)\Pi^{-1}(\cdot)}\Rightarrow 1];$$

$$\mathrm{Adv}_{\tilde{E}}^{tprp}(A)=\Pr[A^{\tilde{E}_K(\cdot,\cdot)}\Rightarrow 1]-\Pr[A^{\tilde{\Pi}(\cdot,\cdot)}\Rightarrow 1];\quad \mathrm{Adv}_{\tilde{E}}^{stprp}(A)=\Pr[A^{\tilde{E}_K(\cdot,\cdot)\tilde{E}_K^{-1}(\cdot,\cdot)}\Rightarrow 1]-\Pr[A^{\tilde{\Pi}(\cdot,\cdot)\tilde{\Pi}^{-1}(\cdot,\cdot)}\Rightarrow 1].$$

其中,Π^{-1} 和 $\tilde{\Pi}^{-1}(T,\cdot)$ 分别表示Π和 $\tilde{\Pi}(T,\cdot)$ 的逆置换.记号 $\mathrm{Adv}_F^{xxx}(q,t)=\max_A\{\mathrm{Adv}_F^{xxx}(A)\}$ 表示敌手在 q 次询问和时间 t 内取得的最大优势.当 $\mathrm{Adv}_E^{prp}(q,t)$ 可忽略时,称 E 是安全的,或者抵抗选择明文攻击的;当 $\mathrm{Adv}_E^{sprp}(q,t)$ 可忽略时,称 E 是强安全的,或者抵抗选择密文攻击的;当 $\mathrm{Adv}_{\tilde{E}}^{tprp}(q,t)$ 可忽略时,称 $\tilde{E}$ 是安全的,或者抵抗选择明文攻击的;当 $\mathrm{Adv}_{\tilde{E}}^{stprp}(q,t)$ 可忽略时,称 $\tilde{E}$ 是强安全的,或者抵抗选择密文攻击的.

由定义可知,如果 $\tilde{E}$ 是(强)安全的,$K\leftarrow\{0,1\}^k$,那么 $\tilde{E}_K^T(T\in\{0,1\}^t)$ 相当于 2^t 个独立的随机置换.调柄带来的灵活性是,仅仅通过一个密钥的随机选取就得到了 2^t 个随机置换.因此,基于可调分组密码的工作模式的设计比基

于分组密码的工作模式的设计要方便得多.

1.2 加密认证模式

设 AE 是一个加密认证模式,通常 AE 是带状态的或者是随机的.带状态是指 AE 用到一个状态,每次加密前状态进行更新,如果每次使用的状态都不一样,这种状态称为现时(nonce),现时通常用一个记数器 C_{tr} 来实现,每次使用前加 1,例如 OCB,CCM,EAX,CWC 模式都用到了现时[1−3];随机的是指 AE 每次使用前先要产生一个随机比特串 *Rnd*,然后利用 *Rnd* 工作,例如,CBC 模式和其他认证模式的组合模式.这里我们统一用 N 表示 C_{tr} 或者 *Rnd*.对同一明密文对,AE 加密和解密时用到同一个 N.AE 加密时,对于明文 M 输出密文(C,σ),记为$(C,\sigma)=AE_K^N(M)$,这里的密文包含认证用的标签 σ.解密时,先对输入(C,σ)计算得到(M',σ'),记为 $(M',\sigma')=(AE_K^N)^{-1}(C,\sigma)$.如果$\sigma=\sigma'$,则认为密文是有效的,输出 M';如果$\sigma\neq\sigma'$,则认为密文是无效的,输出$\perp$.

安全的 AE 同时提供密文的机密性和完整性.概括地讲,机密性是指从密文(C,σ)得到明文 M 的信息在计算上是不可行的;完整性是指伪造有效的密文在计算上是不可行的.这里,我们将机密性定义为密文和等长的随机比特不可区分性[1].这是一个比通常的定义要强的定义.随机函数$\$$每次对任意输入输出和相应密文等长的随机比特串.对于机密性,敌手 A 的优势函数定义为

$$\mathrm{Adv}_{AE}^{priv}(A)=\Pr[A^{AE(\cdot)}\Rightarrow 1]-\Pr[A^{\$(\cdot)}\Rightarrow 1].$$

由于每次询问的消息长度可以不一样,我们用消息的总长度μ和时间对 A 进行限制.当 $\mathrm{Adv}_{AE}^{priv}(\mu,t)$ 可以忽略时,称 *AE* 提供了机密性.对于完整性,敌手 B 利用预言机 $AE(\cdot)$,输出(N,C,σ),要求(N,C,σ)不能由询问直接得到.B 的优势函数定义为

$$\mathrm{Adv}_{AE}^{auth}(B)=\Pr[AE^{-1}(B^{AE(\cdot)})\neq\perp].$$

即 B 成功伪造有效密文的概率.当 $\mathrm{Adv}_{AE}^{auth}(\mu,t)$ 可忽略时,称 AE 提供了完整性.

2 TAE 模式的描述

设 $\tilde{E}:\{0,1\}^k\times\{0,1\}^n\times\{0,1\}^n\to\{0,1\}^n$ 是一个可调分组密码,n 是偶数.以下⊕表示等长比特的异或运算,$\hat{\oplus}$ 表示非等长比特的异或运算,以左边的比特长为标准,如果右边的比特长,则从右截断,反之则在右边补 0,再做等长比特的异或运算.例如$111\hat{\oplus}10=011$,$1\hat{\oplus}100=0$.

文献[4]构造的 TAE 模式如图 1 所示.这一模式用到了一个 $n/2$ 比特的现时 N.TAE 输入 M,输出(C,σ).$i>0$ 时,调柄 T_i 是 N,i 的 $n/2-1$ 比特表示和 0 的级联:$T_i=N\|i\|0$.调柄 T_0 是 N,b 的 $n/2-1$ 比特表示和 1 的级联:$T_0=N\|b\|1$.其中 b 是输入消息的比特长度.首先将消息 M 分成 n 比特长的块,最后一块除外:$M=M_1,\ldots,M_{m-1},M_m$;然后计算相应块的密文 $C_i=\tilde{E}_K^{T_i}(M_i)$,$0<i<m$.$Len$ 是长度函数,设 $y_m=Len(M_m)$,则最后一块密文 $C_m=M_m\hat{\oplus}(\hat{E}_K^{T_m}(y_m))$.$checksum=M_1\oplus\ldots\oplus M_{m-1}\hat{\oplus}M$.最后计算 $\tilde{E}_K^{T_0}(Checksum)$,取其前$\tau$比特得到标签$\sigma$.注意到,加密过程是可逆的,解密时输入$(N,C,\sigma)$,先计算消息 M',然后计算标签σ',如果$\sigma=\sigma'$,则认为密文是有效的,输出(M',σ'),否则认为密文是无效的,输出$\perp$.

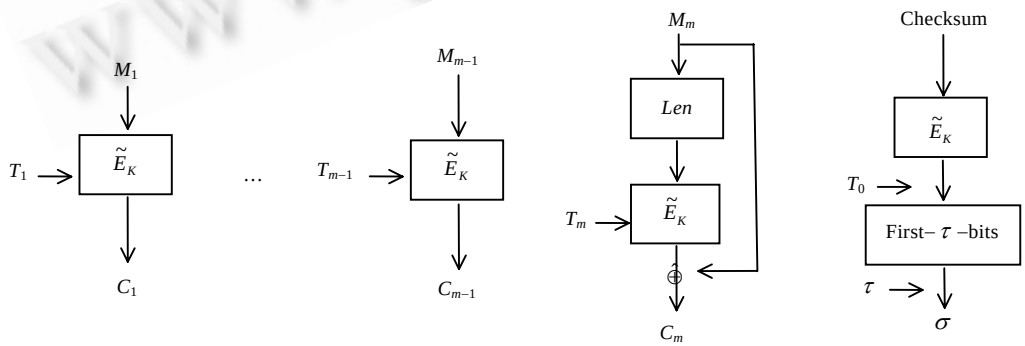

Fig.1 TAE mode

图 1 TAE 模式

3 反例和分析

Liskov 等人认为,当 $\tilde{E}$ 是安全的可调分组密码时,所构造的 TAE 模式是安全的,即同时提供了机密性和完整性.我们可以构造一个反例来说明这一结论是错误的,条件是不充分的,安全的可调分组密码不能保证密文的完整性.

设 $E:\{0,1\}^k\times\{0,1\}^n\to\{0,1\}^n$ 是一个安全的分组密码,函数 $H:\{0,1\}^n\times\{0,1\}^n\to\{0,1\}^n$,$H(h,x)=H_h(x)=h\cdot x$.其中,$\cdot$是有限域 $GF(2^n)$上的乘法.我们利用 E 和 H 构造一个可调分组密码 $T[E,H]:\{0,1\}^{k+n}\times\{0,1\}^n\times\{0,1\}^n\to\{0,1\}^n$:

$$T[E,H]^T_{K,h}(M)=E_K(M\oplus H_h(T))=E_K(M\oplus h\cdot T).$$

注意到,H_h是一个 $1/2^n$-hash 函数,即对任意的 $x,y,z\in\{0,1\}^n$,$x\neq y$,有 $\Pr[H_h(x)\oplus H_h(y)=z]\le 1/2^n$,其中 h 是随机选取的,并且 H_h 还是一个线性函数.如果我们将 $T[E,H]$的输出再和 $h\cdot T$ 做一次异或,就与文献[4]中第 3.1 节的构造相同.使用与文献[4]中定理 3 相同的方法,我们可以很容易证明如下定理:

定理 **1**. $\mathrm{Adv}^{tprp}_{T[E,H]}(q,t)\le \mathrm{Adv}^{prp}_E(q,t)+3q^2/2^n$.

也就是说,当 E 是安全的时候,$T[E,H]$也是安全的.但 $T[E,H]$不是强安全的.这是因为,如果我们取 4 个互不相同的调柄 T_1,T_2,T_3,T_4 满足 $T_1\oplus T_2\oplus T_3\oplus T_4=0^n$,则可以验证 $T^{T_4}_{K,h}=T^{T_3}_{K,h}\circ(T^{T_2}_{K,h})^{-1}\circ T^{T_1}_{K,h}$,这里$\circ$表示函数的复合.这样,我们可以利用 3 次加密询问和 1 次解密询问,将这个可调分组密码和其可调随机置换区分开.

利用 $T[E,H]$构造的 TAE 模式,记为 TAE[T].注意到,$T_4\oplus T_5\oplus T_6\oplus T_7=0^n$,如果取 $C_4=C_5=C_6=C_7=X$,则相应的明文块为 $M_4\oplus M_5\oplus M_6\oplus M_7=(Y\oplus h\cdot T_4)\oplus(Y\oplus h\cdot T_5)\oplus(Y\oplus h\cdot T_6)\oplus(Y\oplus h\cdot T_7)=0^n$,其中 $Y=E_K^{-1}(X)$.

对 TAE[T]的攻击如下:

攻击算法.

1. 对 TAE[T]询问 $M_1M_2M_3M_4M_5M_6M_7$,其中 $M_4\oplus M_5\oplus M_6\oplus M_7=0^n$,得到$(N,C_1C_2C_3C_4C_5C_6C_7,\sigma)$;
2. 伪造密文$(N,C_1C_2C_3AAAA,\sigma)$,其中 $A\notin\{C_4,C_5,C_6,C_7\}$.

设解密$(N,C_1C_2C_3AAAA,\sigma)$得到 $(M'_1M'_2M'_3M'_4M'_5M'_6M'_7,\sigma')$,则 $M'_1=M_1$, $M'_2=M_2$, $M'_3=M_3$,又由于 $M'_4\oplus M'_5\oplus M'_6\oplus M'_7=0^n$,所以 Checksum 不变,$\sigma=\sigma'$,因此密文是有效的.这样,我们仅仅利用了 1 次询问就伪造了一个有效的密文.

因此,有如下结论:

定理 **2**. 存在安全的可调分组密码,其上的 TAE 模式不提供密文的完整性.

4 改进和证明

由 TAE 模式的定义可知:

1. 所用到的可调分组密码的调柄长度 t 与明文长度 n 相同,实际上可以在一般的情况下构造.
2. 现时 N 的长度是调柄长度的一半,这时每次可加密长度小于 $2^{n/2-1}$ 块的消息,而现时 N 最多只能使用 $2^{n/2}$ 次,否则就会出现重复.实际上,N 的作用是保证所用到的调柄互不相同,其长度可以是任意的,这样可以根据实际环境决定 N 的长度.例如,当每次加密的消息都比较短时,可以选取比较长的现时.
3. 对最后一块消息的加密用到了最后一块长度的密文,实际上可以是任意常值比特的密文.

针对这 3 点,我们对 TAE 模式进行了改进,得到 MTAE(modified tweakable authenticated encryption)模式.MTAE 模式是构造在一般调柄长度 t 的可调分组密码上的,现时的长度取为 $l(0<l<t)$,可以根据实际情况决定其取值,对最后一块消息的加密用到了常值 W,因此可以预计算,提高计算效率.

设 $\tilde{E}:\{0,1\}^k\times\{0,1\}^t\times\{0,1\}^n\to\{0,1\}^n$ 是一个可调分组密码,N 是 $l(0<l<t)$比特长的现时,$i>0$ 时,调柄 T_i 是 N,i 的 $t–l–1$ 比特表示和 0 的级联:$T_i=N\|i\|0$,调柄 T_0 是 N,b 的 $t–l–1$ 比特表示和 1 的级联:$T_0=N\|b\|1$,其中 b 是输入消息的比特长度.W 是一个 n 比特的常值.$0<\tau<n$ 是标签的长度.MTAE 模式描述如下:

算法. $\mathrm{MTAE.Enc}_K^N(M)$.

将 M 分块 $M[1]\ldots M[m]$;

for $i\in\{1,\ldots,m-1\}$ do $C[i]\leftarrow \tilde{E}_K^{T_i}(M[i])$;

$Y\leftarrow \tilde{E}_K^{T_0}(W)$; $C[m]\leftarrow M[m]\hat{\oplus}Y$;

$Checksum\leftarrow M[1]\oplus\cdots\oplus M[m-1]\hat{\oplus}M[m]$;

$\mathrm{Tag}\leftarrow \tilde{E}_K^{T_0}(Checksum)$;

$\sigma\leftarrow$first$-\tau-$bits(Tag);

return (C,σ)

算法. $\mathrm{MTAE.Dec}_K^N(M)$.

将 C 分块 $C[1]\ldots C[m]$;

for $i\in\{1,\ldots,m-1\}$ do $M[i]\leftarrow(\tilde{E}_K^{T_i})^{-1}(C[i])$

$Y\leftarrow \tilde{E}_K^{T_0}(W)$; $M[m]\leftarrow C[m]\hat{\oplus}Y$;

$Checksum\leftarrow M[1]\oplus\cdots\oplus M[m-1]\hat{\oplus}M[m]$;

$\mathrm{Tag}\leftarrow \tilde{E}_K^{T_0}(Checksum)$; $\sigma'\leftarrow$first$-\tau-$bits(Tag);

if $\sigma'=\sigma$ then return M

else return $\perp$

下面证明其安全性,以下消息的总长度以块为单位.首先考虑 $\tilde{E}$ 是可调随机置换 $\tilde{\prod}$ 时的情况:

定理 **3**. 1) $\mathrm{Adv}^{priv}_{\mathrm{MTAE}[\tilde{\prod}]}(\mu,t)=0$;

2) $\mathrm{Adv}^{auth}_{\mathrm{MTAE}[\tilde{\prod}]}(\mu,t)\le 2^{n-\tau}/(2^n-1)$.

证明:由于现时 N 保证了用到的所有调柄互不相同,因此,对每一块作用的是相互独立的随机置换,每次询问输出的是随机比特,所以和随机比特的区分优势为 0,即式 1)成立.下面证明式 2)成立.假设敌手询问了 q 次,第 i 次询问用到的现时是 N^i,询问的消息是 M^i,得到的密文是(C^i,σ_i),$1\le i\le q$.然后敌手伪造(N,C,σ).我们对(N,C,σ)进行解密,看是否有$\sigma'=\sigma$.假设敌手可以对每个用过的可调随机置换的逆进行询问.在这种增强敌手的能力的情况下,我们分下面几种情况进行讨论:

1. 当 $N\ne N^i$,$1\le i\le q$ 时,$T\ne T^i$,对 Checksum 作用的是一个新的随机置换,因此 Tag 是随机的,又由于σ的长是τ,所以$\sigma'=\sigma$的概率是 $1/2^\tau$.
2. 当 $N=N^i$,$Len(C)\ne \mathrm{Len}(C^i)$时,同样有 $T\ne T^i$,$\sigma'=\sigma$的概率是 $1/2^\tau$.
3. 当 $N=N^i$,$Len(C)=\mathrm{Len}(C^i)$,$C[m]\ne C^i[m]$,$C[j]=C^i[j]$,$0<j<m$ 时,$T=T^i$,$Checksum\ne Checksum^i$,只知道随机置换 $\tilde{\prod}^{T_i}$ 一个明密文对$(Checksum^i,Tag^i)$,则 $Checksum$ 对应的 Tag 有 2^n-1 种等可能的取值.因此$\sigma'=\sigma$的概率是 $2^{n-\tau}/(2^n-1)$.
4. 当 $N=N^i$,$Len(C)=Len(C^i)$,存在 $0<j<m$,$C[j]\ne C^i[j]$时,只知道随机置换 $\tilde{\prod}^{T_i}$ 一个明密文对$(M^i[j],C^i[j])$,因此,$C[j]$对应的明文 $M[j]$有 2^n-1 种可能的取值,所以 $Checksum=Checksum^i$ 的概率不超过 $1/(2^n-1)$,$\sigma'=\sigma$的概率不超过 $2^{n-\tau}/(2^n-1)$. □

对于一般的可调分组密码 $\tilde{E}$ 有下列定理:

定理 **4**. 1) $\mathrm{Adv}^{priv}_{\mathrm{MTAE}[\tilde{E}]}(\mu,t)\le \mathrm{Adv}^{tprp}_{\tilde{E}}(\mu,t)$;

2) $\mathrm{Adv}^{auth}_{\mathrm{MTAE}[\tilde{\prod}]}(\mu,t)\le \mathrm{Adv}^{stprp}_{\tilde{E}}(\mu,t)+2^{n-\tau}/(2^n-1)$.

证明:先给出式 1)的证明.假设敌手 A 在总长为μ询问和时间 t 内取得了最佳的优势 $\mathrm{Adv}^{priv}_{\mathrm{MTAE}[\tilde{E}]}(\mu,t)$.我们利用 A 构造区分 $\tilde{E}$ 和 $\tilde{\Pi}$ 的算法 B.算法 B 用其预示机模拟 A,当 A 停止并且输出的时候,B 停止并且输出相同的值.因此,$\mathrm{Adv}^{tprp}_{\tilde{E}}(B)=\Pr[B^{\tilde{E}}\Rightarrow 1]-\Pr[B^{\tilde{\Pi}}\Rightarrow 1]=\Pr[A^{\mathrm{MTAE}[\tilde{E}]}\Rightarrow 1]-\Pr[A^{\mathrm{MTAE}[\tilde{\Pi}]}\Rightarrow 1]$,由定理 3 可知:$\Pr[A^{\mathrm{MTAE}[\tilde{\Pi}]}\Rightarrow 1]=\Pr[A^{\$}\Rightarrow 1]$,所以 $\mathrm{Adv}^{tprp}_{\tilde{E}}(B)=\Pr[A^{\mathrm{MTAE}[\tilde{E}]}\Rightarrow 1]-\Pr[A^{\$}\Rightarrow 1]=Adv^{priv}_{\mathrm{MTAE}[\tilde{E}]}(A)$,因此,式 1)成立.式 2)的证明类似.只是要注意到定理 3 中式 2)的证明给了敌手一定的解密的能力,所以式子右边是度量强安全的优势而不是度量安全的优势. □

以上定理说明,当 $\tilde{E}$ 是安全的时候,MTAE 提供了密文的机密性,当 $\tilde{E}$ 是强安全的时候,MTAE 提供了密文的完整性,当 $\tilde{E}$ 是强安全的时候,MTAE 同时提供了密文的机密性和完整性.

5 结束语

我们对 TAE 模式的安全性进行了分析,讨论了安全的条件,指出了文献[4]的错误之处.只有当可调分组密码是强安全的时候,其上的 TAE 模式才同时提供了密文的机密性和完整性.我们还对 TAE 模式进行了一些改进,

得到 MTAE 模式,并证明了其安全性.由于调柄带来的灵活性,基于可调分组密码上的其他工作模式的设计,如设计加密模式、设计认证模式,或者设计其他更为灵活、有效的加密认证模式,是一个值得研究的问题.

致谢 感谢吴文玲老师的鼓励和帮助.

References:

[1] Rogaway P, Bellare M, Black J, Krovetz T. OCB: A block-cipher mode of operation for efficient authenticated encryption. In: Samarati P, ed. Proc. of the 8th ACM Conf. on Computer and Communication Security. New York: ACM Press, 2001. 196−205.

[2] Bellare M, Rogaway P, Wagner D. The EAX mode of operation. In: Roy B, Meier W, eds. Fast Software Encryption 2004. LNCS 3017, Springer-Verlag, 2004. 389−407.

[3] Kohno T, Viega J, Whiting D. CWC: A high-performance conventional authenticated encryption mode. In: Roy B, Meier W, ed. Fast Software Encryption 2004. LNCS 3017, Springer-Verlag, 2004. 408−426.

[4] Liskvo M, Rivset RL, Wagner D. Tweakable block cipher. In: Yung M, ed. Advances in Cryptology-CRYPTO 2002. LNCS 2442, Springer-Verlag, 2002. 31−46.

[5] Crowley P. Mercy: A fast large block cipher for disk sector encryption. In: Schneier B, ed. Fast Software Encryption 2000. LNCS 1978, Springer-Verlag, 2001. 49−63.

王鹏(1976－),男,湖北黄冈人,博士生,主要研究领域为分组密码的设计和分析.

冯登国(1965－),男,研究员,博士生导师,主要研究领域为信息与网络安全.